NVE または NAE を使用してボリュームデータを暗号化する

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/ja-jp/ontap/encryption-at-rest/encrypt-volumes-concept.html on February 12, 2026. Always check docs.netapp.com for the latest.

目次

NVE または NAE を使用してボリューム データを暗号化する

NVEを使用したONTAPボリュームデータの暗号化について学ぶ

ONTAP 9.7以降では、NVEライセンスがあり、オンボードまたは外部のキー管理を使用している場合、アグリゲートとボリュームの暗号化がデフォルトで有効になります。ONTAP 9.6以前のバージョンでは、新しいボリュームおよび既存のボリュームで暗号化を有効にできます。ボリューム暗号化を有効にするには、VEライセンスをインストールしてキー管理を有効にしておく必要があります。NVEはFIPS-140-2レベル1に準拠しています。

ONTAPでVEライセンスを使用したアグリゲートレベルの暗号化を有効にする

ONTAP 9.7以降では、"VEライセンス"とオンボードまたは外部キー管理を使用している場合、新規に作成されたアグリゲートとボリュームはデフォルトで暗号化されます。ONTAP 9.6以降では、アグリゲートレベルの暗号化を使用して、暗号化するボリュームの包含アグリゲートにキーを割り当てることができます。

タスク概要

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

アグリゲートレベルの暗号化が有効になっているアグリゲートは、*NAE*アグリゲート（NetApp Aggregate Encryptionの略）と呼ばれます。NAEアグリゲート内のすべてのボリュームは、NAE暗号化またはNVE暗号化で暗号化する必要があります。アグリゲートレベルの暗号化では、アグリゲート内に作成するボリュームはデフォルトでNAE暗号化で暗号化されます。このデフォルトを上書きして、NVE暗号化を使用するように設定することもできます。

NAEアグリゲートではプレーンテキスト ボリュームがサポートされません。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. アグリゲートレベルの暗号化を有効または無効にします。

目的	使用するコマンド
ONTAP 9.7以降でNAEアグリゲートを作成する	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`*

ONTAP 9.6でNAEアグリゲートを作成する	`storage aggregate create -aggregate *aggregate_name* -node *node_name* -encrypt-with -aggr-key true`
非NAEアグリゲートをNAEアグリゲートに変換する	`storage aggregate modify -aggregate *aggregate_name* -node *node_name* -encrypt-with -aggr-key true`
NAEアグリゲートを非NAEアグリゲートに変換する	`storage aggregate modify -aggregate *aggregate_name* -node *node_name* -encrypt-with -aggr-key false`

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

次のコマンドは、 `aggr1`の集約レベルの暗号化を有効にします：

- ONTAP 9.7以降：

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

- ONTAP 9.6以前：

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

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

2. アグリゲートで暗号化が有効になっていることを確認します。

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

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

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

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

終了後の操作

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

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

ONTAPで新しいボリュームの暗号化を有効にする

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

タスク概要

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

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

新しいボリュームの暗号化を有効にする手順は、使用しているONTAPのバージョンと環境によって異なります。

- ONTAP 9.4以降では、オンボードキーマネージャのセットアップ時に `cc-mode`を有効にすると、 `-encrypt true`を指定したかどうかに関係なく、 `volume create`コマンドで作成したボリュームが自動的に暗号化されます。
- ONTAP 9.6以前のリリースでは、暗号化を有効にするには `-encrypt true`と `volume create`コマンドを使用する必要があります（ `cc-mode`を有効にしていない場合）。
- ONTAP 9.6でNAEボリュームを作成する場合は、アグリゲートレベルでNAEを有効にする必要があります。このタスクの詳細については、VEライセンスでアグリゲートレベルの暗号化を有効にするを参照してください。

- ONTAP 9.7以降では、"VEライセンス"とオンボードまたは外部キー管理を使用している場合、新規作成されたボリュームはデフォルトで暗号化されます。デフォルトでは、NAEアグリゲートに作成される新規ボリュームは、NVEではなくNAEタイプになります。
  - ONTAP 9.7以降のリリースでは、NAEアグリゲートにボリュームを作成する `volume create`コマンドに `-encrypt true`を追加すると、そのボリュームはNAEではなくNVE暗号化されます。NAEアグリゲート内のすべてのボリュームは、NVEまたはNAEのいずれかで暗号化する必要があります。

NAEアグリゲートではプレーンテキスト ボリュームがサポートされません。

手順

1. 新しいボリュームを作成し、そのボリュームで暗号化を有効にするかどうかを指定します。新しいボリュームがNAEアグリゲートに配置する場合、デフォルトでNAEで暗号化されます。

作成するには...	使用するコマンド
NAEボリューム	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`*
NVEボリューム	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt true` NAEがサポートされていないONTAP 9.6以前では、 `-encrypt true`ボリュームをNVEで暗号化することを指定します。ボリュームがNAEアグリゲート内に作成されるONTAP 9.7以降では、`-encrypt true`NAEのデフォルトの暗号化タイプをオーバーライドして、代わりにNVEボリュームを作成します。
プレーンテキスト ボリューム	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt false`

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

2. ボリュームで暗号化が有効になっていることを確認します。

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

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

結果

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

既存のONTAPボリュームでNAEまたはNVEを有効にする

既存のボリュームで暗号化を有効にするには、 `volume move start`コマンドまたは `volume encryption conversion start`コマンドのいずれかを使用できます。

