WORMファイルの管理

ONTAP 9

NetApp
February 12, 2026

目次

WORMファイルの管理

ONTAP SnapLockでWORMファイルを管理

WORMファイルは次の方法で管理できます。

- "ファイルのWORM状態へのコミット"
- "スナップショットをボールト デスティネーションの WORM にコミットする"
- "ディザスタ リカバリ用のWORMファイルのミラーリング"
- "訴訟期間中のWORMファイルの保持"
- "WORMファイルの削除"

ONTAP SnapLockを使用してファイルをWORMにコミット

ファイルのWORM（Write Once, Read Many）状態へのコミットは、手動で、または自動的に行うことができます。追記可能WORMファイルを作成することもできます。

ファイルのWORM状態への手動コミット

ファイルを手動でWORM状態にコミットするには、ファイルを読み取り専用にします。ファイルの読み書き属性は、NFSまたはCIFSで適切なコマンドやプログラムを使用して読み取り専用に変更できます。ファイルが早期にコミットされないようアプリケーションがファイルへの書き込みを完了したことを確認したい場合や、ボリューム数が多いために自動コミット スキャナでスケーリングの問題が発生する場合は、手動でファイルをコミットすることができます。

開始する前に

- コミットするファイルがSnapLockボリュームに格納されている必要があります。
- ファイルが書き込み可能になっている必要があります。

タスク概要

コマンドまたはプログラムが実行されると、ボリュームComplianceClock時間がファイルの `ctime`フィールドに書き込まれます。ComplianceClock時間によって、ファイルの保存期間に達したかどうかが判断されます。

手順

1. 適切なコマンドまたはプログラムを使用して、ファイルの読み書き属性を読み取り専用に変更します。

   UNIXシェルでは、次のコマンドを使用して、 `document.txt`という名前のファイルを読み取り専用にします：

   ```
   chmod -w document.txt
   ```

   Windowsシェルで次のコマンドを使用して、 `document.txt`という名前のファイルを読み取り専用にします：

```
attrib +r document.txt
```

ファイルのWORM状態への自動コミット

SnapLock自動コミット機能を使用すると、ファイルを自動的にWORM状態にコミットできます。自動コミット機能は、ファイルが自動コミット期間内に変更されなかった場合、SnapLockボリューム上のファイルをWORM状態にコミットします。自動コミット機能はデフォルトで無効になっています。

開始する前に

- 自動コミットするファイルがSnapLockボリュームに格納されている必要があります。
- SnapLockがオンラインである必要があります。
- SnapLockボリュームが読み書き可能ボリュームである必要があります。

> SnapLockの自動コミット機能は、ボリューム内のすべてのファイルをスキャンし、自動コミットの要件を満たすファイルをコミットします。ファイルが自動コミットできる状態になってから、SnapLockの自動コミット スキャナによって実際にコミットされるまでに、時間が空くことがあります。ただし、ファイルは自動コミットの対象になった時点からファイルシステムによる削除や変更から保護されます。

タスク概要

_自動コミット期間_は、ファイルが自動コミットされるまでに変更されない期間を指定します。自動コミット期間が経過する前にファイルを変更すると、そのファイルの自動コミット期間が再開されます。

自動コミット期間に指定できる値は次のとおりです。

Value	単位	注記
なし	-	デフォルト
5 - 5256000	minutes	-
1 - 87600	hours	-
1 - 3650	days	-
1 - 120	months	-
1 - 10	years	-

> 最小値は5分、最大値は10年です。

手順

1. SnapLockボリュームのファイルをWORM状態に自動コミットします。

```
volume snaplock modify -vserver SVM_name -volume volume_name -autocommit
```

-period *autocommit_period*

`volume snaplock modify`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/volume-snaplock-modify.html["ONTAPコマンド リファレンス"^]を参照してください。

次のコマンドは、ファイルが5時間変更されない限り、SVM vs1のボリューム `vol1`上のファイルを自動コミットします：

```
cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -autocommit
-period 5hours
```

追記可能**WORM**ファイルの作成

追記可能なWORMファイルは、ログエントリのように増分的に書き込まれるデータを保持します。適切なコマンドやプログラムを使用してWORM追記可能ファイルを作成するか、SnapLock _ボリューム追記モード_機能を使用してデフォルトでWORM追記可能ファイルを作成することもできます。

コマンドまたはプログラムを使用した追記可能**WORM**ファイルの作成

追記可能WORMファイルは、NFSまたはCIFSで適切なコマンドやプログラムを使用して作成できます。追記可能WORMファイルには、ログ エントリのように段階的に書き込まれるデータが格納されます。データは256KBのチャンク単位でファイルに追加されます。チャンクが書き込まれるたびに、前のチャンクがWORM方式で保護されます。このファイルは保持期間が経過するまで削除できません。

