Configure el cifrado de volúmenes de NetApp

ONTAP 9

NetApp
April 24, 2024

Tabla de contenidos

Configure el cifrado de volúmenes de NetApp

Configure la información general de cifrado de volúmenes de NetApp

El cifrado de volúmenes de NetApp (NVE) es una tecnología basada en software para cifrar datos en reposo un volumen por vez. Una clave de cifrado a la que solo se puede acceder el sistema de almacenamiento garantiza que los datos de volumen no se puedan leer si el dispositivo subyacente se reasigna, se devuelve, se pierde o es robado.

Comprender NVE

Con NVE, tanto los metadatos como los datos (incluidas las copias Snapshot) están cifrados. El acceso a los datos se proporciona mediante una clave XTS-AES-256 exclusiva, una por volumen. Un servidor de gestión de claves externo o un gestor de claves incorporado (OKM) proporciona claves a los nodos:

- El 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). Se recomienda configurar servidores de gestión de claves externos a partir de sus datos en un sistema de almacenamiento diferente.
- El gestor de claves incorporado es una herramienta integrada que proporciona claves para nodos desde el mismo sistema de almacenamiento que los datos.

A partir de ONTAP 9.7, el cifrado de volúmenes y agregados se habilita de forma predeterminada si se dispone de una licencia de cifrado de volúmenes (ve) y se usa un gestor de claves incorporado o externo. La licencia VE se incluye con "ONTAP One". Siempre que se configure un gestor de claves externo o incorporado, habrá un cambio en el modo en que la configuración del cifrado de datos en reposo está establecida para los agregados y volúmenes totalmente nuevos. Los nuevos agregados tendrán activado de forma predeterminada el cifrado de agregados de NetApp (NAE). Los volúmenes nuevos que no forman parte de un agregado de NAE tendrán habilitado el cifrado de volúmenes de NetApp (NVE), de forma predeterminada. Si una máquina virtual de almacenamiento de datos (SVM) está configurada con su propio gestor de claves mediante la gestión de claves multi-tenant, el volumen creado para esa SVM se configura automáticamente con NVE.

Puede habilitar el cifrado en un volumen nuevo o existente. NVE es compatible con toda la gama de funciones de eficiencia del almacenamiento, incluidas la deduplicación y la compresión. A partir de ONTAP 9.14.1, puede hacerlo Habilite NVE en los volúmenes raíz de la SVM existentes.

> Si utiliza SnapLock, puede habilitar el cifrado solo en volúmenes de SnapLock nuevos y vacíos. No puede habilitar el cifrado en un volumen de SnapLock existente.

Es posible utilizar el NVE en cualquier tipo de agregado (HDD, SSD, híbrido, LUN de cabina), con cualquier tipo de RAID y en cualquier implementación de ONTAP compatible, incluido ONTAP Select. También puede utilizar NVE con cifrado basado en hardware para «doble cifrado» de datos en unidades con autocifrado.

Cuando NVE está habilitado, el volcado de memoria también se cifra.

Cifrado a nivel de agregado

Normalmente, a cada volumen cifrado se le asigna una clave única. Cuando se elimina el volumen, la clave se

elimina con él.

A partir de ONTAP 9.6, puede usar *NetApp Aggregate Encryption (NAE)* para asignar claves al agregado que contiene los volúmenes que se van a cifrar. Cuando se elimina un volumen cifrado, se conservan las claves del agregado. Las claves se eliminan si se elimina todo el agregado.

Debe utilizar el cifrado a nivel de agregado si tiene pensado realizar deduplicación en línea o en segundo plano a nivel de agregado. De lo contrario, NVE no admite la deduplicación a nivel de agregado.

A partir de ONTAP 9.7, el cifrado de volúmenes y agregados se habilita de forma predeterminada si se dispone de una licencia de cifrado de volúmenes (ve) y se usa un gestor de claves incorporado o externo.

Los volúmenes NVE y NAE pueden coexistir en el mismo agregado. Los volúmenes cifrados con el cifrado a nivel de agregado son, de forma predeterminada, los volúmenes NAE. Puede anular el valor predeterminado al cifrar el volumen.

Puede utilizar el `volume move` Comando para convertir un volumen NVE en un volumen NAE y viceversa. Es posible replicar un volumen NAE en un volumen NVE.

No puede utilizar `secure purge` Comandos en un volumen NAE.

Cuándo usar servidores de gestión de claves externos

Aunque es menos caro y, en general, más práctico para usar el gestor de claves incorporado, debe configurar los servidores KMIP si se da alguna de las siguientes situaciones:

- Su solución de gestión de claves de cifrado debe cumplir con el estándar de procesamiento de información federal (FIPS) 140-2 o el estándar KMIP DE OASIS.
- Necesita una solución de varios clústeres con gestión centralizada de las claves de cifrado.
- Su empresa requiere una seguridad añadida para almacenar claves de autenticación en un sistema o en una ubicación distinta de los datos.

