CLIを使用した暗号化の管理

ONTAP 9

NetApp
February 12, 2026

目次

CLIを使用した暗号化の管理 1
ONTAPの保存データ暗号化について学ぶ 1
NetAppボリュームとアグリゲートの暗号化を設定する 1
ONTAP NetAppボリュームとアグリゲートの暗号化について学ぶ 1
ONTAP NetApp Volume Encryption ワークフロー 5
NVEの設定 6
NVE または NAE を使用してボリューム データを暗号化する 30
NetAppのハードウェアベースの暗号化の設定 41
ONTAP ハードウェアベース暗号化について学ぶ 41
外部キー管理の設定 44
オンボード キー管理の設定 58
ONTAP FIPSドライブにFIPS 140-2認証キーを割り当てる 65
ONTAPでKMIPサーバ接続のクラスタ全体のFIPS準拠モードを有効にする 66
NetApp Encryptionの管理 68
ONTAPでボリュームデータの暗号化を解除する 68
ONTAPで暗号化されたボリュームを移動する 69
ONTAPのvolume encryption rekey startコマンドを使用してボリュームの暗号化キーを変更する 70
ONTAP volume move startコマンドを使用してボリュームの暗号化キーを変更します 71
ONTAP NetApp Storage Encryptionの認証キーをローテーションする 72
ONTAPで暗号化されたボリュームを削除する 73
暗号化されたボリュームでのデータのセキュア パージ 74
ONTAPオンボードキー管理パスフレーズを変更する 79
ONTAPオンボードキー管理情報を手動でバックアップする 81
ONTAPでオンボードキー管理暗号化キーをリストアする 83
ONTAP外部キー管理暗号化キーを復元する 84
ONTAPクラスタ上のKMIP SSL証明書を置き換える 85
ONTAPでFIPSドライブまたはSEDを交換する 86
FIPSドライブまたはSEDのデータにアクセスできない状態にする方法 88
ONTAPで認証キーが失われた場合にFIPSドライブまたはSEDをサービスに戻す 96
ONTAP で FIPS ドライブまたは SED を非保護モードに戻す 98
ONTAPで外部キーマネージャ接続を削除する 101
ONTAP外部キー管理サーバーのプロパティを変更する 102
ONTAPでのオンボードキー管理から外部キー管理への移行 103
外部キー管理からONTAPオンボードキー管理に切り替える 104
ONTAPブートプロセス中にキー管理サーバにアクセスできない場合の動作 105
ONTAPの暗号化をデフォルトで無効にする 107

CLIを使用した暗号化の管理

ONTAPの保存データ暗号化について学ぶ

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

- NetApp Volume Encryption（NVE）を使用したソフトウェアベースの暗号化では、一度に1つのボリュームのデータ暗号化がサポートされます。
- NetApp Storage Encryption（NSE）を使用したハードウェアベースの暗号化では、データを書き込み時に暗号化するフルディスク暗号化（FDE）がサポートされます。

