Configure la gestión de claves externas

ONTAP 9

NetApp
April 24, 2024

Tabla de contenidos

Configure la gestión de claves externas

Configure información general sobre la gestión de claves externas

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).

Para ONTAP 9.1 y versiones anteriores, las LIF de gestión de nodos se deben asignar a los puertos que están configurados con el rol de gestión de nodos antes de poder usar el gestor de claves externo.

El cifrado de volúmenes de NetApp (NVE) se puede implementar con el administrador de claves incorporado en ONTAP 9.1 y versiones posteriores. 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 de. Consulte Configurar servidores de claves en cluster.

Recopilar información de red en ONTAP 9.2 y versiones anteriores

Si utiliza ONTAP 9.2 o una versión anterior, debe rellenar la hoja de datos de configuración de red antes de habilitar la gestión de claves externas.

> A partir de ONTAP 9.3, el sistema detecta automáticamente toda la información de red necesaria.

Elemento	Notas	Valor
Nombre de la interfaz de red de gestión de claves		
Dirección IP de la interfaz de red de gestión de claves	Dirección IP de LIF de gestión de nodos, en formato IPv4 o IPv6	
Longitud del prefijo de red IPv6 de la interfaz de red de gestión de claves	Si utiliza IPv6, la longitud del prefijo de red IPv6	
Máscara de subred de la interfaz de red de gestión de claves		
Dirección IP de puerta de enlace de la interfaz de red de gestión de claves		

La dirección IPv6 de la interfaz de red del clúster	Solo es obligatorio si se utiliza IPv6 para la interfaz de red de gestión de claves	
Número de puerto para cada servidor KMIP	Opcional. El número de puerto debe ser el mismo para todos los servidores KMIP. Si no proporciona un número de puerto, se establece de forma predeterminada en el puerto 5696, que es el puerto asignado por Internet Numbers Authority (IANA) para KMIP.	
Nombre de etiqueta de clave	Opcional. El nombre de etiqueta de clave se utiliza para identificar todas las claves que pertenecen a un nodo. El nombre de etiqueta de clave predeterminado es el nombre del nodo.	

Información relacionada

"Informe técnico de NetApp 3954: Requisitos y procedimientos previos a la instalación de cifrado del almacenamiento de NetApp para IBM Tivoli Lifetime Key Manager"

"Informe técnico de NetApp 4074: Requisitos y procedimientos previos a la instalación de cifrado del almacenamiento de NetApp para SafeNet KeySecure"

Instale los certificados SSL en el clúster

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
   ```

Habilitar gestión de claves externa en ONTAP 9.6 y posterior (basada en hardware)

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.
- Debe configurar el entorno de MetroCluster antes de configurar un gestor de claves externo.
- En un entorno de MetroCluster, debe instalar el 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
   ```

- La `security key-manager external enable` el comando sustituye al `security key-manager setup` comando. Puede ejecutar el `security key-manager external modify` comando para cambiar la configuración de gestión de claves externas. Para obtener una sintaxis de comando completa, consulte las páginas man.
- En un entorno de MetroCluster, si va a configurar la gestión de claves externa para la SVM de administrador, debe repetir el `security key-manager external enable` en el clúster de partners.

El siguiente comando habilita la gestión de claves externas para `cluster1` con tres servidores de claves externas. 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
```

La `security key-manager external show-status` el comando sustituye al `security key-manager show -status` comando. Para obtener una sintaxis de comando completa, consulte la página man.

```
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.
```

Habilite la gestión de claves externas 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 de MetroCluster, debe instalar el 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 de MetroCluster, debe ejecutar este comando en ambos clústeres.

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
```