Ámbito de la gestión de claves externas

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, se puede usar un *SVM Scope* para configurar la gestión de claves externas para una SVM con nombre 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.
- A partir de ONTAP 9.10.1, se puede utilizar Azure Key Vault y Google Cloud KMS Para proteger las claves NVE solo para SVM de datos. Está disponible para el KMS de AWS a partir de 9.12.0.

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.

Hay disponible una lista de los gestores de claves externos validados en la "Herramienta de matriz de interoperabilidad de NetApp (IMT)". Puede encontrar esta lista introduciendo el término «gestores clave» en la función de búsqueda de IMT.

Detalles de soporte

En la siguiente tabla se muestran los detalles de soporte de NVE:

Recurso o característica	Detalles de soporte
Plataformas	Se requiere capacidad de descarga de AES-ni. Consulte Hardware Universe (HWU) para verificar que NVE y NAE son compatibles con su plataforma.

Cifrado	A partir de ONTAP 9.7, los agregados y volúmenes recién creados se cifran de forma predeterminada cuando se añade una licencia de cifrado de volúmenes (ve) y se configura un gestor de claves externo o integrado. Si necesita crear un agregado no cifrado, utilice el siguiente comando:
	
	`storage aggregate create -encrypt-with-aggr-key false`
	
	Si necesita crear un volumen de texto sin formato, utilice el siguiente comando:
	
	`volume create -encrypt false`
	
	El cifrado no está activado de forma predeterminada si:
	
	• LA licencia VE no está instalada.
	• El gestor de claves no está configurado.
	• La plataforma o el software no admiten el cifrado.
	• El cifrado de hardware está activado.

ONTAP	Todas las implementaciones de ONTAP. La compatibilidad con ONTAP Cloud está disponible en ONTAP 9.5 y versiones posteriores.
Dispositivos	HDD, SSD, híbrido, LUN de cabina.
RAID	RAID0, RAID4, RAID-DP, RAID-TEC.
Volúmenes	Volúmenes de datos y volúmenes raíz de SVM existentes. No se pueden cifrar datos en volúmenes de metadatos de MetroCluster. En versiones de ONTAP anteriores a 9.14.1, no se pueden cifrar datos en el volumen raíz de la SVM con NVE. A partir de ONTAP 9.14.1, ONTAP admite NVE en volúmenes raíz de SVM.

