Gestione el cifrado de NetApp

ONTAP 9

NetApp
February 12, 2026

Tabla de contenidos

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--------------------------
    TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
    QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
    dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAAACgAAAAAAAAAAA
    3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAAAA
    IgAAAAAAAAAAoAAAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAAAJAGr3tJA/LRzU
    QRHwv+1aWvAAAAAAAAAAAACQAAAAAAAAAAgAAAAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
    BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
    AQAAAAMAAAAYAQAAAAAAAADA5/ccAAAAAIgAAAAAAAAAAoAAAAAAAAAAAEOTcR0AAAAA
    AAAAAAAAAAACAAAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAAACIAAAAAAAAAAA
    KAAAAAAAAAACI8z/bAAAAAAAAAAAAAAAAAgAAAAAAAAAQAbxMcI4qiaMS4Uts5tTUnU
    AAAAAAAAAAAkAAAAAAAAAAAIAAAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5Smyj
    LSgoK/qc8FAmMMcrRXY6uriulnL0WPB/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAAwAAABgBAAAAAAAAAAA
    1cNLLwAAAAAAiAAAAAAAAAAACgAAAAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAAAIAAAAAAAAAkA
    ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAAAAIgAAAAAAAAAAAoAAAAAAAAAAAJ4/cQsAAAAA
    AAAAAAAAAAACAAAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAAAAACQAAAAAAAAAAA
    gAAAAAAAAAAAAN3Zq7AAAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rrH4nPQM0n
    rDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    ---------------------------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 :

```
clusterl::> 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:

```
cluster1::> 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
   ```