配置 NetApp 卷加密

ONTAP 9

NetApp
September 12, 2024

This PDF was generated from https://docs.netapp.com/zh-cn/ontap/encryption-at-rest/configure-netapp-volume-encryption-concept.html on September 12, 2024. Always check docs.netapp.com for the latest.

目录

配置 NetApp 卷加密 1
配置 NetApp 卷加密概述 1
NetApp 卷加密工作流 4
配置NVE 5
使用 NVE 对卷数据进行加密 21

配置 NetApp 卷加密

配置 NetApp 卷加密概述

NetApp 卷加密（ NVE ）是一种基于软件的技术，用于一次对一个卷上的空闲数据进行加密。只有存储系统可以访问的加密密钥可确保在底层设备被重新利用，退回，放置在不当位置或被盗时无法读取卷数据。

了解 NVE

使用NVE时、元数据和数据(包括Snapshot副本)均会加密。数据访问由一个唯一的 XTS-AES-256 密钥提供，每个卷一个。外部密钥管理服务器或板载密钥管理器(Onboard Key Manager、OKM)为节点提供密钥：

- 外部密钥管理服务器是存储环境中的第三方系统，可使用密钥管理互操作性协议（ Key Management Interoperability Protocol ， KMIP ）为节点提供密钥。最佳做法是，在与数据不同的存储系统上配置外部密钥管理服务器。
- 板载密钥管理器是一个内置工具，可为数据所在存储系统中的节点提供密钥。

从 ONTAP 9.7 开始，如果您拥有卷加密（ Volume Encryption ， VE ）许可证并使用板载或外部密钥管理器，则默认情况下会启用聚合和卷加密。VE许可证随一起提供"ONTAP One"。每当配置外部或板载密钥管理器时，为全新聚合和全新卷配置空闲数据加密的方式都会发生变化。默认情况下，全新聚合将启用 NetApp 聚合加密（ NAE ）。默认情况下，不属于 NAE 聚合的全新卷将启用 NetApp 卷加密（ NVE ）。如果使用多租户密钥管理为数据存储虚拟机（ SVM ）配置了自己的密钥管理器，则为该 SVM 创建的卷将自动配置 NVE 。

您可以对新卷或现有卷启用加密。NVE 支持所有存储效率功能，包括重复数据删除和数据压缩。从ONTAP 9.14.1开始、您可以执行此操作 在现有SVM根卷上启用NVE。

> 如果您使用的是 SnapLock ，则只能对新的空 SnapLock 卷启用加密。您不能在现有 SnapLock 卷上启用加密。

您可以在任何类型的聚合（ HDD ， SSD ，混合，阵列 LUN ）上使用任何 RAID 类型以及任何受支持的 ONTAP 实施（包括 ONTAP Select ）中使用 NVE 。您还可以将 NVE 与基于硬件的加密结合使用，在 d自加密驱动器上 " 双重加密 " 数据。

启用NVE后、核心转储也会进行加密。

聚合级加密

通常，每个加密卷都分配有一个唯一的密钥。删除卷后，此密钥将随之删除。

从 ONTAP 9.6 开始，您可以使用 _NetApp 聚合加密（ NAE ） _ 为要加密的卷所在的聚合分配密钥。删除加密卷后，聚合的密钥将保留下来。如果删除整个聚合、则这些密钥将被删除。

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。

从 ONTAP 9.7 开始，如果您拥有卷加密（ Volume Encryption ， VE ）许可证并使用板载或外部密钥管理器，则默认情况下会启用聚合和卷加密。

NVE 和 NAE 卷可以同时位于同一聚合上。默认情况下，在聚合级别加密下加密的卷为 NAE 卷。对卷进行加密时，您可以覆盖默认值。

您可以使用 `volume move` 命令将NVE卷转换为NAE卷、反之亦然。您可以将 NAE 卷复制到 NVE 卷。

您不能使用 `secure purge` NAE卷上的命令。

何时使用外部密钥管理服务器

尽管使用板载密钥管理器成本较低且通常更方便，但如果满足以下任一条件，则应设置 KMIP 服务器：

- 您的加密密钥管理解决方案必须符合联邦信息处理标准（ FIPS ） 140-2 或 OASIS KMIP 标准。
- 您需要一个具有集中管理加密密钥的多集群解决方案。
- 您的企业需要将身份验证密钥存储在系统或与数据不同的位置，从而提高安全性。

外部密钥管理的范围

外部密钥管理的范围决定了密钥管理服务器是保护集群中的所有 SVM 还是仅保护选定 SVM ：

- 您可以使用 *cluster scopter* 为集群中的所有 SVM 配置外部密钥管理。集群管理员可以访问存储在服务器上的每个密钥。
- 从 ONTAP 9.6 开始，您可以使用 *SVM scopter* 为集群中的指定 SVM 配置外部密钥管理。这最适合多租户环境，其中每个租户都使用不同的 SVM （或一组 SVM ）来提供数据。只有给定租户的 SVM 管理员才能访问该租户的密钥。
- 从 ONTAP 9.10.1 开始，您可以使用 Azure 密钥存储和 Google Cloud KMS 仅保护数据SVM的NVE密钥。从9.12.0开始、此功能可用于AWS的KMS。

您可以在同一集群中使用这两个范围。如果为 SVM 配置了密钥管理服务器，则 ONTAP 仅使用这些服务器来保护密钥。否则， ONTAP 将使用为集群配置的密钥管理服务器来保护密钥。

