Configurar NVE

ONTAP 9

NetApp
January 08, 2026

Tabla de contenidos

Configurar NVE

Determine si la versión de su clúster ONTAP es compatible con NVE

Debe determinar si la versión de clúster es compatible con NVE antes de instalar la licencia. Puede usar el `version` comando para determinar la versión del clúster.

Acerca de esta tarea

La versión del clúster es la versión más baja de ONTAP que se ejecuta en cualquier nodo del clúster.

Pasos

1. Determine si la versión de clúster es compatible con NVE:

   ```
   version -v
   ```

   NVE no se admite si el resultado del comando muestra el texto `1Ono-DARE` (para «sin cifrado de datos en reposo»), o si utiliza una plataforma que no aparece en "Detalles de soporte".

Instalar la licencia de cifrado de volumen en un clúster ONTAP

Una licencia ve le permite usar la función en todos los nodos del clúster. Esta licencia es necesaria para poder cifrar datos con NVE. Está incluido con "ONTAP One".

Antes de ONTAP One, la licencia VE se incluía con el paquete de cifrado. El bundle de cifrado ya no se ofrece, pero sigue siendo válido. Aunque actualmente no es necesario, los clientes existentes pueden optar por "Actualice a ONTAP One".

Antes de empezar

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Debe haber recibido la clave de licencia de VE de su representante de ventas o tener instalado ONTAP One.

Pasos

1. "Compruebe que la licencia VE está instalada".

   El nombre del paquete de licencias de VE es `VE`.

2. Si la licencia no está instalada, "Use System Manager o la interfaz de línea de comandos de ONTAP para instalarlo".

Configure la gestión de claves externas

Obtenga información sobre cómo configurar la administración de claves externas con ONTAP NetApp Volume Encryption

Puede usar uno o más servidores externos de administración de claves para proteger las claves que el clúster utiliza para acceder a los datos cifrados. Un servidor externo de administración de claves es un sistema externo en su entorno de almacenamiento que proporciona claves a los nodos mediante el Protocolo de Interoperabilidad de Administración de Claves (KMIP). Además del Administrador de Claves Integrado, ONTAP admite varios servidores externos de administración de claves.

A partir de ONTAP 9.10.1, puede usar Azure Key Vault o Google Cloud Key Manager Service para proteger sus claves NVE para SVM de datos. A partir de ONTAP 9.11.1, puede configurar varios administradores de claves externos en un clúster. VerConfigurar servidores de claves en clúster . A partir de ONTAP 9.12.0, puede usar "KMS DE AWS" para proteger sus claves NVE para SVM de datos. A partir de ONTAP 9.17.1, puede usar OpenStack Barbican KMS para proteger sus claves NVE para SVM de datos.

Administre administradores de claves externos con ONTAP 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**, seleccione ⚙.

2. Para agregar un servidor de claves principal, seleccione + Add y complete los campos **Dirección IP o Nombre de host** y **Puerto**.
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 ⋮ y luego seleccione **Editar administrador de claves externo**.

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 ⋮ y luego selecciona **Editar Administrador de claves externo**.

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 .
   - Suprima un servidor de claves seleccionando ⋮ 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**, seleccione Seleccionar y ⋮ luego seleccione **Eliminar Administrador de claves externo**.
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**, seleccione ⋮ y luego seleccione **Eliminar Administrador de claves externo**.

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.

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 NVE en ONTAP 9.6 y versiones posteriores

Utilice servidores KMIP para proteger las claves que utiliza el clúster para acceder a datos cifrados. A partir de ONTAP 9.6, tiene la opción de configurar un administrador de claves externo independiente para proteger las claves que utiliza una SVM de datos para acceder a 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

