WORMファイルを管理します。

ONTAP 9

NetApp
December 20, 2024

目次

WORMファイルを管理します。

WORMファイルを管理します。

WORMファイルは次の方法で管理できます。

- "ファイルをWORM状態にコミット"
- "SnapVaultデスティネーションでSnapshotコピーをWORM状態にコミットする"
- "ディザスタリカバリ用にWORMファイルをミラーリング"
- "訴訟時にWORMファイルを保持"
- "WORMファイルの削除"

ファイルを**WORM**状態にコミット

ファイルをWORM（Write Once、Read Many）にコミットするには、手動でコミットするか、自動的にコミットします。追記可能WORMファイルを作成することもできます。

ファイルを**WORM**状態に手動でコミット

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。ファイルの読み取り/書き込み属性は、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。ファイルの書き込みが完了してファイルが途中でコミットされないようにする場合や、ボリューム数が多いために自動コミットスキャナの拡張に問題がある場合は、ファイルを手動でコミットすることを選択できます。

必要なもの

- コミットするファイルがSnapLockボリューム上にある必要があります。
- ファイルは書き込み可能である必要があります。

タスクの内容

ボリュームComplianceClock時間は、コマンドまたはプログラムの実行時にファイルのフィールドに書き込まれ `ctime`ます。ComplianceClock時間に基づいて、ファイルの保持期限に達したかどうかが決まります。

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

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

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

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

ファイルを**WORM**状態に自動的にコミット

SnapLockの自動コミット機能を使用すると、ファイルをWORMに自動的にコミットできます。自動コミット機能では、自動コミット期間中に変更されなかったファイルがSnapLock ボリュームのWORM状態にコミットされます。自動コミット機能は、デフォルトでは無効になっています。

必要なもの

- 自動コミットするファイルがSnapLockボリューム上に存在している必要があります。
- SnapLockボリュームはオンラインである必要があります。
- SnapLockボリュームは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している場合は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、時間がかかることがあります。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。

タスクの内容

_autocommit_period _ は、ファイルが自動コミットされるまでに、ファイルに変更がないようにする期間を指定します。この期間が経過する前にファイルが変更された場合、自動コミット期間はもう一度最初からカウントされます。

自動コミット期間に指定できる値は次のとおりです。

値	単位	脚注
なし	-	デフォルトです。
5-5256000	分	-
1-87600	時間	-
1～3650	日	-
1 ~ 120	月	-
1 ~ 10	年	-

> 最小値は5分、最大値は10年です。

手順

1. SnapLockボリューム上のファイルを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*

すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。

次のコマンドは、5時間変更がないかぎり、SVM vs1のボリューム上のファイルを自動コミットし `vol1`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WORMファイルには、ログエントリと同様に段階的に書き込まれたデータが保持されます。追記可能 WORM ファイルは、適切なコマンドやプログラムを使用して作成するか、 SnapLock のボリュームアペンドモード機能を使用してデフォルトで作成できます。

コマンドまたはプログラムを使用して追記可能**WORM**ファイルを作成する

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、ログエントリと同様に段階的に書き込まれたデータが保持されます。データは256KBのチャンク単位でファイルに追加されます。各チャンクが書き込まれると、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。

必要なもの

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。

タスクの内容

データは、アクティブな256KBチャンクに順番に書き込まれる必要はありません。ファイルの n * 256KB+1 バイトにデータが書き込まれると、 1 つ前の 256KB セグメントが WORM 方式で保護されます。

現在アクティブな256KBチャンクを超える順序付けされていない書き込みは、アクティブな256KB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「読み取り専用ファイルシステム（ROFS）」エラーで失敗します。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。追記可能WORMファイル書き込みセマンティクスに準拠していないクライアントが原因で、書き込み内容が誤って終了する可能性があります。したがって、順序付けされていない書き込みのオフセット制限に従うか、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を確保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、という名前のゼロ長ファイルに保持期限を2020年11月21日午前6時に設定し `document.txt`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、次のコマンドを使用して、という名前のファイルを読み取り専用にし `document.txt`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、次のコマンドを使用して、という名前のファイルを書き込み可能にし `document.txt`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、次のコマンドを使用してにデータを書き込み `document.txt`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て追記可能**WORM**ファイルを作成する