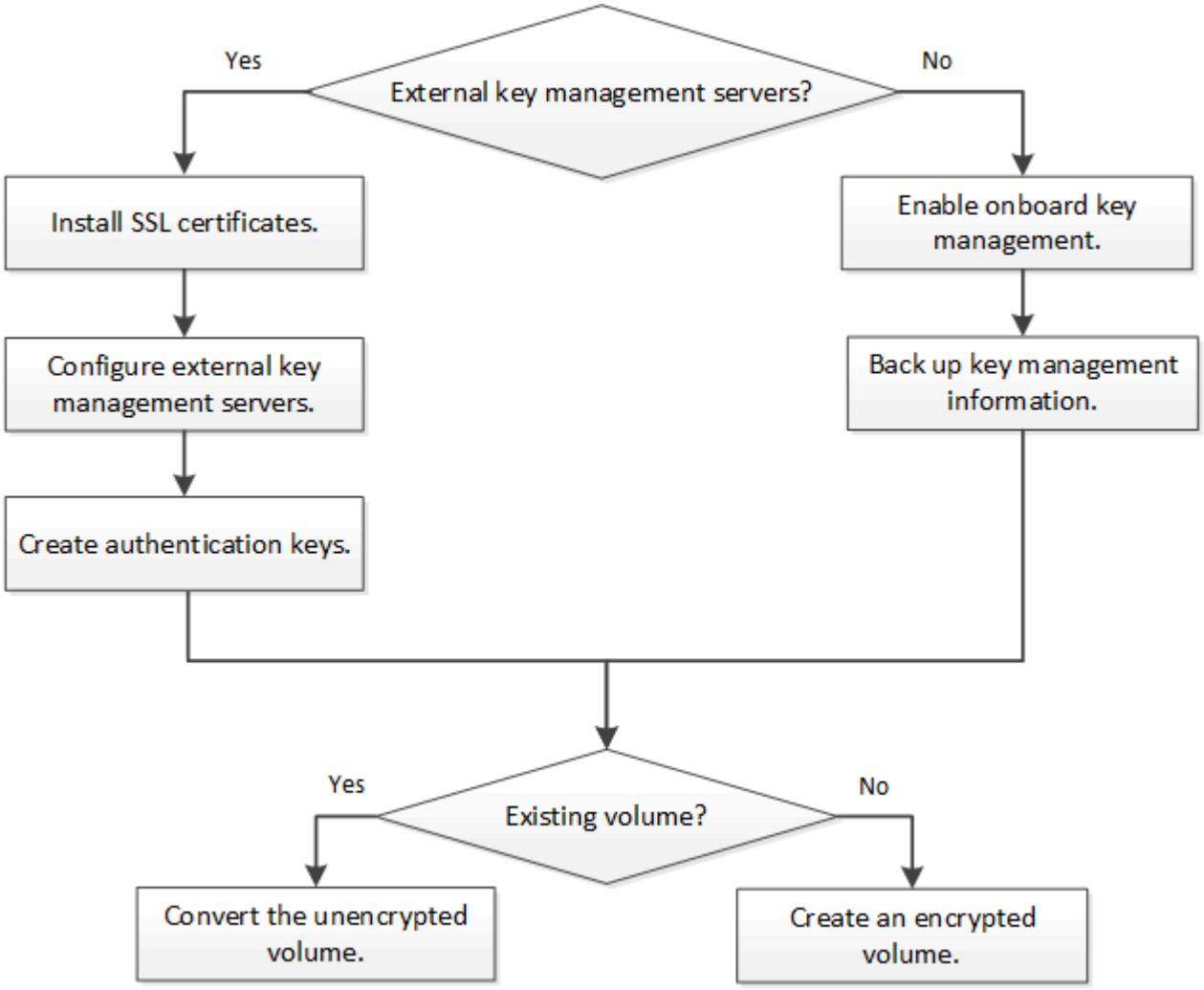
Cifrado a nivel de agregado	A partir de ONTAP 9.6, NVE admite el cifrado a nivel de agregado (NAE): • Debe utilizar el cifrado a nivel de agregado si tiene pensado realizar deduplicación en línea o en segundo plano a nivel de agregado. • No se puede volver a introducir la clave de un volumen de cifrado en el nivel de un agregado. • La opción de purga segura no es compatible con los volúmenes de cifrado a nivel de agregado. • Además de los volúmenes de datos, NAE admite el cifrado de volúmenes raíz de SVM y el volumen de metadatos de MetroCluster. NAE no admite el cifrado del volumen raíz.
Alcance de SVM	A partir de ONTAP 9.6, NVE admite el ámbito de SVM solo para la gestión de claves externas, no para el gestor de claves incorporado. MetroCluster es compatible a partir de ONTAP 9.8.
Eficiencia del almacenamiento	Deduplicación, compresión, compactación, FlexClone. Los clones utilizan la misma clave que el elemento principal, incluso después de dividir el clon del elemento principal. Debe realizar un `volume move` en un clon dividido, después del cual el clon dividido tendrá una clave diferente.
Replicación	• Para la replicación de volúmenes, los volúmenes de origen y destino pueden tener diferentes configuraciones de cifrado. El cifrado se puede configurar para el origen y sin configurar para el destino, y viceversa. • Para la replicación de SVM, el volumen de destino se cifra automáticamente, a menos que el destino no contenga un nodo compatible con el cifrado de volúmenes, en cuyo caso la replicación se realice correctamente, pero el volumen de destino no está cifrado. • Para las configuraciones de MetroCluster, cada clúster extrae claves de gestión de claves externas de sus servidores de claves configurados. El servicio de replicación de configuración replica las claves de OKM al sitio del partner.
Cumplimiento de normativas	A partir de ONTAP 9.2, SnapLock es compatible en los modos Compliance y Enterprise, sólo para nuevos volúmenes. No puede habilitar el cifrado en un volumen de SnapLock existente.
FlexGroups	A partir de ONTAP 9.2, los FlexGroup son compatibles. Los agregados de destino deben tener el mismo tipo que los agregados de origen, ya sea a nivel de volumen o de agregado. A partir de ONTAP 9.5, se admite la reclave sin movimiento de volúmenes FlexGroup.
Transición de 7-Mode	A partir de 7-Mode Transition Tool 3.3, puede utilizar la CLI de 7-Mode Transition Tool para realizar una transición basada en copias a los volúmenes de destino habilitados para NVE en el sistema en clúster.

Información relacionada

"Preguntas más frecuentes: Cifrado de volúmenes de NetApp y cifrado de agregados de NetApp"

Flujo de trabajo de cifrado de volúmenes de NetApp

Es necesario configurar servicios de gestión de claves para poder habilitar el cifrado de volúmenes. Puede habilitar el cifrado en un volumen nuevo o en uno existente.



"Debe instalar la licencia VE" Y configure los servicios de gestión de claves antes de poder cifrar datos con NVE. Antes de instalar la licencia, debería "Determine si la versión de ONTAP es compatible con NVE".

Configure NVE

Determine si la versión del clúster es compatible con NVE

Debe determinar si la versión de clúster es compatible con NVE antes de instalar la licencia. Puede utilizar 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.

Paso

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

   `version -v`

   NVE no es compatible si el resultado del comando muestra el texto «'1Ono-DARE» (del cifrado «no de datos en reposo») o si utiliza una plataforma que no aparezca en la "Detalles de soporte".

   El siguiente comando determina si se admite NVE a. `cluster1`.

   ```
   cluster1::> version -v
   NetApp Release 9.1.0: Tue May 10 19:30:23 UTC 2016 <1Ono-DARE>
   ```

   El resultado de `1Ono-DARE` Indica que la versión del clúster no es compatible con NVE.

Instale la licencia

Una licencia ve le permite usar la función en todos los nodos del clúster. Esta licencia es necesaria para poder cifrar datos con NVE. Se incluye 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 obligatorio, los clientes existentes pueden optar por hacerlo "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 licencia 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

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"

Habilitar la gestión de claves incorporada en ONTAP 9.6 y versiones posteriores (NVE)

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 el `security key-manager onboard sync` cada vez que añada un nodo al clúster.

