Eliminar datos de forma segura en un volumen cifrado

ONTAP 9

NetApp
April 13, 2024

This PDF was generated from https://docs.netapp.com/es-es/ontap/encryption-at-rest/secure-purge-data-encrypted-volume-concept.html on April 13, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Eliminar datos de forma segura en un volumen cifrado 1
Purgue los datos de forma segura en una información general de los volúmenes cifrados 1
Purgue los datos de forma segura en un volumen cifrado sin ninguna relación de SnapMirror 2
Purgue los datos de forma segura en un volumen cifrado con una relación de SnapMirror asíncrono 3
Limpie los datos en un volumen cifrado con una relación de SnapMirror síncrono 5

Eliminar datos de forma segura en un volumen cifrado

Purgue los datos de forma segura en una información general de los volúmenes cifrados

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 se pueden cambiar con `secure purge re-encryption-method [volume-move|in-place-rekey]` 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 se pueden cambiar con `secure purge delete-all-snapshots [true|false]` 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 hay copias Snapshot ocupadas en el volumen, debe liberar las copias Snapshot 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.

Purgue los datos de forma segura en un volumen cifrado sin ninguna relación de 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 utilizar el `volume encryption secure-purge show` comando para ver el estado de la operación. Puede utilizar el `volume encryption secure-purge abort` 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 manera segura los archivos eliminados de `vol1` En 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
   ```

Purgue los datos de forma segura en un volumen cifrado con una relación de SnapMirror asíncrono

A partir de ONTAP 9.8, puede utilizar una purga segura para datos «crub» sin interrupciones en volúmenes habilitados para NVE 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 utilizar el `volume encryption secure-purge show` comando para ver el estado de la operación. Puede utilizar el `volume encryption secure-purge abort` 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 con cada volumen de la relación de SnapMirror asíncrono.

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

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

5. Si los archivos que desea purgar de forma segura están en las copias snapshot básicas, haga lo siguiente:

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

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

   b. Actualización de SnapMirror para hacer avanzar la copia snapshot básica:

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

   Repita este paso con cada volumen de la relación de SnapMirror asíncrono.

a. Repita los pasos (a) y (b) igual al número de copias Snapshot base y una.

   Por ejemplo, si tiene dos copias Snapshot base, deberá repetir los pasos (a) y (b) tres veces.

b. Compruebe que la copia Snapshot básica está presente:
   `snapshot show -vserver SVM_name -volume volume_name`

c. Elimine la copia Snapshot básica:
   `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 con cada volumen de la relación de SnapMirror asíncrono.

   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`

Limpie los datos en un volumen cifrado con una relación de SnapMirror síncrono

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 de SnapMirror síncrono.

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 utilizar el `volume encryption secure-purge show` comando para ver el estado de la operación. Puede utilizar el `volume encryption secure-purge abort` 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 con el otro volumen de la relación de SnapMirror síncrono.

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

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

5. Si el archivo de purga segura está en la base o en copias snapshot comunes, actualice SnapMirror para mover la copia snapshot común hacia delante:

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

   Existen dos copias Snapshot comunes, por lo que este comando debe emitirse dos veces.

6. Si el archivo de purga segura está en la copia Snapshot coherente con las aplicaciones, elimine la copia Snapshot en ambos volúmenes de la relación de SnapMirror síncrono:

   ```
   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 con cada volumen de la relación de SnapMirror síncrono.

   El siguiente comando purga de forma segura los archivos eliminados en «'vol1'» en la SMV «'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 de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.