ONTAP 9.3 以降では、 SnapLock のボリュームアペンドモード（ VAM ）機能を使用して、追記可能 WORM ファイルをデフォルトで作成できます。追記可能WORMファイルには、ログエントリと同様に段階的に書き込まれたデータが保持されます。データは256KBのチャンク単位でファイルに追加されます。各チャンクが書き込まれると、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。

必要なもの

- 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ボリュームがアンマウントされていて、Snapshotコピーとユーザが作成したファイルが空である必要があります。

タスクの内容

データは、アクティブな256KBチャンクに順番に書き込まれる必要はありません。ファイルの n * 256KB+1 バイトにデータが書き込まれると、 1 つ前の 256KB セグメントが WORM 方式で保護されます。

ボリュームに自動コミット期間を指定した場合、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

   すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。

   次のコマンドは、SVMvs1のボリュームでVAMを有効にし `vol1`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、書き込み権限を持つ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です。

SnapVaultデスティネーションでのSnapshotのWORM状態へのコミット

SnapLock for SnapVaultを使用すると、セカンダリストレージ上のSnapshotをWORM方式で保護できます。SnapLockの基本タスクはすべてSnapVault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、SnapshotをWORM状態に明示的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"です。
  - "コンプライアンスクロックの初期化"です。
  - 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」である必要があります。
- 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64ビットである必要があります。
- ソースボリュームをSnapLockボリュームにすることはできません。
- ONTAP CLIを使用している場合は、およびにソースボリュームとデスティネーションボリュームを作成する必要があります"ヒアリンククラスタ""SVM"。

タスクの内容

ソースボリュームでは、NetAppまたはNetApp以外のストレージを使用できます。NetApp以外のストレージの場合は、FlexArray仮想化を使用する必要があります。

WORM状態にコミットされたSnapshotの名前は変更できません。

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

SnapLockボリュームではLUNはサポートされません。SnapLockでは、SnapLock以外のボリュームで作成されたSnapshotをSnapLockバックアップ関係の一部として保護するためにSnapLockに転送する場合にのみ、LUNがサポートされます。読み取り/書き込みSnapLockボリュームではLUNはサポートされません。ただし、改ざん防止Snapshotは、SnapMirrorのソースボリュームと、LUNを含む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SnapLock以外のボリュームを同じアグリゲート上に配置できます。そのため、ONTAP 9 .10.1を使用している場合は、SnapLockアグリゲートを別途作成する必要はありません。Compliance SnapLockまたはEnterprise SnapLockのボリュームタイプを指定するには、ボリューム「-Enterprise-type」オプションを使用します。ONTAP 9 10.1より前のONTAPリリースでは、SnapLockモード（ComplianceまたはEnterprise）が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は、ソースボリュームの言語設定と一致している必要があります。

バックアップデスティネーションであるSnapLockには、デフォルトの保持期間が割り当てられています。この期間の最初の値は、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年です。各NetApp Snapshotは、最初はこのデフォルトの保持期間でコミットされます。保持期間は、必要に応じてあとから延長できます。詳細については、を参照してください "保持期限の設定の概要を確認します"。

