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) es compatible con el gestor de claves incorporado en ONTAP 9.1 y versiones posteriores. A partir de ONTAP 9.3, NVE admite la gestión de claves externas (KMIP) y el gestor de claves incorporado. A partir de ONTAP 9.10.1, puede utilizar Azure Key Vault o el servicio de Google Cloud Key Manager Para proteger las claves NVE. 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.

Gestione los administradores de claves externos con System Manager

A partir de ONTAP 9,7, puede almacenar y administrar claves de autenticación y cifrado con el Administrador de claves integrado. A partir de ONTAP 9.13.1, también es posible usar gestores de claves externos para almacenar y gestionar estas claves.

El gestor de claves incorporado almacena y gestiona claves en una base de datos segura interna del clúster. Su alcance es el cluster. Un gestor de claves externo almacena y gestiona claves fuera del clúster. Su alcance puede ser el clúster o el equipo virtual de almacenamiento. Pueden usarse uno o más administradores de claves externos. Se aplican las siguientes condiciones:

- Si se habilita el gestor de claves incorporado, no es posible habilitar un gestor de claves externo en el nivel del clúster, pero se puede habilitar en el nivel de máquina virtual de almacenamiento.
- Si se habilita un gestor de claves externo en el nivel de clúster, no se puede habilitar el administrador de claves incorporado.

Al usar administradores de claves externos, puede registrar hasta cuatro servidores de claves primarios por máquina virtual y clúster de almacenamiento. Cada servidor de claves primario se puede agrupar en clúster con hasta tres servidores de claves secundarios.

Configure un gestor de claves externo

Para añadir un administrador de claves externo para una máquina virtual de almacenamiento, debe añadir una puerta de enlace opcional al configurar la interfaz de red para la máquina virtual de almacenamiento. Si la máquina virtual de almacenamiento se creó sin la ruta de red, deberá crear la ruta explícitamente para el gestor de claves externo. Consulte "Crear una LIF (interfaz de red)".

Pasos

Es posible configurar un administrador de claves externo comenzando desde distintas ubicaciones de System Manager.

1. Para configurar un gestor de claves externo, realice uno de los siguientes pasos de inicio.

Flujo de trabajo	Navegación	Paso inicial
Configure el Administrador de claves	**Clúster** > **Ajustes**	Desplácese a la sección **Seguridad**. En **Cifrado**, seleccione ⚙. Seleccione **External Key Manager**.
Agregar nivel local	**Almacenamiento** > **Niveles**	Seleccione **+ Agregar nivel local**. Marque la casilla de verificación denominada Configurar Administrador de claves. Seleccione **External Key Manager**.
Prepare el almacenamiento	**Tablero**	En la sección **Capacidad**, selecciona **Preparar almacenamiento**. A continuación, seleccione Configure Key Manager. Seleccione **External Key Manager**.
Configurar cifrado (gestor de claves únicamente en el ámbito de la VM de almacenamiento)	**Almacenamiento** > **VM de almacenamiento**	Seleccione la máquina virtual de almacenamiento. Seleccione la pestaña **Ajustes**. En la sección **Cifrado** en **Seguridad**, selecciona ⚙.

2. Para agregar un servidor de claves primario, seleccione + Add , Y complete los campos **IP Address o Host Name** y **Port**.
3. Los certificados instalados existentes se enumeran en los campos **Certificados de CA de servidor KMIP** y **Certificado de cliente KMIP**. Puede realizar cualquiera de las siguientes acciones:
   - Seleccione ⌄ para seleccionar los certificados instalados que desea asignar al gestor de claves. (Se pueden seleccionar varios certificados de CA de servicio, pero solo se puede seleccionar un certificado de cliente).
   - Seleccione **Añadir nuevo certificado** para agregar un certificado que aún no se haya instalado y asignarlo al administrador de claves externo.
   - Seleccione × junto al nombre del certificado para eliminar los certificados instalados que no desea asignar al gestor de claves externo.
4. Para agregar un servidor de claves secundario, seleccione **Agregar** en la columna **Servidores de claves secundarios** y proporcione sus detalles.
5. Seleccione **Guardar** para completar la configuración.

Edite un gestor de claves externo existente

Si ya configuró un administrador de claves externo, es posible modificar su configuración.

