使用 CLI 管理加密

ONTAP 9

NetApp
April 24, 2024

目录

使用 CLI 管理加密

NetApp加密概述

NetApp 提供了基于软件和基于硬件的加密技术，可确保在存储介质被重新利用，退回，放置在不当位置或被盗时无法读取空闲数据。

- 使用NetApp卷加密(NVE)的基于软件的加密支持一次对一个卷进行数据加密
- 使用NetApp存储加密(NetApp Storage Encryption、NSE)的基于硬件的加密支持在数据写入时对其进行全磁盘加密(FDE)。

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 。

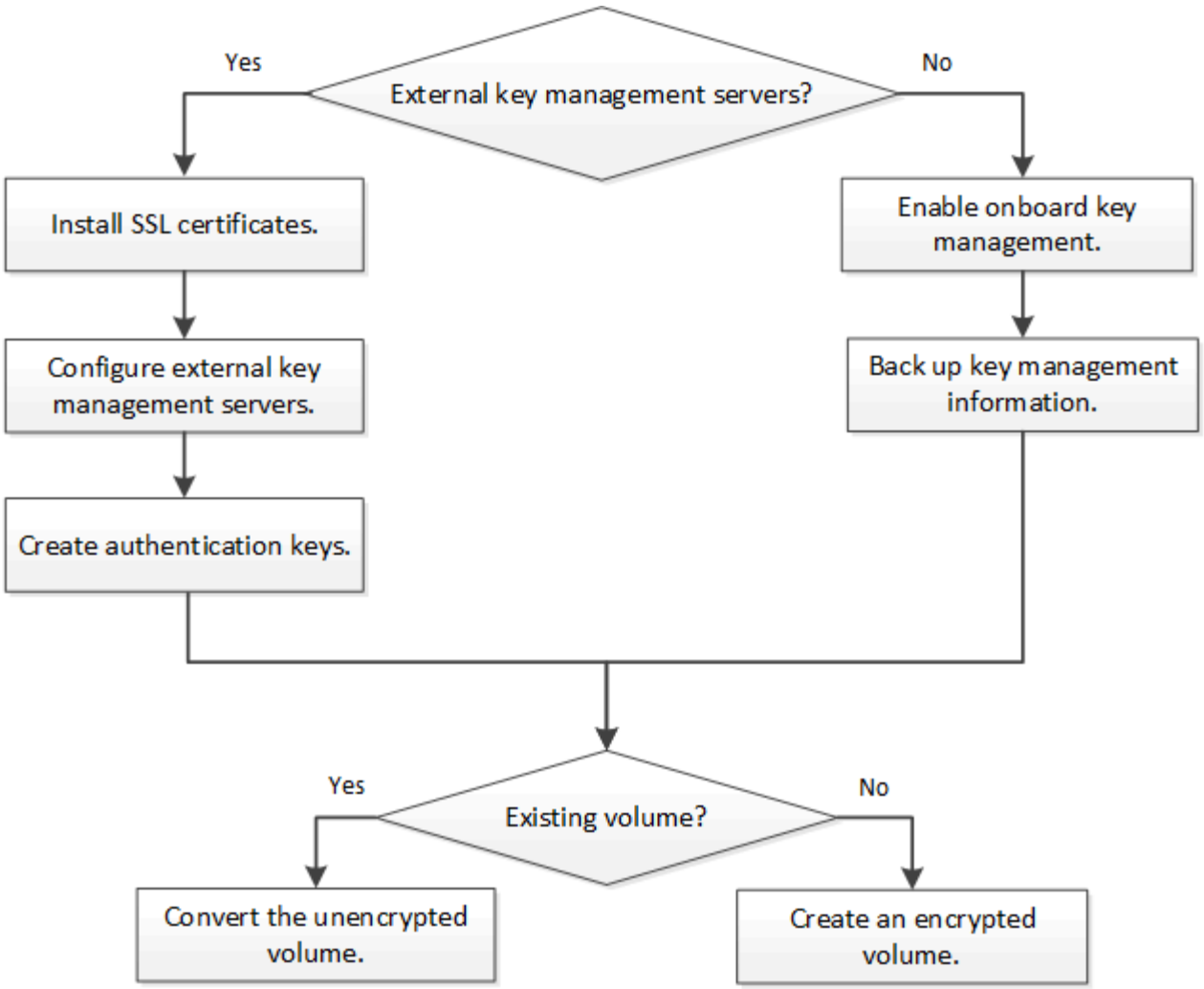
存储效率	重复数据删除，数据压缩，数据缩减， FlexClone 。 即使从父级拆分克隆后，克隆也会使用与父级相同的密钥。您应执行 `volume move` 在拆分的克隆上、之后、拆分的克隆将具有不同的密钥。
Replication	• 对于卷复制、源卷和目标卷可以具有不同的加密设置。可以为源配置加密，也可以为目标取消配置加密，反之亦然。 • 对于 SVM 复制，目标卷会自动加密，除非目标卷不包含支持卷加密的节点（在这种情况下复制成功，但目标卷不会加密）。 • 对于 MetroCluster 配置，每个集群从其配置的密钥服务器中提取外部密钥管理密钥。配置复制服务会将 OKM 密钥复制到配对站点。
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，您应先执行此操作 "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。虽然目前不需要、但现有客户可以选择这样做 "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"。

   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*安全性*下的*加密*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“端口”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 … ⌄ 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 … × 旁边的证书名称可删除不想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*安全性*下的*加密*部分中，选择 ⋮，然后选择*编辑外部密钥管理器*。

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 。
   - 通过选择删除密钥服务器 ⋮ 位于包含密钥服务器名称的表单元格的末尾。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*安全性*下的*加密*部分中，选择 ⋮，然后选择*删除外部密钥管理器*。

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：

```
clusterl::> 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"。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:
   00000000000000000200000000000100056178fc6ace6d91472df8a9286daacc00000000
   00000000

   node1                                   NSE-AK   AES-256      true

       Key ID:
   00000000000000000200000000000100df1689a148fdfbf9c2b198ef974d0baa00000000
   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
-----------------------------------------------------------------------
--------
000000000000000002000000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                                   Used By
-----------------------------------------------------------------------
--------
000000000000000002000000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000000001008C07CC0AF1EF49E0105300EFC83004BF 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、如果您有、则新创建的聚合和卷会默认进行加密 "VE许可证" 以及板载或外部密钥管理。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、如果具有、则新创建的卷会默认进行加密 "VE许可证" 以及板载或外部密钥管理。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-9141/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 "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
   ```

配置基于 NetApp 硬件的加密

配置 NetApp 基于硬件的加密概述

NetApp 基于硬件的加密支持在数据写入时对其进行全磁盘加密（FDE）。如果固件上未存储加密密钥，则无法读取数据。而加密密钥只能由经过身份验证的节点访问。

了解 NetApp 基于硬件的加密

节点使用从外部密钥管理服务器或板载密钥管理器检索的身份验证密钥向自加密驱动器进行自我身份验证：

- 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，可从与数据相同的存储系统为节点提供身份验证密钥。

您可以将 NetApp 卷加密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。

启用自加密驱动器后、核心转储也会进行加密。

> 如果 HA 对使用加密 SAS 或 NVMe 驱动器（ SED ， NSE ， FIPS ），则必须按照主题中的说明进行操作 将 FIPS 驱动器或 SED 恢复到未受保护的模式 初始化系统之前 HA 对中的所有驱动器（启动选项 4 或 9 ）。如果不这样做，则在重新利用驱动器时，可能会导致未来数据丢失。

支持的自加密驱动器类型

支持两种类型的自加密驱动器：

- 所有 FAS 和 AFF 系统均支持自加密 FIPS 认证的 SAS 或 NVMe 驱动器。这些驱动器称为 _fips drives ， _ 符合联邦信息处理标准出版物 140-2 第 2 级的要求。经过认证的功能除了加密之外，还可以提供保护，例如防止驱动器受到拒绝服务攻击。不能在同一节点或 HA 对上将 FIPS 驱动器与其他类型的驱动器混合使用。
- 从ONTAP 9.6开始、AFF A800、A320及更高版本的系统支持未经过FIPS测试的自加密NVMe驱动器。这些驱动器称为_SED、可提供与FIPS驱动器相同的加密功能、但可以与同一节点或HA对上的非加密驱动器混合使用。
- 所有经过FIPS验证的驱动器都使用经过FIPS验证的固件加密模块。 FIPS驱动器加密模块不使用在驱动器外部生成的任何密钥(驱动器的固件加密模块使用输入到驱动器的身份验证密码短语来获取密钥加密密钥)。

> 非加密驱动器是指非SED或FIPS驱动器的驱动器。

> 如果在具有Flash Cache模块的系统上使用NSE、则还应启用NVE或NAE。NSE不会对驻留在Flash Cache模块上的数据进行加密。

何时使用外部密钥管理

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、则应使用外部密钥管理：

- 贵组织的策略要求密钥管理解决方案 使用FIPS 140-2 2级(或更高)加密模块。
- 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。

