使用 NVE 对卷数据进行加密

ONTAP 9

NetApp
July 11, 2025

This PDF was generated from https://docs.netapp.com/zh-cn/ontap/encryption-at-rest/encrypt-volumes-concept.html on July 11, 2025. Always check docs.netapp.com for the latest.

目录

使用 NVE 对卷数据进行加密 1
使用 NVE 概述对卷数据进行加密 1
在ONTAP中使用VE许可证启用聚合级加密 1
在ONTAP中对新卷启用加密 2
在ONTAP中使用volume Encryption conversion start命令对现有卷启用加密 4
对现有卷启用加密 5
使用 volume encryption conversion start 命令在现有卷上启用加密 5
使用 volume move start 命令在现有卷上启用加密 6
在SVM根卷上配置NetApp卷加密 9
启用节点根卷加密 10

使用 NVE 对卷数据进行加密

使用 NVE 概述对卷数据进行加密

从 ONTAP 9.7 开始，如果您拥有 VE 许可证以及板载或外部密钥管理，则默认情况下会启用聚合和卷加密。对于 ONTAP 9.6 及更早版本，您可以对新卷或现有卷启用加密。您必须先安装VE许可证并启用密钥管理、然后才能启用卷加密。NVE 符合 FIPS-140-2 1 级标准。

在ONTAP中使用VE许可证启用聚合级加密

从ONTAP 9．7开始，如果已"VE许可证"管理和板载密钥或外部密钥，则新创建的聚合和卷将默认进行加密。从 ONTAP 9.6 开始，您可以使用聚合级别的加密为要加密的卷的所属聚合分配密钥。

关于此任务

如果计划执行实时或后台聚合级重复数据删除，则必须使用聚合级加密。否则， NVE 不支持聚合级重复数据删除。

启用聚合级别加密的聚合称为 *NAE aggregate* （适用于 NetApp 聚合加密）。NAE聚合中的所有卷都必须使用NAE或NVE加密进行加密。默认情况下、使用聚合级别加密时、在聚合中创建的卷会使用NAE加密进行加密。您可以覆盖默认值以改用NVE加密。

NAE 聚合不支持纯文本卷。

开始之前

您必须是集群管理员才能执行此任务。

步骤

1. 启用或禁用聚合级别加密：

至 …	使用此命令 …
使用 ONTAP 9.7 或更高版本创建 NAE 聚合	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`*
使用 ONTAP 9.6 创建 NAE 聚合	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
将非 NAE 聚合转换为 NAE 聚合	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`

将 NAE 聚合转换为非 NAE 聚合	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key false`

有关此过程中所述命令的更多信息，请参见"ONTAP 命令参考"。

以下命令将在上启用聚合级别加密 `aggr1`：

- ONTAP 9.7 或更高版本

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

- ONTAP 9.6 或更早版本：

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

2. 验证是否已为聚合启用加密：

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

   有关的详细信息 `storage aggregate show`，请参见"ONTAP 命令参考"。

   以下命令将对此进行验证 `aggr1` 已启用加密：

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

完成后

运行 `volume create` 命令以创建加密卷。

如果您使用 KMIP 服务器存储节点的加密密钥，则在对卷进行加密时， ONTAP 会自动 "`推送` " 加密密钥到服务器。

在ONTAP中对新卷启用加密

您可以使用 `volume create` 命令以对新卷启用加密。

关于此任务

您可以使用NetApp卷加密(NVE)对卷进行加密、从ONTAP 9.6开始、还可以使用NetApp聚合加密(NAE)对卷进行加密。要了解有关NAE和NVE的更多信息、请参见 卷加密概述。

有关此过程中所述命令的更多信息，请参见"ONTAP 命令参考"。

在ONTAP 中为新卷启用加密的操作步骤 会根据您使用的ONTAP 版本和特定配置而有所不同：

- 从ONTAP 9.4开始、如果您启用了 `cc-mode` 设置板载密钥管理器时、您使用创建的卷 `volume create` 无论是否指定、命令都会自动加密 `-encrypt true`。
- 在ONTAP 9.6及更早版本中、您必须使用 `-encrypt true` 使用 `volume create` 用于启用加密的命令(前提是您未启用 `cc-mode`）。
- 如果要在ONTAP 9.6中创建NAE卷、则必须在聚合级别启用NAE。请参见 使用VE许可证启用聚合级别加密 了解有关此任务的更多详细信息。
- 从ONTAP 9．7开始，如果您有"VE许可证"和板载或外部密钥管理，则新创建的卷将默认加密。默认情况下、在NAE聚合中创建的新卷的类型为NAE、而不是NVE。
  - 在ONTAP 9.7及更高版本中、如果您添加了 `-encrypt true` 到 `volume create` 命令要在NAE聚合中创建卷、此卷将采用NVE加密、而不是NAE加密。NAE聚合中的所有卷都必须使用NVE或NAE进行加密。

