



暗号化されたボリューム上のデータのセキュア ページ 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ページ.....	1
暗号化されたボリューム上のデータのセキュアページの概要	1
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ページ.....	2
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ページ	3
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	5

暗号化されたボリューム上のデータのセキュアページ

暗号化されたボリューム上のデータのセキュアページの概要

ONTAP 9.4以降では、セキュアページを使用して、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。

セキュアページは、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。

セキュアペ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、セキュアページはサポートされません。
- セキュアページは、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。

セキュアページの動作は、ONTAPのバージョンによって異なります。

ONTAP 9.8以降

- セキュアパーズは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ズ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、セキュアパーズ処理の実行中に、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、セキュアパーズ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：

- セキュアパーズでは、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、ボリュームをパーズする前に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、ボリュームをパーズする前に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。

- セキュアパーズ機能呼び出すと、ボリューム移動がトリガーされ、パーズ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、パーズ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ズ

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ズを使用できます。

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、セキュアパーズ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ズを実行するには、パーズするファイルを含むLUN全体を削除するか、パーズ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、セキュアパーズを実行できません。

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. セキュアパーズ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、セキュアパーズを実行するファイルを削除します。
 - SANホストで、セキュアパーズを実行するLUNを削除するか、パーズ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. セキュアパーズ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ズを実行します。

```
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ズを実行し `vol1` ます。

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

5. セキュアパーズ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ズ

ONTAP 9.8以降では、セキュアパーズを使用して、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、セキュアパーズ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ズを実行するには、パーズするファイルを含むLUN全体を削除するか、パーズ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、セキュアパーズを実行できません。

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. セキュアパーズ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、セキュアパーズを実行するファイルを削除します。
- SANホストで、セキュアパーズを実行するLUNを削除するか、パーズ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ズする準備をします。

```
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. セキュアパーズ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. セキュアパーズ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. セキュアパーズ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、セキュアパーズを実行するファイルを削除します。
- SANホストで、セキュアパーズを実行するLUNを削除するか、パーズ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ズする準備をします。

```
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. セキュアパーズ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ズ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. セキュアパーズ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ズを実行します。

```
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ズします

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

8. セキュアパーズ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

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。