CLI を使用して暗号化を管理します

ONTAP 9

NetApp
September 12, 2024

目次

CLI を使用して暗号化を管理します 1
NetApp暗号化の概要 1
NetApp Volume Encryption を設定する 1
ネットアップのハードウェアベースの暗号化を設定 33
ネットアップの暗号化を管理 57

CLI を使用して暗号化を管理します

NetApp暗号化の概要

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

- NetApp Volume Encryption（NVE）を使用したソフトウェアベースの暗号化では、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、データ書き込み時のFull Disk Encryption（FDE；フルディスク暗号化）がサポートされます。

NetApp Volume Encryption を設定する

NetApp Volume Encryption の設定の概要

NetApp Volume Encryption （ NVE ）は、一度に 1 ボリュームずつ保管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コピーを含む）の両方が暗号化されます。データへのアクセスには、ボリュームごとに 1 つずつ、一意の XTS-AES-256 キーを使用します。外部キー管理サーバまたはオンボードキーマネージャ（OKM）がノードにキーを提供します。

- 外部キー管理サーバはストレージ環境に配置されたサードパーティのシステムで、 Key Management Interoperability Protocol （ KMIP ）を使用してノードにキーを提供します。外部キー管理サーバは、データとは別のストレージシステム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、Volume Encryption（VE）ライセンスがあり、オンボードまたは外部のキー管理ツールを使用している場合、アグリゲートとボリュームの暗号化がデフォルトで有効になります。VEライセンスはに含まれて"ONTAP One"ます。外部キーマネージャまたはオンボードキーマネージャが設定されている場合は、新しいアグリゲートおよび新しいボリュームに対する保存データの暗号化の設定方法が変更されます。新しいアグリゲートでは、NetAppアグリゲート暗号化（NAE）がデフォルトで有効になります。NAEアグリゲートに含まれていない新しいボリュームでは、デフォルトでNetApp Volume Encryption（NVE）が有効になります。マルチテナントキー管理を使用してデータStorage Virtual Machine（SVM）に独自のキー管理機能が設定されている場合、そのSVM用に作成されたボリュームには自動的にNVEが設定されます。

新規または既存のボリュームで暗号化を有効にできます。NVE は、重複排除や圧縮など、ストレージ効率化のためのさまざまな機能をサポートしています。ONTAP 9.14.1以降では、次のことが可能です。 既存のSVMルートボリュームでNVEを有効にする。

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

NVEを有効にすると、コアダンプも暗号化されます。

アグリゲートレベルの暗号化

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

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

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、ボリューム暗号化（ VE ）ライセンスがあり、オンボードキーマネージャまたは外部キーマネージャを使用している場合、アグリゲートとボリューム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。

を使用できます `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ます。その逆も同様です。NAE ボリュームは NVE ボリュームにレプリケートできます。

を使用することはできません `secure purge` NAEボリュームに対するコマンド。

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解決策が必要な場合。
- 暗号化キーを一元管理するマルチクラスタ解決策が必要です。
- 認証キーをデータとは別のシステムや場所に格納してセキュリティを強化する必要がある場合。

外部キー管理の範囲

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

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

- ONTAP 9.6 以降では、 *svm scop* を使用して、クラスタ内の指定した SVM に外部キー管理を設定できます。各テナントが異なる SVM （または SVM のセット）を使用してデータを提供するマルチテナント環境には、この方法が最適です。特定のテナントの SVM 管理者だけが、そのテナントのキーにアクセスできます。
- ONTAP 9.10.1 以降では、を使用できます Azure Key Vault と Google Cloud KMS データSVMのNVEキーのみを保護する。これは、9.12.0以降のAWS KMSで利用できるようになりました。

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

検証済みの外部キー管理ツールのリストは、にあります "ネットアップの Interoperability Matrix Tool （ IMT ）"。このリストを確認するには、IMTの検索機能に「キー管理ツール」と入力します。

サポートの詳細

次の表に、 NVE のサポートの詳細を示します。

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

暗号化	ONTAP 9.7 以降では、ボリューム暗号化（ VE ）ライセンスを追加し、オンボードキーマネージャまたは外部キーマネージャを設定すると、新しく作成したアグリゲートとボリュームがデフォルトで暗号化されます。暗号化されていないアグリゲートを作成する必要がある場合は、次のコマンドを使用します。
	
	`storage aggregate create -encrypt-with-aggr-key false`
	
	プレーンテキスト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は有効になりません。
	
	• VE ライセンスがインストールされていません。
	• キー管理ツールが設定されていません
	• プラットフォームまたはソフトウェアは暗号化をサポートしていません
	• ハードウェアの暗号化が有効です

ONTAP	すべての ONTAP 実装。ONTAP 9.5 以降では、 ONTAP クラウドがサポートされます。
デバイス	HDD 、 SSD 、ハイブリッド、アレイ LUN

RAID の場合	RAID0 、 RAID 4 、 RAID-DP 、 RAID-TEC のいずれかです。
個のボリューム	データボリュームと既存のSVMルートボリューム。MetroClusterメタデータボリュームのデータは暗号化できません。9.14.1より前のバージョンのONTAPでは、NVEを使用してSVMルートボリュームのデータを暗号化できません。ONTAP 9.14.1以降では、ONTAPでサポートされます。 SVMルートボリュームのNVE。
アグリゲートレベルの暗号化	ONTAP 9.6 以降では、 NVE でアグリゲートレベルの暗号化（ NAE ）がサポートされます。 • アグリゲートレベルの重複排除をインラインまたはバックグラウンドで実行する場合は、アグリゲートレベルの暗号化を使用する必要があります。 • アグリゲートレベルで暗号化されたボリュームのキーは変更できません。 • アグリゲートレベルで暗号化されたボリュームでは、セキュアパージがサポートされません。 • NAE では、データボリュームに加えて、 SVM ルートボリュームと MetroCluster メタデータボリュームの暗号化がサポートされます。ただし、ルートボリュームの暗号化はサポートされません。
SVM スコープ	ONTAP 9.6 以降では、 NVE で外部キー管理のみを対象に SVM スコープがサポートされます。オンボードキーマネージャに対してはサポートされません。MetroCluster は ONTAP 9.8 以降でサポートされています。
ストレージ効率	重複排除、圧縮、コンパクション、 FlexClone 。 クローンでは、親からスプリットしたあとも親と同じキーを使用します。を実行する必要があります `volume move` スプリットクローンの場合、スプリットクローンには別のキーが割り当てられます。
レプリケーション	• ボリュームレプリケーションでは、ソースボリュームとデスティネーションボリュームで異なる暗号化設定を使用できます。暗号化は、送信元に対して設定することも、宛先に対して設定解除することもできます。逆も同様です。 • 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 キーは、構成レプリケーションサービスによってパートナーサイトにレプリケートされます。
コンプライアンス	ONTAP 9.2 以降では、新しいボリュームのみを対象に、 SnapLock が Compliance モードと Enterprise モードの両方でサポートされます。既存の SnapLock ボリュームで暗号化を有効にすることはできません。

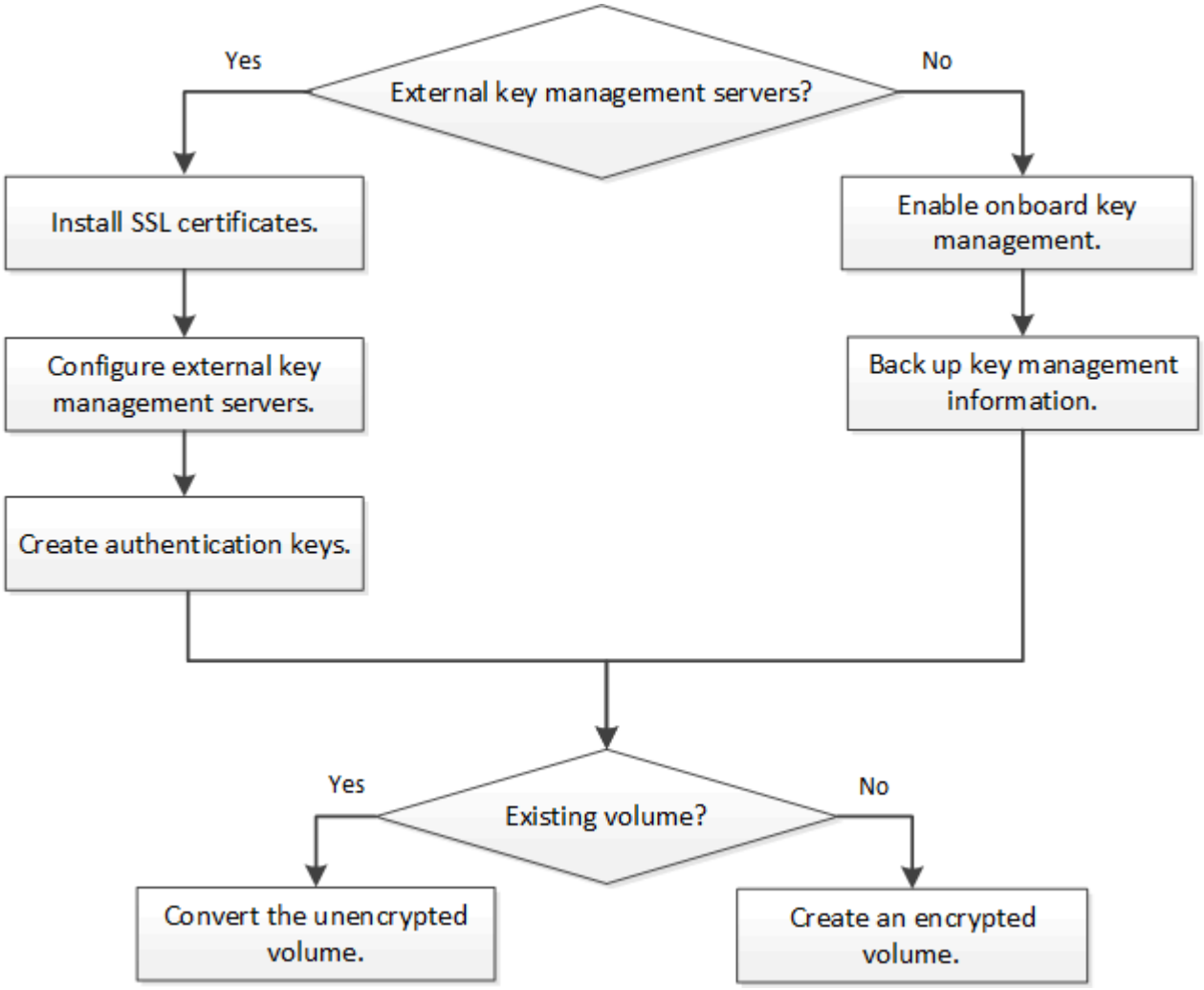
FlexGroup	ONTAP 9.2 以降では、 FlexGroup がサポートされます。デスティネーションアグリゲートのタイプは、ボリュームレベルまたはアグリゲートレベルのソースアグリゲートと同じである必要があります。ONTAP 9.5 以降では、 FlexGroup ボリュームのキーをインプレースで変更できます。
7-Mode からの移行	7-Mode Transition Tool 3.3 以降では、 7-Mode Transition Tool CLI を使用して、クラスタシステムの NVE 対応デスティネーションボリュームへのコピーベースの移行を実行できます。

関連情報

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

NetApp Volume Encryption のワークフロー

ボリューム暗号化を有効にする前に、キー管理サービスを設定する必要があります。暗号化は新しいボリュームでも既存のボリュームでも有効にすることができます。



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

NVEの設定

クラスタのバージョンが **NVE** をサポートしているかどうかを確認します

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

このタスクについて

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

ステップ

1. クラスタのバージョンが NVE をサポートしているかどうかを確認します。

   ```
   version -v
   ```

   コマンドの出力に「 1Ono-dARE 」というテキスト（「 no Data at Rest Encryption 」の場合）、または 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は、 NVE はサポートされません "サポートの詳細"。