支持详细信息

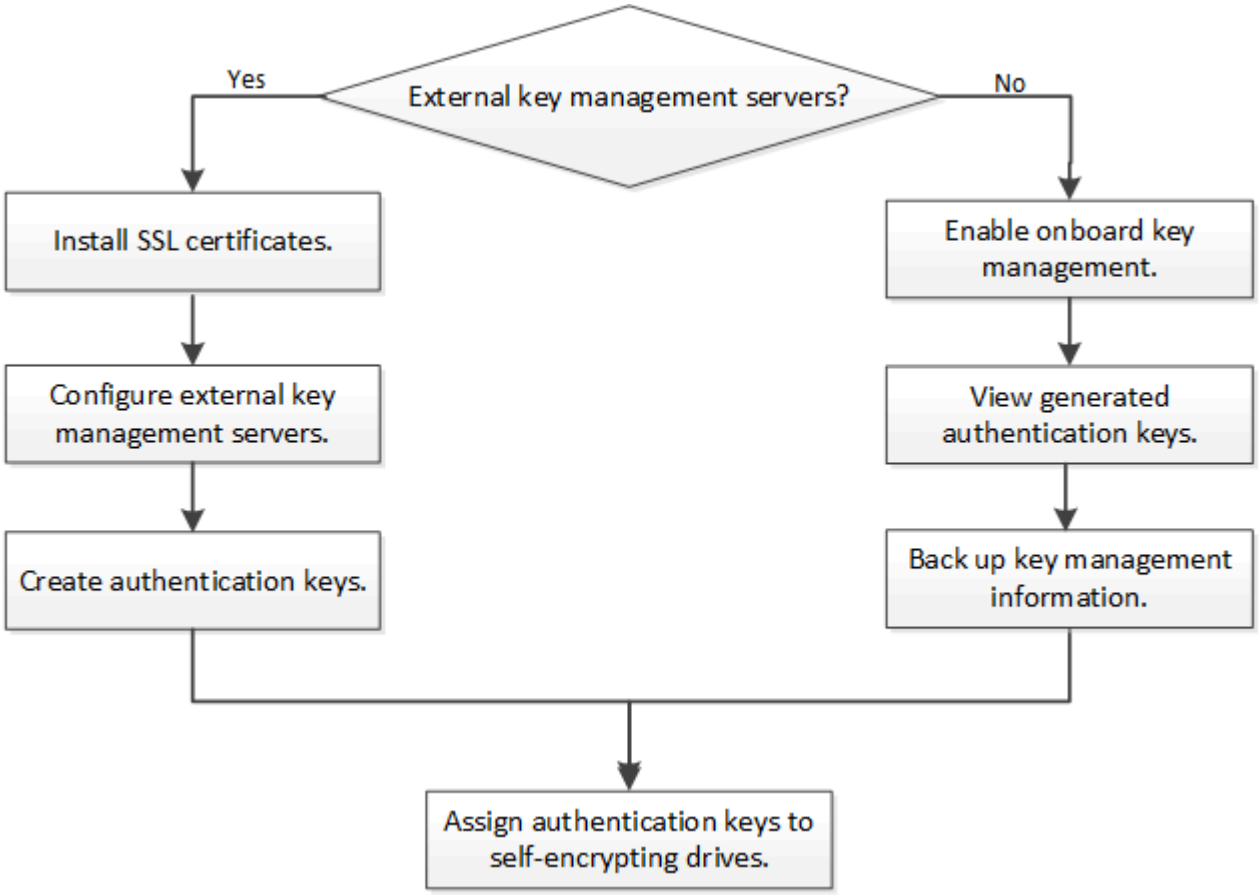
下表显示了重要的硬件加密支持详细信息。有关受支持的 KMIP 服务器，存储系统和磁盘架的最新信息，请参见互操作性表。

资源或功能	支持详细信息
非同构磁盘集	• 不能在同一节点或 HA 对上将 FIPS 驱动器与其他类型的驱动器混合使用。在同一集群中，遵从的 HA 对可以与不遵从的 HA 对共存。 • SED可以与同一节点或HA对上的非加密驱动器混合使用。

驱动器类型	• FIPS 驱动器可以是 SAS 或 NVMe 驱动器。 • SED 必须是 NVMe 驱动器。
10 Gb 网络接口	从 ONTAP 9.3 开始， KMIP 密钥管理配置支持使用 10 Gb 网络接口与外部密钥管理服务器进行通信。
用于与密钥管理服务器通信的端口	从 ONTAP 9.3 开始，您可以使用任何存储控制器端口与密钥管理服务器进行通信。否则、您应使用端口e0M与密钥管理服务器进行通信。根据存储控制器型号，某些网络接口在启动过程中可能不可用，无法与密钥管理服务器进行通信。
MetroCluster （MCC）	• NVMe 驱动器支持 MCC 。 • SAS 驱动器不支持 MCC 。

基于硬件的加密工作流

您必须先配置密钥管理服务，然后集群才能向自加密驱动器进行身份验证。您可以使用外部密钥管理服务器或板载密钥管理器。



相关信息

- "NetApp Hardware Universe"
- "NetApp 卷加密和 NetApp 聚合加密"

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。

在 ONTAP 9.1 及更高版本中，可以使用板载密钥管理器实施 NetApp 卷加密（NVE）。在 ONTAP 9.3 及更高版本中， NVE 可通过外部密钥管理（KMIP）和板载密钥管理器来实施。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。

在 **ONTAP 9.2** 及更早版本中收集网络信息

如果您使用的是 ONTAP 9.2 或更早版本，则应先填写网络配置工作表，然后再启用外部密钥管理。

从 ONTAP 9.3 开始，系统会自动发现所有需要的网络信息。

项目	注释：	价值
密钥管理网络接口名称		
密钥管理网络接口 IP 地址	节点管理 LIF 的 IP 地址，采用 IPv4 或 IPv6 格式	
密钥管理网络接口 IPv6 网络前缀长度	如果使用的是 IPv6 ，则为 IPv6 网络前缀长度	
密钥管理网络接口子网掩码		
密钥管理网络接口网关 IP 地址		
集群网络接口的 IPv6 地址	只有在对密钥管理网络接口使用 IPv6 时才需要此参数	
每个 KMIP 服务器的端口号	可选。所有 KMIP 服务器的端口号必须相同。如果不提供端口号，则默认为端口 5696 ，即为 KMIP 的 Internet 分配的编号颁发机构（IANA）分配的端口。	

密钥标记名称	可选。密钥标记名称用于标识属于某个节点的所有密钥。默认密钥标记名称是节点名称。	

相关信息

"NetApp 技术报告 3954：《适用于 IBM Tivoli Lifetime Key Manager 的 NetApp 存储加密安装前要求和过程》"

"NetApp 技术报告 4074：《 SafeNet KeySecure 的 NetApp 存储加密安装前要求和过程》"

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（基于硬件）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。

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。

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. 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：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。有关完整的命令语法，请参见手册页。
   - 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：

   ```
   clusterl::> security key-manager external enable -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. 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 -vserver SVM -key
   -server host_name|IP_address:port -key-server-status available|not-
   responding|unknown
   ```

   。 `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
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available
node2
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available

6 entries were displayed.
```

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。

配置集群模式外部密钥服务器

从ONTAP 9.11.1开始、您可以配置与SVM上的集群模式外部密钥管理服务器的连接。使用集群模式密钥服务器、您可以在SVM上指定主密钥服务器和二级密钥服务器。注册密钥时、ONTAP 会先尝试访问主密钥服务器、然后再按顺序尝试访问二级服务器、直到操作成功完成、从而防止密钥重复。

外部密钥服务器可用于NSE、NVE、NAE和SED密钥。一个SVM最多可支持四个主外部KMIP服务器。每个主服

务器最多可支持三个二级密钥服务器。

开始之前

- "必须为SVM启用KMIP密钥管理"。
- 此过程仅支持使用KMIP的密钥服务器。有关支持的密钥服务器列表、请查看 "NetApp 互操作性表工具"。
- 集群中的所有节点都必须运行ONTAP 9.11.1或更高版本。
- 服务器的顺序列出中的参数 `-secondary-key-servers` 参数反映外部密钥管理(KMIP)服务器的访问顺序。

创建集群密钥服务器

配置操作步骤 取决于您是否配置了主密钥服务器。

将主密钥服务器和二级密钥服务器添加到**SVM**

1. 确认尚未为集群启用密钥管理：
   `security key-manager external show -vserver` *`svm_name`*
   如果SVM已启用最多四个主密钥服务器、则必须先删除其中一个现有主密钥服务器、然后再添加新的主密钥服务器。
2. 启用主密钥管理器：
   `security key-manager external enable -vserver` *`svm_name`* `-key-servers` *`server_ip`* `-client-cert` *`client_cert_name`* `-server-ca-certs` *`server_ca_cert_names`*
3. 修改主密钥服务器以添加二级密钥服务器。。 `-secondary-key-servers` 参数可接受最多包含三个密钥服务器的逗号分隔列表。
   `security key-manager external modify-server -vserver` *`svm_name`* `-key-servers` *`primary_key_server`* `-secondary-key-servers` *`list_of_key_servers`*

将二级密钥服务器添加到现有主密钥服务器

1. 修改主密钥服务器以添加二级密钥服务器。。 `-secondary-key-servers` 参数可接受最多包含三个密钥服务器的逗号分隔列表。
   `security key-manager external modify-server -vserver` *`svm_name`* `-key-servers` *`primary_key_server`* `-secondary-key-servers` *`list_of_key_servers`*
   有关二级密钥服务器的详细信息、请参见 [mod-secondary]。

修改集群模式密钥服务器

您可以通过更改特定密钥服务器的状态(主或二级)、添加和删除二级密钥服务器或更改二级密钥服务器的访问顺序来修改外部密钥服务器集群。

转换主密钥服务器和辅助密钥服务器

要将主密钥服务器转换为二级密钥服务器、必须先使用将其从SVM中删除 `security key-manager external remove-servers` 命令：

要将二级密钥服务器转换为主密钥服务器、必须先从其现有主密钥服务器中删除二级密钥服务器。请参见 [mod-secondary]。如果在删除现有密钥的同时将二级密钥服务器转换为主服务器、则在完成删除和转换之前尝试添加新服务器可能会导致密钥重复。

修改二级密钥服务器

二级密钥服务器通过进行管理 `-secondary-key-servers` 的参数 `security key-manager external modify-server` 命令：。 `-secondary-key-servers` 参数接受逗号分隔列表。此列表中二级密钥服务器的指定顺序决定了二级密钥服务器的访问顺序。可以通过运行命令来修改访问顺序 `security key-manager external modify-server` 次密钥服务器按不同顺序输入。

要删除辅助密钥服务器、请 `-secondary-key-servers` 参数应包括要保留的密钥服务器、而不包括要删除的密钥服务器。要删除所有辅助密钥服务器、请使用参数 `-`，表示无。

对于追加信息 、请参见 `security key-manager external` 页面 "ONTAP 命令参考"。

在 **ONTAP 9.6** 及更高版本中创建身份验证密钥

您可以使用 `security key-manager key create` 命令为节点创建身份验证密钥并将其存储在已配置的KMIP服务器上。

关于此任务

如果您的安全设置要求您使用不同的密钥进行数据身份验证和 FIPS 140-2 身份验证，则应为每个密钥创建一个单独的密钥。否则、您可以使用与数据访问相同的身份验证密钥来满足FIPS合规性要求。

ONTAP 会为集群中的所有节点创建身份验证密钥。

- 启用板载密钥管理器后，不支持此命令。但是，启用板载密钥管理器后，系统会自动创建两个身份验证密钥。可以使用以下命令查看这些密钥：

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

- 如果已配置的密钥管理服务器已存储超过 128 个身份验证密钥，则会收到警告。
- 您可以使用 `security key-manager key delete` 命令以删除任何未使用的密钥。。 `security key-manager key delete` 如果给定密钥当前正由ONTAP使用、则命令将失败。（要使用此命令，您的权限必须大于 "`admin` "。）

> 在MetroCluster 环境中、删除密钥之前、必须确保配对集群上未使用此密钥。您可以在配对集群上使用以下命令来检查此密钥是否未被使用：
>
> - `storage encryption disk show -data-key-id` *`key-id`*
> - `storage encryption disk show -fips-key-id` *`key-id`*

开始之前

您必须是集群管理员才能执行此任务。

步骤

1. 为集群节点创建身份验证密钥：

   ```
   security key-manager key create -key-tag passphrase_label -prompt-for-key
   true|false
   ```

> 正在设置 ... `prompt-for-key=true` 使系统提示集群管理员在对加密驱动器进行身份验证时使用密码短语。否则，系统将自动生成 32 字节密码短语。 。 `security key-manager key create` 命令用于替换 `security key-manager create-key` 命令：有关完整的命令语法，请参见手册页。

以下示例将为创建身份验证密钥 `cluster1`，自动生成32字节密码短语：