Puede conectar hasta cuatro servidores KMIP a un clúster o SVM. Utilice al menos dos servidores para redundancia y 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>
  ```

  Obtenga más información sobre `system license add` en el "Referencia de comandos del ONTAP".

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 usar el `security key-manager key migrate` comando para migrar claves de la gestión de claves incorporada en el ámbito del clúster a gestores de claves externos en el ámbito de SVM.

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

Antes de empezar

- Deben haberse instalado el cliente KMIP SSL y los certificados de servidor.
- El servidor KMIP debe ser accesible desde el LIF de administración de nodos de cada nodo.
- Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.
- En un entorno MetroCluster :
  - MetroCluster debe estar completamente configurado antes de habilitar la administración de claves externas.
  - Debe instalar el mismo certificado SSL KMIP en ambos clústeres.
  - Se debe configurar un administrador de claves externo 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` El comando reemplaza el `security key-manager setup` dominio. Si ejecuta el comando en el indicador de inicio de sesión del clúster, *`admin_SVM`* El valor predeterminado es el SVM de administración del clúster actual. Puedes ejecutar el `security key-manager external modify` Comando para cambiar la configuración de administración de claves externas.

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:

```
clusterl::> 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 el indicador de inicio de sesión de SVM, `SVM` Por defecto es el SVM actual. Puedes ejecutar el `security key-manager external modify` Comando para cambiar la configuración de administración de claves externas.
- En un entorno MetroCluster, si va a configurar la gestión de claves externa para una SVM de datos, no tendrá que repetir `security key-manager external enable` el comando en el clúster de socios.

El siguiente comando habilita la gestión de claves externa para `svm1` con un único servidor de claves que escucha 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. El `security key-manager external add-servers` comando reemplaza `security key-manager add` el comando. Obtenga más información sobre `security key-manager external add-servers` en el "Referencia de comandos del ONTAP".

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

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

> 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
      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
   ```

   Se debe configurar completamente un administrador de claves externo antes de convertir los volúmenes.

Información relacionada

- Configurar servidores de claves externas en cluster
- "agregar licencia del sistema"
- "migración de claves del administrador de claves de seguridad"
- "Administrador de claves de seguridad, servidores de complementos externos"
- "administrador de claves de seguridad externo mostrar estado"

Habilitar la administración de claves externas para NVE 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.

Administrar claves NVE para SVM de datos ONTAP con un proveedor de nube

A partir de ONTAP 9.10.1, puede usar "Azure Key Vault (AKV)" y "Servicio de gestión de claves de Google Cloud Platform (Cloud KMS)"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 usar para proteger "Claves de cifrado de volúmenes de NetApp (NVE)" solo las 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 usará 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. Establezca el nivel de privilegio en avanzado: `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`*

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

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`. Obtenga más información sobre `cluster show` en el "Referencia de comandos del ONTAP".
2. Establezca el nivel con privilegios en Avanzado `set -priv advanced`
3. Habilite AKV en la 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 de su 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 de la LIF de Data SVM.

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

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`. Obtenga más información sobre `cluster show` en el "Referencia de comandos del ONTAP".

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 la cuenta de servicio
4. Verifique que Cloud KMS esté 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 han creado volúmenes cifrados. Si la accesibilidad del servicio no es correcta, establezca la conectividad con el servicio de administración de claves de GCP a través del LIF de SVM de datos.

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

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"
- "administrador de claves de seguridad externo"

Administrar claves ONTAP con Barbican KMS

A partir de ONTAP 9.17.1, puede utilizar OpenStack "Barbican KMS" Para proteger las claves de cifrado de ONTAP . Barbican KMS es un servicio para almacenar y acceder a las claves de forma segura. Barbican KMS puede utilizarse para proteger las claves de NetApp Volume Encryption (NVE) para las máquinas virtuales de datos (SVM). Barbican se basa en "OpenStack Keystone" , Servicio de identidad de OpenStack, para autenticación.

Acerca de esta tarea

Puede configurar la administración de claves con Barbican KMS mediante la CLI o la API REST de ONTAP . Con la versión 9.17.1, la compatibilidad con Barbican KMS presenta las siguientes limitaciones:

- Barbican KMS no es compatible con NetApp Storage Encryption (NSE) ni NetApp Aggregate Encryption (NAE). Como alternativa, puede usar "KMIP externos" o el "Administrador de claves integrado (OKM)" para claves NSE y NVE.
- Barbican KMS no es compatible con configuraciones de MetroCluster .
- Barbican KMS solo se puede configurar para una SVM de datos. No está disponible para la SVM de administración.

A menos que se indique lo contrario, los administradores de la `admin` El nivel de privilegio puede realizar los siguientes procedimientos.

Antes de empezar

- Es necesario configurar Barbican KMS y OpenStack Keystone . La SVM que utilice con Barbican debe tener acceso de red a los servidores Barbican y OpenStack Keystone .
- Si está utilizando una autoridad de certificación (CA) personalizada para los servidores Barbican y OpenStack Keystone , debe instalar el certificado de CA con `security certificate install -type server-ca -vserver <admin_svm>` .

Crear y activar una configuración de Barbican KMS

Puede crear una nueva configuración de Barbican KMS para una SVM y activarla. Una SVM puede tener varias configuraciones de Barbican KMS inactivas, pero solo una puede estar activa a la vez.

Pasos

1. Cree una nueva configuración inactiva de Barbican KMS para una SVM:

```
security key-manager external barbican create-config -vserver <svm_name>
-config-name <unique_config_name> -key-id <key_id> -keystone-url
<keystone_url> -application-cred-id
<keystone_applications_credentials_id>
```

   - `-key-id` es el identificador de clave de la clave de cifrado de Barbican (KEK). Introduzca una URL completa, incluyendo `https://` .

     Algunas URL incluyen el signo de interrogación (?). Este signo activa la ayuda activa de la línea de comandos de ONTAP . Para introducir una URL con un signo de interrogación, primero debe desactivar la ayuda activa con el comando. `set -active -help false` La ayuda activa se puede volver a habilitar posteriormente con el comando `set -active-help true` . Obtenga más información en el "Referencia de comandos del ONTAP" .

   - `-keystone-url` es la URL del host de autorización de OpenStack Keystone . Ingrese una URL completa, incluyendo `https://` .
   - `-application-cred-id` Es el ID de las credenciales de la aplicación.

     Tras introducir este comando, se le solicitará la clave secreta de las credenciales de la aplicación. Este comando crea una configuración de Barbican KMS inactiva.

     El siguiente ejemplo crea una nueva configuración inactiva de Barbican KMS denominada `config1` para el SVM `svm1` :

```
cluster1::> security key-manager external barbican create-config
-vserver svm1 -config-name config1 -keystone-url
https://172.21.76.152:5000/v3 -application-cred-id app123 -key-id
https://172.21.76.153:9311/v1/secrets/<id_value>

Enter the Application Credentials Secret for authentication with
Keystone: <key_value>
```

2. Activar la nueva configuración de Barbican KMS:

```
security key-manager keystore enable -vserver <svm_name> -config-name
<unique_config_name> -keystore barbican
```

Puede usar este comando para cambiar entre las configuraciones de Barbican KMS. Si ya hay una configuración de Barbican KMS activa en la SVM, se desactivará y se activará la nueva configuración.

3. Verifique que la nueva configuración de Barbican KMS esté activa:

```
security key-manager external barbican check -vserver <svm_name> -node
<node_name>
```

Este comando proporcionará el estado de la configuración activa de Barbican KMS en la SVM o el nodo. Por ejemplo, si la SVM `svm1` en el nodo `node1` tiene una configuración Barbican KMS activa, el siguiente comando devolverá el estado de esa configuración:

```
cluster1::> security key-manager external barbican check -node node1

Vserver: svm1
Node: node1

Category: service_reachability
             Status: OK

Category: kms_wrapped_key_status
             Status: OK
```

Actualizar las credenciales y la configuración de una configuración de Barbican KMS

Puede ver y actualizar la configuración actual de una configuración de Barbican KMS activa o inactiva.

Pasos

1. Ver las configuraciones actuales de Barbican KMS para un SVM:

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

El ID de clave, la URL de OpenStack Keystone y el ID de credenciales de la aplicación se muestran para cada configuración de Barbican KMS en SVM.

2. Actualizar la configuración de un KMS de Barbican:

```
security key-manager external barbican update-config -vserver <svm_name>
-config-name <unique_config_name> -timeout <timeout> -verify
<true|false> -verify-host <true|false>
```

Este comando actualiza la configuración de tiempo de espera y verificación de la configuración de Barbican KMS especificada. `timeout` Determina el tiempo en segundos que ONTAP esperará a que Barbican responda antes de que falle la conexión. El valor predeterminado `timeout` Son diez segundos. `verify` y `verify-host` Determinar si se debe verificar la identidad y el nombre de host del host Barbican antes de la conexión. De forma predeterminada, estos parámetros están configurados en `true` . El `vserver` y `config-name` Los parámetros son obligatorios. Los demás parámetros son opcionales.

3. Si es necesario, actualice las credenciales de una configuración de Barbican KMS activa o inactiva:

```
security key-manager external barbican update-credentials -vserver
<svm_name> -config-name <unique_config_name> -application-cred-id
<keystone_applications_credentials_id>
```

Después de ingresar este comando, se le solicitará la nueva clave secreta de las credenciales de la aplicación.

4. Si es necesario, restaure una clave de cifrado de clave SVM (KEK) faltante para una configuración activa de Barbican KMS:
   a. Restaurar una KEK de SVM faltante con `security key-manager external barbican restore` :

```
security key-manager external barbican restore -vserver <svm_name>
```

Este comando restaurará la KEK de SVM para la configuración activa de Barbican KMS comunicándose con el servidor Barbican.

5. Si es necesario, vuelva a introducir la clave KEK de SVM para una configuración de Barbican KMS:
   a. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

   b. Vuelva a crear la clave KEK de SVM con `security key-manager external barbican rekey-internal` :

```
security key-manager external barbican rekey-internal -vserver
<svm_name>
```

Este comando genera una nueva KEK de SVM para el SVM especificado y reencapsula las claves de cifrado del volumen con la nueva KEK de SVM. La nueva KEK de SVM estará protegida por la configuración activa de Barbican KMS.

Migrar claves entre Barbican KMS y el administrador de claves integrado

Puede migrar claves de Barbican KMS al Administrador de claves integrado (OKM) y viceversa. Para obtener más información sobre OKM, consulte "Habilite la gestión de claves incorporada en ONTAP 9.6 y versiones posteriores" .

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Si es necesario, migre claves de Barbican KMS a OKM:

```
security key-manager key migrate -from-vserver <svm_name> -to-vserver
<admin_svm_name>
```

`svm_name` es el nombre del SVM con la configuración Barbican KMS.

3. Si es necesario, migre claves de OKM a Barbican KMS:

```
security key-manager key migrate -from-vserver <admin_svm_name> -to
-vserver <svm_name>
```

Deshabilitar y eliminar una configuración de Barbican KMS

Puede deshabilitar una configuración de Barbican KMS activa sin volúmenes cifrados y puede eliminar una configuración de Barbican KMS inactiva.

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Deshabilitar una configuración activa de Barbican KMS:

```
security key-manager keystore disable -vserver <svm_name>
```

Si existen volúmenes cifrados NVE en la SVM, debe descifrarlos o migrar las claves Antes de deshabilitar la configuración de Barbican KMS, active una nueva configuración de Barbican KMS sin descifrar volúmenes NVE ni migrar claves. Deshabilitará la configuración actual de Barbican KMS.

3. Eliminar una configuración inactiva de Barbican KMS:

```
security key-manager keystore delete -vserver <svm_name> -config-name
<unique_config_name> -type barbican
```

Habilitar la administración de claves integrada para NVE en ONTAP 9.6 y versiones posteriores

Puede usar el administrador de claves incorporado para proteger las claves que el clúster utiliza para acceder a los datos cifrados. Debe habilitar el administrador de claves incorporado en cada clúster que tenga acceso a un volumen cifrado o a un disco de autocifrado.

Acerca de esta tarea

Debe ejecutar `security key-manager onboard sync` el comando cada vez que añade un nodo al clúster.

Si tiene una configuración MetroCluster, debe ejecutar `security key-manager onboard enable` el comando en el clúster local primero y luego ejecutar `security key-manager onboard sync` el comando en el clúster remoto, usando la misma clave de acceso en cada uno. Al ejecutar `security key-manager onboard enable` el comando desde el clúster local y sincronizarse en el clúster remoto, no es necesario que `enable` vuelva a ejecutar el comando desde el clúster remoto.

Obtenga más información sobre `security key-manager onboard enable` y `security key-manager onboard sync` en el"Referencia de comandos del ONTAP" .

De forma predeterminada, no es necesario introducir la clave de acceso del administrador de claves cuando se reinicia un nodo. Puede usar `cc-mode-enabled=yes` la opción para solicitar que los usuarios introduzcan la frase de acceso después de reiniciar.

Para NVE, si establece `cc-mode-enabled=yes`, los volúmenes que cree con los `volume create` `volume move start` comandos y se cifran automáticamente. Para `volume create`, no es necesario especificar `-encrypt true`. Para `volume move start`, no es necesario especificar `-encrypt-destination true`.

Al configurar el cifrado de datos en reposo de ONTAP , para cumplir con los requisitos de Soluciones comerciales para clasificados (CSfC), debe usar NSE con NVE y asegurarse de que el Administrador de claves integrado esté habilitado en el modo de Criterios comunes. Ver"Breve descripción de la solución CSfC" .

Cuando Onboard Key Manager está activado en el modo Common Criteria (`cc-mode-enabled=yes`), el comportamiento del sistema se cambia de las siguientes formas:

- El sistema supervisa los intentos fallidos consecutivos de acceso al clúster cuando funciona en modo de criterios comunes.

  Si no logra ingresar la frase de contraseña del clúster 5 veces, espere 24 horas o reinicie el nodo para restablecer el límite.

- Las actualizaciones de imágenes del sistema utilizan el certificado de firma de código RSA-3072 de NetApp junto con los resúmenes firmados con código SHA-384 para comprobar la integridad de la imagen en lugar del certificado de firma de código RSA-2048 de NetApp habitual y los resúmenes firmados con código SHA-256.

  El comando de actualización verifica que el contenido de la imagen no haya sido alterado o dañado comprobando varias firmas digitales. El sistema procede al siguiente paso en el proceso de actualización de la imagen si la validación tiene éxito; de lo contrario, falla la actualización de la imagen. Obtenga más información sobre `cluster image` en el"Referencia de comandos del ONTAP" .

El administrador de claves integrado almacena claves en la memoria volátil. El contenido de la memoria volátil se borra cuando se reinicia o se detiene el sistema. El sistema borra la memoria volátil en 30 segundos cuando se detiene.

Antes de empezar

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Debe configurar el entorno de MetroCluster antes de configurar el gestor de claves incorporado.

Pasos

1. Inicie la configuración del gestor de claves:

   ```
   security key-manager onboard enable -cc-mode-enabled yes|no
   ```

   Establezca esta opción `cc-mode-enabled=yes` para que los usuarios introduzcan la frase de contraseña del gestor de claves después de reiniciar. Para NVE, si establece `cc-mode-enabled=yes`, los volúmenes que cree con los `volume create` `volume move start` comandos y se cifran automáticamente. - `cc-mode-enabled`La opción no es compatible con las configuraciones de MetroCluster. El `security key-manager onboard enable` comando reemplaza `security key-manager setup` el comando.

2. Introduzca una frase de contraseña entre 32 y 256 caracteres, o para “cc-mode”, una frase de contraseña entre 64 y 256 caracteres.

   Si la frase de paso "'cc-mode'" especificada es menor de 64 caracteres, hay un retraso de cinco segundos antes de que la operación de configuración del gestor de claves vuelva a mostrar la indicación de contraseña.

3. En la solicitud de confirmación de contraseña, vuelva a introducir la frase de contraseña.
4. Compruebe que se han creado las claves de autenticación:

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

> El `security key-manager key query` comando reemplaza `security key-manager query key` el comando.

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

5. Opcionalmente, puede convertir volúmenes de texto simple en volúmenes cifrados.