中提供了经过验证的外部密钥管理器列表 "NetApp 互操作性表工具（ IMT ）"。您可以通过在IMT的搜索功能中输入术语"密钥管理器"来查找此列表。

支持详细信息

下表显示了 NVE 支持详细信息：

资源或功能	支持详细信息
平台	需要 AES-NI 卸载功能。请参见 Hardware Universe （ HWU ）以验证您的平台是否支持 NVE 和 NAE 。

加密	从 ONTAP 9.7 开始，在添加卷加密（ Volume Encryption ， VE ）许可证并配置板载或外部密钥管理器时，新创建的聚合和卷会默认加密。如果需要创建未加密的聚合，请使用以下命令：
	
	`storage aggregate create -encrypt-with-aggr-key false`
	
	如果需要创建纯文本卷，请使用以下命令：
	
	`volume create -encrypt false`
	
	在以下情况下，默认情况下不启用加密：
	
	• 未安装 Ve 许可证。
	• 未配置密钥管理器
	• 平台或软件不支持加密
	• 已启用硬件加密

ONTAP	所有 ONTAP 实施。ONTAP 9.5 及更高版本支持 ONTAP 云。
设备	HDD ， SSD ，混合，阵列 LUN 。
RAID	RAID0 ， RAID4 ， RAID-DP ， RAID-TEC 。
Volumes	数据卷和现有SVM根卷。您不能对MetroCluster元数据卷上的数据进行加密。在9.14.1之前的ONTAP版本中、不能使用NVE对SVM根卷上的数据进行加密。从ONTAP 9.14.1开始、ONTAP支持 SVM根卷上的NVE。
聚合级加密	从 ONTAP 9.6 开始， NVE 支持聚合级加密（ Aggregate-Level Encryption ， NAE ）： • 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。 • 您不能为聚合级别的加密卷重新设置密钥。 • 聚合级加密卷不支持安全清除。 • 除了数据卷之外， NAE 还支持对 SVM 根卷和 MetroCluster 元数据卷进行加密。NAE 不支持对根卷进行加密。
SVM 范围	从 ONTAP 9.6 开始， NVE 仅支持用于外部密钥管理的 SVM 范围，而不支持板载密钥管理器。从 ONTAP 9.8 开始，支持 MetroCluster 。
存储效率	重复数据删除，数据压缩，数据缩减， FlexClone 。 即使从父级拆分克隆后，克隆也会使用与父级相同的密钥。您应执行 `volume move` 在拆分的克隆上、之后、拆分的克隆将具有不同的密钥。

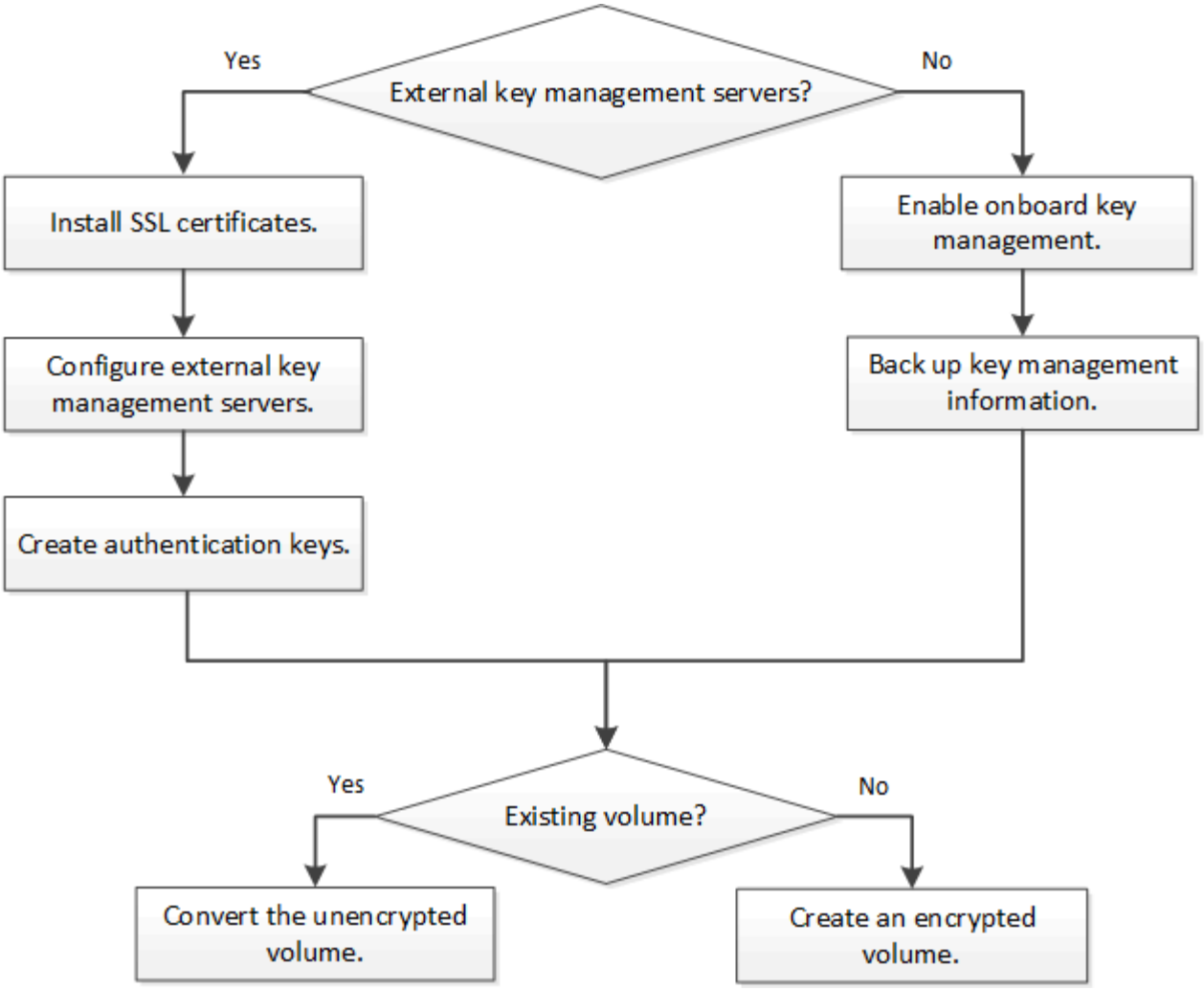
Replication	• 对于卷复制、源卷和目标卷可以具有不同的加密设置。可以为源配置加密，也可以为目标取消配置加密，反之亦然。 • 对于 SVM 复制，目标卷会自动加密，除非目标卷不包含支持卷加密的节点（在这种情况下复制成功，但目标卷不会加密）。 • 对于 MetroCluster 配置，每个集群从其配置的密钥服务器中提取外部密钥管理密钥。配置复制服务会将 OKM 密钥复制到配对站点。
合规性	从 ONTAP 9.2 开始， SnapLock 在合规和企业模式下均受支持，仅适用于新卷。您不能在现有 SnapLock 卷上启用加密。
FlexGroup	从 ONTAP 9.2 开始，支持 FlexGroup 。目标聚合的类型必须与源聚合相同，可以是卷级聚合，也可以是聚合级聚合。从 ONTAP 9.5 开始，支持对 FlexGroup 卷进行原位重新设置密钥。
7- 模式过渡	从 7- 模式过渡工具 3.3 开始，您可以使用 7- 模式过渡工具命令行界面对集群系统上启用了 NVE 的目标卷执行基于副本的过渡。