```
cluster1::> security key-manager key create
Key ID:
00000000000000000200000000000001006268333f870860128fbe17d393e5083b00000000
00000000
```

2. 验证是否已创建身份验证密钥：

   `security key-manager key query -node node`

   > 。 `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。 输出中显示的密钥 ID 是用于引用身份验证密钥的标识符。它不是实际的身份验证密钥或数据加密密钥。

   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
       Vserver: cluster1
   Key Manager: external
          Node: node1

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

       Vserver: cluster1
   Key Manager: external
          Node: node2

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node2                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

在 **ONTAP 9.5** 及更早版本中创建身份验证密钥

您可以使用 `security key-manager create-key` 命令为节点创建身份验证密钥并将其存储在已配置的KMIP服务器上。

关于此任务

如果您的安全设置要求您使用不同的密钥进行数据身份验证和 FIPS 140-2 身份验证，则应为每个密钥创建一个单独的密钥。否则，您可以使用与数据访问相同的身份验证密钥来满足 FIPS 合规性要求。

ONTAP 会为集群中的所有节点创建身份验证密钥。

- 启用板载密钥管理后，不支持此命令。
- 如果已配置的密钥管理服务器已存储超过 128 个身份验证密钥，则会收到警告。

您可以使用密钥管理服务器软件删除任何未使用的密钥，然后再次运行命令。

开始之前

您必须是集群管理员才能执行此任务。

步骤

1. 为集群节点创建身份验证密钥：

   `security key-manager create-key`

   有关完整的命令语法，请参见命令手册页。

   > 输出中显示的密钥 ID 是用于引用身份验证密钥的标识符。它不是实际的身份验证密钥或数据加密密钥。

   以下示例将为创建身份验证密钥 `cluster1`：

   ```
   cluster1::> security key-manager create-key
      (security key-manager create-key)
   Verifying requirements...

   Node: cluster1-01
   Creating authentication key...
   Authentication key creation successful.
   Key ID: F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

   Node: cluster1-01
   Key manager restore operation initialized.
   Successfully restored key information.

   Node: cluster1-02
   Key manager restore operation initialized.
   Successfully restored key information.
   ```

2. 验证是否已创建身份验证密钥：

   `security key-manager query`

   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 query

  (security key-manager query)

          Node: cluster1-01
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag        Key Type  Restored
-------------  --------  --------
cluster1-01    NSE-AK    yes
       Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C


          Node: cluster1-02
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag        Key Type  Restored
-------------  --------  --------
cluster1-02    NSE-AK    yes
       Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
```

将数据身份验证密钥分配给 **FIPS** 驱动器或 **SED** （外部密钥管理）

您可以使用 `storage encryption disk modify` 用于将数据身份验证密钥分配给FIPS驱动器或SED的命令。集群节点使用此密钥锁定或解锁驱动器上的加密数据。

关于此任务

只有当自加密驱动器的身份验证密钥 ID 设置为非默认值时，才会保护其免遭未经授权的访问。密钥 ID 为 0x0 的制造商安全 ID （ MSID ）是 SAS 驱动器的标准默认值。对于 NVMe 驱动器，标准默认值为空密钥，表示为空密钥 ID 。将密钥 ID 分配给自加密驱动器时，系统会将其身份验证密钥 ID 更改为非默认值。

此操作步骤 不会造成中断。

开始之前

您必须是集群管理员才能执行此任务。

步骤

1. 将数据身份验证密钥分配给 FIPS 驱动器或 SED：

   `storage encryption disk modify -disk` *`disk_ID`* `-data-key-id` *`key_ID`*

   有关完整的命令语法，请参见命令手册页。

您可以使用 `security key-manager query -key-type NSE-AK` 用于查看密钥ID的命令。

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

2. 验证是否已分配身份验证密钥：

   `storage encryption disk show`

   有关完整的命令语法，请参见手册页。

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
--------------------------------------------------------------------
0.0.0   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
0.0.1   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
[...]
```

配置板载密钥管理

在 **ONTAP 9.6** 及更高版本中启用板载密钥管理

您可以使用板载密钥管理器向 FIPS 驱动器或 SED 验证集群节点的身份。板载密钥管理器是一个内置工具，可从与数据相同的存储系统为节点提供身份验证密钥。板载密钥管理器符合 FIPS-140-2 1 级标准。

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 enable` 命令。在MetroCluster配置中、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。

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。除了在MetroCluster中、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。

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。

  如果启用了 NetApp 存储加密（NSE），但在启动时未输入正确的集群密码短语，则系统将无法向其驱动器进行身份验证并自动重新启动。要更正此问题，您必须在启动提示符处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。有关系统更新的信息，请参见 "`cluster image` " 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

- 如果将 NSE 与外部密钥管理（KMIP）服务器结合使用，则必须已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，您必须先配置 MetroCluster 环境。

步骤

1. 启动密钥管理器设置命令：

   ```
   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。。 `- 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 -node node
```

> 。 `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
       Vserver: cluster1
   Key Manager: onboard
          Node: node1

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
00000000000000000200000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
00000000000000000200000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

       Vserver: cluster1
   Key Manager: onboard
          Node: node2

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
00000000000000000200000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                    NSE-AK    yes
    Key ID:
00000000000000000200000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

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。

所有密钥管理信息都会自动备份到集群的复制数据库（RDB）。您还应手动备份此信息，以便在发生灾难时使用。

在 **ONTAP 9.5** 及更早版本中启用板载密钥管理

您可以使用板载密钥管理器向 FIPS 驱动器或 SED 验证集群节点的身份。板载密钥管理器是一个内置工具，可从与数据相同的存储系统为节点提供身份验证密钥。板载密钥管理器符合 FIPS-140-2 1 级标准。

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 与外部密钥管理（ KMIP ）服务器结合使用，则必须已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，您必须先配置 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
-------------------------------------------------------------------
--------
00000000000000000200000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
00000000000000000200000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                                   Used By
-------------------------------------------------------------------
--------
00000000000000000200000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
00000000000000000200000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

完成后

所有密钥管理信息都会自动备份到集群的复制数据库（RDB）。

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"。

将数据身份验证密钥分配给 **FIPS** 驱动器或 **SED** （板载密钥管理）

您可以使用 `storage encryption disk modify` 用于将数据身份验证密钥分配给FIPS驱动器或SED的命令。集群节点使用此密钥访问驱动器上的数据。

关于此任务

只有当自加密驱动器的身份验证密钥 ID 设置为非默认值时，才会保护其免遭未经授权的访问。密钥 ID 为 0x0 的制造商安全 ID （MSID）是 SAS 驱动器的标准默认值。对于 NVMe 驱动器，标准默认值为空密钥，表示为空密钥 ID 。将密钥 ID 分配给自加密驱动器时，系统会将其身份验证密钥 ID 更改为非默认值。

开始之前

您必须是集群管理员才能执行此任务。

步骤

1. 将数据身份验证密钥分配给 FIPS 驱动器或 SED：

   `storage encryption disk modify -disk` *`disk_ID`* `-data-key-id` *`key_ID`*

   有关完整的命令语法，请参见命令手册页。

   > 您可以使用 `security key-manager key query -key-type NSE-AK` 用于查看密钥ID的命令。

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   00000000000000000200000000000010019215b9738bc7b43d4698c80246db1f4

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

2. 验证是否已分配身份验证密钥：

   `storage encryption disk show`

   有关完整的命令语法，请参见手册页。

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
--------------------------------------------------------------------
0.0.0   data
000000000000000002000000000010019215b9738bc7b43d4698c80246db1f4
0.0.1   data
000000000000000002000000000010059851742AF2703FC91369B7DB47C4722
[...]
```

将 FIPS 140-2 身份验证密钥分配给 FIPS 驱动器

您可以使用 `storage encryption disk modify` 命令 `-fips-key-id` 用于将FIPS 140-2身份验证密钥分配给FIPS驱动器的选项。集群节点将此密钥用于数据访问以外的驱动器操作，例如防止驱动器受到拒绝服务攻击。

关于此任务

您的安全设置可能要求您使用不同的密钥进行数据身份验证和 FIPS 140-2 身份验证。否则，您可以使用与数据访问相同的身份验证密钥来满足 FIPS 合规性要求。

此操作步骤 不会造成中断。

开始之前

驱动器固件必须支持 FIPS 140-2 合规性。。 "NetApp 互操作性表工具" 包含有关支持的驱动器固件版本的信息。

步骤

1. 您必须首先确保已分配数据身份验证密钥。可以使用来完成此操作 外部密钥管理器 或 板载密钥管理器。使用命令验证是否已分配密钥 `storage encryption disk show`。
2. 将 FIPS 140-2 身份验证密钥分配给 SED：

   `storage encryption disk modify -disk` *`disk_id`* `-fips-key-id` *`fips_authentication_key_id`*

   您可以使用 `security key-manager query` 用于查看密钥ID的命令。

   ```
   cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
   6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

3. 验证是否已分配身份验证密钥：

```
storage encryption disk show -fips
```

有关完整的命令语法，请参见手册页。

```
cluster1::> storage encryption disk show -fips
Disk    Mode FIPS-Compliance Key ID
------  ----
-------------------------------------------------------------------
2.10.0  full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
2.10.1  full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
[...]
```

为 KMIP 服务器连接启用集群范围 FIPS 兼容模式

您可以使用 `security config modify` 命令 `-is-fips-enabled` 用于为传输中的数据启用集群范围FIPS兼容模式的选项。这样做会强制集群在连接到 KMIP 服务器时在 FIPS 模式下使用 OpenSSL 。

关于此任务

启用集群范围 FIPS 兼容模式后，集群将仅自动使用 TLS1.2 和 FIPS 验证的密码套件。默认情况下，集群范围 FIPS 兼容模式处于禁用状态。

修改集群范围的安全配置后，您必须手动重新启动集群节点。

开始之前

- 存储控制器必须配置为 FIPS 兼容模式。
- 所有 KMIP 服务器都必须支持 TLSv1.2 。启用集群范围 FIPS 兼容模式后，系统需要使用 TLSv1.2 完成与 KMIP 服务器的连接。

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 验证是否支持 TLSv1.2：

   ```
   security config show -supported-protocols
   ```

   有关完整的命令语法，请参见手册页。