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

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

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

ライセンスをインストール

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

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

作業を開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- 営業担当者からVEライセンスキーを入手するか、ONTAP Oneをインストールしておく必要があります。

手順

1. "VEライセンスがインストールされていることを確認します。"です。

   VEライセンスパッケージ名は `VE`。

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

ール"を参照してください。

外部キー管理を設定

外部キー管理の概要の設定

1 つ以上の外部キー管理サーバを使用して、暗号化されたデータにアクセスする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。

> ONTAP 9.1 以前のバージョンでは、外部キー管理ツールを使用する前に、ノード管理ロールが設定されたポートにノード管理 LIF を割り当てる必要があります。

ONTAP 9.1 以降では、 NetApp Volume Encryption （ NVE ）によってオンボードキーマネージャがサポートされます。ONTAP 9.3以降では、NVEで外部キー管理（KMIP）とオンボードキーマネージャがサポートされます。ONTAP 9.10.1 以降では、を使用できます Azure Key VaultサービスまたはGoogle Cloud Key Manager サービス NVEキーを保護するため。ONTAP 9.11.1以降では、1つのクラスタに複数の外部キー管理ツールを設定できます。を参照してください クラスタ化されたキーサーバを設定

System Managerを使用して外部キー管理ツールを管理します。

ONTAP 9.7以降では、オンボードキーマネージャを使用して認証キーと暗号化キーを格納および管理できます。ONTAP 9.13.1以降では、外部キー管理ツールを使用してこれらのキーを格納および管理することもできます。

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

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

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

外部キー管理ツールを設定する

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

手順

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

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

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

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

既存の外部キー管理ツールを編集します

すでに外部キー管理ツールを設定している場合は、その設定を変更できます。

手順

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

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

Storage VMスコープの外部キー管理ツール	ストレージ>* Storage VM *	Storage VMを選択します。[設定]タブを選択します。セクションの[セキュリティ]で、を選択し ⋮、[外部キーマネージャの編集]*を選択します。

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

外部キー管理ツールを削除します

ボリュームが暗号化されていない場合は、外部キー管理ツールを削除できます。

手順

1. 外部キー管理ツールを削除するには、次のいずれかの手順を実行します。

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

キー管理ツール間でキーを移行する

クラスタで複数のキー管理ツールを有効にしている場合は、キー管理ツール間でキーを移行する必要があります。このプロセスはSystem Managerで自動的に完了します。

- オンボードキーマネージャまたは外部キーマネージャ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は、 その後、Storage VMレベルで外部キー管理ツールを設定する際には、それらのキーを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移行する必要があります。 このプロセスは、System Managerによって自動的に実行されます。
- Storage VMで暗号化なしでボリュームを作成した場合は、キーを移行する必要はありません。

クラスタに **SSL** 証明書をインストールします

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。

このタスクについて

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。

作業を開始する前に

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

> KMIP サーバへのクライアント証明書とサーバ証明書のインストールは、クラスタに証明書をインストールする前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
   ```

ONTAP 9.6 以降で外部キー管理を有効にする（ **NVE** ）

1 つ以上の KMIP サーバを使用して、暗号化されたデータにアクセスする際にクラスタで使用するキーを安全に保管できます。ONTAP 9.6以降では、データSVMが暗号化されたデータにアクセスする際に使用するキーを保護するための独立した外部キー管理ツールを設定できます。

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

このタスクについて

1 つのクラスタまたは SVM に最大 4 つの KMIP サーバを接続できます。冗長性とディザスタリカバリのために、少なくとも 2 台のサーバを使用することを推奨します。

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すべての SVM になるか、選択した SVM のみになるかが決まります。

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

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

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

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、 ONTAP はそれらのサーバのみを使用してキーを保護します。それ以外 ONTAP の場合は、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。を使用できます `security key-manager key migrate` コマンドを使用して、クラスタスコープのオンボードキー管理からSVMスコープの外部キー管理ツールにキーを移行します。

作業を開始する前に

- KMIP SSL クライアント証明書とサーバ証明書をインストールしておく必要があります。
- このタスクを実行するには、クラスタ管理者または SVM の管理者である必要があります。
- MetroCluster 環境で外部キー管理を有効にする場合は、外部キー管理を有効にする前に MetroCluster が完全に設定されている必要があります。
- MetroCluster 環境では、両方のクラスタに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、に置き換わるものです `security key-manager setup` コマンドを実行しますクラスタのログインプロンプトでコマンドを実行すると、 *`admin_SVM`* デフォルトでは、現在のクラスタの管理SVMが使用されます。 クラスタスコープを設定するには、クラスタ管理者である必要があります。を実行できます `security key-manager external modify` コマンドを使用して、外部キー管理の設定を変更します。
   - MetroCluster 環境で管理SVMに外部キー管理を設定する場合は、を繰り返す必要があります `security key-manager external enable` パートナークラスタに対して実行します。

   次のコマンドは、の外部キー管理を有効にします `cluster1` 3つの外部キーサーバで構成されます。最初のキーサーバはホスト名とポートで指定し、 2 番目のキーサーバは IP アドレスとデフォルトポートで指定し、 3 番目のキーサーバは IPv6 アドレスとポートで指定します。

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

2. キー管理ツールとして SVM 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のログインプロンプトでコマンドを実行すると、 `SVM` デフォルトは現在のSVMです。 SVM スコープを設定するには、クラスタ管理者または SVM 管理者である必要があります。を実行できます `security key-manager external modify` コマンドを使用して、外部キー管理の設定を変更します。
   > ◦ MetroCluster 環境でデータSVMに外部キー管理を設定する場合は、の手順を繰り返す必要はありません `security key-manager external enable` パートナークラスタに対して実行します。

   次のコマンドは、の外部キー管理を有効にします `svm1` 単一のキーサーバがデフォルトポート5696でリスンしている場合：

```
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。

   > を使用することもできます `security key-manager external add-servers` コマンドを使用して追加のSVMを設定します。。 `security key-manager external add-servers` コマンドは、に置き換わるものです `security key-manager add` コマンドを実行しますコマンド構文全体については、マニュアルページを参照してください。

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、に置き換わるものです `security key-manager show -status` コマンドを実行しますコマンド構文全体については、マニュアルページを参照してください。

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

Node  Vserver  Key Server                                       Status
----  -------  ----------------------------------------
-------------
node1
      svm1
               keyserver.svm1.com:5696                          available
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available
node2
      svm1
               keyserver.svm1.com:5696                          available
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available

8 entries were displayed.
```

5. 必要に応じて、プレーンテキストボリュームを暗号化ボリュームに変換します。

   ```
   volume encryption conversion start
   ```

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

ONTAP 9.5 以前で外部キー管理を有効にします

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

このタスクについて

ONTAP は、クラスタ内のすべてのノードについて KMIP サーバの接続を設定します。

作業を開始する前に

- 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。

2. 各プロンプトで適切な応答を入力します。
3. KMIP サーバを追加します。

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

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

   > MetroCluster 環境では、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
   ```

   コマンド構文全体については、マニュアルページを参照してください。

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

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

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

   ```
   volume encryption conversion start
   ```

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

クラウドプロバイダを使用してキーを管理します

ONTAP 9.10.1 以降では、を使用できます "Azure キーボールト（ AKV ）" および "Google Cloud Platform のキー管理サービス（ Cloud KMS ）" クラウドでホストされるアプリケーションでONTAP暗号化キーを保護する。ONTAP 9.12.0以降では、を使用してNVEキーを保護することもできます "AWS KMS"。

AWS KMS、AKV、Cloud KMSを使用して保護できます "NetApp Volume Encryption （ NVE ）キー" データSVMの場合のみ。

このタスクについて

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

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

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

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

作業を開始する前に

- 適切なクラウドプロバイダでKMSを設定しておく必要があります。
- ONTAPクラスタのノードでNVEがサポートされている必要があります。
- "Volume Encryption（VE）ライセンスとマルチテナントEncryption Key Management（MTEKM）ライセンスをインストールしておく必要があります。"です。これらのライセンスはに含まれてい"ONTAP One"ます。
- クラスタ管理者またはSVM管理者である必要があります。
- データSVMに暗号化されたボリュームが含まれていないか、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。

外部キー管理を有効にします

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。該当するキー管理ツールと環境のタブを選択します。

AWS

作業を開始する前に

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

ONTAP SVMでAWS KMVを有効にします

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

Azure

ONTAP SVMでAzure Key Vaultを有効にします

1. 作業を開始する前に、クライアントシークレットまたは証明書のいずれかで、 Azure アカウントから適切な認証クレデンシャルを取得する必要があります。
   また、クラスタ内のすべてのノードが正常であることを確認する必要があります。これを確認するには、コマンドを使用します `cluster show`。
2. 特権レベルを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 アカウントから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が正しく有効になっていることを確認します。
   `security key-manager external azure show vserver` *`svm_name`*
   サービスの到達可能性がOKでない場合は、データSVM LIFを介したAKVキー管理サービスへの接続を確立します。

Google Cloud

ONTAP SVMでCloud KMSを有効にします

1. 開始する前に、Google Cloud KMSアカウントキーファイルの秘密鍵をJSON形式で取得します。これは GCP アカウントにあります。

また、クラスタ内のすべてのノードが正常であることを確認する必要があります。これを確認するには、コマンドを使用します `cluster show`。

2. 特権レベルをadvancedに設定します。
   `set -priv advanced`
3. SVMでCloud KMSを有効にします
   `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、サービスアカウントの秘密鍵を使用して 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構成されていることを確認します。
   `security key-manager external gcp show vserver` *`svm_name`*
   のステータス `kms_wrapped_key_status` になります "`UNKNOWN`" 暗号化されたボリュームが作成されていない場合。
   サービスへの到達可能性がOKでない場合は、データSVM LIFを介してGCPキー管理サービスへの接続を確立します。

データSVM用にすでに暗号化されたボリュームが1つ以上設定され、管理SVMのオンボードキーマネージャで対応するNVEキーが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用に暗号化された新しいボリュームを作成することはできません。

関連情報

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

ONTAP 9.6 以降でオンボードキー管理を有効にする（ **NVE** ）

オンボードキーマネージャを使用して、暗号化されたデータにアクセスする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または自己暗号化ディスクにアクセスする各クラスタで有効にする必要があります。

このタスクについて

を実行する必要があります `security key-manager onboard sync` コマンドはクラスタにノードを追加するたびに実行します。

MetroCluster構成を使用している場合は、 `security key-manager onboard enable` 最初にローカルクラスタでコマンドを実行してから、 `security key-manager onboard sync` リモートクラスタで同じパスフレーズを使用してコマンドを実行します。を実行すると `security key-manager onboard enable` ローカルクラスタからコマンドを実行し、リモートクラスタで同期する必要はありません。 `enable` リモートクラスタからコマンドを再実行します。

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

NVEの場合は、を設定します `cc-mode-enabled=yes`を使用して作成したボリューム `volume create` および `volume move start` コマンドは自動的に暗号化されます。の場合 `volume create`を指定する必

要はありません `-encrypt true。の場合 volume move start`を指定する必要はありません `-encrypt-destination true。

保管データの ONTAP 暗号化を設定する場合、 CSfC （ Commercial Solutions for Classified ）の要件を満たすために、 NVE で NSE を使用し、 Common Criteria モードでオンボードキーマネージャが有効になっていることを確認する必要があります。を参照してください "CSfC 解決策 Brief （ CSfC の概要" CSfC の詳細については、を参照してください。

