安全地清除加密卷上的数据

ONTAP 9

NetApp
April 24, 2024

目录

安全地清除加密卷上的数据

安全清除加密卷上的数据概述

从 ONTAP 9.4 开始，您可以使用安全清除功能无中断擦洗启用了 NVE 的卷上的数据。擦除加密卷上的数据可确保无法从物理介质恢复数据，例如，在 " s占用， " 的情况下，覆盖块时可能会留下数据跟踪，或者用于安全删除空出租户的数据。

安全清除仅适用于启用了 NVE 的卷上先前删除的文件。您不能擦除未加密的卷。您必须使用 KMIP 服务器提供密钥，而不是板载密钥管理器。

使用安全清除的注意事项

- 在为NetApp聚合加密(NAE)启用的聚合中创建的卷不支持安全清除。
- 安全清除仅适用于启用了 NVE 的卷上先前删除的文件。
- 您不能擦除未加密的卷。
- 您必须使用 KMIP 服务器提供密钥，而不是板载密钥管理器。

安全清除功能因 ONTAP 版本而异。

ONTAP 9.8及更高版本

- MetroCluster 和 FlexGroup 支持安全清除。
- 如果要清除的卷是 SnapMirror 关系的源，则无需中断 SnapMirror 关系即可执行安全清除。
- 对于使用 SnapMirror 数据保护的卷，重新加密方法与不使用 SnapMirror 数据保护（ DP ）或使用 SnapMirror 扩展数据保护的卷不同。
  - 默认情况下，使用 SnapMirror 数据保护（ DP ）模式的卷使用卷移动重新加密方法重新加密数据。
  - 默认情况下，未使用 SnapMirror 数据保护的卷或使用 SnapMirror 扩展数据保护（ XDP ）模式的卷使用原位重新加密方法。
  - 可以使用更改这些默认值 `secure purge re-encryption-method [volume-move|in-place-rekey]` 命令：
- 默认情况下， FlexVol 卷中的所有 Snapshot 副本都会在安全清除操作期间自动删除。默认情况下，在安全清除操作期间，不会自动删除使用 SnapMirror 数据保护的 FlexGroup 卷和卷中的快照。可以使用更改这些默认值 `secure purge delete-all-snapshots [true|false]` 命令：

ONTAP 9.7及更早版本：

- 安全清除不支持以下内容：
  - FlexClone
  - SnapVault
  - FabricPool
- 如果要清除的卷是 SnapMirror 关系的源，则必须先断开 SnapMirror 关系，然后才能清除该卷。

  如果卷中的 Snapshot 副本繁忙，则必须先释放 Snapshot 副本，然后才能清除卷。例如，您可能需要将 FlexClone 卷从其父卷拆分。

- 成功调用安全清除功能将触发卷移动，以便使用新密钥重新加密其余未清除的数据。

  移动的卷将保留在当前聚合上。旧密钥会自动销毁，以确保已清除的数据无法从存储介质恢复。

安全地清除加密卷上的数据，而不存在 **SnapMirror** 关系

从 ONTAP 9.4 开始，您可以使用安全清除功能在启用了 NVE 的卷上无中断地生成 " `scrub` " 数据。

关于此任务

完成安全清除可能需要几分钟到数小时，具体取决于已删除文件中的数据量。您可以使用 `volume encryption secure-purge show` 命令以查看操作状态。您可以使用 `volume encryption secure-purge abort` 命令以终止操作。

> 要在 SAN 主机上执行安全清除，您必须删除包含要清除的文件的整个 LUN ，或者您必须能够在 LUN 中为属于要清除的文件的块打孔。如果无法删除 LUN ，或者主机操作系统不支持 LUN 中的打孔，则无法执行安全清除。

开始之前

- 您必须是集群管理员才能执行此任务。
- 此任务需要高级权限。

步骤

1. 删除要安全清除的文件或 LUN 。
   - 在 NAS 客户端上，删除要安全清除的文件。
   - 在 SAN 主机上，删除要安全清除的 LUN ，或者为要清除的文件中的块打孔。
2. 在存储系统上，更改为高级权限级别：