```
cluster1::> security config show
          Cluster                                                   Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       false      TLSv1.2, TLSv1.1, TLSv1 ALL:!LOW:         yes
                                             !aNULL:!EXP:
                                             !eNULL
```

3. 启用集群范围 FIPS 兼容模式：

   `security config modify -is-fips-enabled true -interface SSL`

   有关完整的命令语法，请参见手册页。

4. 手动重新启动集群节点。
5. 验证是否已启用集群范围 FIPS 兼容模式：

   `security config show`

```
cluster1::> security config show
          Cluster                                                   Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       true       TLSv1.2, TLSv1.1        ALL:!LOW:         yes
                                             !aNULL:!EXP:
                                             !eNULL:!RC4
```

管理 NetApp 加密

取消卷数据加密

您可以使用 `volume move start` 用于移动和取消加密卷数据的命令。

开始之前

您必须是集群管理员才能执行此任务。或者、您也可以是集群管理员已向其委派权限的SVM管理员。有关详细信息，请参见 "委派运行 volume move 命令的权限"。

步骤

1. 移动现有加密卷并取消对卷上的数据加密：

   `volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false`

   有关完整的命令语法，请参见命令手册页。

   以下命令将移动名为的现有卷 `vol1` 目标聚合 `aggr3` 并对卷上的数据取消加密：

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3 -encrypt-destination false
   ```

   系统将删除卷的加密密钥。卷上的数据未加密。

2. 验证卷是否已禁用加密：

   `volume show -encryption`

   有关完整的命令语法，请参见命令手册页。

   以下命令将显示卷是否位于上 `cluster1` 已加密：

   ```
   cluster1::> volume show -encryption

   Vserver  Volume   Aggregate   State    Encryption State
   -------  ------   ---------   -----    ----------------
   vs1      vol1     aggr1       online   none
   ```

移动加密卷

您可以使用 `volume move start` 命令以移动加密卷。移动的卷可以位于同一聚合或不同聚合上。

关于此任务

如果目标节点或目标卷不支持卷加密，则移动操作将失败。

。 `-encrypt-destination` 选项 `volume move start` 对于加密卷、默认为true。指定您不希望对目标卷进行加密的要求可确保您不会无意中对卷上的数据取消加密。

开始之前

您必须是集群管理员才能执行此任务。或者、您也可以是集群管理员已向其委派权限的SVM管理员。有关详细信息，请参见 "委派运行卷移动命令的权限"。

步骤

1. 移动现有加密卷并保持卷上的数据处于加密状态：

`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name`

有关完整的命令语法，请参见命令手册页。

以下命令将移动名为的现有卷 `vol1` 目标聚合 `aggr3` 并保持卷上的数据处于加密状态：

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr3
```

2. 验证卷是否已启用加密：

   `volume show -is-encrypted true`

   有关完整的命令语法，请参见命令手册页。

   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    aggr3     online    RW  200GB    160.0GB  20%
```

委派运行 volume move 命令的权限

您可以使用 `volume move` 用于对现有卷进行加密、移动加密卷或取消卷加密的命令。集群管理员可以运行 `volume move` 命令本身、也可以将运行命令的权限委派给SVM管理员。

关于此任务

默认情况下、系统会为SVM管理员分配 `vsadmin` 角色、不包括移动卷的权限。您必须分配 `vsadmin-volume` SVM管理员的角色、以使其能够运行 `volume move` 命令：

步骤

1. 委派运行的权限 `volume move` 命令：

   `security login modify -vserver SVM_name -user-or-group-name user_or_group_name -application application -authmethod authentication_method -role vsadmin-volume`

   有关完整的命令语法，请参见命令手册页。

   以下命令授予SVM管理员运行的权限 `volume move` 命令：

```
cluster1::>security login modify -vserver engData -user-or-group-name
SVM-admin -application ssh -authmethod domain -role vsadmin-volume
```

使用 volume encryption rekey start 命令更改卷的加密密钥

安全最佳做法是定期更改卷的加密密钥。从ONTAP 9.3开始、您可以使用 `volume encryption rekey start` 命令以更改加密密钥。

关于此任务

启动重新设置密钥操作后，该操作必须完成。不会返回到旧密钥。如果您在操作期间遇到性能问题描述、则可以运行 `volume encryption rekey pause` 命令以暂停操作、以及 `volume encryption rekey resume` 命令以恢复操作。

在重新设置密钥操作完成之前，卷将具有两个密钥。新写入及其相应读取将使用新密钥。否则，读取将使用旧密钥。

> 您不能使用 `volume encryption rekey start` 重新设置SnapLock卷密钥。

步骤

1. 更改加密密钥：

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

   以下命令将更改的加密密钥 `vol1` 在SVM上`vs1`：

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

2. 验证重新设置密钥操作的状态：

   `volume encryption rekey show`

   有关完整的命令语法，请参见命令手册页。

   以下命令显示重新设置密钥操作的状态：

   ```
   cluster1::> volume encryption rekey show

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

3. 重新设置密钥操作完成后，验证卷是否已启用加密：

   `volume show -is-encrypted true`

有关完整的命令语法，请参见命令手册页。

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%
```

使用 **volume move start** 命令更改卷的加密密钥

安全最佳做法是定期更改卷的加密密钥。您可以使用 `volume move start` 命令以更改加密密钥。您必须使用 `volume move start` 在ONTAP 9.2及更早版本中。移动的卷可以位于同一聚合或不同聚合上。

关于此任务

您不能使用 `volume move start` 重新设置SnapLock或FlexGroup卷的密钥。

开始之前

您必须是集群管理员才能执行此任务。或者、您也可以是集群管理员已向其委派权限的SVM管理员。有关详细信息，请参见 "委派运行卷移动命令的权限"。

步骤

1. 移动现有卷并更改加密密钥：

   `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-generate-destination-key true`

   有关完整的命令语法，请参见命令手册页。

   以下命令将移动名为的现有卷 **`vol1`** 目标聚合 **`aggr2`** 并更改加密密钥：

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

   此时将为此卷创建一个新的加密密钥。卷上的数据将保持加密状态。

2. 验证卷是否已启用加密：

   `volume show -is-encrypted true`

   有关完整的命令语法，请参见命令手册页。

   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%
```

轮换 NetApp 存储加密的身份验证密钥

使用 NetApp 存储加密（NetApp Storage Encryption， NSE）时，您可以轮换身份验证密钥。

关于此任务

如果您使用的是外部密钥管理器（KMIP），则支持在 NSE 环境中轮换身份验证密钥。

> 板载密钥管理器（OKM）不支持在 NSE 环境中轮换身份验证密钥。

步骤

1. 使用 `security key-manager create-key` 命令生成新的身份验证密钥。

   您需要先生成新的身份验证密钥，然后才能更改身份验证密钥。

2. 使用 `storage encryption disk modify -disk * -data-key-id` 命令以更改身份验证密钥。

删除加密卷

您可以使用 `volume delete` 命令以删除加密卷。

开始之前

- 您必须是集群管理员才能执行此任务。或者、您也可以是集群管理员已向其委派权限的SVM管理员。有关详细信息，请参见 "委派运行卷移动命令的权限"。
- 卷必须处于脱机状态。

步骤

1. 删除加密卷：

   `volume delete -vserver` *`SVM_name`* `-volume` *`volume_name`*

   有关完整的命令语法，请参见命令手册页。

   以下命令将删除名为的加密卷 `vol1`：

   ```
   cluster1::> volume delete -vserver vs1 -volume vol1
   ```

   输入 ... `yes` 系统提示您确认删除时。

系统将在 24 小时后删除卷的加密密钥。

使用 ... `volume delete` 使用 `-force true` 可选择立即删除卷并销毁相应的加密密钥。此命令需要高级权限。有关详细信息，请参见手册页。

完成后

您可以使用 `volume recovery-queue` 命令以在发出后的保留期限内恢复已删除的卷 `volume delete` 命令：

```
volume recovery-queue SVM_name -volume volume_name
```

"如何使用卷恢复功能"

安全地清除加密卷上的数据

安全清除加密卷上的数据概述

从 ONTAP 9.4 开始，您可以使用安全清除功能无中断擦洗启用了 NVE 的卷上的数据。擦除加密卷上的数据可确保无法从物理介质恢复数据，例如，在 " s占用， " 的情况下，覆盖块时可能会留下数据跟踪，或者用于安全删除空出租户的数据。

安全清除仅适用于启用了 NVE 的卷上先前删除的文件。您不能擦除未加密的卷。您必须使用 KMIP 服务器提供密钥，而不是板载密钥管理器。

使用安全清除的注意事项

- 在为NetApp聚合加密(NAE)启用的聚合中创建的卷不支持安全清除。
- 安全清除仅适用于启用了 NVE 的卷上先前删除的文件。
- 您不能擦除未加密的卷。
- 您必须使用 KMIP 服务器提供密钥，而不是板载密钥管理器。

安全清除功能因 ONTAP 版本而异。

ONTAP 9.8及更高版本

- MetroCluster 和 FlexGroup 支持安全清除。
- 如果要清除的卷是 SnapMirror 关系的源，则无需中断 SnapMirror 关系即可执行安全清除。
- 对于使用 SnapMirror 数据保护的卷，重新加密方法与不使用 SnapMirror 数据保护（ DP ）或使用 SnapMirror 扩展数据保护的卷不同。
  - 默认情况下，使用 SnapMirror 数据保护（ DP ）模式的卷使用卷移动重新加密方法重新加密数据。
  - 默认情况下，未使用 SnapMirror 数据保护的卷或使用 SnapMirror 扩展数据保护（ XDP ）模式的卷使用原位重新加密方法。
  - 可以使用更改这些默认值 `secure purge re-encryption-method [volume-move|in-place-rekey]` 命令：
- 默认情况下， FlexVol 卷中的所有 Snapshot 副本都会在安全清除操作期间自动删除。默认情况下，在安全清除操作期间，不会自动删除使用 SnapMirror 数据保护的 FlexGroup 卷和卷中的快照。可以使用更改这些默认值 `secure purge delete-all-snapshots [true|false]` 命令：

ONTAP 9.7及更早版本：

- 安全清除不支持以下内容：
  - FlexClone
  - SnapVault
  - FabricPool
- 如果要清除的卷是 SnapMirror 关系的源，则必须先断开 SnapMirror 关系，然后才能清除该卷。

  如果卷中的 Snapshot 副本繁忙，则必须先释放 Snapshot 副本，然后才能清除卷。例如，您可能需要将 FlexClone 卷从其父卷拆分。
- 成功调用安全清除功能将触发卷移动，以便使用新密钥重新加密其余未清除的数据。

  移动的卷将保留在当前聚合上。旧密钥会自动销毁，以确保已清除的数据无法从存储介质恢复。

安全地清除加密卷上的数据，而不存在 **SnapMirror** 关系

从 ONTAP 9.4 开始，您可以使用安全清除功能在启用了 NVE 的卷上无中断地生成 " `scrub` " 数据。

关于此任务

完成安全清除可能需要几分钟到数小时，具体取决于已删除文件中的数据量。您可以使用 `volume encryption secure-purge show` 命令以查看操作状态。您可以使用 `volume encryption secure-purge abort` 命令以终止操作。

> 要在 SAN 主机上执行安全清除，您必须删除包含要清除的文件的整个 LUN ，或者您必须能够在 LUN 中为属于要清除的文件的块打孔。如果无法删除 LUN ，或者主机操作系统不支持 LUN 中的打孔，则无法执行安全清除。

开始之前

- 您必须是集群管理员才能执行此任务。
- 此任务需要高级权限。

步骤

1. 删除要安全清除的文件或 LUN 。
   - 在 NAS 客户端上，删除要安全清除的文件。
   - 在 SAN 主机上，删除要安全清除的 LUN ，或者为要清除的文件中的块打孔。
2. 在存储系统上，更改为高级权限级别：

   ```
   set -privilege advanced
   ```

3. 如果要安全清除的文件位于快照中，请删除这些快照：

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

4. 安全清除已删除的文件：

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   ```

   以下命令可安全清除上已删除的文件 `vol1` 在SVM上`vs1`：

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

5. 验证安全清除操作的状态：

   ```
   volume encryption secure-purge show
   ```

使用异步 **SnapMirror** 关系安全地清除加密卷上的数据

从 ONTAP 9.8 开始，您可以使用安全清除功能在具有异步 SnapMirror 关系且已启用 NVE 的卷上无中断地传输 " `scrub` " 数据。

开始之前

- 您必须是集群管理员才能执行此任务。
- 此任务需要高级权限。

关于此任务

完成安全清除可能需要几分钟到数小时，具体取决于已删除文件中的数据量。您可以使用 `volume encryption secure-purge show` 命令以查看操作状态。您可以使用 `volume encryption secure-purge abort` 命令以终止操作。

> 要在 SAN 主机上执行安全清除，您必须删除包含要清除的文件的整个 LUN ，或者您必须能够在 LUN 中为属于要清除的文件的块打孔。如果无法删除 LUN ，或者主机操作系统不支持 LUN 中的打孔，则无法执行安全清除。

步骤

1. 在存储系统上、切换到高级权限级别：

   ```
   set -privilege advanced
   ```

2. 删除要安全清除的文件或 LUN 。
   - 在 NAS 客户端上，删除要安全清除的文件。
   - 在 SAN 主机上，删除要安全清除的 LUN ，或者为要清除的文件中的块打孔。

3. 准备异步关系中要安全清除的目标卷：

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   -prepare true
   ```

