配置基于 NetApp 硬件的加密

ONTAP 9

NetApp
January 09, 2026

This PDF was generated from https://docs.netapp.com/zh-cn/ontap/encryption-at-rest/support-storage-encryption-concept.html on January 09, 2026. Always check docs.netapp.com for the latest.

目录

配置基于 NetApp 硬件的加密 1
- 了解ONTAP基于硬件的加密 1
  - 了解 NetApp 基于硬件的加密 1
  - 支持的自加密驱动器类型 1
  - 何时使用外部密钥管理 1
  - 支持详细信息 2
  - 基于硬件的加密工作流 2
- 配置外部密钥管理 3
  - 了解如何配置ONTAP外部密钥管理 3
  - 在ONTAP集群上安装 SSL 证书 3
  - 在ONTAP 9.6 及更高版本中启用基于硬件的加密的外部密钥管理 4
  - 在ONTAP 9.5 及更早版本中启用基于硬件的加密的外部密钥管理 6
  - 在ONTAP中配置集群模式外部密钥服务器 8
  - 在 ONTAP 9.6 及更高版本中创建身份验证密钥 11
  - 在 ONTAP 9.5 及更早版本中创建身份验证密钥 13
  - 使用ONTAP外部密钥管理将数据身份验证密钥分配给 FIPS 驱动器或 SED 15
- 配置板载密钥管理 16
  - 在 ONTAP 9.6 及更高版本中启用板载密钥管理 16
  - 在 ONTAP 9.5 及更早版本中启用板载密钥管理 18
  - 使用ONTAP板载密钥管理将数据身份验证密钥分配给 FIPS 驱动器或 SED 20
- 将 FIPS 140-2 身份验证密钥分配给ONTAP FIPS 驱动器 21
- 在ONTAP中为KMIP服务器连接启用集群范围FIPS兼容模式 23

