



## 配置外部密钥管理 ONTAP 9

NetApp  
April 24, 2024

# 目录

- 配置外部密钥管理..... 1
  - 配置外部密钥管理概述..... 1
  - 使用System Manager管理外部密钥管理器..... 1
  - 在集群上安装 SSL 证书..... 3
  - 在 ONTAP 9.6 及更高版本（ NVE ）中启用外部密钥管理..... 4
  - 在 ONTAP 9.5 及更早版本中启用外部密钥管理..... 6
  - 通过云提供商管理密钥..... 8

# 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 9.13.1 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  。

- 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。
- 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。
- 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。
- 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

- 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*。

- 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 scoper* 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 scoper* 为集群中的数据 SVM 配置外部密钥管理。这最适合多租户环境，其中每个租户都使用不同的 SVM（或一组 SVM）来提供数据。只有给定租户的 SVM 管理员才能访问该租户的密钥。
- 对于多租户环境，请使用以下命令为 *MT\_EK\_MGMT* 安装许可证：

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

有关完整的命令语法，请参见命令手册页。

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

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

开始之前

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

- 在MetroCluster 环境中、必须在两个集群上安装KMIP SSL证书。

## 步骤

### 1. 配置集群的密钥管理器连接：

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



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

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

```
cluster1::> security key-manager external enable -vserver cluster1 -key
-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

### 2. 配置密钥管理器 SVM：

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



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

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

```
svm11::> 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			
	svml	keyserver.svml.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			
	svml	keyserver.svml.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
```

```
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
```

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AWS文档 ["赠款"](#)。

### 在ONTAP SVM上启用AWS KMS

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 vsriver 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"](#)

## 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。