NetAppボリューム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。

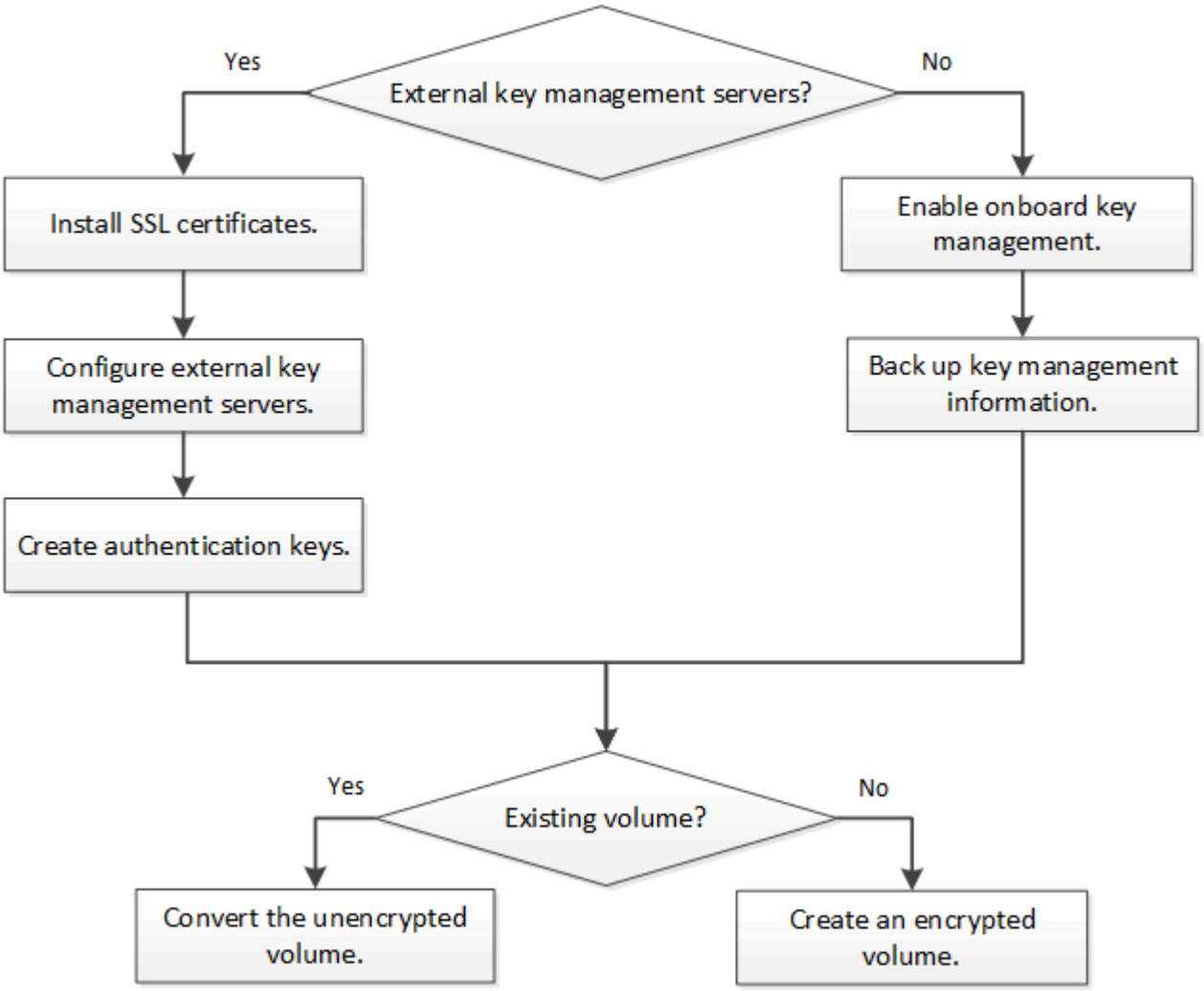
SVMスコープ	MetroClusterはONTAP 9.8以降でサポートされます。 ONTAP 9.6以降では、NVEで外部キー管理のみを対象にSVMスコープがサポートされます。オンボード キー マネージャに対してはサポートされません。
ストレージ効率	重複排除、圧縮、コンパクション、FlexClone。 クローンは、親からクローンを分割した後でも、親と同じキーを使用します。分割されたクローンに対して `volume move`を実行する必要があります。これにより、分割されたクローンのキーは異なります。
レプリケーション	• ボリュームレプリケーションでは、ソースボリュームとデスティネーショ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
   ```

   ```
   clusterl::> 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
   ```

   ```
   clusterl::> 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
   ```

NetAppのハードウェアベースの暗号化の設定

ONTAP ハードウェアベース暗号化について学ぶ

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

NetAppのハードウェアベースの暗号化について

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

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

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

自己暗号化ドライブを有効にすると、コア ダンプも暗号化されます。

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

サポートされている自己暗号化ドライブのタイプ

2種類の自己暗号化ドライブがサポートされています。

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

> 非暗号化ドライブとは、SEDでもFIPSでもないドライブです。

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

外部キー管理を使用する状況

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

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

サポートの詳細

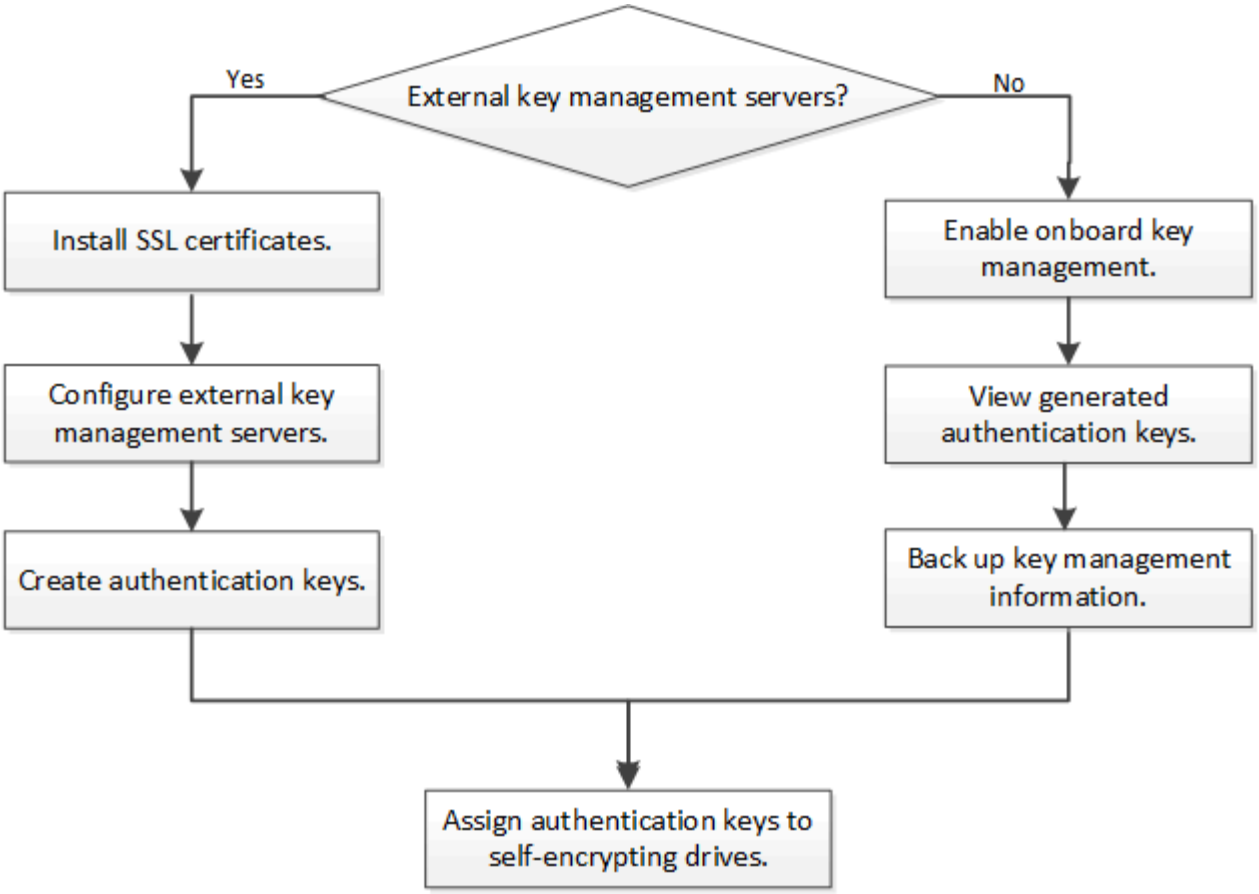
次の表に、重要なハードウェア暗号化のサポートの詳細を示します。サポート対象のKMIPサーバ、ストレージ システム、ディスク シェルフの最新情報については、Interoperability Matrixを参照してください。

リソースまたは機能	サポートの詳細

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

ハードウェアベースの暗号化のワークフロー

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



関連情報

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

外部キー管理の設定

ONTAP外部キー管理の設定について学ぶ

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

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

ONTAPクラスタにSSL証明書をインストールする

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

タスク概要

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

開始する前に

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

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

手順

1. クラスタにSSL KMIPクライアント証明書をインストールします。

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

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

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

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

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

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

関連情報

- "security certificate install"

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

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

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

開始する前に

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

手順

1. クラスタのキー管理ツールの接続を設定します。

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

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

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

```
cluster1::> security key-manager external enable -key-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

2. 設定したすべてのKMIPサーバが接続されていることを確認します。

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

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

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

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

6 entries were displayed.
```

関連情報

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

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

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

タスク概要

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

開始する前に

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

手順

1. クラスタ ノードのキー管理ツールの接続を設定します。

   ```
   security key-manager setup
   ```

キー管理ツールのセットアップが開始されます。

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

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

   `security key-manager add -address key_management_server_ipaddress`

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

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

4. 冗長性を確保するためにKMIPサーバをもう1つ追加します。

   `security key-manager add -address key_management_server_ipaddress`

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

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

5. 設定したすべてのKMIPサーバが接続されていることを確認します。

   `security key-manager show -status`

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

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

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

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

   `volume encryption conversion start`

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

ONTAPでクラスタ化された外部キーサーバを設定する

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

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

タスク概要

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

開始する前に

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

クラスタ化されたキー サーバの作成

設定手順は、プライマリ キー サーバを設定済みかどうかによって異なります。

SVMへのプライマリ キー サーバとセカンダリ キー サーバの追加

手順

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

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

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

2. プライマリ キー管理ツールを有効にします。

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

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

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

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

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

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

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

既存のプライマリ キー サーバへのセカンダリ キー サーバの追加

手順

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

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

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

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

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

クラスタ化されたキー サーバの変更

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

セカンダリ キー サーバの変更

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

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

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

プライマリ キー サーバとセカンダリ キー サーバの変換

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

プライマリキーサーバをセカンダリキーサーバに変換

手順

1. SVMからプライマリキーサーバを削除します。

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

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

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

セカンダリキーサーバをプライマリキーサーバに変換する

手順

1. 既存のプライマリキーサーバーからセカンダリキーサーバーを削除します：

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

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

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

詳細については、[mod-secondary]を参照してください。

関連情報

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

ONTAP 9.6以降での認証キーの作成

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

タスク概要

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

使用できます。

ONTAPでは、クラスタ内のすべてのノードについて認証キーが作成されます。

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

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

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

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

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. クラスタ ノードの認証キーを作成します。

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

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

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

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

2. 認証キーが作成されたことを確認します。

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

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

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

次の例では、`cluster1`の認証キーが作成されたことを確認します：

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

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

       Vserver: cluster1
   Key Manager: external
          Node: node2

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

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

関連情報

- "storage disk show | more"

ONTAP 9.5以前での認証キーの作成

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

タスク概要

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

ONTAPでは、クラスタ内のすべてのノードについて認証キーが作成されます。

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

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

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. クラスタ ノードの認証キーを作成します。

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

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

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

   次の例では、`cluster1`の認証キーを作成します：

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

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

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

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

2. 認証キーが作成されたことを確認します。

   `security key-manager query`

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

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

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

  (security key-manager query)

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

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


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

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

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

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

タスク概要

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

これはシステムの停止を伴わない手順です。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. FIPSドライブまたはSEDにデータ認証キーを割り当てます。

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

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

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

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

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

2. 認証キーが割り当てられたことを確認します。

   `storage encryption disk show`

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

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

関連情報

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

オンボード キー管理の設定

オンボード キー管理の有効化（**ONTAP 9.6**以降）

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

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

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

タスク概要

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

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

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

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

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

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

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

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

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

開始する前に

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

  "外部キー管理からオンボード キー管理への移行"

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

手順

1. キー管理ツール セットアップ コマンドを開始します。

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

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

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

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

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

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

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

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

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

終了後の操作

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

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

関連情報

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

オンボード キー管理の有効化（**ONTAP 9.5**以前）

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

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

タスク概要

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

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

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

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

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

パスフレーズの試行が失敗した場合は、ノードを再起動する必要があります。

開始する前に

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

  "外部キー管理からオンボード キー管理への移行"

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

手順

1. キー管理ツールのセットアップを開始します。

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

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

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

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

   ...

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

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

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

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

   ```
   security key-manager show-key-store
   ```

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

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

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

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

終了後の操作

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

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

関連情報

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

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

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

タスク概要

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

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. FIPSドライブまたはSEDにデータ認証キーを割り当てます。

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

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

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

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

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

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

2. 認証キーが割り当てられたことを確認します。

   `storage encryption disk show`

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

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

関連情報

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

ONTAP FIPSドライブにFIPS 140-2認証キーを割り当てる

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

タスク概要

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

これはシステムの停止を伴わない手順です。

開始する前に

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

手順

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

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

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

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

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

3. 認証キーが割り当てられたことを確認します。

   ```
   storage encryption disk show -fips
   ```

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

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

関連情報

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

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

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

タスク概要

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

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

開始する前に

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

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. TLSv1.2がサポートされていることを確認します。

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

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

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

3. クラスタ全体のFIPS準拠モードを有効にします。

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

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

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

