暗号化されたボリューム上のデータのセキュアパージ

ONTAP 9

NetApp
December 20, 2024

目次

暗号化されたボリューム上のデータのセキュアパージ

暗号化されたボリューム上のデータのセキュアパージの概要

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。

セキュアパージは、NVE対応ボリューム上で以前に削除されたファイルに対してのみ機能します。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したボリュームでは、セキュアパージはサポートされません。
- セキュアパージは、NVE対応ボリューム上で以前に削除されたファイルに対してのみ機能します。
- 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。

セキュアパージの動作は、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と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、SnapMirror関係を解除してセキュアパージを実行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）を使用しないボリューム、またはSnapMirror拡張データ保護を使用するボリュームで異なります。
  - SnapMirrorデータ保護（DP）モードを使用するボリュームでは、デフォルトでボリューム移動再暗号化方式を使用してデータが再暗号化されます。
  - SnapMirrorデータ保護を使用しないボリューム、またはSnapMirror XDP（拡張データ保護）モードを使用するボリュームでは、インプレース再暗号化方式がデフォルトで使用されます。
  - これらのデフォルト値は、コマンドを使用して変更でき `secure purge re-encryption-method [volume-move|in-place-rekey]`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およびSnapMirrorデータ保護を使用するボリューム内のSnapshotは、セキュアパージ処理で自動的に削除されません。これらのデフォルト値は、コマンドを使用して変更でき `secure purge delete-all-snapshots [true|false]`ます。

ONTAP 9 .7以前：

- セキュアパージでは、次の項目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、パージされてい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。古いキーは自動的に破棄されるため、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ません。

SnapMirror関係のない暗号化されたボリューム上のデータのセキュアパージ

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。

タスクの内容

削除されたファイル内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。処理のステータスは、コマンドを使用して確認できます `volume encryption secure-purge show`。処理を終了するには、コマンドを使用し `volume encryption secure-purge abort`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に対してLUNに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のホールパンチング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。

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。
- このタスクには高度なPrivilegesが必要です。

手順

1. セキュアパージを実行するファイルまたはLUNを削除します。
   - NASクライアントで、セキュアパージを実行するファイルを削除します。
   - SANホストで、セキュアパージを実行するLUNを削除するか、パージするファイルに属するブロックに対してLUNでホールパンチングを実行します。
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. セキュアパージを実行するファイルがSnapshotに含まれている場合は、Snapshotを削除します。

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

4. 削除したファイルのセキュアパージを実行します。

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

   次のコマンドは、SVM上`vs1`で削除したファイルのセキュアパージを実行し `vol1`ます。

   ```
   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
   ```

SnapMirror非同期関係にある暗号化されたボリューム上のデータのセキュアパージ

ONTAP 9 .8以降では、セキュアパージを使用して、SnapMirror非同期関係にあるNVE対応ボリュームで無停止でデータを「スクラビング」できます。

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。
- このタスクには高度なPrivilegesが必要です。

タスクの内容

削除されたファイル内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。処理のステータスは、コマンドを使用して確認できます `volume encryption secure-purge show`。処理を終了するには、コマンドを使用し `volume encryption secure-purge abort`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に対してLUNに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のホールパンチング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. セキュアパージを実行するファイルまたはLUNを削除します。
   - NASクライアントで、セキュアパージを実行するファイルを削除します。
   - SANホストで、セキュアパージを実行するLUNを削除するか、パージするファイルに属するブロックに対してLUNでホールパンチングを実行します。
3. 非同期関係のデスティネーションボリュームをセキュアパージする準備をします。

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

   SnapMirror非同期関係の各ボリュームに対してこの手順を繰り返します。

4. セキュアパージを実行するファイルがSnapshotコピーに含まれている場合は、Snapshotコピーを削除します。

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

5. セキュアパージを実行するファイルがベースSnapshotコピーに含まれている場合は、次の手順を実行します。
   a. SnapMirror非同期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コピーを転送します。

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

   SnapMirror非同期関係の各ボリュームに対してこの手順を繰り返します。

a. 手順（a）と（b）を、ベースSnapshotコピーの数に1を足した数だけ繰り返します。

   たとえば、ベースSnapshotコピーが2つある場合は、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. 削除したファイルのセキュアパージを実行します。

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

   SnapMirror非同期関係の各ボリュームに対し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`

SnapMirror同期関係にある暗号化されたボリュームのデータをスクラビングする

ONTAP 9 8以降では、セキュアパージを使用して、SnapMirror同期関係にある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。

タスクの内容

セキュアパージは、削除されたファイル内のデータ量によっては、完了までに数分から数時間かかることがあります。処理のステータスは、コマンドを使用して確認できます `volume encryption secure-purge show`。処理を終了するには、コマンドを使用し `volume encryption secure-purge abort`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に対してLUNに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のホールパンチング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。

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。
- このタスクには高度なPrivileges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. セキュアパージを実行するファイルまたはLUNを削除します。
   - NASクライアントで、セキュアパージを実行するファイルを削除します。
   - SANホストで、セキュアパージを実行するLUNを削除するか、パージするファイルに属するブロックに対してLUNでホールパンチングを実行します。
3. 非同期関係のデスティネーションボリュームをセキュアパージする準備をします。

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

   SnapMirror同期関係のもう一方のボリュームに対してこの手順を繰り返します。
4. セキュアパージを実行するファイルがSnapshotコピーに含まれている場合は、Snapshotコピーを削除します。

   ```
   snapshot delete -vserver <SVM_name> -volume <volume_name> -snapshot <snapshot>
   ```
5. ベースのSnapshotコピーまたは共通のSnapshotコピーにセキュアパージファイルが含まれている場合は、SnapMirrorを更新して共通のSnapshotコピーを転送します。

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

   共通のSnapshotコピーは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、SnapMirror同期関係の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. 削除したファイルのセキュアパージを実行します。

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

   SnapMirror同期関係の各ボリュームに対してこの手順を繰り返します。

   次のコマンドは 'SVM "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
   ```

著作権に関する情報

商標に関する情報