Para obtener una sintaxis de comando completa, consulte la página man.

```
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.

Configurar servidores de claves externas en cluster

A partir de ONTAP 9.11.1, se puede configurar la conectividad a los servidores de gestión de claves externos en clúster en una SVM. Con los servidores de claves en clúster, puede designar servidores de claves principales y secundarios en una SVM. Al registrar claves, ONTAP primero intentará acceder a un servidor de claves primario antes de intentar acceder secuencialmente a los servidores secundarios hasta que la operación se complete correctamente, lo que evita la duplicación de claves.

Los servidores de claves externos pueden utilizarse para las claves NSE, NVE, NAE y SED. Una SVM puede admitir hasta cuatro servidores KMIP externos principales. Cada servidor primario puede admitir hasta tres servidores de claves secundarios.

Antes de empezar

- "La gestión de claves KMIP debe estar habilitada para la SVM".
- Este proceso solo admite servidores de claves que utilizan KMIP. Para obtener una lista de los servidores de claves compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp".
- Todos los nodos del clúster deben ejecutar ONTAP 9.11.1 o una versión posterior.
- El orden de los servidores enumera los argumentos en la `-secondary-key-servers` El parámetro refleja el orden de acceso de los servidores de gestión 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

1. Confirme que no se ha habilitado ninguna gestión de claves para el clúster:
   `security key-manager external show -vserver` *`svm_name`*
   Si la SVM ya tiene el máximo de cuatro servidores de claves primarias habilitados, debe eliminar uno de los servidores de claves primarios existentes antes de añadir uno nuevo.
2. Habilite el gestor de claves principal:
   `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. Modifique el servidor de claves primario para añadir servidores de claves secundarios. La `-secondary-key-servers` el parámetro acepta una lista de hasta tres servidores de claves separados por coma.
   `security key-manager external modify-server -vserver` *`svm_name`* `-key-servers` *`primary_key_server`* `-secondary-key-servers` *`list_of_key_servers`*

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

1. Modifique el servidor de claves primario para añadir servidores de claves secundarios. La `-secondary-key-servers` el parámetro acepta una lista de hasta tres servidores de claves separados por coma.
   `security key-manager external modify-server -vserver` *`svm_name`* `-key-servers` *`primary_key_server`* `-secondary-key-servers` *`list_of_key_servers`*
   Para obtener más información sobre los servidores de claves secundarios, consulte [mod-secondary].

Modifique los servidores de claves en cluster

Para modificar clústeres de servidores de claves externos, cambie el estado (principal o secundario) de servidores de claves específicos, añada o elimine servidores de claves secundarios, o cambie el orden de acceso de los servidores de claves secundarios.

Convertir servidores de claves primarios y secundarios

Para convertir un servidor de claves primario en un servidor de claves secundario, primero debe eliminarlo de la SVM con el `security key-manager external remove-servers` comando.

Para convertir un servidor de claves secundario en un servidor de claves primario, primero se debe quitar el servidor de claves secundario de su servidor de claves primario existente. Consulte [mod-secondary]. Si convierte un servidor de claves secundario en un servidor primario mientras elimina una clave existente, intentar agregar un servidor nuevo antes de completar la eliminación y conversión puede provocar la duplicación de claves.

Modificar servidores de claves secundarios

Los servidores de claves secundarios se gestionan con el `-secondary-key-servers` parámetro de `security key-manager external modify-server` comando. La `-secondary-key-servers` el parámetro acepta una lista separada por comas. El orden especificado de los servidores de claves secundarios de la lista determina la secuencia de acceso de los servidores de claves secundarios. El orden de acceso se puede modificar ejecutando el comando `security key-manager external modify-server` con los servidores de claves secundarios introducidos en un orden diferente.

Para eliminar un servidor de claves secundario, el `-secondary-key-servers` los argumentos deben incluir

los servidores de claves que desea guardar mientras omite el que se va a quitar. Para quitar todos los servidores de claves secundarios, use el argumento `-`, significando ninguno.

Para obtener más información, consulte `security key-manager external` en la "Referencia de comandos de la ONTAP".

Cree claves de autenticación en ONTAP 9.6 y versiones posteriores

Puede utilizar 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 utilizar el `security key-manager key delete` comando para eliminar las claves no utilizadas. La `security key-manager key delete` El comando falla si ONTAP utiliza actualmente la clave proporcionada. (Debe tener privilegios superiores a «'admin'» para utilizar este comando).

> 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
   ```

> Ajuste `prompt-for-key=true` hace que el sistema solicite al administrador del clúster la clave de acceso que se usará en la autenticación de unidades cifradas. De lo contrario, el sistema genera automáticamente una frase de acceso de 32 bytes. La `security key-manager key create` el comando sustituye al `security key-manager create-key` comando. Para obtener una sintaxis de comando completa, consulte la página man.

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

```
cluster1::> security key-manager key create
Key ID:
000000000000000002000000000001006268333f870860128fbe17d393e5083b00000000
00000000
```

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

   `security key-manager key query -node node`

   > La `security key-manager key query` el comando sustituye al `security key-manager query key` comando. Para obtener una sintaxis de comando completa, consulte la página man. 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.

   El ejemplo siguiente verifica para qué se han creado claves de autenticación `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
```

Cree claves de autenticación en ONTAP 9.5 y versiones anteriores

Puede utilizar 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
   ```

   Para obtener una sintaxis de comando completa, consulte la página de manual del 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 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: 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. Compruebe que se han creado las claves de autenticación:

   ```
   security key-manager query
   ```

   Para obtener una sintaxis de comando completa, consulte la página man.

   El ejemplo siguiente verifica para qué se han creado claves de autenticación `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
```

Asignar una clave de autenticación de datos a una unidad FIPS o SED (gestión de claves externa)

Puede utilizar el `storage encryption disk modify` 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`

   Para obtener una sintaxis de comando completa, consulte la página de manual del comando.

   > Puede utilizar el `security key-manager query -key-type NSE-AK` Comando para ver los ID clave.

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

   `storage encryption disk show`

   Para obtener una sintaxis de comando completa, consulte la página man.

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   --------------------------------------------------------------
   0.0.0   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   [...]
   ```