開始する前に

追記可能WORMファイルはSnapLockボリュームに格納する必要があります。

タスク概要

アクティブな256 KBチャンクにデータを順番に書き込む必要はありません。ファイルのn×256KB+1バイト目にデータが書き込まれると、前の256 KBセグメントはWORM保護されます。

現在アクティブな256KBのチャンクを超える順不同の書き込みが発生すると、アクティブな256KBのチャンクが最新のオフセットにリセットされ、古いオフセットへの書き込みが失敗して「Read Only File System (ROFS)」エラーが表示されます。書き込みオフセットは、クライアント アプリケーションによって異なります。クライアントが追記可能WORMファイルの書き込みセマンティクスに準拠していないと、書き込み内容が誤って終了する可能性があります。そのため、クライアントを順不同の書き込みのオフセット制限に準拠させるか、ファイルシステムを同期モードでマウントして同期書き込みが行われるようにすることを推奨します。

手順

1. 適切なコマンドまたはプログラムを使用して、必要な保持期限を指定した空のファイルを作成します。

   UNIXシェルで、次のコマンドを使用して、 `document.txt`という名前の長さがゼロのファイルの保持時間を2020年11月21日午前6：00に設定します：

```
touch -a -t 202011210600 document.txt
```

2. 適切なコマンドまたはプログラムを使用して、ファイルの読み書き属性を読み取り専用に変更します。

   UNIXシェルでは、次のコマンドを使用して、 `document.txt`という名前のファイルを読み取り専用にします：

```
chmod 444 document.txt
```

3. 適切なコマンドまたはプログラムを使用して、ファイルの読み書き属性を書き込み可能に戻します。

   ファイル内にデータがないため、この手順はコンプライアンス リスクとはみなされません。

   UNIXシェルでは、次のコマンドを使用して、 `document.txt`という名前のファイルを書き込み可能にします：

```
chmod 777 document.txt
```

4. 適切なコマンドまたはプログラムを使用して、ファイルへのデータの書き込みを開始します。

   UNIX シェルでは、次のコマンドを使用して `document.txt`にデータを書き込みます：

```
echo test data >> document.txt
```

   ファイルにデータを追加する必要がなくなったら、ファイル権限を読み取り専用に戻してください。

ボリューム アペンド モードを使用した追記可能**WORM**ファイルの作成

ONTAP 9.3以降では、SnapLock_ボリューム追加モード_（VAM）機能を使用して、デフォルトでWORM形式の追記可能ファイルを作成できます。WORM形式の追記可能ファイルは、ログエントリのように増分的に書き込まれるデータを保持します。データは256KBのチャンク単位でファイルに追加されます。各チャンクが書き込まれるたびに、前のチャンクはWORM保護されます。保持期間が経過するまで、ファイルを削除することはできません。

開始する前に

- 追記可能WORMファイルはSnapLockボリュームに格納する必要があります。
- SnapLockボリュームはアンマウントされ、Snapshotとユーザが作成したファイルが含まれていない状態である必要があります。

タスク概要

アクティブな256 KBチャンクにデータを順番に書き込む必要はありません。ファイルのn×256KB+1バイト目

にデータが書き込まれると、前の256 KBセグメントはWORM保護されます。

ボリュームに自動コミット期間を指定している場合、追記可能WORMファイルに変更がなかった期間が自動コミット期間を超えると、そのファイルはWORM状態にコミットされます。

VAMはSnapLock監査ログ ボリュームではサポートされません。

手順

1. VAMを有効にします。

   volume snaplock modify -vserver *SVM_name* -volume *volume_name* -is-volume-append -mode-enabled true|false

   `volume snaplock modify`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/volume-snaplock-modify.html["ONTAPコマンド リファレンス"^]を参照してください。

   次のコマンドは、SVMvs1のボリューム `vol1`上でVAMを有効にします：

   ```
   cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -is-volume
   -append-mode-enabled true
   ```

2. 適切なコマンドまたはプログラムを使用して、書き込み権限を指定してファイルを作成します。

   ファイルはデフォルトで追記可能WORMファイルになります。

ONTAPヴォールト デスティネーションでSnapshotをWORMにコミットする

セカンダリストレージ上のスナップショットをWORM保護するために、SnapLock for SnapVaultを使用できます。すべての基本的なSnapLockタスクは、ボールトのデスティネーションで実行します。デスティネーションボリュームは自動的に読み取り専用でマウントされるため、スナップショットを明示的にWORMにコミットする必要はありません。

開始する前に

- System Managerを使用して関係を設定する場合は、ソースとデスティネーションの両方のクラスタでONTAP 9.15.1以降が実行されている必要があります。
- デスティネーション クラスタ：
  - "SnapLockライセンスをインストールする"。
  - "コンプライアンス クロックの初期化"。
  - ONTAP 9.10.1より前のONTAPリリースでCLIを使用している場合は、"SnapLockアグリゲートを作成する"。

