Gestione el cifrado con la interfaz de línea de comandos

ONTAP 9

NetApp
February 12, 2026

Tabla de contenidos

Gestione el cifrado con la interfaz de línea de comandos

Obtenga más información sobre el cifrado de datos en reposo de ONTAP

NetApp ofrece tecnologías de cifrado basadas en software y hardware para garantizar que los datos en reposo no se puedan leer en caso de reasignación, devolución, pérdida o robo del medio de almacenamiento.

- El cifrado basado en software con el cifrado de volúmenes de NetApp (NVE) admite el cifrado de datos de un volumen por vez
- El cifrado basado en hardware con el cifrado del almacenamiento de NetApp (NSE) admite el cifrado de disco completo (FDE) de los datos a medida que se escriben.

Configurar el volumen de NetApp y el cifrado agregado

Obtenga más información sobre el cifrado de volumen y agregados de ONTAP 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. Comenzando con ONTAP 9.14,1, usted puede 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 usar `volume move` el comando para convertir un volumen NVE en un volumen de NAE y viceversa. Es posible replicar un volumen NAE en un volumen NVE.

No se pueden 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 9.17.1, puede utilizar Barbican KMS para proteger las claves NVE solo para SVM de datos.
  - A partir de ONTAP 9.10,1, puede utilizar Azure Key Vault y Google Cloud KMS para proteger las claves de NVE solo para las 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 gestores de claves externos validados en la "Herramienta de matriz de interoperabilidad de NetApp (IMT)". Para encontrar esta lista, se debe introducir el término "administradores de claves" en la función de búsqueda de IMT.

Los proveedores de KMS de cloud, como Azure Key Vault y AWS KMS, no son compatibles con KMIP. Como resultado, no aparecen en 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 Cloud Volumes ONTAP 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	MetroCluster es compatible a partir de ONTAP 9.8. A partir de ONTAP 9.6, NVE admite el alcance SVM solo para la administración de claves externas, no para el administrador de claves integrado.
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` clon en una división, después del cual el clon dividido tendrá una clave diferente.

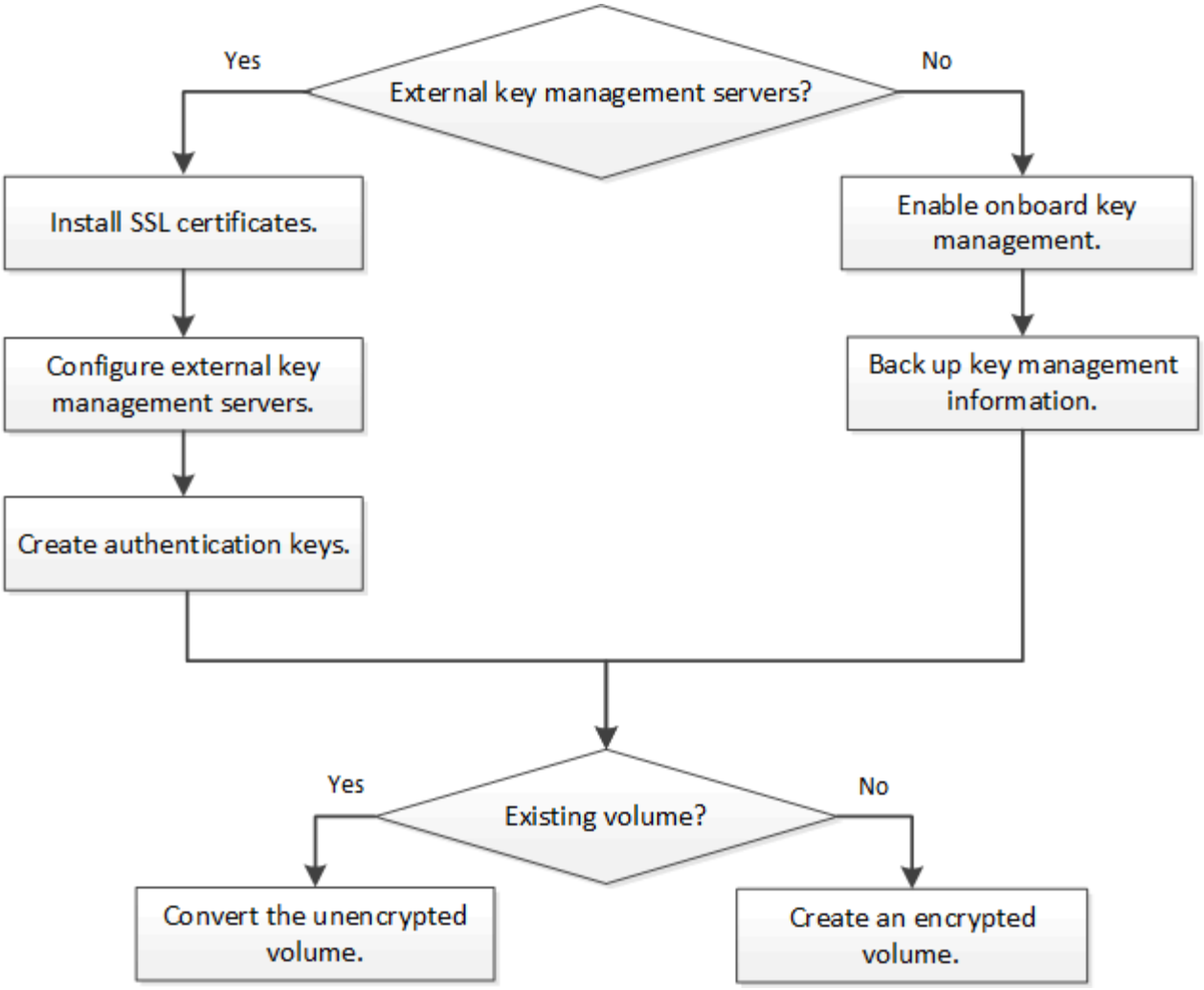
Replicación	• Para la replicación de volúmenes, los volúmenes de origen y destino pueden tener diferentes configuraciones de cifrado. El cifrado se puede configurar para el origen y sin configurar para el destino, y viceversa. El cifrado configurado en el origen no se replicará en el destino. El cifrado debe configurarse manualmente en el origen y el destino. Consulte Configurar NVEy.Cifre datos de volúmenes con NVE • 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	SnapLock es compatible con los modos Cumplimiento y Empresa, únicamente para volúmenes nuevos. No puede habilitar el cifrado en un volumen de SnapLock existente.
Volúmenes de FlexGroup	Se admiten volúmenes FlexGroup . 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"
- "creación de agregados de almacenamiento"

Flujo de trabajo de cifrado de volumen de ONTAP 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, debe "Determine si la versión de ONTAP es compatible con NVE".

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:

   ```
   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 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"

Cifrar datos de volumen con NVE o NAE

Obtenga información sobre el cifrado de datos de volumen de ONTAP con 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 licencia VE en ONTAP

A partir de ONTAP 9.7, los agregados y los volúmenes recién creados se cifran de forma predeterminada cuando dispone de "LICENCIA VE"la gestión de claves externa o incorporada. 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`

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

El siguiente comando activa el cifrado a nivel de agregado en `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
```

Obtenga más información sobre `storage aggregate create` en el "Referencia de comandos del ONTAP".

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

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

El siguiente comando verifica que `aggr1` está activado 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.
```

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

Después de terminar

Ejecute `volume create` el 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 en ONTAP

Puede usar `volume create` el 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 volúmenesel .

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

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` al configurar el Administrador de claves integrado, los volúmenes que se crean con el `volume create` comando se cifran automáticamente, independientemente de si se especifica o no `-encrypt true` .
- En ONTAP 9.6 y versiones anteriores, debe utilizar `-encrypt true` `volume create` los comandos WITH para activar el cifrado (siempre que no se haya activado `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 vepara obtener más detalles sobre esta tarea.
- A partir de ONTAP 9.7, los volúmenes recién creados se cifran de forma predeterminada cuando se cuenta con "LICENCIA VE"la gestión de claves externa o incorporada. De forma predeterminada, los nuevos volúmenes que se crean en un agregado de NAE serán del tipo NAE en lugar de NVE.
  - En ONTAP 9 Intersight 7 y versiones posteriores, si agrega `-encrypt true` al `volume create` comando para crear un volumen en un agregado de NAE, el volumen tendrá 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 de 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, etc. 6 y versiones anteriores, donde no se admite NAE, `-encrypt true` especifica que el volumen debe cifrarse con NVE. En ONTAP 9, 7 y versiones posteriores, en las que se crean volúmenes en agregados de NAE, `-encrypt true` se anula el tipo de cifrado predeterminado de NAE para crear un volumen de NVE.

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

Obtenga más información sobre `volume create` en el "Referencia de comandos del ONTAP".

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

   `volume show -is-encrypted true`

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

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.

Habilitar NAE o NVE en un volumen ONTAP existente

Puede utilizar el `volume move start` `volume encryption conversion start` comando o el comando para habilitar el cifrado en un volumen existente.

Acerca de esta tarea

Puedes utilizar el `volume encryption conversion start` Comando para habilitar el cifrado de un volumen existente "in situ", sin tener que moverlo a otra ubicación. Alternativamente, puede usar el comando `volume move start` dominio.

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

Puedes utilizar el `volume encryption conversion start` comando para habilitar el cifrado de un volumen existente "en su lugar", sin tener que mover el volumen a una ubicación diferente.

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

> No se puede usar `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`

   Obtenga más información sobre `volume encryption conversion start` en el "Referencia de comandos del ONTAP".

   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`

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

   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`

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

   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 usar el `volume move start` comando para habilitar el cifrado mediante la transferencia de un volumen existente. Se puede usar el mismo agregado o uno diferente.

Acerca de esta tarea

- A partir de ONTAP 9.8, se puede usar `volume move start` para habilitar el cifrado en un volumen SnapLock o FlexGroup.
- A partir de ONTAP 9.4, si habilita «`cc-mode`» al configurar el Administrador de claves integrado, los volúmenes que cree con el `volume move start` comando se cifran automáticamente. No es necesario especificar `-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`
Un volumen NAE a un volumen de texto sin texto	`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`

Obtenga más información sobre `volume move start` en el "Referencia de comandos del ONTAP".

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

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

Suponiendo 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` en un volumen NAE:

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

El siguiente comando convierte un volumen de NAE llamado `vol2` en 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 denominado `vol2` en 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 NVE llamado `vol2` en 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`

   ```
   `encryption-type`El campo está disponible en ONTAP 9.6 y posterior.
   ```

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

   El siguiente comando muestra el tipo de cifrado de los 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
```

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

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.

Configurar NVE en un volumen raíz SVM de ONTAP

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. El `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`

   Obtenga más información sobre `volume move` en el "Referencia de comandos del ONTAP".

2. Confirme que `volume move` la operación se ha realizado correctamente con `volume move show` el comando. El `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 SVM que desea cifrar, seleccione **Editar**.
3. En el encabezado **Almacenamiento y optimización**, seleccione **Activar cifrado**.
4. Selecciona **Guardar**.