   ```
   set -privilege advanced
   ```

3. 如果要安全清除的文件位于快照中，请删除这些快照：

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

4. 安全清除已删除的文件：

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

   以下命令可安全清除上已删除的文件 `vol1` 在SVM上`vs1`：

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

5. 验证安全清除操作的状态：

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

使用异步 SnapMirror 关系安全地清除加密卷上的数据

从 ONTAP 9.8 开始，您可以使用安全清除功能在具有异步 SnapMirror 关系且已启用 NVE 的卷上无中断地传输 " `scrub` " 数据。

开始之前

- 您必须是集群管理员才能执行此任务。
- 此任务需要高级权限。

关于此任务

完成安全清除可能需要几分钟到数小时，具体取决于已删除文件中的数据量。您可以使用 `volume encryption secure-purge show` 命令以查看操作状态。您可以使用 `volume encryption secure-purge abort` 命令以终止操作。

> 要在 SAN 主机上执行安全清除，您必须删除包含要清除的文件的整个 LUN ，或者您必须能够在 LUN 中为属于要清除的文件的块打孔。如果无法删除 LUN ，或者主机操作系统不支持 LUN 中的打孔，则无法执行安全清除。

步骤

1. 在存储系统上、切换到高级权限级别：

   ```
   set -privilege advanced
   ```

2. 删除要安全清除的文件或 LUN 。
   - 在 NAS 客户端上，删除要安全清除的文件。
   - 在 SAN 主机上，删除要安全清除的 LUN ，或者为要清除的文件中的块打孔。

3. 准备异步关系中要安全清除的目标卷：

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

   对异步 SnapMirror 关系中的每个卷重复此步骤。

4. 如果要安全清除的文件位于 Snapshot 副本中，请删除 Snapshot 副本：

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

5. 如果要安全清除的文件位于基本 Snapshot 副本中，请执行以下操作：

   a. 在异步 SnapMirror 关系中的目标卷上创建 Snapshot 副本：

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

   b. 更新 SnapMirror 以将基本 Snapshot 副本向前移动：

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

   对异步 SnapMirror 关系中的每个卷重复此步骤。

   a. 重复步骤（a）和（b），使其等于基本 Snapshot 副本数加 1 。

      例如，如果您有两个基本 Snapshot 副本，则应重复步骤（a）和（b）三次。

   b. 验证是否存在基本Snapshot副本：
      `snapshot show -vserver SVM_name -volume volume_name`

   c. 删除基本Snapshot副本：
      `snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot`

6. 安全清除已删除的文件：

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

对异步 SnapMirror 关系中的每个卷重复此步骤。

以下命令可安全清除 SVM "`vs1` " 上 "`vol1` " 上的已删除文件：

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

7. 验证安全清除操作的状态：

   `volume encryption secure-purge show`

擦除具有同步 SnapMirror 关系的加密卷上的数据

从ONTAP 9.8开始、您可以使用安全清除功能无故障"擦除"启用了NVE且具有同步SnapMirror关系的卷上的数据。

关于此任务

安全清除可能需要几分钟到几小时才能完成，具体取决于已删除文件中的数据量。您可以使用 `volume encryption secure-purge show` 命令以查看操作状态。您可以使用 `volume encryption secure-purge abort` 命令以终止操作。

> 要在 SAN 主机上执行安全清除，您必须删除包含要清除的文件的整个 LUN ，或者您必须能够在 LUN 中为属于要清除的文件的块打孔。如果无法删除 LUN ，或者主机操作系统不支持 LUN 中的打孔，则无法执行安全清除。

开始之前

- 您必须是集群管理员才能执行此任务。
- 此任务需要高级权限。

步骤

1. 在存储系统上，更改为高级权限级别：

   `set -privilege advanced`

2. 删除要安全清除的文件或 LUN 。
   - 在 NAS 客户端上，删除要安全清除的文件。
   - 在 SAN 主机上，删除要安全清除的 LUN ，或者为要清除的文件中的块打孔。
3. 准备异步关系中要安全清除的目标卷：

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

   对同步 SnapMirror 关系中的另一个卷重复此步骤。

4. 如果要安全清除的文件位于 Snapshot 副本中，请删除 Snapshot 副本：

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

5. 如果安全清除文件位于基本 Snapshot 副本或通用 Snapshot 副本中，请更新 SnapMirror 以将通用 Snapshot 副本前移：

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

   有两个通用 Snapshot 副本，因此必须发出此命令两次。

6. 如果安全清除文件位于应用程序一致的 Snapshot 副本中，请删除同步 SnapMirror 关系中两个卷上的 Snapshot 副本：

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

   对两个卷执行此步骤。

7. 安全清除已删除的文件：

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

   对同步 SnapMirror 关系中的每个卷重复此步骤。

   以下命令可安全清除 SMV"`vs1` " 上 "`vol1` " 上已删除的文件。

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

8. 验证安全清除操作的状态：

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