Configure la gestión de claves externas

ONTAP 9

NetApp
February 12, 2026

Tabla de contenidos

Configure la gestión de claves externas

Obtenga información sobre cómo configurar la administración de claves externas de ONTAP

Puede usar uno o varios servidores de gestión de claves externos para proteger las claves que utiliza el clúster para acceder a los datos cifrados. Un servidor de gestión de claves externo es un sistema de terceros en el entorno de almacenamiento que proporciona claves a los nodos mediante el protocolo de interoperabilidad de gestión de claves (KMIP).

El cifrado de volúmenes de NetApp (NVE) se puede implementar con el gestor de claves incorporado. En ONTAP 9.3 y versiones posteriores, el NVE puede implementarse con gestión de claves externa (KMIP) y el gestor de claves incorporado. A partir de ONTAP 9.11.1, es posible configurar varios administradores de claves externos en un clúster. Consulte Configurar servidores de claves en cluster.

Instalar certificados SSL en el clúster ONTAP

El clúster y el servidor KMIP utilizan certificados SSL KMIP para verificar la identidad de las otras y establecer una conexión SSL. Antes de configurar la conexión SSL con el servidor KMIP, debe instalar los certificados SSL de cliente KMIP para el clúster y el certificado público SSL para la entidad de certificación (CA) raíz del servidor KMIP.

Acerca de esta tarea

En una pareja de alta disponibilidad, ambos nodos deben usar los mismos certificados KMIP públicos y privados. Si conecta varias parejas de alta disponibilidad con el mismo servidor KMIP, todos los nodos de las parejas de alta disponibilidad deben utilizar los mismos certificados KMIP públicos y privados.

Antes de empezar

- La hora debe sincronizarse en el servidor que crea los certificados, el servidor KMIP y el clúster.
- Debe haber obtenido el certificado de cliente SSL KMIP público para el clúster.
- Debe haber obtenido la clave privada asociada con el certificado de cliente SSL KMIP para el clúster.
- El certificado de cliente SSL KMIP no debe estar protegido por contraseña.
- Debe haber obtenido el certificado público de SSL para la entidad de certificación (CA) raíz del servidor KMIP.
- En un entorno de MetroCluster, debe instalar los mismos certificados SSL KMIP en ambos clústeres.

Es posible instalar los certificados de cliente y de servidor en el servidor KMIP antes o después de instalar los certificados en el clúster.

Pasos

1. Instale los certificados de cliente SSL KMIP para el clúster:

   ```
   security certificate install -vserver admin_svm_name -type client
   ```

   Se le solicita que introduzca los certificados públicos y privados de SSL KMIP.

```
cluster1::> security certificate install -vserver cluster1 -type client
```

2. Instale el certificado público SSL para la entidad de certificación (CA) raíz del servidor KMIP:

```
security certificate install -vserver admin_svm_name -type server-ca
```

```
cluster1::> security certificate install -vserver cluster1 -type server-ca
```

Información relacionada

- "instalación del certificado de seguridad"

Habilitar la administración de claves externas para el cifrado basado en hardware en ONTAP 9.6 y versiones posteriores

Puede utilizar uno o varios servidores KMIP para proteger las claves que utiliza el clúster para acceder a los datos cifrados. Se pueden conectar hasta cuatro servidores KMIP a un nodo. Se recomienda un mínimo de dos servidores para la redundancia y la recuperación ante desastres.

A partir de ONTAP 9.11.1, puede agregar hasta 3 servidores de claves secundarios por servidor de claves primario para crear un servidor de claves en clúster. Para obtener más información, consulte Configurar servidores de claves externas en cluster.

Antes de empezar

- Deben haberse instalado el cliente KMIP SSL y los certificados de servidor.
- Para realizar esta tarea, debe ser un administrador de clústeres.
- En un entorno MetroCluster :
  - Debe configurar el entorno de MetroCluster antes de configurar un gestor de claves externo.
  - Debe instalar el mismo certificado SSL KMIP en ambos clústeres.

