SnapLockテクノロジを使用したアーカイブとコンプライアンス

ONTAP 9

NetApp
February 12, 2026

目次

SnapLockテクノロジを使用したアーカイブとコンプライアンス

ONTAP SnapLockについて学ぶ

SnapLockは、規制やガバナンスに準拠するためにWORMストレージを使用して変更不可能な状態でファイルを保管する組織向けの、ハイパフォーマンスなコンプライアンスソリューションです。

データの削除、変更、名前変更を防止でき、SEC 17a-4（f）、HIPAA、FINRA、CFTC、GDPRなどの規制に準拠することができます。専用のボリュームを作成して、指定した保持期間または永久にファイルを消去および書き換え不可能な状態で保存およびコミットできます。SnapLockでは、CIFSやNFSなどの標準オープン ファイル プロトコルにより、ファイル レベルでこのようなデータ保持を実行できます。サポートされるオープン ファイル プロトコルは、NFS（バージョン2、3、4）とCIFS（SMB 1.0、2.0、3.0）です。

SnapLockを使用すると、ファイルとスナップショットをWORMストレージにコミットし、WORM保護されたデータの保持期間を設定できます。SnapLock WORMストレージはNetAppスナップショット技術を使用し、SnapMirrorレプリケーションとSnapVaultバックアップを基盤技術として活用することで、データのバックアップ・リカバリ保護を実現します。WORMストレージの詳細については、こちらをご覧ください："NetApp SnapLockを使用した準拠のWORMストレージ - TR-4526"

アプリケーションを使用してNFSまたはCIFS経由でファイルをWORM状態にコミットするか、SnapLock自動コミット機能を使用してファイルを自動的にWORM状態にコミットすることができます。ログ情報のように増分的に書き込まれるデータを保持するには、_WORM追記可能ファイル_を使用できます。詳細については、"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"を参照してください。

SnapLockでサポートされるデータ保護方法は、ほとんどのコンプライアンス要件に対応します。

- 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。"スナップショットをWORMにコミットする" を参照してください。
- SnapMirrorを使用して、災害復旧のためにWORMファイルを別の地理的な場所に複製できます。"WORMファイルのミラーリング"を参照してください。

SnapLockは、ONTAPのライセンスベースの機能です。1つのライセンスで、SnapLockを、SEC Rule 17a-4(f)などの外部規制を満たす厳格なコンプライアンスモードと、デジタル資産の保護に関する社内規制を満たすより緩やかなエンタープライズモードで使用できます。SnapLockライセンスは、"ONTAP One"ソフトウェアスイートの一部です。

SnapLockは、すべてのAFFおよびFASシステム、さらにONTAP Selectでサポートされています。SnapLockはソフトウェアのみのソリューションではなく、ハードウェアとソフトウェアが統合されたソリューションです。この違いは、SEC 17a-4（f）のような統合されたハードウェアとソフトウェアのソリューションを要求する厳格なWORM規制にとって重要です。詳細については、"SECによる電子記憶媒体の使用に関するブローカー・ディーラー向けガイダンス"を参照してください。

SnapLockの機能

SnapLockの設定が完了したら、次のタスクを実行できます。

- "ファイルのWORM状態へのコミット"

- "セカンダリ ストレージのWORMにSnapshotをコミットする"
- "ディザスタ リカバリ用のWORMファイルのミラーリング"
- "リーガル ホールドを使用した訴訟期間中のWORMファイルの保持"
- "privileged delete機能を使用したWORMファイルの削除"
- "ファイルの保持期間の設定"
- "SnapLockボリュームの移動"
- "ランサムウェア攻撃から保護するためにSnapshotをロックする"
- "監査ログでの snapLock の使用を確認する"
- "SnapLock APIの使用"

SnapLockのComplianceモードとEnterpriseモード

SnapLockのComplianceモードとEnterpriseモードの最も大きな違いは、WORMファイルの保護レベルです。

SnapLockモード	保護レベル	保持中のWORMファイルの削除
Complianceモード	ディスク レベル	削除できません
Enterpriseモード	ファイル レベル	コンプライアンス管理者が監査済みの「特権削除」手順を使用して削除できる

保持期間が経過したあとに不要となったファイルは手動で削除する必要があります。一度WORM状態にコミットされたファイルは、ComplianceモードかEnterpriseモードかに関係なく、保持期間が経過したあとも変更することはできません。

WORMファイルは保持期間中も保持期間後も移動できません。WORMファイルはコピーできますが、コピーしたファイルはWORM状態にはなりません。

次の表に、SnapLockのComplianceモードとEnterpriseモードでサポートされる機能の違いを示します。

機能	SnapLock Compliance	SnapLock Enterprise
privileged deleteを使用したファイルの有効化と削除	いいえ	はい
ディスクの再初期化	いいえ	はい
保持期間中のSnapLockアグリゲートとボリュームの破棄	いいえ	○（SnapLock監査ログ ボリュームを除く）
アグリゲートまたはボリュームの名前変更	いいえ	はい

NetApp以外のディスクの使用	いいえ	いいえ
監査ログでのSnapLockボリュームの使用	はい	○（ONTAP 9.5以降）

SnapLockでサポートされる機能とされない機能

次の表は、SnapLock ComplianceモードとSnapLock Enterpriseモードでサポートされる機能を示しています。

機能	SnapLock Compliance に対応	SnapLock Enterprise に対応
整合性グループ	いいえ	いいえ
暗号化されたボリューム	はい、暗号化とSnapLockについて詳しくご覧ください。	はい、暗号化とSnapLockについて詳しくご覧ください。
SnapLockアグリゲート上のFabricPool	いいえ	はい、ONTAP 9.8以降で可能です。SnapLock Enterpriseアグリゲート上のFabricPoolの詳細をご覧ください。
Flash Poolアグリゲート	○	○
FlexClone	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。	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。
FlexGroupボリューム	はい、ONTAP 9.11.1 以降で可能です。[flexgroup]の詳細をご覧ください。	はい、ONTAP 9.11.1 以降で可能です。[flexgroup]の詳細をご覧ください。
LUN	いいえ。SnapLockを使用したLUNのサポートの詳細については、こちらをご覧ください。	いいえ。SnapLockを使用したLUNのサポートの詳細については、こちらをご覧ください。
MetroCluster構成	はい、ONTAP 9.3以降で可能です。MetroClusterのサポートの詳細をご覧ください。	はい、ONTAP 9.3以降で可能です。MetroClusterのサポートの詳細をご覧ください。
マルチ管理者認証（MAV）	はい、ONTAP 9.13.1 以降で可能です。MAVのサポートの詳細をご覧ください。	はい、ONTAP 9.13.1 以降で可能です。MAVのサポートの詳細をご覧ください。
SAN	いいえ	いいえ

Single File SnapRestore	いいえ	はい
SnapMirrorアクティブ同期	いいえ	いいえ
SnapRestore	いいえ	はい
SMTape	いいえ	いいえ
SnapMirror Synchronous	いいえ	いいえ
SSD	○	○
Storage Efficiency機能	はい、ONTAP 9.9.1以降で可能です。ストレージ効率のサポートの詳細をご覧ください。	はい、ONTAP 9.9.1以降で可能です。ストレージ効率のサポートの詳細をご覧ください。

SnapLock EnterpriseアグリゲートのFabricPool

ONTAP 9.8以降では、FabricPoolがSnapLock Enterpriseアグリゲートでサポートされます。ただし、アカウント チームがProduct Variance Requestを申請して、パブリック クラウドまたはプライベート クラウドに階層化されたFabricPoolのデータは、クラウド管理者が削除できるためSnapLockでは保護されないことを承諾する必要があります。

FabricPoolでパブリック クラウドまたはプライベート クラウドに階層化されたデータはクラウド管理者が削除できるため、SnapLockでは保護されなくなりました。

FlexGroupボリューム

ONTAP 9.11.1以降、SnapLockではFlexGroupボリュームがサポートされますが、次の機能はサポートされません。

- リーガル ホールド
- イベントベースの保持
- SnapLock for SnapVault（ONTAP 9.12.1以降でサポート）

また、次の点についても理解しておく必要があります。

- FlexGroupボリュームのボリューム コンプライアンス クロック（VCC）は、ルート コンスティチュエントのVCCによって決まります。すべての非ルート コンスティチュエントのVCCは、ルートのVCCと密接に同期されます。
- SnapLockの設定プロパティは、FlexGroup全体に対してのみ設定されます。個々のコンスティチュエントに、デフォルトの保持期限や自動コミット期間などの設定プロパティを指定することはできません。