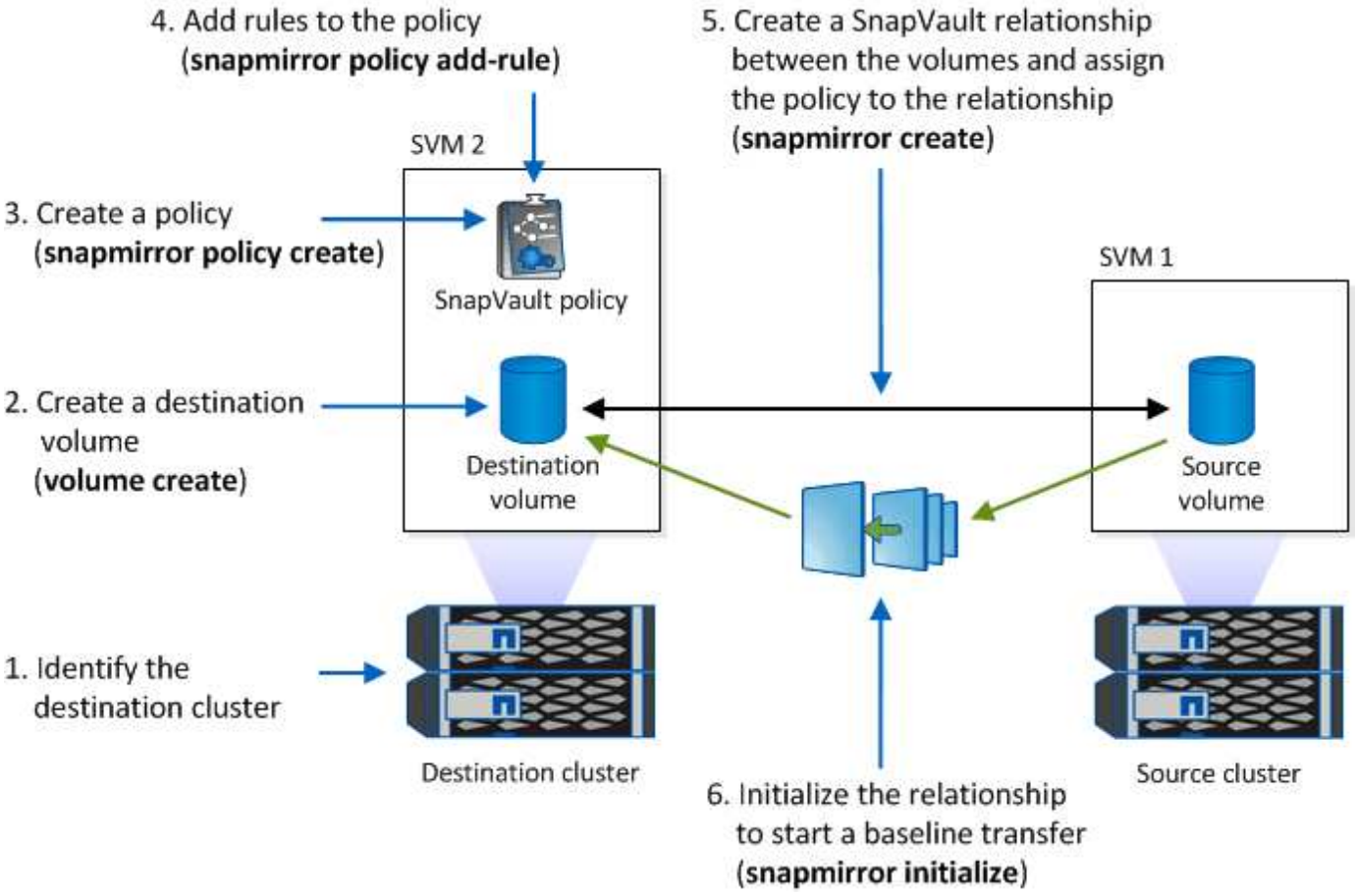
ONTAP 9.14.1以降では、SnapMirror関係のSnapMirrorポリシーに特定のSnapMirrorラベルの保持期間を指定できます。これにより、ソースボリュームからデスティネーションボリュームにレプリケートされたSnapshotが、ルールで指定された保持期間に保持されます。保持期間を指定しない場合は、デスティネーションボリュームのデフォルトの保持期間が使用されます。