```
volume encryption conversion start
```

El gestor de claves incorporado debe estar completamente configurado antes de convertir los volúmenes. En un entorno MetroCluster, el gestor de claves incorporado debe configurarse en ambos sitios.

Después de terminar

Copie la clave de acceso en una ubicación segura fuera del sistema de almacenamiento para usarla en el futuro.

Después de configurar la contraseña del Onboard Key Manager, realice manualmente una copia de seguridad de la información en una ubicación segura fuera del sistema de almacenamiento. Ver"Realice un backup manual de la información de gestión de claves incorporada" .

Información relacionada

- "comandos de imagen de clúster"
- "Habilitación externa del administrador de claves de seguridad"
- "consulta de claves del administrador de claves de seguridad"
- "Habilitación integrada del administrador de claves de seguridad"

Habilitar la administración de claves integrada para NVE en ONTAP 9.5 y versiones anteriores

Puede usar el administrador de claves incorporado para proteger las claves que el clúster utiliza para acceder a los datos cifrados. Debe habilitar el gestor de claves incorporado en cada clúster que acceda a un volumen cifrado o un disco de autocifrado.

Acerca de esta tarea

Debe ejecutar `security key-manager setup` el comando cada vez que añade un nodo al clúster.

Si tiene una configuración de MetroCluster, revise las siguientes directrices:

- En ONTAP 9.5, debe ejecutarse `security key-manager setup` en el clúster local y `security key-manager setup -sync-metrocluster-config yes` en el clúster remoto, con la misma clave de acceso en cada uno.
- Antes de usar ONTAP 9.5, debe ejecutarse `security key-manager setup` en el clúster local, esperar aproximadamente 20 segundos y, luego, ejecutarse `security key-manager setup` en el clúster remoto, usando la misma clave de acceso en cada uno.

De forma predeterminada, no es necesario introducir la clave de acceso del administrador de claves cuando

se reinicia un nodo. A partir de ONTAP 9.4, puede usar la `-enable-cc-mode yes` opción para solicitar que los usuarios introduzcan la frase de acceso después de reiniciar.

Para NVE, si establece `-enable-cc-mode yes`, los volúmenes que cree con los `volume create` `volume move start` comandos y se cifran automáticamente. Para `volume create`, no es necesario especificar `-encrypt true`. Para `volume move start`, no es necesario especificar `-encrypt-destination true`.

Después de un intento de clave de acceso con errores, debe reiniciar el nodo de nuevo.

Antes de empezar

- Si utiliza NSE o NVE con un servidor de administración de claves externo (KMIP), elimine la base de datos del administrador de claves externo.

  "Transición a la gestión de claves incorporada desde la gestión de claves externas"

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Configure el entorno MetroCluster antes de configurar el Administrador de claves integrado.

Pasos

1. Inicie la configuración del gestor de claves:

   ```
   security key-manager setup -enable-cc-mode yes|no
   ```

   A partir de ONTAP 9.4, puede usar la `-enable-cc-mode yes` opción para solicitar que los usuarios introduzcan la frase de contraseña del administrador de claves después de un reinicio. Para NVE, si establece `-enable-cc-mode yes`, los volúmenes que cree con los `volume create` `volume move start` comandos y se cifran automáticamente.

   En el siguiente ejemplo, se inicia la configuración del gestor de claves en cluster1 sin necesidad de introducir la clave de acceso después de cada reinicio:

   ```
   cluster1::> security key-manager setup
   Welcome to the key manager setup wizard, which will lead you through
   the steps to add boot information.

   ...