   对异步 SnapMirror 关系中的每个卷重复此步骤。

4. 如果要安全清除的文件位于 Snapshot 副本中，请删除 Snapshot 副本：

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

5. 如果要安全清除的文件位于基本 Snapshot 副本中，请执行以下操作：

   a. 在异步 SnapMirror 关系中的目标卷上创建 Snapshot 副本：

      ```
      volume snapshot create -snapshot snapshot_name -vserver SVM_name -volume
      volume_name
      ```

   b. 更新 SnapMirror 以将基本 Snapshot 副本向前移动：

      ```
      snapmirror update -source-snapshot snapshot_name -destination-path
      destination_path
      ```

   对异步 SnapMirror 关系中的每个卷重复此步骤。

   a. 重复步骤（a）和（b），使其等于基本 Snapshot 副本数加 1 。

      例如，如果您有两个基本 Snapshot 副本，则应重复步骤（a）和（b）三次。

   b. 验证是否存在基本Snapshot副本：

      ```
      snapshot show -vserver SVM_name -volume volume_name
      ```

   c. 删除基本Snapshot副本：

      ```
      snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot
      ```

6. 安全清除已删除的文件：

```
volume encryption secure-purge start -vserver svm_name -volume volume_name
```

对异步 SnapMirror 关系中的每个卷重复此步骤。

以下命令可安全清除 SVM "`vs1` " 上 "`vol1` " 上的已删除文件：

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume
vol1
```

7. 验证安全清除操作的状态：

```
volume encryption secure-purge show
```

擦除具有同步 **SnapMirror** 关系的加密卷上的数据

从ONTAP 9.8开始、您可以使用安全清除功能无故障"擦除"启用了NVE且具有同步SnapMirror关系的卷上的数据。

关于此任务

安全清除可能需要几分钟到几小时才能完成，具体取决于已删除文件中的数据量。您可以使用 `volume encryption secure-purge show` 命令以查看操作状态。您可以使用 `volume encryption secure-purge abort` 命令以终止操作。

> 要在 SAN 主机上执行安全清除，您必须删除包含要清除的文件的整个 LUN ，或者您必须能够在 LUN 中为属于要清除的文件的块打孔。如果无法删除 LUN ，或者主机操作系统不支持 LUN 中的打孔，则无法执行安全清除。

开始之前

- 您必须是集群管理员才能执行此任务。
- 此任务需要高级权限。

步骤

1. 在存储系统上，更改为高级权限级别：

```
set -privilege advanced
```

2. 删除要安全清除的文件或 LUN 。
   - 在 NAS 客户端上，删除要安全清除的文件。
   - 在 SAN 主机上，删除要安全清除的 LUN ，或者为要清除的文件中的块打孔。
3. 准备异步关系中要安全清除的目标卷：

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name
-prepare true
```

对同步 SnapMirror 关系中的另一个卷重复此步骤。

4. 如果要安全清除的文件位于 Snapshot 副本中，请删除 Snapshot 副本：

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot snapshot
   ```

5. 如果安全清除文件位于基本 Snapshot 副本或通用 Snapshot 副本中，请更新 SnapMirror 以将通用 Snapshot 副本前移：

   ```
   snapmirror update -source-snapshot snapshot_name -destination-path
   destination_path
   ```

   有两个通用 Snapshot 副本，因此必须发出此命令两次。

6. 如果安全清除文件位于应用程序一致的 Snapshot 副本中，请删除同步 SnapMirror 关系中两个卷上的 Snapshot 副本：

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot snapshot
   ```

   对两个卷执行此步骤。

7. 安全清除已删除的文件：

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   ```

   对同步 SnapMirror 关系中的每个卷重复此步骤。

   以下命令可安全清除 SMV"`vs1` " 上 "`vol1` " 上已删除的文件。

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

8. 验证安全清除操作的状态：

   ```
   volume encryption secure-purge show
   ```

更改板载密钥管理密码短语

安全最佳做法是定期更改板载密钥管理密码短语。您应将新的板载密钥管理密码短语复制到存储系统以外的安全位置，以供将来使用。

开始之前

- 要执行此任务，您必须是集群或 SVM 管理员。
- 此任务需要高级权限。

步骤

1. 更改为高级权限级别：

   ```
   set -privilege advanced
   ```

2. 更改板载密钥管理密码短语：

对于此 ONTAP 版本 …	使用此命令 …
ONTAP 9.6 及更高版本	`security key-manager onboard update-passphrase`
ONTAP 9.5 及更早版本	`security key-manager update-passphrase`

有关完整的命令语法，请参见手册页。

以下ONTAP 9.6命令可用于更改的板载密钥管理密码短语 `cluster1`：

```
cluster1::> security key-manager onboard update-passphrase
Warning: This command will reconfigure the cluster passphrase for
onboard key management for Vserver "cluster1".
Do you want to continue? {y|n}: y
Enter current passphrase:
Enter new passphrase:
```

3. 输入 … `y` 在提示更改板载密钥管理密码短语时。
4. 在当前密码短语提示符处输入当前密码短语。
5. 在新的密码短语提示符处，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。

6. 在密码短语确认提示符处，重新输入密码短语。

完成后

在 MetroCluster 环境中，您必须更新配对集群上的密码短语：

- 在ONTAP 9.5及更早版本中、必须运行 `security key-manager update-passphrase` 在配对集群上使用相同密码短语。
- 在ONTAP 9.6及更高版本中、系统会提示您运行 `security key-manager onboard sync` 在配对集群上使用相同密码短语。

您应将板载密钥管理密码短语复制到存储系统以外的安全位置，以供将来使用。

更改板载密钥管理密码短语时，您应手动备份密钥管理信息。

"手动备份板载密钥管理信息"

手动备份板载密钥管理信息

配置板载密钥管理器密码短语时，应将板载密钥管理信息复制到存储系统外的安全位置。

您需要的内容

- 您必须是集群管理员才能执行此任务。
- 此任务需要高级权限。

关于此任务

所有密钥管理信息都会自动备份到集群的复制数据库（RDB）。您还应手动备份密钥管理信息，以便在发生灾难时使用。

步骤

1. 更改为高级权限级别：

   ```
   set -privilege advanced
   ```

2. 显示集群的密钥管理备份信息：

对于此 ONTAP 版本 …	使用此命令 …
ONTAP 9.6 及更高版本	`security key-manager onboard show-backup`
ONTAP 9.5 及更早版本	`security key-manager backup show`

有关完整的命令语法，请参见手册页。

+
以下9.6命令显示的密钥管理备份信息 `cluster1`：

+

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

     --------------------------BEGIN BACKUP--------------------------
     TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
     QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
     dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
     3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
     IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
     QRHwv+1aWvAAAAAAAAAAACQAAAAAAAAAgAAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
     BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
     AQAAAAMAAAAYAQAAAAAAADA5/ccAAAAAIgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAA
     AAAAAAAAAAACAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAACIAAAAAAAAA
     KAAAAAAAAACI8z/bAAAAAAAAAAAAAAAAAgAAAAAAAAQAbxMcI4qiaMS4Uts5tTUnU
     AAAAAAAAAAAkAAAAAAAAAAIAAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5Smyj
     LSgoK/qc8FAmMMcrRXY6uriulnL0WPB/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAwAAABgBAAAAAAAA
     1cNLLwAAAAAiAAAAAAAAACgAAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAIAAAAAAAAkA
     ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAAIgAAAAAAAAAoAAAAAAAAAAJ4/cQsAAAAA
     AAAAAAAAAAACAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAAAACQAAAAAAAAA
     gAAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rrH4nPQM0n
     rDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     ---------------------------END BACKUP---------------------------
```

1. 将备份信息复制到存储系统以外的安全位置，以便在发生灾难时使用。

还原板载密钥管理加密密钥

根据您的ONTAP版本、您还原板载密钥管理加密密钥所遵循的操作步骤会有所不同。

开始之前

- 如果将 NSE 与外部密钥管理（KMIP）服务器结合使用，则必须已删除外部密钥管理器数据库。有关详细信息，请参见 "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。

> 如果在具有Flash Cache模块的系统上使用NSE、则还应启用NVE或NAE。NSE不会对驻留在Flash Cache模块上的数据进行加密。

具有加密根卷的**ONTAP 9.8**及更高版本

> 如果您运行的是ONTAP 9.8或更高版本、并且根卷未加密、请遵循适用于ONTAP 9.6或更高版本的操作步骤。

如果您运行的是 ONTAP 9.8 及更高版本，并且根卷已加密，则必须在启动菜单中设置板载密钥管理恢复密码短语。如果要更换启动介质、也需要执行此过程。

1. 将节点启动至启动菜单、然后选择选项 `(10) Set onboard key management recovery secrets`。
2. 输入 … `y` 以使用此选项。
3. 在提示符处，输入集群的板载密钥管理密码短语。
4. 在提示符处，输入备份密钥数据。

   节点将返回到启动菜单。

5. 从启动菜单中、选择选项 `(1) Normal Boot`。

ONTAP 9.6 及更高版本

1. 验证是否需要还原密钥：+
   `security key-manager key query -node` *`node`*
2. 还原密钥：+
   `security key-manager onboard sync`

   有关完整的命令语法，请参见手册页。

   以下 ONTAP 9.6 命令可同步板载密钥层次结构中的密钥：

   ```
   cluster1::> security key-manager onboard sync