Si tiene una configuración MetroCluster, debe ejecutar el `security key-manager onboard enable` primero en el clúster local y, a continuación, ejecute el `security key-manager onboard sync` en el clúster remoto, utilizando la misma clave de acceso en cada uno. Cuando ejecute el `security key-manager onboard enable` del clúster local y, a continuación, sincronice en el clúster remoto, no es necesario ejecutar el `enable` comando de nuevo desde el clúster remoto.

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

Para NVE, si estableció `cc-mode-enabled=yes`, volúmenes creados con `volume create` y.. `volume move start` los comandos 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 de ONTAP en reposo, para cumplir los requisitos de las soluciones comerciales para la clasificación (CSfC), debe usar NSE con NVE y asegurarse de que el gestor de claves incorporado esté habilitado en modo de criterios comunes. Consulte la "Breve descripción de la solución CSfC" Para obtener más información sobre CSfC.

Cuando el gestor de claves incorporado se habilita en el modo de criterios comunes (`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 puede introducir la clave de acceso del clúster correcta en el arranque, los volúmenes cifrados no se montan. Para corregir esto, debe reiniciar el nodo e introducir la clave de acceso del clúster correcta. Una vez arrancado, el sistema permite 5 introducir correctamente la clave de acceso del clúster en un periodo de 24 horas para cualquier comando que requiera la clave de acceso del clúster como parámetro. Si se alcanza el límite (por ejemplo, no ha podido introducir correctamente la clave de acceso del clúster 5 veces en una fila), debe esperar al tiempo de espera de 24 horas o reiniciar 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 upgrade verifica que el contenido de la imagen no se ha alterado o dañado comprobando varias firmas digitales. El proceso de actualización de imágenes continúa con el paso siguiente si la validación se realiza correctamente; de lo contrario, la actualización de la imagen falla. Consulte `cluster image` página del comando man para obtener información sobre las actualizaciones del sistema.

El gestor de claves incorporado almacena claves en la memoria volátil. El contenido de la memoria volátil se borra al reiniciar o detener el sistema. En condiciones normales de funcionamiento, el contenido de la memoria volátil se borrará en un plazo de 30 segundos cuando se pare un sistema.

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
   ```

> Configurado `cc-mode-enabled=yes` para solicitar que los usuarios introduzcan la frase de acceso del administrador de claves después de un reinicio. Para NVE, si estableció `cc-mode-enabled=yes`, volúmenes creados con `volume create` y.. `volume move start` los comandos se cifran automáticamente. La `- cc-mode-enabled` La opción no es compatible con las configuraciones de MetroCluster. La `security key-manager onboard enable` el comando sustituye al `security key-manager setup` comando.

En el siguiente ejemplo, se inicia el comando key Manager setup en cluster1 sin necesidad de introducir la frase de contraseña después de cada reinicio:

```
cluster1::> security key-manager onboard enable

Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1"::    <32..256 ASCII characters long text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. 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.

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
```

> 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 ejemplo siguiente verifica para qué se han creado claves de autenticación `cluster1`:

```
cluster1::> security key-manager key query -key-type NSE-AK
               Node: node1
            Vserver: cluster1
        Key Manager: onboard
   Key Manager Type: OKM
 Key Manager Policy: -

 Key Tag                                Key Type Encryption   Restored

-----------------------------------  -------- ------------ --------

node1                                 NSE-AK   AES-256      true

    Key ID:
00000000000000000200000000000100056178fc6ace6d91472df8a9286daacc00000000
00000000

node1                                 NSE-AK   AES-256      true

    Key ID:
00000000000000000200000000000100df1689a148fdfbf9c2b198ef974d0baa00000000
00000000

2 entries were displayed.
```

5. Opcionalmente, convierta volúmenes de texto sin formato 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.

Siempre que configure la clave de acceso de Onboard Key Manager, también debe realizar un backup manual de la información en una ubicación segura fuera del sistema de almacenamiento para usarla en caso de desastre. Consulte "Realice un backup manual de la información de gestión de claves incorporada".

Habilitar la gestión de claves incorporada en ONTAP 9.5 y versiones anteriores (NVE)

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 el `security key-manager setup` cada vez que añada un nodo al clúster.

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

- En ONTAP 9.5, debe ejecutar `security key-manager setup` en el clúster local y. `security key-manager setup -sync-metrocluster-config yes` en el clúster remoto, utilizando la misma clave de acceso en cada uno.
- Antes de ONTAP 9.5, debe ejecutar `security key-manager setup` en el clúster local, espere aproximadamente 20 segundos y después ejecute `security key-manager setup` en el clúster remoto, utilizando 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 utilizar el `-enable-cc-mode yes` opción para solicitar que los usuarios introduzcan la frase de contraseña después de un reinicio.

Para NVE, si estableció `-enable-cc-mode yes`, volúmenes creados con `volume create` y.. `volume move start` los comandos 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 gestión de claves externa (KMIP), debe haber eliminado la base de datos del gestor 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.
- 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 setup -enable-cc-mode yes|no
   ```

   > A partir de ONTAP 9,4, puede utilizar el `-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 estableció `-enable-cc-mode yes`, volúmenes creados con `volume create` y.. `volume move start` los comandos 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 símbolo del sistema de para configurar la gestión integrada de claves.
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 key show`

   Para obtener la sintaxis completa del comando, consulte la página man.