> オンボードキーマネージャがCCモードで有効になっている場合 (`cc-mode-enabled=yes`）では、システムの動作は次のように変更されます。
>
> - Common Criteria モードで動作している場合、クラスタパスフレーズの試行に連続して失敗したかどうかが監視されます。
>
> ブート時に正しいクラスタパスフレーズを入力しなかった場合、暗号化されたボリュームはマウントされません。これを修正するには、ノードをリブートし、正しいクラスタパスフレーズを入力する必要があります。ブート後、パラメータとしてクラスタパスフレーズを必要とするコマンドに対して、最大 5 回連続してクラスタパスフレーズを 24 時間以内に入力することができます。制限に達した場合（たとえば、クラスタのパスフレーズを 5 回連続して正しく入力できなかった場合など）は、 24 時間のタイムアウトが経過するまで待つか、ノードをリブートして制限をリセットする必要があります。
>
> - システムイメージの更新では、 NetApp RSA-3072 コード署名証明書と SHA-384 コード署名ダイジェストを使用して、通常の NetApp RSA-2048 コード署名証明書および SHA-256 コード署名ダイジェストではなく、イメージの整合性をチェックします。
>
> upgrade コマンドは、さまざまなデジタル署名をチェックして、イメージの内容が変更されていないか、壊れていないかを確認します。検証に成功した場合は、イメージの更新プロセスが次の手順に進みます。成功しなかった場合は、イメージの更新が失敗します。を参照してください `cluster image` のマニュアルページを参照してください。

> オンボードキーマネージャは、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。通常の動作条件下では、システムが停止すると 30 秒以内に揮発性メモリの内容がクリアされます。

作業を開始する前に

- 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
```

> 設定 `cc-mode-enabled=yes` リブート後にユーザにキー管理ツールのパスフレーズの入力を求める場合。NVEの場合は、を設定します `cc-mode-enabled=yes`を使用して作成したボリューム `volume create` および `volume move start` コマンドは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ません。 。 `security key-manager onboard enable` コマンドは、に置き換わるものです `security key-manager setup` コマンドを実行します

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

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

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

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

   指定された "cc-mode" パスフレーズが 64 文字未満の場合、キー管理ツールのセットアップ操作によってパスフレーズのプロンプトが再表示されるまでに 5 秒の遅延が発生します。

3. パスフレーズの確認のプロンプトでパスフレーズをもう一度入力します。
4. 認証キーが作成されたことを確認します。

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

   。 `security key-manager key query` コマンドは、に置き換わるものです `security key-manager query key` コマンドを実行しますコマンド構文全体については、マニュアルページを参照してください。

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

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

 Key Tag                                  Key Type Encryption   Restored

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

node1                                    NSE-AK   AES-256      true

    Key ID:
00000000000000000200000000000100056178fc6ace6d91472df8a9286daacc00000000
00000000

node1                                    NSE-AK   AES-256      true

    Key ID:
00000000000000000200000000000100df1689a148fdfbf9c2b198ef974d0baa00000000
00000000

2 entries were displayed.
```

5. 必要に応じて、プレーンテキストボリュームを暗号化ボリュームに変換します。

   ```
   volume encryption conversion start
   ```

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

完了後

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

オンボードキーマネージャのパスフレーズを設定するときは、災害時に備えて、ストレージシステムの外部の安全な場所にも手動で情報をバックアップしておく必要があります。を参照してください "オンボードキー管理情報を手動でバックアップ"。

ONTAP 9.5 以前でオンボードキー管理を有効にする（ **NVE** ）

オンボードキーマネージャを使用して、暗号化されたデータにアクセスする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。

このタスクについて

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

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

デフォルトでは、ノードのリブート時にキー管理ツールのパスフレーズを入力する必要はありません。ONTAP 9.4以降では、 `-enable-cc-mode yes` リブート後にユーザにパスフレーズの入力を求めるオプション。

NVEの場合は、を設定します `-enable-cc-mode yes`を使用して作成したボリューム `volume create` および `volume move start` コマンドは自動的に暗号化されます。の場合 `volume create`を指定する必要はありません `-encrypt true`。の場合 `volume move start`を指定する必要はありません `-encrypt-destination true`。

> パスフレーズの試行に失敗した場合は、ノードを再起動する必要があります。

作業を開始する前に

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

  "外部キー管理からオンボードキー管理への移行"

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

手順

1. キー管理ツールのセットアップを開始します。

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

   > ONTAP 9.4以降では、 `-enable-cc-mode yes` リブート後にユーザにキー管理ツールのパスフレーズの入力を求めるオプション。NVEの場合は、を設定します `-enable-cc-mode yes`を使用して作成したボリューム `volume create` および `volume move start` コマンドは自動的に暗号化されます。

   次の例では、リブートのたびにパスフレーズの入力を求めずに、 cluster1 でキー管理ツールをセットアップします。

```
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. 入力するコマンド `yes` オンボードキー管理を設定するプロンプトが表示されます。
3. パスフレーズのプロンプトで 32 ～ 256 文字のパスフレーズを入力します。または、 64 ～ 256 文字のパスフレーズを「 cc-mode] 」に入力します。

   > 指定された "cc-mode" パスフレーズが 64 文字未満の場合、キー管理ツールのセットアップ操作によってパスフレーズのプロンプトが再表示されるまでに 5 秒の遅延が発生します。

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

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

   コマンド構文全体については、マニュアルページを参照してください。

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

Node: node1
Key Store: onboard
Key ID                                                                   Used By
-------------------------------------------------------------------
--------
00000000000000000200000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
00000000000000000200000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                                   Used By
-------------------------------------------------------------------
--------
00000000000000000200000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
00000000000000000200000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

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

   `volume encryption conversion start`

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

完了後

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

オンボードキーマネージャのパスフレーズを設定するときは、災害時に備えて、ストレージシステムの外部の安全な場所にも手動で情報をバックアップしておく必要があります。を参照してください "オンボードキー管理情報を手動でバックアップ"。

新しく追加したノードでオンボードキー管理を有効にします

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。

> ONTAP 9.5以前の場合は、を実行する必要があります `security key-manager setup` コマンドはクラスタにノードを追加するたびに実行します。
>
> ONTAP 9.6以降の場合は、を実行する必要があります `security key-manager sync` コマンドはクラスタにノードを追加するたびに実行します。
>
> オンボードキー管理が設定されているクラスタにノードを追加した場合は、このコマンドを実行して不足しているキーを更新します。

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

- ONTAP 9.6以降では、を実行する必要があります `security key-manager onboard enable` を実行してから、を実行します `security key-manager onboard sync` リモートクラスタで、それぞれで同じパスフレーズを使用します。
- ONTAP 9.5では、を実行する必要があります `security key-manager setup` ローカルクラスタおよび `security key-manager setup -sync-metrocluster-config yes` リモートクラスタで、それぞれで同じパスフレーズを使用します。
- ONTAP 9.5より前のバージョンでは、を実行する必要があります `security key-manager setup` ローカルクラスタで、約20秒待ってからを実行します `security key-manager setup` リモートクラスタで、それぞれで同じパスフレーズを使用します。

デフォルトでは、ノードのリブート時にキー管理ツールのパスフレーズを入力する必要はありません。ONTAP 9.4以降では、 `-enable-cc-mode yes` リブート後にユーザにパスフレーズの入力を求めるオプション。

NVEの場合は、を設定します `-enable-cc-mode yes`を使用して作成したボリューム `volume create` および `volume move start` コマンドは自動的に暗号化されます。の場合 `volume create`を指定する必要はありません `-encrypt true`。の場合 `volume move start`を指定する必要はありません `-encrypt-destination true`。

パスフレーズの試行に失敗した場合は、ノードを再起動する必要があります。

NVE を使用してボリュームデータを暗号化する

NVE を使用したボリュームデータの暗号化の概要

ONTAP 9.7 以降では、 VE ライセンスとオンボードキー管理または外部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暗号化がデフォルトで有効になります。ONTAP 9.6 以前では、新しいボリュームまたは既存のボリュームで暗号化を有効にできます。ボリューム暗号化を有効にする前に、VEライセンスをインストールし、キー管理を有効にしておく必要があります。NVE は FIPS-140-2 レベル 1 に準拠しています。

VEライセンスでアグリゲートレベルの暗号化を有効にする

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

このタスクについて

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

アグリゲートレベルの暗号化が有効になっているアグリゲートは、 _NAE アグリゲートと呼ばれます（NetApp Aggregate Encryption の場合）。NAEアグリゲート内のすべてのボリュームは、NAEまたはNVE暗号化を使用して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したボリュームはデフォルトでNAE暗号化を使用して暗号化されます。デフォルトの設定を変更して、NVE暗号化を使用することもできます。

NAE アグリゲートではプレーンテキストボリュームがサポートされません。

作業を開始する前に

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します	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`*
ONTAP 9.6 で NAE アグリゲートを作成します	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`

非 NAE アグリゲートを NAE アグリゲートに変換します	`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します	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key false`

コマンド構文全体については、マニュアルページを参照してください。

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

- ONTAP 9.7 以降

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

- ONTAP 9.6 以前：

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

2. アグリゲートで暗号化が有効になっていることを確認します。

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

   コマンド構文全体については、マニュアルページを参照してください。

   次のコマンドは、を確認します `aggr1` 暗号化が有効：

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

完了後

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

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

を使用できます `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します。

このタスクについて

NetApp Volume Encryption（NVE）を使用してボリュームを暗号化できます。また、ONTAP 9.6以降では、NetApp Aggregate Encryption（NAE）を使用できます。NAEおよびNVEの詳細については、を参照してください ボリューム暗号化の概要。

ONTAP の新しいボリュームで暗号化を有効にする手順 は、使用するONTAP のバージョンと構成によって異なります。

- ONTAP 9.4以降では、を有効にした場合 `cc-mode` オンボードキーマネージャをセットアップする場合は、でボリュームを作成します `volume create` コマンドは、指定したかどうかに関係なく自動的に暗号化されます `-encrypt true`。
- ONTAP 9.6以前のリリースでは、を使用する必要があります `-encrypt true` を使用 `volume create` 暗号化を有効にするコマンド（を有効にしていない場合） `cc-mode`）。
- ONTAP 9.6でNAEボリュームを作成するには、アグリゲートレベルでNAEを有効にする必要があります。を参照してください VEライセンスでアグリゲートレベルの暗号化を有効にします 詳細については、を参照してください。
- ONTAP 9 .7以降では"VEライセンス"、およびオンボードまたは外部キー管理を使用している場合、新しく作成したボリュームはデフォルトで暗号化されます。NAEアグリゲート内に作成される新しいボリュームのタイプは、デフォルトではNVEではなくNAEになります。
  - ONTAP 9.7以降のリリースでは、を追加した場合 `-encrypt true` に移動します `volume create` NAEアグリゲート内にボリュームを作成するコマンドは、NAEではなくNVE暗号化を使用します。NAEアグリゲート内のすべてのボリュームは、NVEまたはNAEを使用して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アグリゲートに含まれている場合、デフォルトではボリュームがNAEボリュームになります。

作成対象	使用するコマンド
NAEボリューム	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`*

NVEボリューム	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt true` [+] NAEがサポートされないONTAP 9.6以前では、 `-encrypt true` ボリュームをNVEで暗号化するように指定します。NAEアグリゲートでボリュームが作成されるONTAP 9.7以降では、 `-encrypt true` 代わりにデフォルトの暗号化タイプが無効になり、NVEボリュームが作成されます。
プレーンテキストのボリューム	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt false`

コマンド構文の詳細については、コマンドリファレンスページのリンク：https://docs.netapp.com/us-en/ontap-cli/volume-create.htmlを参照してください。[`volume create`^]をクリックします。

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
   ```

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

結果

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

=
:allow-uri-read:

既存のボリュームで暗号化を有効にする

どちらかを使用できます `volume move start` または `volume encryption conversion start` コマンドを使用して、既存のボリュームで暗号化を有効にします。

このタスクについて

- ONTAP 9.3以降では、を使用できます `volume encryption conversion start` 既存のボリュームの暗号化を「インプレース」で有効にするコマンド。ボリュームを別の場所に移動する必要はありません。または、 `volume move start` コマンドを実行します
- ONTAP 9.2以前では、 `volume move start` コマンドを使用して既存のボリュームを移動して暗号化を有効にします。

volume encryption conversion start コマンドを使用して既存のボリュームの暗号化を有効にします

ONTAP 9.3以降では、を使用できます `volume encryption conversion start` 既存のボリュームの暗号化を「インプレース」で有効にするコマンド。ボリュームを別の場所に移動する必要はありません。