相关信息

"常见问题解答—NetApp卷加密和NetApp聚合加密"

NetApp 卷加密工作流

必须先配置密钥管理服务，然后才能启用卷加密。您可以对新卷或现有卷启用加密。



"您必须安装VE许可证"并配置密钥管理服务、然后才能使用NVE加密数据。在安装许可证之前，您应该"确定您的 ONTAP 版本是否支持 NVE"。

配置NVE

确定您的集群版本是否支持 NVE

在安装许可证之前，您应确定集群版本是否支持 NVE 。您可以使用 `version` 命令以确定集群版本。

关于此任务

集群版本是集群中任何节点上运行的最低 ONTAP 版本。

步骤

1. 确定您的集群版本是否支持 NVE：

   ```
   version -v
   ```

   如果命令输出显示文本 "`1Ono-dare` " （对于 "`no Data at Rest Encryption` " ），或者您使用的平台未在中列出，则不支持 NVE "支持详细信息"。

以下命令可确定上是否支持NVE `cluster1`。

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

的输出 `1Ono-DARE` 表示您的集群版本不支持NVE。

安装许可证

VE 许可证使您有权在集群中的所有节点上使用此功能。要使用NVE对数据进行加密、必须先获得此许可证。随一起提供"ONTAP One"。

在ONTAP One之前、加密包附带VE许可证。加密包不再提供、但仍然有效。虽然目前并不需要，但现有客户可以选择"升级到ONTAP One"。

开始之前

- 您必须是集群管理员才能执行此任务。
- 您必须已从销售代表处收到VE许可证密钥、或者已安装ONTAP One。

步骤

1. "验证是否已安装VE许可证"(英文)

   VE许可证包名称为 `VE`。

2. 如果未安装许可证，"使用System Manager或ONTAP命令行界面安装它"。

配置外部密钥管理

配置外部密钥管理概述

您可以使用一个或多个外部密钥管理服务器来保护集群用于访问加密数据的密钥。外部密钥管理服务器是存储环境中的第三方系统，可使用密钥管理互操作性协议（ Key Management Interoperability Protocol ， KMIP ）为节点提供密钥。

> 对于 ONTAP 9.1 及更早版本，必须先将节点管理 LIF 分配给已配置节点管理角色的端口，然后才能使用外部密钥管理器。

NetApp 卷加密（ NVE ）在 ONTAP 9.1 及更高版本中支持板载密钥管理器。从ONTAP 9.3开始、NVE支持外部密钥管理(KMIP)和板载密钥管理器。从 ONTAP 9.10.1 开始，您可以使用 Azure密钥存储或Google Cloud密钥管理器服务 保护NVE密钥。从ONTAP 9.11.1开始、您可以在一个集群中配置多个外部密钥管理器。请参见 配置集群模式密钥服务器。

使用**System Manager**管理外部密钥管理器

从ONTAP 9.7开始、您可以使用板载密钥管理器存储和管理身份验证和加密密钥。从ONTAP 9.131开始、您还可以使用外部密钥管理器来存储和管理这些密钥。

板载密钥管理器将密钥存储在集群内部的安全数据库中并对其进行管理。其范围为集群。外部密钥管理器可在集群外部存储和管理密钥。其范围可以是集群或Storage VM。可以使用一个或多个外部密钥管理器。需满足以下条件：

- 如果启用了板载密钥管理器、则无法在集群级别启用外部密钥管理器、但可以在Storage VM级别启用外部密钥管理器。
- 如果在集群级别启用了外部密钥管理器、则无法启用板载密钥管理器。

使用外部密钥管理器时、每个Storage VM和集群最多可以注册四个主密钥服务器。每个主密钥服务器最多可与三个二级密钥服务器组成集群。

配置外部密钥管理器

要为Storage VM添加外部密钥管理器、您应在为Storage VM配置网络接口时添加可选网关。如果创建的Storage VM没有网络路由、则必须为外部密钥管理器明确创建路由。请参见 "创建LIF (网络接口)"。