LUNのサポート

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 vaultリレーションシップの一部として保護のためにSnapLockボリュームに転送されるシナリオにおいてのみ、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。

MetroClusterのサポート

MetroCluster構成でのSnapLockのサポートは、SnapLock ComplianceモードとSnapLock Enterpriseモードで異なります。

SnapLock Compliance

- ONTAP 9.3以降では、ミラーされていないMetroClusterアグリゲートでSnapLock Complianceがサポートされます。
- ONTAP 9.3以降、ミラーされたアグリゲートでは、SnapLock監査ログ ボリュームのホストとして使用する場合に限りSnapLock Complianceがサポートされます。
- MetroClusterを使用して、プライマリ サイトとセカンダリ サイトにSVM固有のSnapLock構成をレプリケートできます。

SnapLock Enterprise

- SnapLock Enterprise アグリゲートがサポートされています。
- ONTAP 9.3以降では、privileged deleteを使用するSnapLock Enterpriseアグリゲートがサポートされます。
- MetroClusterを使用して、両方のサイトにSVM固有のSnapLock構成をレプリケートできます。

MetroCluster構成とコンプライアンス クロック

MetroCluster構成では、Volume Compliance Clock（VCC;ボリューム コンプライアンス クロック）とSystem Compliance Clock（SCC;システム コンプライアンス クロック）の2つのコンプライアンス クロック メカニズムが使用されます。VCCとSCCはすべてのSnapLock構成で使用できます。ノードに新しいボリュームを作成すると、ボリュームのVCCはそのノードの現在のSCCの値に初期化されます。ボリューム作成後のボリュームとファイルの保持期限の追跡には、常にVCCが使用されます。

ボリュームを別のサイトにレプリケートすると、ボリュームのVCCも一緒にレプリケートされます。ボリュームのスイッチオーバー（サイトAからサイトB）が発生した場合、VCCの更新はサイトBで継続されますが、サイトAのSCCはサイトAがオフラインになると停止します。

サイトAがオンラインに戻ってボリュームのスイッチバックが実行されると、サイトAのSCCのクロックが再開されますが、ボリュームのVCCは引き続き更新されます。VCCは継続的に更新されるため、スイッチオーバーやスイッチバックの処理に関係なくファイルの保持期限はSCCに依存せず、期限が延びることはありません。

マルチ管理者認証（MAV）のサポート

ONTAP 9.13.1以降、クラスタ管理者はクラスタ上でマルチ管理者検証を明示的に有効にすることで、一部のSnapLock操作を実行する前にクォーラム承認を必須にすることができます。MAVを有効にすると、SnapLockボリュームプロパティ（default-retention-time、minimum-retention-time、maximum-retention-time、volume-append-mode、autocommit-period、privileged-delete）でクォーラム承認が必要になります。"MAV"の詳細をご覧ください。

ストレージ効率

ONTAP 9.9.1 以降、SnapLock は、SnapLock ボリュームおよびアグリゲートに対して、データ圧縮、ボリューム間重複排除、アダプティブ圧縮などのストレージ効率化機能をサポートしています。ストレージ効率化の詳細については、"ONTAP Storage Efficiencyの概要" を参照してください。

暗号化

ONTAPは、ストレージ メディアの転用、返却、置き忘れ、盗難に際して保存データが読み取られることがないようにソフトウェア ベースとハードウェア ベースの暗号化テクノロジを提供します。

*免責事項：*NetAppは、認証キーを紛失した場合、または認証失敗回数が規定の制限を超え、ドライブが永久にロックされた場合、自己暗号化ドライブまたはボリューム上のSnapLock保護されたWORMファイルの復旧を保証することはできません。認証失敗に対する対策はお客様の責任となります。

暗号化されたボリュームはSnapLockアグリゲートでサポートされます。

7-Modeからの移行

7-Mode Transition Toolのコピーベースの移行（CBT）機能を使用して、SnapLockボリュームを7-ModeからONTAPに移行できます。デスティネーション ボリュームのSnapLockモード（ComplianceまたはEnterprise）とソース ボリュームのSnapLockモードが一致している必要があります。コピーフリーの移行（CFT）はSnapLockボリュームの移行には使用できません。

SnapLockの設定

ONTAP SnapLockの設定について学ぶ

SnapLockを使用する前に、SnapLockボリュームを含むアグリゲートをホストする各ノードに対して"SnapLockライセンスをインストールする"を初期化する、"コンプライアンス クロック"を初期化する、ONTAP 9.10.1より前のONTAPリリースを実行しているクラスタのSnapLockアグリゲートを作成する、"SnapLockボリュームを作成してマウントする"などのさまざまなタスクを完了してSnapLockを設定する必要があります。

ONTAP Compliance Clockを初期化する

SnapLockは、WORMファイルの保存期間を変更する可能性のある改ざんを防止するため、_volume Compliance Clock_を使用します。まず、SnapLockアグリゲートをホストする各ノードで_system ComplianceClock_を初期化する必要があります。

ONTAP 9.14.1以降では、SnapLockボリュームがない場合、またはSnapshotロックが有効になっているボリュームがない場合に、システムCompliance Clockを初期化または再初期化できます。再初期化機能により、システム管理者は、システムCompliance Clockが誤って初期化された場合にリセットしたり、システムのクロックドリフトを修正したりできます。ONTAP 9.13.1以前のリリースでは、ノード上でCompliance Clockを一度初期化すると、再度初期化することはできません。

開始する前に

コンプライアンス クロックを再初期化するには：

- クラスタ内のすべてのノードが正常な状態になっている必要があります。
- すべてのボリュームがオンラインになっている必要があります。
- リカバリ キューにボリュームが存在してはいけません。
- SnapLockボリュームが存在してはいけません。
- Snapshot ロックが有効になっているボリュームは存在できません。

コンプライアンス クロックを初期化するための一般的な要件：

- 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。
- "SnapLock ライセンスはノードにインストールする必要があります"。

タスク概要

システムCompliance Clockの時刻は_ボリュームCompliance Clock_に継承されます。ボリュームCompliance Clockは、ボリューム上のWORMファイルの保存期間を制御します。ボリュームCompliance Clockは、新しいSnapLockボリュームを作成すると自動的に初期化されます。

> システム コンプライアンス クロックの初期設定は、現在のハードウェア システム クロックに基づきます。そのため、各ノードでシステム コンプライアンス クロックを初期化する前に、システム時間とタイムゾーンが正しいことを確認する必要があります。ノードでシステム コンプライアンス クロックを初期化したあとに、ロックが有効になっているSnapLockボリュームが存在する場合、再度初期化することはできません。

手順

ONTAP CLIを使用してコンプライアンス クロックを初期化できます。また、ONTAP 9.12.1以降では、System Managerを使用してコンプライアンス クロックを初期化できます。

System Manager

1. **Cluster > Overview** に移動します。
2. *ノード*セクションで、*SnapLock Complianceクロックの初期化*をクリックします。
3. コンプライアンス クロック 列を表示し、コンプライアンス クロックが初期化されていることを確認するには、クラスタ **>** 概要 **>** ノード セクションで、表示 **/** 非表示 をクリックし、**SnapLock** コンプライアンス クロック を選択します。

CLI

1. システム コンプライアンス クロックを初期化します。

   ```
   snaplock compliance-clock initialize -node node_name
   ```

   次のコマンドは、 `node1`のシステムのコンプライアンス クロックを初期化します：

   ```
   cluster1::> snaplock compliance-clock initialize -node node1
   ```

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

2. 確認のプロンプトで、システム クロックが正しいこととコンプライアンス クロックの初期化を実行することを確認します。

   ```
   Warning: You are about to initialize the secure ComplianceClock of
   the node "node1" to the current value of the node's system clock.
   This procedure can be performed only once on a given node, so you
   should ensure that the system time is set correctly before
   proceeding.

   The current node's system clock is: Mon Apr 25 06:04:10 GMT 2016

   Do you want to continue? (y|n): y
   ```

