安全地清除加密磁碟區上的資料
ONTAP 9

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/zh-tw/ontap/encryption-at-rest/secure-purge-data-encrypted-volume-concept.html on April 24, 2024. Always check docs.netapp.com for the latest.

目錄

安全地清除加密磁碟區上的資料 1
在加密磁碟區總覽中安全清除資料 1
安全地清除加密磁碟區上的資料、而無需SnapMirror關係 2
使用非同步SnapMirror關係、安全地清除加密磁碟區上的資料 3
以同步SnapMirror關係來清理加密磁碟區上的資料 5

安全地清除加密磁碟區上的資料

在加密磁碟區總覽中安全清除資料

從支援NVE的磁碟區開始、您可以使用安全清除功能、在不中斷營運的情況下清除資料。ONTAP加密磁碟區上的資料清理功能可確保資料無法從實體媒體中恢復、例如在「資源回收」的情況下、資料追蹤可能會在區塊遭到覆寫時留下、或是安全地刪除租戶的資料。

安全清除僅適用於已啟用NVE的磁碟區上先前刪除的檔案。您無法清理未加密的Volume。您必須使用KMIP伺服器來提供金鑰、而非內建金鑰管理程式。

使用安全清除的考量事項

- 在啟用NetApp Aggregate Encryption（NAE）的Aggregate中建立的磁碟區不支援安全清除。
- 安全清除僅適用於已啟用NVE的磁碟區上先前刪除的檔案。
- 您無法清理未加密的Volume。
- 您必須使用KMIP伺服器來提供金鑰、而非內建金鑰管理程式。

視ONTAP 您的版本而定、安全清除功能會有所不同。

更新版本**ONTAP**

- 支援安全清除MetroCluster 功能的不受支援。FlexGroup
- 如果要清除的磁碟區是SnapMirror關係的來源、您就不需要中斷SnapMirror關係、就能執行安全的清除。
- 對於使用SnapMirror資料保護的磁碟區而言、重新加密方法不同於未使用SnapMirror資料保護（DP）或使用SnapMirror延伸資料保護的磁碟區。
  - 根據預設、使用SnapMirror資料保護（DP）模式的磁碟區會使用Volume Move Re-Encryption方法重新加密資料。
  - 根據預設、未使用SnapMirror資料保護的磁碟區或使用SnapMirror延伸資料保護（XDP）模式的磁碟區、會使用就地重新加密方法。
  - 您可以使用變更這些預設值 `secure purge re-encryption-method [volume-move|in-place-rekey]` 命令。
- 根據預設、FlexVol 在安全清除作業期間、會自動刪除所有位於Shapes Volume中的Snapshot複本。根據預設、FlexGroup 在安全清除作業期間、不會自動刪除使用SnapMirror資料保護的所有SnapMirror Volume和Snapshot快照。您可以使用變更這些預設值 `secure purge delete-all-snapshots [true|false]` 命令。

更新版本：**ONTAP**

- 安全清除不支援下列項目：
  - FlexClone
  - SnapVault
  - FabricPool
- 如果要清除的磁碟區是SnapMirror關係的來源、您必須先中斷SnapMirror關係、才能清除該磁碟區。

  如果磁碟區中有使用中的Snapshot複本、您必須先釋出Snapshot複本、才能清除該磁碟區。例如、您可能需要從其父磁碟區分割FlexClone磁碟區。

- 成功叫用安全清除功能會觸發磁碟區移動、以新金鑰重新加密其餘未清除的資料。

  移動的磁碟區會保留在目前的Aggregate上。舊金鑰會自動銷毀、確保清除的資料無法從儲存媒體中恢復。

安全地清除加密磁碟區上的資料、而無需**SnapMirror**關係

從使用支援NVE的磁碟區開始、您可以使用安全清除功能、在不中斷營運的「crub」資料中進行安全清除。ONTAP

關於這項工作

視刪除檔案中的資料量而定、安全清除可能需要數分鐘到數小時才能完成。您可以使用 `volume encryption secure-purge show` 檢視作業狀態的命令。您可以使用 `volume encryption secure-purge abort` 命令以終止作業。

若要在SAN主機上執行安全清除、您必須刪除包含您要清除之檔案的整個LUN、或者您必須能夠在LUN上為屬於您要清除之檔案的區塊鑽孔。如果您無法刪除LUN或主機作業系統不支援在LUN上打孔、則無法執行安全清除。

開始之前

- 您必須是叢集管理員才能執行此工作。
- 此工作需要進階權限。

步驟

1. 刪除您要安全清除的檔案或LUN。
   - 在NAS用戶端上、刪除您要安全清除的檔案。
   - 在SAN主機上、針對屬於您要清除之檔案的區塊、刪除您要安全清除LUN上的LUN或在LUN上鑽孔。
2. 在儲存系統上、變更為進階權限層級：

