配置外部密钥管理

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/zh-cn/ontap/encryption-at-rest/configure-external-key-management-concept.html on April 24, 2024. Always check docs.netapp.com for the latest.

目录

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
```

```
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。

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
[...]
```

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。