```
security config show
```

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

NetApp Encryptionの管理

ONTAPでボリュームデータの暗号化を解除する

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

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

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

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

   `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`という名前の既存のボリュームを宛先アグリゲート`aggr3`に移動し、ボリューム上のデータを暗号化解除します：

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

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

2. ボリュームで暗号化が無効になっていることを確認します。

   `volume show -encryption`

   `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`上のボリュームが暗号化されているかどうかを表示します：

```
cluster1::> volume show -encryption

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

ONTAPで暗号化されたボリュームを移動する

`volume move start`コマンドを使用して、暗号化されたボリュームを移動できます。移動したボリュームは、同じアグリゲートまたは別のアグリゲートに配置できます。

タスク概要

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

`-encrypt-destination`オプションは、 `volume move start`暗号化されたボリュームの場合、デフォルトで`true`に設定されます。宛先ボリュームを暗号化しないことを指定する必要があるのは、ボリューム上のデータが誤って暗号化解除されないようにするためです。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

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

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

   `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`という名前の既存のボリュームを宛先アグリゲート`aggr3`に移動し、ボリューム上のデータを暗号化されたままにします（：）

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

2. ボリュームで暗号化が有効になっていることを確認します。

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

`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    aggr3     online    RW  200GB    160.0GB  20%
```

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

ボリュームの暗号化キーを定期的に変更することは、セキュリティ上のベストプラクティスです。ONTAP 9.3以降では、`volume encryption rekey start`コマンドを使用して暗号化キーを変更できます。

タスク概要

キー再生成操作を開始すると、必ず完了する必要があります。以前のキーに戻すことはできません。操作中にパフォーマンスの問題が発生した場合は、`volume encryption rekey pause`コマンドを実行して操作を一時停止し、`volume encryption rekey resume`コマンドを実行して操作を再開することができます。

キー更新操作が完了するまで、ボリュームには2つのキーが存在します。新しい書き込みとそれに対応する読み取りには新しいキーが使用されます。それ以外の場合、読み取りには古いキーが使用されます。

`volume encryption rekey start`を使用してSnapLockボリュームのキーを再設定することはできません。

手順

1. 暗号化キーを変更します。

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

   次のコマンドは、SVM`vs1`上の`vol1`の暗号化キーを変更します：

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

2. キー変更処理のステータスを確認します。

volume encryption rekey show

`volume encryption rekey show`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/volume-encryption-rekey-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、キー再生成操作のステータスを表示します：

```
cluster1::> volume encryption rekey show

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

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

volume show -is-encrypted true

`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%
```

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

セキュリティ上のベストプラクティスとして、ボリュームの暗号化キーを定期的に変更することをお勧めします。 `volume move start`コマンドを使用して暗号化キーを変更できます。移動したボリュームは、同じアグリゲート上にあっても、別のアグリゲート上にあっても構いません。

タスク概要

`volume move start`を使用してSnapLockまたは
FlexGroupボリュームのキーを再設定することはできません。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. 既存のボリュームを移動し、暗号化キーを変更します。

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

   `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**`という名前の既存のボリュームを宛先アグリゲート`**aggr2**`に移動し、暗号化キーを変更します：

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

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

2. ボリュームで暗号化が有効になっていることを確認します。

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

   `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%
   ```

ONTAP NetApp Storage Encryptionの認証キーをローテーションする

NetApp Storage Encryption（NSE）を使用する場合、認証キーをローテーションすることができます。

タスク概要

外部キー管理ツール（KMIP）を使用している場合、NSE環境での認証キーのローテーションがサポートされます。

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

手順

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

   認証キーを変更する前に、新しい認証キーを生成しておく必要があります。

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

関連情報

- "ストレージ暗号化ディスクの変更"

ONTAPで暗号化されたボリュームを削除する

`volume delete`コマンドを使用して暗号化されたボリュームを削除できます。

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。
- ボリュームはオフラインである必要があります。

手順

1. 暗号化されたボリュームを削除します。

   `volume delete -vserver SVM_name -volume volume_name`

   `volume delete`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/volume-delete.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、`vol1`という名前の暗号化されたボリュームを削除します：

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

   削除の確認を求められたら `yes`を入力します。

   24時間後にボリュームの暗号化キーが削除されます。

   `volume delete`と `-force true`オプションを使用して、ボリュームを削除し、対応する暗号化キーを直ちに破棄します。このコマンドには高度な権限が必要です。 `volume delete`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/volume-delete.html["ONTAPコマンド リファレンス"^]を参照してください。

終了後の操作

`volume delete`コマンドを発行した後、保持期間中に `volume recovery-queue`コマンドを使用して削除されたボリュームを回復できます：

```
volume recovery-queue SVM_name -volume volume_name
```

"ボリュームリカバリ機能の使い方"

暗号化されたボリュームでのデータのセキュア パージ

暗号化された**ONTAP**ボリュームからデータを安全に消去する方法について説明します。

ONTAP 9.4以降では、セキュアパージを使用して、NVE対応ボリューム上のデータを無停止でスクラブできます。暗号化されたボリューム上のデータをスクラブすることで、例えばブロックの上書き時にデータの痕跡が残ってしまう「スピレッジ」が発生した場合や、退去するテナントのデータを安全に削除する場合など、物理メディアからのデータの復元を不可能にすることができます。