   ```
   set -privilege advanced
   ```

3. 如果您要安全清除的檔案位於快照中、請刪除快照：

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

4. 安全地清除刪除的檔案：

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

   下列命令可安全地清除上刪除的檔案 `vol1` 在 SVM 上`vs1`：

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

5. 驗證安全清除作業的狀態：

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

使用非同步SnapMirror關係、安全地清除加密磁碟區上的資料

從功能不中斷的「crub」資料、開始ONTAP 使用支援NVE的磁碟區、並與非同步SnapMirror關係、安全地清除資料。

開始之前

- 您必須是叢集管理員才能執行此工作。
- 此工作需要進階權限。

關於這項工作

視刪除檔案中的資料量而定、安全清除可能需要數分鐘到數小時才能完成。您可以使用 `volume encryption`

`secure-purge show` 檢視作業狀態的命令。您可以使用 `volume encryption secure-purge abort` 命令以終止作業。

> 若要在SAN主機上執行安全清除、您必須刪除包含您要清除之檔案的整個LUN、或者您必須能夠在LUN上為屬於您要清除之檔案的區塊鑽孔。如果您無法刪除LUN或主機作業系統不支援在LUN上打孔、則無法執行安全清除。

步驟

1. 在儲存系統上、切換至進階權限層級：

   ```
   set -privilege advanced
   ```

2. 刪除您要安全清除的檔案或LUN。
   - 在NAS用戶端上、刪除您要安全清除的檔案。
   - 在SAN主機上、針對屬於您要清除之檔案的區塊、刪除您要安全清除LUN上的LUN或在LUN上鑽孔。
3. 在非同步關係中準備好要安全清除的目的地Volume：

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

   在您的「非同步SnapMirror」關係中的每個磁碟區上重複此步驟。

4. 如果您要安全清除的檔案位於Snapshot複本中、請刪除Snapshot複本：

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

5. 如果您要安全清除的檔案位於基礎Snapshot複本中、請執行下列步驟：

   a. 在非同步SnapMirror關係的目的地磁碟區上建立Snapshot複本：

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

   b. 更新SnapMirror以將基礎Snapshot複本移至下一頁：

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

   針對非同步SnapMirror關係中的每個磁碟區重複此步驟。

   a. 重複步驟（a）和（b）、等於基礎Snapshot複本數加上1。

      例如、如果您有兩個基礎Snapshot複本、則應重複步驟（a）和（b）三次。

   b. 驗證基礎 Snapshot 複本是否存在：
      `snapshot show -vserver SVM_name -volume volume_name`
   c. 刪除基礎 Snapshot 複本：
      `snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot`
6. 安全地清除刪除的檔案：

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

在非同步SnapMirror關係中的每個磁碟區上重複此步驟。

下列命令可安全清除SVM「'VS1'」上「'vol1'」上的刪除檔案：

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

7. 確認安全清除作業的狀態：

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

以同步SnapMirror關係來清理加密磁碟區上的資料

從 ONTAP 9.8 開始、您可以使用安全的清除功能、在具有同步 SnapMirror 關係的 NVE 磁碟區上進行不中斷的「清理」資料。

關於這項工作

視刪除檔案中的資料量而定、安全清除可能需要數分鐘到數小時才能完成。您可以使用 `volume encryption secure-purge show` 檢視作業狀態的命令。您可以使用 `volume encryption secure-purge abort` 命令以終止作業。

> 若要在SAN主機上執行安全清除、您必須刪除包含您要清除之檔案的整個LUN、或者您必須能夠在LUN上為屬於您要清除之檔案的區塊鑽孔。如果您無法刪除LUN或主機作業系統不支援在LUN上打孔、則無法執行安全清除。

開始之前

- 您必須是叢集管理員才能執行此工作。
- 此工作需要進階權限。

步驟

1. 在儲存系統上、變更為進階權限層級：

```
set -privilege advanced
```

2. 刪除您要安全清除的檔案或LUN。
   - 在NAS用戶端上、刪除您要安全清除的檔案。
   - 在SAN主機上、針對屬於您要清除之檔案的區塊、刪除您要安全清除LUN上的LUN或在LUN上鑽孔。
3. 在非同步關係中準備好要安全清除的目的地Volume：

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

針對同步SnapMirror關係中的其他磁碟區重複此步驟。

4. 如果您要安全清除的檔案位於Snapshot複本中、請刪除Snapshot複本：

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

5. 如果安全清除檔案位於基礎或通用Snapshot複本中、請更新SnapMirror以將通用Snapshot複本移至下一頁：

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

   共有兩個常見的Snapshot複本、因此必須發出兩次此命令。

6. 如果安全清除檔案位於應用程式一致的Snapshot複本中、請刪除同步SnapMirror關係中兩個磁碟區上的Snapshot複本：

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

   在兩個磁碟區上執行此步驟。

7. 安全地清除刪除的檔案：

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

   在同步SnapMirror關係中的每個磁碟區上重複此步驟。

   下列命令可安全清除SMV「'VS1'」上「'vol1'」上的刪除檔案。

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

8. 確認安全清除作業的狀態：

   `volume encryption secure-purge show`

版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。 美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 http://www.netapp.com/TM 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。