步骤

您可以从System Manager中的不同位置开始配置外部密钥管理器。

1. 要配置外部密钥管理器、请执行以下开始步骤之一。

工作流	导航	开始步骤
配置密钥管理器	集群>*设置*	滚动到*Security*部分。在*加密*下，选择 。选择*外部密钥管理器*。
添加本地层	存储>*层*	选择*+添加本地层*。选中标有"配置密钥管理器"的复选框。选择*外部密钥管理器*。
准备存储	信息板	在*容量*部分中，选择*准备存储*。 然后、选择"配置密钥管理器"。选择*外部密钥管理器*。
配置加密(仅限Storage VM范围的密钥管理器)	存储>*存储VM*	选择 Storage VM 。选择*Settings*选项卡。在*Security*下的*Encryption部分中，选择 。

2. 要添加主密钥服务器，请选择 + Add ，然后填写*IP地址或主机名*和*Port*字段。
3. 已安装的现有证书列在*KMIP服务器CA证书*和*KMIP客户端证书*字段中。 您可以执行以下任一操作：
   - 选择以选择 要映射到密钥管理器的已安装证书。(可以选择多个服务CA证书、但只能选择一个客户端证书。)
   - 选择*添加新证书*以添加尚未安装的证书并将其映射到外部密钥管理器。
   - 选择 × 证书名称旁边的以删除不希望映射到外部密钥管理器的已安装证书。
4. 要添加辅助密钥服务器，请在*辅助密钥服务器*列中选择*Add*，并提供其详细信息。
5. 选择*保存*以完成配置。

编辑现有外部密钥管理器

如果您已配置外部密钥管理器、则可以修改其设置。

步骤

1. 要编辑外部密钥管理器的配置、请执行以下开始步骤之一。

范围	导航	开始步骤
集群范围外部密钥管理器	集群>*设置*	滚动到*Security*部分。在*加密*下，选择，然后选择 ⋮ 编辑外部密钥管理器。
Storage VM范围外部密钥管理器	存储>*存储VM*	选择 Storage VM 。选择*Settings*选项卡。在*Security*下的*Encryption部分中，选择，然后选择 ⋮ **Edit External Key Manager**。

2. 现有密钥服务器列在*密钥服务器*表中。您可以执行以下操作：
   - 通过选择添加新密钥服务器 + Add 。
   - 通过在包含密钥服务器名称的表单元格末尾选择来删除 ⋮ 密钥服务器。与该主密钥服务器关联的辅助密钥服务器也会从配置中删除。

删除外部密钥管理器

如果卷未加密、则可以删除外部密钥管理器。

步骤

1. 要删除外部密钥管理器、请执行以下步骤之一。

范围	导航	开始步骤
集群范围外部密钥管理器	集群>*设置*	滚动到*Security*部分。在*加密*下，选择 ⋮ ，然后选择*删除外部密钥管理器*。
Storage VM范围外部密钥管理器	存储>*存储VM*	选择 Storage VM 。选择*Settings*选项卡。在*Security*下的*Encryption部分中，选择，然后选择 ⋮ **Delete External Key Manager**。

在密钥管理器之间迁移密钥

如果在集群上启用了多个密钥管理器、则必须将密钥从一个密钥管理器迁移到另一个密钥管理器。此过程可通过System Manager自动完成。

- 如果在集群级别启用了板载密钥管理器或外部密钥管理器、并且某些卷已加密、 然后、在Storage VM级别配置外部密钥管理器时、必须将这些密钥从集群级别的板载密钥管理器或外部密钥管理器迁移到Storage VM级别的外部密钥管理器。 此过程由System Manager自动完成。
- 如果在Storage VM上创建卷时未进行加密、则不需要迁移密钥。

在集群上安装 **SSL** 证书

集群和 KMIP 服务器使用 KMIP SSL 证书来验证彼此的身份并建立 SSL 连接。在配置与 KMIP 服务器的 SSL 连接之前，必须为集群安装 KMIP 客户端 SSL 证书，并为 KMIP 服务器的根证书颁发机构（ CA ）安装 SSL 公有证书。

关于此任务

在 HA 对中，两个节点必须使用相同的公有和专用 KMIP SSL 证书。如果将多个 HA 对连接到同一个 KMIP 服务器，则 HA 对中的所有节点都必须使用相同的公有和专用 KMIP SSL 证书。

开始之前

- 创建证书的服务器， KMIP 服务器和集群上的时间必须同步。
- 您必须已获取集群的公有 SSL KMIP 客户端证书。
- 您必须已获取与集群的 SSL KMIP 客户端证书关联的专用密钥。
- SSL KMIP 客户端证书不能受密码保护。
- 您必须已为 KMIP 服务器的根证书颁发机构（ CA ）获取 SSL 公有证书。
- 在MetroCluster环境中、您必须在两个集群上安装相同的KMIP SSL证书。

> 在集群上安装客户端和服务器证书之前或之后，您可以在 KMIP 服务器上安装这些证书。

步骤

1. 为集群安装 SSL KMIP 客户端证书：

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

   系统将提示您输入 SSL KMIP 公有和专用证书。

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

2. 为 KMIP 服务器的根证书颁发机构（ CA ）安装 SSL 公有证书：

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

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

在 **ONTAP 9.6** 及更高版本（ **NVE** ）中启用外部密钥管理

您可以使用一个或多个 KMIP 服务器来保护集群用于访问加密数据的密钥。从ONTAP 9.6开始、您可以选择配置一个单独的外部密钥管理器、以保护数据SVM用于访问加密数据的密钥。