変換処理を開始したら、完了する必要があります。処理中にパフォーマンス問題 が発生した場合は、を実行できます `volume encryption conversion pause` 処理を一時停止するコマンド、および `volume`

`encryption conversion resume` コマンドを実行して処理を再開します。

> を使用することはできません `volume encryption conversion start` SnapLock ボリュームを変換します。

手順

1. 既存のボリュームで暗号化を有効にします。

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

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

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

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

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

2. 変換処理のステータスを確認します。

   `volume encryption conversion show`

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

   次のコマンドは、変換処理のステータスを表示します。

   ```
   cluster1::> volume encryption conversion show

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

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

   `volume show -is-encrypted true`

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

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

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

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

結果

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

volume move start コマンドを使用して、既存のボリュームの暗号化を有効にします

を使用できます `volume move start` コマンドを使用して既存のボリュームを移動して暗号化を有効にします。を使用する必要があります `volume move start` ONTAP 9.2以前では、使用するアグリゲートは同じアグリゲートでも別のアグリゲートでもかまいません。

このタスクについて

- ONTAP 9.8以降では、を使用できます `volume move start` SnapLock またはFlexGroup ボリュームで暗号化を有効にします。
- 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、を使用してボリュームを作成できます `volume move start` コマンドは自動的に暗号化されます。指定する必要はありません `-encrypt-destination true`。
- ONTAP 9.6 以降では、アグリゲートレベルの暗号化を使用して、移動するボリュームの包含アグリゲートにキーを割り当てることができます。一意のキーで暗号化されたボリュームは、_NVEボリューム_と呼ばれます（NetAppボリューム暗号化を使用することを意味します）。アグリゲートレベルのキーで暗号化されたボリュームは、 _NAE ボリューム（ NetApp Aggregate Encryption の場合）と呼ばれます。NAE アグリゲートではプレーンテキストボリュームがサポートされません。
- ONTAP 9.14.1以降では、NVEでSVMルートボリュームを暗号化できます。詳細については、を参照してください SVMルートボリュームでのNetAppボリューム暗号化の設定。

作業を開始する前に

このタスクを実行するには、クラスタ管理者であるか、クラスタ管理者から権限を委譲された SVM 管理者である必要があります。

"volume move コマンドの実行権限の委譲"

手順

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

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

NAE ボリュームからプレーンテキストボリューム	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false -encrypt-with-aggr-key false`
NVEボリュームからプレーンテキストボリューム	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false`

コマンド構文全体については、コマンドのマニュアルページを参照してください。

次のコマンドは、という名前のプレーンテキストボリュームを変換します `vol1` NVEボリュームへの移動：

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

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

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

次のコマンドは、という名前のNAEボリュームを変換します `vol2` NVEボリュームへの移動：

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

次のコマンドは、という名前のNAEボリュームを変換します `vol2` プレーンテキストボリュームへ：

```
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、次の名前のNVEボリュームを変換します。 `vol2` プレーンテキストボリュームへ：

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

2. クラスタボリュームの暗号化タイプを表示します。

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

。 `encryption-type` フィールドはONTAP 9.6以降で使用できます。

コマンド構文全体については、コマンドのマニュアルページを参照してください。

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

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

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

3. ボリュームで暗号化が有効になっていることを確認します。

   `volume show -is-encrypted true`

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

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

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

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

結果

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

SVMルートボリュームでの**NetApp**ボリューム暗号化の設定

ONTAP 9.14.1以降では、Storage VM（SVM）のルートボリュームでNetApp Volume Encryption（NVE）を有効にすることができます。NVEでは、ルートボリュームが一意のキーで暗号化されるため、SVMのセキュリティが向上します。

このタスクについて

SVMルートボリューム上のNVEは、SVMの作成後にのみ有効にできます。

作業を開始する前に

- NetAppアグリゲート暗号化（NAE）で暗号化されたアグリゲートにSVMルートボリュームを配置しないでください。
- オンボードキーマネージャまたは外部キーマネージャを使用した暗号化を有効にしておく必要がありま

す。

- ONTAP 9.14.1以降が実行されている必要があります。
- NVEで暗号化されたルートボリュームを含む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、SVMルートボリュームを再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ある場合は、次の手順を実行します。
  - 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NVEを個別に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がNAEを使用する場合、SVMルートボリュームはNAEを使用します。

手順

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

CLI の使用

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

ルートボリュームをインプレースで暗号化

1. ルートボリュームを暗号化されたボリュームに変換します。

   ```
   volume encryption conversion start -vserver svm_name -volume volume
   ```

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

SVMルートボリュームの移動による暗号化

1. ボリュームの移動を開始します。

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

   詳細情報 `volume move`を参照してください ボリュームを移動する。

2. を確認します。 `volume move` で操作が成功しました `volume move show` コマンドを実行します。 `volume show -encryption-type volume` NVEを使用しているすべてのボリュームのリストを表示します。

System Manager の略

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

ノードのルートボリューム暗号化を有効にします

ONTAP 9.8 以降では、ネットアップのボリューム暗号化を使用してノードのルートボリュームを保護できます。

> このタスクについて
>
> この手順環境はノードのルートボリュームを表します。SVM のルートボリュームには適用されません。SVMルートボリュームは、アグリゲートレベルの暗号化で保護できます。 ONTAP 9.14.1以降、NVE。

ルートボリュームの暗号化を開始したら、暗号化を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ることができなくなり、セキュアパージ処理を実行することもできなくなります。

作業を開始する前に

- システムで HA 構成を使用している必要があります。
- ノードのルートボリュームを作成しておく必要があります。
- システムに、 Key Management Interoperability Protocol （ KMIP ）を使用したオンボードキーマネージャまたは外部キー管理サーバが必要です。

手順

1. ルートボリュームを暗号化します。

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

2. 変換処理のステータスを確認します。

   ```
   volume encryption conversion show
   ```

3. 変換処理が完了したら、ボリュームが暗号化されていることを確認します。

   ```
   volume show -fields
   ```

   次の例は、暗号化されたボリュームの出力を示しています。

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

ネットアップのハードウェアベースの暗号化を設定

ネットアップのハードウェアベースの暗号化の概要を設定

ネットアップ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ません。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。

ネットアップのハードウェアベースの暗号化について理解する

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ともに使用すると、自己暗号化ドライブのデータを「暗号化」できます。

自己暗号化ドライブが有効な場合は、コアダンプも暗号化されます。

> HA ペアが 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、トピックの手順に従う必要があります FIPS ドライブまたは SED を非保護モードに戻します システムを初期化する前の HA ペア内のすべてのドライブ（ブートオプション 4 または 9 ）。そうしないと、ドライブを転用した場合にデータが失われる可能性があります。

サポートされている自己暗号化ドライブのタイプ

2種類の自己暗号化ドライブがサポートされています。

- すべての FAS システムおよび AFF システムで、自己暗号化機能を備えた FIPS 認定の SAS ドライブまたは NVMe ドライブがサポートされます。これらのドライブは _FIPS ドライブと呼ばれ、 Federal Information Processing Standard Publication 140-2 レベル 2 の要件に準拠しています。認定された機能により、ドライブに対する DoS 攻撃を防止するなど、暗号化に加えて保護が可能になります。FIPS ドライブは、同じノードまたは HA ペアで他のタイプのドライブと混在させることはできません。
- ONTAP 9.6以降では、AFF A800、A320、およびそれ以降のシステムで、FIPSのテストを実施し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もできます。
- すべてのFIPS検証済みドライブは、FIPS検証に合格し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は、ドライブのファームウェア暗号化モジュールでキー暗号化キーの取得に使用されます）。

> 非暗号化ドライブとは、SEDやFIPSドライブではないドライブです。

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

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ことを推奨します。

- 組織のポリシーには、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解決策 が必要です。
- 暗号化キーを一元管理するマルチクラスタ解決策が必要です。
- 認証キーをデータとは別のシステムや場所に格納してセキュリティを強化する必要がある場合。

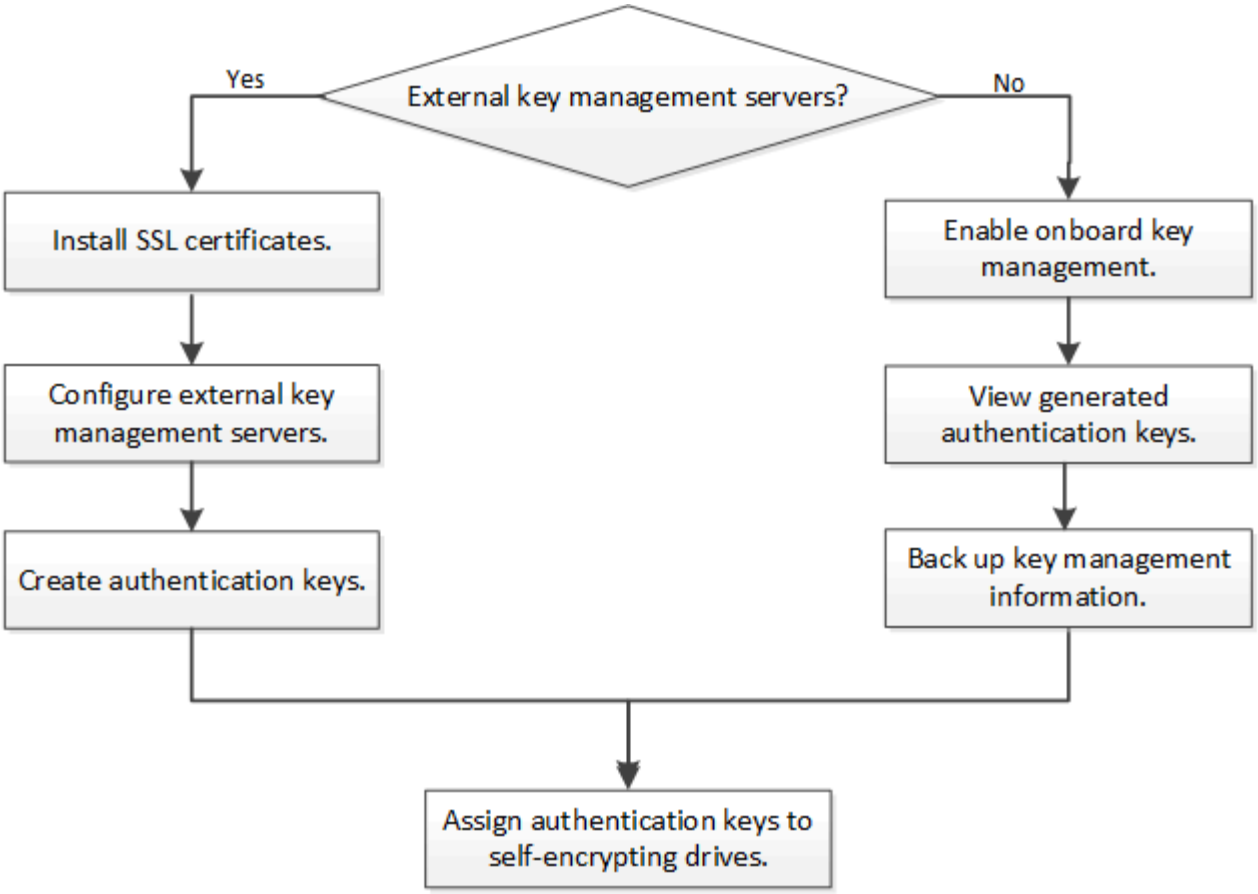
サポートの詳細

次の表に、重要なハードウェア暗号化のサポートの詳細を示します。サポートされている 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ペアで暗号化されていない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に使用するポートを指定します	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 の略"
- "NetApp Volume Encryption および NetApp Aggregate Encryption の略"

外部キー管理を設定

外部キー管理の概要の設定

1 つ以上の外部キー管理サーバを使用して、暗号化されたデータにアクセスする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。

