



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

- セキュアパーズは、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、セキュアパーズを実行するために 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 の Snapshot および SnapMirror データ保護を使用するボリュームは、セキュアパーズ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：

- セキュアパーズでは、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。

- セキュアパーズ機能呼び出すと、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ズを使用できます。

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. セキュアパーズするファイルまたは LUN を削除します。

- NAS クライアントで、セキュアパーズするファイルを削除します。
- SAN ホストで、パーズするファイルに属するブロックのために、LUN から安全にパーズ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ズ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. セキュアにパーズするファイルが 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. セキュアなパーズ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、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ズします。

```
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ズします


```
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

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。