



# **NVEの設定**

## **ONTAP 9**

NetApp  
February 12, 2026

# 目次

NVEの設定 .....	1
ONTAPクラスタバージョンがNVEをサポートしているかどうかを確認する .....	1
ONTAPクラスタにボリューム暗号化ライセンスをインストールする .....	1
外部キー管理の設定 .....	2
ONTAP NetApp Volume Encryptionを使用した外部キー管理の設定について学習します .....	2
ONTAP System Managerで外部キーマネージャを管理する .....	2
ONTAPクラスタにSSL証明書をインストールする .....	4
ONTAP 9.6以降でNVEの外部キー管理を有効にする .....	5
ONTAP 9.5以前でNVEの外部キー管理を有効にする .....	9
クラウド プロバイダを使用したONTAP データSVMのNVEキーの管理 .....	10
Barbican KMSでONTAPキーを管理する .....	13
ONTAP 9.6以降でNVEのオンボードキー管理を有効にする .....	18
ONTAP 9.5以前でNVEのオンボードキー管理を有効にする .....	20
新しく追加されたONTAPノードでオンボードキー管理を有効にする .....	23

# NVEの設定

## ONTAP クラスタバージョンがNVEをサポートしているかどうかを確認する

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

### タスク概要

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

### 手順

1. クラスタ バージョンがNVEをサポートしているかどうかを確認します。

```
version -v
```

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

## ONTAP クラスタにボリューム暗号化ライセンスをインストールする

VEライセンスを取得すると、クラスタ内のすべてのノードでこの機能を使用できます。NVEでデータを暗号化するには、このライセンスが必要です。["ONTAP One"](#)に含まれています。

ONTAP One より前のバージョンでは、VE ライセンスは暗号化バンドルに含まれていました。暗号化バンドルは現在提供されていませんが、引き続き有効です。現在必須ではありませんが、既存のお客様は["ONTAP Oneにアップグレード"](#)を選択できます。

### 開始する前に

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

### 手順

1. ["VEライセンスがインストールされていることを確認します"](#)。

VE ライセンスパッケージ名は `VE` です。

2. ライセンスがインストールされていない場合は、["System ManagerまたはONTAP CLIを使用してインストールします"](#)。

# 外部キー管理の設定

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

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

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

## ONTAP System Managerで外部キーマネージャを管理する

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

オンボード キー マネージャを使用する場合、キーはクラスタ内部のセキュアなデータベースで格納、管理されます。スコープはクラスタです。外部キー管理ツールを使用する場合、キーはクラスタの外部で格納、管理されます。スコープは、クラスタでもStorage VMでもあり得ます。1つ以上の外部キー管理ツールを使用できます。次の条件が適用されます。

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

外部キー管理ツールを使用する場合、Storage VMとクラスタごとに最大4つのプライマリ キー サーバを登録できます。各プライマリ キー サーバには、最大3台のセカンダリ キー サーバを追加してクラスタ化できます。

## 外部キー管理ツールの設定

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



### 手順

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

1. 次のいずれかのオプションを使用して、外部キー管理の設定を開始します。

ワークフロー	ナビゲーション	開始ステップ
--------	---------	--------

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


- プライマリ キー サーバーを追加するには、 **Add** を選択し、**IP Address or Host Name** および **Port** フィールドに入力します。
- 既にインストールされている証明書は、「**KMIP サーバー CA 証明書**」および「**KMIP クライアント証明書**」フィールドに表示されます。以下のいずれかの操作を実行できます：
  -  を選択して、キー マネージャーにマップするインストール済みの証明書を選択します。（複数のサービス CA 証明書を選択できますが、クライアント証明書は 1 つだけ選択できます。）
  - まだインストールされていない証明書を追加し、外部キー マネージャーにマップするには、\*新しい証明書の追加\*を選択します。
  - 外部キー マネージャーにマップしないインストール済みの証明書を削除するには、証明書名の横にある **x** を選択します。
- セカンダリ キー サーバーを追加するには、\*セカンダリ キー サーバー\*列で\*追加\*を選択し、詳細を入力します。
- \*保存\*を選択して設定を完了します。


## 既存の外部キー管理ツールの編集

すでに外部キー管理ツールの設定が完了している場合は、その設定を変更できます。



### 手順

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

Scope	ナビゲーション	開始ステップ
クラスタ スコープの外部キー マネージャ	クラスター > 設定	*セキュリティ*セクションまでスクロールします。*暗号化*で  を選択し、*外部キーマネージャーの編集*を選択します。

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

2. 既存の鍵サーバーは\*鍵サーバー\*テーブルにリストされます。以下の操作を実行できます：



-  **Add** を選択して新しいキー サーバーを追加します。
- キーサーバーを削除するには、キーサーバー名を含むテーブルセルの末尾にある  を選択します。そのプライマリキーサーバーに関連付けられているセカンダリキーサーバーも設定から削除されます。