Configurar NVE en un volumen raíz del nodo ONTAP

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 pueden protegerse con 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
   ```

Configuración del cifrado basado en hardware de NetApp

Obtenga más información sobre el cifrado basado en hardware de ONTAP

El cifrado basado en hardware de NetApp admite el cifrado de disco completo (FDE) de los datos mientras se escriben. No se pueden leer los datos sin una clave de cifrado almacenada en el firmware. La clave de cifrado, a su vez, sólo es accesible a un nodo autenticado.

Cifrado basado en hardware de NetApp

Un nodo se autentica a una unidad de autocifrado mediante una clave de autenticación recuperada de un servidor de gestión de claves externo o Onboard Key Manager:

- 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 de autenticación a nodos del mismo sistema de almacenamiento que los datos.

Puede utilizar el cifrado de volúmenes de NetApp con cifrado basado en hardware para «cifrar doble» los datos de unidades con autocifrado.

Cuando se habilitan unidades de autocifrado, también se cifra el volcado de memoria.

Si una pareja de alta disponibilidad utiliza cifrado de unidades SAS o NVMe (SED, NSE, FIPS), debe seguir las instrucciones del tema Devolver una unidad FIPS o SED al modo sin protección para todas las unidades de la pareja de alta disponibilidad antes de inicializar el sistema (opciones de arranque 4 o 9). Si las unidades se reasignan, es posible que no se produzcan pérdidas de datos futuras.

Tipos de unidades de autocifrado compatibles

Se admiten dos tipos de unidades de autocifrado:

- Las unidades SAS o NVMe con certificación FIPS de autocifrado son compatibles con todos los sistemas FAS y AFF. Estas unidades, denominadas _unidades FIPS, cumplen con los requisitos del nivel 2 de la publicación estándar de procesamiento de información federal 140-2. Las capacidades certificadas ofrecen protecciones además del cifrado, como la prevención de ataques de denegación de servicio en la unidad. Las unidades FIPS no pueden combinarse con otros tipos de unidades en el mismo nodo o en la pareja de alta disponibilidad.
- A partir de ONTAP 9.6, las unidades NVMe de autocifrado que no se han sometido a pruebas FIPS son compatibles con los sistemas AFF A800, A320 y posteriores. Estas unidades, denominadas *SED*, ofrecen las mismas funcionalidades de cifrado que las unidades FIPS, pero se pueden combinar con unidades sin cifrado en el mismo nodo o par de alta disponibilidad.
- Todas las unidades validadas con FIPS utilizan un módulo criptográfico de firmware que se ha realizado mediante la validación FIPS. El módulo criptográfico de la unidad FIPS no utiliza ninguna clave generada fuera de la unidad (el módulo criptográfico del firmware de la unidad utiliza la frase de acceso de autenticación que se introduce en la unidad para obtener una clave de cifrado).

Las unidades sin cifrado son unidades que no están de SED o FIPS.

Si utiliza NSE en un sistema con un módulo Flash Cache, también debe habilitar NVE o NAE. NSe no cifra los datos que residen en el módulo de Flash Cache.

Cuándo utilizar la gestión de claves externas

Aunque resulta menos caro y, por lo general, más práctico, utilizar el gestor de claves incorporado, se debe utilizar la gestión de claves externa si se da alguna de las siguientes situaciones:

- La política de su organización requiere una solución de gestión de claves que utilice un módulo criptográfico FIPS 140-2 de nivel 2 (o superior).
- 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.

Detalles de soporte

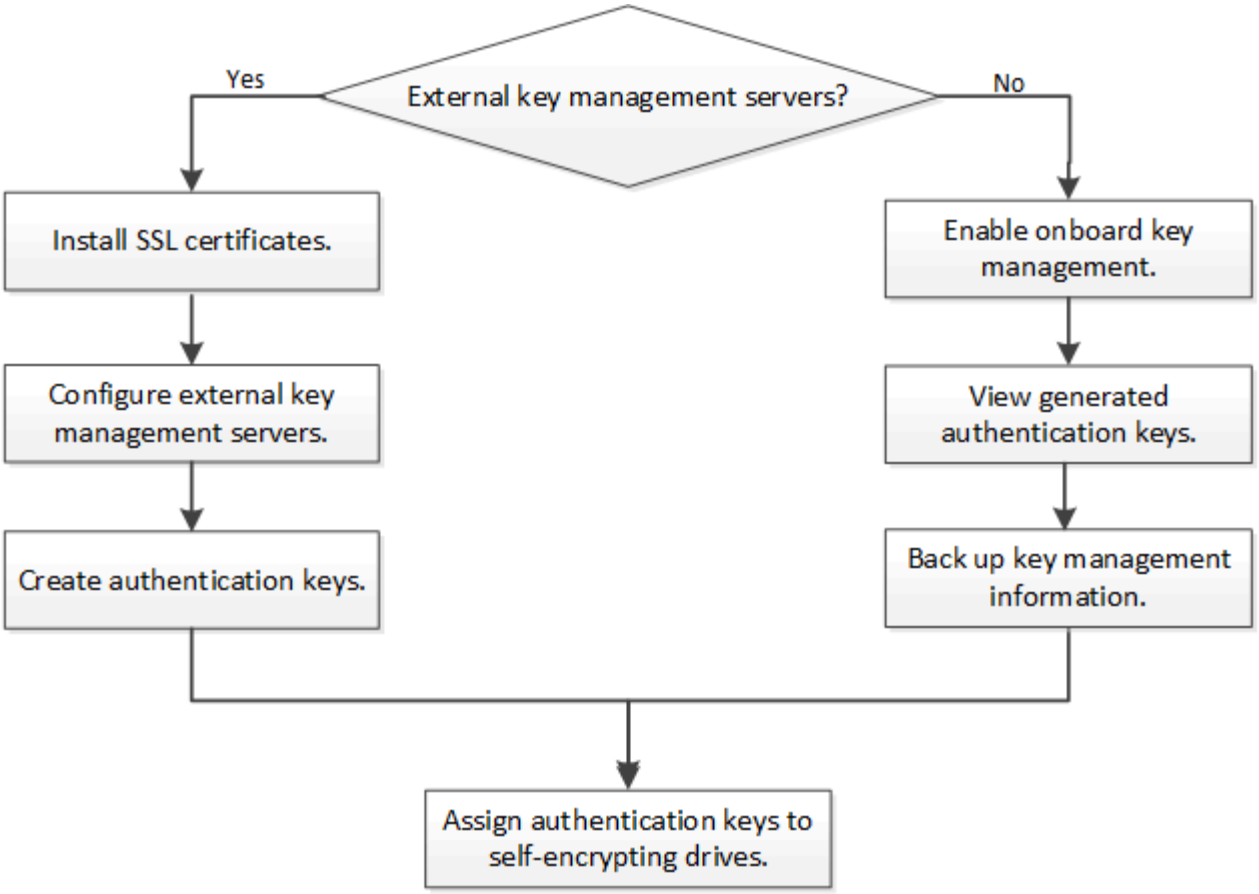
En la siguiente tabla se muestran detalles importantes de compatibilidad con el cifrado de hardware. Consulte la matriz de interoperabilidad para obtener la información más reciente sobre servidores KMIP, sistemas de almacenamiento y bandejas de discos compatibles.

Recurso o característica	Detalles de soporte

Conjuntos de discos no homogéneos	• Las unidades FIPS no pueden combinarse con otros tipos de unidades en el mismo nodo o en la pareja de alta disponibilidad. Las parejas de alta disponibilidad conformes pueden coexistir con parejas de alta disponibilidad no conformes en el mismo clúster. • SEDS puede combinarse con unidades sin cifrado en el mismo nodo o en la pareja de alta disponibilidad.
Tipo de unidad	• Las unidades FIPS pueden ser SAS o NVMe. • SEDS debe ser unidades NVMe.
Interfaces de red de 10 GB	A partir de ONTAP 9.3, las configuraciones de gestión de claves KMIP admiten interfaces de red de 10 GB para las comunicaciones con servidores de gestión de claves externos.
Puertos para la comunicación con el servidor de gestión de claves	A partir de ONTAP 9.3, es posible usar cualquier puerto de la controladora de almacenamiento para la comunicación con el servidor de gestión de claves. De lo contrario, debe utilizar el puerto e0M para la comunicación con los servidores de gestión de claves. Según el modelo de controladora de almacenamiento, es posible que ciertas interfaces de red no estén disponibles durante el proceso de arranque para establecer la comunicación con los servidores de gestión de claves.
MetroCluster (MCC) (en inglés)	• Las unidades NVMe admiten MCC. • Las unidades SAS no son compatibles con MCC.

Flujo de trabajo de cifrado basado en hardware

Debe configurar los servicios de gestión de claves para que el clúster pueda autenticarse en la unidad de autocifrado. Es posible usar un servidor de gestión de claves externo o un administrador de claves incorporado.



Información relacionada

- "NetApp Hardware Universe"
- "Cifrado de volúmenes de NetApp y cifrado de agregados de NetApp"

Configure la gestión de claves externas

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

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

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

Instalar certificados SSL en el clúster ONTAP

El clúster y el servidor KMIP utilizan certificados SSL KMIP para verificar la identidad de las otras y establecer una conexión SSL. Antes de configurar la conexión SSL con el servidor KMIP, debe instalar los certificados SSL de cliente KMIP para el clúster y el

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

Acerca de esta tarea

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

Antes de empezar

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

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

Pasos

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

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

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

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

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

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

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

Información relacionada

- "instalación del certificado de seguridad"

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

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

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

Antes de empezar

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

Pasos

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

   ```
   security key-manager external enable -vserver admin_SVM -key-servers
   host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert
   server_CA_certificates
   ```

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

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

   ```
   clusterl::> security key-manager external enable -key-servers
   ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
   -client-cert AdminVserverClientCert -server-ca-certs
   AdminVserverServerCaCert
   ```

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

   ```
   security key-manager external show-status -node node_name -vserver SVM -key
   -server host_name|IP_address:port -key-server-status available|not-
   responding|unknown
   ```

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

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

Node  Vserver  Key Server                                       Status
----  -------  ------------------------------------
-------------
node1
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available
node2
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available

6 entries were displayed.
```

Información relacionada

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

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

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

Acerca de esta tarea

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

Antes de empezar

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

Pasos

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

   ```
   security key-manager setup
   ```

Se inicia la configuración del gestor de claves.

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

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

   `security key-manager add -address key_management_server_ipaddress`

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

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

4. Añada un servidor KMIP adicional para redundancia:

   `security key-manager add -address key_management_server_ipaddress`

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

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

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

   `security key-manager show -status`

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

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

   Node            Port      Registered Key Manager  Status
   --------------  ----      ----------------------  ---------------
   cluster1-01     5696      20.1.1.1                available
   cluster1-01     5696      20.1.1.2                available
   cluster1-02     5696      20.1.1.1                available
   cluster1-02     5696      20.1.1.2                available
   ```

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

   `volume encryption conversion start`

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

Configure servidores de claves externas en clúster en ONTAP

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

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

Acerca de esta tarea

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

Antes de empezar

- "La gestión de claves KMIP debe estar habilitada para la SVM".
- Todos los nodos del clúster deben ejecutar ONTAP 9.11.1 o una versión posterior.
- El orden de los servidores enumerados en el `-secondary-key-servers` El parámetro refleja el orden de acceso de los servidores de administración de claves externas (KMIP).

Cree un servidor de claves en clúster

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

Añada servidores de claves primarios y secundarios a una SVM

Pasos

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

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

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

2. Habilitar el administrador de claves principal:

   ```
   security key-manager external enable -vserver <svm_name> -key-servers
   <primary_key_server_ip> -client-cert <client_cert_name> -server-ca-certs
   <server_ca_cert_names>
   ```

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

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

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

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

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

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

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

Pasos

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

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

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

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

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

Modifique los servidores de claves en cluster

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

Modificar servidores de claves secundarios

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

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

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

Convertir servidores de claves primarios y secundarios

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

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

Pasos

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

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

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

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

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

Pasos

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

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

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

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

Referirse a[mod-secondary] Para más información.

Información relacionada

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

Cree claves de autenticación en ONTAP 9.6 y versiones posteriores

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

Acerca de esta tarea

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

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

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

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

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

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

Antes de empezar

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

Pasos

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

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

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

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

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

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

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

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

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

En el siguiente ejemplo se verifica que se han creado claves de autenticación para `cluster1`:

```
cluster1::> security key-manager key query
       Vserver: cluster1
   Key Manager: external
          Node: node1

Key Tag                                 Key Type  Restored
--------------------------------------  --------  --------
node1                                   NSE-AK    yes
    Key ID: <id_value>
node1                                   NSE-AK    yes
    Key ID: <id_value>

       Vserver: cluster1
   Key Manager: external
          Node: node2

Key Tag                                 Key Type  Restored
--------------------------------------  --------  --------
node2                                   NSE-AK    yes
    Key ID: <id_value>
node2                                   NSE-AK    yes
    Key ID: <id_value>
```

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

Información relacionada

- "Mostrar disco de cifrado de almacenamiento"

Cree claves de autenticación en ONTAP 9.5 y versiones anteriores

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

Acerca de esta tarea

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

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

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

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

Antes de empezar

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

Pasos

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

   `security key-manager create-key`

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

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

   En el siguiente ejemplo se crean las claves de autenticación para `cluster1`:

```
cluster1::> security key-manager create-key
   (security key-manager create-key)
Verifying requirements...