ONTAP 9.13.1以降では、ボリュームクローン作成処理の実行時にオプションをに設定し `non-snaplock` てFlexCloneを作成し、そのSnapshotを「parent-snapshot」として指定することで、SnapLockバックアップ関係のデスティネーションSnapLockボリュームでロックされたSnapshotを瞬時にリストアできます。`snaplock-type`詳細については、をご覧ください "SnapLock タイプのFlexCloneボリュームを作成します"。

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、同期元のSVMと同期先のSVM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

CLIを使用してSnapLockバックアップ関係を作成することも、.15.1以降ではONTAP ONTAP 9を使用してSnapLockバックアップ関係を作成することもできます。

System Manager

1. [ストレージ]>[ボリューム]に移動し、[追加]*を選択します。
2. ウィンドウで、[その他のオプション]*を選択します。
3. ボリューム名、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. 削除を防止するためにデスティネーションSnapshotをロックする*を選択し、ロック方法*セクションで SnapLock for SnapVault *を選択します。選択したポリシータイプが「vault」でない場合、SnapLockライセンスがインストールされていない場合、またはコンプライアンスクロックが初期化されていない場合、この選択は表示されません。
5. SnapLockコンプライアンスクロックがまだ有効になっていない場合は、*[Initialize Compliance Clock]*を選択します。
6. 変更を保存します。

CLI

1. デスティネーションクラスタで、ソースボリュームと同じサイズ以上のタイプのSnapLockデスティネーションボリュームを作成し `DP`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、という名前の2GBのSnapLock Complianceボリュームを `dstvolB` `SVM2`アグリゲート上に作成し `node01_aggr`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、"デフォルトの保持期間を設定する"を実行します。
3. "新しいレプリケーション関係を作成"SnapLock以外のソースと作成した新しいSnapLockデスティネーション間。

この例では、ポリシーを使用して、dailyおよびweeklyというラベルのSnapshotを毎時スケジュールでバックアップするように、 `XDPDefault`デスティネーションSnapLockボリュームとの新しいSnapMirror関係を作成し `dstvolB`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を作成します。"または"カスタムスケジュール"、使用可能なデフォルト値が適切でない場合に使用します。

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、の `SVM1`ソースボリュームとの `SVM2`デスティネーションボリューム `dstvolB` 間の関係を初期化し `srcvolA`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コマンドを使用して `snapshot show`、レプリケートされたSnapshotに適用されているSnapLock有効期限を確認します。