タスク概要

`volume encryption conversion start`コマンドを使用すると、ボリュームを別の場所に移動することなく、既存のボリュームの暗号化を「インプレース」で有効にできます。または、 `volume move start`コマンドを使用することもできます。

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

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

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

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

手順

1. 既存のボリュームで暗号化を有効にします。

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

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

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

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

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

2. 変換処理のステータスを確認します。

```
volume encryption conversion show
```

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

次のコマンドは、変換処理のステータスを表示します。

```
cluster1::> volume encryption conversion show

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

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

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

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

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

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

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

結果

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

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

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

タスク概要

- ONTAP 9.8以降では、 `volume move start`を使用してSnapLockまたはFlexGroupボリュームの暗号化を有

効にすることができます。

- ONTAP 9.4以降では、オンボードキーマネージャのセットアップ時に「`cc-mode`」を有効にすると、`volume move start`コマンドで作成したボリュームは自動的に暗号化されます。`-encrypt-destination true`を指定する必要はありません。
- ONTAP 9.6以降では、アグリゲートレベルの暗号化を使用して、移動するボリュームの包含アグリゲートにキーを割り当てることができます。一意のキーで暗号化されたボリュームは、*NVE*ボリューム（NetAppボリューム暗号化を使用していることを意味します）と呼ばれます。アグリゲートレベルのキーで暗号化されたボリュームは、*NAE*ボリューム（NetAppアグリゲート暗号化の略）と呼ばれます。プレーンテキストボリュームはNAEアグリゲートではサポートされていません。
- ONTAP 9.14.1以降では、SVMルートボリュームをNVEで暗号化できます。詳細については、SVMルートボリュームでのNetApp Volume Encryptionの設定を参照してください。

開始する前に

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

"volume moveコマンドの実行権限の委譲"

手順

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

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

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

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

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

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

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

次のコマンドは、 `vol2`という名前の NAE ボリュームを NVE ボリュームに変換します：

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

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

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

次のコマンドは、 `vol2`という名前の NVE ボリュームをプレーンテキスト ボリュームに変換します：

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

2. クラスタのボリュームの暗号化タイプを表示します。

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

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

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

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

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

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

3. ボリュームで暗号化が有効になっていることを確認します。

   `volume show -is-encrypted true`

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

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

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

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

結果

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

ONTAP SVMルートボリュームにNVEを設定する

ONTAP 9.14.1以降では、Storage VM（SVM）のルート ボリュームでNetApp Volume Encryption（NVE）を有効にできます。NVEを使用すると、ルート ボリュームが一意のキーで暗号化されるため、SVMのセキュリティが強化されます。

タスク概要

SVMルート ボリュームでのNVEは、SVMの作成後にのみ有効にできます。

開始する前に

- SVMルート ボリュームは、NetApp Aggregate Encryption（NAE）で暗号化されたアグリゲートに配置しないでください。
- オンボード キー マネージャや外部キー マネージャを使用した暗号化を有効にしておく必要があります。
- ONTAP 9.14.1以降が実行されている必要があります。

- NVEで暗号化されたルート ボリュームが含まれるSVMを移行するには、移行の完了後にSVMルート ボリュームをプレーンテキスト ボリュームに変換したうえで、再度SVMルート ボリュームを暗号化する必要があります。
  - SVM移行のデスティネーション アグリゲートでNAEを使用する場合、ルート ボリュームはデフォルトでNAEを継承します。
- SVMがSVMディザスタ リカバリ関係に含まれる場合、次のことに注意してください。
  - ミラーされたSVMの暗号化設定は、デスティネーションにコピーされません。ソースまたはデスティネーションでNVEを有効にする場合は、ミラーされたSVMルート ボリュームで個別にNVEを有効にする必要があります。
  - デスティネーション クラスタ内のすべてのアグリゲートでNAEが使用される場合、SVMルート ボリュームでもNAEが使用されます。

手順

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

CLI

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

ルート ボリュームをインプレースで暗号化する

1. ルート ボリュームを暗号化されたボリュームに変換します。

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

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

SVMルート ボリュームを移動して暗号化する

1. ボリュームの移動を開始します。

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

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

2. `volume move`操作が `volume move show`コマンドで成功したことを確認します。 `volume show -encryption-type volume`には、NVEを使用しているすべてのボリュームのリストが表示されます。

System Manager

1. ストレージ > ボリューム に移動します。
2. 暗号化する SVM ルート ボリュームの名前の横にあるを選択し、次に 編集 を選択します。
3. ストレージと最適化の見出しで、暗号化を有効にするを選択します。
4. 保存を選択します。

ONTAPノードのルートボリュームにNVEを構成する

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

タスク概要

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

ルート ボリュームの暗号化は、いったん開始したら最後まで完了する必要があります。処理を一時停止することはできません。暗号化が完了すると、ルート ボリュームに新しいキーを割り当てられなくなるほか、セキュア パージ処理を実行できなくなります。

開始する前に

- システムでHA構成を使用している必要があります。
- ノード ルート ボリュームを作成しておく必要があります。
- オンボード キー マネージャまたはKey Management Interoperability Protocol（KMIP）を使用する外部キー管理サーバがシステムに搭載されている必要があります。

手順

1. ルート ボリュームを暗号化します。

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

2. 変換処理のステータスを確認します。

   ```
   volume encryption conversion show
   ```

3. 変換処理が完了したら、ボリュームが暗号化されたことを確認します。

   ```
   volume show -fields
   ```

   以下は、暗号化されたボリュームの出力例です。

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

著作権に関する情報

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権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

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