Node: cluster1-01
Creating authentication key...
Authentication key creation successful.
Key ID: <id_value>

Node: cluster1-01
Key manager restore operation initialized.
Successfully restored key information.

Node: cluster1-02
Key manager restore operation initialized.
Successfully restored key information.
```

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

   `security key-manager query`

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

   En el siguiente ejemplo se verifica que se han creado claves de autenticación para `cluster1`:

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

  (security key-manager query)

          Node: cluster1-01
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag         Key Type  Restored
--------------  --------  --------
cluster1-01     NSE-AK    yes
       Key ID: <id_value>


          Node: cluster1-02
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag         Key Type  Restored
--------------  --------  --------
cluster1-02     NSE-AK    yes
       Key ID: <id_value>
```

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

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

Acerca de esta tarea

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

Este procedimiento no causa interrupciones.

Antes de empezar

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

Pasos

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

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

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

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

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   <id_value>

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

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

   `storage encryption disk show`

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

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

Información relacionada

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

Configure la gestión de claves incorporada

Habilite la gestión de claves incorporada en ONTAP 9.6 y versiones posteriores

Puede usar el gestor de claves incorporado para autenticar nodos de clúster en una unidad FIPS o SED. El gestor de claves incorporado es una herramienta integrada que

proporciona claves de autenticación a nodos del mismo sistema de almacenamiento que los datos. El gestor de claves incorporado es conforme a la normativa FIPS-140-2 de nivel 1.

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 onboard enable` el comando cada vez que añade un nodo al clúster. En configuraciones de MetroCluster, `security key-manager onboard enable` primero debe ejecutar en el clúster local y luego ejecutar `security key-manager onboard sync` en el clúster remoto, con 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" .

De forma predeterminada, no es necesario introducir la clave de acceso del administrador de claves cuando se reinicia un nodo. Excepto en MetroCluster, puede usar `cc-mode-enabled=yes` la opción para requerir que los usuarios introduzcan la clave de acceso después de un reinicio.

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 se habilitó el cifrado en almacenamiento de NetApp (NSE) y no se puede introducir la clave de acceso del clúster correcta en el arranque, el sistema no puede autenticarse en sus unidades y se reinicia automáticamente. Para corregir esto, debe introducir la clave de acceso correcta del clúster en el símbolo del sistema de arranque. 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 de actualización verifica que el contenido de la imagen no haya sido alterado o dañado comprobando varias firmas digitales. Si la validación funciona, la actualización de la imagen pasa al siguiente paso. Si la validación no funciona, la actualización de la imagen falla. Obtenga más información sobre `cluster image` en el"Referencia de comandos del ONTAP" .

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

- Si utiliza NSE con un servidor de gestión de claves externa (KMIP), debe haber eliminado la base de datos de 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 el comando de 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. `- 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.

   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:

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. Verifique que el sistema cree las claves de autenticación:

   `security key-manager key query -node node`

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

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

Después de terminar

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

El sistema realiza automáticamente una copia de seguridad de la información de administración de claves en la base de datos replicada (RDB) del clúster. También debe realizar una copia de seguridad de esta información manualmente para la recuperación ante desastres.

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

Habilite la gestión de claves incorporada en ONTAP 9.5 y versiones anteriores

Puede usar el gestor de claves incorporado para autenticar nodos de clúster en una unidad FIPS o SED. El gestor de claves incorporado es una herramienta integrada que proporciona claves de autenticación a nodos del mismo sistema de almacenamiento que los datos. El gestor de claves incorporado es conforme a la normativa FIPS-140-2 de nivel 1.

Puede utilizar el Administrador de claves integrado para proteger las claves que utiliza el clúster para acceder a datos cifrados. Habilite el Administrador de claves integrado en cada clúster que acceda a volúmenes cifrados o discos con cifrado automático.

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 está utilizando NSE 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`

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

```
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
```

Después de terminar

ONTAP realiza automáticamente una copia de seguridad de la información de administración de claves en la base de datos replicada (RDB) del clúster.

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

- "Realice un backup manual de la información de gestión de claves incorporada"
- "configuración del administrador de claves de seguridad"
- "administrador de claves de seguridad mostrar almacén de claves"
- "Transición a la gestión de claves incorporada desde la gestión de claves externas"

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

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

Acerca de esta tarea

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

Antes de empezar

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

Pasos

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

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

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

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

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   <id_value>

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

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

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

   `storage encryption disk show`

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

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

Información relacionada

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

Asignar una clave de autenticación FIPS 140-2 a una unidad FIPS de ONTAP

Puede usar `storage encryption disk modify` el comando con `-fips-key-id` la

opción para asignar una clave de autenticación FIPS 140-2 a una unidad FIPS. Los nodos de clúster utilizan esta clave para las operaciones de unidad distintas del acceso a los datos, como evitar ataques de denegación de servicio en la unidad.

Acerca de esta tarea

Es posible que la configuración de seguridad requiera el uso de claves diferentes para la autenticación de datos y la autenticación FIPS 140-2-2. Si no es así, puede usar la misma clave de autenticación para el cumplimiento de FIPS que se usa para acceder a los datos.

Este procedimiento no causa interrupciones.

Antes de empezar

El firmware de la unidad debe ser compatible con el cumplimiento de normativas FIPS 140-2-2. El "Herramienta de matriz de interoperabilidad de NetApp" contiene información sobre las versiones de firmware de la unidad compatibles.

Pasos

1. Primero debe asegurarse de que ha asignado una clave de autenticación de datos. Esto se puede hacer con un gestor de claves externas o un gestión de claves incorporada. Compruebe que la clave se ha asignado con el comando `storage encryption disk show`.
2. Asigne una clave de autenticación FIPS 140-2 a SED:

   `storage encryption disk modify -disk` *`disk_id`* `-fips-key-id` *`fips_authentication_key_id`*

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

   ```
   cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
   <id_value>

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

3. Compruebe que se ha asignado la clave de autenticación:

   `storage encryption disk show -fips`

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

```
cluster1::> storage encryption disk show -fips
Disk    Mode FIPS-Compliance Key ID
------  ----
--------------------------------------------------------------------
2.10.0  full <id_value>
2.10.1  full <id_value>
[...]
```

Información relacionada

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

Habilite el modo conforme a FIPS para todo el clúster para las conexiones del servidor KMIP en ONTAP

Puede usar `security config modify` el comando con -`is-fips-enabled`la opción de habilitar un modo conforme a FIPS para todo el clúster con los datos sobre transferencia. Al hacerlo, obliga al clúster a usar OpenSSL en modo FIPS al conectarse a servidores KMIP.

Acerca de esta tarea

Cuando habilita el modo compatible con FIPS en todo el clúster, el clúster utilizará únicamente paquetes de cifrado validados TLS1.2 y FIPS. El modo compatible con FIPS para todo el clúster está deshabilitado de forma predeterminada.

Debe reiniciar los nodos del clúster de forma manual después de modificar la configuración de seguridad de todo el clúster.

Antes de empezar

- La controladora de almacenamiento debe configurarse en modo conforme a FIPS.
- Todos los servidores KMIP deben ser compatibles con TLSv1.2. El sistema requiere TLSv1.2 para completar la conexión con el servidor KMIP cuando se habilita el modo compatible con FIPS en todo el clúster.

Pasos

1. Configure el nivel de privilegio en Advanced:

   `set -privilege advanced`

2. Compruebe que TLSv1.2 es compatible:

   `security config show -supported-protocols`

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

```
cluster1::> security config show
          Cluster                                                  Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ---------------------- -----------------
----------------
SSL       false      TLSv1.2, TLSv1.1, TLSv1 ALL:!LOW:         yes
                                             !aNULL:!EXP:
                                             !eNULL
```

3. Habilite el modo compatible con FIPS para todo el clúster:

   `security config modify -is-fips-enabled true -interface SSL`

   Obtenga más información sobre `security config modify` en el "Referencia de comandos del ONTAP".

4. Reiniciar nodos del clúster de forma manual.
5. Compruebe que el modo compatible con FIPS en todo el clúster esté habilitado:

   `security config show`

```
cluster1::> security config show
          Cluster                                                  Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ---------------------- -----------------
----------------
SSL       true       TLSv1.2, TLSv1.1       ALL:!LOW:         yes
                                             !aNULL:!EXP:
                                             !eNULL:!RC4
```

Gestione el cifrado de NetApp

Descifre los datos de volúmenes en ONTAP

Puede utilizar `volume move start` el comando para mover y descifrar datos de volumen.

Antes de empezar

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

Pasos

1. Mueva un volumen de cifrado existente y descifre los datos en el volumen:

   `volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false`

   Obtenga más información sobre `volume move start` en el "Referencia de comandos del ONTAP".

   El siguiente comando mueve un volumen existente denominado `vol1` al agregado de destino `aggr3` y descifra los datos del volumen:

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3 -encrypt-destination false
   ```

   El sistema elimina la clave de cifrado del volumen. Los datos del volumen no están cifrados.

2. Compruebe que el volumen esté deshabilitado para el cifrado:

   `volume show -encryption`

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

   El siguiente comando muestra si los volúmenes de `cluster1` están cifrados:

   ```
   cluster1::> volume show -encryption

   Vserver  Volume   Aggregate   State    Encryption State
   -------  ------   ---------   -----    ----------------
   vs1      vol1     aggr1       online   none
   ```

Mueva un volumen cifrado en ONTAP

Puede utilizar `volume move start` el comando para mover un volumen de cifrado. El volumen movido puede residir en el mismo agregado o en otra diferente.

Acerca de esta tarea

El movimiento generará un error si el nodo de destino o el volumen de destino no admiten el cifrado de volúmenes.

```
`-encrypt-destination`La opción de `volume move start` forma
predeterminada es TRUE para los volúmenes cifrados. El requisito para
especificar que no desea que el volumen de destino cifrado garantice que
no se descifren de forma accidental los datos del volumen.
```

Antes de empezar

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

Pasos

1. Mueva un volumen de cifrado existente y deje los datos en el volumen cifrado:

   `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`*

   Obtenga más información sobre `volume move start` en el "Referencia de comandos del ONTAP".

   El siguiente comando mueve un volumen existente llamado `vol1` al agregado de destino `aggr3` y deja los datos del volumen cifrado:

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3
   ```

2. Compruebe que el volumen esté habilitado para el cifrado:

   `volume show -is-encrypted true`

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

   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    aggr3     online    RW  200GB    160.0GB  20%
   ```

Cambie la clave de cifrado de un volumen con el comando volume encryption rekey start en ONTAP

Es una práctica recomendada para cambiar la clave de cifrado de un volumen periódicamente. A partir de ONTAP 9.3, puede usar `volume encryption rekey start` el comando para cambiar la clave de cifrado.