3. SnapLockアグリゲートをホストする各ノードについて、同じ手順を繰り返します。

NTPが設定されたシステムのコンプライアンス クロック再同期の有効化

NTP サーバーが構成されている場合、SnapLock コンプライアンス クロックの同期機能を有効にできます。

開始する前に

- この機能は、advanced権限レベルでのみ使用できます。

- 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。
- "SnapLock ライセンスはノードにインストールする必要があります"。
- この機能は、Cloud Volumes ONTAP、ONTAP Select、およびVSIMのプラットフォームでのみ使用できます。

タスク概要

SnapLockのセキュア クロック デーモンがしきい値を超えるスキューを検出すると、システム時間を使用してシステムとボリュームの両方のコンプライアンス クロックがリセットされます。スキューのしきい値は24時間に設定されています。つまり、システム コンプライアンス クロックはスキューが1日を超えた場合にのみシステム クロックに同期されます。

スキューの検出とシステム時間へのコンプライアンス クロックの変更は、SnapLockのセキュア クロック デーモンによって行われます。コンプライアンス クロックはシステム時間がNTPの時間と同期されている場合しかシステム時間と同期されないため、システム時間を変更してコンプライアンス クロックをシステム時間に強制的に同期しようとしても失敗します。

手順

1. NTP サーバーが構成されている場合は、SnapLock Compliance Clock 同期機能を有効にします：

   `snaplock compliance-clock ntp`

   次のコマンドは、システムの Compliance Clock 同期機能を有効にします。

   ```
   cluster1::*> snaplock compliance-clock ntp modify -is-sync-enabled true
   ```

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

2. 確認のプロンプトで、設定されているNTPサーバが信頼できることと通信チャネルがセキュアであることを確認して機能を有効にします。
3. 機能が有効になっていることを確認します。

   `snaplock compliance-clock ntp show`

   次のコマンドは、システムの Compliance Clock 同期機能が有効になっているかどうかを確認します：

   ```
   cluster1::*> snaplock compliance-clock ntp show

   Enable clock sync to NTP system time: true
   ```

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

ONTAP SnapLockアグリゲートを作成する

ボリューム `-snaplock-type`オプションを使用して、ComplianceまたはEnterprise のSnapLockボリューム タイプを指定します。ONTAP 9.10.1より前のリリースでは、別個のSnapLockアグリゲートを作成する必要があります。ONTAP 9.10.1以降では、SnapLockボリュームと非SnapLockボリュームが同じアグリゲート上に存在できるようになりました。そのため、ONTAP 9.10.1を使用している場合は、別個のSnapLockアグリゲートを作成する必要はありません。

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。
- ノード上のSnapLock "ライセンスをインストールする必要があります"。このライセンスは"ONTAP One"に含まれています。
- "ノード上のコンプライアンスクロックを初期化する必要があります"。
- ディスクを「root」、「data1」、および「data2」としてパーティション分割している場合は、スペアディスクが使用可能であることを確認する必要があります。

アップグレード時の考慮事項

ONTAP 9.10.1にアップグレードすると、既存のSnapLockおよび非SnapLockアグリゲートがSnapLockボリュームと非SnapLockボリュームの両方をサポートするようにアップグレードされますが、既存のSnapLockボリュームの属性は自動的には更新されません。たとえば、data-compaction、cross-volume-dedupe、cross-volume-background-dedupeの各フィールドは変更されません。既存のアグリゲートに作成された新しいSnapLockボリュームには非SnapLockボリュームと同じデフォルト値が使用され、新しいボリュームとアグリゲートにはプラットフォームに応じて異なるデフォルト値が適用されます。

リバートに関する考慮事項

ONTAP 9.10.1よりも前のバージョンにリバートする必要がある場合は、すべてのSnapLock Complianceボリューム、SnapLock Enterpriseボリューム、およびSnapLockボリュームをそれぞれのSnapLockアグリゲートに移動する必要があります。

タスク概要

- SyncMirrorオプションを指定してComplianceアグリゲートを作成することはできません。
- ミラーされたComplianceアグリゲートをMetroCluster構成に作成できるのは、アグリゲートをSnapLock 監査ログ ボリュームのホストとして使用する場合だけです。

MetroCluster構成では、SnapLock Enterpriseは、ミラーされたアグリゲートとミラーされていないアグリゲートでサポートされます。SnapLock Complianceは、ミラーされていないアグリゲートでのみサポートされます。

手順

1. SnapLockアグリゲートを作成します。

```
storage aggregate create -aggregate <aggregate_name> -node <node_name>
-diskcount <number_of_disks> -snaplock-type <compliance|enterprise>
```

次のコマンドは、 `node1`上の3つのディスクを使用して `aggr1`という名前のSnapLock `Compliance`アグリゲートを作成します：

```
cluster1::> storage aggregate create -aggregate aggr1 -node node1
-diskcount 3 -snaplock-type compliance
```

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

ONTAP SnapLockボリュームを作成してマウントする

ファイルやスナップショットをWORM状態にコミットするには、SnapLockボリュームを作成する必要があります。ONTAP 9.10.1以降では、アグリゲートの種類に関係なく、作成されるすべてのボリュームはデフォルトで非SnapLockボリュームとして作成されます。明示的にSnapLockボリュームを作成するには、 `-snaplock-type`オプションを使用し、SnapLockタイプとしてComplianceまたはEnterpriseのいずれかを指定する必要があります。デフォルトでは、SnapLockタイプは `non-snaplock`に設定されています。

開始する前に

- SnapLockアグリゲートがオンラインになっている必要があります。
- "SnapLockライセンスがインストールされていることを確認する"する必要があります。SnapLockライセンスがノードにインストールされていない場合は、"インストール"する必要があります。このライセンスは"ONTAP One"に含まれています。ONTAP Oneより前のバージョンでは、SnapLockライセンスはSecurity and Complianceバンドルに含まれていました。Security and Complianceバンドルは現在提供されていませんが、引き続き有効です。現在必須ではありませんが、既存のお客様は"ONTAP Oneにアップグレード"を選択できます。
- "ノード上のコンプライアンスクロックを初期化する必要があります"。

タスク概要

SnapLockの適切な権限があれば、Enterpriseボリュームはいつでも破棄または名前変更できます。Complianceボリュームの削除は保持期間が終了するまでは実行できません。Complianceボリュームの名前は一切変更できません。

SnapLockボリュームはクローニングできますが、SnapLockボリュームのファイルはクローニングできません。クローン ボリュームのSnapLockタイプは親ボリュームと同じになります。

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。

このタスクは、ONTAP System ManagerまたはONTAP CLIを使用して実行します。

System Manager

ONTAP 9.12.1以降では、System Managerを使用してSnapLockボリュームを作成できます。

手順

1. ストレージ > ボリューム に移動し、追加 をクリックします。
2. *ボリュームの追加*ウィンドウで、*その他のオプション*をクリックします。
3. 新しいボリュームの情報（ボリュームの名前とサイズなど）を入力します。
4. *SnapLockを有効にする*を選択し、SnapLockタイプ（ComplianceまたはEnterprise）を選択します。
5. *ファイルの自動コミット*セクションで*変更済み*を選択し、ファイルが変更されずに保持される期間を入力すると、その期間経過後に自動的にコミットされます。最小値は5分、最大値は10年です。
6. *Data Retention*セクションで、最小および最大保持期間を選択します。
7. デフォルトの保持期間を選択します。
8. *保存*をクリックします。
9. ボリューム ページで新しいボリュームを選択し、SnapLock 設定を確認します。

CLI

1. SnapLockボリュームを作成します。

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

`volume create`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/volume-create.html["ONTAPコマンド リファレンス"^]を参照してください。次のオプションはSnapLockボリュームでは使用できません：`-nvfail`、 `-atime-update`、 `-is-autobalance-eligible`、 `-space-mgmt-try-first`、および `vmalign`。

次のコマンドは、 `vs1`上の `aggr1`に `vol1`という名前のSnapLock `Compliance`ボリュームを作成します：

```
cluster1::> volume create -vserver vs1 -volume vol1 -aggregate aggr1
-snaplock-type compliance
```