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

Node: node1
Key Store: onboard
Key ID                                                                   Used By
-----------------------------------------------------------------------
--------
00000000000000000200000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
00000000000000000200000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                                   Used By
-----------------------------------------------------------------------
--------
00000000000000000200000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
00000000000000000200000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

6. Opcionalmente, convierta volúmenes de texto sin formato 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.

Siempre que configure la clave de acceso de Onboard Key Manager, también debe realizar un backup manual de la información en una ubicación segura fuera del sistema de almacenamiento para usarla en caso de desastre. Consulte "Realice un backup manual de la información de gestión de claves incorporada".

Habilite la gestión de claves incorporada en los nodos recién añadidos

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 9.5 y versiones anteriores, debe ejecutar el `security key-manager setup` cada vez que añada un nodo al clúster.
>
> Para ONTAP 9.6 y versiones posteriores, debe ejecutar el `security key-manager sync` cada vez que añada un nodo al clúster.
>
> Si añade un nodo a un clúster que tiene configurada la gestión de claves integrada, este comando se ejecutará para actualizar las claves que faltan.

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

- A partir de ONTAP 9.6, debe ejecutar `security key-manager onboard enable` en el clúster local primero y después ejecute `security key-manager onboard sync` en el clúster remoto, utilizando la misma clave de acceso en cada uno.
- En ONTAP 9.5, debe ejecutar `security key-manager setup` en el clúster local y. `security key-manager setup -sync-metrocluster-config yes` en el clúster remoto, utilizando la misma clave de acceso en cada uno.
- Antes de ONTAP 9.5, debe ejecutar `security key-manager setup` en el clúster local, espere aproximadamente 20 segundos y después ejecute `security key-manager setup` en el clúster remoto, utilizando 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 utilizar el `-enable-cc-mode yes` opción para solicitar que los usuarios introduzcan la frase de contraseña después de un reinicio.

Para NVE, si estableció `-enable-cc-mode yes`, volúmenes creados con `volume create` y.. `volume move start` los comandos 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.

Cifre datos de volúmenes con NVE

Cifre datos de volúmenes con la información general de NVE

A partir de ONTAP 9.7, el cifrado de volúmenes y agregados se habilita de forma predeterminada cuando se dispone de la licencia ve y la gestión de claves interna o externa. Para ONTAP 9.6 y versiones anteriores, es posible habilitar el cifrado en un volumen nuevo o en uno existente. Debe haber instalado la licencia ve y haber habilitado la gestión de claves para poder habilitar el cifrado de volúmenes. NVE es conforme a la normativa FIPS-140-2 de nivel 1.

Habilite el cifrado a nivel de agregado con la licencia ve

A partir de ONTAP 9,7, los agregados y volúmenes recién creados se cifran de forma predeterminada cuando tenga el "LICENCIA VE" o la gestión de claves externas o incorporadas. A partir de ONTAP 9.6, puede utilizar el cifrado a nivel de agregado para asignar claves al agregado que contiene para los volúmenes que se van a cifrar.

Acerca de esta tarea

Debe utilizar el cifrado a nivel de agregado si tiene pensado realizar deduplicación en línea o en segundo plano a nivel de agregado. De lo contrario, NVE no admite la deduplicación a nivel de agregado.

Un agregado habilitado para el cifrado a nivel de agregado se denomina agregado *NAE* (para el cifrado de agregados de NetApp). Todos los volúmenes de un agregado de NAE deben estar cifrados con NAE o NVE. Con el cifrado a nivel de agregado, los volúmenes que cree en el agregado se cifran de forma predeterminada con el cifrado NAE. Puede anular el valor predeterminado para utilizar el cifrado NVE en su lugar.

No se admiten volúmenes de texto sin formato en los agregados de la NAE.

Antes de empezar

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

Pasos

1. Habilite o deshabilite el cifrado de nivel de agregado:

Para…	Se usa este comando…
Cree un agregado de NAE con ONTAP 9.7 o posterior	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`*
Cree un agregado de NAE con ONTAP 9.6	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`

Convertir un agregado que no sea NAE en un agregado de NAE	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
Convertir un agregado de NAE en un agregado que no sea NAE	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key false`

Para obtener una sintaxis de comando completa, consulte las páginas man.