Pasos

1. Para editar la configuración de un gestor de claves externo, realice uno de los siguientes pasos de inicio.

Ámbito	Navegación	Paso inicial
Gestor de claves externo de ámbito del clúster	**Clúster** > **Ajustes**	Desplácese a la sección **Seguridad**. En **Cifrado**, seleccione ⋮, A continuación, seleccione **Editar External Key Manager**.
Gestor de claves externo de ámbito de Storage VM	**Almacenamiento** > **VM de almacenamiento**	Seleccione la máquina virtual de almacenamiento. Seleccione la pestaña **Ajustes**. En la sección **Cifrado** en **Seguridad**, selecciona ⋮, A continuación, seleccione **Editar External Key Manager**.

2. Los servidores de claves existentes se enumeran en la tabla **Servidores de claves**. Es posible realizar las siguientes operaciones:
   - Para agregar un nuevo servidor de claves, seleccione + Add .
   - Para suprimir un servidor de claves, seleccione ⋮ al final de la celda de la tabla que contiene el nombre del servidor de claves. Los servidores de claves secundarios asociados con ese servidor de claves primario también se eliminan de la configuración.

Elimine un gestor de claves externo

Es posible eliminar un gestor de claves externo si los volúmenes no están cifrados.

Pasos

1. Para eliminar un gestor de claves externo, realice uno de los siguientes pasos.

Ámbito	Navegación	Paso inicial
Gestor de claves externo de ámbito del clúster	**Clúster** > **Ajustes**	Desplácese a la sección **Seguridad**. En **Cifrado**, selecciona Seleccionar ⋮, A continuación, seleccione **Eliminar External Key Manager**.
Gestor de claves externo de ámbito de Storage VM	**Almacenamiento** > **VM de almacenamiento**	Seleccione la máquina virtual de almacenamiento. Seleccione la pestaña **Ajustes**. En la sección **Cifrado** en **Seguridad**, selecciona ⋮, A continuación, seleccione **Eliminar External Key Manager**.

Migrar claves entre gestores de claves

Cuando se habilitan varios administradores de claves en un clúster, las claves deben migrarse de un administrador de claves a otro. Este proceso se completa automáticamente con System Manager.

- Si se habilita el administrador de claves incorporado o un gestor de claves externo en el nivel del clúster y algunos volúmenes están cifrados, A continuación, cuando se configura un administrador de claves externo en el nivel de la máquina virtual de almacenamiento, las claves se deben migrar desde el administrador de claves incorporado o el administrador de claves externo en el nivel del clúster al administrador de claves externo en el nivel de la máquina virtual de almacenamiento. System Manager completa automáticamente este proceso.

- Si se crearon volúmenes sin cifrado en una máquina virtual de almacenamiento, no es necesario migrar las claves.

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 externas en ONTAP 9.6 y versiones posteriores (NVE)

Puede utilizar uno o varios servidores KMIP para proteger las claves que utiliza el clúster para acceder a los datos cifrados. A partir de ONTAP 9.6, tiene la opción de configurar

un gestor de claves externo independiente para proteger las claves que utiliza una SVM de datos para acceder a los datos cifrados.

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.

Acerca de esta tarea

Se pueden conectar hasta cuatro servidores KMIP a un clúster o una SVM. Se recomienda un mínimo de dos servidores para la redundancia y la recuperación ante desastres.

El alcance de la gestión de claves externas determina si los servidores de gestión de claves protegen todas las SVM del clúster o solo las SVM seleccionadas:

- Puede usar un *cluster scope* a fin de configurar la gestión de claves externas para todas las SVM del clúster. El administrador de clúster tiene acceso a todas las claves almacenadas en los servidores.
- A partir de ONTAP 9.6, puede usar un *SVM Scope* para configurar la gestión de claves externa para una SVM de datos en el clúster. Esto es mejor para entornos multi-tenant en los que cada inquilino usa una SVM (o un conjunto de SVM) diferente para servir datos. Solo el administrador de SVM para un inquilino determinado tiene acceso a las claves de ese inquilino.
- Para entornos multi-tenant, instale una licencia para *MT_EK_MGMT* mediante el siguiente comando:

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

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

Puede utilizar ambos ámbitos en el mismo clúster. Si se configuraron servidores de gestión de claves para una SVM, ONTAP solo usa esos servidores para proteger las claves. De lo contrario, ONTAP protege las claves con los servidores de gestión de claves configurados para el clúster.