Acerca de esta tarea

Una vez que se inicia una operación de reclave, ésta debe completarse. No hay vuelta a la llave antigua. Si se encuentra con un problema de rendimiento durante la operación, puede ejecutar `volume encryption rekey pause` el comando para pausar la operación y el `volume encryption rekey resume` comando para reanudarla.

Hasta que finalice la operación de reclave, el volumen tendrá dos teclas. Las nuevas escrituras y sus lecturas correspondientes utilizarán la nueva clave. De lo contrario, las lecturas utilizarán la clave antigua.

> No se puede utilizar `volume encryption rekey start` para regenerar volúmenes de SnapLock.

Pasos

1. Cambiar una clave de cifrado:

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

   El comando siguiente cambia la clave de cifrado de `vol1` en la SVM`vs1`:

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

2. Verificar el estado de la operación de rellave:

   `volume encryption rekey show`

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

   El siguiente comando muestra el estado de la operación de nueva clave:

   ```
   cluster1::> volume encryption rekey show

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

3. Una vez finalizada la operación de nueva clave, compruebe que el volumen esté habilitado para el cifrado:

   `volume show -is-encrypted true`

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

   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%
   ```

Cambie la clave de cifrado de un volumen con el comando ONTAP volume move start

Es una práctica recomendada para cambiar la clave de cifrado de un volumen periódicamente. Puede usar `volume move start` el comando para cambiar la clave de cifrado. El volumen movido puede residir en el mismo agregado o en otra diferente.

Acerca de esta tarea

No se puede utilizar `volume move start` para regenerar volúmenes de SnapLock o FlexGroup.

Antes de empezar

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

Pasos

1. Mueva un volumen existente y cambie la clave de cifrado:

   `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-generate-destination-key true`

   Obtenga más información sobre `volume move start` en el "Referencia de comandos del ONTAP".

   El siguiente comando mueve un volumen existente llamado **`vol1`** al agregado de destino **`aggr2`** y cambia la clave de cifrado:

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

   Se crea una nueva clave de cifrado para el volumen. Los datos del volumen permanecen cifrados.

2. Compruebe que el volumen esté habilitado para el cifrado:

   `volume show -is-encrypted true`

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

   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%
   ```

Rotar claves de autenticación para el cifrado de almacenamiento de ONTAP NetApp

Puede rotar las claves de autenticación cuando utiliza Storage Encryption (NSE) de NetApp.

Acerca de esta tarea

La rotación de claves de autenticación en un entorno de NSE es compatible si se utiliza External Key Manager (KMIP).

> No se admite la rotación de claves de autenticación en un entorno de NSE en el gestor de claves incorporado (OKM).

Pasos

1. Utilice `security key-manager create-key` el comando para generar nuevas claves de autenticación.

   Debe generar nuevas claves de autenticación para poder cambiar las claves de autenticación.

2. Utilice `storage encryption disk modify -disk * -data-key-id` el comando para cambiar las claves de autenticación.

Información relacionada

- "modificar disco de cifrado de almacenamiento"

Elimine un volumen cifrado en ONTAP

Puede usar el `volume delete` comando para eliminar un volumen de cifrado.

Antes de empezar

- Para realizar esta tarea, debe ser un administrador de clústeres.
- El volumen debe estar fuera de línea.

Paso

1. Elimine un volumen cifrado:

   `volume delete -vserver` *`SVM_name`* `-volume` *`volume_name`*

   Obtenga más información sobre `volume delete` en el "Referencia de comandos del ONTAP".

   El siguiente comando elimina un volumen de cifrado llamado `vol1`:

   ```
   cluster1::> volume delete -vserver vs1 -volume vol1
   ```

   Introduzca `yes` cuando se le pida que confirme la eliminación.

   El sistema elimina la clave de cifrado del volumen después de 24 horas.

   Utilice `volume delete` con `-force true` la opción para eliminar un volumen y destruir la clave de cifrado correspondiente de inmediato. Este comando requiere privilegios avanzados. Obtenga más información sobre `volume delete` en el "Referencia de comandos del ONTAP".

Después de terminar

Puede utilizar `volume recovery-queue` el comando para recuperar un volumen eliminado durante el período de retención después de emitir `volume delete` el comando:

`volume recovery-queue` *`SVM_name`* `-volume` *`volume_name`*

"Cómo usar la función Volume Recovery"

Eliminar datos de forma segura en un volumen cifrado

Obtenga información sobre cómo purgar de forma segura los datos de un volumen ONTAP cifrado

A partir de ONTAP 9.4, puede utilizar la purga segura para eliminar datos sin interrupciones en volúmenes con la función NVE habilitada. La depuración de datos en un volumen cifrado garantiza que no pueda recuperarse de los medios físicos, por ejemplo, en casos de "eliminación de columnas", donde los seguimientos de datos pueden haberse quedado atrás cuando se sobrescriben los bloques o cuando se eliminan de forma segura los datos de un inquilino que están vaciando.

La purga segura solo funciona con los archivos eliminados previamente en volúmenes habilitados para NVE. No puede limpiar un volumen no cifrado. Debe usar los servidores KMIP para suministrar claves, no el gestor de claves incorporado.

Consideraciones que tener en cuenta al utilizar la purga segura

- Los volúmenes creados en un agregado habilitado para el cifrado de agregados de NetApp (NAE) no admiten la purga segura.
- La purga segura solo funciona con los archivos eliminados previamente en volúmenes habilitados para NVE.
- No puede limpiar un volumen no cifrado.
- Debe usar los servidores KMIP para suministrar claves, no el gestor de claves incorporado.

Las funciones de purga segura varían dependiendo de su versión de ONTAP.

ONTAP 9,8 y versiones posteriores

- MetroCluster y FlexGroup admiten la purga segura.
- Si el volumen que se purga es el origen de una relación de SnapMirror, no es necesario interrumpir la relación de SnapMirror para realizar una purga segura.
- El método de recifrado es diferente para los volúmenes que utilizan protección de datos SnapMirror frente a los volúmenes que no utilizan protección de datos de SnapMirror (DP) o los que utilizan protección de datos ampliada de SnapMirror.
  - De forma predeterminada, los volúmenes que utilizan el modo de protección de datos de SnapMirror (DP) vuelven a cifrar los datos con el método de recifrado del volumen.
  - De forma predeterminada, los volúmenes que no utilizan la protección de datos de SnapMirror o volúmenes mediante el modo de protección de datos ampliada (XDP) de SnapMirror utilizan el método de recifrado in situ.
  - Estos valores predeterminados pueden cambiarse con `secure purge re-encryption-method [volume-move|in-place-rekey]` el comando.
- De manera predeterminada, todas las copias de Snapshot de los volúmenes FlexVol se eliminan automáticamente durante la operación de purga segura. De manera predeterminada, las snapshots en volúmenes de FlexGroup y los volúmenes que utilizan la protección de datos de SnapMirror no se eliminan automáticamente durante la operación de purga segura. Estos valores predeterminados pueden cambiarse con `secure purge delete-all-snapshots [true|false]` el comando.

ONTAP 9,7 y anteriores:

- La purga segura no admite lo siguiente:
  - FlexClone
  - SnapVault
  - FabricPool
- Si el volumen que se purga es el origen de una relación de SnapMirror, debe interrumpir la relación de SnapMirror para poder purgar el volumen.

  Si existen snapshots ocupadas en el volumen, se deben liberar las snapshots antes de poder purgar el volumen. Por ejemplo, es posible que deba dividir un volumen FlexClone de su principal.
- Al invocar correctamente la función de purga de seguridad, se activa un movimiento de volúmenes que se vuelve a cifrar los datos restantes sin purgar con una clave nueva.

  El volumen movido permanece en el agregado actual. La clave antigua se destruye automáticamente, lo que garantiza que los datos purgados no puedan recuperarse del medio de almacenamiento.

Borrar datos de un volumen ONTAP cifrado sin una relación SnapMirror

A partir de ONTAP 9.4, puede utilizar la purga segura para obtener datos «crub» sin interrupciones en volúmenes con NVE habilitado.

Acerca de esta tarea

La purga segura puede tardar de varios minutos a varias horas en completarse, dependiendo de la cantidad de datos de los archivos eliminados. Puede usar `volume encryption secure-purge show` el comando

para ver el estado de la operación. Puede usar `volume encryption secure-purge abort` el comando para finalizar la operación.

> Para realizar una purga segura en un host SAN, debe eliminar todo el LUN que contiene los archivos que desea purgar, o debe poder perforar agujeros en la LUN para los bloques que pertenecen a los archivos que desea purgar. Si no puede eliminar la LUN, o el sistema operativo del host no admite orificios de perforación en la LUN, no puede realizar una purga segura.

Antes de empezar

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Se requieren privilegios avanzados para esta tarea.

Pasos

1. Elimine los archivos o la LUN que desea purgar de forma segura.
   - En un cliente NAS, elimine los archivos que desea purgar de forma segura.
   - En un host SAN, elimine la LUN que desea purgar o perforar agujeros en la LUN de los bloques que pertenecen a los archivos que desea purgar.
2. En el sistema de almacenamiento, cambie al nivel de privilegio avanzado:

   `set -privilege advanced`

3. Si los archivos que desea purgar de forma segura están en instantáneas, elimine las instantáneas:

   `snapshot delete -vserver` *`SVM_name`* `-volume` *`volume_name`* `-snapshot`

4. Elimine de forma segura los archivos eliminados:

   `volume encryption secure-purge start -vserver` *`SVM_name`* `-volume` *`volume_name`*

   El siguiente comando purga de forma segura los archivos eliminados en `vol1` la SVM`vs1`:

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

5. Compruebe el estado de la operación de purga segura:

   `volume encryption secure-purge show`

Eliminar datos de un volumen ONTAP cifrado con una relación asincrónica de SnapMirror

A partir de ONTAP 9.8, puede usar una purga segura para datos «crub» sin interrupciones de volúmenes con NVE habilitado con una relación asíncrona de SnapMirror.

Antes de empezar

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

- Se requieren privilegios avanzados para esta tarea.

Acerca de esta tarea

La purga segura puede tardar de varios minutos a varias horas en completarse, dependiendo de la cantidad de datos de los archivos eliminados. Puede usar `volume encryption secure-purge show` el comando para ver el estado de la operación. Puede usar `volume encryption secure-purge abort` el comando para finalizar la operación.

> Para realizar una purga segura en un host SAN, debe eliminar todo el LUN que contiene los archivos que desea purgar, o debe poder perforar agujeros en la LUN para los bloques que pertenecen a los archivos que desea purgar. Si no puede eliminar la LUN, o el sistema operativo del host no admite orificios de perforación en la LUN, no puede realizar una purga segura.

Pasos

1. En el sistema de almacenamiento, cambie al nivel de privilegio avanzado:

   ```
   set -privilege advanced
   ```

2. Elimine los archivos o la LUN que desea purgar de forma segura.
   - En un cliente NAS, elimine los archivos que desea purgar de forma segura.
   - En un host SAN, elimine la LUN que desea purgar o perforar agujeros en la LUN de los bloques que pertenecen a los archivos que desea purgar.
3. Prepare el volumen de destino en la relación asíncrona para que se purgue de forma segura:

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   -prepare true
   ```

   Repita este paso en cada volumen de su relación asíncrona SnapMirror.

4. Si los archivos que desea purgar de forma segura están en instantáneas, elimine las instantáneas:

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

5. Si los archivos que desea depurar de forma segura se encuentran en las instantáneas base, haga lo siguiente:

   a. Cree una copia Snapshot en el volumen de destino en la relación asíncrona de SnapMirror:

      ```
      volume snapshot create -snapshot snapshot_name -vserver SVM_name -volume
      volume_name
      ```

   b. Actualizar SnapMirror para mover la instantánea base hacia delante:

      ```
      snapmirror update -source-snapshot snapshot_name -destination-path
      destination_path
      ```

   Repita este paso para cada volumen de la relación asíncrona de SnapMirror.

   a. Repita los pasos (a) y (b) iguales al número de instantáneas base más una.