Pasos

1. Configure la conectividad del gestor de claves para el clúster:

```
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
```

> ◦ El `security key-manager external enable` comando reemplaza `security key-manager setup` el comando. Es posible ejecutar `security key-manager external modify` el comando para cambiar la configuración de gestión de claves externas. Obtenga más información sobre `security key-manager external enable` en el "Referencia de comandos del ONTAP".
>
> ◦ En un entorno MetroCluster, si se configura la gestión de claves externa para la SVM de administrador, debe repetir `security key-manager external enable` el comando en el clúster de socios.

El siguiente comando habilita la gestión de claves externas `cluster1` con tres servidores de claves externos. El primer servidor de claves se especifica mediante su nombre de host y puerto, el segundo se especifica mediante una dirección IP y el puerto predeterminado, y el tercero se especifica mediante una dirección IPv6 y un puerto:

```
cluster1::> 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. Compruebe que todos los servidores KMIP configurados están conectados:

`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`

> El `security key-manager external show-status` comando reemplaza `security key-manager show -status` el comando. Obtenga más información sobre `security key-manager external show-status` en el "Referencia de comandos del ONTAP".

```
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.
```

Información relacionada

- Configurar servidores de claves externas en cluster
- "administrador de claves de seguridad habilitado externamente"
- "administrador de claves de seguridad externo para mostrar el estado"

Habilitar la administración de claves externas para el cifrado basado en hardware en ONTAP 9.5 y versiones anteriores

Puede utilizar uno o varios servidores KMIP para proteger las claves que utiliza el clúster para acceder a los datos cifrados. Se pueden conectar hasta cuatro servidores KMIP a un nodo. Se recomienda un mínimo de dos servidores para la redundancia y la recuperación ante desastres.

Acerca de esta tarea

ONTAP configura la conectividad de los servidores KMIP para todos los nodos del clúster.

Antes de empezar

- Deben haberse instalado el cliente KMIP SSL y los certificados de servidor.
- Para realizar esta tarea, debe ser un administrador de clústeres.
- Debe configurar el entorno de MetroCluster antes de configurar un gestor de claves externo.
- En un entorno MetroCluster, debe instalar el mismo certificado SSL KMIP en ambos clústeres.

Pasos

1. Configure la conectividad de Key Manager para los nodos del clúster:

   `security key-manager setup`

   Se inicia la configuración del gestor de claves.

   > En un entorno MetroCluster , debe ejecutar este comando en ambos clústeres. Obtenga más información sobre `security key-manager setup` en el"Referencia de comandos del ONTAP" .

2. Introduzca la respuesta adecuada en cada solicitud.
3. Añadir un servidor KMIP:

   `security key-manager add -address key_management_server_ipaddress`

   ```
   clusterl::> security key-manager add -address 20.1.1.1
   ```

   > En un entorno de MetroCluster, debe ejecutar este comando en ambos clústeres.

4. Añada un servidor KMIP adicional para redundancia:

   `security key-manager add -address key_management_server_ipaddress`

   ```
   clusterl::> security key-manager add -address 20.1.1.2
   ```

En un entorno de MetroCluster, debe ejecutar este comando en ambos clústeres.

5. Compruebe que todos los servidores KMIP configurados están conectados:

   `security key-manager show -status`

   Obtenga más información sobre los comandos descritos en este procedimiento en el"Referencia de comandos del ONTAP" .

```
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. Opcionalmente, convierta volúmenes de texto sin formato en volúmenes cifrados.

   `volume encryption conversion start`

   Debe haber configurado completamente un gestor de claves externo para poder convertir los volúmenes. En un entorno MetroCluster, debe configurarse un gestor de claves externo en ambos sitios.

Configure servidores de claves externas en clúster en ONTAP

A partir de ONTAP 9.11.1, puede configurar la conectividad a servidores de administración de claves externos agrupados en un SVM. Con servidores de claves agrupados, puede designar servidores de claves principales y secundarios en una SVM. Al registrar o recuperar claves, ONTAP primero intenta acceder al servidor de clave principal antes de intentar acceder secuencialmente a los servidores secundarios hasta que la operación se complete exitosamente.

Puede utilizar servidores de claves externos para claves NetApp Storage Encryption (NSE), NetApp Volume Encryption (NVE) y NetApp Aggregate Encryption (NAE). Una SVM puede admitir hasta cuatro servidores KMIP externos primarios. Cada servidor principal puede admitir hasta tres servidores clave secundarios.

