暗号化されたボリューム上のデータをセキュアにパージします

ONTAP 9

NetApp
April 24, 2024

目次

暗号化されたボリューム上のデータをセキュアにパージします 1
暗号化されたボリュームのデータをセキュアにパージする方法の概要 1
SnapMirror 関係なしで暗号化されたボリューム上のデータをセキュアにパージします 2
非同期 SnapMirror 関係によって暗号化されたボリューム上のデータをセキュアにパージします 4
同期 SnapMirror 関係が設定された暗号化されたボリュームのデータをスクラビングします 5

暗号化されたボリューム上のデータをセキュアにパージします

暗号化されたボリュームのデータをセキュアにパージする方法の概要

ONTAP 9.4 以降では、セキュアパージを使用して、 NVE 対応ボリューム上のデータを無停止でスクラビングできます。暗号化されたボリュームのデータをスクラビングすることで、「柱」、「ブロックが上書きされたときにデータトレースが残されている」などの物理メディアからデータをリカバリすることができなくなります。また、解約するテナントのデータを安全に削除することもできます。

セキュアパージの対象となるのは、 NVE 対応ボリューム上で以前に削除されたファイルだけです。暗号化されていないボリュームはスクラビングできません。キーの提供には、オンボードキーマネージャではなく、 KMIP サーバを使用する必要があります。

セキュアパージを使用する場合の考慮事項

- NetApp Aggregate Encryption（NAE）が有効になっているアグリゲートで作成されたボリュームでは、セキュアパージがサポートされません。
- セキュアパージの対象となるのは、 NVE 対応ボリューム上で以前に削除されたファイルだけです。
- 暗号化されていないボリュームはスクラビングできません。
- キーの提供には、オンボードキーマネージャではなく、 KMIP サーバを使用する必要があります。

セキュアパージの機能は、 ONTAP のバージョンによって異なります。

ONTAP 9.8以降

- セキュアパージは、 MetroCluster および FlexGroup でサポートされています。
- パージするボリュームが SnapMirror 関係のソースである場合は、セキュアパージを実行するために SnapMirror 関係を解除する必要はありません。
- 再暗号化の方法は、 SnapMirror データ保護を使用するボリュームと、 SnapMirror データ保護（ DP ）を使用していないボリュームまたは SnapMirror 拡張データ保護を使用しているボリュームで異なります。
  - デフォルトでは、 SnapMirror データ保護（ DP ）モードを使用するボリュームは、ボリューム移動の再暗号化方式を使用してデータを再暗号化します。
  - デフォルトでは、 SnapMirror データ保護を使用していないボリュームや SnapMirror 拡張データ保護（ XDP ）モードを使用しているボリュームでは、インプレースの再暗号化方式を使用します。
  - これらのデフォルト値は、を使用して変更できます `secure purge re-encryption-method [volume-move|in-place-rekey]` コマンドを実行します
- デフォルトでは、セキュアパージ処理の実行中に、 FlexVol ボリューム内のすべての Snapshot コピーが自動的に削除されます。デフォルトでは、 FlexGroup の Snapshot および SnapMirror データ保護を使用するボリュームは、セキュアパージ処理の実行中に自動的に削除されません。これらのデフォルト値は、を使用して変更できます `secure purge delete-all-snapshots [true|false]` コマンドを実行します

ONTAP 9.7以前：

- セキュアパージでは、次のものはサポートされません。
  - FlexClone
  - SnapVault
  - FabricPool
- パージするボリュームが SnapMirror 関係のソースである場合は、ボリュームをパージする前に SnapMirror 関係を解除する必要があります。

  ボリューム内に使用中の Snapshot コピーがある場合は、ボリュームをパージする前にその Snapshot コピーを解放する必要があります。たとえば、 FlexClone ボリュームを親ボリュームからスプリットする必要がある場合があります。

- セキュアパージ機能を呼び出すと、ボリューム移動がトリガーされ、パージされない残りのデータが新しいキーで再暗号化されます。

  移動されたボリュームは現在のアグリゲートに残ります。パージされたデータをストレージメディアからリカバリできないように、古いキーは自動的に破棄されます。

SnapMirror 関係なしで暗号化されたボリューム上のデータをセキュアにパージします

ONTAP 9.4 以降では、 NVE 対応ボリューム上で、システムを停止することなく「 crub 」データにセキュアパージを使用できます。

このタスクについて

削除されたファイルのデータ量によっては、セキュアパージが完了するまでに数分から数時間かかることがあります。を使用できます `volume encryption secure-purge show` コマンドを使用して処理のステータスを表示します。を使用できます `volume encryption secure-purge abort` コマンドを入力して処理を終了します。

> SAN ホストでセキュアパージを実行するには、パージするファイルを含む LUN 全体を削除するか、パージするファイルに属するブロックの LUN で穴を開ける必要があります。LUN を削除できない場合や、ホストオペレーティングシステムで LUN のパンチ穴がサポートされていない場合は、セキュアパージを実行できません。

作業を開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- このタスクを実行するには advanced 権限が必要です。

手順

1. セキュアパージするファイルまたは LUN を削除します。
   - NAS クライアントで、セキュアパージするファイルを削除します。
   - SAN ホストで、パージするファイルに属するブロックのために、 LUN から安全にパージまたはパンチ穴を開ける LUN を削除します。
2. ストレージシステムで、 advanced 権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