      Por ejemplo, si tiene dos instantáneas base, debe repetir los pasos (a) y (b) tres veces.

b. Compruebe que la instantánea base está presente:
`snapshot show -vserver SVM_name -volume volume_name`

c. Elimine la instantánea base:
`snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot`

6. Elimine de forma segura los archivos eliminados:

`volume encryption secure-purge start -vserver svm_name -volume volume_name`

Repita este paso en cada volumen de la relación asíncrona de SnapMirror.

El siguiente comando purga de forma segura los archivos eliminados de «'vol1'» de la SVM «'vs1'»:

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume
vol1
```

7. Compruebe el estado de la operación de purga segura:

`volume encryption secure-purge show`

Información relacionada

- "actualización de SnapMirror"

Eliminar datos de un volumen ONTAP cifrado con una relación sincrónica de SnapMirror

A partir de ONTAP 9.8, puede utilizar una purga segura para «depurar» datos sin interrupciones en los volúmenes con NVE habilitados con una relación síncrona de SnapMirror.

Acerca de esta tarea

Una purga segura puede tardar de varios minutos a varias horas en completarse, dependiendo de la cantidad de datos de los archivos eliminados. Puede usar `volume encryption secure-purge show` el comando para ver el estado de la operación. Puede usar `volume encryption secure-purge abort` el comando para finalizar la operación.

> Para realizar una purga segura en un host SAN, debe eliminar todo el LUN que contiene los archivos que desea purgar, o debe poder perforar agujeros en la LUN para los bloques que pertenecen a los archivos que desea purgar. Si no puede eliminar la LUN, o el sistema operativo del host no admite orificios de perforación en la LUN, no puede realizar una purga segura.

Antes de empezar

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Se requieren privilegios avanzados para esta tarea.

Pasos

1. En el sistema de almacenamiento, cambie al nivel de privilegio avanzado:

`set -privilege advanced`

2. Elimine los archivos o la LUN que desea purgar de forma segura.
   - En un cliente NAS, elimine los archivos que desea purgar de forma segura.
   - En un host SAN, elimine la LUN que desea purgar o perforar agujeros en la LUN de los bloques que pertenecen a los archivos que desea purgar.
3. Prepare el volumen de destino en la relación asíncrona para que se purgue de forma segura:

   ```
   volume encryption secure-purge start -vserver <SVM_name> -volume <volume_name>
   -prepare true
   ```

   Repita este paso para el otro volumen de la relación síncrona de SnapMirror.

4. Si los archivos que desea purgar de forma segura están en instantáneas, elimine las instantáneas:

   ```
   snapshot delete -vserver <SVM_name> -volume <volume_name> -snapshot <snapshot>
   ```

5. Si el archivo de depuración segura está en las instantáneas base o comunes, actualice SnapMirror para mover la instantánea común hacia delante:

   ```
   snapmirror update -source-snapshot <snapshot_name> -destination-path
   <destination_path>
   ```

   Hay dos instantáneas comunes, por lo que este comando debe emitirse dos veces.

6. Si el archivo de purga segura se encuentra en la snapshot coherente con las aplicaciones, elimine la snapshot de ambos volúmenes en la relación síncrona de SnapMirror:

   ```
   snapshot delete -vserver <SVM_name> -volume <volume_name> -snapshot <snapshot>
   ```

   Ejecute este paso en ambos volúmenes.

7. Elimine de forma segura los archivos eliminados:

   ```
   volume encryption secure-purge start -vserver <SVM_name> -volume <volume_name>
   ```

   Repita este paso en cada volumen de la relación síncrona de SnapMirror.

   El siguiente comando purga de forma segura los archivos eliminados en «'vol1'» en la SVM «'vs1'».

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

8. Compruebe el estado de la operación de purga segura:

   ```
   volume encryption secure-purge show
   ```

Información relacionada

- "actualización de SnapMirror"

Cambiar la contraseña de administración de claves integrada de ONTAP

NetApp recomienda cambiar periódicamente la frase de contraseña de administración de claves integrada. Debe guardar la nueva contraseña en un lugar seguro fuera del sistema de almacenamiento.

Antes de empezar

- Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.
- Se requieren privilegios avanzados para esta tarea.
- En un entorno MetroCluster , después de actualizar la contraseña en el clúster local, sincronice la actualización de la contraseña en el clúster asociado.

Pasos

1. Cambie al nivel de privilegio avanzado:

   ```
   set -privilege advanced
   ```

2. Cambie la contraseña de gestión de la llave integrada. El comando que utilice depende de la versión de ONTAP que esté ejecutando.

   ONTAP 9,6 y versiones posteriores

   ```
   security key-manager onboard update-passphrase
   ```

   ONTAP 9,5 y anteriores

   ```
   security key-manager update-passphrase
   ```

3. 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.

4. En la solicitud de confirmación de contraseña, vuelva a introducir la frase de contraseña.
5. Si se encuentra en una configuración MetroCluster , sincronice la contraseña actualizada en el clúster asociado.
   a. Sincronice la contraseña en el clúster asociado seleccionando el comando correcto para su versión de ONTAP :

ONTAP 9,6 y versiones posteriores

```
security key-manager onboard sync
```

ONTAP 9,5 y anteriores

- En ONTAP 9.5, ejecute:

  ```
  security key-manager setup -sync-metrocluster-config
  ```

- En ONTAP 9.4 y versiones anteriores, después de actualizar la contraseña en el clúster local, espere 20 segundos y, a continuación, ejecute el siguiente comando en el clúster asociado:

  ```
  security key-manager setup
  ```

b. Introduzca la nueva contraseña cuando se le solicite.

   Debe utilizarse la misma contraseña en ambos clústeres.

Después de terminar

Copie la contraseña de gestión de claves integrada en una ubicación segura fuera del sistema de almacenamiento para su uso futuro.

Realice copias de seguridad manuales de la información de gestión de claves siempre que cambie la contraseña de gestión de claves integrada.

Información relacionada

- "Realice un backup manual de la información de gestión de claves incorporada"
- "Administrador de claves de seguridad integrado, actualización de frase de contraseña"

Realice una copia de seguridad manual de la información de administración de claves integrada de ONTAP

Se debe copiar la información de gestión de claves incorporada en una ubicación segura fuera del sistema de almacenamiento siempre que se configure la clave de acceso de Onboard Key Manager.

Antes de empezar

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Se requieren privilegios avanzados para esta tarea.

Acerca de esta tarea

Se realiza automáticamente un backup de toda la información de gestión de claves en la base de datos replicada (RDB) del clúster. También debe realizar un backup de la información de gestión de claves manualmente para su uso en caso de desastre.

Pasos

1. Cambie al nivel de privilegio avanzado:

   ```
   set -privilege advanced
   ```

2. Muestre la información de backup de gestión de claves para el clúster:

Para esta versión de ONTAP…	Se usa este comando…
ONTAP 9,6 y versiones posteriores	`security key-manager onboard show-backup`
ONTAP 9,5 y anteriores	`security key-manager backup show`

El siguiente comando 9.6 muestra la información de respaldo de administración de claves para `cluster1`:

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

     ---------------------------BEGIN BACKUP---------------------------
     TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAADuD+byAAAAACEAAAAAAAAA
     QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
     dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAA
     3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAA
     IgAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
     QRHwv+1aWvAAAAAAAAAACQAAAAAAAAgAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
     BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     ---------------------------END BACKUP-----------------------------
```

3. Copie la información del backup en una ubicación segura fuera del sistema de almacenamiento para usarla en caso de desastre.

Información relacionada

- "Administrador de claves de seguridad integrado show-backup"
- "administrador de claves de seguridad, copia de seguridad, mostrar"

Restaure las claves de cifrado de gestión de claves incorporadas en ONTAP

Ocasionalmente, es posible que necesite restaurar una clave de cifrado de administración de claves incorporada. Una vez que haya verificado que es necesario restaurar una clave, puede configurar el Administrador de claves integrado para restaurar la clave. El procedimiento que sigue para restaurar sus claves de cifrado de administración de claves integrado varía según su versión de ONTAP.

Antes de empezar

- Elimina la base de datos del administrador de claves externo si usas NSE con un servidor KMIP externo. Para más detalles, consulte"Transición de la gestión de claves externa a la gestión de claves integrada de ONTAP" .
- Para realizar esta tarea, debe ser un administrador de clústeres.

> Si utiliza NSE en un sistema con un módulo Flash Cache, también debe habilitar NVE o NAE. NSe no cifra los datos que residen en el módulo de Flash Cache.

ONTAP 9,6 y versiones posteriores

> Si ejecuta ONTAP 9,8 o una versión posterior y el volumen raíz está cifrado, siga el procedimiento para [ontap-9-8].

1. Compruebe que la clave debe restaurarse:
   `security key-manager key query -node` *node*

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

2. Restaurar la clave:
   `security key-manager onboard sync`

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

3. En la solicitud de contraseña, introduzca la clave de acceso de gestión de claves incorporada para el clúster.

ONTAP 9,8 o posterior con un volumen raíz cifrado

Si ejecuta ONTAP 9.8 y versiones posteriores y el volumen raíz está cifrado, debe configurar una clave de recuperación de gestión de claves incorporada con el menú de arranque. Este proceso también es necesario si realiza un reemplazo del soporte de arranque.

1. Inicie el nodo en el menú de inicio y seleccione la opción `(10) Set onboard key management recovery secrets`.

2. Introduzca `y` para utilizar esta opción.
3. En el aviso de, introduzca la clave de acceso de gestión de claves incorporada para el clúster.
4. En el aviso, introduzca los datos de la clave de backup.

   Después de ingresar los datos de la clave de respaldo, el nodo regresa al menú de arranque.

5. En el menú de inicio, seleccione Opción `(1) Normal Boot`.

ONTAP 9,5 y anteriores

1. Compruebe que la clave debe restaurarse:
   `security key-manager key show`
2. Restaurar la clave:
   `security key-manager setup -node` *node*

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

3. En la solicitud de contraseña, introduzca la clave de acceso de gestión de claves incorporada para el clúster.

Restaurar claves de cifrado de administración de claves externas de ONTAP

Puede restaurar manualmente claves de cifrado de gestión de claves externas e insertarlas en otro nodo. Tal vez desee hacer esto si va a reiniciar un nodo que estaba inactivo temporalmente cuando creó las claves para el clúster.

Acerca de esta tarea

En ONTAP 9.6 y posterior, puede utilizar el `security key-manager key query -node node_name` comando para verificar si su clave necesita ser restaurada.

En ONTAP 9, 5 y anteriores, puede utilizar el `security key-manager key show` comando para verificar si su clave necesita ser restaurada.

> Si utiliza NSE en un sistema con un módulo Flash Cache, también debe habilitar NVE o NAE. NSe no cifra los datos que residen en el módulo de Flash Cache.

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

Antes de empezar

Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.

Pasos

1. Si ejecuta ONTAP 9.8 o una versión posterior y el volumen raíz está cifrado, haga lo siguiente:

   Si está ejecutando ONTAP 9.7 o una versión anterior, o si está ejecutando ONTAP 9.8 o una versión posterior y el volumen raíz no está cifrado, omita este paso.

   a. Establezca los arranques: +

```
setenv kmip.init.ipaddr <ip-address>
setenv kmip.init.netmask <netmask> +
setenv kmip.init.gateway <gateway> +
setenv kmip.init.interface e0M
boot_ontap
```

b. Inicie el nodo en el menú de inicio y seleccione la opción `(11) Configure node for external key management`.

c. Siga las instrucciones para introducir el certificado de gestión.