   Enter the cluster-wide passphrase for onboard key management in Vserver
   "cluster1"::    <32..256 ASCII characters long text>
   ```

3. 在密码短语提示符处，输入集群的板载密钥管理密码短语。

ONTAP 9.5 及更早版本

1. 验证是否需要还原密钥：+
   `security key-manager key show`
2. 如果您运行的是 ONTAP 9.8 及更高版本，并且根卷已加密，请完成以下步骤：

   如果您运行的是 ONTAP 9.6 或 9.7 ，或者运行的是 ONTAP 9.8 或更高版本，并且根卷未加密，请跳过此步骤。

3. 还原密钥：+
   `security key-manager setup -node node`

   有关完整的命令语法，请参见手册页。

4. 在密码短语提示符处，输入集群的板载密钥管理密码短语。

还原外部密钥管理加密密钥

您可以手动还原外部密钥管理加密密钥并将其推送到其他节点。如果要重新启动在为集群创建密钥时临时关闭的节点，则可能需要执行此操作。

关于此任务

在ONTAP 9.6及更高版本中、您可以使用 `security key-manager key query -node node_name` 命令以验证是否需要还原密钥。

在ONTAP 9.5及更早版本中、您可以使用 `security key-manager key show` 命令以验证是否需要还原密钥。

> 如果在具有Flash Cache模块的系统上使用NSE、则还应启用NVE或NAE。NSE不会对驻留在Flash Cache模块上的数据进行加密。

开始之前

要执行此任务，您必须是集群或 SVM 管理员。

步骤

1. 如果您运行的是 ONTAP 9.8 或更高版本，并且根卷已加密，请执行以下操作：

   如果您运行的是 ONTAP 9.7 或更早版本，或者运行的是 ONTAP 9.8 或更高版本，并且根卷未加密，请跳过此步骤。

   a. 设置Bootargs：

      ```
      setenv kmip.init.ipaddr <ip-address>

      setenv kmip.init.netmask <netmask>

      setenv kmip.init.gateway <gateway>

      setenv kmip.init.interface e0M

      boot_ontap
      ```

   b. 将节点启动至启动菜单、然后选择选项 `(11) Configure node for external key management`。

   c. 按照提示输入管理证书。

      输入所有管理证书信息后，系统将返回到启动菜单。

   d. 从启动菜单中、选择选项 `(1) Normal Boot`。

2. 还原密钥：

对于此 ONTAP 版本 …	使用此命令 …
ONTAP 9.6 及更高版本	`security key-manager external restore -vserver SVM -node node -key-server host_name
IP_address:port -key-id key_id -key -tag key_tag`	ONTAP 9.5 及更早版本

> node 默认为所有节点。有关完整的命令语法，请参见手册页。启用板载密钥管理后，不支持此命令。

以下ONTAP 9.6命令可将外部密钥管理身份验证密钥还原到中的所有节点 `cluster1`：

```
clusterl::> security key-manager external restore
```

替换 SSL 证书

所有 SSL 证书都具有到期日期。您必须在证书到期之前对其进行更新，以防止对身份验证密钥的访问丢失。

开始之前

- 您必须已获取集群的替代公有证书和专用密钥（ KMIP 客户端证书）。
- 您必须已获取 KMIP 服务器的替代公有证书（ KMIP server-ca 证书）。
- 要执行此任务，您必须是集群或 SVM 管理员。
- 在MetroCluster 环境中、必须替换两个集群上的KMIP SSL证书。

> 在集群上安装证书之前或之后，您可以在 KMIP 服务器上安装替代客户端和服务器证书。

步骤

1. 安装新的 KMIP server-ca 证书：

   ```
   security certificate install -type server-ca -vserver <>
   ```

2. 安装新的 KMIP 客户端证书：

   ```
   security certificate install -type client -vserver <>
   ```

3. 更新密钥管理器配置以使用新安装的证书：

   ```
   security key-manager external modify -vserver <> -client-cert <> -server-ca
   -certs <>
   ```

   如果您在MetroCluster 环境中运行ONTAP 9.6或更高版本、并且要修改管理SVM上的密钥管理器配置、则必须在配置中的两个集群上运行命令。

> 如果新客户端证书的公共 / 专用密钥与先前安装的密钥不同，则更新密钥管理器配置以使用新安装的证书将返回错误。请参见知识库文章 "新的客户端证书公有 或专用密钥与现有客户端证书不同" 有关如何覆盖此错误的说明。

更换 FIPS 驱动器或 SED

您可以像替换普通磁盘一样更换 FIPS 驱动器或 SED 。确保为替代驱动器分配新的数据身份验证密钥。对于 FIPS 驱动器，您可能还需要分配新的 FIPS 140-2 身份验证密钥。

> HA 对使用时 "加密 SAS 或 NVMe 驱动器（ SED ， NSE ， FIPS ）"，您必须按照主题中的说明进行操作 "将 FIPS 驱动器或 SED 恢复到未受保护的模式" 初始化系统之前 HA 对中的所有驱动器（启动选项 4 或 9 ）。如果不这样做，则在重新利用驱动器时，可能会导致未来数据丢失。

开始之前

- 您必须知道驱动器使用的身份验证密钥的密钥 ID 。
- 您必须是集群管理员才能执行此任务。

步骤

1. 确保磁盘已标记为故障：

   ```
   storage disk show -broken
   ```

   有关完整的命令语法，请参见手册页。

   ```
   cluster1::> storage disk show -broken
   Original Owner: cluster1-01
     Checksum Compatibility: block
                                                                    Usable
   Physical
       Disk    Outage Reason HA Shelf Bay Chan    Pool  Type     RPM      Size
   Size
       ------ ---- ------------ ---- --- ---- ------ -----   -----   -------
   -------
       0.0.0   admin   failed   0b    1   0    A   Pool0   FCAL   10000   132.8GB
   133.9GB
       0.0.7   admin   removed 0b    2   6    A   Pool1   FCAL   10000   132.8GB
   134.2GB
   [...]
   ```

2. 按照适用于您的磁盘架型号的硬件指南中的说明，删除故障磁盘并将其更换为新的 FIPS 驱动器或 SED 。
3. 分配新更换磁盘的所有权：

   ```
   storage disk assign -disk disk_name -owner node
   ```

   有关完整的命令语法，请参见手册页。

```
cluster1::> storage disk assign -disk 2.1.1 -owner cluster1-01
```

4. 确认已分配新磁盘：

   `storage encryption disk show`

   有关完整的命令语法，请参见手册页。

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
--------------------------------------------------------------------
0.0.0   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
0.0.1   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
1.10.0  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
1.10.1  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
2.1.1   open 0x0
[...]
```

5. 将数据身份验证密钥分配给 FIPS 驱动器或 SED 。

   "将数据身份验证密钥分配给 FIPS 驱动器或 SED （外部密钥管理）"

6. 如有必要，请为 FIPS 驱动器分配 FIPS 140-2 身份验证密钥。

   "将 FIPS 140-2 身份验证密钥分配给 FIPS 驱动器"

使 FIPS 驱动器或 SED 上的数据无法访问

使 FIPS 驱动器或 SED 上的数据无法访问概述

如果要使 FIPS 驱动器或 SED 上的数据永久不可访问，但要为新数据保留驱动器的未用空间，则可以对磁盘进行清理。如果要使数据永久不可访问且无需重复使用驱动器，可以将其销毁。

- 磁盘清理

  清理自加密驱动器时，系统会将磁盘加密密钥更改为新的随机值，将开机锁定状态重置为 false ，并将密钥 ID 设置为默认值，即制造商安全 ID 0x0 （ SAS 驱动器）或空密钥（ NVMe 驱动器）。这样做会使磁盘上的数据无法访问且无法检索。您可以将已清理的磁盘重复用作未置零的备用磁盘。

- 磁盘销毁

销毁 FIPS 驱动器或 SED 后，系统会将磁盘加密密钥设置为未知的随机值，并永久锁定磁盘。这样做会使磁盘永久不可用，并且磁盘上的数据永久不可访问。

您可以清理或销毁节点的单个自加密驱动器或所有自加密驱动器。

清理 **FIPS** 驱动器或 **SED**

如果要使FIPS驱动器或SED上的数据永久不可访问、并使用该驱动器存储新数据、则可以使用 `storage encryption disk sanitize` 命令以对驱动器进行磁盘管理。

关于此任务

清理自加密驱动器时，系统会将磁盘加密密钥更改为新的随机值，将开机锁定状态重置为 false ，并将密钥 ID 设置为默认值，即制造商安全 ID 0x0 （ SAS 驱动器）或空密钥（ NVMe 驱动器）。这样做会使磁盘上的数据无法访问且无法检索。您可以将已清理的磁盘重复用作未置零的备用磁盘。

开始之前

您必须是集群管理员才能执行此任务。

步骤

1. 将需要保留的所有数据迁移到另一个磁盘上的聚合。
2. 删除要清理的 FIPS 驱动器或 SED 上的聚合：

   `storage aggregate delete -aggregate` *`aggregate_name`*

   有关完整的命令语法，请参见手册页。

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

3. 确定要清理的 FIPS 驱动器或 SED 的磁盘 ID ：

   `storage encryption disk show -fields data-key-id,fips-key-id,owner`

   有关完整的命令语法，请参见手册页。

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   --------------------------------------------------------------------
   0.0.0   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   1.10.2  data
   F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
   [...]
   ```

4. 如果 FIPS 驱动器以 FIPS 兼容模式运行，请将节点的 FIPS 身份验证密钥 ID 设置回默认 MSID 0x0：

   `storage encryption disk modify -disk disk_id -fips-key-id 0x0`

   您可以使用 `security key-manager query` 用于查看密钥ID的命令。