Acerca de esta tarea

- Este proceso solo admite servidores de claves que utilizan KMIP. Para obtener una lista de los servidores de claves compatibles, compruebe el "Herramienta de matriz de interoperabilidad de NetApp".

Antes de empezar

- "La gestión de claves KMIP debe estar habilitada para la SVM".
- Todos los nodos del clúster deben ejecutar ONTAP 9.11.1 o una versión posterior.

- El orden de los servidores enumerados en el `-secondary-key-servers` El parámetro refleja el orden de acceso de los servidores de administración de claves externas (KMIP).

Cree un servidor de claves en clúster

El procedimiento de configuración depende de si se ha configurado o no un servidor de claves primario.

Añada servidores de claves primarios y secundarios a una SVM

Pasos

1. Confirme que no se ha habilitado ninguna administración de claves para el clúster (SVM de administrador):

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

   Si la SVM ya tiene habilitado el máximo de cuatro servidores de clave principal, debe eliminar uno de los servidores de clave principal existentes antes de agregar uno nuevo.

2. Habilitar el administrador de claves principal:

   ```
   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>
   ```

   - Si no especifica un puerto en el `-key-servers` parámetro, se utiliza el puerto predeterminado 5696.

   > Si está ejecutando el `security key-manager external enable` comando para el SVM de administrador en una configuración de MetroCluster , debe ejecutar el comando en ambos clústeres. Si está ejecutando el comando para un SVM de datos individual, no necesita ejecutar el comando en ambos clústeres. NetApp recomienda encarecidamente utilizar los mismos servidores clave en ambos clústeres.

3. Modifique el servidor de clave principal para agregar servidores de clave secundaria. El `-secondary -key-servers` El parámetro acepta una lista separada por comas de hasta tres servidores clave:

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

   - No incluya un número de puerto para servidores de clave secundaria en el `-secondary-key -servers` parámetro. Utiliza el mismo número de puerto que el servidor de clave principal.

   > Si está ejecutando el `security key-manager external` comando para el SVM de administrador en una configuración de MetroCluster , debe ejecutar el comando en ambos clústeres. Si está ejecutando el comando para un SVM de datos individual, no necesita ejecutar el comando en ambos clústeres. NetApp recomienda encarecidamente utilizar los mismos servidores clave en ambos clústeres.

Añadir servidores de claves secundarios a un servidor de claves primario existente

Pasos

1. Modifique el servidor de clave principal para agregar servidores de clave secundaria. El `-secondary -key-servers` El parámetro acepta una lista separada por comas de hasta tres servidores clave:

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

- No incluya un número de puerto para servidores de clave secundaria en el `-secondary-key-servers` parámetro. Utiliza el mismo número de puerto que los servidores de clave principal.

> Si está ejecutando el `security key-manager external modify-server` comando para el SVM de administrador en una configuración de MetroCluster , debe ejecutar el comando en ambos clústeres. Si está ejecutando el comando para un SVM de datos individual, no necesita ejecutar el comando en ambos clústeres. NetApp recomienda encarecidamente utilizar los mismos servidores clave en ambos clústeres.

Para obtener más información sobre los servidores de claves secundarias, consulte [mod-secondary].

Modifique los servidores de claves en cluster

Puede modificar servidores de claves externos agrupados agregando y eliminando servidores de claves secundarios, cambiando el orden de acceso de los servidores de claves secundarios o cambiando la designación (principal o secundaria) de servidores de claves particulares. Si modifica servidores de clave externos agrupados en una configuración de MetroCluster , NetApp recomienda enfáticamente utilizar los mismos servidores de clave en ambos clústeres.

Modificar servidores de claves secundarios

Utilice el parámetro `-secondary-key-servers` del comando `security key-manager external modify-server` para gestionar servidores de claves secundarios. El `-secondary-key-servers` El parámetro acepta una lista separada por comas. El orden especificado de los servidores de clave secundaria en la lista determina la secuencia de acceso para los servidores de clave secundaria. Puede modificar el orden de acceso ejecutando el comando `security key-manager external modify-server` con los servidores de claves secundarios introducidos en una secuencia diferente. No incluya un número de puerto para servidores de clave secundaria.