SnapLockボリュームのマウント

NASクライアントからアクセスできるように、SnapLockボリュームをSVMネームスペースのジャンクションパスにマウントすることができます。

開始する前に

SnapLockがオンラインである必要があります。

タスク概要

- SnapLockボリュームはSVMのルートにしかマウントできません。
- 通常のボリュームをSnapLockボリュームにマウントすることはできません。

手順

1. SnapLockボリュームをマウントします。

   volume mount -vserver *SVM_name* -volume *volume_name* -junction-path *path*

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

   次のコマンドは、SnapLockボリューム `vol1`を `vs1`名前空間内のジャンクションパス `/sales`にマウントします：

   ```
   cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path /sales
   ```

ONTAP SnapLock保持期間を設定する

保持期限の設定については、ファイルに対して明示的に設定する方法と、ボリュームのデフォルトの保持期間から自動的に設定する方法があります。保持期限を明示的に設定しない場合は、デフォルトの保持期間に基づいて保持期限が計算されます。イベント後にファイルの保持期限を設定することもできます。

保持期間と保持期限について

WORMファイルの_保持期間_は、ファイルがWORM状態にコミットされた後、保持する必要がある期間を指定します。WORMファイルの_保持時間_は、そのファイルを保持する必要がなくなるまでの時間です。例えば、2020年11月10日午前6：00にWORM状態にコミットされたファイルの保持期間が20年の場合、保持時間は2040年11月10日午前6：00になります。

ONTAP 9.10.1以降では、最長で保持期限を3058年10月26日、保持期間を100年に設定できます。保持期限を延長すると、古いポリシーは自動的に変換されます。ONTAP 9.9.1以前のリリースでは、デフォルトの保持期間を無期限に設定した場合を除き、サポートされる最も遅い保持期限は2071年1月19日（GMT）です。

レプリケーションに関する重要な考慮事項

保持期限を2071年1月19日（GMT）よりもあとに設定してSnapLockソース ボリュームとのSnapMirror関係を確立する場合は、デスティネーション クラスタでONTAP 9.10.1以降が実行されている必要があります。そうでない場合、SnapMirror転送が失敗します。

リバートに関する重要な考慮事項

ONTAPでは、保持期間が「2071年1月19日午前8時44分7秒」以降のファイルがある場合、クラスタをONTAP 9.10.1から以前のONTAPバージョンにリバートすることはできません。

保持期間について

SnapLock ComplianceまたはSnapLock Enterpriseボリュームには、次の4種類の保持期間があります。

- 最小保存期間(`min`）、デフォルトは0
- 最大保存期間(`max`）、デフォルトは30年
- デフォルトの保持期間。ONTAP 9.10.1以降では、コンプライアンスモードとエンタープライズモードの両方でデフォルトが `min`になります。ONTAP 9.10.1より前のONTAPリリースでは、デフォルトの保持期間はモードによって異なります：
  - コンプライアンス モードの場合、デフォルトは `max`になります。
  - エンタープライズ モードの場合、デフォルトは `min`になります。
- 未指定の保持期間。

> ONTAP 9.10.1より前のリリースでは、コンプライアンスモードのファイルをWORM状態にコミットする前に明示的に保持期間を設定せず、デフォルトも変更していない場合、ファイルは30年間保持されます。この変更は元に戻すことが_できません_。同様に、ONTAP 9.10.1以降では、エンタープライズモードのファイルをWORM状態にコミットする前に明示的に保持期間を設定せず、デフォルトも変更していない場合、ファイルは0年間保持され、実質的に全く保持されないことになります。

ONTAP 9.8以降では、ボリューム内のファイルの保持期間を `unspecified`に設定することで、絶対保持期間を設定するまでファイルを保持できるようになりました。絶対保持期間が設定されているファイルを、無指定の保持期間に設定し、新しい絶対保持期間が以前に設定した絶対保持期間よりも後であれば、絶対保持期間に戻すことができます。

ONTAP 9.12.1以降、保持期間が `unspecified`に設定されているWORMファイルは、SnapLockボリュームに設定されている最小保持期間に設定されることが保証されます。ファイルの保持期間を `unspecified`から絶対保持時間に変更する場合、指定する新しい保持時間は、ファイルに既に設定されている最小保持時間よりも長くする必要があります。

デフォルトの保持期間の設定

`volume snaplock modify`コマンドを使用して、SnapLockボリューム上のファイルのデフォルトの保持期間を設定できます。

開始する前に

SnapLockがオンラインである必要があります。

タスク概要

次の表に、デフォルトの保持期間に指定できる値を示します。

デフォルトの保持期間は、最小保持期間以上、最大保持期間以下にする必要があります。

Value	単位	注記
0 - 65535	seconds	
0 - 24	hours	
0 - 365	days	
0 - 12	months	
0 - 100	years	ONTAP 9.10.1以降。以前のリリースのONTAPの場合、値は0 - 70です。
max	-	最大保持期間を使用します。
min	-	最小保持期間を使用します。
infinite	-	ファイルを無期限に保持します。
unspecified	-	明確な保持期間が設定されるまでファイルを保持します。

最大保存期間と最小保存期間の値と範囲は、 `max`と `min`を除き同一です。ただし、これらは適用されません。このタスクの詳細については、"保持期限の設定 - 概要"を参照してください。

`volume snaplock show`
コマンドを使用して、ボリュームの保持期間設定を表示できます。link:https://docs.netapp.com/us-en/ontap-cli/volume-snaplock-show.html["ONTAPコマンド リファレンス"^]の `volume snaplock show`の詳細をご覧ください。

ファイルがWORM状態にコミットされたあとは、保持期間を延長することはできますが短縮することはできません。

手順

1. SnapLockボリューム上のファイルにデフォルトの保持期間を設定します。

```
volume snaplock modify -vserver SVM_name -volume volume_name -default
-retention-period default_retention_period -minimum-retention-period
min_retention_period -maximum-retention-period max_retention_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。

以下の例は、最大保持期間と最小保持期間が過去に変更されていないことを想定しています。

次のコマンドは、ComplianceボリュームまたはEnterpriseボリュームのデフォルトの保持期間を20日に設定します。

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period 20days
```

次のコマンドは、Complianceボリュームのデフォルトの保持期間を70年に設定します。

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -maximum
-retention-period 70years
```

次のコマンドは、Enterpriseボリュームのデフォルトの保持期間を10年に設定します。

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period max -maximum-retention-period 10years
```

次のコマンドは、Enterpriseボリュームのデフォルトの保持期間を10日に設定します。

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -minimum
-retention-period 10days
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period min
```

次のコマンドは、Complianceボリュームのデフォルトの保持期間を無期限に設定します。

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period infinite -maximum-retention-period infinite
```

ファイルに対する保持期限の明示的な設定

ファイルに対して保持期限を明示的に設定するには、最終アクセス時刻を変更します。最終アクセス時刻は、NFSまたはCIFSで適切なコマンドやプログラムを使用して変更できます。

タスク概要

ファイルがWORMモードにコミットされた後、保持期間を延長することはできますが、短縮することはできません。保持期間はファイルの `atime`フィールドに保存されます。