## 外部キー管理ツールの削除

ボリュームが暗号化されていない場合は、外部キー管理ツールを削除できます。

### 手順

1. 次のいずれかの手順を実行して、外部キー管理を削除します。

Scope	ナビゲーション	開始ステップ
クラスタ スコープの外部キー マネージャ	クラスター > 設定	*Security*セクションまでスクロールします。*Encryption*で  を選択し、*Delete External Key Manager*を選択します。
Storage VMスコープ外部キー マネージャ	ストレージ > <b>Storage VM</b>	ストレージVMを選択します。*設定*タブを選択します。*セキュリティ*の*暗号化*セクションで、  を選択し、*外部キーマネージャの削除*を選択します。

## キー管理ツール間のキーの移行

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

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

## ONTAPクラスタにSSL証明書をインストールする

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

### タスク概要

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

開始する前に

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



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

手順

1. クラスタにSSL KMIPクライアント証明書をインストールします。

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

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

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

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

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

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

関連情報

- ["security certificate install"](#)

## ONTAP 9.6以降でNVEの外部キー管理を有効にする

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

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

タスク概要

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

台のサーバーを使用してください。

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

- `_クラスタスコープ_`を使用すると、クラスタ内のすべてのSVMに対して外部キー管理を設定できます。クラスタ管理者は、サーバーに保存されているすべてのキーにアクセスできます。
- ONTAP 9.6以降では、`_SVMスコープ_`を使用して、クラスタ内のデータSVMの外部キー管理を設定できます。これは、各テナントが異なるSVM（またはSVMセット）を使用してデータを提供するマルチテナント環境に最適です。特定のテナントのキーにアクセスできるのは、そのテナントのSVM管理者のみです。
- マルチテナント環境の場合は、次のコマンドを使用して `MT_EK_MGMT` のライセンスをインストールします：

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

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

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

オンボードキー管理はクラスタスコープで設定でき、外部キー管理はSVMスコープで設定できます。``security key-manager key migrate``コマンドを使用すると、クラスタスコープのオンボードキー管理からSVMスコープの外部キーマネージャにキーを移行できます。

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

開始する前に

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

手順

1. クラスタのキー管理ツールの接続を設定します。

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



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



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

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

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

## 2. SVMのキー管理ツールを設定します。

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



- SVMログインプロンプトでコマンドを実行すると、`SVM`デフォルトで現在のSVMが選択されます。`security key-manager external modify`コマンドを実行して、外部キー管理設定を変更できます。
- MetroCluster環境で、データSVMの外部キー管理を設定する場合、パートナークラスタで`security key-manager external enable`コマンドを繰り返す必要はありません。

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

```
svm11::> security key-manager external enable -vserver svm1 -key-servers
keyserver.svm1.com -client-cert SVM1ClientCert -server-ca-certs
SVM1ServerCaCert
```

## 3. 最後の手順をその他のSVMに対して繰り返します。



`security key-manager external add-servers` コマンドを使用して追加のSVMを設定することもできます。  
 `security key-manager external add-servers` コマンドは `security key-manager add` コマンドに代わるものです。link:<https://docs.netapp.com/us-en/ontap-cli/security-key-manager-external-add-servers.html>["ONTAPコマンド リファレンス"]で `security key-manager external add-servers` の詳細をご覧ください。

#### 4. 設定したすべてのKMIPサーバが接続されていることを確認します。

```
security key-manager external show-status -node node_name
```



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

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

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

8 entries were displayed.

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

```
volume encryption conversion start
```

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

#### 関連情報

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

## ONTAP 9.5以前でNVEの外部キー管理を有効にする

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

#### タスク概要

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

#### 開始する前に

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

#### 手順

1. クラスタ ノードのキー管理ツールの接続を設定します。

```
security key-manager setup
```

キー管理ツールのセットアップが開始されます。



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

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

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

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



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

- 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。

- 設定したすべてのKMIPサーバが接続されていることを確認します。

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

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

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

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

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

```
volume encryption conversion start
```

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

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

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

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

## タスク概要

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

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

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

- クラウド プロバイダ キー管理は、NetApp Storage Encryption（NSE）およびNetApp Aggregate Encryption（NAE）では使用できません。代わりに["外部KMIP"](#)を使用できます。
- クラウド プロバイダによるキー管理は、MetroCluster構成では利用できません。
- クラウド プロバイダによるキー管理を設定できるのは、データSVMのみです。

## 開始する前に

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

## 外部キー管理の有効化

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

## AWS

### 開始する前に

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

### ONTAP SVMでAWS KMSを有効にする

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

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

## Azure

### ONTAP SVMでAzure Key Vaultを有効にする

1. 始める前に、Azureアカウントから適切な認証クレデンシャル（クライアントシークレットまたは証明書）を取得する必要があります。また、クラスター内のすべてのノードが正常であることを確認する必要があります。これは次のコマンドで確認できます `cluster show`。`cluster show`の詳細については、"[ONTAPコマンド リファレンス](#)"を参照してください。
2. 権限レベルを advanced に設定します `set -priv advanced`
3. SVM で AKV を有効にします。`security key-manager external azure enable -client-id *client\_id* -tenant-id *tenant\_id* -name -key-id *key\_id* -authentication-method {certificate|client-secret}` プロンプトが表示されたら、Azure アカウントのクライアント証明書またはクライアント シークレットを入力します。
4. AKV が正しく有効化されていることを確認します： `security key-manager external azure show vserver svm\_name` サービスの到達可能性が正常でない場合は、データ SVM LIF を介して AKV キー管理サービスへの接続を確立します。

```
`security key-manager external azure`
```