从ONTAP 9.11.1开始、您可以为每个主密钥服务器最多添加3个二级密钥服务器、以创建集群模式密钥服务器。有关详细信息，请参见 配置集群模式外部密钥服务器。

关于此任务

您最多可以将四个 KMIP 服务器连接到一个集群或 SVM 。建议至少使用两台服务器来实现冗余和灾难恢复。

外部密钥管理的范围决定了密钥管理服务器是保护集群中的所有 SVM 还是仅保护选定 SVM：

- 您可以使用 *cluster scopter* 为集群中的所有 SVM 配置外部密钥管理。集群管理员可以访问存储在服务器上的每个密钥。
- 从 ONTAP 9.6 开始，您可以使用 *SVM scopter* 为集群中的数据 SVM 配置外部密钥管理。这最适合多租户环境，其中每个租户都使用不同的 SVM （或一组 SVM ）来提供数据。只有给定租户的 SVM 管理员才能访问该租户的密钥。
- 对于多租户环境，请使用以下命令为 *MT_EK_MGMT* 安装许可证：

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

  有关完整的命令语法，请参见命令手册页。

您可以在同一集群中使用这两个范围。如果为 SVM 配置了密钥管理服务器，则 ONTAP 仅使用这些服务器来保护密钥。否则， ONTAP 将使用为集群配置的密钥管理服务器来保护密钥。

您可以在集群范围配置板载密钥管理，并在 SVM 范围配置外部密钥管理。您可以使用 `security key-manager key migrate` 命令将密钥从集群范围的板载密钥管理迁移到SVM范围的外部密钥管理器。

开始之前

- 必须已安装 KMIP SSL 客户端和服务器证书。
- 要执行此任务，您必须是集群或 SVM 管理员。
- 如果要为 MetroCluster 环境启用外部密钥管理，则必须在启用外部密钥管理之前完全配置 MetroCluster 。
- 在MetroCluster 环境中、必须在两个集群上安装KMIP SSL证书。

步骤

1. 配置集群的密钥管理器连接：

   ```
   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` 命令用于替换 `security key-manager setup` 命令：如果在集群登录提示符处运行命令、 *`admin_SVM`* 默认为当前集群的管理SVM。 您必须是集群管理员才能配置集群范围。您可以运行 `security key-manager external modify` 用于更改外部密钥管理配置的命令。
   >
   > ◦ 在MetroCluster 环境中、如果要为管理SVM配置外部密钥管理、则必须重复 `security key-manager external enable` 命令。

   以下命令将为启用外部密钥管理 `cluster1` 使用三个外部密钥服务器。第一个密钥服务器使用其主机名和端口指定，第二个密钥服务器使用 IP 地址和默认端口指定，第三个密钥服务器使用 IPv6 地址和端口指定：

```
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. 配置密钥管理器 SVM：

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

- 如果在SVM登录提示符处运行命令、 `SVM` 默认为当前SVM。 您必须是集群或 SVM 管理员才能配置 SVM 范围。您可以运行 `security key-manager external modify` 用于更改外部密钥管理配置的命令。
- 在MetroCluster 环境中、如果要为数据SVM配置外部密钥管理、则不必重复 `security key-manager external enable` 命令。

以下命令将为启用外部密钥管理 `svm1` 使用单密钥服务器侦听默认端口5696：

```
svm1l::> security key-manager external enable -vserver svm1 -key-servers
keyserver.svm1.com -client-cert SVM1ClientCert -server-ca-certs
SVM1ServerCaCert
```

3. 对任何其他 SVM 重复最后一步。

您也可以使用 `security key-manager external add-servers` 命令以配置其他SVM。。 `security key-manager external add-servers` 命令用于替换 `security key-manager add` 命令：有关完整的命令语法，请参见手册页。

4. 验证所有已配置的 KMIP 服务器是否均已连接：

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

。 `security key-manager external show-status` 命令用于替换 `security key-manager show -status` 命令：有关完整的命令语法，请参见手册页。

```
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. (可选)将纯文本卷转换为加密卷。

   ```
   volume encryption conversion start
   ```

   转换卷之前、必须完全配置外部密钥管理器。在MetroCluster环境中、必须同时在两个站点上配置外部密钥管理器。

在 **ONTAP 9.5** 及更早版本中启用外部密钥管理

您可以使用一个或多个 KMIP 服务器来保护集群用于访问加密数据的密钥。最多可以将四个 KMIP 服务器连接到一个节点。建议至少使用两台服务器来实现冗余和灾难恢复。

关于此任务

ONTAP 为集群中的所有节点配置 KMIP 服务器连接。

开始之前

- 必须已安装 KMIP SSL 客户端和服务器证书。
- 您必须是集群管理员才能执行此任务。
- 在配置外部密钥管理器之前，您必须配置 MetroCluster 环境。
- 在MetroCluster 环境中、必须在两个集群上安装KMIP SSL证书。

步骤

1. 为集群节点配置密钥管理器连接：

   ```
   security key-manager setup
   ```

   此时将启动密钥管理器设置。

   在MetroCluster 环境中、必须在两个集群上运行此命令。

2. 在每个提示符处输入相应的响应。
3. 添加 KMIP 服务器：

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

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

   在MetroCluster 环境中、必须在两个集群上运行此命令。

4. 添加额外的 KMIP 服务器以实现冗余：

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

   ```
   clusterl::> security key-manager add -address 20.1.1.2
   ```

   在MetroCluster 环境中、必须在两个集群上运行此命令。

5. 验证所有已配置的 KMIP 服务器是否均已连接：

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

   有关完整的命令语法，请参见手册页。

   ```
   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. (可选)将纯文本卷转换为加密卷。

