



# 配置板载密钥管理 ONTAP 9

NetApp  
February 12, 2026

# 目录

|   |   |
|---|---|
| 配置板载密钥管理 .....                                  | 1 |
| 在 ONTAP 9.6 及更高版本中启用板载密钥管理 .....                | 1 |
| 在 ONTAP 9.5 及更早版本中启用板载密钥管理 .....                | 2 |
| 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 ..... | 5 |

# 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"](#)

## 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。