- 保護ポリシーのタイプは「vault」であることが必要です。
- ソース アグリゲートとデスティネーション アグリゲートはどちらも64ビットである必要があります。
- ソース ボリュームにSnapLockボリュームを使用することはできません。
- ONTAP CLIを使用している場合は、ソース ボリュームとデスティネーション ボリュームを"ピア クラスタ"および"SVM"に作成する必要があります。

タスク概要

ソース ボリュームで使用するストレージは、NetAppのストレージでもNetApp以外のストレージでもかまいません。

WORM状態にコミットされたSnapshotの名前を変更することはできません。

SnapLockボリュームはクローニングできますが、SnapLockボリュームのファイルはクローニングできません。

LUNはSnapLockボリュームではサポートされません。LUNは、非SnapLockボリューム上で作成されたスナップショットがSnapLockヴォールト関係の一部として保護のためにSnapLockボリュームに転送される場合にのみ、SnapLockボリュームでサポートされます。LUNは読み取り / 書き込みSnapLockボリュームではサポートされません。ただし、改ざん防止スナップショットは、LUNを含むSnapMirrorソースボリュームとデスティネーション ボリュームの両方でサポートされます。

ONTAP 9.10.1以降では、SnapLockボリュームと非SnapLockボリュームを同じアグリゲートに配置できるため、ONTAP 9.10.1を使用している場合はSnapLockアグリゲートを別々に作成する必要はありません。ボリュームの「-snaplock-type」オプションを使用して、SnapLockボリューム タイプ（ComplianceまたはEnterprise）を指定します。ONTAP 9.10.1より前のリリースでは、SnapLockモード（ComplianceまたはEnterprise）はアグリゲートから継承されます。バージョンに依存しないデスティネーション ボリュームはサポートされません。デスティネーション ボリュームの言語設定とソース ボリュームの言語設定が一致している必要があります。

ボールトのデスティネーションであるSnapLockボリュームには、デフォルトの保持期間が割り当てられています。この期間の値は、SnapLock Enterpriseボリュームの場合は最小0年、SnapLock Complianceボリュームの場合は最大30年に最初に設定されます。各NetAppスナップショットは、最初にこのデフォルトの保持期間でコミットされます。必要に応じて、保持期間は後から延長することができます。詳細については、"保持時間の設定の概要"を参照してください。

ONTAP 9.14.1以降では、SnapMirror関係のSnapMirrorポリシーで特定のSnapMirrorラベルの保持期間を指定できるようになりました。これにより、ソースボリュームからデスティネーションボリュームにレプリケートされたスナップショットは、ルールで指定された保持期間の間保持されます。保持期間が指定されていない場合は、デスティネーションボリュームのデフォルトの保持期間が使用されます。