セキュア パージの対象となるのは、NVE対応ボリューム上で以前に削除されたファイルだけです。暗号化されていないボリュームはスクラビングできません。キーの提供には、オンボード キー マネージャではなく、KMIPサーバを使用する必要があります。

セキュア パージを使用する場合の考慮事項

- NetApp Aggregate Encryption（NAE）が有効になっているアグリゲートに作成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。
- セキュア パージの対象となるのは、NVE対応ボリューム上で以前に削除されたファイルだけです。
- 暗号化されていないボリュームはスクラビングできません。
- キーの提供には、オンボード キー マネージャではなく、KMIPサーバを使用する必要があります。

セキュア パージの動作は、ONTAPのバージョンによって異なります。

ONTAP 9.8以降

- セキュア パージはMetroClusterとFlexGroupでサポートされます。
- パージするボリュームがSnapMirror関係のソースである場合、セキュア パージを実行するためにSnapMirror関係を解除する必要はありません。
- 再暗号化の方法は、SnapMirrorデータ保護（DP）を使用するボリュームと使用しないボリューム、またはSnapMirror拡張データ保護を使用するボリュームとで異なります。
  - SnapMirrorデータ保護（DP）モードを使用するボリュームでは、デフォルトでボリューム移動方式を使用してデータが再暗号化されます。
  - SnapMirrorデータ保護を使用しないボリュームまたはSnapMirror拡張データ保護（XDP）モードを使用するボリュームでは、インプレース再暗号化方式がデフォルトで使用されます。
  - これらのデフォルトは `secure purge re-encryption-method [volume-move|in-place-rekey]`コマンドを使用して変更できます。
- デフォルトでは、FlexVolボリューム内のすべてのスナップショットは、セキュアパージ操作中に自動的に削除されます。デフォルトでは、FlexGroupボリューム内のスナップショットおよびSnapMirrorデータ保護を使用しているボリューム内のスナップショットは、セキュアパージ操作中に自動的に削除されません。これらのデフォルトは、 `secure purge delete-all-snapshots [true|false]`コマンドを使用して変更できます。

ONTAP 9.7以前

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

  ボリューム内に使用中のスナップショットがある場合は、ボリュームをパージする前にスナップショットを解放する必要があります。たとえば、FlexCloneボリュームを親ボリュームから分割する必要がある場合などです。

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

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

暗号化された**ONTAP**ボリュームから**SnapMirror**関係なしでデータを消去する

ONTAP 9.4 以降では、 secure-purge を使用して、 NVE 対応ボリューム上のデータを中断せずに「スクラブ」することができます。

タスク概要

セキュアパージは、削除されたファイルのデータ量に応じて、数分から数時間かかる場合があります。 `volume encryption secure-purge show`コマンドを使用して、操作のステータスを表示できます。 `volume

encryption secure-purge abort`コマンドを使用して、操作を終了できます。

> SANホストでセキュアパージを実行するには、パージ対象のファイルを含むLUN全体を削除するか、パージ対象のファイルに属するブロックのLUNにパンチホールを作成できる必要があります。LUNを削除できない場合、またはホストOSがLUNのパンチホール作成をサポートしていない場合は、セキュアパージを実行できません。

開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- このタスクを実行するにはadvanced権限が必要です。

手順

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

   ```
   set -privilege advanced
   ```

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

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

4. 削除したファイルのセキュア パージを実行します。

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

   次のコマンドは、SVM`vs1`上の `vol1`で削除されたファイルを安全に消去します：

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

5. セキュア パージ処理のステータスを確認します。

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

SnapMirror非同期関係を持つ暗号化された **ONTAP** ボリュームからデータをスクラブする

ONTAP 9.8 以降では、セキュア パージを使用して、SnapMirror 非同期関係にある NVE 対応ボリューム上のデータを中断することなく「スクラブ」することができます。

開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- このタスクを実行するにはadvanced権限が必要です。

タスク概要

セキュアパージは、削除されたファイルのデータ量に応じて、数分から数時間かかる場合があります。 `volume encryption secure-purge show`コマンドを使用して、操作のステータスを表示できます。 `volume encryption secure-purge abort`コマンドを使用して、操作を終了できます。

SANホストでセキュアパージを実行するには、パージ対象のファイルを含むLUN全体を削除するか、パージ対象のファイルに属するブロックのLUNにパンチホールを作成できる必要があります。LUNを削除できない場合、またはホストOSがLUNのパンチホール作成をサポートしていない場合は、セキュアパージを実行できません。

手順

1. ストレージ システムで、advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

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

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

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

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

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

5. セキュア パージを実行するファイルがベースSnapshotに含まれている場合は、次の手順を実行します。
   a. SnapMirror非同期関係の宛先ボリュームにSnapshotを作成します：

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

   b. SnapMirrorを更新してベーススナップショットを前進させる：

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

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

   a. 手順（a）と（b）を、ベースSnapshotの数に1を加えた回数だけ繰り返します。

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

   b. ベーススナップショットが存在することを確認します：+
   `snapshot show -vserver SVM_name -volume volume_name`

c. ベーススナップショットを削除します：+
`snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot`

6. 削除したファイルのセキュア パージを実行します。

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

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

次のコマンドは、SVM “vs1” 上の “vol1” 上の削除されたファイルを安全に消去します：

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

7. セキュア パージ処理のステータスを確認します。

`volume encryption secure-purge show`

関連情報

- "snapmirror update"

SnapMirror同期関係を持つ暗号化された **ONTAP** ボリュームからデータをスクラブする

ONTAP 9.8以降では、セキュア パージを使用して、SnapMirror同期関係にあるNVE対応ボリュームのデータを無停止で「スクラビング」できます。

タスク概要

セキュアパージは、削除されたファイルのデータ量に応じて、完了までに数分から数時間かかる場合があります。 `volume encryption secure-purge show`コマンドを使用して操作のステータスを確認できます。 `volume encryption secure-purge abort`コマンドを使用して操作を終了できます。

SANホストでセキュアパージを実行するには、パージ対象のファイルを含むLUN全体を削除するか、パージ対象のファイルに属するブロックのLUNにパンチホールを作成できる必要があります。LUNを削除できない場合、またはホストOSがLUNのパンチホール作成をサポートしていない場合は、セキュアパージを実行できません。

開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- このタスクを実行するにはadvanced権限が必要です。

手順

1. ストレージ システムで、advanced権限レベルに切り替えます。

`set -privilege advanced`

2. セキュア パージを実行するファイルまたはLUNを削除します。
   - NASクライアントで、セキュア パージを実行するファイルを削除します。

- SANホストで、セキュア パージを実行するLUNを削除するか、パージするファイルに属するブロックに対してLUNでホール パンチングを実行します。

3. 非同期関係のデスティネーション ボリュームでセキュア パージを準備します。

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

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

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

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

5. 対象ファイルがベースSnapshotまたは共通Snapshotに含まれている場合は、SnapMirrorを更新して共通Snapshotを最新の状態にします。

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

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

6. セキュア パージ ファイルがアプリケーション整合性スナップショット内にある場合は、SnapMirror 同期関係にある両方のボリューム上のスナップショットを削除します：

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

   この手順は両方のボリュームで実行します。

7. 削除したファイルのセキュア パージを実行します。

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

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

   次のコマンドは、SVM "`vs1`"上の"`vol1`"上の削除されたファイルを安全に消去します。

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

8. セキュア パージ処理のステータスを確認します。

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

関連情報

- "snapmirror update"

