NVE を使用してボリュームデータを暗号化する

ONTAP 9

NetApp
September 12, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/ontap/encryption-at-rest/encrypt-volumes-concept.html on September 12, 2024. Always check docs.netapp.com for the latest.

目次

NVE を使用してボリュームデータを暗号化する 1
NVE を使用したボリュームデータの暗号化の概要 1
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 1
新しいボリュームで暗号化を有効にします 3
既存のボリュームで暗号化を有効にする 4
SVMルートボリュームでのNetAppボリューム暗号化の設定 8
ノードのルートボリューム暗号化を有効にします 10

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。

新しいボリュームで暗号化を有効にします

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
   ```

著作権に関する情報

Copyright © 2024 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。