   この例では、SnapMirrorラベルとSnapLockの有効期限が設定されたボリューム上のSnapshotを表示して `dstvolB`います。

```
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によるボリュームのバックアップ"

ディザスタリカバリ用にWORMファイルをミラーリング

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がSnapLock用に設定されていて、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

ピアSVMを含むピア クラスタにソース ボリュームとデスティネーション ボリュームを作成する必要があります。詳細については、を参照してください "クラスタとSVMのピアリング"。

タスクの内容

- .5以降では、ONTAP 9（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の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はるかに簡単になります。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、を参照してください"データ保護"。
- ComplianceモードのボリュームでDPタイプのSnapMirror関係を再同期する場合、再同期によってデータが失われるとSnapLockで判断されると処理は失敗します。再同期処理に失敗した場合は、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 `volume clone create`ます。その後、ソースボリュームとクローンを再同期できます。

- SnapLock準拠ボリューム間のXDPタイプのSnapMirror関係では、解除後の再同期がサポートされます。これは、解除後にデスティネーションのデータがソースから分岐していた場合でも同様です。

  再同期では、共通のSnapshotを超え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がカットされます。新しいSnapshotと共通のSnapshotの両方が次の保持期間でロックされます。

  - 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リーガルホールドが設定されている場合、実際のボリューム有効期限はマスクされて「無期限」と表示されますが、Snapshotは実際のボリューム有効期限内はロックされます。

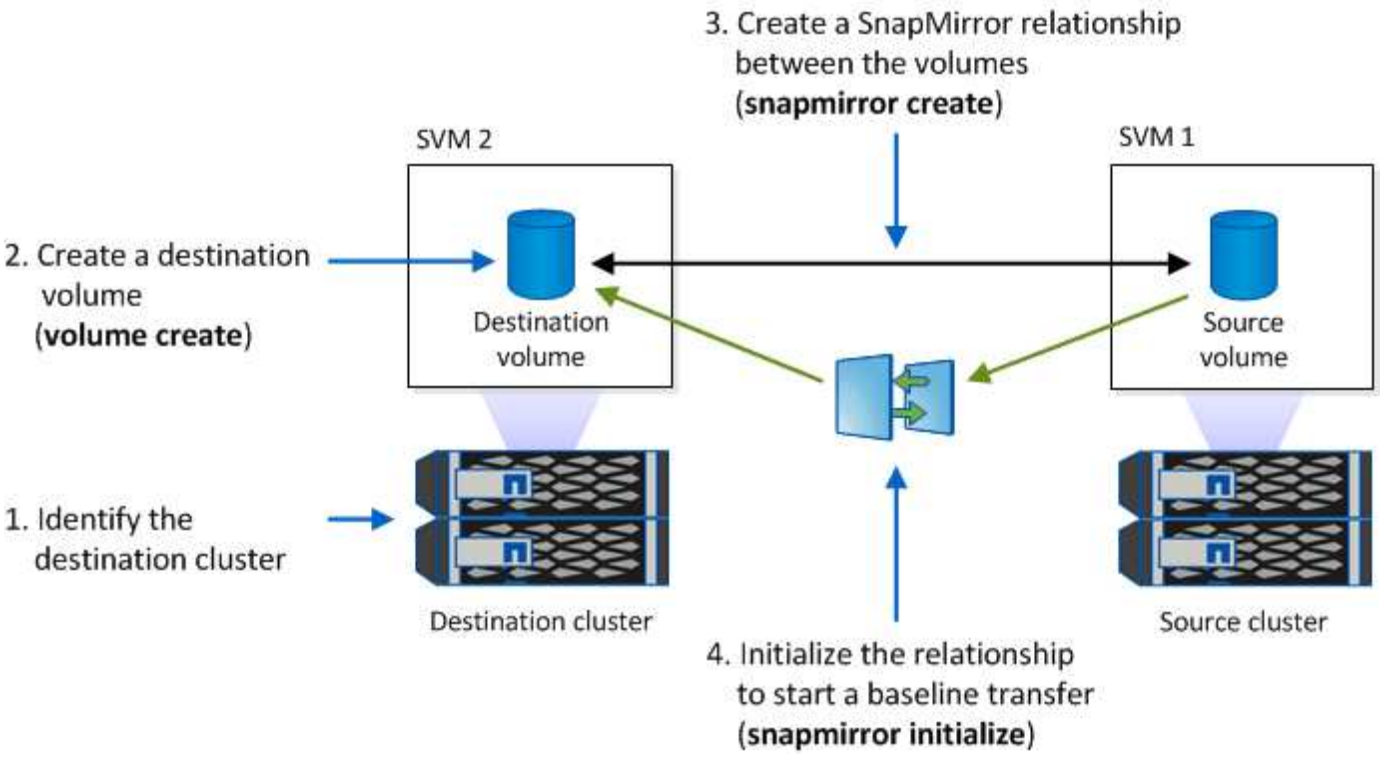
デスティネーションボリュームの有効期限がソースよりもあとの場合、デスティネーションの有効期限が保持され、再同期後にソースボリュームの有効期限で上書きされることはありません。

デスティネーションにソースとは異なるリーガルホールドが設定されている場合、再同期は許可されません。再同期を試行する前に、ソースとデスティネーションのリーガルホールドが同一であるか、デスティネーションのリーガルホールドがすべて解除されている必要があります。

異なる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コピーは、CLIでコマンドを実行してソースにコピーできます `snapmirror update -s snapshot`。コピーされたSnapshotは、ソースでも引き続きロックされます。

- 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。



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. [ストレージ]>[ボリューム]に移動します。
2. 表示/非表示*をクリックし、 SnapLock タイプ*を選択して、*ボリューム*ウィンドウに列を表示します。
3. SnapLockボリュームを探します。
4. をクリックし、*[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
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. 「接続先設定の詳細」セクションで「転送スケジュールの上書き」を選択し、「*時間単位」を選択します。
9. [保存（ Save ）] 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、「保護関係」に移動します。
12. 関係を検索し、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表示します。
13. デスティネーションボリュームのSnapLockタイプやその他の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
2. 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"、および9.10.1より前のONTAP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、ソースボリュームと同じサイズ以上のSnapLockデスティネーションボリュームを作成し `DP`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SnapLock以外のボリュームを同じアグリゲート上に配置できます。そのため、ONTAP 9 .10.1を使用している場合は、SnapLockアグリゲートを別途作成する必要はありません。ComplianceまたはEnterprise SnapLockのボリュームタイプを指定するには、volume SnapLock -typeオプションを使用します。ONTAP 9 10.1より前のONTAPリリースでは、SnapLockモード（ComplianceまたはEnterprise）が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は、ソースボリュームの言語設定と一致している必要があります。