ONTAPオンボードキー管理パスフレーズを変更する

NetAppでは、オンボードキー管理パスフレーズを定期的に変更することを推奨していま

す。新しいパスフレーズは、ストレージシステム外の安全な場所に保管する必要があります。

開始する前に

- このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。
- このタスクを実行するにはadvanced権限が必要です。
- MetroCluster環境では、ローカル クラスタでパスフレーズを更新した後、パートナー クラスタでパスフレーズの更新を同期します。

手順

1. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. オンボードキー管理パスフレーズを変更します。使用するコマンドは、実行している ONTAP のバージョンによって異なります。

   ONTAP 9.6以降

   ```
   security key-manager onboard update-passphrase
   ```

   ONTAP 9.5以前

   ```
   security key-manager update-passphrase
   ```

3. 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。

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. MetroCluster構成の場合は、パートナー クラスタで更新されたパスフレーズを同期します。
   a. ONTAPバージョンに適したコマンドを選択して、パートナー クラスタのパスフレーズを同期します：

ONTAP 9.6以降

```
security key-manager onboard sync
```

ONTAP 9.5以前

- ONTAP 9.5 では、次のコマンドを実行します。

  ```
  security key-manager setup -sync-metrocluster-config
  ```

- ONTAP 9.4 以前では、ローカル クラスタでパスフレーズを更新した後、20 秒待ってから、パートナー クラスタで次のコマンドを実行します：

  ```
  security key-manager setup
  ```

b. プロンプトが表示されたら、新しいパスフレーズを入力します。

   両方のクラスターで同じパスフレーズを使用する必要があります。

終了後の操作

将来使用するために、オンボード キー管理パスフレーズをストレージ システム外部の安全な場所にコピーします。

オンボードキー管理パスフレーズを変更するたびに、キー管理情報を手動でバックアップします。

関連情報

- "オンボード キー管理情報の手動バックアップ"
- "セキュリティキー・マネージャーオンボードのパスフレーズ更新"

ONTAPオンボードキー管理情報を手動でバックアップする

オンボード キー マネージャのパスフレーズを設定するときは必ず、オンボード キー管理情報をストレージ システム外部の安全な場所にコピーする必要があります。

開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- このタスクを実行するにはadvanced権限が必要です。

タスク概要

すべてのキー管理情報は、クラスターの複製データベース（RDB）に自動的にバックアップされます。災害発生時に備えて、キー管理情報を手動でバックアップすることも必要です。

手順

1. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. クラスターのキー管理バックアップ情報を表示します：

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

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

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

     --------------------------BEGIN BACKUP--------------------------
     TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAAADuD+byAAAAACEAAAAAAAA
     QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
     dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAAACgAAAAAAAAAAA
     3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAAAA
     IgAAAAAAAAAAoAAAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAAAAJAGr3tJA/LRzU
     QRHwv+1aWvAAAAAAAAAAAACQAAAAAAAAAAAgAAAAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
     BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
     AQAAAAMAAAAYAQAAAAAAAADA5/ccAAAAAIgAAAAAAAAAAoAAAAAAAAAAAEOTcR0AAAAA
     AAAAAAAAAAACAAAAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAAACIAAAAAAAAAA
     KAAAAAAAAAACI8z/bAAAAAAAAAAAAAAAAAAgAAAAAAAAAQAbxMcI4qiaMS4Uts5tTUnU
     AAAAAAAAAAAkAAAAAAAAAAAIAAAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5Smyj
     LSgoK/qc8FAmMMcrRXY6uriulnL0WPB/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAwAAABgBAAAAAAAAAA
     1cNLLwAAAAAiAAAAAAAAAAACgAAAAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAAAAIAAAAAAAAAkA
     ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAAAIgAAAAAAAAAAAoAAAAAAAAAAAJ4/cQsAAAAA
     AAAAAAAAAAACAAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAAAAAACQAAAAAAAAAA
     gAAAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rrH4nPQM0n
     rDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     ---------------------------END BACKUP---------------------------
```

3. 災害発生時に使用するために、バックアップ情報をストレージ システム外部の安全な場所にコピーします。

関連情報

- "security key-manager onboard show-backup"
- "security key-manager backup show"

ONTAPでオンボードキー管理暗号化キーをリストアする

場合によっては、オンボードキー管理暗号化キーを復元する必要があります。キーの復元が必要であることを確認したら、オンボードキーマネージャを設定してキーを復元できます。オンボードキー管理暗号化キーの復元手順は、ONTAPのバージョンによって異なります。

開始する前に

- NSEを外部KMIPサーバーと併用する場合は、外部キーマネージャーデータベースを削除してください。詳細については、"外部キー管理からONTAPオンボードキー管理への移行"を参照してください。
- このタスクを実行するには、クラスタ管理者である必要があります。

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

ONTAP 9.6以降

> ONTAP 9.8以降を実行していて、ルートボリュームが暗号化されている場合は、[ontap-9-8]の手順に従ってください。

1. キーを復元する必要があることを確認します：+
`security key-manager key query -node node`

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

2. キーを復元する：+
`security key-manager onboard sync`

> `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-sync.html["ONTAPコマンド リファレンス
> "^]を参照してください。

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

ONTAP 9.8以降でルート ボリュームが暗号化されている場合

ONTAP 9.8以降を実行していてルート ボリュームが暗号化されている場合は、ブート メニューを使用してオンボード キー管理のリカバリ パスフレーズを設定する必要があります。ブート メディアを交換する場合にも、このプロセスが必要です。

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

   バックアップキーデータを入力すると、ノードはブートメニューに戻ります。

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

ONTAP 9.5以前

1. キーを復元する必要があることを確認します：+
   `security key-manager key show`
2. キーを復元する：+
   `security key-manager setup -node node`

   `security key-manager setup`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli-9161/security-key-manager-setup.html["ONTAPコマンド リファレンス"^]を参照してください。

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

ONTAP外部キー管理暗号化キーを復元する

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

タスク概要

ONTAP 9.6 以降では、 `security key-manager key query -node node_name`コマンドを使用して、キーを復元する必要があるかどうかを確認できます。

ONTAP 9.5 以前では、 `security key-manager key show`コマンドを使用して、暗号化キーを復元する必要があるかどうかを確認できます。

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

`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。

開始する前に

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

手順

1. ONTAP 9.8以降を実行していてルート ボリュームが暗号化されている場合は、次の手順を実行します。

   ONTAP 9.7以前を実行している場合、またはONTAP 9.8以降を実行していてルート ボリュームが暗号化されていない場合は、この手順を省略してください。

   a. ブート引数を設定します：+
   ```
   setenv kmip.init.ipaddr <ip-address>
   setenv kmip.init.netmask <netmask>
   setenv kmip.init.gateway <gateway>
   setenv kmip.init.interface e0M
   boot_ontap
   ```

   b. ノードをブートメニューにブートし、オプション `(11) Configure node for external key management` を選択します。

   c. プロンプトに従って管理証明書を入力します。

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

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

2. キーをリストアします。

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

   `node`デフォルトではすべてのノードが対象になります。

   このコマンドは、オンボード キー管理が有効な場合はサポートされません。

   次のONTAP 9.6コマンドは、外部キー管理認証キーを `cluster1`のすべてのノードに復元します：

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

関連情報

- "セキュリティキー・マネージャ外部リストア"

ONTAPクラスタ上のKMIP SSL証明書を置き換える

すべてのSSL証明書には有効期限があります。認証キーへのアクセスが失われないよう

に、証明書の有効期限が切れる前に証明書を更新する必要があります。

開始する前に

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

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

手順

1. 新しいKMIPサーバCA証明書をインストールします。

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

2. 新しいKMIPクライアント証明書をインストールします。

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

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

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

   MetroCluster環境でONTAP 9.6以降を実行している場合に管理SVMのキー管理ツールの設定を変更するには、構成内の両方のクラスタでコマンドを実行する必要があります。

新しくインストールされた証明書を使用するようにキーマネージャーの設定を更新すると、新しいクライアント証明書の公開鍵/秘密鍵が以前にインストールされた鍵と異なる場合、エラーが返されます。このエラーを回避する方法については、"NetAppナレッジベース：新しいクライアント証明書の公開鍵または秘密鍵が既存のクライアント証明書と異なります"をご覧ください。

関連情報

- "security certificate install"
- "セキュリティキー・マネージャ外部変更"

ONTAPでFIPSドライブまたはSEDを交換する

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

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

開始する前に

- ドライブで使用される認証キーのキーIDを確認しておく必要があります。
- このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. ディスクが障害状態とマークされていることを確認します。

   ```
   storage disk show -broken
   ```

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

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

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

   ```
   storage disk assign -disk disk_name -owner node
   ```

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