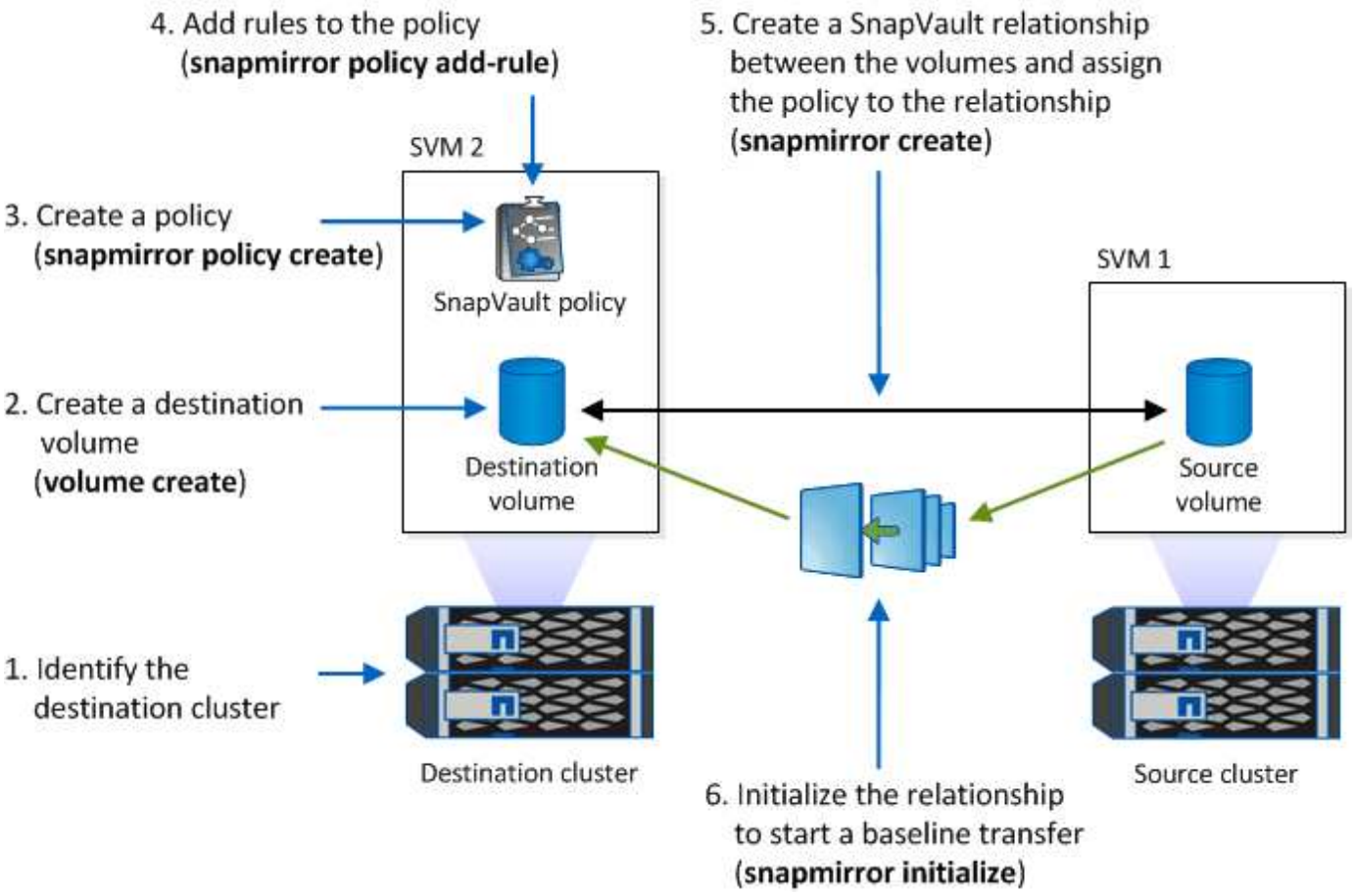
ONTAP 9.13.1から、SnapLockボルト関係のデスティネーションSnapLockボリューム上でロックされたスナップショットを、FlexCloneを作成し、 `snaplock-type`オプションを `non-snaplock`に設定し、ボリュームクローン作成操作を実行する際にスナップショットを「parent-snapshot」として指定することで、即座にリストアできます。"SnapLockタイプのFlexCloneボリュームを作成する"について詳しくはこちら。

MetroCluster構成の場合は、次の点に注意してください。

- SnapVault関係は、同期元のSVM間でのみ作成できます。同期元のSVMと同期先のSVMの間では作成できません。

- 同期元のSVMのボリュームからデータ提供用のSVMへのSnapVault関係を作成できます。
- データ提供用のSVMのボリュームから同期元のSVMのDPボリュームへのSnapVault関係を作成できます。

次の図は、SnapLockバックアップ関係を初期化する手順を示しています。



手順

ONTAP CLIを使用して、SnapLockバックアップ関係を作成できます。また、ONTAP 9.15.1以降では、System Managerを使用して、SnapLockバックアップ関係を作成できます。

System Manager

1. ボリュームがまだ存在しない場合は、ソース クラスタで*[ストレージ] > に移動し、[追加]*を選択します。
2. *ボリュームの追加*ウィンドウで、*その他のオプション*を選択します。
3. ボリュームの名前、サイズ、エクスポート ポリシー、および共有名を入力します。
4. 変更を保存します。
5. デスティネーション クラスタで、*保護 > 関係*に移動します。
6. *ソース*列の上で、*保護*を選択し、メニューから*ボリューム*を選択します。
7. ボリュームの保護 ウィンドウで、保護ポリシーとして **Vault** を選択します。
8. *ソース*セクションで、保護するクラスタ、Storage VM、ボリュームを選択します。
9. *宛先*セクションの*構成の詳細*で、*宛先スナップショットをロック*を選択し、ロック方法として*SnapLock for SnapVault*を選択します。選択したポリシータイプがタイプ `vault`ではない場合、SnapLockライセンスがインストールされていない場合、またはCompliance Clockが初期化されていない場合、*ロック方法*は表示されません。
10. まだ有効になっていない場合は、*SnapLock Complianceクロックの初期化*を選択します。
11. 変更を保存します。

CLI

1. デスティネーション クラスタで、SnapLockデスティネーション ボリュームのタイプを `DP`ソース ボリュームと同じかそれより大きいサイズで作成します：

   ```
   volume create -vserver <SVM_name> -volume <volume_name> -aggregate
   <aggregate_name> -snaplock-type <compliance|enterprise> -type DP
   -size <size>
   ```

   次のコマンドは、アグリゲート `node01_aggr`上の `SVM2`に `dstvolB`という名前の2GB のSnapLock Complianceボリュームを作成します：

   ```
   cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
   node01_aggr -snaplock-type compliance -type DP -size 2GB
   ```

