Securely purge data on an encrypted volume

ONTAP 9

NetApp
July 19, 2023

Table of Contents

Securely purge data on an encrypted volume

Securely purge data on an encrypted volume overview

Beginning with ONTAP 9.4, you can use secure purge to non-disruptively scrub data on NVE-enabled volumes. Scrubbing data on an encrypted volume ensures that it cannot be recovered from the physical media, for example, in cases of “spillage,” where data traces may have been left behind when blocks were overwritten, or for securely deleting a vacating tenant’s data.

Secure purge works only for previously deleted files on NVE-enabled volumes. You cannot scrub an unencrypted volume. You must use KMIP servers to serve keys, not the onboard key manager.

Considerations for using secure purge

- Volumes created in an aggregate enabled for NetApp Aggregate Encryption (NAE) do not support secure purge.
- Secure purge works only for previously deleted files on NVE-enabled volumes.
- You cannot scrub an unencrypted volume.
- You must use KMIP servers to serve keys, not the onboard key manager.

Secure purge functions differently depending upon your version of ONTAP.

ONTAP 9.8 and later

- Secure purge is supported by MetroCluster and FlexGroup.
- If the volume being purged is the source of a SnapMirror relationship, you do not have to break the SnapMirror relationship to perform a secure purge.
- The re-encryption method is different for volumes using SnapMirror data protection versus volumes not using SnapMirror data protection (DP) or those using SnapMirror extended data protection..
  - By default, volumes using SnapMirror data protection (DP) mode re-encrypt data using the volume move re-encryption method.
  - By default, volumes not using SnapMirror data protection or volumes using SnapMirror extended data protection (XDP) mode use the in-place re-encryption method.
  - These defaults can be changed using the `secure purge re-encryption-method [volume-move|in-place-rekey]` command.
- By default, all Snapshot copies in FlexVol volumes are automatically deleted during the secure purge operation. By default, Snapshots in FlexGroup volumes and volumes using SnapMirror data protection are not automatically deleted during the secure purge operation. These defaults can be changed using the `secure purge delete-all-snapshots [true|false]` command.

ONTAP 9.7 and earlier:

- Secure purge does not support the following:
  - FlexClone
  - SnapVault
  - FabricPool
- If the volume being purged is the source of a SnapMirror relationship, you must break the SnapMirror relationship before you can purge the volume.

  If there are busy Snapshot copies in the volume, you must release the Snapshot copies before you can purge the volume. For example, you may need to split a FlexClone volume from its parent.
- Successfully invoking the secure-purge feature triggers a volume move that re-encrypts the remaining, unpurged data with a new key.

  The moved volume remains on the current aggregate. The old key is automatically destroyed, ensuring that purged data cannot be recovered from the storage media.

Securely purge data on an encrypted volume without a SnapMirror relationship

Beginning with ONTAP 9.4, you can use secure-purge to non-disruptively “scrub” data on NVE-enabled volumes.

What you’ll need

- You must be a cluster administrator to perform this task.
- Advanced privileges are required for this task.

About this task

Secure-purge may take from several minutes to many hours to complete, depending on the amount of data in the deleted files. You can use the `volume encryption secure-purge show` command to view the status of the operation. You can use the `volume encryption secure-purge abort` command to terminate the operation.

> In order to do a secure purge on a SAN host, you must delete the entire LUN containing the files you want to purge, or you must be able to punch holes in the LUN for the blocks that belong to the files you want purge. If you cannot delete the LUN or your host operating system does not support punching holes in the LUN, you cannot perform a secure purge.

Steps

1. Delete the files or the LUN you want to securely purge.
   - On a NAS client, delete the files you want to securely purge.
   - On a SAN host, delete the LUN you want to securely purge or punch holes in the LUN for the blocks that belong to the files you want to purge.
2. On the storage system, change to advanced privilege level:

   ```
   set -privilege advanced
   ```

3. If the files you want to securely purge are in snapshots, delete the snapshots:

   ```
   snapshot delete -vserver SVM_name -volume vol_name -snapshot
   ```

4. Securely purge the deleted files:

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

   The following command securely purges the deleted files on `vol1` on SVM`vs1`:

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

5. Verify the status of the secure-purge operation:

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

Securely purge data on an encrypted volume with an Asynchronous SnapMirror relationship

Beginning with ONTAP 9.8, you can use a secure purge to non-disruptively “scrub” data on NVE-enabled volumes with an Asynchronous SnapMirror relationship.