```
cluster1::> storage disk assign -disk 2.1.1 -owner cluster1-01
```

4. 新しいディスクが割り当てられていることを確認します。

   `storage encryption disk show`

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

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
------------------------------------------------------------------------
0.0.0   data <id_value>
0.0.1   data <id_value>
1.10.0  data <id_value>
1.10.1  data <id_value>
2.1.1   open 0x0
[...]
```

5. FIPSドライブまたはSEDにデータ認証キーを割り当てます。

   "FIPSドライブまたはSEDへのデータ認証キーの割り当て（外部キー管理）"

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

   "FIPSドライブへのFIPS 140-2認証キーの割り当て"

関連情報

- "storage disk assign"
- "storage disk show"
- "storage disk show | more"

FIPSドライブまたはSEDのデータにアクセスできない状態にする方法

FIPSドライブまたは**SED**上の**ONTAP**データをアクセス不能にする方法について学習します

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

- ディスク完全消去

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

- ディスクの破棄

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

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

ONTAPで**FIPS**ドライブまたは**SED**を完全消去する

FIPS ドライブまたは SED 上のデータを永続的にアクセス不能にし、そのドライブを新しいデータ用に使用する場合は、 `storage encryption disk sanitize` コマンドを使用してドライブをサニタイズできます。

タスク概要

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

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. 保持しておく必要があるデータを別のディスクのアグリゲートにすべて移行します。
2. 完全消去するFIPSドライブまたはSEDのアグリゲートを削除します。

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

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

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

3. 完全消去するFIPSドライブまたはSEDのディスクIDを確認します。

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

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

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

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

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

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

```
cluster1::> storage encryption disk modify -disk 1.10.2 -fips-key-id 0x0

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

5. ドライブを完全消去します。