```
cluster1::> storage encryption disk modify -disk 1.10.2 -fips-key-id 0x0

Info: Starting modify on 1 disk.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

5. 清理驱动器：

   `storage encryption disk sanitize -disk disk_id`

   您只能使用此命令清理热备用磁盘或损坏的磁盘。要清理所有磁盘、而不管其类型如何、请使用 `-force -all-state` 选项有关完整的命令语法，请参见手册页。

   ONTAP将提示您输入确认短语、然后再继续。输入屏幕上所示的短语。

```
cluster1::> storage encryption disk sanitize -disk 1.10.2

Warning: This operation will cryptographically sanitize 1 spare or
broken self-encrypting disk on 1 node.
         To continue, enter sanitize disk: sanitize disk

Info: Starting sanitize on 1 disk.
      View the status of the operation using the
      storage encryption disk show-status command.
```

销毁 **FIPS** 驱动器或 **SED**

如果要使FIPS驱动器或SED上的数据永久不可访问、并且不需要重复使用该驱动器、则可以使用 `storage encryption disk destroy` 命令销毁磁盘。

关于此任务

销毁 FIPS 驱动器或 SED 后，系统会将磁盘加密密钥设置为未知的随机值，并永久锁定该驱动器。这样做会使磁盘几乎不可用，并且磁盘上的数据永远不可访问。但是，您可以使用磁盘标签上印有的物理安全 ID （ PSID ）将磁盘重置为出厂配置的设置。有关详细信息，请参见 "丢失身份验证密钥后，使 FIPS 驱动器或 SED 恢复正常运行"。

除非您拥有不可退回的磁盘加载服务（ NRD Plus ），否则不应销毁 FIPS 驱动器或 SED 。销毁磁盘将使其保修失效。

开始之前

您必须是集群管理员才能执行此任务。

步骤

1. 将需要保留的所有数据迁移到另一个磁盘上的聚合。
2. 删除要销毁的 FIPS 驱动器或 SED 上的聚合：

   ```
   storage aggregate delete -aggregate aggregate_name
   ```

   有关完整的命令语法，请参见手册页。

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

3. 确定要销毁的 FIPS 驱动器或 SED 的磁盘 ID：

   ```
   storage encryption disk show
   ```

   有关完整的命令语法，请参见手册页。

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   --------------------------------------------------------------
   0.0.0   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   1.10.2  data
   F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
   [...]
   ```

4. 销毁磁盘：

   ```
   storage encryption disk destroy -disk disk_id
   ```

   有关完整的命令语法，请参见手册页。

   > 系统将提示您输入确认短语，然后再继续。输入屏幕上所示的短语。

```
cluster1::> storage encryption disk destroy -disk 1.10.2

Warning: This operation will cryptographically destroy 1 spare or broken
         self-encrypting disks on 1 node.
         You cannot reuse destroyed disks unless you revert
         them to their original state using the PSID value.
         To continue, enter
          destroy disk
         :destroy disk

Info: Starting destroy on 1 disk.
      View the status of the operation by using the
      "storage encryption disk show-status" command.
```

紧急粉碎**FIPS**驱动器或**SED**上的数据

在发生安全紧急情况时，您可以立即阻止访问 FIPS 驱动器或 SED ，即使存储系统或 KMIP 服务器没有电源也是如此。

开始之前

- 如果您使用的 KMIP 服务器没有电源，则必须为 KMIP 服务器配置一个易于销毁的身份验证项（例如，智能卡或 USB 驱动器）。
- 您必须是集群管理员才能执行此任务。

步骤

1. 对 FIPS 驱动器或 SED 上的数据执行紧急粉碎：

条件	那么 ...

存储系统已通电，您有时间使存储系统正常脱机	a. 如果存储系统配置为 HA 对，请禁用接管。
	b. 使所有聚合脱机并将其删除。
	c. 将权限级别设置为高级：
	`set -privilege advanced`
	d. 如果驱动器处于 FIPS 兼容模式，请将节点的 FIPS 身份验证密钥 ID 重新设置为默认 MSID：
	`storage encryption disk modify -disk * -fips-key-id 0x0`
	e. 暂停存储系统。
	f. 启动至维护模式：
	g. 清理或销毁磁盘：
	◦ 如果要使磁盘上的数据无法访问、并且仍然能够重复使用这些磁盘、请清理这些磁盘：
	`disk encrypt sanitize -all`
	◦ 如果要使磁盘上的数据无法访问、并且不需要保存磁盘、请销毁磁盘：
	`disk encrypt destroy disk_id1 disk_id2 …`
	ⓘ ◦ `disk encrypt sanitize` 和 `disk encrypt destroy` 命令仅保留用于维护模式。这些命令必须在每个 HA 节点上运行，并且不适用于损坏的磁盘。
	h. 对配对节点重复上述步骤。这会使存储系统处于永久禁用状态，并擦除所有数据。要再次使用系统，必须重新配置它。
		存储系统已通电，您必须立即粉碎数据

a. * 如果要使磁盘上的数据无法访问且仍能重复使用这些磁盘，请清理磁盘：*
b. 如果存储系统配置为 HA 对，请禁用接管。
c. 将权限级别设置为高级：
`set -privilege advanced`
d. 如果驱动器处于 FIPS 兼容模式，请将节点的 FIPS 身份验证密钥 ID 重新设置为默认 MSID：
`storage encryption disk modify -disk * -fips-key-id 0x0`
e. 清理磁盘：
`storage encryption disk sanitize -disk * -force-all-states true`
	a. * 如果要使磁盘上的数据无法访问，并且不需要保存磁盘，请销毁磁盘：*
	b. 如果存储系统配置为 HA 对，请禁用接管。
	c. 将权限级别设置为高级：
	`set -privilege advanced`
	d. 销毁磁盘：
	`storage encryption disk destroy -disk * -force-all-states true`
		存储系统崩溃，使系统处于永久禁用状态，并擦除所有数据。要再次使用系统，必须重新配置它。

KMIP 服务器可以通电，但存储系统不能通电	a. 登录到KMIP服务器。 b. 销毁与包含要阻止访问的数据的 FIPS 驱动器或 SED 关联的所有密钥。 这样会阻止存储系统访问磁盘加密密钥。	KMIP 服务器或存储系统不能通电

有关完整的命令语法，请参见手册页。

如果身份验证密钥丢失，请将 **FIPS** 驱动器或 **SED** 恢复使用

如果您永久丢失 FIPS 驱动器或 SED 的身份验证密钥，并且无法从 KMIP 服务器检索这些密钥，则系统会将其视为已损坏。虽然您无法访问或恢复磁盘上的数据，但可以采取措施使 SED 的未用空间再次可用于数据。

开始之前

您必须是集群管理员才能执行此任务。

关于此任务

只有在确定 FIPS 驱动器或 SED 的身份验证密钥永久丢失且无法恢复时，才应使用此过程。

如果磁盘已分区、则必须先取消分区、然后才能启动此过程。

> 取消磁盘分区的命令只能在diag级别使用、并且只能在NetApp支持监督下执行。强烈建议您在继续操作之前联系**NetApp**支持部门。您也可以参考知识库文章 "如何在ONTAP 中取消对备用驱动器的分区"。

步骤

1. 将 FIPS 驱动器或 SED 恢复正常运行：

SED 是否为 …	请执行以下步骤 …

不在 FIPS 兼容模式或 FIPS 兼容模式下，并且 FIPS 密钥可用	a. 将权限级别设置为高级：
	`set -privilege advanced`
	b. 将FIPS密钥重置为默认制造安全ID 0x0：
	`storage encryption disk modify -fips-key-id 0x0 -disk disk_id`
	c. 验证操作是否成功：
	`storage encryption disk show-status`
	如果操作失败、请使用本主题中的PSID过程。
	d. 对已损坏的磁盘进行分区：
	`storage encryption disk sanitize -disk disk_id`
	使用命令验证操作是否成功 `storage encryption disk show-status` 然后再继续下一步。
	e. 使已清除的磁盘恢复失败：
	`storage disk unfail -spare true -disk disk_id`
	f. 检查磁盘是否具有所有者：
	`storage disk show -disk disk_id`
	如果磁盘没有所有者、请分配一个。
	`storage disk assign -owner node -disk disk_id`
	i. 输入拥有要清理的磁盘的节点的 nodeshell ：
	`system node run -node node_name`
	运行 `disk sanitize release` 命令：
	g. 退出nokeshell。再次解除磁盘故障：
	`storage disk unfail -spare true -disk disk_id`
	h. 验证磁盘现在是否为备用磁盘并可在聚合中重复使用：
	`storage disk show -disk disk_id`

在 FIPS 兼容模式下，FIPS 密钥不可用， SED 的标签上印有 PSID	a. 从磁盘标签中获取磁盘的 PSID 。 b. 将权限级别设置为高级： `set -privilege advanced` c. 将磁盘重置为出厂配置设置： `storage encryption disk revert-to-original-state -disk` *`disk_id`* `-psid` *`disk_physical_secure_id`* 使用命令验证操作是否成功 `storage encryption disk show-status` 然后再继续下一步。 d. 如果您运行的是ONTAP 9.8P5或更早版本、请跳至下一步。如果您运行的是ONTAP 9.8p6或更高版本、请使已检查的磁盘恢复故障。 `storage disk unfail -disk` *`disk_id`* e. 检查磁盘是否具有所有者： `storage disk show -disk` *`disk_id`* 如果磁盘没有所有者、请分配一个。 `storage disk assign -owner node -disk` *`disk_id`* i. 输入拥有要清理的磁盘的节点的 nodeshell ： `system node run -node` *`node_name`* 运行 `disk sanitize release` 命令： f. 退出nokeshell。再次解除磁盘故障： `storage disk unfail -spare true -disk` *`disk_id`* g. 验证磁盘现在是否为备用磁盘并可在聚合中重复使用： `storage disk show -disk` *`disk_id`*

有关完整的命令语法，请参见 "命令参考"。

将 FIPS 驱动器或 SED 恢复到未受保护的模式

只有当节点的身份验证密钥 ID 设置为非默认值时， FIPS 驱动器或 SED 才会受到保护，防止未经授权的访问。您可以使用将FIPS驱动器或SED返回到未受保护的模式 `storage encryption disk modify` 命令将密钥ID设置为默认值。

如果 HA 对使用加密 SAS 或 NVMe 驱动器（ SED ， NSE ， FIPS ），则必须在初始化系统之前对 HA 对中的所有驱动器执行此过程（启动选项 4 或 9 ）。如果不这样做，则在重新利用驱动器时，可能会导致未来数据丢失。

开始之前

您必须是集群管理员才能执行此任务。

步骤

1. 将权限级别设置为高级：