> Si está ejecutando el `security key-manager external modify-server` comando para el SVM de administrador en una configuración de MetroCluster , debe ejecutar el comando en ambos clústeres. Si está ejecutando el comando para un SVM de datos individual, no necesita ejecutar el comando en ambos clústeres.

Para eliminar un servidor de clave secundaria, incluya los servidores de clave que desea conservar en el `-secondary-key-servers` parámetro y omite el que deseas eliminar. Para eliminar todos los servidores de claves secundarias, utilice el argumento `-` , que significa ninguno.

Convertir servidores de claves primarios y secundarios

Puede utilizar los siguientes pasos para cambiar la designación (principal o secundaria) de servidores de claves particulares.

Convertir un servidor de clave principal en un servidor de clave secundaria

Pasos

1. Eliminar el servidor de clave principal de la SVM:

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

   > Si está ejecutando el `security key-manager external remove-servers` comando para el SVM de administrador en una configuración de MetroCluster , debe ejecutar el comando en ambos clústeres. Si está ejecutando el comando para un SVM de datos individual, no necesita ejecutar el comando en ambos clústeres.

2. Realizar elCree un servidor de claves en clúster procedimiento que utiliza el antiguo servidor de clave principal como servidor de clave secundaria.

Convertir un servidor de clave secundaria en un servidor de clave principal

Pasos

1. Eliminar el servidor de clave secundaria de su servidor de clave principal existente:

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

- Si está ejecutando el `security key-manager external modify-server -secondary-key -servers` comando para el SVM de administrador en una configuración de MetroCluster , debe ejecutar el comando en ambos clústeres. Si está ejecutando el comando para un SVM de datos individual, no necesita ejecutar el comando en ambos clústeres.
- Si convierte un servidor de clave secundario en un servidor de clave principal mientras elimina un servidor de clave existente, intentar agregar un nuevo servidor de clave antes de completar la eliminación y la conversión puede generar la duplicación de claves.

1. Realizar elCree un servidor de claves en clúster procedimiento que utiliza el antiguo servidor de clave secundaria como servidor de clave principal del nuevo servidor de clave agrupado.

Referirse a[mod-secondary] Para más información.

Información relacionada

- Obtenga más información sobre `security key-manager external` en el"Referencia de comandos del ONTAP"

Cree claves de autenticación en ONTAP 9.6 y versiones posteriores

Puede usar el `security key-manager key create` comando para crear las claves de autenticación de un nodo y almacenarlas en los servidores KMIP configurados.

Acerca de esta tarea

Si la configuración de seguridad requiere el uso de claves diferentes para la autenticación de datos y la autenticación FIPS 140-2-2, debe crear una clave independiente para cada una. Si este no es el caso, puede

usar la misma clave de autenticación para el cumplimiento de FIPS que utiliza para el acceso a los datos.

ONTAP crea claves de autenticación para todos los nodos del clúster.

- Este comando no es compatible cuando el gestor de claves incorporado está habilitado. Sin embargo, se crean automáticamente dos claves de autenticación cuando se habilita el gestor de claves incorporado. Las teclas se pueden ver con el siguiente comando:

```
security key-manager key query -key-type NSE-AK
```

- Recibe una advertencia si los servidores de gestión de claves configurados ya almacenan más de 128 claves de autenticación.
- Puede usar el `security key-manager key delete` comando para eliminar las claves no utilizadas. El `security key-manager key delete` comando falla si la clave dada está actualmente en uso en ONTAP. (Para utilizar este comando, debe tener un Privileges mayor que `admin`).

> En un entorno de MetroCluster, antes de eliminar una clave, debe asegurarse de que la clave no se esté utilizando en el clúster de partners. Puede utilizar los siguientes comandos en el clúster de partners para comprobar que la clave no esté en uso:
>
> - `storage encryption disk show -data-key-id <key-id>`
> - `storage encryption disk show -fips-key-id <key-id>`

Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

Pasos

1. Cree las claves de autenticación para los nodos del clúster:

```
security key-manager key create -key-tag <passphrase_label> -prompt-for
-key true|false
```

> Al establecer esta configuración `prompt-for-key=true`, el sistema solicita al administrador del clúster que la clave de acceso se use al autenticar las unidades cifradas. De lo contrario, el sistema genera automáticamente una frase de acceso de 32 bytes. El `security key-manager key create` comando reemplaza `security key-manager create-key` el comando. Obtenga más información sobre `security key-manager key create` en el "Referencia de comandos del ONTAP".