2. デスティネーション クラスタで、"デフォルトの保存期間を設定する"。
3. "新しいレプリケーション関係を作成する"非SnapLockソースと作成した新しいSnapLockデスティネーションの間。

   この例では、SnapMirrorのデスティネーションSnapLockボリューム `dstvolB`との新しい関係を、`XDPDefault`のポリシーを使用して作成します。このポリシーでは、dailyおよびweeklyのラベルが付けられたSnapshotを時間単位のスケジュールでバックアップします。

```
cluster2::> snapmirror create -source-path SVM1:srcvolA -destination
-path SVM2:dstvolB -vserver SVM2 -policy XDPDefault -schedule hourly
```

"カスタム レプリケーション ポリシーの作成"または、使用可能なデフォルトが適切でない場合は"カスタムスケジュール"になります。

4. デスティネーションSVMで、作成したSnapVault関係を初期化します。

```
snapmirror initialize -destination-path <destination_path>
```

次のコマンドは、 `SVM1`のソース ボリューム `srcvolA`と `SVM2`のデスティネーション ボリューム `dstvolB`間の関係を初期化します：

```
cluster2::> snapmirror initialize -destination-path SVM2:dstvolB
```

5. 関係が初期化されアイドル状態になったら、デスティネーションで `snapshot show`コマンドを使用して、複製されたSnapshotに適用されたSnapLock有効期限を確認します。

この例では、SnapMirrorラベルとSnapLock有効期限を持つボリューム `dstvolB`上のSnapshotを表示します：

```
cluster2::> snapshot show -vserver SVM2 -volume dstvolB -fields
snapmirror-label, snaplock-expiry-time
```

関連情報

- "クラスタとSVMのピアリング"
- "SnapVaultを使用したボリュームのバックアップ"
- "snapmirror initialize"

災害復旧のためにONTAP SnapMirrorでWORMファイルをミラーリングする

SnapMirrorを使用すると、ディザスタ リカバリなどの目的で、地理的に離れた別の場所にWORMファイルをレプリケートできます。ソース ボリュームとデスティネーション ボリュームの両方でSnapLockが設定されていて、両方のボリュームのSnapLockモード（ComplianceまたはEnterprise）が同じである必要があります。ボリュームとファイルの主要なSnapLockプロパティがすべてレプリケートされます。

前提条件

ソースボリュームとデスティネーションボリュームは、ピアSVMを含むピアクラスタ内に作成する必要があ

ります。詳細については、 "クラスタとSVMのピアリング"を参照してください。

タスク概要

- ONTAP 9.5以降では、DP（データ保護）タイプの関係ではなく、XDP（拡張データ保護）タイプのSnapMirror関係を使用してWORMファイルをレプリケートできます。XDPモードはONTAPバージョンに依存せず、同じブロックに格納されているファイルを区別できるため、レプリケートされたComplianceモードのボリュームの再同期が大幅に容易になります。既存のDPタイプの関係をXDPタイプの関係に変換する方法については、"データ保護"を参照してください。
- DPタイプのSnapMirror関係の再同期処理は、SnapLockがデータ損失につながると判断した場合、コンプライアンスモードボリュームで失敗します。再同期処理が失敗した場合は、 `volume clone create`コマンドを使用してデスティネーションボリュームのクローンを作成できます。その後、ソースボリュームをクローンと再同期できます。
- SnapLock ボリュームの SnapMirror 関係は、async-mirror タイプの `MirrorAllSnapshots` ポリシーのみをサポートします。SnapLock ボリュームの保持期間は、そのボリューム内にあるすべての WORM ファイルの中で最大の保持期間によって決まります。デスティネーションはソースの DR コピーであるため、デスティネーションの SnapLock ボリュームの保持期間はソースと同じになります。
- SnapLock Complianceボリューム間のXDPタイプのSnapMirror関係では、関係解除後にデスティネーションのデータがソースから変化している場合も再同期がサポートされます。

  再同期時に共通のSnapshotに基づいてソースとデスティネーションの間でデータの相違が検出されると、この相違をキャプチャするためにデスティネーションで新しいSnapshotが作成されます。新しいSnapshotと共通のSnapshotの両方が次の期間ロックされます。

  - デスティネーションのボリューム有効期限
  - ボリューム有効期限が過ぎているか設定されていない場合、Snapshotは30日間ロックされます。
  - デスティネーションに法的保留がある場合、実際のボリューム有効期限はマスクされ、「`indefinite`」と表示されます。ただし、実際のボリューム有効期限の間、Snapshotはロックされます。