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

## Google Cloud

### ONTAP SVMでCloud KMSを有効にする

1. 始める前に、Google Cloud KMSアカウントキーファイルの秘密鍵をJSON形式で取得してください。これはGCPアカウントで確認できます。また、クラスタ内のすべてのノードが正常であることを確認する必要があります。これはコマンド ``cluster show`` で確認できます。 ``cluster show`` の詳細については、["ONTAPコマンド リファレンス"](#)を参照してください。
2. 特権レベルを詳細に設定します： `set -priv advanced`
3. SVMでCloud KMSを有効にする ``security key-manager external gcp enable -vserver svm_name -project-id project_id-key-ring-name key_ring_name-key-ring-location key_ring_location -key-name key_name`` プロンプトが表示されたら、Service Account Private Keyを含むJSONファイルの内容を入力します
4. Cloud KMS が正しいパラメータで設定されていることを確認してください： `security key-manager external gcp show vservers svm_name`kms_wrapped_key_status`` のステータスは、暗号化されたボリュームが作成されていない場合、 `"UNKNOWN"` になります。サービス到達可能性が OK でない場合は、データ SVM LIF を介して GCP 鍵管理サービスへの接続を確立してください。

```
`security key-manager external gcp`
```

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

データSVMに1つ以上の暗号化ボリュームがすでに設定されており、対応するNVEキーが管理SVMのオンボードキーマネージャによって管理されている場合は、それらのキーを外部キー管理サービスに移行する必要があります。CLIでこれを行うには、次のコマンドを実行します： ``security key-manager key migrate -from -Vserver admin_SVM -to-Vserver data_SVM`` データSVMのすべてのNVEキーが正常に移行されるまで、テナントのデータSVMに新しい暗号化ボリュームを作成することはできません。

## 関連情報

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

## Barbican KMSでONTAPキーを管理する

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



Keystone"を認証に使用します。

#### タスク概要

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

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

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

#### 開始する前に

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

#### Barbican KMS 構成を作成してアクティブ化する

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

#### 手順

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

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

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



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

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



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

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

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

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

## 2. 新しい Barbican KMS 構成をアクティブ化します：

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

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

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

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

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

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

Vserver: svm1
Node: node1

Category: service_reachability
          Status: OK

Category: kms_wrapped_key_status
          Status: OK
```

## Barbican KMS構成の認証クレデンシャルと設定を更新する

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

### 手順

1. SVM の現在の Barbican KMS 構成を表示します：

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

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

2. Barbican KMS 構成の設定を更新します：

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

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

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

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

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

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

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

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

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

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

- a. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

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

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

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

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

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

#### 手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

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

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

`svm\_name`は、Barbican KMS 構成を持つ SVM の名前です。

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

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

### Barbican KMS 構成を無効化して削除する

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

## 手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. アクティブな Barbican KMS 構成を無効にします：

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

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

3. 非アクティブな Barbican KMS 構成を削除します：

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

## ONTAP 9.6以降でNVEのオンボードキー管理を有効にする

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

### タスク概要

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

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

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

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

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

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

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

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

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



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

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



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

#### 開始する前に

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

#### 手順

1. キー管理ツールのセットアップを開始します。

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



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

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



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

- 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。
- 認証キーが作成されたことを確認します。

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



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

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

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

```
volume encryption conversion start
```

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

#### 終了後の操作

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

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

#### 関連情報

- ["クラスターイメージコマンド"](#)
- ["セキュリティキー・マネージャ外部有効化"](#)
- ["セキュリティキー・マネージャキーのクエリ"](#)
- ["セキュリティキー・マネージャオンボード有効化"](#)

## ONTAP 9.5以前でNVEのオンボードキー管理を有効にする

オンボード キー マネージャを使用して、暗号化されたデータにアクセスする際にクラスター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ーで有効にする必要があります。

## タスク概要

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

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

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

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

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



パスフレーズの試行が失敗した場合は、ノードを再起動する必要があります。

## 開始する前に

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

### "外部キー管理からオンボード キー管理への移行"

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

## 手順

1. キー管理ツールのセットアップを開始します。

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



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

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

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

...

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

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



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

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

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

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

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

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



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

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

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

```
volume encryption conversion start
```

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

#### 終了後の操作

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

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

#### 関連情報

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

## 新しく追加されたONTAPノードでオンボードキー管理を有効にする

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



ONTAP 9.6 以降では、クラスタにノードを追加するたびに `security key-manager onboard sync` コマンドを実行する必要があります。

ONTAP 9.5 以前では、クラスタにノードを追加するたびに `security key-manager setup` コマンドを実行する必要があります。

オンボードキー管理を使用してクラスタにノードを追加する場合は、このコマンドを実行して、不足しているキーを更新します。

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

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

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

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

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

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



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

#### 関連情報

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

## 著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

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

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

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

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

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

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

## 商標に関する情報

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