配置基于 NetApp 硬件的加密

了解ONTAP基于硬件的加密

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。

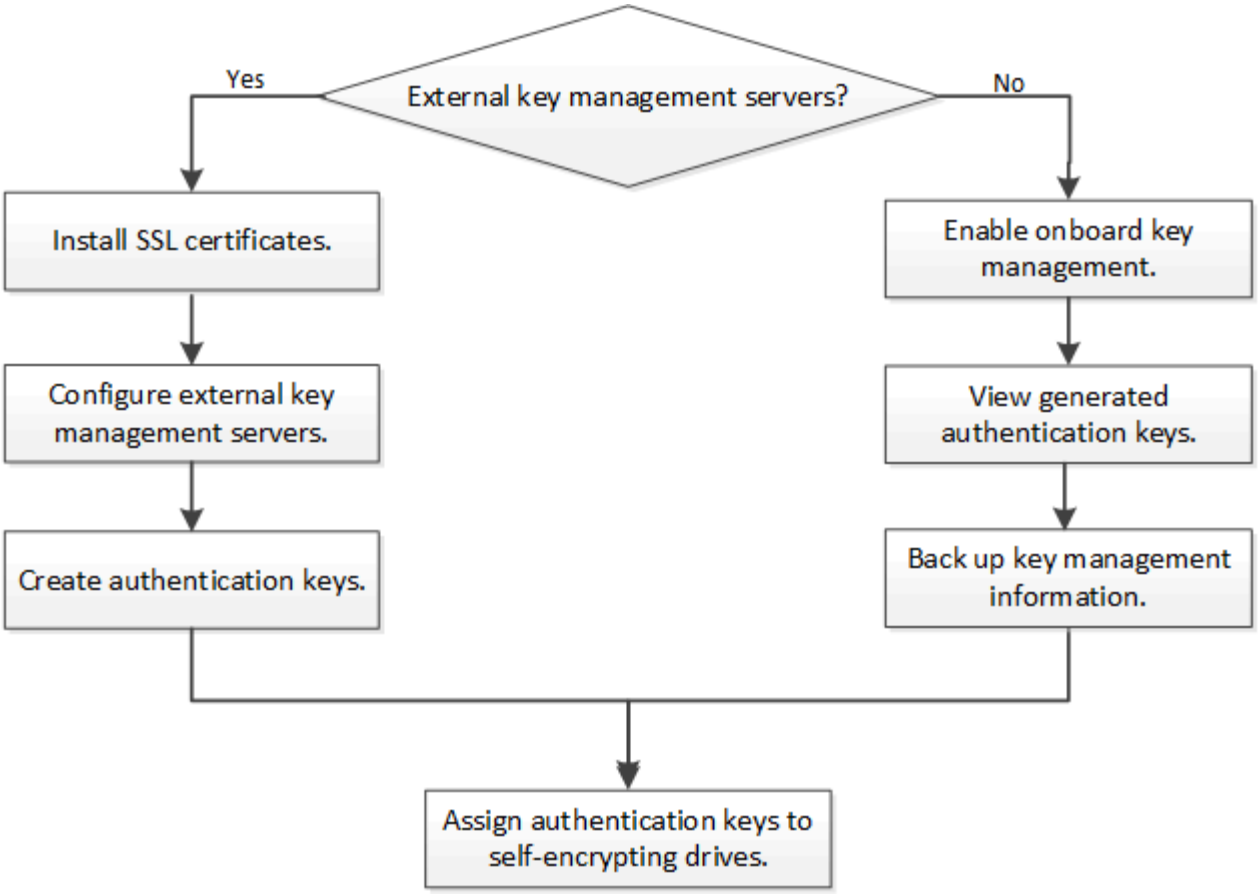
支持详细信息

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

了解如何配置ONTAP外部密钥管理

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。

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
   ```

相关信息

- "安全证书安装"

在ONTAP 9.6 及更高版本中启用基于硬件的加密的外部密钥管理

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MetroCluster环境中：
  - 在配置外部密钥管理器之前，您必须配置 MetroCluster 环境。
  - 您必须在两个集群上安装相同的 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`命令将取代 `security key-manager setup`命令。您可以运行 `security key-manager external modify`命令来更改外部密钥管理配置。有关的详细信息 `security key-manager external enable`，请参见"ONTAP 命令参考"。
>
> ◦ 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`命令将取代 `security key-manager show -status`命令。有关的详细信息 `security key-manager external show-status`
> ，请参见link:https://docs.netapp.com/us-en/ontap-cli/security-key-manager-external-show-status.html["ONTAP 命令参考"^]。

```
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.
```

相关信息

- 配置集群模式外部密钥服务器
- "安全密钥管理器外部启用"
- "安全密钥管理器外部显示状态"

在ONTAP 9.5 及更早版本中启用基于硬件的加密的外部密钥管理

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、您必须在两个集群上安装相同的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，您必须在两个集群上运行此命令。详细了解 `security key-manager setup`在"ONTAP 命令参考"。

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`

```
cluster1::> 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`

```
cluster1::> 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`

   详细了解此过程中描述的命令"ONTAP 命令参考"。

```
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。

在ONTAP中配置集群模式外部密钥服务器

从ONTAP 9.11.1 开始，您可以在 SVM 上配置与集群外部密钥管理服务器的连接。使用集群密钥服务器，您可以在 SVM 上指定主密钥服务器和辅助密钥服务器。注册或检索密钥时， ONTAP首先尝试访问主密钥服务器，然后依次尝试访问辅助服务器，直到操作成功完成。

您可以使用外部密钥服务器来获取NetApp存储加密 (NSE)、 NetApp卷加密 (NVE) 和NetApp聚合加密 (NAE) 密钥。一个 SVM 最多可以支持四个主外部 KMIP 服务器。每个主服务器最多可支持三个辅助密钥服务器。

关于此任务

- 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"。

开始之前

- "必须为SVM启用KMIP密钥管理"。
- 集群中的所有节点都必须运行ONTAP 9.11.1或更高版本。
- 服务器的排列顺序 `-secondary-key-servers`该参数反映了外部密钥管理（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**