ONTAP 9.1 以前のバージョンでは、外部キー管理ツールを使用する前に、ノード管理ロールが設定されたポートにノード管理 LIF を割り当てる必要があります。

ONTAP 9.1 以降では、オンボードキーマネージャを使用して NetApp Volume Encryption （ NVE ）を実装できます。ONTAP 9.3 以降では、 NVE を外部キー管理（ KMIP ）およびオンボードキーマネージャとともに実装できます。ONTAP 9.11.1以降では、1つのクラスタに複数の外部キー管理ツールを設定できます。を参照してください クラスタ化されたキーサーバを設定

ONTAP 9.2 以前でネットワーク情報を収集

ONTAP 9.2 以前を使用している場合は、外部キー管理を有効にする前にネットワーク設

定ワークシートに情報を記入してください。

ONTAP 9.3 以降では、必要なすべてのネットワーク情報が自動的に検出されます。

項目	注：	価値
キー管理ネットワークインターフェイスの名前		
キー管理ネットワークインターフェイスの IP アドレス	ノード管理 LIF の IPv4 形式または IPv6 形式の IP アドレス	
キー管理ネットワークインターフェイスの IPv6 ネットワークプレフィックス長	IPv6 を使用している場合、 IPv6 ネットワークプレフィックス長	
キー管理ネットワークインターフェイスのサブネットマスク		
キー管理ネットワークインターフェイスのゲートウェイの IP アドレス		
クラスタネットワークインターフェイスの IPv6 アドレス	キー管理ネットワークインターフェイスに IPv6 を使用している場合にのみ必要です	
各 KMIP サーバのポート番号	任意。すべての KMIP サーバで同じポート番号を使用してください。ポート番号を指定しなかった場合は、デフォルトでポート 5696 が使用されます。これは、 Internet Assigned Numbers Authority （ IANA ）が KMIP に割り当てているポートです。	
キータグ名	任意。キータグ名は、ノードに属するすべてのキーを識別するために使用されます。デフォルトのキータグ名はノード名です。	

関連情報

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

"ネットアップテクニカルレポート 4074 ：『 NetApp Storage Encryption Preinstallation Requirements and Procedures for SafeNet KeySecure 』"

クラスタに **SSL** 証明書をインストールします

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。

このタスクについて

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。

作業を開始する前に

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

> KMIP サーバへのクライアント証明書とサーバ証明書のインストールは、クラスタに証明書をインストールする前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
   ```

ONTAP 9.6 以降で外部キー管理を有効にする（ハードウェアベース）

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

化されたキーサーバを作成できます。詳細については、を参照してください クラスタ構成の外部キーサーバを構成。

作業を開始する前に

- 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、に置き換わるものです `security key-manager setup` コマンドを実行しますを実行できます `security key-manager external modify` コマンドを使用して、外部キー管理の設定を変更します。コマンド構文全体については、マニュアルページを参照してください。
   > ◦ MetroCluster 環境で管理SVMに外部キー管理を設定する場合は、を繰り返す必要があります `security key-manager external enable` パートナークラスタに対して実行します。

   次のコマンドは、の外部キー管理を有効にします `cluster1` 3つの外部キーサーバで構成されます。最初のキーサーバはホスト名とポートで指定し、 2 番目のキーサーバは IP アドレスとデフォルトポートで指定し、 3 番目のキーサーバは IPv6 アドレスとポートで指定します。

   ```
   clusterl::> 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、に置き換わるものです `security key-manager show -status` コマンドを実行しますコマンド構文全体については、マニュアルページを参照してください。

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

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

6 entries were displayed.
```

ONTAP 9.5 以前で外部キー管理を有効にします

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

このタスクについて

ONTAP は、クラスタ内のすべてのノードについて KMIP サーバの接続を設定します。

作業を開始する前に

- 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。

2. 各プロンプトで適切な応答を入力します。

3. KMIP サーバを追加します。

   `security key-manager add -address key_management_server_ipaddress`

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

   MetroCluster 環境では、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`

   コマンド構文全体については、マニュアルページを参照してください。

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

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

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

   `volume encryption conversion start`

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

クラスタ構成の外部キーサーバを構成

ONTAP 9.11.1以降では、SVM上のクラスタ化された外部キー管理サーバへの接続を設定できます。クラスタ化されたキーサーバを使用すると、SVMのプライマリキーサーバとセカンダリキーサーバを指定できます。キーを登録すると、ONTAP は、処理が正常に完了するまで、プライマリキーサーバへのアクセスを順次試行する前に、キーの重複を防

止します。

外部キーサーバは、NSE、NVE、NAE、およびSEDのキーに使用できます。SVMでは、最大4つのプライマリ外部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。

作業を開始する前に

- "SVMでKMIPキー管理が有効になっている必要があります。"。
- このプロセスでサポートされるのは、KMIPを使用するキーサーバのみです。サポートされているキーサーバの一覧については、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。
- クラスタ内のすべてのノードでONTAP 9.11.1以降が実行されている必要があります。
- サーバの順序は、で引数をリストします `-secondary-key-servers` パラメータには、外部キー管理（KMIP）サーバのアクセス順序が反映されます。

クラスタ化されたキーサーバを作成します

設定手順 は、プライマリキーサーバを設定したかどうかによって異なります。

SVMにプライマリキーサーバとセカンダリキーサーバを追加する

1. クラスタでキー管理が有効になっていないことを確認します。
   `security key-manager external show -vserver` *`svm_name`*
   SVMですでに最大4つのプライマリキーサーバが有効になっている場合は、新しいプライマリキーサーバを追加する前に既存のプライマリキーサーバの1つを削除する必要があります。
2. プライマリキー管理ツールを有効にします。
   `security key-manager external enable -vserver` *`svm_name`* `-key-servers` *`server_ip`* `-client-cert` *`client_cert_name`* `-server-ca-certs` *`server_ca_cert_names`*
3. プライマリキーサーバを変更してセカンダリキーサーバを追加します。。 `-secondary-key-servers` パラメータには、最大3つのキーサーバをカンマで区切って指定できます。
   `security key-manager external modify-server -vserver` *`svm_name`* `-key-servers` *`primary_key_server`* `-secondary-key-servers` *`list_of_key_servers`*

既存のプライマリキーサーバにセカンダリキーサーバを追加する

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

クラスタ化されたキーサーバを変更

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

プライマリキーサーバとセカンダリキーサーバの変換

プライマリキーサーバをセカンダリキーサーバに変換するには、まずを使用してSVMからプライマリキーサーバを削除する必要があります `security key-manager external remove-servers` コマンドを実行します

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には、まず既存のプライマリキーサーバからセカンダリキーサーバを削除する必要があります。を参照してください [mod-secondary]。既存のキーの削除中にセカンダリキーサーバをプライマリサーバに変換する場合、削除および変換を実行する前に新しいサーバを追加しようとすると、キーが重複する可能性があります。

セカンダリキーサーバを変更します。

セカンダリキーサーバの管理はで行います `-secondary-key-servers` のパラメータ `security key-manager external modify-server` コマンドを実行します。 `-secondary-key-servers` パラメータにはカンマで区切ったリストを指定できます。リスト内で指定されたセカンダリキーサーバの順序によって、セカンダリキーサーバのアクセスシーケンスが決まります。アクセス順序は、コマンドを実行して変更できます `security key-manager external modify-server` セカンダリキーサーバを別の順序で入力します。

セカンダリキーサーバを削除するには、を実行します `-secondary-key-servers` 引数には、削除するキーサーバを省略して保持するキーサーバを指定する必要があります。すべてのセカンダリキーサーバを削除するには、引数を使用します -「なし」を意味します。

追加情報 の場合は、を参照してください `security key-manager external` ページのを参照してください "ONTAP コマンドリファレンス"。

ONTAP 9.6 以降で認証キーを作成します

を使用できます `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、設定したKMIPサーバに格納します。

このタスクについて

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への準拠にデータアクセスと同じ認証キーを使用できます。

ONTAP では、クラスタ内のすべてのノードに対し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になっている場合はサポートされません。ただし、オンボードキーマネージャを有効にすると、 2 つの認証キーが自動的に作成されます。キーを表示するには、次のコマンドを使用します。

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

- 設定済みのキー管理サーバにすでに 128 個を超える認証キーが格納されている場合は警告が表示されます。
- を使用できます `security key-manager key delete` 使用されていないキーを削除するコマンド。。 `security key-manager key delete` 指定したキーがONTAP で現在使用されている場合、コマンドは失敗します。(このコマンドを使用するには 'admin より大きい特権が必要です)

> MetroCluster 環境でキーを削除する前に、キーがパートナークラスタで使用されていないことを確認する必要があります。パートナークラスタで次のコマンドを使用して、キーが使用されていないことを確認できます。
>
> - `storage encryption disk show -data-key-id` *`key-id`*
> - `storage encryption disk show -fips-key-id` *`key-id`*

作業を開始する前に

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

   次の例は、の認証キーを作成します `cluster1`では、32バイトのパスフレーズが自動的に生成されます。

   ```
   cluster1::> security key-manager key create
   Key ID:
   0000000000000000020000000000001006268333f870860128fbe17d393e5083b00000000
   00000000
   ```

2. 認証キーが作成されたことを確認します。

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

   > 。 `security key-manager key query` コマンドは、に置き換わるものです `security key-manager query key` コマンドを実行しますコマンド構文全体については、マニュアルページを参照してください。 出力に表示されるキー ID は、認証キーを参照するために使用される識別子です。実際の認証キーまたはデータ暗号化キーではありません。

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

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

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

       Vserver: cluster1
   Key Manager: external
          Node: node2

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node2                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

ONTAP 9.5 以前で認証キーを作成します

を使用できます `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、設定したKMIPサーバに格納します。

このタスクについて

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対し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未使用のキーを削除し、もう一度コマンドを実行できます。

作業を開始する前に

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
   ```

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

   > 出力に表示されるキー ID は、認証キーを参照するために使用される識別子です。実際の認証キーまたはデータ暗号化キーではありません。

   次の例は、の認証キーを作成します `cluster1`：

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

   Node: cluster1-01
   Creating authentication key...
   Authentication key creation successful.
   Key ID: F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

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

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

2. 認証キーが作成されたことを確認します。

   ```
   security key-manager query
   ```

   コマンド構文全体については、マニュアルページを参照してください。

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

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

  (security key-manager query)

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

Key Tag        Key Type  Restored
-------------  --------  --------
cluster1-01    NSE-AK    yes
       Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C


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

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

FIPS ドライブまたは **SED** にデータ認証キーを割り当てる（外部キー管理）

を使用できます `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。このキーは、クラスタノードでドライブ上の暗号化されたデータをロックまたはロック解除する際に使用します。

このタスクについて

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

この手順 はシステムの停止を伴いません。

作業を開始する前に

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
```

コマンド構文全体については、コマンドのマニュアルページを参照してください。

> を使用できます `security key-manager query -key-type NSE-AK` キーIDを表示するコマンド。

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

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

2. 認証キーが割り当てられたことを確認します。