ファイルの保持期間を明示的に `infinite`に設定することはできません。この値は、デフォルトの保持期間を使用して保持期間を計算する場合にのみ使用できます。

手順

1. 適切なコマンドまたはプログラムを使用して、保持期限を設定するファイルの最終アクセス時刻を変更します。

   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
   ```

   Windowsでは、任意の適切なコマンドまたはプログラムを使用して最終アクセス時刻を変更できます。

イベント発生後のファイル保持期間の設定

ONTAP 9.3 以降では、SnapLock _Event Based Retention（EBR）_機能を使用して、イベント発生後にファイルを保持する期間を定義できます。

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

_イベント保持ポリシー_は、イベント発生後のファイルの保持期間を定義します。このポリシーは、単一のファイルまたはディレクトリ内のすべてのファイルに適用できます。

- WORMファイル以外のファイルの場合、ポリシーで定義された保持期間にわたってWORM状態にコミットされます。
- WORMファイルまたは追記可能WORMファイルの場合、保持期間がポリシーで定義された保持期間まで延長されます。

ComplianceモードまたはEnterpriseモードのボリュームを使用できます。

EBRポリシーは、リーガル ホールド中のファイルには適用できません。

高度な使用方法については、"NetApp SnapLockを使用した準拠WORMストレージ"を参照してください。

EBRを使用して既存の***WORM***ファイルの保持期間を延長する

EBRは、既存のWORMファイルの保持期間を延長する場合に便利です。たとえば、会社の規定で、従業員が源泉徴収の選択を変更した場合に、変更後3年間は従業員のW-4レコードを変更不可能な状態で保管するように定められているとします。さらに、従業員の退職後はW-4レコードを5年間保管するように定めた規定もあります。

このような状況では、5年間の保持期間を設定したEBRポリシーを作成できます。従業員が退職した後（「event」）、EBRポリシーを従業員のW-4レコードに適用し、保持期間を延長します。これは通常、手動で保持期間を延長するよりも簡単で、特に大量のファイルが関係する場合は効果的です。

手順

1. EBRポリシーを作成します。

   `snaplock event-retention policy create -vserver` *`SVM_name`* `-name` *`policy_name`* `-retention-period` *`retention_period`*

   次のコマンドは、 `vs1`上に保持期間が10年のEBRポリシー `employee_exit`を作成します：

   ```
   cluster1::>snaplock event-retention policy create -vserver vs1 -name
   employee_exit -retention-period 10years
   ```

2. EBRポリシーを適用します。

   `snaplock event-retention apply -vserver` *`SVM_name`* `-name` *`policy_name`* `-volume` *`volume_name`* `-path` *`path_name`*

   次のコマンドは、 `vs1`上の `d1`ディレクトリ内のすべてのファイルにEBRポリシー `employee_exit`を適用します：

   ```
   cluster1::>snaplock event-retention apply -vserver vs1 -name
   employee_exit -volume vol1 -path /d1
   ```

関連情報

- "SnapLockイベント保持ポリシーの作成"
- "SnapLockイベント保持適用"

ONTAP SnapLockで保護された監査ログを作成する

ONTAP 9.9.1以前を使用している場合は、まずSnapLockアグリゲートを作成したうえで、privileged deleteまたはSnapLockボリュームの移動を実行する前に、SnapLockで保護された監査ログを作成しておく必要があります。この監査ログには、SnapLock管理者アカウントの作成と削除、ログ ボリュームに対する変更、privileged deleteが有効になっているかどうか、privileged delete処理、およびSnapLockボリューム移動処理に関する情報が記録されます。

ONTAP 9.10.1以降では、SnapLockアグリゲートを作成しなくなりました。-snaplock-typeオプションを使用して、SnapLockタイプとしてComplianceまたはEnterpriseを指定することで"明示的にSnapLockボリュームを作成する"する必要があります。

開始する前に

ONTAP 9.9.1以前を使用している場合、SnapLockアグリゲートを作成するにはクラスタ管理者になる必要があります。

タスク概要

監査ログは、ログ ファイルの保持期間が経過するまで削除できません。保持期間が経過したあとも、監査ログを変更することはできません。これは、SnapLockのComplianceモードとEnterpriseモードの両方に該当します。

ONTAP 9.4以前では、監査ログにSnapLock Enterpriseボリュームは使用できません。SnapLock Complianceボリュームを使用する必要があります。ONTAP 9.5以降では、監査ログにSnapLock EnterpriseボリュームまたはSnapLock Complianceボリュームのいずれかを使用できます。いずれの場合も、監査ログボリュームはジャンクションパス `/snaplock_audit_log`にマウントする必要があります。他のボリュームはこのジャンクションパスを使用できません。

SnapLock監査ログは、監査ログボリュームのルート下の `/snaplock_log`ディレクトリにあり、`privdel_log`（特権削除操作）および `system_log`（その他すべて）という名前のサブディレクトリに格納されています。監査ログファイル名には、最初に記録された操作のタイムスタンプが含まれるため、操作が実行されたおおよその時刻でレコードを簡単に検索できます。

- `snaplock log file show`コマンドを使用して、監査ログ ボリューム上のログ ファイルを表示できます。
- `snaplock log file archive`コマンドを使用すると、現在のログ ファイルをアーカイブし、新しいログ ファイルを作成できます。これは、監査ログ情報を別のファイルに記録する必要がある場合に便利です。

`snaplock log file show`および `snaplock log file archive`の詳細については、`link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=snaplock+log+file["ONTAP`コマンド リファレンス`"^]`を参照してください。

データ保護ボリュームは、SnapLock監査ログ ボリュームとしては使用できません。

手順

1. SnapLockアグリゲートを作成します。

   SnapLockアグリゲートの作成

2. 監査ログを設定するSVMにSnapLockボリュームを作成します。

   SnapLockボリュームの作成

3. SVMに監査ログを設定します。

   ```
   snaplock log create -vserver SVM_name -volume snaplock_volume_name -max-log
   ```

`-size size -retention-period default_retention_period`

> 監査ログファイルのデフォルトの最小保持期間は6か月です。影響を受けるファイルの保持期間が監査ログの保持期間よりも長い場合、監査ログの保持期間はファイルの保持期間を継承します。したがって、特権削除を使用して削除されたファイルの保持期間が10か月で、監査ログの保持期間が8か月の場合、監査ログの保持期間は10か月に延長されます。保持期間とデフォルトの保持期間の詳細については、"保持期限の設定"を参照してください。

次のコマンドは、SnapLockボリューム `logVol`を使用して `SVM1`の監査ログを設定します。監査ログの最大サイズは20 GBで、8か月間保持されます。

```
SVM1::> snaplock log create -vserver SVM1 -volume logVol -max-log-size
20GB -retention-period 8months
```

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

4. 監査ログ用に設定したSVMで、SnapLockボリュームをジャンクション パスにマウントします `/snaplock_audit_log`。

   SnapLockボリュームのマウント

ONTAP SnapLock設定を確認する

`volume file fingerprint start`コマンドと `volume file fingerprint dump`コマンドを使用すると、ファイルの種類（通常、WORM、またはWORM追加可能）、ボリュームの有効期限など、ファイルとボリュームに関する重要な情報を表示できます。

手順

1. ファイル フィンガープリントを生成します。

   `volume file fingerprint start -vserver <SVM_name> -file <file_path>`

```
svm1::> volume file fingerprint start -vserver svm1 -file
/vol/sle/vol/f1
File fingerprint operation is queued. Run "volume file fingerprint show
-session-id 16842791" to view the fingerprint session status.
```

このコマンドは、 `volume file fingerprint dump`コマンドへの入力として使用できるセッション ID を生成します。

`volume file fingerprint show`コマンドをセッションIDとともに使用して、フィンガープリント操作の進行状況を監視できます。フィンガープリントを表示する前に、操作が完了していることを確認してください。

2. ファイルのフィンガープリントを表示します。

`volume file fingerprint dump -session-id <session_ID>`

```
svm1::> volume file fingerprint dump -session-id 33619976
        Vserver:svm1
        Session-ID:33619976
        Volume:slc_vol
        Path:/vol/slc_vol/f1
        Data
Fingerprint:MOFJVevxNSJm3C/4Bn5oEEYH51CrudOzZYK4r5Cfy1g=Metadata

Fingerprint:8iMjqJXiNcqgXT5XuRhLiEwIrJEihDmwS0hrexnjgmc=Fingerprint
Algorithm:SHA256
        Fingerprint Scope:data-and-metadata
        Fingerprint Start Time:1460612586
        Formatted Fingerprint Start Time:Thu Apr 14 05:43:06 GMT 2016
        Fingerprint Version:3
        **SnapLock License:available**
        Vserver UUID:acf7ae64-00d6-11e6-a027-0050569c55ae
        Volume MSID:2152884007
        Volume DSID:1028
        Hostname:my_host
        Filer ID:5f18eda2-00b0-11e6-914e-6fb45e537b8d
        Volume Containing Aggregate:slc_aggr1
        Aggregate ID:c84634aa-c757-4b98-8f07-eefe32565f67
        **SnapLock System ComplianceClock:1460610635
        Formatted SnapLock System ComplianceClock:Thu Apr 14 05:10:35
GMT 2016
        Volume SnapLock Type:compliance
        Volume ComplianceClock:1460610635
        Formatted Volume ComplianceClock:Thu Apr 14 05:10:35 GMT 2016
        Volume Expiry Date:1465880998**
         Is Volume Expiry Date Wraparound:false
        Formatted Volume Expiry Date:Tue Jun 14 05:09:58 GMT 2016
        Filesystem ID:1028
        File ID:96
        File Type:worm
        File Size:1048576
        Creation Time:1460612515
```