Una vez introducida toda la información del certificado de gestión, el sistema vuelve al menú de arranque.

d. En el menú de inicio, seleccione Opción `(1) Normal Boot`.

2. Restaure la clave:

Para esta versión de ONTAP…	Se usa este comando…
ONTAP 9,6 y versiones posteriores	`security key-manager external restore -vserver SVM -node node -key-server host_name
IP_address:port -key-id key_id -key -tag key_tag`	ONTAP 9,5 y anteriores

`node` por defecto en todos los nodos.

Este comando no es compatible cuando la gestión de claves incorporada está habilitada.

El siguiente comando de la ONTAP 9.6 restaura las claves de autenticación de gestión de claves externa en todos los nodos `cluster1` de :

```
cluster1::> security key-manager external restore
```

Información relacionada

- "Restauración externa del administrador de claves de seguridad"

Reemplazar los certificados SSL de KMIP en el clúster ONTAP

Todos los certificados SSL tienen una fecha de vencimiento. Debe actualizar los certificados antes de que caduquen para evitar la pérdida de acceso a las claves de autenticación.

Antes de empezar

- Debe haber obtenido el certificado público de reemplazo y la clave privada para el clúster (certificado de cliente KMIP).
- Debe haber obtenido el certificado público de reemplazo para el servidor KMIP (certificado de servidor KMIP).
- Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.

- Si va a reemplazar los certificados SSL KMIP en un entorno MetroCluster, debe instalar el mismo certificado SSL KMIP de reemplazo en ambos clústeres.

Puede instalar los certificados de cliente y servidor de repuesto en el servidor KMIP antes o después de instalar los certificados en el clúster.

Pasos

1. Instale el nuevo certificado de CA de servidor KMIP:

   ```
   security certificate install -type server-ca -vserver <>
   ```

2. Instale el nuevo certificado de cliente KMIP:

   ```
   security certificate install -type client -vserver <>
   ```

3. Actualice la configuración del gestor de claves para usar los certificados recién instalados:

   ```
   security key-manager external modify -vserver <> -client-cert <> -server-ca
   -certs <>
   ```

   Si ejecuta ONTAP 9.6 o una versión posterior en un entorno MetroCluster y desea modificar la configuración de gestor de claves en la SVM de administrador, debe ejecutar el comando en ambos clústeres de la configuración.

La actualización de la configuración del administrador de claves para usar los certificados recién instalados devolverá un error si las claves públicas/privadas del nuevo certificado de cliente son diferentes de las claves instaladas previamente. Ver el"Base de conocimientos de NetApp : Las claves públicas o privadas del nuevo certificado de cliente son diferentes del certificado de cliente existente" para obtener instrucciones sobre cómo anular este error.

Información relacionada

- "instalación del certificado de seguridad"
- "Modificación externa del administrador de claves de seguridad"

Reemplace una unidad FIPS o SED en ONTAP

Puede reemplazar una unidad FIPS o SED de la misma manera que reemplaza un disco normal. Asegúrese de asignar nuevas claves de autenticación de datos a la unidad de reemplazo. Para una unidad FIPS, puede asignar también una nueva clave de autenticación FIPS 140-2.

Si una pareja de alta disponibilidad está utilizando "Cifrar unidades SAS o NVMe (SED, NSE, FIPS)", debe seguir las instrucciones del tema "Devolver una unidad FIPS o SED al modo sin protección" para todas las unidades de la pareja de alta disponibilidad antes de inicializar el sistema (opciones de arranque 4 o 9). Si las unidades se reasignan, es posible que no se produzcan pérdidas de datos futuras.

Antes de empezar

- Debe conocer el ID de clave de la clave de autenticación que utiliza la unidad.

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

Pasos

1. Asegúrese de que el disco se ha marcado como erróneo:

   `storage disk show -broken`

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

   ```
   cluster1::> storage disk show -broken
   Original Owner: cluster1-01
     Checksum Compatibility: block
                                                                      Usable
   Physical
       Disk   Outage Reason HA Shelf Bay Chan   Pool  Type    RPM     Size
   Size
       ------ ---- ------------ ---- --- ---- ------ -----  -----  -------
   -------
       0.0.0  admin  failed  0b    1   0    A  Pool0  FCAL  10000  132.8GB
   133.9GB
       0.0.7  admin  removed 0b    2   6    A  Pool1  FCAL  10000  132.8GB
   134.2GB
   [...]
   ```

2. Quite el disco con error y sustitúyalo por una nueva unidad FIPS o SED siguiendo las instrucciones de la guía de hardware para su modelo de bandeja de discos.
3. Asigne la propiedad del disco recién sustituido:

   `storage disk assign -disk disk_name -owner node`

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

   ```
   cluster1::> storage disk assign -disk 2.1.1 -owner cluster1-01
   ```

4. Confirme que se ha asignado el disco nuevo:

   `storage encryption disk show`

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

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
------------------------------------------------------------------
0.0.0   data <id_value>
0.0.1   data <id_value>
1.10.0  data <id_value>
1.10.1  data <id_value>
2.1.1   open 0x0
[...]
```

5. Asigne las claves de autenticación de datos a la unidad FIPS o SED.

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

6. Si es necesario, asigne una clave de autenticación FIPS 140-2 a la unidad FIPS.

   "Asignar una clave de autenticación FIPS 140-2 a una unidad FIPS"

Información relacionada

- "asignación de disco de almacenamiento"
- "Mostrar disco de almacenamiento"
- "Mostrar disco de cifrado de almacenamiento"

Haga que los datos en una unidad FIPS o SED sean inaccesibles

Obtenga información sobre cómo hacer que los datos ONTAP en una unidad FIPS o SED sean inaccesibles

Si desea que los datos de una unidad FIPS o SED sean inaccesibles permanentemente, pero mantenga el espacio no utilizado de la unidad disponible para los nuevos datos, puede desinfectar el disco. Si desea que los datos no se puedan acceder a ellos de forma permanente y no es necesario volver a utilizar la unidad, es posible destruirlos.

- El saneamiento de disco

  Cuando se limpia una unidad de autocifrado, el sistema cambia la clave de cifrado de disco a un nuevo valor aleatorio, restablece el estado de bloqueo de encendido a FALSE y establece el ID de clave en un valor predeterminado, es decir, el ID seguro de fabricante 0x0 (unidades SAS) o una clave nula (unidades NVMe). Si lo hace, los datos del disco son inaccesibles y es imposible recuperarlos. Puede reutilizar discos sanitizados como discos de repuesto no ceros.

- Destrucción de discos

  Cuando destruye una unidad FIPS o SED, el sistema establece la clave de cifrado del disco en un valor aleatorio desconocido y bloquea el disco de forma irreversible. De este modo, el disco se vuelve inutilizable de forma permanente y los datos del mismo no se podrán acceder de forma permanente.

Puede desinfectar o destruir unidades de autocifrado individuales o todas las unidades de autocifrado de un nodo.

Desinfecte una unidad FIPS o SED en ONTAP

Si desea que datos en una unidad FIPS o SED no se puedan acceder de forma permanente y usar la unidad para datos nuevos, puede usar `storage encryption disk sanitize` el comando para sanear la unidad.

Acerca de esta tarea

Cuando se limpia una unidad de autocifrado, el sistema cambia la clave de cifrado de disco a un nuevo valor aleatorio, restablece el estado de bloqueo de encendido a FALSE y establece el ID de clave en un valor predeterminado, es decir, el ID seguro de fabricante 0x0 (unidades SAS) o una clave nula (unidades NVMe). Si lo hace, los datos del disco son inaccesibles y es imposible recuperarlos. Puede reutilizar discos sanitizados como discos de repuesto no ceros.

Antes de empezar

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

Pasos

1. Migre los datos que se deben conservar a un agregado en otro disco.
2. Elimine el agregado de la unidad FIPS o SED para que se sanean:

   `storage aggregate delete -aggregate` *`aggregate_name`*

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

   Obtenga más información sobre `storage aggregate delete` en el "Referencia de comandos del ONTAP".

3. Identifique el ID de disco para la unidad FIPS o SED para sanitización:

   `storage encryption disk show -fields data-key-id,fips-key-id,owner`

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

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

4. Si una unidad FIPS se ejecuta en el modo de cumplimiento de normativas FIPS, establezca el ID de clave de autenticación FIPS del nodo nuevamente en el ID de MSID 0x0 predeterminado:

`storage encryption disk modify -disk disk_id -fips-key-id 0x0`

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

```
cluster1::> storage encryption disk modify -disk 1.10.2 -fips-key-id 0x0

Info: Starting modify on 1 disk.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

5. Desinfecte la unidad:

   `storage encryption disk sanitize -disk disk_id`

   Puede utilizar este comando para desinfectar solo los discos duros o los discos rotos. Para sanear todos los discos independientemente del tipo, use `-force-all-state` la opción. Obtenga más información sobre `storage encryption disk sanitize` en el "Referencia de comandos del ONTAP".

   ONTAP le pedirá que introduzca una frase de confirmación antes de continuar. Introduzca la frase exactamente como se muestra en la pantalla.

```
cluster1::> storage encryption disk sanitize -disk 1.10.2

Warning: This operation will cryptographically sanitize 1 spare or
broken self-encrypting disk on 1 node.
         To continue, enter sanitize disk: sanitize disk

Info: Starting sanitize on 1 disk.
      View the status of the operation using the
      storage encryption disk show-status command.
```

6. Elimine el error del disco saneado:
   `storage disk unfail -spare true -disk disk_id`
7. Compruebe si el disco tiene un propietario
   `storage disk show -disk disk_id`: + Si el disco no tiene un propietario, asigne uno.
   `storage disk assign -owner node -disk disk_id`
8. Introduzca el nodo que posee los discos que desea desinfectar:

   `system node run -node node_name`

   Ejecute `disk sanitize release` el comando.

9. Salga del infierno. Elimine el error del disco de nuevo:
   `storage disk unfail -spare true -disk disk_id`
10. Compruebe que el disco ahora es un disco de reserva y listo para volver a utilizarse en un agregado:

```
storage disk show -disk disk_id
```

Información relacionada

- "asignación de disco de almacenamiento"
- "Mostrar disco de almacenamiento"
- "El disco de almacenamiento no falla"
- "modificar disco de cifrado de almacenamiento"
- "Cifrado de almacenamiento, desinfección de disco"
- "estado del disco de cifrado de almacenamiento"

Destruya una unidad FIPS o SED en ONTAP

Si desea que los datos en una unidad FIPS o SED no sean accesibles de forma permanente y no es necesario volver a utilizar la unidad, puede utilizar `storage encryption disk destroy` el comando para destruir el disco.

Acerca de esta tarea

Cuando destruye una unidad FIPS o SED, el sistema configura la clave de cifrado de disco para tener un valor aleatorio desconocido y bloquea la unidad de forma irreversible. De este modo, el disco se vuelve prácticamente inutilizable y los datos del disco se dejan permanentemente inaccesibles. No obstante, puede restablecer el disco a su configuración de fábrica mediante el ID seguro físico (PSID) impreso en la etiqueta del disco. Para obtener más información, consulte "Devolver una unidad FIPS o SED al servicio cuando se pierden las claves de autenticación".

> No debe destruir una unidad FIPS o SED a menos que tenga el servicio no retornable Disk Plus (NRD Plus). La destrucción de un disco anula su garantía.

Antes de empezar

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

Pasos

1. Migre los datos que se deben conservar a un agregado en otro disco diferente.
2. Elimine el agregado en la unidad FIPS o SED para destruirse:

   ```
   storage aggregate delete -aggregate aggregate_name
   ```

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

   Obtenga más información sobre `storage aggregate delete` en el "Referencia de comandos del ONTAP".