3. 安全にパージするファイルがスナップショットにある場合は、スナップショットを削除します。

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

4. 削除したファイルを安全にパージします。

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

   次のコマンドは、で削除したファイルをセキュアパージします `vol1` SVM上`vs1`：

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

5. セキュアパージ処理のステータスを確認します。

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

非同期 SnapMirror 関係によって暗号化されたボリューム上のデータをセキュアにパージします

ONTAP 9.8 以降では、非同期 SnapMirror 関係を持つ NVE 対応ボリュームで、システムを停止せずに「 crub 」データをセキュアパージできます。

作業を開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- このタスクを実行するには advanced 権限が必要です。

このタスクについて

削除されたファイルのデータ量によっては、セキュアパージが完了するまでに数分から数時間かかることがあります。を使用できます `volume encryption secure-purge show` コマンドを使用して処理のステータスを表示します。を使用できます `volume encryption secure-purge abort` コマンドを入力して処理を終了します。

> SAN ホストでセキュアパージを実行するには、パージするファイルを含む LUN 全体を削除するか、パージするファイルに属するブロックの LUN で穴を開ける必要があります。LUN を削除できない場合や、ホストオペレーティングシステムで LUN のパンチ穴がサポートされていない場合は、セキュアパージを実行できません。

手順

1. ストレージシステムで、advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. セキュアパージするファイルまたは LUN を削除します。
   - NAS クライアントで、セキュアパージするファイルを削除します。
   - SAN ホストで、パージするファイルに属するブロックのために、 LUN から安全にパージまたはパンチ穴を開ける LUN を削除します。
3. 非同期関係のデスティネーションボリュームを安全にパージするように準備します。

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

   非同期 SnapMirror 関係の各ボリュームについて、この手順を繰り返します。

4. セキュアにパージするファイルが Snapshot コピーにある場合は、 Snapshot コピーを削除します。

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

5. セキュアパージの対象となるファイルがベース Snapshot コピー内にある場合は、次の手順を実行します。

   a. 非同期 SnapMirror 関係のデスティネーションボリュームに Snapshot コピーを作成します。

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

b. SnapMirror を更新してベースの Snapshot コピーをフォワードします。

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

非同期 SnapMirror 関係のボリュームごとにこの手順を繰り返します。

a. ベース Snapshot コピーの数に 1 を加えた値と同じ手順（ a ）および（ b ）を繰り返します。

   たとえば、 2 つのベース Snapshot コピーがある場合は、手順（ a ）と（ b ）を 3 回繰り返します。

b. ベースのSnapshotコピーが存在することを確認します。 [+] `snapshot show -vserver SVM_name -volume volume_name`

c. ベースのSnapshotコピーを削除します。 [+] `snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot`

6. 削除したファイルを安全にパージします。

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

   非同期 SnapMirror 関係の各ボリュームについて、この手順を繰り返します。

   次のコマンドは、 SVM 「 vs1 」上の「 vol1 」にある削除済みファイルを安全にパージします。

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

7. セキュアパージ処理のステータスを確認します。

   `volume encryption secure-purge show`

同期 SnapMirror 関係が設定された暗号化されたボリュームのデータをスクラビングします

ONTAP 9.8以降では、セキュアパージを使用して、同期SnapMirror関係にあるNVE対応ボリュームのデータを無停止で「スクラビング」できます。

このタスクについて

削除されたファイルのデータ量によっては、セキュアパージが完了するまでに数分から数時間かかることがあります。を使用できます `volume encryption secure-purge show` コマンドを使用して処理のステータスを表示します。を使用できます `volume encryption secure-purge abort` コマンドを入力して処理を終了します。

> SAN ホストでセキュアパージを実行するには、パージするファイルを含む LUN 全体を削除するか、パージするファイルに属するブロックの LUN で穴を開ける必要があります。LUN を削除できない場合や、ホストオペレーティングシステムで LUN のパンチ穴がサポートされていない場合は、セキュアパージを実行できません。

作業を開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- このタスクを実行するには advanced 権限が必要です。

手順

1. ストレージシステムで、 advanced 権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. セキュアパージするファイルまたは LUN を削除します。
   - NAS クライアントで、セキュアパージするファイルを削除します。
   - SAN ホストで、パージするファイルに属するブロックのために、 LUN から安全にパージまたはパンチ穴を開ける LUN を削除します。

3. 非同期関係のデスティネーションボリュームを安全にパージするように準備します。

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

   同期 SnapMirror 関係にある他のボリュームに対してこの手順を繰り返します。

4. セキュアにパージするファイルが Snapshot コピーにある場合は、 Snapshot コピーを削除します。

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

5. セキュアなパージファイルがベースまたは共通の Snapshot コピーに含まれている場合は、 SnapMirror を更新して共通の Snapshot コピーをフォワードします。

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

   共通の Snapshot コピーが 2 つあるため、このコマンドは 2 回実行する必要があります。

6. セキュアなパージファイルがアプリケーションと整合性のある Snapshot コピーに含まれている場合は、同期 SnapMirror 関係にある両方のボリュームで Snapshot コピーを削除します。

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

   この手順は両方のボリュームで実行します。

7. 削除したファイルを安全にパージします。

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

   同期 SnapMirror 関係にある各ボリュームについて、この手順を繰り返します。

   次のコマンドは 'SMV "vs1 `" 上の "vol1" 上の削除されたファイルを安全にパージします

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

8. セキュアパージ処理のステータスを確認します。

   `volume encryption secure-purge show`