```
        Formatted Creation Time:Thu Apr 14 05:41:55 GMT 2016
        Modification Time:1460612515
        Formatted Modification Time:Thu Apr 14 05:41:55 GMT 2016
        Changed Time:1460610598
        Is Changed Time Wraparound:false
        Formatted Changed Time:Thu Apr 14 05:09:58 GMT 2016
        Retention Time:1465880998
        Is Retention Time Wraparound:false
        Formatted Retention Time:Tue Jun 14 05:09:58 GMT 2016
        Access Time:-
        Formatted Access Time:-
        Owner ID:0
        Group ID:0
        Owner SID:-
        Fingerprint End Time:1460612586
        Formatted Fingerprint End Time:Thu Apr 14 05:43:06 GMT 2016
```

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。

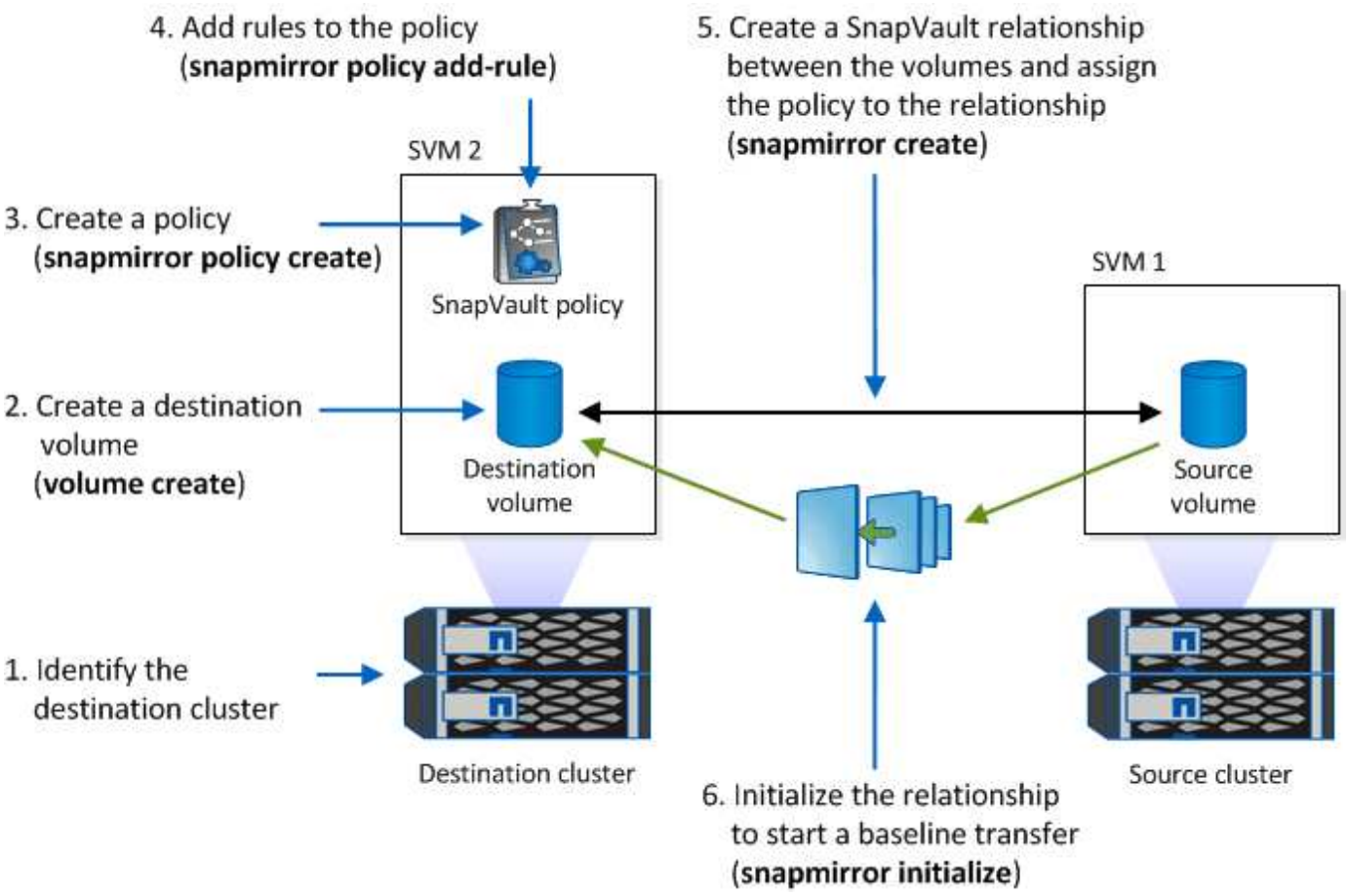
ONTAP 9.14.1以降では、SnapMirror関係のSnapMirrorポリシーで特定のSnapMirrorラベルの保持期間を指定できるようになりました。これにより、ソースボリュームからデスティネーションボリュームにレプリケートされたスナップショットは、ルールで指定された保持期間の間保持されます。保持期間が指定されていない場合は、デスティネーションボリュームのデフォルトの保持期間が使用されます。

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。

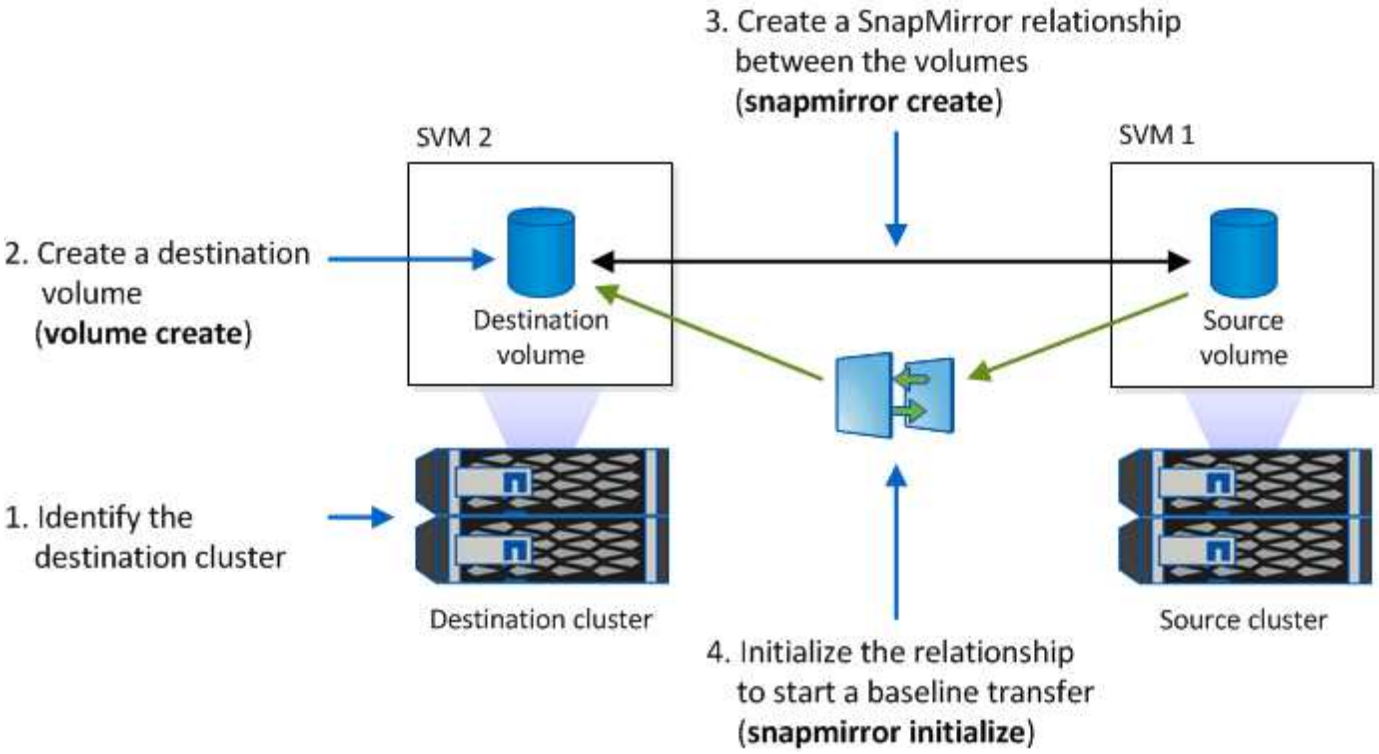
デスティネーション ボリュームの有効期限がソースよりもあとの場合、デスティネーションの有効期限が維持され、再同期後にソース ボリュームの有効期限で上書きされることはありません。

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
   ```