   ```
   volume encryption conversion start
   ```

转换卷之前、必须完全配置外部密钥管理器。在MetroCluster环境中、必须同时在两个站点上配置外部密钥管理器。

通过云提供商管理密钥

从 ONTAP 9.10.1 开始，您可以使用 "Azure 密钥存储（ AKV ）" 和 "Google Cloud Platform 的密钥管理服务（ Cloud KMS ）" 保护云托管应用程序中的ONTAP加密密钥。从ONTAP 9.12.0开始、您还可以使用保护NVE密钥 "AWS的KMS"。

AWS KMS、AKV和Cloud KMS可用于保护 "NetApp 卷加密（ NVE ）密钥" 仅适用于数据SVM。

关于此任务

可以使用命令行界面或ONTAP REST API启用云提供程序的密钥管理。

在使用云提供商保护密钥时、请注意、默认情况下、数据SVM LIF用于与云密钥管理端点进行通信。节点管理网络用于与云提供商的身份验证服务进行通信（适用于 Azure 的 login.microsoftonline.com ；适用于 Cloud KMS 的 oauth2.googleapis.com ）。如果集群网络配置不正确，集群将无法正确利用密钥管理服务。

在使用云提供商密钥管理服务时、您应注意以下限制：

- 云提供商密钥管理不适用于NetApp存储加密(NSE)和NetApp聚合加密(NAE)。 "外部 KMIP" 可以改为使用。
- 云提供商密钥管理不适用于MetroCluster配置。
- 只能在数据SVM上配置云提供程序密钥管理。

开始之前

- 您必须已在相应的云提供程序上配置KMS。
- ONTAP集群的节点必须支持NVE。
- "您必须已安装卷加密(VE)和多租户加密密钥管理(MTEKM)许可证"(英文)这些许可证包含在中"ONTAP One"。
- 您必须是集群或SVM管理员。
- 数据SVM不能包含任何加密卷、也不能使用密钥管理器。如果数据SVM包含加密卷、则必须先迁移这些卷、然后再配置KMS。

启用外部密钥管理

启用外部密钥管理取决于您使用的特定密钥管理器。选择相应密钥管理器和环境的选项卡。

AWS

开始之前

- 您必须为管理加密的IAM角色要使用的AWS KMS密钥创建授权。IAM角色必须包含一个允许执行以下操作的策略：
  - `DescribeKey`
  - `Encrypt`
  - `Decrypt`

  有关详细信息、请参见的AWS文档 "赠款"。

在**ONTAP SVM**上启用**AWS KMV**

1. 开始之前、请从AWS KMS获取访问密钥ID和机密密钥。
2. 将权限级别设置为高级：
   `set -priv advanced`
3. 启用AWS KMS：
   `security key-manager external aws enable -vserver` *`svm_name`* `-region` *`AWS_region`* `-key-id` *`key_ID`* `-encryption-context` *`encryption_context`*
4. 出现提示时、输入机密密钥。
5. 确认已正确配置AWS KMS：
   `security key-manager external aws show -vserver` *`svm_name`*

Azure 酒店

在**ONTAP SVM**上启用**Azure**密钥存储

1. 开始之前，您需要从 Azure 帐户获取适当的身份验证凭据，即客户端密钥或证书。
   此外，还必须确保集群中的所有节点运行状况良好。您可以使用命令来检查此情况 `cluster show`。
2. 将权限级别设置为高级
   `set -priv advanced`
3. 在SVM上启用AKV
   `security key-manager external azure enable -client-id` *`client_id`* `-tenant-id` *`tenant_id`* `-name -key-id` *`key_id`* `-authentication-method {certificate|client-secret}`
   出现提示时，输入 Azure 帐户的客户端证书或客户端密钥。
4. 验证是否已正确启用AKV：
   `security key-manager external azure show vserver` *`svm_name`*
   如果服务可访问性不正常、请通过数据SVM LIF建立与AKV密钥管理服务的连接。

Google Cloud

在**ONTAP SVM**上启用云**KMS**

1. 开始之前、请以JSON格式获取Google Cloud KMS帐户密钥文件的专用密钥。您可以在 GCP 帐户中找到此信息。
   此外，还必须确保集群中的所有节点运行状况良好。您可以使用命令来检查此情况 `cluster show`。
2. 将权限级别设置为高级：
   `set -priv advanced`

3. 在SVM上启用Cloud KMS
   `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`
   出现提示时，使用服务帐户专用密钥输入 JSON 文件的内容
4. 验证Cloud KMS是否配置了正确的参数：
   `security key-manager external gcp show vserver svm_name`
   的状态 `kms_wrapped_key_status` 将是 "UNKNOWN" 如果尚未创建加密卷。
   如果服务可访问性不正常、请通过数据SVM LIF与GCP密钥管理服务建立连接。

如果已为数据SVM配置一个或多个加密卷、并且相应的NVE密钥由管理SVM板载密钥管理器管理、则这些密钥应迁移到外部密钥管理服务。要使用命令行界面执行此操作、请运行以下命令：
`security key-manager key migrate -from-Vserver admin_SVM -to-Vserver data_SVM`
只有在成功迁移数据SVM的所有NVE密钥之后、才能为租户的数据SVM创建新的加密卷。

相关信息

- "使用适用于Cloud Volumes ONTAP的NetApp加密解决方案加密卷"