> NAE 聚合不支持纯文本卷。

步骤

1. 创建新卷并指定是否在卷上启用加密。如果新卷位于NAE聚合中、则默认情况下、此卷将为NAE卷：

要创建 …	使用此命令 …
NAE卷	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`*
NVE卷	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt true` 在不支持NAE的ONTAP 9.6及更早版本中、 `-encrypt true` 指定应使用NVE对卷进行加密。在ONTAP 9.7及更高版本中、如果在NAE聚合中创建卷、 `-encrypt true` 覆盖默认的NAE加密类型以创建NVE卷。
纯文本卷	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt false`

   有关的详细信息 `volume create`，请参见"ONTAP 命令参考"。

2. 验证是否已为卷启用加密：

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

   有关的详细信息 `volume show`，请参见"ONTAP 命令参考"。

结果

如果使用KMIP服务器存储节点的加密密钥、则在对卷进行加密时、ONTAP 会自动将加密密钥"推送"到服务器。

在ONTAP中使用volume Encryption conversion start命令对现有卷启用加密

从ONTAP 9.3开始、您可以使用 `volume encryption conversion start` 命令以"原位"加密现有卷、而无需将卷移动到其他位置。

关于此任务

启动转换操作后，该操作必须完成。如果您在操作期间遇到性能问题描述、则可以运行 `volume encryption conversion pause` 命令以暂停操作、以及 `volume encryption conversion resume` 命令以恢复操作。

从ONTAP 9.14.1开始、您可以使用 `volume encryption conversion start` 在SVM根卷上。有关详细信息，请参见 在SVM根卷上配置NetApp卷加密。

> 您不能使用 `volume encryption conversion start` 转换SnapLock卷。

步骤

1. 在现有卷上启用加密：

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

   有关的详细信息 `volume encryption conversion start`，请参见"ONTAP 命令参考"。

   以下命令将对现有卷启用加密 `vol1`：

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

   系统会为卷创建加密密钥。卷上的数据已加密。

2. 验证转换操作的状态：

   `volume encryption conversion show`

   有关的详细信息 `volume encryption conversion show`，请参见"ONTAP 命令参考"。

   以下命令显示转换操作的状态：

   ```
   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. 转换操作完成后，验证卷是否已启用加密：

   `volume show -is-encrypted true`

   有关的详细信息 `volume show -is-encrypted true`，请参见"ONTAP 命令参考"。

   以下命令将显示上的加密卷 `cluster1`：

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

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

结果

如果您使用KMIP服务器存储节点的加密密钥、则在对卷进行加密时、ONTAP会自动将加密密钥推送到服务器。

对现有卷启用加密

您可以使用 `volume move start` 或 `volume encryption conversion start` 命令以对现有卷启用加密。

关于此任务

您可以使用 `volume encryption conversion start`命令可以“就地”启用现有卷的加密，而无需将卷移动到其他位置。或者，您可以使用 `volume move start`命令。

使用 **volume encryption conversion start** 命令在现有卷上启用加密

您可以使用 `volume encryption conversion start`命令来启用现有卷的“就地”加密，而无需将卷移动到其他位置。

启动转换操作后、必须完成该操作。如果您在操作期间遇到性能问题描述、则可以运行 `volume encryption conversion pause` 命令以暂停操作、以及 `volume encryption conversion resume` 命令以恢复操作。

> 您不能使用 `volume encryption conversion start` 转换SnapLock卷。

步骤

1. 在现有卷上启用加密：

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

   有关的详细信息 `volume encryption conversion start`，请参见"ONTAP 命令参考"。

   以下命令将对现有卷启用加密 `vol1`：

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

系统会为卷创建加密密钥。卷上的数据已加密。

2. 验证转换操作的状态：

   `volume encryption conversion show`

   有关的详细信息 `volume encryption conversion show`，请参见"ONTAP 命令参考"。

   以下命令显示转换操作的状态：

```
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. 转换操作完成后、验证卷是否已启用加密：

   `volume show -is-encrypted true`

   有关的详细信息 `volume show`，请参见"ONTAP 命令参考"。

   以下命令将显示上的加密卷 `cluster1`：

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

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

结果

如果您使用 KMIP 服务器存储节点的加密密钥，则在对卷进行加密时， ONTAP 会自动 "`推送` " 加密密钥到服务器。

使用 **volume move start** 命令在现有卷上启用加密

您可以使用 `volume move start`命令通过移动现有卷来启用加密。您可以使用同一个聚合或不同的聚合。

关于此任务

- 从ONTAP 9.8开始、您可以使用 `volume move start` 在SnapLock或FlexGroup卷上启用加密。
- 从ONTAP 9.4开始、如果在设置板载密钥管理器时启用"`cc-mode`"、则会显示使用创建的卷 `volume move start` 命令会自动加密。您无需指定 `-encrypt-destination true`。

- 从 ONTAP 9.6 开始，您可以使用聚合级别的加密为要移动的卷所在的聚合分配密钥。使用唯一密钥加密的卷称为_NVE卷_(表示它使用NetApp卷加密)。使用聚合级别密钥加密的卷称为 *NAE volume* （适用于 NetApp 聚合加密）。NAE 聚合不支持纯文本卷。
- 从ONTAP 9.14.1开始、您可以使用NVE对SVM根卷进行加密。有关详细信息，请参见 在SVM根卷上配置NetApp卷加密。