```
storage encryption disk show
```

コマンド構文全体については、マニュアルページを参照してください。

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

オンボードキー管理を設定

ONTAP 9.6 以降ではオンボードキー管理を有効にしてください

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。

このタスクについて

を実行する必要があります `security key-manager onboard enable` コマンドはクラスタにノードを追

加するたびに実行します。MetroCluster 構成では、を実行する必要があります `security key-manager onboard enable` を実行してから、を実行します `security key-manager onboard sync` リモートクラスタで、それぞれで同じパスフレーズを使用します。

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

> オンボードキーマネージャがCCモードで有効になっている場合 (`cc-mode-enabled=yes`）では、システムの動作は次のように変更されます。
>
> - Common Criteria モードで動作している場合、クラスタパスフレーズの試行に連続して失敗したかどうかが監視されます。
>
> NetApp Storage Encryption （ NSE ）が有効になっている場合に、ブート時に正しいクラスタパスフレーズを入力しないと、システムはドライブを認証できず、自動的にリブートされます。これを修正するには、ブートプロンプトで正しいクラスタパスフレーズを入力する必要があります。ブート後、パラメータとしてクラスタパスフレーズを必要とするコマンドに対して、最大 5 回連続してクラスタパスフレーズを 24 時間以内に入力することができます。制限に達した場合（たとえば、クラスタのパスフレーズを 5 回連続して正しく入力できなかった場合など）は、 24 時間のタイムアウトが経過するまで待つか、ノードをリブートして制限をリセットする必要があります。
>
> - システムイメージの更新では、 NetApp RSA-3072 コード署名証明書と SHA-384 コード署名ダイジェストを使用して、通常の NetApp RSA-2048 コード署名証明書および SHA-256 コード署名ダイジェストではなく、イメージの整合性をチェックします。
>
> upgrade コマンドは、さまざまなデジタル署名をチェックして、イメージの内容が変更されていないか、壊れていないかを確認します。検証に成功した場合は、イメージの更新プロセスが次の手順に進みます。成功しなかった場合は、イメージの更新が失敗します。システムの更新については ' cluster image マニュアル・ページを参照してください

> オンボードキーマネージャは、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。通常の動作条件下では、システムが停止すると 30 秒以内に揮発性メモリの内容がクリアされます。

作業を開始する前に

- 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. キー管理ツールの setup コマンドを開始します。

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

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

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

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

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

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

   指定された "cc-mode" パスフレーズが 64 文字未満の場合、キー管理ツールのセットアップ操作によってパスフレーズのプロンプトが再表示されるまでに 5 秒の遅延が発生します。

3. パスフレーズの確認のプロンプトでパスフレーズをもう一度入力します。
4. 認証キーが作成されたことを確認します。

   `security key-manager key query -node node`

   。 `security key-manager key query` コマンドは、に置き換わるものです `security key-manager query key` コマンドを実行しますコマンド構文全体については、マニュアルページを参照してください。

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

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

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

       Vserver: cluster1
   Key Manager: onboard
          Node: node2

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

完了後

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

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

ONTAP 9.5 以前でオンボードキー管理を有効にします

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。

このタスクについて

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

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

デフォルトでは、ノードのリブート時にキー管理ツールのパスフレーズを入力する必要はありません。ONTAP 9.4以降では、 `-enable-cc-mode yes` リブート後にユーザにパスフレーズの入力を求めるオプション。

NVEの場合は、を設定します `-enable-cc-mode yes`を使用して作成したボリューム `volume create` および `volume move start` コマンドは自動的に暗号化されます。の場合 `volume create`を指定する必要はありません `-encrypt true`。の場合 `volume move start`を指定する必要はありません `-encrypt-destination true`。

> パスフレーズの試行に失敗した場合は、ノードを再起動する必要があります。

作業を開始する前に

- 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` リブート後にユーザにキー管理ツールのパスフレーズの入力を求めるオプション。NVEの場合は、を設定します `-enable-cc-mode yes`を使用して作成したボリューム `volume create` および `volume move start` コマンドは自動的に暗号化されます。

   次の例では、リブートのたびにパスフレーズの入力を求めずに、 cluster1 でキー管理ツールをセットアップします。

```
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. 入力するコマンド `yes` オンボードキー管理を設定するプロンプトが表示されます。
3. パスフレーズのプロンプトで 32 ～ 256 文字のパスフレーズを入力します。または、 64 ～ 256 文字のパスフレーズを「 cc-mode] 」に入力します。

> 指定された "cc-mode" パスフレーズが 64 文字未満の場合、キー管理ツールのセットアップ操作によってパスフレーズのプロンプトが再表示されるまでに 5 秒の遅延が発生します。

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

   `security key-manager key show`

   コマンド構文全体については、マニュアルページを参照してください。

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

Node: node1
Key Store: onboard
Key ID                                                           Used By
-----------------------------------------------------------------
--------
00000000000000000200000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
00000000000000000200000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                           Used By
-----------------------------------------------------------------
--------
00000000000000000200000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
00000000000000000200000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

完了後

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

オンボードキーマネージャのパスフレーズを設定するときは、災害時に備えて、ストレージシステムの外部の安全な場所にも手動で情報をバックアップしておく必要があります。を参照してください "オンボードキー管理情報を手動でバックアップ"。

FIPS ドライブまたは **SED** にデータ認証キーを割り当てる（オンボードキー管理）

を使用できます `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。このキーは、クラスタノードでドライブのデータにアクセスする際に使用します。

このタスクについて

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

作業を開始する前に

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`*

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

   > を使用できます `security key-manager key query -key-type NSE-AK` キーIDを表示するコマンド。

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   0000000000000000020000000000010019215b9738bc7b43d4698c80246db1f4

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

2. 認証キーが割り当てられたことを確認します。

   `storage encryption disk show`

   コマンド構文全体については、マニュアルページを参照してください。

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
--------------------------------------------------------------------
0.0.0   data
000000000000000002000000000000100192 15b9738bc7b43d4698c80246db1f4
0.0.1   data
000000000000000002000000000000100598 51742AF2703FC91369B7DB47C4722
[...]
```

FIPS ドライブに FIPS 140-2 認証キーを割り当てます

を使用できます `storage encryption disk modify` コマンドにを指定します `-fips-key-id` FIPS 140-2認証キーをFIPSドライブに割り当てるオプション。このキーは、ドライブに対する DoS 攻撃を防止するなど、データアクセス以外のドライブ処理に使用されます。

このタスクについて

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。

この手順 はシステムの停止を伴いません。

作業を開始する前に

ドライブファームウェアで FIPS 140-2 準拠がサポートされている必要があります。。 "NetApp Interoperability Matrix Tool で確認できます" サポートされているドライブファームウェアのバージョンに関する情報が含まれます。

手順

1. 最初に、データ認証キーを割り当てておく必要があります。これは、を使用して実行できます 外部キー管理ツール または オンボードキーマネージャ。コマンドを使用して、キーが割り当てられていることを確認します `storage encryption disk show`。
2. SED に FIPS 140-2 認証キーを割り当てます。

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

   を使用できます `security key-manager query` キーIDを表示するコマンド。

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

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

3. 認証キーが割り当てられたことを確認します。

   `storage encryption disk show -fips`

   コマンド構文全体については、マニュアルページを参照してください。

```
cluster1::> storage encryption disk show -fips
Disk    Mode FIPS-Compliance Key ID
------  ----
-------------------------------------------------------------------
2.10.0  full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
2.10.1  full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
[...]
```

KMIP サーバ接続に対して、クラスタ全体の FIPS 準拠モードを有効にします

を使用できます `security config modify` コマンドにを指定します `-is-fips-enabled` 転送中のデータに対してクラスタ全体のFIPS準拠モードを有効にするオプション。これにより、クラスタが KMIP サーバに接続する際に FIPS モードの OpenSSL が使用されるようになります。

このタスクについて

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。

作業を開始する前に

- 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
```

コマンド構文全体については、マニュアルページを参照してください。

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

3. クラスタ全体の FIPS 準拠モードを有効にします。

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

コマンド構文全体については、マニュアルページを参照してください。

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

```
security config show
```

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

ネットアップの暗号化を管理

ボリュームデータの暗号化を解除します

を使用できます `volume move start` ボリュームデータを移動および暗号化解除するコマンド。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。または、クラスタ管理者から権限を委譲されたSVM管理者を指定することもできます。詳細については、を参照してください "volume move コマンドの実行権限を委譲します"。

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`

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

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

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

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

2. ボリュームで暗号化が無効になっていることを確認します。

   `volume show -encryption`

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

   次のコマンドは、ボリュームが上にあるかどうかを表示します `cluster1` 暗号化：

   ```
   cluster1::> volume show -encryption

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

暗号化されたボリュームを移動します

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

このタスクについて

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

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。または、クラスタ管理者から権限を委譲されたSVM管理者を指定することもできます。詳細については、を参照してください "volume moveコマンドの実行権限を委譲する"。

手順

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

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

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

   次のコマンドは、という名前の既存のボリュームを移動します `vol1` デスティネーションアグリゲートに移動します `aggr3` ボリューム上のデータは暗号化されたままになります。

   ```
   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`

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

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

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

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

volume move コマンドの実行権限を委譲します

を使用できます `volume move` コマンドを使用して、既存のボリュームを暗号化したり、暗号化されたボリュームを移動したり、ボリュームの暗号化を解除したりできます。クラスタ管理者はを実行できます `volume move` コマンド自体を実行することも、

コマンドの実行権限をSVM管理者に委譲することもできます。

このタスクについて

デフォルトでは、SVM管理者にはが割り当てられます `vsadmin` ロール。ボリュームを移動する権限は含まれません。を割り当てる必要があります `vsadmin-volume` の実行を許可するSVM管理者のロール `volume move` コマンドを実行します

ステップ

1. を実行する権限を委任します `volume move` コマンドを実行します

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

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

   次のコマンドは、SVM管理者にを実行する権限を付与します `volume move` コマンドを実行します

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

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

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

このタスクについて

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

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

> を使用することはできません `volume encryption rekey start` をクリックしてSnapLockボリュームのキーを変更します。

手順

1. 暗号化キーを変更します。

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

   次の例は、の暗号化キーを変更します `vol1` SVM上`vs1`：

```
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`

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

   次のコマンドは、キー変更処理のステータスを表示します。

```
cluster1::> volume encryption rekey show

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

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

   `volume show -is-encrypted true`

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

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

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

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

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

セキュリティのベストプラクティスとして、ボリュームの暗号化キーを定期的に変更することが重要です。を使用できます `volume move start` コマンドを使用して暗号化キーを変更します。を使用する必要があります `volume move start` ONTAP 9.2以前では、ボリュームを移動するアグリゲートは同じアグリゲートでも別のアグリゲートでもかまいません。

このタスクについて

を使用することはできません `volume move start` をクリックしてSnapLock またはFlexGroup ボリュームのキーを変更します。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。または、クラスタ管理者から権限を委譲