En el siguiente ejemplo se crean las claves de autenticación para `cluster1`, generar automáticamente una frase de contraseña de 32 bytes:

```
cluster1::> security key-manager key create
Key ID: <id_value>
```

2. Compruebe que se han creado las claves de autenticación:

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

> El `security key-manager key query` comando reemplaza `security key-manager query key` el comando.
>
> El ID de clave que se muestra en el resultado es un identificador que se utiliza para hacer referencia a la clave de autenticación. No es la clave de autenticación real ni la clave de cifrado de datos.

En el siguiente ejemplo se verifica que se han creado claves de autenticación para `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>
```

Obtenga más información sobre `security key-manager key query` en el "Referencia de comandos del ONTAP".

Información relacionada

- "Mostrar disco de cifrado de almacenamiento"

Cree claves de autenticación en ONTAP 9.5 y versiones anteriores

Puede usar el `security key-manager create-key` comando para crear las claves de autenticación de un nodo y almacenarlas en los servidores KMIP configurados.

Acerca de esta tarea

Si la configuración de seguridad requiere el uso de claves diferentes para la autenticación de datos y la autenticación FIPS 140-2-2, debe crear una clave independiente para cada una. Si no es así, puede usar la misma clave de autenticación para el cumplimiento de FIPS que se usa para acceder a los datos.

ONTAP crea claves de autenticación para todos los nodos del clúster.

- Este comando no es compatible cuando la gestión de claves incorporada está habilitada.
- Recibe una advertencia si los servidores de gestión de claves configurados ya almacenan más de 128 claves de autenticación.

  Se puede usar el software del servidor de gestión de claves para eliminar las claves sin usar y, a continuación, ejecutar el comando de nuevo.

Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

Pasos

1. Cree las claves de autenticación para los nodos del clúster:

   `security key-manager create-key`

   Obtenga más información sobre `security key-manager create-key` en el "Referencia de comandos del ONTAP".

   > El ID de clave que se muestra en el resultado es un identificador que se utiliza para hacer referencia a la clave de autenticación. No es la clave de autenticación real ni la clave de cifrado de datos.

   En el siguiente ejemplo se crean las claves de autenticación para `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. Compruebe que se han creado las claves de autenticación:

   `security key-manager query`

   Obtenga más información sobre `security key-manager query` en el "Referencia de comandos del ONTAP".

   En el siguiente ejemplo se verifica que se han creado claves de autenticación para `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>
```

Asignar una clave de autenticación de datos a una unidad FIPS o SED con la administración de claves externas ONTAP

Puede utilizar `storage encryption disk modify` el comando para asignar una clave de autenticación de datos a una unidad FIPS o SED. Los nodos de clúster utilizan esta clave para bloquear o desbloquear los datos cifrados en la unidad.

Acerca de esta tarea

Una unidad de autocifrado está protegida contra el acceso no autorizado solo si su ID de clave de autenticación se configura como un valor no predeterminado. El ID seguro del fabricante (MSID), que tiene el ID de clave 0x0, es el valor predeterminado estándar para las unidades SAS. Para las unidades NVMe, el valor predeterminado estándar es una clave nula, que se representa como un ID de clave en blanco. Cuando se asigna el ID de clave a una unidad de autocifrado, el sistema cambia el ID de clave de autenticación por un valor no predeterminado.

Este procedimiento no causa interrupciones.

Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

Pasos

1. Asigne una clave de autenticación de datos a una unidad FIPS o SED:

   `storage encryption disk modify -disk disk_ID -data-key-id key_ID`

   Obtenga más información sobre `storage encryption disk modify` en el "Referencia de comandos del ONTAP".

   > Puede usar el `security key-manager query -key-type NSE-AK` comando para ver ID de claves.

   ```
   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. Compruebe que se han asignado las claves de autenticación:

   `storage encryption disk show`

   Obtenga más información sobre `storage encryption disk show` en el "Referencia de comandos del ONTAP".

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

Información relacionada

- "Mostrar disco de cifrado de almacenamiento"
- "estado del disco de cifrado de almacenamiento"