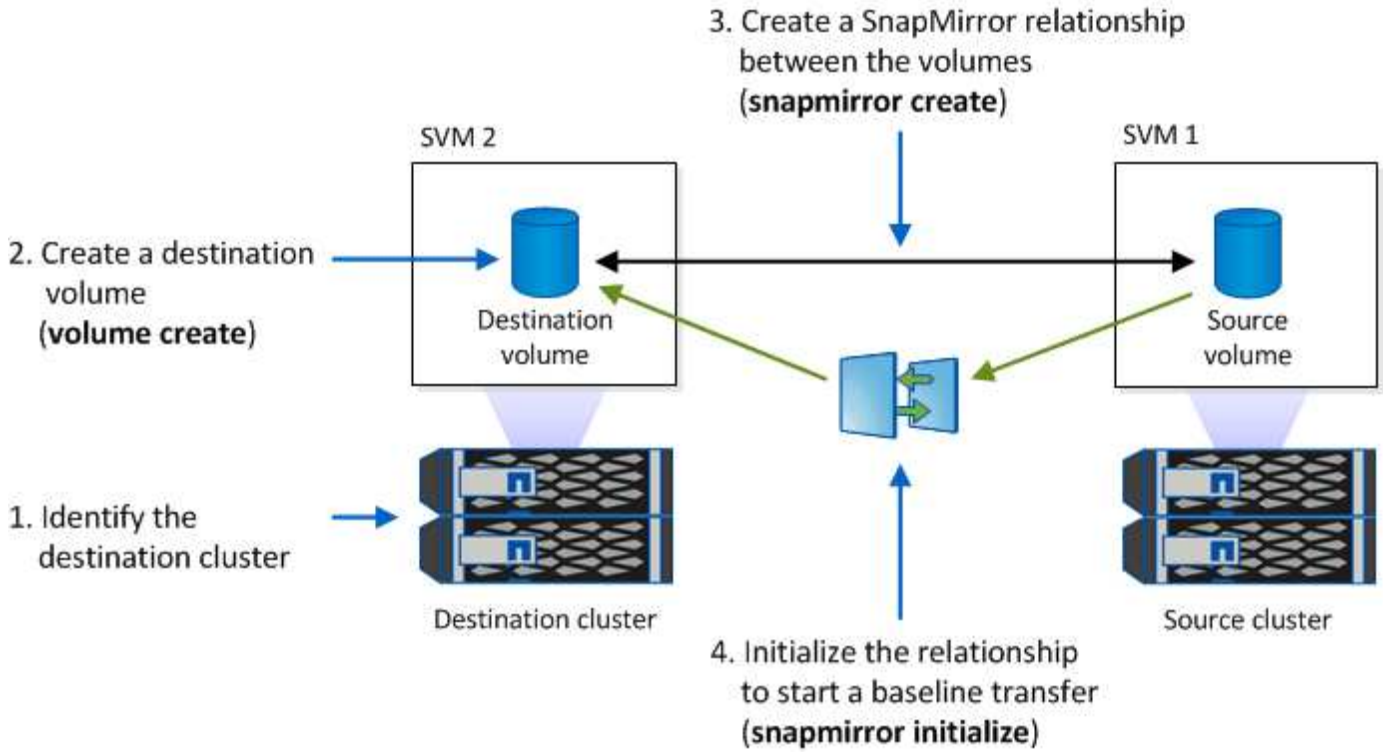
デスティネーション ボリュームの有効期限がソースよりもあとの場合、デスティネーションの有効期限が維持され、再同期後にソース ボリュームの有効期限で上書きされることはありません。

デスティネーションにソースと異なるリーガル ホールドが設定されている場合は、再同期を実行できません。再同期を試行する前に、ソースとデスティネーションに同じリーガル ホールドを設定するか、またはデスティネーションのリーガル ホールドをすべて解除する必要があります。

相違データをキャプチャするために作成された、デスティネーション ボリューム上のロックされたSnapshotは、 `snapmirror update -s snapshot`コマンドを実行することでCLIを使用してソースにコピーできます。コピーされたSnapshotは、ソースでも引き続きロックされたままになります。

- SVMデータ保護関係はサポートされません。
- 負荷共有データ保護関係はサポートされません。

次の図は、SnapMirror関係を初期化する手順を示しています。


3. Create a SnapMirror relationship between the volumes (**snapmirror create**)
SVM 2
SVM 1
2. Create a destination volume (**volume create**)
Destination volume
Source volume
1. Identify the destination cluster
Destination cluster
Source cluster
4. Initialize the relationship to start a baseline transfer (**snapmirror initialize**)