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

手順

1. 既存のボリュームを移動し、暗号化キーを変更します。

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

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

   次のコマンドは、という名前の既存のボリュームを移動します **vol1** デスティネーションアグリゲートに移動します **aggr2** 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
   ```

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

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

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

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

NetApp Storage Encryption の認証キーをローテーションします

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

このタスクについて

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

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

手順

1. を使用します `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する必要があります。

2. を使用します `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。

暗号化されたボリュームを削除する

を使用できます `volume delete` 暗号化されたボリュームを削除するコマンド。

作業を開始する前に

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

ステップ

1. 暗号化されたボリュームを削除します。

   `volume delete -vserver` *`SVM_name`* `-volume` *`volume_name`*

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

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

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

   入力するコマンド `yes` 削除を確認するプロンプトが表示されたら、

   24 時間後にボリュームの暗号化キーが削除されます。

   使用 `volume delete` を使用 `-force true` ボリュームを削除して対応する暗号化キーをただちに破棄するオプション。このコマンドには advanced 権限が必要です。詳細については、のマニュアルページを参照してください。

完了後

を使用できます `volume recovery-queue` コマンドを使用して、を実行したあとに保持期間内に削除されたボリュームをリカバリします `volume delete` コマンドを実行します

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

"ボリュームリカバリ機能の使用方法"

暗号化されたボリューム上のデータをセキュアにパージします

暗号化されたボリュームのデータをセキュアにパージする方法の概要

ONTAP 9.4 以降では、セキュアパージを使用して、 NVE 対応ボリューム上のデータを無停止でスクラビングできます。暗号化されたボリュームのデータをスクラビングすることで、「柱」、「ブロックが上書きされたときにデータトレースが残されている」などの物理メディアからデータをリカバリすることができなくなります。また、解約するテナントのデータを安全に削除することもできます。

セキュアパージの対象となるのは、 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で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。

セキュアパージの機能は、 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 および FlexGroup でサポートされています。
- パージするボリュームが SnapMirror 関係のソースである場合は、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 データ保護を使用するボリュームと、 SnapMirror データ保護（ DP ）を使用していないボリュームまたは SnapMirror 拡張データ保護を使用しているボリュームで異なります。
  - デフォルトでは、 SnapMirror データ保護（ DP ）モードを使用するボリュームは、ボリューム移動の再暗号化方式を使用してデータを再暗号化します。
  - デフォルトでは、 SnapMirror データ保護を使用していないボリュームや SnapMirror 拡張データ保護（ XDP ）モードを使用しているボリュームでは、インプレースの再暗号化方式を使用します。
  - これらのデフォルト値は、を使用して変更できます `secure purge re-encryption-method [volume-move|in-place-rekey]` コマンドを実行します
- デフォルトでは、セキュアパージ処理の実行中に、 FlexVol ボリューム内のすべての Snapshot コピーが自動的に削除されます。デフォルトでは、 FlexGroup の Snapshot および SnapMirror データ保護を使用するボリュームは、セキュアパージ処理の実行中に自動的に削除されません。これらのデフォルト値は、を使用して変更できます `secure purge delete-all-snapshots [true|false]` コマンドを実行します

ONTAP 9.7以前：

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

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

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

  移動されたボリュームは現在のアグリゲートに残ります。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。

SnapMirror 関係なしで暗号化されたボリューム上のデータをセキュアにパージします

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

このタスクについて

削除されたファイルのデータ量によっては、セキュアパージが完了するまでに数分から数時間かかることがあります。を使用できます `volume encryption secure-purge show` コマンドを使用して処理のステータスを表示します。を使用できます `volume encryption secure-purge abort` コマンドを入力して処理を終了します。

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

作業を開始する前に

- 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、セキュアパージするファイルを削除します。
   - SAN ホストで、パージするファイルに属するブロックのために、 LUN から安全にパージまたはパンチ穴を開ける LUN を削除します。
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. 安全にパージするファイルがスナップショットにある場合は、スナップショットを削除します。

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

4. 削除したファイルを安全にパージします。

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

   次のコマンドは、で削除したファイルをセキュアパージします `vol1` SVM上`vs1`：

   ```
   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非同期関係にある暗号化されたボリューム上のデータのセキュアパージ

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

作業を開始する前に

- 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。

このタスクについて

削除されたファイルのデータ量によっては、セキュアパージが完了するまでに数分から数時間かかることがあります。を使用できます `volume encryption secure-purge show` コマンドを使用して処理のステータスを表示します。を使用できます `volume encryption secure-purge abort` コマンドを入力して処理を終了します。

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

手順

1. ストレージシステムで、advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. セキュアパージするファイルまたは LUN を削除します。
   - NAS クライアントで、セキュアパージするファイルを削除します。
   - SAN ホストで、パージするファイルに属するブロックのために、 LUN から安全にパージまたはパンチ穴を開ける LUN を削除します。
3. 非同期関係のデスティネーションボリュームを安全にパージするように準備します。

   ```
   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. セキュアにパージするファイルが Snapshot コピーにある場合は、 Snapshot コピーを削除します。

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

5. セキュアパージの対象となるファイルがベース Snapshot コピー内にある場合は、次の手順を実行します。

   a. SnapMirror非同期関係のデスティネーションボリュームにSnapshotコピーを作成します。

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

   b. SnapMirror を更新してベースの Snapshot コピーをフォワードします。

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

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

a. ベース Snapshot コピーの数に 1 を加えた値と同じ手順（ a ）および（ b ）を繰り返します。

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

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

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

6. 削除したファイルを安全にパージします。

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

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

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

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

7. セキュアパージ処理のステータスを確認します。

   `volume encryption secure-purge show`

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

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

このタスクについて

削除されたファイルのデータ量によっては、セキュアパージが完了するまでに数分から数時間かかることがあります。を使用できます `volume encryption secure-purge show` コマンドを使用して処理のステータスを表示します。を使用できます `volume encryption secure-purge abort` コマンドを入力して処理を終了します。

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

作業を開始する前に

- 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、セキュアパージするファイルを削除します。
   - SAN ホストで、パージするファイルに属するブロックのために、 LUN から安全にパージまたはパンチ穴を開ける LUN を削除します。

3. 非同期関係のデスティネーションボリュームを安全にパージするように準備します。

   ```
   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. セキュアにパージするファイルが Snapshot コピーにある場合は、 Snapshot コピーを削除します。

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

5. セキュアなパージファイルがベースまたは共通の Snapshot コピーに含まれている場合は、 SnapMirror を更新して共通の Snapshot コピーをフォワードします。

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

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

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

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

   この手順は両方のボリュームで実行します。

7. 削除したファイルを安全にパージします。

   ```
   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 'SMV "vs1 `" 上の "vol1" 上の削除されたファイルを安全にパージします

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

8. セキュアパージ処理のステータスを確認します。

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

オンボードキー管理のパスフレーズを変更します

セキュリティのベストプラクティスとして、オンボードキー管理のパスフレーズを定期的に変更することが重要です。あとで使用できるように、ストレージシステムの外部の安全な場所にオンボードキー管理の新しいパスフレーズをコピーしておく必要があります。

作業を開始する前に

- 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。

手順

1. advanced 権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. オンボードキー管理のパスフレーズを変更します。

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

   コマンド構文全体については、マニュアルページを参照してください。

   次のONTAP 9.6のコマンドでは、のオンボードキー管理のパスフレーズを変更できます `cluster1`：

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

3. 入力するコマンド `y` で、オンボードキー管理のパスフレーズを変更するよう求められます。
4. 現在のパスフレーズのプロンプトで現在のパスフレーズを入力します。
5. 新しいパスフレーズのプロンプトで 32 〜 256 文字のパスフレーズを入力します。または、 64 〜 256 文字のパスフレーズを「 cc-mode] 」に入力します。

   指定された "cc-mode" パスフレーズが 64 文字未満の場合、キー管理ツールのセットアップ操作によってパスフレーズのプロンプトが再表示されるまでに 5 秒の遅延が発生します。

6. パスフレーズの確認のプロンプトでパスフレーズをもう一度入力します。

完了後

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

- ONTAP 9.5以前では、を実行する必要があります `security key-manager update-passphrase` パートナークラスタで同じパスフレーズを使用。
- ONTAP 9.6以降では、を実行するように求められます `security key-manager onboard sync` パートナークラスタで同じパスフレーズを使用。

あとで使用できるように、ストレージシステムの外部の安全な場所にオンボードキー管理のパスフレーズをコピーしておく必要があります。

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

"オンボードキー管理情報の手動でのバックアップ"

オンボードキー管理情報を手動でバックアップ

オンボードキーマネージャのパスフレーズを設定する場合、ストレージシステムの外部の安全な場所にオンボードキー管理の情報をコピーしておく必要があります。

必要なもの

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

このタスクについて

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

手順

1. advanced 権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. クラスタのキー管理バックアップ情報を表示します。

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

コマンド構文全体については、マニュアルページを参照してください。

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

[+]

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

     --------------------------BEGIN BACKUP--------------------------
     TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
     QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
     dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
     3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAA
     IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAAJAGr3tJA/LRzU
     QRHwv+1aWvAAAAAAAAAAACQAAAAAAAAAgAAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
     BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
     AQAAAAMAAAAYAQAAAAAAADA5/ccAAAAAIgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAA
     AAAAAAAAAAACAAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAACIAAAAAAAAA
     KAAAAAAAAACI8z/bAAAAAAAAAAAAAAAAAgAAAAAAAAAQAbxMcI4qiaMS4Uts5tTUnU
     AAAAAAAAAAAkAAAAAAAAAAAIAAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5Smyj
     LSgoK/qc8FAmMMcrRXY6uriulnL0WPB/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAwAAABgBAAAAAAAA
     1cNLLwAAAAAiAAAAAAAAAAACgAAAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAAAIAAAAAAAAAkA
     ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAAIgAAAAAAAAAoAAAAAAAAAAJ4/cQsAAAAA
     AAAAAAAAAAACAAAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAAAAACQAAAAAAAAAA
     gAAAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rrH4nPQM0n
     rDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     ---------------------------END BACKUP---------------------------
```

1. 災害時に備えて、ストレージシステムの外部の安全な場所にバックアップ情報をコピーします。

オンボードキー管理の暗号化キーをリストア

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

作業を開始する前に

- 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。詳細については、を参照してください "外部キー管理からオンボードキー管理への移行"
- このタスクを実行するには、クラスタ管理者である必要があります。

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

ONTAP 9.6 以降

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

1. キーのリストアが必要であることを確認します。+
   `security key-manager key query -node node`
2. キーを復元します。+
   `security key-manager onboard sync`

   コマンド構文全体については、マニュアルページを参照してください。

   ONTAP 9.6 の次のコマンドを使用して、オンボードキー階層のキーを同期します。

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

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

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

ルートボリュームを暗号化した**ONTAP 9.8**以降

ONTAP 9.8 以降を実行していて、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。ブートメディアの交換を行う場合も、このプロセスが必要です。

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

   ノードがブートメニューに戻ります。

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

ONTAP 9.5 以前

1. キーのリストアが必要であることを確認します。+
   `security key-manager key show`
2. ONTAP 9.8 以降を実行していて、ルート・ボリュームが暗号化されている場合は、次の手順を実行します。

ONTAP 9.6 または 9.7 を実行している場合、または ONTAP 9.8 以降を実行していて、ルートボリュームが暗号化されていない場合は、この手順を省略してください。

3. キーを復元します。+
   `security key-manager setup -node node`

   コマンド構文全体については、マニュアルページを参照してください。

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

外部キー管理の暗号化キーをリストアします

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などに実行します。

このタスクについて

ONTAP 9.6以降では、を使用できます `security key-manager key query -node node_name` コマンドを実行して、キーのリストアが必要かどうかを確認します。

ONTAP 9.5以前では、を使用できます `security key-manager key show` コマンドを実行して、キーのリストアが必要かどうかを確認します。

> 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は、Flash Cacheモジュール上のデータを暗号化しません。

作業を開始する前に

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. bootargを設定します。
      [] `setenv kmip.init.ipaddr <ip-address>` []
      `setenv kmip.init.netmask <netmask>`
      [] `setenv kmip.init.gateway <gateway>` []
      `setenv kmip.init.interface e0M`
      [+]
      `boot_ontap`

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

   c. プロンプトに従って管理証明書を入力します。

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

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

2. キーをリストアします。

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

> node デフォルトはすべてのノードです。コマンド構文全体については、マニュアルページを参照してください。このコマンドは、オンボードキー管理が有効な場合はサポートされません。

次のONTAP 9.6のコマンドは、外部キー管理の認証キーをのすべてのノードにリストアします cluster1：

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

SSL 証明書を交換します

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。

作業を開始する前に

- クラスタ（ KMIP クライアント証明書）の交換用のパブリック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（ KMIP server-ca 証明書）の交換用のパブリック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 環境では、両方のクラスタのKMIP SSL証明書を置き換える必要があります。

> 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で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した証明書を使用するようにキー管理ツールの設定を更新すると、新しいクライアント証明書の公開鍵と秘密鍵が以前にインストールしたキーと異なる場合にエラーが返されます。サポート技術情報の記事を参照してください "新しいクライアント証明書の公開鍵または秘密鍵が、既存のクライアント証明書と異なります" このエラーを無視する方法については、を参照してください。

FIPS ドライブまたは SED を交換します

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 ペアが使用している場合 "SAS ドライブまたは NVMe ドライブの暗号化（ SED 、 NSE 、 FIPS ）"、の手順に従ってください "FIPS ドライブまたは SED を非保護モードに戻します" システムを初期化する前の HA ペア内のすべてのドライブ（ブートオプション 4 または 9 ）。そうしないと、ドライブを転用した場合にデータが失われる可能性があります。