El siguiente comando habilita el cifrado a nivel de agregado para `aggr1`:

- ONTAP 9.7 o posterior:

```
cluster1::> storage aggregate create -aggregate aggr1
```

- ONTAP 9.6 o anterior:

```
cluster1::> storage aggregate create -aggregate aggr1 -encrypt-with
-aggr-key true
```

2. Compruebe que el agregado está habilitado para el cifrado:

   `storage aggregate show -fields encrypt-with-aggr-key`

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

   El siguiente comando lo verifica `aggr1` está habilitado para el cifrado:

```
cluster1::> storage aggregate show -fields encrypt-with-aggr-key
aggregate            encrypt-aggr-key
-------------------- ----------------
aggr0_vsim4          false
aggr1                true
2 entries were displayed.
```

Después de terminar

Ejecute el `volume create` comando para crear los volúmenes cifrados.

Si utiliza un servidor KMIP para almacenar las claves de cifrado de un nodo, ONTAP inserta automáticamente una clave de cifrado en el servidor al cifrar un volumen.

Habilite el cifrado en un nuevo volumen

Puede utilizar el `volume create` comando para habilitar el cifrado en un volumen nuevo.

Acerca de esta tarea

Puede cifrar volúmenes con el cifrado de volúmenes de NetApp (NVE) y, para comenzar con ONTAP 9.6, el cifrado de agregados de NetApp (NAE). Para obtener más información sobre NAE y NVE, consulte información general de cifrado de volúmenes.

El procedimiento para habilitar el cifrado en un nuevo volumen en ONTAP varía en función de la versión de ONTAP que esté usando y su configuración específica:

- A partir de ONTAP 9.4, si se habilita `cc-mode` Cuando se configura el gestor de claves incorporado, los volúmenes que se crean con el `volume create` el comando se cifra automáticamente, tanto si se especifica como si no `-encrypt true`.
- En ONTAP 9.6 y versiones anteriores, es necesario utilizar `-encrypt true` con `volume create` comandos para habilitar el cifrado (siempre que no se haya habilitar `cc-mode`).
- Si desea crear un volumen NAE en ONTAP 9.6, debe habilitar NAE en el nivel de agregado. Consulte Habilite el cifrado a nivel de agregado con la licencia ve para obtener más detalles sobre esta tarea.
- A partir de ONTAP 9,7, los volúmenes recién creados se cifran de forma predeterminada cuando el "LICENCIA VE" o la gestión de claves externas o incorporadas. De forma predeterminada, los nuevos volúmenes que se crean en un agregado de NAE serán del tipo NAE en lugar de NVE.
  - Si añade, en ONTAP 9.7 y versiones posteriores `-encrypt true` para la `volume create` Comando para crear un volumen en un agregado de NAE, el volumen tendrá el cifrado NVE en lugar de NAE. Todos los volúmenes de un agregado de NAE deben estar cifrados con NVE o NAE.

> No se admiten los volúmenes de texto sin formato en los agregados de NAE.

Pasos

1. Cree un volumen nuevo y especifique si el cifrado está habilitado en el volumen. Si el nuevo volumen se encuentra en un agregado de NAE, de forma predeterminada el volumen será un volumen de NAE:

Para crear…	Se usa este comando…
Un volumen NAE	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`*
Un volumen de NVE	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt true` + En ONTAP 9.6 y versiones anteriores en las que NAE no es compatible, `-encrypt true` Especifica que el volumen se debe cifrar con NVE. En ONTAP 9.7 y posteriores, donde se crean volúmenes en agregados de NAE, `-encrypt true` Reemplaza el tipo de cifrado predeterminado de NAE para crear un volumen NVE en su lugar.

Un volumen de texto sin formato	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt false`

Para obtener la sintaxis completa del comando, consulte la página de referencia de comandos de LINK:https://docs.netapp.com/us-en/ontap-cli-9141/volume-create.html[`volume create`#].

2. Compruebe que los volúmenes estén habilitados para el cifrado:

   ```
   volume show -is-encrypted true
   ```

   Para obtener una sintaxis completa del comando, consulte "referencia de comandos".

Resultado

Si utiliza un servidor KMIP para almacenar las claves de cifrado de un nodo, ONTAP "inserta automáticamente" una clave de cifrado en el servidor cuando se cifra un volumen.

=
:allow-uri-read:

Habilite el cifrado en un volumen existente

Puede utilizar cualquiera de los dos `volume move start` o la `volume encryption conversion start` comando para habilitar el cifrado en un volumen existente.

Acerca de esta tarea

- A partir de ONTAP 9.3, puede utilizar la `volume encryption conversion start` comando para habilitar el cifrado de un volumen existente «in situ», sin necesidad de mover el volumen a otra ubicación. Como alternativa, puede utilizar el `volume move start` comando.
- Para ONTAP 9,2 y versiones anteriores, solo puede utilizar el `volume move start` comando para habilitar el cifrado mediante el movimiento de un volumen existente.

Habilite el cifrado en un volumen existente con el comando volume Encryption conversion start

A partir de ONTAP 9.3, puede utilizar la `volume encryption conversion start` comando para habilitar el cifrado de un volumen existente «in situ», sin necesidad de mover el volumen a otra ubicación.

Después de iniciar una operación de conversión, debe completarse. Si se encuentra con un problema de rendimiento durante la operación, puede ejecutar el `volume encryption conversion pause` para pausar la operación y el `volume encryption conversion resume` comando para reanudar la operación.