System Manager

ONTAP 9.12.1以降では、System Managerを使用して、WORMファイルのSnapMirrorレプリケーションを設定できます。

手順

1. *Storage > Volumes*に移動します。
2. *表示 / 非表示*をクリックし、*SnapLockタイプ*を選択すると、*ボリューム*ウィンドウに列が表示されます。
3. SnapLockボリュームを探します。
4. ⋮をクリックして*保護*を選択します。
5. デスティネーション クラスタとデスティネーションStorage VMを選択します。
6. *その他のオプション*をクリックします。
7. **Show legacy policies** を選択し、**DPDefault (legacy)** を選択します。
8. *Destination Configuration details*セクションで、*Override transfer schedule*を選択し、*hourly*を選択します。
9. *保存*をクリックします。
10. ソース ボリューム名の左側にある矢印をクリックしてボリュームの詳細を展開し、ページの右側でリモートSnapMirror保護の詳細を確認します。
11. リモート クラスタで、* Protection Relationships * に移動します。
12. 関係を探し、デスティネーション ボリューム名をクリックして関係の詳細を確認します。
13. デスティネーション ボリュームのSnapLockタイプおよびその他のSnapLock情報を確認します。

CLI

1. デスティネーション クラスタを特定します。
2. デスティネーション クラスタで、"SnapLockライセンスをインストールする"、"Compliance Clockを初期化する"、および ONTAP 9.10.1 より前のリリースを使用している場合は、"SnapLockアグリゲートを作成する"。
3. デスティネーション クラスタで、SnapLockデスティネーション ボリュームのタイプを `DP`ソース ボリュームと同じサイズまたはそれより大きいサイズで作成します：

```
volume create -vserver SVM_name -volume volume_name -aggregate
aggregate_name -snaplock-type compliance|enterprise -type DP -size size
```

> ONTAP 9.10.1以降では、SnapLockボリュームと非SnapLockボリュームを同じアグリゲートに配置できるため、ONTAP 9.10.1を使用している場合はSnapLockアグリゲートを別々に作成する必要はありません。ボリュームの-snaplock-typeオプションを使用して、SnapLockボリューム タイプ（ComplianceまたはEnterprise）を指定します。ONTAP 9.10.1より前のリリースでは、SnapLockモード（ComplianceまたはEnterprise）はアグリゲートから継承されます。デスティネーション ボリュームの言語設定とソース ボリュームの言語設定が一致している必要があります。

次のコマンドは、アグリゲート `node01_aggr`に `dstvolB`という名前の2 GBのSnapLock `Compliance`ボリュームを `SVM2`に作成します：

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

4. デスティネーションSVMで、SnapMirrorポリシーを作成します。

   `snapmirror policy create -vserver *SVM_name* -policy *policy_name*`

   次のコマンドは、SVM 全体のポリシー `SVM1-mirror`を作成します：

```
SVM2::> snapmirror policy create -vserver SVM2 -policy SVM1-mirror
```

5. デスティネーションSVMで、SnapMirrorスケジュールを作成します。

   `job schedule cron create -name *schedule_name* -dayofweek *day_of_week* -hour *hour* -minute *minute*`

   次のコマンドは、 `weekendcron`という名前のSnapMirrorスケジュールを作成します：

```
SVM2::> job schedule cron create -name weekendcron -dayofweek
"Saturday, Sunday" -hour 3 -minute 0
```

6. デスティネーションSVMで、SnapMirror関係を作成します。

   `snapmirror create -source-path *source_path* -destination-path *destination_path* -type XDP|DP -policy *policy_name* -schedule *schedule_name*`

   次のコマンドは、 `SVM1`のソース ボリューム `srcvolA`と `SVM2`のデスティネーション ボリューム `dstvolB`の間にSnapMirror関係を作成し、ポリシー `SVM1-mirror`とスケジュール `weekendcron`を割り当てます：

```
SVM2::> snapmirror create -source-path SVM1:srcvolA -destination
-path SVM2:dstvolB -type XDP -policy SVM1-mirror -schedule
weekendcron
```

   XDPタイプはONTAP 9.5以降で使用できます。ONTAP 9.4以前ではDPタイプを使用する必要があります。

7. デスティネーションSVMで、SnapMirror関係を初期化します。

   `snapmirror initialize -destination-path *destination_path*`

   初期化プロセスでは、デスティネーション ボリュームへの_ベースライン転送_が実行されます。SnapMirrorは、ソース ボリュームのSnapshotコピーを作成し、そのコピーとそれが参照するすべてのデータ ブロックをデスティネーション ボリュームに転送します。また、ソース ボリューム上の他のSnapshotコピーもデスティネーション ボリュームに転送されます。

次のコマンドは、 `SVM1`のソース ボリューム `srcvolA`と `SVM2`のデスティネーション ボリューム `dstvolB`間の関係を初期化します：

```
SVM2::> snapmirror initialize -destination-path SVM2:dstvolB
```

関連情報

- "クラスタとSVMのピアリング"
- "ボリュームのディザスタ リカバリの準備"
- "データ保護"
- "snapmirror create"
- "snapmirror initialize"
- "snapmirror policy create"