```
storage encryption disk sanitize -disk disk_id
```

このコマンドは、ホットスペアディスクまたは破損ディスクのみをサニタイズするために使用できます。ディスクの種類に関係なくすべてのディスクをサニタイズするには、 `-force-all-state`オプションを使用してください。 `storage encryption disk sanitize`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。

続行する前に、ONTAPから確認フレーズの入力を求められます。画面に表示されたフレーズを正確に入力します。

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

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

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

6. サニタイズされたディスクをアンフェイルします：
`storage disk unfail -spare true -disk disk_id`
7. ディスクに所有者がいるかどうかを確認します：
`storage disk show -disk disk_id`ディスクに所有者がいない場合は、所有者を割り当てます。
`storage disk assign -owner node -disk disk_id`
8. 完全消去するディスクを所有するノードのノードシェルに切り替えます。

   `system node run -node node_name`

   `disk sanitize release`コマンドを実行します。

9. ノードシェルを終了します。ディスクの障害を再度解除します：
`storage disk unfail -spare true -disk disk_id`
10. ディスクがスペアになり、アグリゲート内で再利用できる状態になっていることを確認します：
`storage disk show -disk disk_id`

関連情報

- "storage disk assign"
- "storage disk show"
- "ストレージディスクのアンフェイル"
- "ストレージ暗号化ディスクの変更"
- "ストレージ暗号化ディスク完全消去"
- "storage encryption disk show-status"

ONTAPで**FIPS**ドライブまたは**SED**を破棄する

FIPS ドライブまたは SED 上のデータを永続的にアクセス不能にし、ドライブを再利用する必要がない場合は、 `storage encryption disk destroy`コマンドを使用してディスクを破棄できます。

タスク概要

FIPSドライブまたはSEDを破壊すると、システムはディスク暗号化キーを未知のランダム値に設定し、ドラ

イブを不可逆的にロックします。これにより、ディスクは事実上使用できなくなり、ディスク上のデータにも永久にアクセスできなくなります。ただし、ディスクのラベルに記載されている物理セキュアID（PSID）を使用して、ディスクを工場出荷時の設定にリセットすることができます。詳細については、"認証キーが失われた場合にFIPSドライブまたはSEDを使用可能な状態に戻す"をご覧ください。

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

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. 保持しておく必要があるデータを別のディスクのアグリゲートにすべて移行します。
2. 破棄する FIPS ドライブまたは SED 上のアグリゲートを削除します：

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

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

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

3. 破棄する FIPS ドライブまたは SED のディスク ID を特定します：

   ```
   storage encryption disk show
   ```

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

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

4. ディスクを破壊します：

   ```
   storage encryption disk destroy -disk disk_id
   ```

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

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

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

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

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

関連情報

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

ONTAPの**FIPS**ドライブまたは**SED**で緊急データ消去を実行

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

開始する前に

- 使用しているKMIPサーバに給電されていない場合は、KMIPサーバに簡単に破棄できる認証アイテム（スマート カードやUSBドライブなど）が設定されている必要があります。
- このタスクを実行するには、クラスタ管理者である必要があります。

手順

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

状況	操作

ストレージ システムに給電されており、ストレージ システムを適切な手順でオフラインにする時間がある	a. ストレージ システムがHAペアとして設定されている場合は、テイクオーバーを無効にします。
	b. すべてのアグリゲートをオフラインにしてから削除します。
	c. 権限レベルを詳細に設定します：+
	`set -privilege advanced`
	d. ドライブが FIPS 準拠モードの場合は、ノードの FIPS 認証キー ID をデフォルトの MSID に戻します：+
	`storage encryption disk modify -disk * -fips-key-id 0x0`
	e. ストレージ システムを停止します。
	f. メンテナンス モードでブートします。
	g. ディスクを完全消去するか破棄します。
	◦ ディスク上のデータにアクセスできないようにしながらもディスクを再利用できるようにするには、ディスクをサニタイズします：+
	`disk encrypt sanitize -all`
	◦ ディスク上のデータにアクセスできないようにし、ディスクを保存する必要がない場合は、ディスクを破棄します：
	`disk encrypt destroy disk_id1 disk_id2 …`
		ストレージ システムに給電されており、データをただちにシュレッディングする必要がある

a. ディスク上のデータにアクセスできないようにしながらもディスクを再利用できるようにするには、ディスクをサニタイズします：
b. ストレージ システムがHAペアとして設定されている場合は、テイクオーバーを無効にします。
c. 権限レベルをadvancedに設定します。
`set -privilege advanced`
d. ドライブがFIPS準拠モードの場合は、ノードのFIPS認証キーIDをデフォルトのMSIDに戻します。
`storage encryption disk modify -disk * -fips-key-id 0x0`
e. ディスクをサニタイズします：
`storage encryption disk sanitize -disk * -force-all-states true`
	a. ディスク上のデータにアクセスできないようにし、ディスクを保存する必要がない場合は、ディスクを破壊します：
	b. ストレージ システムがHAペアとして設定されている場合は、テイクオーバーを無効にします。
	c. 権限レベルをadvancedに設定します。
	`set -privilege advanced`
	d. ディスクを破壊します：
	`storage encryption disk destroy -disk * -force-all-states true`
		ストレージ システムがパニック状態になります。これで、ストレージ システムは永続的に無効な状態になり、すべてのデータが消去されます。システムを再度使用するには、再設定する必要があります。

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

関連情報

- "ストレージ暗号化ディスク破壊"
- "ストレージ暗号化ディスクの変更"
- "ストレージ暗号化ディスク完全消去"

ONTAPで認証キーが失われた場合にFIPSドライブまたはSEDをサービスに戻す

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

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

タスク概要

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

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

> ディスクのパーティションを解除するコマンドは、diagレベルでのみ使用可能であり、NetAppサポートの監督下でのみ実行する必要があります。続行する前に**NetApp**サポートに連絡することを強くお勧めします。"NetAppナレッジベース：ONTAPでスペアドライブのパーティション化を解除する方法"を参照することもできます。

手順

1. FIPSドライブまたはSEDを使用可能な状態に戻します。

SEDS が…	次の手順を使用します…

FIPS準拠モードでない、またはFIPS準拠モードでFIPSキーを使用できる	a. 権限レベルをadvancedに設定します：
	`set -privilege advanced`
	b. FIPS キーをデフォルトの製造元セキュア ID 0x0 にリセットします：
	`storage encryption disk modify -fips-key-id 0x0 -disk disk_id`
	c. 操作が成功したことを確認します：
	`storage encryption disk show-status`操作が失敗した場合は、このトピックの PSID プロセスを使用します。
	d. 壊れたディスクをサニタイズする：
	`storage encryption disk sanitize -disk disk_id`次の手順に進む前に、コマンド `storage encryption disk show-status`で操作が成功したことを確認します。
	e. サニタイズされたディスクをアンフェイルします：
	`storage disk unfail -spare true -disk disk_id`
	f. ディスクに所有者がいるかどうかを確認します：
	`storage disk show -disk disk_id`ディスクに所有者がいない場合は、所有者を割り当てます。
	`storage disk assign -owner node -disk disk_id`
	i. 完全消去するディスクを所有するノードのノードシェルに切り替えます。
	`system node run -node node_name`
	`disk sanitize release`コマンドを実行します。
	g. ノードシェルを終了します。ディスクの障害を再度解除します：
	`storage disk unfail -spare true -disk disk_id`
	h. ディスクがスペアになり、アグリゲート内で再利用できる状態になっていることを確認します：
	`storage disk show -disk disk_id`

FIPS準拠モードであるがFIPSキーは使用できず、SEDのPSIDがラベルに印刷されている	a. ディスクのPSIDをディスク ラベルで確認します。
	b. 権限レベルをadvancedに設定します：
	`set -privilege advanced`
	c. ディスクを工場出荷時の設定にリセットします：
	`storage encryption disk revert-to-original-state -disk *disk_id* -psid *disk_physical_secure_id*`次の手順に進む前に、コマンド`storage encryption disk show-status`で操作が成功したことを確認します。
	d. ONTAP 9.8P5以前を実行している場合は、次の手順に進んでください。ONTAP 9.8P6以降を実行している場合は、サニタイズされたディスクの障害を解除してください。
	`storage disk unfail -disk *disk_id*`
	e. ディスクに所有者がいるかどうかを確認します：
	`storage disk show -disk *disk_id*`ディスクに所有者がいない場合は、所有者を割り当てます。
	`storage disk assign -owner node -disk *disk_id*`
	i. 完全消去するディスクを所有するノードのノードシェルに切り替えます。
	`system node run -node *node_name*`
	`disk sanitize release`コマンドを実行します。
	f. ノードシェルを終了します。ディスクの障害を再度解除します：
	`storage disk unfail -spare true -disk *disk_id*`
	g. ディスクがスペアになり、アグリゲート内で再利用できる状態になっていることを確認します：
	`storage disk show -disk *disk_id*`

関連情報

- "ストレージ暗号化ディスクの変更"
- "ストレージ暗号化ディスクの元の状態へのリバート"
- "ストレージ暗号化ディスク完全消去"
- "storage encryption disk show-status"

ONTAP で FIPS ドライブまたは SED を非保護モードに戻す

FIPSドライブまたはSEDは、ノードの認証キーIDがデフォルト以外の値に設定されている場合にのみ、不正アクセスから保護されます。`storage encryption disk modify`コマンドを使用してキーIDをデフォルトに設定することで、FIPSドライブまたはSEDを非保護モードに戻すことができます。非保護モードのFIPSドライブまたはSEDはデフォルトの暗号化キーを使用し、保護モードのFIPSドライブまたはSEDは提供された秘密の暗号化キーを使用します。ドライブ上に暗号化されたデータが存在する場合、ドライブを非保

護モードにリセットしても、データは暗号化されたままであり、漏洩することはありません。

> FIPSドライブまたはSEDが非保護モードに戻った後、暗号化されたデータにアクセスできないようにするには、以下の手順に従ってください。FIPSとデータキーIDがリセットされると、元のキーを復元しない限り、既存のデータは復号化できなくなり、アクセスできなくなります。

HAペアでSASドライブまたはNVMeドライブ（SED、NSE、FIPS）の暗号化を使用している場合は、システムを初期化（ブート オプション4または9）する前に、HAペア内のすべてのドライブに対してこのプロセスを実行しておく必要があります。この手順を実行しないと、将来ドライブを転用した場合にデータが失われる可能性があります。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

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

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

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

   ```
   cluster1::> storage encryption disk modify -disk 2.10.11 -fips-key-id
   0x0