在 ONTAP 9.6 及更高版本（ NVE ）中启用板载密钥管理

您可以使用板载密钥管理器保护集群用于访问加密数据的密钥。您必须在访问加密卷或自加密磁盘的每个集群上启用板载密钥管理器。

关于此任务

您必须运行 `security key-manager onboard sync` 命令。

如果您使用的是MetroCluster配置、则必须运行 `security key-manager onboard enable` 命令、然后运行 `security key-manager onboard sync` 命令、并在每个上使用相同的密码短语。运行时 `security key-manager onboard enable` 命令、然后在远程集群上同步、则不需要运行 `enable` 命令。

默认情况下，重新启动节点时不需要输入密钥管理器密码短语。您可以使用 `cc-mode-enabled=yes` 选项、要求用户在重新启动后输入密码短语。

对于NVE (如果已设置) `cc-mode-enabled=yes`、使用创建的卷 `volume create` 和 `volume move start` 命令会自动加密。适用于 `volume create`，则无需指定 `-encrypt true`。适用于 `volume move start`，则无需指定 `-encrypt-destination true`。

配置 ONTAP 空闲数据加密时，为了满足分类商业解决方案（ CSFC ）的要求，您必须将 NSE 与 NVE 结合使用，并确保在通用标准模式下启用板载密钥管理器。请参见 "CSFC 解决方案简介" 有关 CSFC 的详细信息，请参见。

在通用标准模式下启用板载密钥管理器时 (`cc-mode-enabled=yes`)、系统行为将通过以下方式进行更改：

- 在通用标准模式下运行时，系统会监控连续失败的集群密码短语尝试。

  如果在启动时未输入正确的集群密码短语，则不会挂载加密卷。要更正此问题，您必须重新启动节点并输入正确的集群密码短语。启动后，对于需要使用集群密码短语作为参数的任何命令，系统最多允许连续 5 次尝试在 24 小时内正确输入集群密码短语。如果已达到限制（例如，您连续 5 次未正确输入集群密码短语），则必须等待 24 小时超时期限过后，或者重新启动节点，才能重置此限制。

- 系统映像更新使用 NetApp RSA-3072 代码签名证书以及 SHA-384 代码签名摘要来检查映像完整性，而不是使用通常的 NetApp RSA-2048 代码签名证书和 SHA-256 代码签名摘要。

  upgrade 命令可通过检查各种数字签名来验证映像内容是否未被更改或损坏。如果验证成功，映像更新过程将继续执行下一步；否则，映像更新将失败。请参见 `cluster image` 有关系统更新的信息、请参见手册页。

板载密钥管理器将密钥存储在易失性内存中。系统重新启动或暂停后，易失性内存内容将被清除。在正常运行条件下，系统暂停后，易失性内存内容将在 30 秒内清除。

开始之前

- 您必须是集群管理员才能执行此任务。
- 在配置板载密钥管理器之前，您必须配置 MetroCluster 环境。

步骤

1. 启动密钥管理器设置：

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

   设置 `cc-mode-enabled=yes` 要求用户在重新启动后输入密钥管理器密码短语。对于NVE (如果已设置) `cc-mode-enabled=yes`、使用创建的卷 `volume create` 和 `volume move start` 命令会自动加密。。 `- cc-mode-enabled` 选项在MetroCluster配置中不受支持。。 `security key-manager onboard enable` 命令用于替换 `security key-manager setup` 命令：

   以下示例将在 cluster1 上启动密钥管理器设置命令，而无需在每次重新启动后输入密码短语：

   ```
   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. 在密码短语提示符处，输入 32 到 256 个字符的密码短语，或者对于 "`cc-mode` " ，输入 64 到 256 个字符的密码短语。

如果指定的 "`cc-mode` " 密码短语少于 64 个字符，则在密钥管理器设置操作再次显示密码短语提示之前会有五秒的延迟。

3. 在密码短语确认提示符处，重新输入密码短语。
4. 验证是否已创建身份验证密钥：

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

。 `security key-manager key query` 命令用于替换 `security key-manager query key` 命令：有关完整的命令语法，请参见手册页。

以下示例将验证是否已为创建身份验证密钥 `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:
000000000000000002000000000000100056178fc6ace6d91472df8a9286daacc00000000
00000000

node1                                    NSE-AK   AES-256      true

    Key ID:
000000000000000002000000000000100df1689a148fdfbf9c2b198ef974d0baa00000000
00000000

2 entries were displayed.
```

5. (可选)将纯文本卷转换为加密卷。

```
volume encryption conversion start
```

转换卷之前、必须完全配置板载密钥管理器。在MetroCluster环境中、必须同时在两个站点上配置板载密钥管理器。

完成后

将密码短语复制到存储系统以外的安全位置，以供将来使用。

配置板载密钥管理器密码短语时，您还应手动将信息备份到存储系统以外的安全位置，以便在发生灾难时使用。请参见 "手动备份板载密钥管理信息"。

在 ONTAP 9.5 及更早版本（ NVE ）中启用板载密钥管理

您可以使用板载密钥管理器保护集群用于访问加密数据的密钥。您必须在访问加密卷或自加密磁盘的每个集群上启用板载密钥管理器。

关于此任务

您必须运行 `security key-manager setup` 命令。

如果您使用的是 MetroCluster 配置，请查看以下准则：

- 在ONTAP 9.5中、必须运行 `security key-manager setup` 在本地集群上、然后 `security key-manager setup -sync-metrocluster-config yes` 在远程集群上、在每个上使用相同的密码短语。
- 在ONTAP 9.5之前的版本中、您必须运行 `security key-manager setup` 在本地集群上、等待大约20秒、然后运行 `security key-manager setup` 在远程集群上、在每个上使用相同的密码短语。