   Would you like to use onboard key-management? {yes, no} [yes]:
   Enter the cluster-wide passphrase:    <32..256 ASCII characters long
   text>
   Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
   text>
   ```

2. Introduzca `yes` en el aviso para configurar la gestión de claves incorporada.
3. En el indicador de frase de contraseña, introduzca una frase de paso entre 32 y 256 caracteres, o bien, para "'cc-mode'", una frase de paso entre 64 y 256 caracteres.

Si la frase de paso "'cc-mode'" especificada es menor de 64 caracteres, hay un retraso de cinco segundos antes de que la operación de configuración del gestor de claves vuelva a mostrar la indicación de contraseña.

4. En la solicitud de confirmación de contraseña, vuelva a introducir la frase de contraseña.
5. Compruebe que las claves estén configuradas para todos los nodos:

   `security key-manager show-key-store`

   ```
   cluster1::> security key-manager show-key-store

   Node: node1
   Key Store: onboard
   Key ID                                                               Used By
   -------------------------------------------------------------------------
   --------
   <id_value> NSE-AK
   <id_value> NSE-AK

   Node: node2
   Key Store: onboard
   Key ID                                                               Used By
   -------------------------------------------------------------------------
   --------
   <id_value> NSE-AK
   <id_value> NSE-AK
   ```

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

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

   `volume encryption conversion start`

   Configure el administrador de claves integrado antes de convertir volúmenes. En entornos MetroCluster , configúrelo en ambos sitios.

Después de terminar

Copie la clave de acceso en una ubicación segura fuera del sistema de almacenamiento para usarla en el futuro.

Cuando configure la frase de contraseña del Onboard Key Manager, haga una copia de seguridad de la información en una ubicación segura fuera del sistema de almacenamiento en caso de desastre. Ver"Realice un backup manual de la información de gestión de claves incorporada" .

Información relacionada

- "Realice un backup manual de la información de gestión de claves incorporada"

- "Transición a la gestión de claves incorporada desde la gestión de claves externas"
- "administrador de claves de seguridad mostrar almacén de claves"

Habilitar la administración de claves integrada en los nodos ONTAP recién agregados

Puede usar el administrador de claves incorporado para proteger las claves que el clúster utiliza para acceder a los datos cifrados. Debe habilitar el gestor de claves incorporado en cada clúster que acceda a un volumen cifrado o un disco de autocifrado.

> Para ONTAP 9.6 y versiones posteriores, debe ejecutar el `security key-manager onboard sync` Este comando se ejecuta cada vez que se agrega un nodo al clúster.
>
> Para ONTAP 9, 5 y versiones anteriores, debe ejecutar `security key-manager setup` el comando cada vez que añada un nodo al clúster.
>
> Si agrega un nodo a un clúster con administración de claves incorporada, ejecute este comando para actualizar las claves faltantes.

Si tiene una configuración de MetroCluster, revise las siguientes directrices:

- A partir de ONTAP 9.6, se debe ejecutar `security key-manager onboard enable` primero en el clúster local y luego `security key-manager onboard sync` en el clúster remoto, utilizando la misma clave de acceso en cada uno.

  Obtenga más información sobre `security key-manager onboard enable` y `security key-manager onboard sync` en el "Referencia de comandos del ONTAP".

- En ONTAP 9.5, debe ejecutarse `security key-manager setup` en el clúster local y `security key-manager setup -sync-metrocluster-config yes` en el clúster remoto, con la misma clave de acceso en cada uno.
- Antes de usar ONTAP 9.5, debe ejecutarse `security key-manager setup` en el clúster local, esperar aproximadamente 20 segundos y, luego, ejecutarse `security key-manager setup` en el clúster remoto, usando la misma clave de acceso en cada uno.

De forma predeterminada, no es necesario introducir la clave de acceso del administrador de claves cuando se reinicia un nodo. A partir de ONTAP 9.4, puede usar la `-enable-cc-mode yes` opción para solicitar que los usuarios introduzcan la frase de acceso después de reiniciar.

Para NVE, si establece `-enable-cc-mode yes`, los volúmenes que cree con los `volume create` `volume move start` comandos y se cifran automáticamente. Para `volume create`, no es necesario especificar `-encrypt true`. Para `volume move start`, no es necesario especificar `-encrypt-destination true`.

> Si falla el intento de introducir la contraseña, reinicie el nodo. Tras reiniciar el sistema, puede intentar introducir la contraseña de nuevo.

Información relacionada

- "comandos de imagen de clúster"

- "Habilitación externa del administrador de claves de seguridad"
- "Habilitación integrada del administrador de claves de seguridad"