步骤

1. 确认集群（admin SVM）未启用任何密钥管理功能：

   ```
   security key-manager external show -vserver <svm_name>
   ```

   如果 SVM 已启用最多四个主密钥服务器，则必须先删除一个现有的主密钥服务器，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
   <primary_key_server_ip> -client-cert <client_cert_name> -server-ca-certs
   <server_ca_cert_names>
   ```

   - 如果您没有在参数中指定端口， `-key-servers`如果使用参数，则默认使用端口 5696。

   > 如果你正在运行 `security key-manager external enable`对于MetroCluster配置中的管理 SVM 命令，必须在两个集群上运行该命令。如果你要为单个数据 SVM 运行命令，则无需在两个集群上运行该命令。 NetApp强烈建议在两个集群上使用相同的密钥服务器。

3. 修改主密钥服务器，添加辅助密钥服务器。这 `-secondary-key-servers`该参数接受一个以逗号分隔的列表，最多可包含三个密钥服务器：

   ```
   security key-manager external modify-server -vserver <svm_name> -key
   -servers <primary_key_server> -secondary-key-servers <list_of_key_servers>
   ```

   - 请勿在辅助密钥服务器中包含端口号。 `-secondary-key-servers`范围。它使用与主密钥服务器相同的端口号。

   > 如果你正在运行 `security key-manager external`对于MetroCluster配置中的管理 SVM 命令，必须在两个集群上运行该命令。如果你要为单个数据 SVM 运行命令，则无需在两个集群上运行该命令。 NetApp强烈建议在两个集群上使用相同的密钥服务器。

将二级密钥服务器添加到现有主密钥服务器

步骤

1. 修改主密钥服务器，添加辅助密钥服务器。这 `-secondary-key-servers`该参数接受一个以逗号分隔的列表，最多可包含三个密钥服务器：

   ```
   security key-manager external modify-server -vserver <svm_name> -key
   -servers <primary_key_server> -secondary-key-servers <list_of_key_servers>
   ```

   - 请勿在辅助密钥服务器中包含端口号。 `-secondary-key-servers`范围。它使用与主密钥服务器相同的端口号。

如果你正在运行 `security key-manager external modify-server`对于MetroCluster配置中的管理 SVM 命令，必须在两个集群上运行该命令。如果你要为单个数据 SVM 运行命令，则无需在两个集群上运行该命令。 NetApp强烈建议在两个集群上使用相同的密钥服务器。

有关辅助密钥服务器的更多信息，请参阅 [mod-secondary]。

修改集群模式密钥服务器

您可以通过添加和删除辅助密钥服务器、更改辅助密钥服务器的访问顺序或更改特定密钥服务器的指定（主密钥服务器或辅助密钥服务器）来修改集群外部密钥服务器。如果在MetroCluster配置中修改集群外部密钥服务器，NetApp强烈建议在两个集群上使用相同的密钥服务器。

修改二级密钥服务器

使用 `security key-manager external modify-server`命令的 `-secondary-key-servers` 命令的KiKi参数来管理辅助密钥服务器。这 `-secondary-key-servers` 参数接受以逗号分隔的列表。列表中辅助密钥服务器的指定顺序决定了辅助密钥服务器的访问顺序。您可以修改访问顺序，方法是运行 `security key-manager external modify-server` 命令，并按不同的顺序输入二级密钥服务器。辅助密钥服务器无需提供端口号。

如果你正在运行 `security key-manager external modify-server`对于MetroCluster配置中的管理 SVM 命令，必须在两个集群上运行该命令。如果你要为单个数据 SVM 运行命令，则无需在两个集群上运行该命令。

要移除辅助密钥服务器，请将要保留的密钥服务器添加到列表中。 `-secondary-key-servers`参数，并省略要删除的参数。要删除所有辅助密钥服务器，请使用以下参数 `-`表示无。

转换主密钥服务器和辅助密钥服务器

您可以使用以下步骤更改特定密钥服务器的指定（主密钥服务器或辅助密钥服务器）。

将主密钥服务器转换为辅助密钥服务器

步骤

1. 从SVM中移除主密钥服务器：

```
security key-manager external remove-servers
```

> 如果你正在运行 `security key-manager external remove-servers`对于MetroCluster配置中的管理 SVM 命令，必须在两个集群上运行该命令。如果你要为单个数据 SVM 运行命令，则无需在两个集群上运行该命令。

2. 执行[创建集群密钥服务器]使用原主密钥服务器作为辅助密钥服务器进行此过程。

将辅助密钥服务器转换为主密钥服务器

步骤

1. 从现有的主密钥服务器中移除辅助密钥服务器：

```
security key-manager external modify-server -secondary-key-servers
```

- 如果你正在运行 `security key-manager external modify-server -secondary-key-servers`对于MetroCluster配置中的管理 SVM 命令，必须在两个集群上运行该命令。如果你要为单个数据 SVM 运行命令，则无需在两个集群上运行该命令。
- 如果在删除现有密钥服务器的同时将辅助密钥服务器转换为主密钥服务器，则在完成删除和转换之前尝试添加新的密钥服务器可能会导致密钥重复。

1. 执行[创建集群密钥服务器]使用原辅助密钥服务器作为新集群密钥服务器的主密钥服务器进行此过程。

请参阅[mod-secondary]了解更多信息。

相关信息

- 了解更多 `security key-manager external`在"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、必须将Privileges设置为大于 `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
```

> 设置后 `prompt-for-key=true`、系统会提示集群管理员输入密码短语、以便对加密驱动器进行身份验证。否则，系统将自动生成 32 字节密码短语。 `security key-manager key create`命令将取代 `security key-manager create-key`命令。有关的详细信息 `security key-manager key create`，请参见"ONTAP 命令参考"。