ONTAP SnapLockボリュームを移動する

ONTAP 9.8以降では、SnapLockボリュームを同じタイプのデスティネーション アグリゲートに移動できます（EnterpriseからEnterpriseへの移動またはComplianceからComplianceへの移動）。SnapLockボリュームを移動するには、SnapLockのセキュリティ ロールが割り当てられている必要があります。

SnapLockセキュリティ管理者アカウントの作成

SnapLockボリュームの移動を実行するには、SnapLockセキュリティ管理者権限が必要です。この権限は、ONTAP 9.8で導入された_snaplock_ロールによって付与されます。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、このSnapLockセキュリティロールを持つSnapLockセキュリティユーザ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。

タスク概要

snaplockロールは、vsadmin-snaplockロールと違って、データSVMではなく管理SVMに関連付けられます。

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*

   次のコマンドを実行すると、事前定義された `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管理 SVM `cluster1`にアクセスできるようになります：

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

SnapLockボリュームの移動

`volume move`コマンドを使用して、SnapLockボリュームをデスティネーション アグリゲートに移動できます。

開始する前に

- SnapLockボリュームの移動を実行する前に、SnapLockで保護された監査ログを作成しておく必要があります。

  "監査ログの作成"。

- 9.10.1より前のバージョンのONTAPを使用している場合は、デスティネーション アグリゲートのSnapLockタイプが、移動するSnapLockボリュームと同じであることが必要です（ComplianceからComplianceへの移動またはEnterpriseからEnterpriseへの移動）。ONTAP 9.10.1以降ではこの制限がなくなり、SnapLock ComplianceボリュームとSnapLock Enterpriseボリュームの両方、および非SnapLockボリュームをアグリゲートに含めることができます。
- SnapLockのセキュリティ ロールが割り当てられている必要があります。

手順

1. セキュアな接続を使用して、ONTAPクラスタ管理LIFにログインします。

   ```
   ssh snaplock_user@cluster_mgmt_ip
   ```

2. SnapLockボリュームを移動します。

   ```
   volume move start -vserver SVM_name -volume SnapLock_volume_name -destination -aggregate destination_aggregate_name
   ```

3. ボリューム移動処理の現在のステータスを確認します。

   ```
   volume move show -volume SnapLock_volume_name -vserver SVM_name -fields volume,phase,vserver
   ```

ランサムウェア攻撃から保護するために ONTAP スナップショットをロックする

ONTAP 9.12.1以降では、SnapLock以外のボリュームでスナップショットをロックして、ランサムウェア攻撃からの保護を提供できます。スナップショットをロックすることで、誤ってまたは悪意を持って削除されることを防止できます。

SnapLockコンプライアンスクロック機能を使用すると、スナップショットを指定した期間ロックし、有効期

限に達するまで削除できないようにすることができます。スナップショットをロックすることで改ざん防止機能が強化され、ランサムウェアの脅威から保護されます。ランサムウェア攻撃によってボリュームが侵害された場合、ロックされたスナップショットを使用してデータをリカバリできます。

ONTAP 9.14.1以降、スナップショットロックはSnapLockヴォールトデスティネーションおよび非SnapLock SnapMirrorデスティネーションボリューム上の長期保存スナップショットをサポートします。スナップショットロックは、既存のポリシー ラベルに関連付けられたSnapMirrorポリシールールを使用して保存期間を設定することで有効になります。このルールは、ボリュームに設定されているデフォルトの保存期間をオーバーライドします。SnapMirrorラベルに保存期間が関連付けられていない場合は、ボリュームのデフォルトの保存期間が使用されます。

改ざん防止**Snapshot**の要件と考慮事項

- ONTAP CLIを使用する場合は、クラスタ内のすべてのノードでONTAP 9.12.1以降が実行されている必要があります。System Managerを使用する場合は、すべてのノードでONTAP 9.13.1以降が実行されている必要があります。
- "SnapLockライセンスはクラスタにインストールする必要があります"。このライセンスは"ONTAP One"に含まれています。
- "クラスタのコンプライアンスクロックを初期化する必要がある"。
- ボリューム上でスナップショット ロックが有効になっている場合、クラスタをONTAP 9.12.1より新しいバージョンのONTAPにアップグレードできます。ただし、ロックされているすべてのスナップショットが有効期限に達して削除され、スナップショット ロックが無効になるまで、以前のバージョンのONTAPに戻すことはできません。
- スナップショットがロックされている場合、ボリュームの有効期限はスナップショットの有効期限に設定されます。複数のスナップショットがロックされている場合、ボリュームの有効期限はすべてのスナップショットの中で最も長い有効期限に設定されます。
- ロックされたスナップショットの保持期間はスナップショット保持数よりも優先されます。つまり、ロックされたスナップショットのスナップショット保持期間が経過していない場合は、保持数の制限は適用されません。
- SnapMirror関係では、ミラー・ヴォールト・ポリシールールに保持期間を設定でき、デスティネーションボリュームでSnapshotロックが有効になっている場合、デスティネーションにレプリケートされたSnapshotに保持期間が適用されます。保持期間は保持数よりも優先されます。たとえば、有効期限が切れていないSnapshotは、保持数を超えても保持されます。
- SnapLock以外のボリュームでスナップショットの名前を変更できます。SnapMirror関係のプライマリボリュームでのスナップショットの名前変更操作は、ポリシーがMirrorAllSnapshotsの場合のみセカンダリボリュームに反映されます。その他のポリシータイプでは、名前が変更されたスナップショットは更新時に伝播されません。
- ONTAP CLIを使用している場合、ロックされたスナップショットが最新のものである場合にのみ、`volume snapshot restore`コマンドを使用してロックされたスナップショットを復元できます。復元対象のスナップショットよりも後の、有効期限が切れていないスナップショットが存在する場合、スナップショットの復元操作は失敗します。

改ざん防止**Snapshot**でサポートされる機能

- "Cloud Volumes ONTAP"
- FlexGroupボリューム

  スナップショットロックはFlexGroupボリュームでサポートされています。スナップショットロックはルート構成要素のスナップショットでのみ発生します。ルート構成要素の有効期限が過ぎている場合のみ、FlexGroupボリュームの削除が許可されます。

- FlexVolからFlexGroupへの変換

  ロックされたSnapshotを含むFlexVol volumeをFlexGroup volumeに変換できます。変換後もSnapshotはロックされたままです。

- SnapMirror非同期

  コンプライアンス クロックは、ソースとデスティネーションの両方で初期化する必要があります。

- SVMデータの移動（ソース クラスタからデスティネーション クラスタにSVMを移行または再配置する場合に使用）

  ONTAP 9.14.1以降でサポート。

- `-schedule`パラメータを使用したSnapMirrorポリシールール
- SVM DR

  コンプライアンス クロックは、ソースとデスティネーションの両方で初期化する必要があります。

- ボリューム クローンとファイル クローン

  ロックされたスナップショットからボリューム クローンとファイル クローンを作成できます。

- FlexCacheボリューム

  ONTAP 9.16.1以降でサポート。

サポートされない機能

現時点では、改ざん防止Snapshotで次の機能はサポートされていません：

- 整合性グループ
- "FabricPool"

  改ざん防止スナップショットは、削除できない不変の保護を提供します。FabricPool ではデータを削除する機能が必要なため、FabricPool とスナップショットロックを同じボリュームで有効にすることはできません。

- SMTape
- SnapMirrorアクティブ同期
- SnapMirror Synchronous

ボリューム作成時に**Snapshot**のロックを有効にする

ONTAP 9.12.1以降では、CLIで `volume create`コマンドおよび `volume modify`コマンドの `-snapshot-locking-enabled`オプションを使用することで、新しいボリュームを作成するとき、または既存のボリュームを変更するときに、Snapshotロックを有効にできます。ONTAP 9.13.1以降では、System Managerを使用してSnapshotロックを有効にできます。

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. *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. *Enable Snapshot locking*を選択します。SnapLockライセンスがインストールされていない場合、この選択は表示されません。
5. 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。
6. 変更を保存します。
7. ボリューム ウィンドウで、更新したボリュームを選択し、概要 を選択します。
8. *SnapLock Snapshot Locking*が*Enabled*として表示されていることを確認します。