What you’ll need

- You must be a cluster administrator to perform this task.
- Advanced privileges are required for this task.

About this task

Secure-purge may take from several minutes to many hours to complete, depending on the amount of data in the deleted files. You can use the `volume encryption secure-purge show` command to view the status of the operation. You can use the `volume encryption secure-purge abort` command to terminate the operation.

> In order to do a secure purge on a SAN host, you must delete the entire LUN containing the files you want to purge, or you must be able to punch holes in the LUN for the blocks that belong to the files you want purge. If you cannot delete the LUN or your host operating system does not support punching holes in the LUN, you cannot perform a secure purge.

Steps

1. On the storage system, change to advanced privilege level:

   ```
   set -privilege advanced
   ```

2. Delete the files or the LUN you want to securely purge.
   - On a NAS client, delete the files you want to securely purge.
   - On a SAN host, delete the LUN you want to securely purge or punch holes in the LUN for the blocks that belong to the files you want to purge.
3. Prepare the destination volume in the Asynchronous relationship to be securely purged:

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

   Repeat this step on each volume in your Asynchronous SnapMirror relationship.

4. If the files you want to securely purge are in Snapshot copies, delete the Snapshot copies:

   ```
   snapshot delete -vserver SVM_name -volume vol_name -snapshot
   ```

5. If the files you want to securely purge are in the base Snapshot copies, do the following:
   a. Create a Snapshot copy on the destination volume in the Asynchronous SnapMirror relationship:

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

   b. Update SnapMirror to move the base Snapshot copy forward:

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

      Repeat this step for each volume in the Asynchronous SnapMirror relationship.

   c. Repeat steps (a) and (b) equal to the number of base Snapshot copies plus one.

      For example, if you have two base Snapshot copies, you should repeat steps (a) and (b) three times.

   d. Verify that the base Snapshot copy is present:
      `snapshot show -vserver SVM_name -volume vol_name`
   e. Delete the base Snapshot copy:
      `snapshot delete -vserver SVM_name -volume vol_name -snapshot snapshot`

6. Securely purge the deleted files:

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

   Repeat this step on each volume in the Asynchronous SnapMirror relationship.

   The following command securely purges the deleted files on “vol1” on SVM “vs1”:

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

7. Verify the status of the secure purge operation:

   `volume encryption secure-purge show`

Scrub data on an encrypted volume with a Synchronous SnapMirror relationship

Beginning with ONTAP 9.8, you can use a secure purge to non-disruptively “scrub” data on NVE-enabled volumes with a Synchronous SnapMirror relationship.

What you’ll need

- You must be a cluster administrator to perform this task.
- Advanced privileges are required for this task.

About this task

A secure purge might take from several minutes to many hours to complete, depending on the amount of data in the deleted files. You can use the `volume encryption secure-purge show` command to view the status of the operation. You can use the `volume encryption secure-purge abort` command to terminate the operation.

> In order to do a secure purge on a SAN host, you must delete the entire LUN containing the files you want to purge, or you must be able to punch holes in the LUN for the blocks that belong to the files you want purge. If you cannot delete the LUN or your host operating system does not support punching holes in the LUN, you cannot perform a secure purge.

Steps

1. On the storage system, change to advanced privilege level:

   `set -privilege advanced`

2. Delete the files or the LUN you want to securely purge.
   - On a NAS client, delete the files you want to securely purge.
   - On a SAN host, delete the LUN you want to securely purge or punch holes in the LUN for the blocks that belong to the files you want to purge.
3. Prepare the destination volume in the Asynchronous relationship to be securely purged:

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

Repeat this step for the other volume in your Synchronous SnapMirror relationship.

4. If the files you want to securely purge are in Snapshot copies, delete the Snapshot copies:

```
snapshot delete -vserver SVM_name -volume vol_A -snapshot snapshot
```

5. If the secure purge file is in the base or common Snapshot copies, update the SnapMirror to move the common Snapshot copy forward:

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

There are two common Snapshot copies, so this command must be issued twice.

6. If the secure purge file is in the application-consistent Snapshot copy, delete the Snapshot copy on both volumes in the Synchronous SnapMirror relationship:

```
snapshot delete -vserver SVM_name -volume vol_name -snapshot snapshot
```

Perform this step on both volumes.

7. Securely purge the deleted files:

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

Repeat this step on each volume in the synchronous SnapMirror relationship.

The following command securely purges the deleted files on “vol1” on SMV “vs1”.

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

8. Verify the status of the secure purge operation:

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

Copyright information

Trademark information