ONTAP SnapLock Legal Holdを使用して訴訟中にWORMファイルを保持

ONTAP 9.3 以降では、*Legal Hold* 機能を使用して、訴訟期間中コンプライアンス モードの WORM ファイルを保持できます。

開始する前に

- このタスクを実行するには、SnapLock管理者である必要があります。

  "SnapLock管理者アカウントの作成"

- セキュアな接続（SSH、コンソール、またはZAPI）でログインする必要があります。

タスク概要

リーガル ホールド中のファイルは、保持期間の制限がないWORMファイルのように機能します。リーガル ホールドの期限は管理者が指定する必要があります。

リーガル ホールドとして保存できるファイル数は、ボリュームの使用可能なスペースによって決まります。

手順

1. リーガル ホールドを開始します。

   ```
   snaplock legal-hold begin -litigation-name <litigation_name> -volume
   <volume_name> -path <path_name>
   ```

   次のコマンドは、 `vol1`内のすべてのファイルに対して法的保留を開始します：

   ```
   cluster1::>snaplock legal-hold begin -litigation-name litigation1
   -volume vol1 -path /
   ```

2. リーガル ホールドを終了します。

   ```
   snaplock legal-hold end -litigation-name <litigation_name> -volume
   <volume_name> -path <path_name>
   ```

   次のコマンドは、 `vol1`内のすべてのファイルに対する法的保留を終了します：

   ```
   cluster1::>snaplock legal-hold end -litigation-name litigation1 -volume
   vol1 -path /
   ```

関連情報

- "SnapLock legal-hold begin"
- "snaplock リーガルホールド終了"

ONTAP SnapLockでWORMファイルを削除する

privileged delete機能を使用すると、保持期間中にEnterpriseモードのWORMファイルを削除できます。この機能を使用するには、SnapLock管理者アカウントを作成し、そのアカウントを使用して機能を有効にする必要があります。

SnapLock管理者アカウントの作成

SnapLock管理者権限がないと、特権削除を実行できません。これらの権限は、vsadmin-snaplockロールで定義されています。このロールがまだ割り当てられていない場合は、クラスタ管理者に依頼して、SnapLock管理者ロールを持つSVM管理者アカウントを作成してください。

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。
- セキュアな接続（SSH、コンソール、またはZAPI）でログインする必要があります。

手順

1. SnapLock管理者ロールが割り当てられたSVM管理者アカウントを作成します。

   security login create -vserver SVM_name -user-or-group-name user_or_group_name -application application -authmethod authentication_method -role role -comment comment

   次のコマンドは、事前定義された `vsadmin-snaplock`ロールを持つ SVM 管理者アカウント `SnapLockAdmin`が、パスワードを使用して `SVM1`にアクセスできるようにします：

   ```
   cluster1::> security login create -vserver SVM1 -user-or-group-name
   SnapLockAdmin -application ssh -authmethod password -role vsadmin-
   snaplock
   ```

`security login create`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-login-create.html["ONTAPコマンド リファレンス"^]をご覧ください。

privileged delete機能の有効化

privileged delete機能は、削除するWORMファイルが格納されているEnterpriseボリュームに対して明示的に有効にする必要があります。

タスク概要

`-privileged-delete`オプションの値によって、特権削除が有効かどうかが決まります。指定できる値は`enabled`、`disabled`、`permanently-disabled`です。

`permanently-disabled`は終了状態です。状態を`permanently-disabled`に設定した後は、ボリューム上で特権削除を有効にすることはできません。

手順

1. SnapLock Enterpriseボリュームに対してprivileged deleteを有効にします。

   volume snaplock modify -vserver *SVM_name* -volume *volume_name* -privileged -delete disabled|enabled|permanently-disabled

   次のコマンドは、`SVM1`の Enterprise ボリューム`dataVol`の特権削除機能を有効にします：

   ```
   SVM1::> volume snaplock modify -vserver SVM1 -volume dataVol -privileged -delete enabled
   ```

EnterpriseモードのWORMファイルの削除

privileged delete機能を使用して、保持期間中にEnterpriseモードのWORMファイルを削除できます。

開始する前に

- このタスクを実行するには、SnapLock管理者である必要があります。
- Enterpriseボリュームで、SnapLock監査ログを作成し、privileged delete機能を有効にしておく必要があります。

タスク概要

期限切れのWORMファイルを削除するために、特権削除操作を使用することはできません。`volume file retention show`コマンドを使用して、削除するWORMファイルの保持期間を確認できます。"ONTAPコマンド

リファレンス"の `volume file retention show`の詳細をご覧ください。

手順

1. EnterpriseボリュームのWORMファイルを削除します。

   `volume file privileged-delete -vserver *SVM_name* -file *file_path*`

   次のコマンドは、SVM`SVM1`上のファイル `/vol/dataVol/f1`を削除します：

   ```
   SVM1::> volume file privileged-delete -file /vol/dataVol/f1
   ```

著作権に関する情報

商標に関する情報