CLI

1. 新しいボリュームを作成し、スナップショットのロックを有効にするには、次のコマンドを入力します：

   ```
   volume create -vserver <vserver_name> -volume <volume_name> -snapshot
   -locking-enabled true
   ```

   次のコマンドは、vol1という名前の新しいボリュームでスナップショット ロックを有効にします：

   ```
   > volume create -volume vol1 -aggregate aggr1 -size 100m -snapshot
   -locking-enabled true
   Warning: snapshot locking is being enabled on volume "vol1" in
   Vserver "vs1". It cannot be disabled until all locked snapshots are
   past their expiry time. A volume with unexpired locked snapshots
   cannot be deleted.
   Do you want to continue: {yes|no}: y
   [Job 32] Job succeeded: Successful
   ```

既存のボリュームで**Snapshot**ロックを有効にする

ONTAP 9.12.1以降では、ONTAP CLIを使用して既存のボリュームのSnapshotロックを有効にできます。ONTAP 9.13.1以降では、System Managerを使用して既存のボリュームのSnapshotロックを有効にできます。

System Manager

1. *Storage > Volumes*に移動します。
2. ⋮を選択し、*編集>ボリューム*を選択します。
3. *ボリュームの編集*ウィンドウで、スナップショット（ローカル）設定セクションを見つけて、*スナップショットのロックを有効にする*を選択します。

   SnapLockライセンスがインストールされていない場合、このオプションは表示されません。
4. 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。
5. 変更を保存します。
6. ボリューム ウィンドウで、更新したボリュームを選択し、概要 を選択します。
7. *SnapLock Snapshotロック*が*有効*として表示されていることを確認します。

CLI

1. 既存のボリュームを変更してスナップショット ロックを有効にするには、次のコマンドを入力します：

   ```
   volume modify -vserver <vserver_name> -volume <volume_name> -snapshot
   -locking-enabled true
   ```

ロックされた**Snapshot**ポリシーを作成し、保持を適用する

ONTAP 9.12.1以降では、スナップショットの保持期間を適用するスナップショット ポリシーを作成し、そのポリシーをボリュームに適用して、指定した期間スナップショットをロックできます。また、保持期間を手動で設定してスナップショットをロックすることもできます。ONTAP 9.13.1以降では、System Managerを使用してスナップショット ロック ポリシーを作成し、ボリュームに適用できます。

Snapshotロックポリシーを作成する

System Manager

1. ストレージ **> Storage VM** に移動し、Storage VM を選択します。
2. *設定*を選択します。
3. **Snapshot Policies** を見つけて → を選択します。
4. **Add Snapshot Policy** ウィンドウで、ポリシー名を入力します。
5. + Add を選択します。
6. スケジュール名、保持するスナップショットの最大数、SnapLock 保持期間などのスナップショットスケジュールの詳細を指定します。
7. *SnapLock保持期間*列に、スナップショットを保持する時間、日数、月数、または年数を入力します。たとえば、保持期間が5日のスナップショットポリシーでは、スナップショットが作成されてから5日間ロックされ、その間は削除できません。次の保持期間範囲がサポートされています：
   - 年数：0 - 100
   - 月：0 - 1200
   - 日数：0 - 36500
   - 時間：0 - 24
8. 変更を保存します。

CLI

1. スナップショット ポリシーを作成するには、次のコマンドを入力します：

   ```
   volume snapshot policy create -policy <policy_name> -enabled true
   -schedule1 <schedule1_name> -count1 <maximum snapshots> -retention-period1
   <retention_period>
   ```

   次のコマンドは、スナップショット ロック ポリシーを作成します：

   ```
   cluster1> volume snapshot policy create -policy lock_policy -enabled
   true -schedule1 hourly -count1 24 -retention-period1 "1 days"
   ```

   スナップショットは、アクティブな保持期間中は置き換えられません。つまり、まだ期限が切れていないロックされたスナップショットがある場合、保持カウントは考慮されません。

ボリュームへのロック ポリシーの適用

System Manager

1. *Storage > Volumes*に移動します。
2. ⋮を選択し、*編集>ボリューム*を選択します。
3. *ボリュームの編集*ウィンドウで、*スナップショットのスケジュール*を選択します。
4. リストからロック スナップショット ポリシーを選択します。
5. スナップショット ロックがまだ有効になっていない場合は、* Enable snapshot locking * を選択します。
6. 変更を保存します。

CLI

1. 既存のボリュームにスナップショット ロック ポリシーを適用するには、次のコマンドを入力します：

```
volume modify -volume <volume_name> -vserver <vserver_name> -snapshot
-policy <policy_name>
```

手動スナップショット作成時に保持期間を適用する

スナップショットを手動で作成する際に、スナップショットの保持期間を適用できます。ボリュームでスナップショットのロックが有効になっている必要があります。有効になっていない場合、保持期間の設定は無視されます。

System Manager

1. **Storage > Volumes** に移動し、ボリュームを選択します。
2. ボリュームの詳細ページで、**Snapshots** タブを選択します。
3. ＋ Add を選択します。
4. スナップショット名とSnapLock有効期限を入力します。カレンダーを選択して、保持期限の日時を選択できます。
5. 変更を保存します。
6. ボリューム **>** スナップショット ページで、表示/非表示 を選択し、**SnapLock** 有効期限 を選択して **SnapLock** 有効期限 列を表示し、保持時間が設定されていることを確認します。

CLI

1. スナップショットを手動で作成し、ロック保持期間を適用するには、次のコマンドを入力します：

   ```
   volume snapshot create -volume <volume_name> -snapshot <snapshot name>
   -snaplock-expiry-time <expiration_date_time>
   ```

   次のコマンドは、新しいスナップショットを作成し、保持期間を設定します：

   ```
   cluster1> volume snapshot create -vserver vs1 -volume vol1 -snapshot
   snap1 -snaplock-expiry-time "11/10/2022 09:00:00"
   ```

既存の**Snapshot**に保持期間を適用する

System Manager

1. **Storage > Volumes** に移動し、ボリュームを選択します。
2. ボリュームの詳細ページで、**Snapshots** タブを選択します。
3. スナップショットを選択し、⋮を選択し、*SnapLock有効期限の変更*を選択します。カレンダーを選択して、保持期限の日時を指定できます。
4. 変更を保存します。
5. ボリューム **>** スナップショット ページで、表示/非表示 を選択し、**SnapLock** 有効期限 を選択して **SnapLock** 有効期限 列を表示し、保持時間が設定されていることを確認します。

CLI

1. 既存のスナップショットに保持期間を手動で適用するには、次のコマンドを入力します：

   ```
   volume snapshot modify-snaplock-expiry-time -volume <volume_name> -snapshot
   <snapshot name> -snaplock-expiry-time <expiration_date_time>
   ```

   次の例では、既存のスナップショットに保持期間を適用します：

   ```
   cluster1> volume snapshot modify-snaplock-expiry-time -volume vol1
   -snapshot snap2 -snaplock-expiry-time "11/10/2022 09:00:00"
   ```

既存のポリシーの変更による長期保持の適用

SnapMirror関係では、ミラー・ヴォールト・ポリシールールに保持期間を設定でき、デスティネーションボリュームでSnapshotロックが有効になっている場合、デスティネーションにレプリケートされたSnapshotに保持期間が適用されます。保持期間は保持数よりも優先されます。たとえば、有効期限が切れていないSnapshotは、保持数を超えても保持されます。

ONTAP 9.14.1以降では、スナップショットの長期保持を設定するルールを追加することで、既存のSnapMirrorポリシーを変更できます。このルールは、SnapLockヴォールト デスティネーションおよび非SnapLock SnapMirrorデスティネーション ボリュームにおけるデフォルトのボリューム保持期間をオーバーライドするために使用されます。

1. 既存のSnapMirrorポリシーにルールを追加します。

   ```
   snapmirror policy add-rule -vserver <SVM name> -policy <policy name>
   -snapmirror-label <label name> -keep <number of snapshots> -retention-period
   [<integer> days|months|years]
   ```

   次の例では、「lockvault」という既存のポリシーに6カ月の保持期間を適用するルールを作成します。

   ```
   snapmirror policy add-rule -vserver vs1 -policy lockvault -snapmirror
   -label test1 -keep 10 -retention-period "6 months"
   ```

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

著作権に関する情報

商標に関する情報