3. Identifique el ID de disco de la unidad FIPS o SED que se van a destruir:

   ```
   storage encryption disk show
   ```

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

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

4. Destruir el disco:

   `storage encryption disk destroy -disk disk_id`

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

   > Se le pedirá que introduzca una frase de confirmación antes de continuar. Introduzca la frase exactamente como se muestra en la pantalla.

```
cluster1::> storage encryption disk destroy -disk 1.10.2

Warning: This operation will cryptographically destroy 1 spare or broken
         self-encrypting disks on 1 node.
         You cannot reuse destroyed disks unless you revert
         them to their original state using the PSID value.
         To continue, enter
          destroy disk
         :destroy disk

Info: Starting destroy on 1 disk.
      View the status of the operation by using the
      "storage encryption disk show-status" command.
```

Información relacionada

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

Datos de trituración de emergencia en una unidad FIPS o SED en ONTAP

En caso de una emergencia de seguridad, puede evitar al instante el acceso a una unidad FIPS o SED, incluso si no hay alimentación disponible para el sistema de almacenamiento o el servidor KMIP.

Antes de empezar

- Si utiliza un servidor KMIP que no tiene alimentación disponible, el servidor KMIP debe configurarse con un elemento de autenticación fácilmente destruido (por ejemplo, una tarjeta inteligente o una unidad USB).
- Para realizar esta tarea, debe ser un administrador de clústeres.

Paso

1. Lleve a cabo la destrucción de datos de emergencia en una unidad FIPS o SED:

Si…	Realice lo siguiente…

Hay alimentación disponible en el sistema de almacenamiento y hay tiempo para desconectar el sistema de almacenamiento sin problemas	a. Si el sistema de almacenamiento está configurado como un par de alta disponibilidad, deshabilite el respaldo. b. Desconectar y eliminar todos los agregados. c. Establezca el nivel de privilegio en AVANZADO: `set -privilege advanced` d. Si la unidad se encuentra en modo de cumplimiento de FIPS, establezca el ID de clave de autenticación FIPS para el nodo en el MSID predeterminado: `storage encryption disk modify -disk * -fips-key-id 0x0` e. Detenga el sistema de almacenamiento. f. Arranque en modo de mantenimiento. g. Desinfecte o destruya los discos: ◦ Si desea que los datos de los discos sean inaccesibles y aún así pueda reutilizar los discos, desinfecte los discos: `disk encrypt sanitize -all` ◦ Si desea que los datos de los discos sean inaccesibles y no necesita guardar los discos, destruya los discos: `disk encrypt destroy disk_id1 disk_id2 …`	El sistema de almacenamiento dispone de energía y debe purgar los datos inmediatamente

a. **Si desea que los datos de los discos sean inaccesibles y todavía puedan reutilizar los discos, desinfecte los discos:**
b. Si el sistema de almacenamiento está configurado como un par de alta disponibilidad, deshabilite el respaldo.
c. Configure el nivel de privilegio en Advanced:
`set -privilege advanced`
d. Si la unidad está en modo de cumplimiento de normativas FIPS, establezca el identificador de clave de autenticación FIPS del nodo nuevamente en el MSID predeterminado:
`storage encryption disk modify -disk * -fips-key-id 0x0`
e. Desinfecte el disco:
`storage encryption disk sanitize -disk * -force-all-states true`
	a. **Si desea que los datos en los discos sean inaccesibles y no necesita guardar los discos, destruya los discos:**
	b. Si el sistema de almacenamiento está configurado como un par de alta disponibilidad, deshabilite el respaldo.
	c. Configure el nivel de privilegio en Advanced:
	`set -privilege advanced`
	d. Destruya los discos:
	`storage encryption disk destroy -disk * -force-all-states true`
		El sistema de almacenamiento produce una alarma y deja el sistema en un estado de desactivación permanente con todos los datos borrados. Para volver a utilizar el sistema, debe volver a configurarlo.

La alimentación está disponible en el servidor KMIP, pero no en el sistema de almacenamiento	a. Inicie sesión en el servidor KMIP. b. Destruya todas las claves asociadas con las unidades FIPS o SED que contengan los datos a los que desea impedir el acceso. De este modo se evita que el sistema de almacenamiento tenga acceso a las claves de cifrado de disco.	No hay alimentación disponible para el servidor KMIP o el sistema de almacenamiento

Información relacionada

- "destrucción del disco de cifrado de almacenamiento"
- "modificar disco de cifrado de almacenamiento"

- "Cifrado de almacenamiento, desinfección de disco"

Devolver una unidad FIPS o SED al servicio cuando se pierden las claves de autenticación en ONTAP

El sistema trata una unidad FIPS o SED como rota si se pierden las claves de autenticación de ella de forma permanente y no pueden recuperarla del servidor KMIP. Aunque no puede acceder o recuperar los datos en el disco, puede tomar medidas para que el espacio sin usar del SED esté disponible de nuevo para los datos.

Antes de empezar

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

Acerca de esta tarea

Debe utilizar este proceso solo si tiene la seguridad de que las claves de autenticación de la unidad FIPS o SED se pierden de forma permanente y que no puede recuperarlos.

Si los discos se particionan, primero deben desparticionarse para poder iniciar este proceso.

> El comando para desparticionar un disco solo está disponible en el nivel de diagnóstico y debe ejecutarse únicamente bajo la supervisión del soporte de NetApp . **Se recomienda encarecidamente que se comunique con el soporte de NetApp antes de continuar.** También puedes consultar el"Base de conocimientos de NetApp : Cómo desparticionar una unidad de repuesto en ONTAP" .

Pasos

1. Devolver una unidad FIPS o SED a servicio:

Si el SEDS es…	Utilice estos pasos…

No en el modo de cumplimiento de FIPS ni en el modo de cumplimiento de FIPS y la clave FIPS está disponible	a. Establezca el nivel de privilegio en avanzado:
	`set -privilege advanced`
	b. Restablezca la clave FIPS al ID seguro de fabricación predeterminado 0x0:
	`storage encryption disk modify -fips-key-id 0x0 -disk disk_id`
	c. Compruebe que la operación se ha realizado correctamente:
	`storage encryption disk show-status` Si la operación ha fallado, utilice el proceso PSID en este tema.
	d. Sanitize the broken disk:
	`storage encryption disk sanitize -disk disk_id` Verifique que la operación se haya realizado correctamente con el comando `storage encryption disk show-status` antes de continuar con el siguiente paso.
	e. Elimine el error del disco saneado:
	`storage disk unfail -spare true -disk disk_id`
	f. Compruebe si el disco tiene un propietario
	`storage disk show -disk disk_id`: + Si el disco no tiene un propietario, asigne uno.
	`storage disk assign -owner node -disk disk_id`
	i. Introduzca el nodo que posee los discos que desea desinfectar:
	`system node run -node node_name`
	Ejecute `disk sanitize release` el comando.
	g. Salga del infierno. Elimine el error del disco de nuevo:
	`storage disk unfail -spare true -disk disk_id`
	h. Compruebe que el disco ahora es un disco de reserva y listo para volver a utilizarse en un agregado:
	`storage disk show -disk disk_id`

En el modo de cumplimiento de normativas FIPS, la clave FIPS no está disponible y el SED tiene un PSID impreso en la etiqueta	a. Obtenga el PSID del disco de la etiqueta del disco. b. Establezca el nivel de privilegio en avanzado: `set -privilege advanced` c. Restablece el disco a la configuración configurada en fábrica: `storage encryption disk revert-to-original-state -disk` *`disk_id`* `-psid` *`disk_physical_secure_id`* Compruebe que la operación se ha realizado correctamente con el comando `storage encryption disk show-status` antes de continuar con el siguiente paso. d. Si está ejecutando ONTAP 9.8P5 o anterior, vaya al siguiente paso. Si ejecuta ONTAP 9.8P6 o una versión posterior, anule el error del disco saneado. `storage disk unfail -disk` *`disk_id`* e. Compruebe si el disco tiene un propietario `storage disk show -disk` *`disk_id`*: + Si el disco no tiene un propietario, asigne uno. `storage disk assign -owner node -disk` *`disk_id`* i. Introduzca el nodo que posee los discos que desea desinfectar: `system node run -node` *`node_name`* Ejecute `disk sanitize release` el comando. f. Salir del infierno.. Elimine el error del disco de nuevo: `storage disk unfail -spare true -disk` *`disk_id`* g. Compruebe que el disco ahora es un disco de reserva y listo para volver a utilizarse en un agregado: `storage disk show -disk` *`disk_id`*

Información relacionada

- "modificar disco de cifrado de almacenamiento"
- "Cifrado de almacenamiento: disco que vuelve al estado original"
- "Cifrado de almacenamiento, desinfección de disco"
- "estado del disco de cifrado de almacenamiento"

Devolver una unidad FIPS o SED al modo desprotegido en ONTAP

Una unidad FIPS o SED está protegida del acceso no autorizado solo si el ID de clave de autenticación del nodo está establecido en un valor distinto del predeterminado. Puede devolver una unidad FIPS o SED al modo no protegido mediante el `storage encryption disk modify` comando para establecer el identificador de clave en el valor predeterminado. Una unidad FIPS o SED en modo no protegido utiliza las claves de cifrado predeterminadas, mientras que una unidad FIPS o SED en modo protegido utiliza claves de cifrado secretas suministradas. Si hay datos cifrados en la unidad y esta

se restablece al modo no protegido, los datos siguen cifrados y no se exponen.

> Siga este procedimiento para garantizar que todos los datos cifrados se vuelvan inaccesibles después de que la unidad FIPS o SED regrese al modo desprotegido. Una vez que se restablecen los identificadores de claves de datos y FIPS, los datos existentes no se pueden descifrar y se vuelven inaccesibles a menos que se restablezcan las claves originales.

Si una pareja de alta disponibilidad utiliza unidades SAS o NVMe cifradas (SED, NSE, FIPS), debe seguir este proceso para todas las unidades de la pareja de alta disponibilidad antes de inicializar el sistema (opciones de arranque 4 o 9). Si las unidades se reasignan, es posible que no se produzcan pérdidas de datos futuras.

Antes de empezar

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

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Si una unidad FIPS se ejecuta en el modo de cumplimiento de normativas FIPS, establezca el ID de clave de autenticación FIPS del nodo nuevamente en el ID de MSID 0x0 predeterminado:

   ```
   storage encryption disk modify -disk disk_id -fips-key-id 0x0
   ```

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

   ```
   cluster1::> storage encryption disk modify -disk 2.10.11 -fips-key-id
   0x0

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

   Confirme que la operación se ha realizado correctamente con el comando:

   ```
   storage encryption disk show-status
   ```

   Repita el comando show-status hasta que los números en "Disks Begun" y "Disks Done" sean los mismos.

```
cluster1:: storage encryption disk show-status

            FIPS    Latest   Start               Execution   Disks
Disks Disks
Node        Support Request  Timestamp           Time (sec)  Begun
Done  Successful
-------     ------- -------- ------------------  ---------- ------
------  ----------
cluster1    true    modify   1/18/2022 15:29:38    3           14     5
5
1 entry was displayed.
```

3. Vuelva a establecer el ID de clave de autenticación de datos del nodo en el MSID 0x0 predeterminado:

   `storage encryption disk modify -disk disk_id -data-key-id 0x0`

   El valor de `-data-key-id` debe establecerse en 0x0, tanto si va a devolver una unidad SAS o NVMe al modo no protegido.

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

```
cluster1::> storage encryption disk modify -disk 2.10.11 -data-key-id
0x0

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

   Confirme que la operación se ha realizado correctamente con el comando:

   `storage encryption disk show-status`

   Repita el comando show-status hasta que los números sean los mismos. La operación se completa cuando los números en "discos iniciados" y "discos terminados" son los mismos.