次のコマンドは、という名前の2GBのSnapLockボリュームを `dstvolB` `SVM2`アグリゲート上に `node01_aggr`作成し `Compliance`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全体のポリシーを作成し `SVM1-mirror`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、という名前のSnapMirrorスケジュールを作成し `weekendcron`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*

   次のコマンドでは、の `SVM1`ソースボリュームとの `SVM2`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 `srcvolA`、ポリシーとスケジュールを `weekendcron`割り当て `SVM1-mirror`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コピーを作成して、そのコピーおよびコピー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その他のSnapshotコピーもデスティネーションボリュームに転送します。

次のコマンドは、の `SVM1`ソースボリュームとの `SVM2`デスティネーションボリューム `dstvolB`間の関係を初期化し `srcvolA`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"

訴訟時にリーガルホールドを使用して**WORM**ファイルを保持

ONTAP 9.3以降では、_Legal Hold_featureを使用して、ComplianceモードのWORMファイルを訴訟の期間にわたって保持できます。

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）でログインしておく必要があります。

タスクの内容

リーガルホールドの対象となるファイルは、保持期間が無期限のWORMファイルのように動作します。リーガルホールド期間の終了日を指定するのは、お客様の責任です。

リーガルホールドの対象となるファイル数は、ボリュームで使用可能なスペースによって異なります。

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、のすべてのファイルに対してリーガルホールドを開始し `vol1`ます。

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

2. リーガルホールドの終了：

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

   次のコマンドは、のすべてのファイルのリーガルホールドを終了し `vol1`ます。

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

WORMファイルの削除の概要

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。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

privileged deleteを実行するには、SnapLock管理者Privilegesが必要です。これらのPrivilegesは、SnapLockロールで定義されます。このロールが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もらいます。

必要なもの

- 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）でログインしておく必要があります。

手順

1. SnapLock管理者ロールを持つ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、事前定義されたロールが割り当てられた `vsadmin-snaplock`SVM管理者アカウントにパスワードを使用したアクセスを `SVM1`許可し `SnapLockAdmin`ます。

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

privileged delete機能を有効にする

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

タスクの内容

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

> `permanently-disabled`は、終了状態です。ボリュームで状態をに設定したあとに`privileged delete`を有効にすることはできません `permanently-disabled`。

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、の `SVM1`Enterpriseボリュームに対してprivileged delete機能を有効にし `dataVol`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。

必要なもの

- 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。

タスクの内容

privileged delete処理を使用して、期限切れのWORMファイルを削除することはできません。コマンドを使用して、削除するWORMファイルの保持期限を表示できます `volume file retention show`。詳細については、コマンドのマニュアルページを参照してください。

ステップ

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上の`SVM1`ファイルを削除し `/vol/dataVol/f1`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