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

   次のコマンドを使用して、処理が成功したことを確認します。

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

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

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

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

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

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

   SAS ドライブまたは NVMe ドライブを非保護モードに戻す場合は、 `-data-key-id`の値を 0x0 に設定する必要があります。

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

```
cluster1::> storage encryption disk modify -disk 2.10.11 -data-key-id
0x0

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

   次のコマンドを使用して、処理が成功したことを確認します。

   `storage encryption disk show-status`

   数値が同じになるまで、show-statusコマンドを繰り返します。「disks begun」と「disks done」の数値が同じになったら、操作は完了です。

メンテナンスモード

ONTAP 9.7以降では、FIPSドライブのキー変更をメンテナンス モードから行うことができます。メンテナンス モードは、前のセクションに記載したONTAP CLIの手順を実行できない場合にのみ使用してください。

手順

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

   `disk encrypt rekey_fips 0x0 disklist`

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

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

3. FIPS認証キーが正常に変更されたことを確認します。

   ```
   disk encrypt show_fips
   ```

4. 次のコマンドを使用して、データ認証キーが正常に変更されたことを確認します。

   ```
   disk encrypt show
   ```

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

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

関連情報

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

ONTAPで外部キーマネージャ接続を削除する

KMIPサーバが不要になったときはノードから切断できます。たとえば、ボリューム暗号化に移行する場合はKMIPサーバを切断できます。

タスク概要

HAペアのいずれかのノードからKMIPサーバを切断すると、自動的にすべてのクラスタ ノードからサーバが切断されます。

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

開始する前に

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

手順

1. 現在のノードからKMIPサーバを切断します。

ONTAPバージョン	使用するコマンド
ONTAP 9.6以降	`security key-manager external remove-servers -vserver SVM -key -servers host_name

IP_address:port,…`	ONTAP 9.5以前

MetroCluster環境では、これらのコマンドを管理SVMの両方のクラスタで実行する必要があります。

次のONTAP 9.6コマンドは、 `cluster1`の2つの外部キー管理サーバへの接続を無効にします。最初のサーバは `ks1`という名前で、デフォルトポート5696でリッスンしており、2番目のサーバはIPアドレス10.0.0.20で、ポート24482でリッスンしています：

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

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

ONTAP外部キー管理サーバーのプロパティを変更する

ONTAP 9.6 以降では、 `security key-manager external modify-server`コマンドを使用して外部キー管理サーバの I/O タイムアウトとユーザ名を変更できます。

開始する前に

- このタスクを実行するには、クラスタ管理者またはSVMの管理者である必要があります。
- このタスクを実行するにはadvanced権限が必要です。
- MetroCluster環境では、この手順を管理SVMの両方のクラスタで実行する必要があります。

手順

1. ストレージ システムで、advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. クラスタの外部キー管理サーバのプロパティを変更します。

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

   タイムアウト値は秒単位で指定します。ユーザー名を変更すると、新しいパスワードの入力を求められます。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*`デフォルトで現在のクラスタの管理SVMが使用されます。外部キー管理サーバのプロパティを変更するには、クラスタ管理者である必要があります。

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

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

3. SVMの外部キー管理サーバのプロパティを変更します（NVEのみ）。

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

   > タイムアウト値は秒単位で指定します。ユーザー名を変更すると、新しいパスワードの入力を求められます。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に設定されます。外部キーマネージャサーバのプロパティを変更するには、クラスタまたはSVM管理者である必要があります。

   次のコマンドは、デフォルトポート5696でリッスンしている `svm1`外部キー管理サーバーのユーザー名とパスワードを変更します：

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

4. 最後の手順をその他のSVMに対して繰り返します。

関連情報

- "セキュリティキー・マネージャ外部サーバー修正"

ONTAPでのオンボードキー管理から外部キー管理への移行

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

開始する前に

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

  "FIPSドライブまたはSEDを非保護モードに戻す"

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

  "ボリューム データの暗号化の解除"

- このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. クラスタのオンボード キー管理の設定を削除します。

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

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

外部キー管理からONTAPオンボードキー管理に切り替える

オンボードキー管理に切り替えるには、オンボードキー管理を有効にする前に、外部キー管理構成を削除します。

開始する前に

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

  "FIPSドライブまたはSEDを非保護モードに戻す"

- すべての外部キー管理ツールの接続を削除しておく必要があります。

  "外部キー管理ツールの接続の削除"

- このタスクを実行するには、クラスタ管理者である必要があります。

手順

キー管理を移行する手順は、使用しているONTAPのバージョンによって異なります。

ONTAP 9.6以降

1. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. 次のコマンドを使用します。

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

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

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

ONTAP 9.5以前

次のコマンドを使用します：
`security key-manager delete-kmip-config`

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

関連情報

- "セキュリティキー・マネージャ外部無効化"

ONTAPブートプロセス中にキー管理サーバにアクセスできない場合の動作

ONTAP は、NSE 用に設定されたストレージ システムがブート プロセス中に指定されたキー管理サーバのいずれにもアクセスできない場合に、望ましくない動作を回避するために特定の予防措置を講じます。

ストレージシステムがNSE用に設定され、SEDのキーが再設定されてロックされ、SEDの電源がオンになっている場合、ストレージシステムは、データにアクセスする前に、キー管理サーバーから必要な認証キーを取得して、SEDに対して認証を行う必要があります。

ストレージシステムは、指定されたキー管理サーバへの接続を最大3時間試行します。その時間が経過してもいずれのサーバにも接続できない場合、ブートプロセスは停止し、ストレージシステムは停止します。

ストレージシステムが指定されたキー管理サーバへの接続に成功した場合、最大15分間SSL接続の確立を試行します。ストレージシステムが指定されたキー管理サーバとのSSL接続を確立できない場合、ブートプロセス

は停止し、ストレージシステムは停止します。

ストレージシステムがキー管理サーバへの接続を試行している間、失敗した接続試行に関する詳細情報がCLIに表示されます。Ctrl+Cキーを押すことで、いつでも接続試行を中断できます。

セキュリティ対策として、SEDへの無許可のアクセス試行回数には上限があり、試行回数が上限に達すると既存データへのアクセスは無効になります。指定されたどのキー管理サーバにもアクセスできず、適切な認証キーを取得できない場合、ストレージ システムはデフォルト キーでの認証のみ試行できますが、その場合、認証が失敗してパニック状態になります。パニック状態になった場合に自動的にリブートするように構成されている場合、ストレージ システムはブート ループに入り、SEDでの認証は繰り返し失敗します。

このようなシナリオでストレージ システムが停止するのは、ストレージ システムがブート ループに入ることを回避し、上限を超えて連続して認証に失敗したためにSEDが永続的にロックされて意図しないデータ損失が発生することを回避するための設計です。ロックアウト保護の上限とタイプは、SEDの仕様とタイプによって異なります。

SEDタイプ	ロックアウトにつながる認証の連続失敗回数	安全限界に達したときのロックアウト保護タイプ
HDD	1024	永続的。適切な認証キーが再び利用可能になったとしても、データを回復することはできません。
X440_PHM2800MCTO 800GB NSE SSD（ファームウェアリビジョン NA00 または NA01）	5	一時的。ロックアウトはディスクの電源を入れ直すまでのみ有効です。
X577_PHM2800MCTO 800GB NSE SSD（ファームウェアリビジョン NA00 または NA01）	5	一時的。ロックアウトはディスクの電源を入れ直すまでのみ有効です。
X440_PHM2800MCTO 800GB NSE SSD（ファームウェアリビジョンが高いもの）	1024	永続的。適切な認証キーが再び利用可能になったとしても、データを回復することはできません。
X577_PHM2800MCTO 800GB NSE SSD（ファームウェアリビジョンが高いもの）	1024	永続的。適切な認証キーが再び利用可能になったとしても、データを回復することはできません。
その他すべてのSSDモデル	1024	永続的。適切な認証キーが再び利用可能になったとしても、データを回復することはできません。

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

指定されたキー管理サーバーに到達できないためにストレージ システムが停止するというシナリオに遭遇した場合は、ストレージ システムの起動を続行する前に、まず通信障害の原因を特定して修正する必要があります。

ONTAPの暗号化をデフォルトで無効にする

ONTAP 9.7以降では、Volume Encryption（VE）ライセンスがあり、オンボード / 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。必要に応じて、クラスタ全体に対してデフォルトで暗号化が無効になるようにすることができます。

開始する前に

このタスクを実行するには、クラスタ管理者であるか、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。

手順

1. ONTAP 9.7以降でクラスタ全体に対して暗号化をデフォルトで無効にするには、次のコマンドを実行します。

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

著作権に関する情報

商標に関する情報