Modo de mantenimiento

A partir de ONTAP 9.7, es posible volver a introducir una unidad FIPS en modo de mantenimiento. Solo debe utilizar el modo de mantenimiento si no puede utilizar las instrucciones de la CLI de ONTAP de la sección anterior.

Pasos

1. Establezca el ID de clave de autenticación FIPS del nodo de nuevo en el MSID 0x0 predeterminado:

   `disk encrypt rekey_fips 0x0 disklist`

2. Vuelva a establecer el ID de clave de autenticación de datos del nodo en el MSID 0x0 predeterminado:

```
disk encrypt rekey 0x0 disklist
```

3. Confirme que la clave de autenticación FIPS se ha recodificado correctamente:

```
disk encrypt show_fips
```

4. Confirmar que la clave de autenticación de datos se ha recodificado correctamente con:

```
disk encrypt show
```

Es probable que la salida muestre el ID de clave predeterminado de MSID 0x0 o el valor de 64 caracteres que contiene el servidor de claves. El `Locked?` campo hace referencia al bloqueo de datos.

```
Disk       FIPS Key ID                 Locked?
---------- --------------------------- -------
0a.01.0    0x0                          Yes
```

Información relacionada

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

Quite una conexión de gestor de claves externo en ONTAP

Es posible desconectar un servidor KMIP de un nodo cuando ya no se necesita el servidor. Por ejemplo, es posible que se desconecte un servidor KMIP cuando se realiza la transición al cifrado de volúmenes.

Acerca de esta tarea

Cuando desconecta un servidor KMIP de un nodo en un par de alta disponibilidad, el sistema desconecta automáticamente el servidor de todos los nodos del clúster.

Si planea continuar utilizando la gestión de claves externas después de desconectar un servidor KMIP, asegúrese de que haya otro servidor KMIP disponible para servir claves de autenticación.

Antes de empezar

Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.

Paso

1. Desconecte un servidor KMIP del nodo actual:

Para esta versión de ONTAP…	Se usa este comando…
ONTAP 9,6 y versiones posteriores	`security key-manager external remove-servers -vserver SVM -key -servers host_name
IP_address:port,…`	ONTAP 9,5 y anteriores

En un entorno de MetroCluster, debe repetir estos comandos en ambos clústeres para la SVM de

administrador.

El siguiente comando ONTAP 9.6 desactiva las conexiones a dos servidores de gestión de claves externos para `cluster1`, el primero llamado `ks1`, escuchar en el puerto predeterminado 5696, el segundo con la dirección IP 10,0.0,20, escuchar en el puerto 24482:

```
clusterl::> security key-manager external remove-servers -vserver
cluster-1 -key-servers ks1,10.0.0.20:24482
```

Obtenga más información sobre `security key-manager external remove-servers` y `security key-manager delete` en el "Referencia de comandos del ONTAP".

Modificar las propiedades del servidor de administración de claves externas de ONTAP

A partir de ONTAP 9.6, es posible usar `security key-manager external modify-server` el comando para cambiar el tiempo de espera de I/O y el nombre de usuario de un servidor de gestión de claves externo.

Antes de empezar

- Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.
- Se requieren privilegios avanzados para esta tarea.
- En un entorno de MetroCluster, debe repetir estos pasos en ambos clústeres para la SVM de administrador.

Pasos

1. En el sistema de almacenamiento, cambie al nivel de privilegio avanzado:

   ```
   set -privilege advanced
   ```

2. Modifique las propiedades del servidor de administración de claves externo para el clúster:

   ```
   security key-manager external modify-server -vserver admin_SVM -key-server
   host_name|IP_address:port,… -timeout 1…60 -username user_name
   ```

   > El valor del tiempo de espera se expresa en segundos. Si modifica el nombre de usuario, se le solicitará que introduzca una nueva contraseña. Si ejecuta el comando en la solicitud de inicio de sesión del clúster, *`admin_SVM`* se establece de forma predeterminada en la SVM de administrador del clúster actual. Debe ser el administrador de clústeres para modificar las propiedades del servidor de administrador de claves externo.

El siguiente comando cambia el valor de tiempo de espera a 45 segundos para el `cluster1` servidor de gestión de claves externo que escucha en el puerto predeterminado 5696:

```
clusterl::> security key-manager external modify-server -vserver
cluster1 -key-server ks1.local -timeout 45
```

3. Modificar las propiedades del servidor de gestor de claves externo para una SVM (solo NVE):

```
security key-manager external modify-server -vserver SVM -key-server
host_name|IP_address:port,… -timeout 1…60 -username user_name
```

> El valor del tiempo de espera se expresa en segundos. Si modifica el nombre de usuario, se le solicitará que introduzca una nueva contraseña. Si ejecuta el comando en la solicitud de inicio de sesión de SVM, *SVM* pasará a la SVM actual de forma predeterminada. Debe ser el administrador de clúster o de SVM para modificar las propiedades del servidor de administrador de claves externo.

El siguiente comando cambia el nombre de usuario y la contraseña `svm1` del servidor de gestión de claves externo que escucha en el puerto predeterminado 5696:

```
svm1::> security key-manager external modify-server -vserver svm11 -key
-server ks1.local -username svm1user
Enter the password:
Reenter the password:
```

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

Información relacionada

- "administrador de claves de seguridad servidor de modificación externo"

Realice la transición a la gestión de claves externa desde la gestión de claves incorporada en ONTAP

Si desea cambiar a la gestión de claves externas desde la gestión de claves incorporada, debe eliminar la configuración de gestión de claves incorporada para poder habilitar la gestión de claves externas.

Antes de empezar

- Para el cifrado basado en hardware, debe restablecer las claves de datos de todas las unidades FIPS o SED a su valor predeterminado.

  "Devolver una unidad FIPS o SED al modo sin protección"

- Para el cifrado basado en software, debe descifrar todos los volúmenes.

  "Descifrar los datos de volúmenes"

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

Paso

1. Elimine la configuración integrada de gestión de claves para un clúster:

Para esta versión de ONTAP…	Se usa este comando…
ONTAP 9,6 y versiones posteriores	`security key-manager onboard disable -vserver SVM`

ONTAP 9,5 y anteriores	`security key-manager delete-key-database`

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

Cambiar de la gestión de claves externa a la gestión de claves integrada de ONTAP

Para cambiar a la administración de claves integrada, elimine la configuración de administración de claves externa antes de habilitar la administración de claves integrada.

Antes de empezar

- Para el cifrado basado en hardware, debe restablecer las claves de datos de todas las unidades FIPS o SED a su valor predeterminado.

  "Devolver una unidad FIPS o SED al modo sin protección"

- Eliminó todas las conexiones del administrador de claves externo.

  "Eliminación de una conexión de administrador de claves externo"

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

Pasos

Los pasos para realizar la transición de la gestión de claves dependen de la versión de ONTAP que esté utilizando.

ONTAP 9,6 y versiones posteriores

1. Cambie al nivel de privilegio avanzado:

   ```
   set -privilege advanced
   ```

2. Utilizar el comando:

   ```
   security key-manager external disable -vserver admin_SVM
   ```

   ⓘ En un entorno de MetroCluster, debe repetir el comando en ambos clústeres para la SVM de administrador.

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

ONTAP 9,5 y anteriores

Utilice el comando:
`security key-manager delete-kmip-config`

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

Información relacionada

- "Desactivación externa del administrador de claves de seguridad"

¿Qué sucede cuando no se puede acceder a los servidores de administración de claves durante el proceso de arranque de ONTAP?

ONTAP toma ciertas precauciones para evitar un comportamiento no deseado en el caso de que un sistema de almacenamiento configurado para NSE no pueda alcanzar ninguno de los servidores de gestión de claves especificados durante el proceso de arranque.

Si el sistema de almacenamiento está configurado para NSE, el SED está recodificado y bloqueado y el SED está encendido, el sistema de almacenamiento debe recuperar las claves de autenticación necesarias de los servidores de gestión de claves para autenticarse en el SED antes de poder acceder a los datos.

El sistema de almacenamiento intenta contactar con los servidores de gestión de claves especificados durante tres horas. Si el sistema de almacenamiento no puede alcanzar ninguna de ellas después de esa hora, el proceso de arranque se detiene y el sistema de almacenamiento se detiene.

Si el sistema de almacenamiento se contacta correctamente con el servidor de gestión de claves especificado, se intenta establecer una conexión SSL hasta 15 minutos. Si el sistema de almacenamiento no puede establecer una conexión SSL con cualquier servidor de gestión de claves especificado, el proceso de arranque se detiene y el sistema de almacenamiento se detiene.

Mientras el sistema de almacenamiento intenta comunicarse y conectarse a servidores de gestión de claves, muestra información detallada sobre los intentos fallidos en la CLI. Puede interrumpir los intentos de contacto en cualquier momento con Ctrl-C.

Como medida de seguridad, el cifrado de disco automático permite únicamente un número limitado de intentos de acceso no autorizados, tras los cuales se deshabilita el acceso a los datos existentes. Si el sistema de almacenamiento no puede ponerse en contacto con ningún servidor de gestión de claves especificado para obtener las claves de autenticación adecuadas, solo puede intentar autenticarse con la clave predeterminada, lo que provoca un intento fallido y una alarma. Si el sistema de almacenamiento está configurado para reiniciarse automáticamente en caso de producirse una alarma, entra en un bucle de arranque, lo que da como resultado intentos de autenticación con errores constantes en el SED.

Detener el sistema de almacenamiento en estas situaciones es mediante un diseño para evitar que el sistema de almacenamiento entre en un bucle de arranque y posible pérdida de datos involuntaria como resultado del cifrado de disco de forma permanente debido a que se supera el límite de seguridad de un cierto número de intentos de autenticación fallidos consecutivos. El límite y el tipo de protección de bloqueo dependen de las especificaciones de fabricación y del tipo de SED:

Tipo de SED	Número de intentos fallidos consecutivos de autenticación que provocan el bloqueo	Tipo de protección de bloqueo cuando se alcanza el límite de seguridad
HDD	1024	Permanente. No se pueden recuperar los datos, incluso cuando la clave de autenticación correcta vuelva a estar disponible.

SSD X440_PHM2800MCTO 800GB NSE con revisiones de firmware NA00 o NA01	5	Temporal. El bloqueo solo está activo hasta que se somete al disco a un ciclo de encendido y apagado.
SSD X577_PHM2800MCTO 800GB NSE con revisiones de firmware NA00 o NA01	5	Temporal. El bloqueo solo está activo hasta que se somete al disco a un ciclo de encendido y apagado.
SSD X440_PHM2800MCTO 800GB NSE con revisiones de firmware superiores	1024	Permanente. No se pueden recuperar los datos, incluso cuando la clave de autenticación correcta vuelva a estar disponible.
SSD X577_PHM2800MCTO 800GB NSE con revisiones de firmware superiores	1024	Permanente. No se pueden recuperar los datos, incluso cuando la clave de autenticación correcta vuelva a estar disponible.
El resto de modelos de SSD	1024	Permanente. No se pueden recuperar los datos, incluso cuando la clave de autenticación correcta vuelva a estar disponible.

Para todos los tipos de SED, una autenticación correcta restablece el recuento de prueba a cero.

Si encuentra esta situación en la que se detiene el sistema de almacenamiento debido a un error en el cual se llega a los servidores de gestión de claves especificados, primero debe identificar y corregir la causa del error de comunicación antes de intentar seguir arrancando el sistema de almacenamiento.

Deshabilitar el cifrado ONTAP de forma predeterminada

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. Si es necesario, puede deshabilitar el cifrado de forma predeterminada en todo el clúster.

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.

Paso

1. Para deshabilitar el cifrado de forma predeterminada para todo el clúster en ONTAP 9.7 o posterior, ejecute el siguiente comando:

   ```
   options -option-name encryption.data_at_rest_encryption.disable_by_default
   -option-value on
   ```