开始之前

要执行此任务，您必须是集群管理员，或者集群管理员已向其委派权限的 SVM 管理员。

"委派权限以运行 volume move 命令"

步骤

1. 移动现有卷并指定是否在卷上启用加密：

要转换 …	使用此命令 …
纯文本卷到 NVE 卷	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination true`
将 NVE 或纯文本卷连接到 NAE 卷（假设目标上启用了聚合级别加密）	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-with-aggr-key true`
NAE 卷到 NVE 卷	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-with-aggr-key false`
NAE 卷到纯文本卷	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination false -encrypt-with-aggr-key false`
NVE卷转换为纯文本卷	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination false`

有关的详细信息 `volume move start`，请参见"ONTAP 命令参考"。

以下命令将转换名为的纯文本卷 `vol1` 到NVE卷：

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

假设在目标上启用了聚合级加密、则以下命令将转换名为的NVE或纯文本卷 `vol1` 到NAE卷：

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

以下命令将转换名为的NAE卷 `vol2` 到NVE卷：

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

以下命令将转换名为的NAE卷 `vol2` 纯文本卷：

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

以下命令将转换名为的NVE卷 `vol2` 纯文本卷：

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

2. 查看集群卷的加密类型：

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

   。 `encryption-type` 字段在ONTAP 9.6及更高版本中可用。

   有关的详细信息 `volume show`，请参见"ONTAP 命令参考"。

   以下命令显示中卷的加密类型 `cluster2`：

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

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

3. 验证是否已为卷启用加密：

   `volume show -is-encrypted true`

   有关的详细信息 `volume show`，请参见"ONTAP 命令参考"。

以下命令将显示上的加密卷 `cluster2`：

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

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

结果

如果您使用KMIP服务器存储节点的加密密钥、则在对卷进行加密时、ONTAP会自动将加密密钥推送到服务器。

在SVM根卷上配置NetApp卷加密

从ONTAP 9.14.1开始、您可以在Storage VM (SVM)根卷上启用NetApp卷加密(NVE)。使用NVE时、根卷会使用唯一密钥进行加密、从而提高SVM的安全性。

关于此任务

只有在创建SVM之后、才能在SVM根卷上启用NVE。

开始之前

- SVM根卷不能位于使用NetApp聚合加密(NAE)加密的聚合上。
- 您必须已使用板载密钥管理器或外部密钥管理器启用加密。
- 必须运行ONTAP 9.14.1或更高版本。
- 要迁移包含使用NVE加密的根卷的SVM、您必须在迁移完成后将SVM根卷转换为纯文本卷、然后对SVM根卷重新加密。
  - 如果SVM迁移的目标聚合使用NAE、则默认情况下、根卷会继承NAE。
- 如果SVM处于SVM灾难恢复关系中：
  - 镜像SVM上的加密设置不会复制到目标。如果在源或目标上启用NVE、则必须在镜像的SVM根卷上单独启用NVE。
  - 如果目标集群中的所有聚合都使用NAE、则SVM根卷将使用NAE。

步骤

您可以使用ONTAP命令行界面或System Manager在SVM根卷上启用NVE。

命令行界面

您可以在SVM根卷上原位启用NVE、也可以通过在聚合之间移动卷来启用NVE。

对根卷进行原位加密

1. 将根卷转换为加密卷：

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

2. 确认加密成功。。 `volume show -encryption-type volume` 显示使用NVE的所有卷的列表。

通过移动**SVM**根卷对其进行加密

1. 启动卷移动：

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

   有关的详细信息 `volume move`，请参见"ONTAP 命令参考"。

2. 确认 `volume move` 操作成功、使用 `volume move show` 命令：。 `volume show -encryption -type volume` 显示使用NVE的所有卷的列表。

System Manager

1. 导航到存储>卷。
2. 在要加密的SVM根卷的名称旁边，选择，然后选择 ⋮ 编辑.
3. 在存储和优化标题下，选择启用加密。
4. 选择保存。

启用节点根卷加密

从 ONTAP 9.8 开始，您可以使用 NetApp 卷加密来保护节点的根卷。

关于此任务

此操作步骤适用场景为节点根卷。它不适用于 SVM 根卷。SVM根卷可通过聚合级加密进行保护、 从ONTAP 9.14.1开始、为NVE。

根卷加密开始后，必须完成。您不能暂停此操作。加密完成后，您不能为根卷分配新密钥，也不能执行安全清除操作。

开始之前

- 您的系统必须使用 HA 配置。
- 必须已创建节点根卷。
- 您的系统必须具有使用密钥管理互操作性协议（ Key Management Interoperability Protocol ， KMIP ）的板载密钥管理器或外部密钥管理服务器。

步骤

1. 对根卷进行加密：

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

2. 验证转换操作的状态：

   ```
   volume encryption conversion show
   ```

3. 转换操作完成后，验证卷是否已加密：

   ```
   volume show -fields
   ```

   下面显示了加密卷的示例输出。

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

版权信息

版权所有 © 2025 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。 美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 http://www.netapp.com/TM 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。