> No puede utilizar `volume encryption conversion start` Para convertir un volumen de SnapLock.

Pasos

1. Habilitar el cifrado en un volumen existente:

   ```
   volume encryption conversion start -vserver SVM_name -volume volume_name
   ```

   Para obtener información sobre la sintaxis de toda el comando, consulte la página man del comando.

El siguiente comando habilita el cifrado en el volumen existente `vol1`:

```
cluster1::> volume encryption conversion start -vserver vs1 -volume vol1
```

El sistema crea una clave de cifrado para el volumen. Los datos del volumen se cifran.

2. Compruebe el estado de la operación de conversión:

   `volume encryption conversion show`

   Para obtener información sobre la sintaxis de toda el comando, consulte la página man del comando.

   El siguiente comando muestra el estado de la operación de conversión:

```
cluster1::> volume encryption conversion show

Vserver   Volume   Start Time           Status
-------   ------   ------------------   ---------------------------
vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
```

3. Cuando finalice la operación de conversión, compruebe que el volumen esté habilitado para el cifrado:

   `volume show -is-encrypted true`

   Para obtener información sobre la sintaxis de toda el comando, consulte la página man del comando.

   El siguiente comando muestra los volúmenes cifrados en `cluster1`:

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  --------- ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Resultado

Si utiliza un servidor KMIP para almacenar las claves de cifrado de un nodo, ONTAP inserta automáticamente una clave de cifrado en el servidor al cifrar un volumen.

Habilite el cifrado en un volumen existente con el comando volume Move start

Puede utilizar el `volume move start` comando para habilitar el cifrado mediante el movimiento de un volumen existente. Debe usar `volume move start` En ONTAP 9.2 y anteriores. Se puede usar el mismo agregado o uno diferente.

Acerca de esta tarea

- A partir de ONTAP 9.8, se puede utilizar `volume move start` Para habilitar el cifrado en un volumen de

SnapLock o FlexGroup.

- A partir de ONTAP 9.4, si activa "'cc-mode'" cuando configura el Administrador de claves incorporado, los volúmenes que crea con el `volume move start` el comando se cifra automáticamente. No es necesario que especifique `-encrypt-destination true`.
- A partir de ONTAP 9.6, puede utilizar el cifrado a nivel de agregado con el fin de asignar claves al agregado que contiene para mover los volúmenes. Un volumen cifrado con una clave única se denomina *NVE volume* (lo que significa que utiliza cifrado de volúmenes de NetApp). Un volumen cifrado con una clave de nivel de agregado se denomina *NAE volume* (para el cifrado de agregados de NetApp). No se admiten los volúmenes de texto sin formato en los agregados de NAE.
- A partir de ONTAP 9.14.1, se puede cifrar un volumen raíz de SVM con NVE. Para obtener más información, consulte Configure el cifrado de volúmenes NetApp en un volumen raíz de SVM.

Antes de empezar

Debe ser un administrador de clústeres para realizar esta tarea o un administrador de SVM a quien el administrador de clúster haya delegado esta autoridad.

"Delegar la autoridad para ejecutar el comando volume move"

Pasos

1. Mueva un volumen existente y especifique si el cifrado está habilitado en el volumen:

Para convertir…	Se usa este comando…
Un volumen de texto sin formato a un volumen NVE	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination true`
Un volumen NVE o un volumen sin texto en un volumen NAE (suponiendo que se habilite el cifrado a nivel de agregado en el destino)	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-with-aggr-key true`
Un volumen NAE a un volumen NVE	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-with-aggr-key false`
Volumen NAE a un volumen de texto sin formato	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination false -encrypt-with-aggr-key false`
Un volumen NVE a un volumen de texto sin texto	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination false`

Para obtener información sobre la sintaxis de toda el comando, consulte la página man del comando.

El siguiente comando convierte un volumen de texto sin formato denominado `vol1` Para un volumen NVE:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-destination true
```

Si asumimos que el cifrado a nivel de agregado está habilitado en el destino, el siguiente comando convierte un volumen NVE o de texto sin formato denominado `vol1` A un volumen de NAE:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-with-aggr-key true
```

El siguiente comando convierte un volumen NAE llamado `vol2` Para un volumen NVE:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-with-aggr-key false
```

El siguiente comando convierte un volumen NAE llamado `vol2` a un volumen de texto sin formato:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false -encrypt-with-aggr-key false
```

El siguiente comando convierte un volumen de NVE llamado `vol2` a un volumen de texto sin formato:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false
```

2. Vea el tipo de cifrado de volúmenes de clúster:

   `volume show -fields encryption-type none|volume|aggregate`

   La `encryption-type` Campo está disponible en ONTAP 9.6 y versiones posteriores.

   Para obtener información sobre la sintaxis de toda el comando, consulte la página man del comando.

   El siguiente comando muestra el tipo de cifrado de volúmenes en `cluster2`:

```
cluster2::> volume show -fields encryption-type

vserver  volume  encryption-type
-------  ------  ---------------
vs1      vol1    none
vs2      vol2    volume
vs3      vol3    aggregate
```

3. Compruebe que los volúmenes estén habilitados para el cifrado:

   `volume show -is-encrypted true`

   Para obtener información sobre la sintaxis de toda el comando, consulte la página man del comando.

   El siguiente comando muestra los volúmenes cifrados en `cluster2`:

```
cluster2::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  --------- ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Resultado

Si utiliza un servidor KMIP para almacenar las claves de cifrado de un nodo, ONTAP inserta automáticamente una clave de cifrado en el servidor cuando se cifra un volumen.

