テクニカル レポート

NetApp SnapLockを使用した コンプライアンス準拠のWORMストレージ

ONTAP 9

NetApp
Jeannine Walter / Dan Tulledge
2023年7月| TR-4526

概要

多くの企業では、コンプライアンス要件を満たすため、または単にデータ保護ロードマップにレイヤを追加するために、Write Once、Read Many（WORM）データストレージをある程度利用しています。本ドキュメントでは、WORMデータストレージが必要な環境にNetApp® NetApp ONTAP®ソフトウェア（NetApp WORM解決策in SnapLock® 9）を統合する方法について説明します。

目次

表一覧

図一覧

はじめに

多くの企業では、コンプライアンスを満たすため、または重要なファイル（またはデータ）にデータ保護レイヤを追加するために、Write Once、Read Many（WORM）データストレージをある程度使用しています。多種多様なデータストレージオプションが用意されている中で、なぜ多くの企業がWORMデータストレージを導入したのでしょうか。主に2つの理由があります。

- 規制当局は、WORMデータストレージがアーカイブデータの永続性を保護する機能を認識しているため、多くの場合、規制を満たすために消去や書き換えが不可能なWORMストレージのみを使用するよう規定しています。
- 企業は、特定のビジネスレコードや重要なデータファイルを偶発的または意図的な変更や削除から保護することを重視しています。消去や書き換えが不可能なデータストレージなどのWORM機能は、データの長期的な永続性を提供します。

WORMデータストレージに関するビジネス要件の増大に伴う問題に対処し、従来のWORMストレージソリューションに固有の問題を軽減するために、NetAppはSnapLockソフトウェアを導入しました。

SnapLockを使用すると、管理しやすい既存のNetAppディスクストレージテクノロジを使用して、従来のWORMストレージのデータ永続性機能を活用できます。NetAppシステムをSnapLock ComplianceおよびSnapLock Enterpriseソフトウェアで構成できるようになり、高いレベルのデータ整合性、パフォーマンス、保持性を実現し、TCOを削減できます。

SnapLockを使用すると、規制対象の参照データの保持、保護、アクセスに関する社内外の要件に対応できます。SnapLockでは、ファイルをWORM状態にコミットできるボリュームを作成して、指定した保持期限までファイルの書き換えや削除を防止できます。このWORMデータをディスクまたはテープにバックアップして、データ保護を強化できます。NetAppの完全統合データプロテクションポートフォリオにより、ディスクツーディスクバックアップとクロスプラットフォームレプリケーションを同時に実行して、最も貴重なリソースであるデータを保護できます。規制ルールが時間の経過とともに変化する中、SnapLockの柔軟性により、企業はこれらのポリシー変更を実装でき、ビジネスと業界の将来に合わせて拡張可能になります。SnapLockは業界標準のネットワークストレージプロトコルに依存しているため、シンプルさやパフォーマンスを犠牲にすることなく、データ永続性の目標を達成できます。

NetAppは、企業全体のアーカイブとコンプライアンスに関する取り組みを、単一の柔軟性に優れたプラットフォームに統合することで、個別のストレージサイロを排除します。データ量の増大が止まらず、コンプライアンス上の課題が増加している企業では、一部のデータは、データの書き換えや削除を必要としない純粋なコスト削減のためにアーカイブされます。それ以外のデータは、データの書き換えや削除を望まれるコンプライアンスや法的目的のために保持されます。SnapLockはボリュームベースの解決策であるため、WORMボリュームとWORM以外のボリュームを同じユニットに混在させて組み合わせることで、コストと複雑さを軽減できます。

SnapLockの基礎

SnapLockは、保持データのデータ保持とWORM保護の機能を提供する、NetAppの高性能コンプライアンス解決策です。SnapLockでは、変更や消去が不可能なボリュームを作成して、指定した保持期限までファイルの書き換えや削除を防止できます。

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。

SnapLockはONTAPのライセンスベースの機能で、アプリケーションソフトウェアと連携して書き換え不可能なデータストレージを管理します。SnapLockには、SnapLockコンプライアンスとSnapLockエンタープライズの2種類があります。ONTAPでは、1つのアドオンライセンスを使用して両方のタイプをアクティブ化できます。

NetAppの実績あるNetApp ONTAPストレージソフトウェアの一部であるNetApp SnapLockソフトウェアは、HDDとSSD環境にハイパフォーマンスでディスクベースのデータ永続性を提供します。

SnapLockを使用すると、データの整合性と保持が確保され、電子記録を改ざんできず、迅速にアクセスできるようになります。どちらのSnapLock保持機能も、厳しいレコード保持要件を満たすことが認定されているだけでなく、リーガルホールド、イベントベースの保持、ボリュームアペンドモードなど、幅広い保持要件に対応します。

SnapLockは、ハードディスクドライブまたはフラッシュメディアに書き換えや消去が不可能なデータを作成し、あらかじめ設定された保持期限またはデフォルトの保持期限までファイルの書き換えや削除を防止します。SnapLockでは、訴訟ホールドやイベントベースの保持、ロック状態を維持したままファイルを段階的に追加できます（音声監視やビデオ監視、ロギングなど）。

どちらのタイプも、低コストのSATAベースドライブ、高性能のSASまたはファイバ接続ディスクドライブ、SSD /フラッシュドライブを搭載したNetAppシステムで動作します。SnapLock WORMストレージに対するビジネス ニーズに応じて、ストレージの容量やタイプを柔軟に選択できます。

