



管理 NetApp 加密 ONTAP 9

NetApp
September 12, 2024

目录

管理 NetApp 加密	1
取消卷数据加密	1
移动加密卷	1
委派运行 volume move 命令的权限	2
使用 volume encryption rekey start 命令更改卷的加密密钥	3
使用 volume move start 命令更改卷的加密密钥	4
轮换 NetApp 存储加密的身份验证密钥	5
删除加密卷	5
安全地清除加密卷上的数据	6
更改板载密钥管理密码短语	11
手动备份板载密钥管理信息	12
还原板载密钥管理加密密钥	14
还原外部密钥管理加密密钥	16
替换 SSL 证书	17
更换 FIPS 驱动器或 SED	18
使 FIPS 驱动器或 SED 上的数据无法访问	19
如果身份验证密钥丢失，请将 FIPS 驱动器或 SED 恢复使用	25
将 FIPS 驱动器或 SED 恢复到未受保护的模式	27
删除外部密钥管理器连接	29
修改外部密钥管理服务器属性	30
从板载密钥管理过渡到外部密钥管理	31
从外部密钥管理过渡到板载密钥管理	32
启动过程中无法访问密钥管理服务器时会发生什么情况	33
默认情况下禁用加密	34

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、您也可以是由集群管理员向其委派权限的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
```

安全清除具有**SnapMirror**异步关系的加密卷上的数据

从NVE.8开始、您可以对具有SnapMirror异步关系且已启用ONTAP 9的卷上无故障的“scrub”数据使用安全清除。

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。

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 SnapMirror 异步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 SnapMirror 异步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 SnapMirror 异步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SnapMirror异步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**SnapMirror**同步关系的加密卷上的数据

从NVE.8开始、您可以使用安全清除功能无故障"擦除"已启用ONTAP 9且具有SnapMirror同步关系的卷上的数据。

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SnapMirror同步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 SnapMirror 同步关系中两个卷上的 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 SnapMirror 同步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	<code>security key-manager onboard update-passphrase</code>
ONTAP 9.5 及更早版本	<code>security key-manager update-passphrase</code>

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	<code>security key-manager onboard show-backup</code>
ONTAP 9.5 及更早版本	<code>security key-manager backup show</code>

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
```

[illegible]

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。

ONTAP 9.6 及更高版本



如果您运行的是ONTAP 9.8或更高版本，并且根卷已加密，请按照中的过程进行操作 [\[ontap-9-8\]](#)。

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。

使用加密根卷的ONTAP 9.8或更高版本

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 9.5 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	<code>`security key-manager external restore -vserver SVM -node node -key-server host_name`</code>

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:

```
cluster1::> 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端证书。

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

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
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
1.10.0    data
F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
1.10.1    data
F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
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
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
1.10.2    data
F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
[...]
```

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.
```

6. 使已清除的磁盘恢复失败： `storage disk unfail -spare true -disk disk_id`

7. 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`

8. 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：

9. 退出 `nodeshell`。再次解除磁盘故障： `storage disk unfail -spare true -disk disk_id`

10. 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`

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
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
1.10.2    data
F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
[...]
```

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 ...
----	--------

<p>存储系统已通电，您有时间使存储系统正常脱机</p>	<ol style="list-style-type: none"> 如果存储系统配置为 HA 对，请禁用接管。 使所有聚合脱机并将其删除。 将权限级别设置为高级： <pre>set -privilege advanced</pre> 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： <pre>storage encryption disk modify -disk * -fips-key-id 0x0</pre> 暂停存储系统。 启动至维护模式： 清理或销毁磁盘： <ul style="list-style-type: none"> 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： <pre>disk encrypt sanitize -all</pre> 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： <pre>disk encrypt destroy disk_id1 disk_id2 ...</pre> <div data-bbox="699 1472 756 1528">  </div> <div data-bbox="818 1297 1016 1709"> <p>。 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。</p> </div> 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。	<p>存储系统已通电，您必须立即粉碎数据</p>
------------------------------	--	--------------------------

<p>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： *</p> <p>b. 如果存储系统配置为 HA 对，请禁用接管。</p> <p>c. 将权限级别设置为高级：</p> <pre>set -privilege advanced</pre> <p>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：</p> <pre>storage encryption disk modify -disk * -fips-key-id 0x0</pre> <p>e. 清理磁盘：</p> <pre>storage encryption disk sanitize -disk * -force-all-states true</pre>	<p>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： *</p> <p>b. 如果存储系统配置为 HA 对，请禁用接管。</p> <p>c. 将权限级别设置为高级：</p> <pre>set -privilege advanced</pre> <p>d. 销毁磁盘： storage encryption disk destroy -disk * -force -all-states true</p>	<p>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。</p>
<p>KMIP 服务器可以通电，但存储系统不能通电</p>	<p>a. 登录到KMIP服务器。</p> <p>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。 这会阻止存储系统访问磁盘加密密钥。</p>	<p>KMIP 服务器或存储系统不能通电</p>

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

<p>在 FIPS 兼容模式下，FIPS 密钥不可用，SED 的标签上印有 PSID</p>	<ol style="list-style-type: none"> a. 从磁盘标签中获取磁盘的 PSID。 b. 将权限级别设置为高级： <code>set -privilege advanced</code> c. 将磁盘重置为出厂配置设置： <code>storage encryption disk revert-to-original-state -disk <i>disk_id</i> -psid <i>disk_physical_secure_id</i></code> 使用命令验证操作是否成功 <code>storage encryption disk show-status</code> 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。 <code>storage disk unfail -disk <i>disk_id</i></code> e. 检查磁盘是否具有所有者： <code>storage disk show -disk <i>disk_id</i></code> 如果磁盘没有所有者、请分配一个。 <code>storage disk assign -owner node -disk <i>disk_id</i></code> i. 输入拥有要清理的磁盘的节点的 nodeshell： <code>system node run -node <i>node_name</i></code> 运行 <code>disk sanitize release</code> 命令： f. 退出 <code>nokeshell</code>。再次解除磁盘故障： <code>storage disk unfail -spare true -disk <i>disk_id</i></code> g. 验证磁盘现在是否为备用磁盘并可在聚合中重复使用： <code>storage disk show -disk <i>disk_id</i></code>
--	--

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	<code>`security key-manager external remove-servers -vserver SVM -key -servers host_name`</code>
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：

```
cluster1::> 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：

```
svm1::> 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	<code>security key-manager onboard disable -vserver SVM</code>
ONTAP 9.5 及更早版本	<code>security key-manager delete-key-database</code>

有关完整的命令语法，请参见 ["ONTAP 命令参考"](#)。

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
```

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

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

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

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

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

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

商标信息

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