Configure el cifrado de volúmenes NetApp en un volumen raíz de SVM

A partir de ONTAP 9.14.1, puede habilitar el cifrado de volúmenes de NetApp (NVE) en un volumen raíz de una máquina virtual de almacenamiento (SVM). Con NVE, el volumen raíz se cifra con una clave única, lo que permite una mayor seguridad en la SVM.

Acerca de esta tarea

NVE en un volumen raíz de SVM solo se puede habilitar una vez que se creó la SVM.

Antes de empezar

- El volumen raíz de SVM no debe estar en un agregado cifrado con el cifrado de agregados de NetApp (NAE).
- Debe haber habilitado el cifrado con el administrador de claves incorporado o un gestor de claves externo.
- Debe ejecutar ONTAP 9.14.1 o una versión posterior.
- Para migrar una SVM que contiene un volumen raíz cifrado con NVE, debe convertir el volumen raíz de la SVM en un volumen de texto sin formato una vez finalizada la migración y, luego, volver a cifrar el volumen raíz de la SVM.
  - Si el agregado de destino de la migración de SVM utiliza NAE, el volumen raíz hereda NAE de manera predeterminada.
- Si la SVM está en una relación de recuperación ante desastres de SVM:
  - La configuración de cifrado en una SVM reflejada no se copia en el destino. Si habilita NVE en el origen o destino, debe habilitar por separado NVE en el volumen raíz de la SVM reflejada.
  - Si todos los agregados del clúster de destino utilizan NAE, el volumen raíz de SVM utilizará NAE.

Pasos

Puede habilitar NVE en un volumen raíz de SVM con la interfaz de línea de comandos de ONTAP o System Manager.

CLI

Puede habilitar NVE en el volumen raíz de la SVM sin movimiento o mediante el movimiento del volumen entre agregados.

Cifre el volumen raíz en su lugar

1. Convierta el volumen raíz en un volumen de cifrado:

   ```
   volume encryption conversion start -vserver svm_name -volume volume
   ```

2. Confirme que el cifrado se ha realizado correctamente. La `volume show -encryption-type volume` Muestra una lista de todos los volúmenes con NVE.

Cifre el volumen raíz de la SVM al moverlo

1. Inicie un movimiento de volumen:

   ```
   volume move start -vserver svm_name -volume volume -destination-aggregate
   aggregate -encrypt-with-aggr-key false -encrypt-destination true
   ```

   Para obtener más información acerca de `volume move`, consulte Mover un volumen.

2. Confirme el `volume move` la operación se ha realizado correctamente con el `volume move show` comando. La `volume show -encryption-type volume` Muestra una lista de todos los volúmenes con NVE.

System Manager

1. Navegue hasta **Almacenamiento** > **Volúmenes**.
2. Junto al nombre del volumen raíz de la SVM que desea cifrar, seleccione ⋮ Luego **Editar**.
3. En el encabezado **Almacenamiento y optimización**, seleccione **Activar cifrado**.
4. Selecciona **Guardar**.

Habilite el cifrado de volumen raíz del nodo

A partir de ONTAP 9.8, puede usar el cifrado de volúmenes de NetApp para proteger el volumen raíz del nodo.

Acerca de esta tarea

Este procedimiento se aplica al volumen raíz del nodo. No se aplica a los volúmenes raíz de SVM. Los volúmenes raíz de SVM se pueden proteger mediante cifrado a nivel de agregado y A partir de ONTAP 9.14.1, NVE.

Una vez que se inicia el cifrado del volumen raíz, se debe completar. No puede pausar la operación. Una vez completado el cifrado, no puede asignar una nueva clave al volumen raíz y no puede ejecutar una operación de purga segura.

Antes de empezar

- Su sistema debe utilizar una configuración de alta disponibilidad.
- Se debe crear el volumen raíz del nodo.

- El sistema debe tener un administrador de claves incorporado o un servidor de gestión de claves externo mediante el protocolo de interoperabilidad de gestión de claves (KMIP).

Pasos

1. Cifre el volumen raíz:

   ```
   volume encryption conversion start -vserver SVM_name -volume root_vol_name
   ```

2. Compruebe el estado de la operación de conversión:

   ```
   volume encryption conversion show
   ```

3. Una vez completada la operación de conversión, compruebe que el volumen esté cifrado:

   ```
   volume show -fields
   ```

   El siguiente ejemplo muestra el resultado de un volumen cifrado.

   ```
   ::> volume show -vserver xyz  -volume vol0 -fields is-encrypted
   vserver    volume is-encrypted
   ---------- ------ ------------
   xyz        vol0   true
   ```