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: <id_value>
```

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`命令将取代 `security key-manager query key`命令。

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: <id_value>
node1                                    NSE-AK    yes
    Key ID: <id_value>

       Vserver: cluster1
   Key Manager: external
          Node: node2

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node2                                    NSE-AK    yes
    Key ID: <id_value>
node2                                    NSE-AK    yes
    Key ID: <id_value>
```

有关的详细信息 `security key-manager key query`，请参见"ONTAP 命令参考"。

相关信息

- "存储加密磁盘显示"

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`

   有关的详细信息 `security key-manager create-key`，请参见"ONTAP 命令参考"。

   > 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: <id_value>

   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`

   有关的详细信息 `security key-manager query`，请参见"ONTAP 命令参考"。

   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: <id_value>


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

Key Tag         Key Type  Restored
--------------  --------  --------
cluster1-02     NSE-AK    yes
       Key ID: <id_value>
```

使用ONTAP外部密钥管理将数据身份验证密钥分配给 FIPS 驱动器或 SED

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`*

   有关的详细信息 `storage encryption disk modify`，请参见"ONTAP 命令参考"。

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
<id_value>

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`

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

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

相关信息

- "存储加密磁盘显示"
- "存储加密磁盘显示状态"

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。

详细了解 `security key-manager onboard enable`和 `security key-manager onboard sync`在"ONTAP 命令参考"。

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。
>
> 升级命令通过检查各种数字签名来验证图像内容是否被更改或损坏。如果验证有效，图像更新将进入下一步。如果验证无效，则图像更新失败。详细了解 `cluster image`在"ONTAP 命令参考"。

> 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`为要求用户在重新启动后输入密钥管理器密码短语。MetroCluster配置不支持此 `- cc-mode-enabled`选项。 `security key-manager onboard enable`命令将取代 `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：

2. 输入一个介于 32 到 256 个字符之间的密码，或者对于“`cc-mode`”，输入一个介于 64 到 256 个字符之间的密码。

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. 验证系统是否创建了身份验证密钥：

```
security key-manager key query -node node
```

`security key-manager key query`命令将取代 `security key-manager query key`命令。

有关的详细信息 `security key-manager key query`，请参见"ONTAP 命令参考"。

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。

系统自动将关键管理信息备份到集群的复制数据库（RDB）。您还应该手动备份此信息以用于灾难恢复。

相关信息

- "集群图像命令"
- "安全密钥管理器外部启用"
- "安全密钥管理器密钥查询"
- "安全密钥管理器板载启用"
- "从外部密钥管理过渡到板载密钥管理"

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来保护集群用于访问加密数据的密钥。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

- 如果您将 NSE 与外部密钥管理 (KMIP) 服务器一起使用，请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，请先配置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 show-key-store`

   详细了解 `security key-manager show-key-store`在"ONTAP 命令参考"。

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

Node: node1
Key Store: onboard
Key ID                                                               Used By
-----------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK

Node: node2
Key Store: onboard
Key ID                                                               Used By
-----------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK
```

完成后

ONTAP会自动将密钥管理信息备份到集群的复制数据库 (RDB)。

配置板载密钥管理器密码后，请手动将信息备份到存储系统外部的安全位置。看"手动备份板载密钥管理信息"。

相关信息

- "手动备份板载密钥管理信息"
- "安全密钥管理器设置"
- "安全密钥管理器显示密钥库"
- "从外部密钥管理过渡到板载密钥管理"

使用ONTAP板载密钥管理将数据身份验证密钥分配给 FIPS 驱动器或 SED

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`

   有关的详细信息 `storage encryption disk modify`，请参见"ONTAP 命令参考"。

   > 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
   <id_value>

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

   有关的详细信息 `security key-manager key query`，请参见"ONTAP 命令参考"。

2. 验证是否已分配身份验证密钥：

   `storage encryption disk show`

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

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

相关信息

- "存储加密磁盘显示"
- "存储加密磁盘显示状态"

将 FIPS 140-2 身份验证密钥分配给ONTAP 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
   <id_value>

   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`

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

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

相关信息

- "存储加密磁盘修改"

- "存储加密磁盘显示"
- "存储加密磁盘显示状态"

在ONTAP中为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
   ```

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

   ```
   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
   ```

有关的详细信息 `security config modify`，请参见"ONTAP 命令参考"。

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
```

版权信息

版权所有 © 2026 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。