默认情况下，重新启动节点时不需要输入密钥管理器密码短语。从ONTAP 9.4开始、您可以使用 `-enable-cc-mode yes` 选项、要求用户在重新启动后输入密码短语。

对于NVE (如果已设置) `-enable-cc-mode yes`、使用创建的卷 `volume create` 和 `volume move start` 命令会自动加密。适用于 `volume create`，则无需指定 `-encrypt true`。适用于 `volume move start`，则无需指定 `-encrypt-destination true`。

密码短语尝试失败后，必须重新启动节点。

开始之前

- 如果将NSE或NVE与外部密钥管理(KMIP)服务器结合使用、则必须事先删除外部密钥管理器数据库。

  "从外部密钥管理过渡到板载密钥管理"

- 您必须是集群管理员才能执行此任务。
- 在配置板载密钥管理器之前，您必须配置 MetroCluster 环境。

步骤

1. 启动密钥管理器设置：

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

   从ONTAP 9.4开始、您可以使用 `-enable-cc-mode yes` 此选项要求用户在重新启动后输入密钥管理器密码短语。对于NVE (如果已设置) `-enable-cc-mode yes`、使用创建的卷 `volume create` 和 `volume move start` 命令会自动加密。

   以下示例将开始在 cluster1 上设置密钥管理器，而无需在每次重新启动后输入密码短语：

```
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. 输入 ... `yes` 在提示符处配置板载密钥管理。
3. 在密码短语提示符处，输入 32 到 256 个字符的密码短语，或者对于 "`cc-mode` " ，输入 64 到 256 个字符的密码短语。

> 如果指定的 "`cc-mode` " 密码短语少于 64 个字符，则在密钥管理器设置操作再次显示密码短语提示之前会有五秒的延迟。

4. 在密码短语确认提示符处，重新输入密码短语。
5. 验证是否已为所有节点配置密钥：

   `security key-manager key show`

   有关完整的命令语法，请参见手册页。

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

Node: node1
Key Store: onboard
Key ID                                                           Used By
-----------------------------------------------------------------
--------
000000000000000002000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                           Used By
-----------------------------------------------------------------
--------
000000000000000002000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

6. (可选)将纯文本卷转换为加密卷。

   `volume encryption conversion start`

   转换卷之前、必须完全配置板载密钥管理器。在MetroCluster环境中、必须同时在两个站点上配置板载密钥管理器。

完成后

将密码短语复制到存储系统以外的安全位置，以供将来使用。

配置板载密钥管理器密码短语时，您还应手动将信息备份到存储系统以外的安全位置，以便在发生灾难时使用。请参见 "手动备份板载密钥管理信息"。

在新添加的节点中启用板载密钥管理

您可以使用板载密钥管理器保护集群用于访问加密数据的密钥。您必须在访问加密卷或自加密磁盘的每个集群上启用板载密钥管理器。

> 对于ONTAP 9.5及更早版本、必须运行 `security key-manager setup` 命令。
>
> 对于ONTAP 9.6及更高版本、必须运行 `security key-manager sync` 命令。
>
> 如果要将节点添加到配置了板载密钥管理的集群中，您将运行此命令刷新缺少的密钥。

如果您使用的是 MetroCluster 配置，请查看以下准则：

- 从ONTAP 9.6开始、您必须运行 `security key-manager onboard enable` 首先在本地集群上运行 `security key-manager onboard sync` 在远程集群上、在每个上使用相同的密码短语。
- 在ONTAP 9.5中、必须运行 `security key-manager setup` 在本地集群上、然后 `security key-manager setup -sync-metrocluster-config yes` 在远程集群上、在每个上使用相同的密码短语。
- 在ONTAP 9.5之前的版本中、您必须运行 `security key-manager setup` 在本地集群上、等待大约20秒、然后运行 `security key-manager setup` 在远程集群上、在每个上使用相同的密码短语。

默认情况下，重新启动节点时不需要输入密钥管理器密码短语。从ONTAP 9.4开始、您可以使用 `-enable-cc-mode yes` 选项、要求用户在重新启动后输入密码短语。

对于NVE (如果已设置) `-enable-cc-mode yes`、使用创建的卷 `volume create` 和 `volume move start` 命令会自动加密。适用于 `volume create`，则无需指定 `-encrypt true`。适用于 `volume move start`，则无需指定 `-encrypt-destination true`。

> 密码短语尝试失败后，必须重新启动节点。

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。

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`

有关完整的命令语法，请参见手册页。

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`

   有关完整的命令语法，请参见手册页。

   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。

在新卷上启用加密

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。

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`

   有关完整的命令语法、请参见命令参考页面上的链接：https://docs.netapp.com/us-en/ontap-cli/volume-create.html[`volume create`^。

2. 验证是否已为卷启用加密：

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

   有关完整的命令语法，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。

=
:allow-uri-read:

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

- 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。或者、您也可以使用 `volume move start` 命令：
- 对于ONTAP 9.2及更早版本、只能使用 `volume move start` 命令以通过移动现有卷启用加密。

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

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。

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
   ```

   有关整个命令语法、请参见命令的手册页。

   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
   ```

   有关整个命令语法、请参见命令的手册页。

   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
   ```

有关整个命令语法、请参见命令的手册页。

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` 命令以通过移动现有卷启用加密。您必须使用 `volume move start` 在ONTAP 9.2及更早版本中。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`

有关整个命令语法、请参见命令的手册页。

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。

有关整个命令语法、请参见命令的手册页。

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`

   有关整个命令语法、请参见命令的手册页。

   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、请参见 `volume move`，请参阅 移动卷。

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 © 2024 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。