```
set -privilege advanced
```

2. 如果 FIPS 驱动器以 FIPS 兼容模式运行，请将节点的 FIPS 身份验证密钥 ID 设置回默认 MSID 0x0：

   `storage encryption disk modify -disk disk_id -fips-key-id 0x0`

   您可以使用 `security key-manager query` 用于查看密钥ID的命令。

   ```
   cluster1::> storage encryption disk modify -disk 2.10.11 -fips-key-id
   0x0

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

   使用命令确认操作成功：

   `storage encryption disk show-status`

   重复show-status命令、直到"磁盘已开始"和"磁盘已完成"中的数字相同为止。

   ```
   cluster1:: storage encryption disk show-status

               FIPS    Latest   Start                Execution   Disks
   Disks Disks
   Node        Support Request  Timestamp            Time (sec)  Begun
   Done  Successful
   -------     ------- -------- ------------------   ---------- ------
   ------  ----------
   cluster1    true    modify   1/18/2022 15:29:38    3           14     5
   5
   1 entry was displayed.
   ```

3. 将节点的数据身份验证密钥 ID 重新设置为默认 MSID 0x0：

   `storage encryption disk modify -disk disk_id -data-key-id 0x0`

   的值 `-data-key-id` 无论您要将SAS或NVMe驱动器返回到未受保护的模式、都应设置为0x0。

   您可以使用 `security key-manager query` 用于查看密钥ID的命令。

```
cluster1::> storage encryption disk modify -disk 2.10.11 -data-key-id
0x0

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

使用命令确认操作成功：

```
storage encryption disk show-status
```

重复 show-status 命令，直到数字相同为止。如果"disks"(磁盘开始)和"disks Done (磁盘完成)"中的数字相同、则操作完成。

维护模式

从ONTAP 9.7开始、您可以从维护模式重新为FIPS驱动器设置密钥。只有在无法使用上一节中的ONTAP 命令行界面说明时、才应使用维护模式。

步骤

1. 将节点的FIPS身份验证密钥ID重新设置为默认MSID 0x0：

   ```
   disk encrypt rekey_fips 0x0 disklist
   ```

2. 将节点的数据身份验证密钥 ID 重新设置为默认 MSID 0x0 ：

   ```
   disk encrypt rekey 0x0 disklist
   ```

3. 确认已成功重新设置FIPS身份验证密钥密钥：

   ```
   disk encrypt show_fips
   ```

4. 确认已使用成功重新设置数据身份验证密钥密钥：

   ```
   disk encrypt show
   ```

   您的输出可能会显示默认的MSID 0x0密钥ID或密钥服务器持有的64字符值。。 `Locked?` 字段是指数据锁定。

```
Disk       FIPS Key ID                 Locked?
---------- --------------------------- -------
0a.01.0    0x0                          Yes
```

删除外部密钥管理器连接

当您不再需要 KMIP 服务器时，可以将其从节点断开。例如，在过渡到卷加密时，您可能

会断开 KMIP 服务器的连接。

关于此任务

当您从 HA 对中的一个节点断开 KMIP 服务器的连接时，系统会自动断开此服务器与所有集群节点的连接。

> 如果您计划在断开 KMIP 服务器连接后继续使用外部密钥管理，请确保另一个 KMIP 服务器可用于提供身份验证密钥。

开始之前

要执行此任务，您必须是集群或 SVM 管理员。

步骤

1. 断开 KMIP 服务器与当前节点的连接：

对于此 ONTAP 版本 …	使用此命令 …
ONTAP 9.6 及更高版本	`security key-manager external remove-servers -vserver SVM -key -servers host_name
IP_address:port,…`	ONTAP 9.5 及更早版本

在MetroCluster 环境中、必须对管理SVM的两个集群重复这些命令。

有关完整的命令语法，请参见手册页。

以下ONTAP 9.6命令将禁用与两个外部密钥管理服务器的连接 `cluster1`，第一个名为 `ks1`，侦听默认端口5696，第二个端口IP地址为10.0.0.20，侦听端口24482：

```
clusterl::> security key-manager external remove-servers -vserver
cluster-1 -key-servers ks1,10.0.0.20:24482
```

修改外部密钥管理服务器属性

从ONTAP 9.6开始、您可以使用 `security key-manager external modify-server` 用于更改外部密钥管理服务器的I/O超时和用户名的命令。

开始之前

- 要执行此任务，您必须是集群或 SVM 管理员。
- 此任务需要高级权限。
- 在MetroCluster 环境中、必须对管理SVM的两个集群重复这些步骤。

步骤

1. 在存储系统上，更改为高级权限级别：

```
set -privilege advanced
```

2. 修改集群的外部密钥管理器服务器属性：

```
security key-manager external modify-server -vserver admin_SVM -key-server
host_name|IP_address:port,… -timeout 1…60 -username user_name
```

> 超时值以秒为单位。如果您修改了用户名，系统将提示您输入新密码。 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修改外部密钥管理器服务器属性。

以下命令会将的超时值更改为45秒 `cluster1` 侦听默认端口5696的外部密钥管理服务器：

```
cluster1::> security key-manager external modify-server -vserver
cluster1 -key-server ks1.local -timeout 45
```

3. 修改 SVM 的外部密钥管理器服务器属性（仅限 NVE ）：

```
security key-manager external modify-server -vserver SVM -key-server
host_name|IP_address:port,… -timeout 1…60 -username user_name
```

> 超时值以秒为单位。如果您修改了用户名，系统将提示您输入新密码。 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 管理员才能修改外部密钥管理器服务器属性。

以下命令将更改的用户名和密码 `svm1` 侦听默认端口5696的外部密钥管理服务器：

```
svml::> security key-manager external modify-server -vserver svm11 -key
-server ks1.local -username svm1user
Enter the password:
Reenter the password:
```

4. 对任何其他 SVM 重复最后一步。

从板载密钥管理过渡到外部密钥管理

如果要从板载密钥管理切换到外部密钥管理，则必须先删除板载密钥管理配置，然后才能启用外部密钥管理。

开始之前

- 对于基于硬件的加密，必须将所有 FIPS 驱动器或 SED 的数据密钥重置为默认值。

  "将 FIPS 驱动器或 SED 恢复到未受保护的模式"

- 对于基于软件的加密，您必须取消对所有卷的加密。

  "取消卷数据加密"

- 您必须是集群管理员才能执行此任务。

步骤

1. 删除集群的板载密钥管理配置：

对于此 ONTAP 版本 …	使用此命令 …
ONTAP 9.6 及更高版本	`security key-manager onboard disable -vserver SVM`
ONTAP 9.5 及更早版本	`security key-manager delete-key-database`

有关完整的命令语法，请参见 "ONTAP 手册页"。

从外部密钥管理过渡到板载密钥管理

如果要从外部密钥管理切换到板载密钥管理，则必须先删除外部密钥管理配置，然后才能启用板载密钥管理。

开始之前

- 对于基于硬件的加密，必须将所有 FIPS 驱动器或 SED 的数据密钥重置为默认值。

  "将 FIPS 驱动器或 SED 恢复到未受保护的模式"

- 您必须已删除所有外部密钥管理器连接。

  "删除外部密钥管理器连接"

- 您必须是集群管理员才能执行此任务。

操作步骤

过渡密钥管理的步骤取决于您使用的ONTAP版本。

ONTAP 9.6 及更高版本

1. 更改为高级权限级别：

   ```
   set -privilege advanced
   ```

2. 使用命令：

   ```
   security key-manager external disable -vserver admin_SVM
   ```

   在MetroCluster 环境中、必须对管理SVM的两个集群重复此命令。

ONTAP 9.5 及更早版本

使用命令：

```
security key-manager delete-kmip-config
```

启动过程中无法访问密钥管理服务器时会发生什么情况

如果为 NSE 配置的存储系统在启动过程中无法访问任何指定的密钥管理服务器，则 ONTAP 会采取某些预防措施来避免发生意外行为。

如果存储系统配置了 NSE ， SED 已重新设置密钥并锁定，并且 SED 已启动，则存储系统必须从密钥管理服务器检索所需的身份验证密钥，以便向 SED 进行身份验证，然后才能访问数据。

存储系统会尝试联系指定的密钥管理服务器，最长三小时。如果存储系统在该时间后无法访问其中任何一个，则启动过程将停止，存储系统将暂停。

如果存储系统成功联系任何指定的密钥管理服务器，则会尝试建立 SSL 连接，时间最长为 15 分钟。如果存储系统无法与任何指定的密钥管理服务器建立 SSL 连接，则启动过程将停止，存储系统将暂停。

当存储系统尝试联系并连接到密钥管理服务器时，它会在 CLI 中显示有关失败的联系尝试的详细信息。您可以随时按 Ctrl-C 中断联系尝试

作为一项安全措施， SED 仅允许有限数量的未授权访问尝试，之后，它们将禁用对现有数据的访问。如果存储系统无法联系任何指定的密钥管理服务器以获取正确的身份验证密钥，则只能尝试使用默认密钥进行身份验证，从而导致尝试失败并发生崩溃。如果存储系统配置为在发生崩溃时自动重新启动，则它将进入启动环路，从而导致 SED 上的身份验证尝试持续失败。

在这些情况下，暂停存储系统的设计是为了防止存储系统进入启动环路，并防止因连续失败身份验证尝试次数超过安全限制而永久锁定 SED 而可能导致意外数据丢失。锁定保护的限制和类型取决于 SED 的制造规格和类型：

SED类型	导致锁定的连续身份验证尝试失败次数	达到安全限制时的锁定保护类型
HDD	1024	永久。即使正确的身份验证密钥再次可用，数据也无法恢复。

X440_PHM2800MCTO 800 GB NSE SSD ，固件版本为 NA00 或 NA01	5.	临时。只有在磁盘重新启动之前，锁定才有效。
X577_PHM2800MCTO 800 GB NSE SSD、固件版本为NA00或NA01	5.	临时。只有在磁盘重新启动之前，锁定才有效。
具有更高固件版本的 X440_PHM2800MCTO 800 GB NSE SSD	1024	永久。即使正确的身份验证密钥再次可用，数据也无法恢复。
具有更高固件版本的 X567_PHM2800MCTO 800 GB NSE SSD	1024	永久。即使正确的身份验证密钥再次可用，数据也无法恢复。
所有其他 SSD 型号	1024	永久。即使正确的身份验证密钥再次可用，数据也无法恢复。

对于所有 SED 类型，成功的身份验证会将尝试次数重置为零。

如果您遇到存储系统因无法访问任何指定密钥管理服务器而暂停的情况，则必须先确定并更正通信失败的发生原因，然后再尝试继续启动存储系统。

默认情况下禁用加密

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。如有必要、您可以默认为整个集群禁用加密。

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。

步骤

1. 要在 ONTAP 9.7 或更高版本中默认对整个集群禁用加密，请运行以下命令：

   ```
   options -option-name encryption.data_at_rest_encryption.disable_by_default
   -option-value on
   ```