作業を開始する前に

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

手順

1. ディスクが障害状態としてマークされていることを確認します。

   ```
   storage disk show -broken
   ```

   コマンド構文全体については、マニュアルページを参照してください。

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

2. ディスクシェルフモデルのハードウェアガイドの指示に従い、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
   ```

   コマンド構文全体については、マニュアルページを参照してください。

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

4. 新しいディスクが割り当てられたことを確認します。

   ```
   storage encryption disk show
   ```

   コマンド構文全体については、マニュアルページを参照してください。

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
--------------------------------------------------------------------
0.0.0   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
0.0.1   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
1.10.0  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
1.10.1  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
2.1.1   open 0x0
[...]
```

5. FIPS ドライブまたは SED にデータ認証キーを割り当てます。

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

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

   "FIPS ドライブに FIPS 140-2 認証キーを割り当てています"

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します

FIPS ドライブまたは SED のデータにアクセスできない概要を確認します

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。

FIPS ドライブまたは **SED** を完全消去します

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て、そのドライブを新しいデータに使用する場合は、を使用できます `storage encryption disk sanitize` コマンドを使用してドライブを完全消去します。

このタスクについて

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。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. 保持する必要のあるデータを別のディスク上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`*

   コマンド構文全体については、マニュアルページを参照してください。

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

3. 完全消去する FIPS ドライブまたは SED のディスク ID を確認します。

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

   コマンド構文全体については、マニュアルページを参照してください。

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   --------------------------------------------------------------------
   0.0.0   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   1.10.2  data
   F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
   [...]
   ```

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

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

   を使用できます `security key-manager query` キーIDを表示するコマンド。

   ```
   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`

   このコマンドで完全消去できるのは、ホットスペアディスクと破損ディスクのみです。タイプに関係なくすべてのディスクを完全消去するには、を使用します `-force-all-state` オプションコマンド構文全体については、マニュアルページを参照してください。

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

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

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

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

6. 完全消去したディスクの障害状態を解除します。
   `storage disk unfail -spare true -disk disk_id`
7. ディスクに所有者が設定されて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`

   を実行します `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。ディスクの障害状態を再度解除します。
   `storage disk unfail -spare true -disk disk_id`
10. ディスクがスペアとしてアグリゲートで再利用できる状態になったことを確認します。
   `storage disk show -disk disk_id`

FIPS ドライブまたは **SED** を破棄します

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、ドライブを再利用する必要もない場合は、を使用できます `storage encryption disk destroy` コマンドを使用してディスクを破棄します。

このタスクについて

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

> （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。

作業を開始する前に

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. 保持しておく必要のあるデータを別のディスク上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 のアグリゲートを削除します。

   `storage aggregate delete -aggregate aggregate_name`

   コマンド構文全体については、マニュアルページを参照してください。

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

3. 破棄する FIPS ドライブまたは SED のディスク ID を確認します。

   `storage encryption disk show`

   コマンド構文全体については、マニュアルページを参照してください。

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
--------------------------------------------------------------------
0.0.0   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
0.0.1   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
1.10.2  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
[...]
```

4. ディスクを破棄します。

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

   コマンド構文全体については、マニュアルページを参照してください。

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

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

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

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

FIPSドライブまたは**SED**の緊急時のシュレッドデータ

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

作業を開始する前に

- 使用可能な電力がない KMIP サーバを使用している場合は、 KMIP サーバで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。

ステップ

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

状況	作業

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

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

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

コマンド構文全体については、マニュアルページを参照してください。

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

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。

作業を開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

このタスクについて

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、このプロセスを開始する前にパーティショニングされていないディスクである必要があります。

> ディスクのパーティショニングを解除するコマンドはdiagレベルでのみ使用でき、ネットアップサポートの指示があった場合にのみ実行してください。続行する前に、**NetApp**サポートに問い合わせることを強くお勧めします。ナレッジベースの記事も参照してください。 "ONTAP でスペアドライブのパーティショニングを解除する方法"。

手順

1. FIPS ドライブまたは SED を使用可能な状態に戻します。

SED の状況	実行する手順

FIPS 準拠モードでないか、 FIPS 準拠モードで FIPS キーを使用できます	a. 権限レベルを advanced に設定します。
	`set -privilege advanced`
	b. FIPSキーをデフォルトのメーカーセキュアIDである0x0にリセットします。
	`storage encryption disk modify -fips-key-id 0x0 -disk` *`disk_id`*
	c. 処理が成功したことを確認します。
	`storage encryption disk show-status`
	処理に失敗した場合は、このトピックのPSIDプロセスを使用してください。
	d. 破損ディスクを完全消去します。
	`storage encryption disk sanitize -disk` *`disk_id`*
	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` 次の手順に進む前に。
	e. 完全消去したディスクの障害状態を解除します。
	`storage disk unfail -spare true -disk` *`disk_id`*
	f. ディスクに所有者が設定されて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`*
	を実行します `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。ディスクの障害状態を再度解除します。
	`storage disk unfail -spare true -disk` *`disk_id`*
	h. ディスクがスペアとしてアグリゲートで再利用できる状態になったことを確認します。
	`storage disk show -disk` *`disk_id`*

FIPS 準拠モードであるが 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`* 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` 次の手順に進む前に。 d. ONTAP 9.8P5以前を実行している場合は、次の手順に進みます。ONTAP 9.8P6以降を実行している場合は、完全消去したディスクの障害状態を解除します。 `storage disk unfail -disk` *`disk_id`* e. ディスクに所有者が設定されて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`* を実行します `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。ディスクの障害状態を再度解除します。 `storage disk unfail -spare true -disk` *`disk_id`* g. ディスクがスペアとしてアグリゲートで再利用できる状態になったことを確認します。 `storage disk show -disk` *`disk_id`*

コマンド構文全体については、を参照してください "コマンドリファレンス"。

FIPS ドライブまたは SED を非保護モードに戻します

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

HA ペアで暗号化 SAS ドライブまたは NVMe ドライブ（ SED 、 NSE 、 FIPS ）を使用している場合は、システムを初期化する前に、 HA ペア内のすべてのドライブでこのプロセスに従う必要があります（ブートオプション 4 または 9 ）。そうしないと、ドライブを転用した場合にデータが失われる可能性があります。

作業を開始する前に

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
   ```

   を使用できます `security key-manager query` キーIDを表示するコマンド。

   ```
   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.
   ```

   次のコマンドで、処理が成功したことを確認します。

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

   show -statusコマンドを繰り返して、「Disksでした」と「Disks done」の番号が同じになるようにします。

   ```
   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
   ```

   の値 `-data-key-id` SASドライブまたはNVMeドライブを非保護モードに戻すかどうかに関係なく、0x0 に設定する必要があります。

   を使用できます `security key-manager query` キーIDを表示するコマンド。

```
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.
```

次のコマンドで、処理が成功したことを確認します。

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

番号が同じになるまで、 show -status コマンドを繰り返します。「disks begin」と「disks done」の数値が同じであれば、処理は完了です。

メンテナンスモード

ONTAP 9.7以降では、FIPSドライブのキーを保守モードから変更できます。保守モードは、前のセクションのONTAP CLI手順を使用できない場合にのみ使用してください。

手順

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

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

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

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

3. FIPS認証キーのキーが変更されたことを確認します。

   ```
   disk encrypt show_fips
   ```

4. データ認証キーのキーが変更されたことを確認します。

   ```
   disk encrypt show
   ```

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

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

外部キー管理ツールの接続を削除します

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。

このタスクについて

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。

作業を開始する前に

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。

ステップ

1. 現在のノードから KMIP サーバを切断します。

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

MetroCluster 環境では、管理SVMの両方のクラスタで上記のコマンドを繰り返す必要があります。

コマンド構文全体については、マニュアルページを参照してください。

次のONTAP 9.6のコマンドは、に対する2つの外部キー管理サーバへの接続を無効にします `cluster1`、最初の名前 `ks1`では、デフォルトポート5696をリッスンしています。2番目のポートはIPアドレス10.0.0.20で、ポート24482を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
```

外部キー管理サーバのプロパティを変更します

ONTAP 9.6以降では、 `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します。

作業を開始する前に

- 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、管理SVMの両方のクラスタで上記の手順を繰り返す必要があります。

手順

1. ストレージシステムで、 advanced 権限レベルに切り替えます。

```
set -privilege advanced
```

2. クラスタの外部キー管理サーバのプロパティを変更します。

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

> タイムアウト値は秒単位で表されます。ユーザ名を変更すると、新しいパスワードの入力を求められます。 クラスタのログインプロンプトでコマンドを実行すると、 *admin_SVM* デフォルトでは、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、のタイムアウト値を45秒に変更します `cluster1` デフォルトポート5696をリスンしている外部キー管理サーバ：

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

3. SVM の外部キー管理サーバのプロパティを変更します（ NVE のみ）。

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

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

のユーザ名とパスワードを変更するコマンドの例を次に示します `svm1` デフォルトポート5696をリスンしている外部キー管理サーバ：

```
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。

オンボードキー管理から外部キー管理に移行

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。

作業を開始する前に

- 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します"

- 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を解除します"

- このタスクを実行するには、クラスタ管理者である必要があります。

ステップ

1. クラスタのオンボードキー管理の設定を削除します。

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

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

外部キー管理からオンボードキー管理に移行します

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

作業を開始する前に

- 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します"

- 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を削除しています"

- 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

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

ONTAP 9.6 以降

1. advanced 権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. 次のコマンドを使用します。

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

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

ONTAP 9.5 以前

次のコマンドを使用します。

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

ブートプロセス時にキー管理サーバにアクセスできない場合

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

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

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

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

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

SED では、セキュリティ対策として、無許可のアクセス試行回数が制限されています。試行回数が上限に達すると、既存データへのアクセスが無効になります。ストレージシステムが指定されたどのキー管理サーバにもアクセスできず、適切な認証キーを取得できない場合は、デフォルトのキーを使用した認証のみ試行できます。この場合、認証が失敗したり、パニック状態になったりします。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設定されているストレージシステムはブートループに入り、 SED での認証が連続して失敗します。

仕様では、次のような場合にストレージシステムを停止して、認証の連続失敗回数の上限を超えたことが原因で SED が永続的にロックされても、ストレージシステムがブートループに入ったり、意図しないデータ損失が発生したりすることを回避します。ロックアウト保護の制限とタイプは、 SED の仕様とタイプによって異なります。

SEDタイプ	ロックアウトされるまでの認証の連続失敗回数	安全制限に達したときのロックアウト保護タイプ
HDD	一、〇 二四	永続的。適切な認証キーが再び使用可能になった場合でも、データをリカバリできません。
ファームウェアリビジョンが NA00 または NA01 の X440_PHM2800MCTO 800GB NSE SSD	5.	一時的。ロックアウトが有効になるのは、ディスクの電源が再投入されるまでです。
ファームウェアリビジョンがNA00またはNA01のX577_PHM2800MCTO 800GB NSE SSD	5.	一時的。ロックアウトが有効になるのは、ディスクの電源が再投入されるまでです。
ファームウェアリビジョンが上記よりも高い X440_PHM2800MCTO 800GB NSE SSD	一、〇 二四	永続的。適切な認証キーが再び使用可能になった場合でも、データをリカバリできません。
ファームウェアリビジョンが上位のX577_PHM2800MCTO 800GB NSE SSD	一、〇 二四	永続的。適切な認証キーが再び使用可能になった場合でも、データをリカバリできません。
その他すべての SSD モデル	一、〇 二四	永続的。適切な認証キーが再び使用可能になった場合でも、データをリカバリできません。

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

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

暗号化をデフォルトで無効にする

ONTAP 9.7 以降では、ボリューム暗号化（ VE ）ライセンスがあり、オンボードキーマネージャまたは外部キーマネージャを使用している場合、アグリゲートとボリューム暗号化がデフォルトで有効になります。必要に応じて、暗号化をデフォルトでクラスタ全体で無効にすることができます。

作業を開始する前に

このタスクを実行するには、クラスタ管理者であるか、クラスタ管理者から権限を委譲された SVM 管理者である必要があります。

ステップ

1. ONTAP 9.7 以降のクラスタ全体で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
```