Puede configurar la gestión de claves incorporada en el ámbito del clúster y la gestión de claves externas en el ámbito de la SVM. Puede utilizar el `security key-manager key migrate` Comando para migrar claves de la gestión de claves integrada en el ámbito del clúster a administradores de claves externos en el ámbito de la SVM.

Antes de empezar

- Deben haberse instalado el cliente KMIP SSL y los certificados de servidor.
- Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.
- Si desea habilitar la gestión de claves externas para un entorno de MetroCluster, MetroCluster debe estar completamente configurado para poder habilitar la gestión de claves externas.
- 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. Si ejecuta el comando en la solicitud de inicio de sesión del clúster, *`admin_SVM`* Los valores predeterminados en la SVM de administrador del clúster actual. Para poder configurar el ámbito del clúster, debe ser el administrador del clúster. Puede ejecutar el `security key-manager external modify` comando para cambiar la configuración de gestión de claves externas.
- 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 -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. Configure un administrador de claves una 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
```

- Si ejecuta el comando en la solicitud de inicio de sesión de SVM, `SVM` El valor predeterminado es la SVM actual. Para configurar el ámbito de SVM, debe ser un administrador de clústeres o de SVM. Puede ejecutar el `security key-manager external modify` comando para cambiar la configuración de gestión de claves externas.
- En un entorno de MetroCluster, si va a configurar la gestión de claves externas para una SVM de datos, no es necesario repetir el `security key-manager external enable` en el clúster de partners.

El siguiente comando habilita la gestión de claves externas para `svm1` con un único servidor de claves escuchando en el puerto predeterminado 5696:

```
svm1l::> security key-manager external enable -vserver svm1 -key-servers
keyserver.svm1.com -client-cert SVM1ClientCert -server-ca-certs
SVM1ServerCaCert
```

3. Repita el último paso para todas las SVM adicionales.

> También puede utilizar el `security key-manager external add-servers` Comando para configurar SVM adicionales. La `security key-manager external add-servers` el comando sustituye al `security key-manager add` comando. Para obtener una sintaxis de comando completa, consulte la página man.

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

   `security key-manager external show-status -node node_name`

   > 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
      svm1
               keyserver.svm1.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
      svm1
               keyserver.svm1.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. 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.

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.

Gestione claves con un proveedor de cloud

A partir de ONTAP 9.10.1, puede utilizar "Azure Key Vault (AKV)" y.. "Servicio de gestión de claves de Google Cloud Platform (Cloud KMS)" Para proteger sus claves de cifrado de ONTAP en una aplicación alojada en el cloud. A partir de ONTAP 9.12.0, también puede proteger las claves de NVE con "KMS DE AWS".

AWS KMS, AKV y Cloud KMS se pueden utilizar para proteger "Claves de cifrado de volúmenes de NetApp (NVE)" Solo para SVM de datos.

Acerca de esta tarea

La gestión de claves con un proveedor de cloud se puede habilitar con la interfaz de línea de comandos o la API DE REST DE ONTAP.

Al usar un proveedor de cloud para proteger las claves, tiene en cuenta que de forma predeterminada se usa un LIF SVM de datos para comunicarse con el punto final de gestión de claves de cloud. Una red de gestión de nodos se usa para comunicarse con los servicios de autenticación del proveedor de cloud (login.microsoftonline.com para Azure; oauth2.googleapis.com para Cloud KMS). Si la red de clúster no está configurada correctamente, el clúster no utilizará correctamente el servicio de gestión de claves.

Al utilizar el servicio de gestión de claves de un proveedor de cloud, debe tener en cuenta las siguientes limitaciones:

- La gestión de claves para proveedores de cloud no está disponible para el cifrado del almacenamiento de NetApp (NSE) y el cifrado de agregados de NetApp (NAE). "KMIP externos" se puede utilizar en su lugar.
- La gestión de claves para proveedores de cloud no está disponible para las configuraciones de MetroCluster.
- La gestión de claves del proveedor de cloud solo puede configurarse en una SVM de datos.

Antes de empezar

- Debe haber configurado el KMS en el proveedor de nube correspondiente.

- Los nodos del clúster ONTAP deben admitir NVE.
- "Debe haber instalado las licencias de cifrado de volúmenes (VE) y de gestión de claves de cifrado multi-tenant (MTEKM)". Estas licencias se incluyen con "ONTAP One".
- Debe ser un administrador de clúster o de SVM.
- Las SVM de datos no deben incluir ningún volumen cifrado ni emplear un gestor de claves. Si la SVM de datos incluye volúmenes cifrados, debe migrarlos antes de configurar el KMS.

Habilite la gestión de claves externas

La habilitación de la gestión de claves externas depende del administrador de claves específico que se use. Elija la pestaña del gestor de claves y el entorno adecuados.

AWS

Antes de empezar

- Debe crear un permiso para la clave KMS de AWS que utilizará el rol de IAM que gestiona el cifrado. El rol de IAM debe incluir una política que permita las siguientes operaciones:
  - `DescribeKey`
  - `Encrypt`
  - `Decrypt`

  Para obtener más información, consulte la documentación de AWS para "subvenciones".

Habilite AWS KMV en una SVM de ONTAP

1. Antes de comenzar, obtenga tanto el ID de clave de acceso como la clave secreta de su KMS de AWS.
2. Configure el nivel de privilegio en Advanced:
   `set -priv advanced`
3. Habilitar AWS KMS:
   `security key-manager external aws enable -vserver` *`svm_name`* `-region` *`AWS_region`* `-key-id` *`key_ID`* `-encryption-context` *`encryption_context`*
4. Cuando se le solicite, introduzca la clave secreta.
5. Confirme que el KMS de AWS se ha configurado correctamente:
   `security key-manager external aws show -vserver` *`svm_name`*

Azure

Habilite Azure Key Vault en una SVM de ONTAP

1. Antes de empezar, debe obtener las credenciales de autenticación adecuadas de su cuenta de Azure, ya sea un secreto de cliente o un certificado.
   También debe asegurarse de que todos los nodos del clúster estén en buen estado. Puede comprobarlo con el comando `cluster show`.
2. Establezca el nivel privilegiado en avanzado
   `set -priv advanced`
3. Habilite AKV en el SVM
   `security key-manager external azure enable -client-id` *`client_id`* `-tenant-id` *`tenant_id`* `-name -key-id` *`key_id`* `-authentication-method {certificate|client-secret}`
   Cuando se le solicite, introduzca el certificado de cliente o el secreto de cliente desde la cuenta de Azure.
4. Compruebe que AKV está activado correctamente:
   `security key-manager external azure show vserver` *`svm_name`*
   Si la accesibilidad del servicio no es correcta, establezca la conectividad con el servicio de gestión de claves AKV a través del LIF de Data SVM.

Google Cloud

Habilite Cloud KMS en una SVM de ONTAP

1. Antes de comenzar, obtenga la clave privada para el archivo de claves de cuenta de Google Cloud KMS en formato JSON. Se puede encontrar en su cuenta de GCP.

También debe asegurarse de que todos los nodos del clúster estén en buen estado. Puede comprobarlo con el comando `cluster show`.

2. Defina el nivel con privilegios en avanzado:
   `set -priv advanced`
3. Habilite Cloud KMS en la SVM
   `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`*
   Cuando se le solicite, introduzca el contenido del archivo JSON con la clave privada de cuenta de servicio
4. Compruebe que Cloud KMS está configurado con los parámetros correctos:
   `security key-manager external gcp show vserver` *`svm_name`*
   El estado de `kms_wrapped_key_status` será "`UNKNOWN`" si no se crearon volúmenes cifrados.
   Si la accesibilidad del servicio no es correcta, establezca la conectividad con el servicio de gestión de claves de GCP a través de la LIF de SVM de datos.

Si ya hay uno o más volúmenes cifrados configurados para una SVM de datos y el administrador de claves incorporado de la SVM de administrador gestiona las claves NVE correspondientes, esas claves se deben migrar al servicio de gestión de claves externa. Para hacerlo con la CLI, ejecute el comando:
`security key-manager key migrate -from-Vserver` *`admin_SVM`* `-to-Vserver` *`data_SVM`*
No se pueden crear nuevos volúmenes cifrados para la SVM de datos del inquilino hasta que todas las claves NVE de la SVM de datos se migren correctamente.

Información relacionada

- "Cifrar volúmenes con las soluciones de cifrado de NetApp para Cloud Volumes ONTAP"