SnapLockコンプライアンスとSnapLockエンタープライズとは

どちらのSnapLockバージョンも、コスト効率と可用性に優れたRAID構成で、あらゆるタイプのディスクやフラッシュドライブを使用して、消去や書き換えが不可能なWORMデータの永続性を実現します。データ保護に関しては、どちらかのSnapLockタイプで書き換え不可のWORM状態にデータをコミットすれば、光学式ディスクにデータを保存した場合と同じように保護されると考えることができます。どちらのSnapLockタイプでも、WORM状態にコミットされたデータは、光学式ディスクに保存されたデータと同様に、保持期間が終了するまであらゆる書き換えや削除から保護されます。

SnapLock Complianceソフトウェア機能は、SEC Rule 17a-4、FINRA、HIPAA、CFTCなどの厳しい記録保持要件に加え、消去不可能なストレージの使用が求められるドイツ語圏（DACH）やGDPRの国内要件を満たすことが認定されています。SnapLock Complianceは、「信頼されていないストレージ管理者」の操作モデルを提供します。このモデルでは、SnapLock Complianceボリューム上のWORMストレージにコミットされたレコードとファイルは、変更または変更できず、保持期間が終了したあとにのみ削除できます。また、SnapLock Complianceボリュームについては、格納されたすべてのレコードとファイルの保持期間が終了するまで削除できません。SnapLock Complianceの場合、WORMデータを侵害する可能性のあるストレージ管理者による処理は許可されません。また、ファイルレベルだけでなく、ボリューム、アグリゲート、ディスクレベルでも保護が行われます。

対照的に、SnapLockエンタープライズは「信頼できるストレージ管理者」モデルの下で運用され、WORMデータストレージを使用してデジタル資産を保護するための自主規制のベストプラクティスガイドラインを組織が満たすように設計されています。SnapLock Enterpriseボリュームに格納されたデータも書き換えから保護される点は同じですが、SnapLockエンタープライズには、SnapLockコンプライアンスとの主な違いが1つあります。 格納されたデータは厳格な規制に準拠するためのものではないため、SnapLock Enterpriseボリュームを含むストレージシステムのroot権限を持つ管理者は、保持期間が終了する前に、SnapLock Enterpriseボリュームとそのボリュームに格納されたデータを削除できます。

注： ストレージシステムへの管理アクセス権を持つユーザでも、SnapLock EnterpriseボリュームのWORM保護の下で個 々 のファイルを変更することはできません。

Snapshotコピーロックとは何ですか。

ONTAP 9.12.1以降では、SnapLockの機能としてSnapshotコピーロックが採用されています。この機能では、ボリュームのSnapshotコピーポリシーの保持期間を使用して、手動または自動でSnapshotコピーを消去できなくなります。Snapshotコピーロックは、改ざん防止Snapshotコピーロックとも呼ばれます。Snapshotコピーのロックは、SnapLockライセンスとコンプライアンスクロックの初期化が必要ですが、SnapLock ComplianceやSnapLock Enterpriseとは関係ありません。SnapLock Enterpriseほど信頼できるストレージ管理者はおらず、SnapLockコンプライアンスのように基盤となる物理ストレージインフラを保護することもできません。Snapshotコピーロックの目的は、悪意のある管理者や信頼されていない管理者がプライマリおよびセカンダリONTAPシステム上のSnapshotコピーを削除しないようにすることです。この機能は、Snapshotコピーをセカンダリシステムに保管する場合に比べて強化されています。ランサムウェアによって破損したボリュームをリストアするために、プライマリシステム上のロックされたSnapshotコピーを迅速にリカバリできます。Snapshotコピーロックの詳細については、ONTAP 9.12.1のドキュメントを参照してください。

9.13.1以降では、System ManagerでSnapshotコピーロックを設定できます。これには、

- SnapLockライセンスをインストールしています。
- コンプライアンスクロックを設定します。
- ボリュームでSnapLock Snapshotコピーロックを有効にします。
- Snapshotコピーのロックポリシーを作成し、保持期間を設定します。
- ボリュームにロックポリシーを適用します。
- Snapshotコピーを手動で作成するときに保持期間を適用します。
- 既存のSnapshotコピーに保持期間を適用します。

詳細については、ONTAPのドキュメントを参照してください。

SnapLockの使用

ONTAP 9では、CLIとONTAP REST APIのサポートとは別に、ONTAPシステムマネージャとONTAPシステムマネージャもSnapLockでサポートされるようになりました。

ライセンス

ONTAP 9では、1つのノードでSnapLock Compliance機能とSnapLock Enterprise機能の両方を使用するために必要なSnapLockライセンスは1つだけです。SnapLockライセンスはノードロックライセンスです。ノードロックライセンスをインストールすると、ノードでライセンスされた機能を使用できるようになります。ライセンスされた機能をクラスタで使用して準拠させるには、すべてのノードでその機能のライセンスが有効になっている必要があります。

データがWORM状態にコミットされると、SnapLockはライセンスの状態に関係なく、データのWORMプロパティを引き続き適用します。さらに、SnapLockボリュームの作成後は、ライセンスがなくてもファイルをWORM状態にコミットできます。ただし、ライセンスの状態によって、SnapLockの設定変更が決まります。次の処理を実行するには、SnapLockライセンスを有効にする必要があります。

- ComplianceClockの初期化
- SnapLockアグリゲートの作成
- SnapLockボリュームの作成
- 自動コミットスキャナの電源投入
- vsadmin-snaplockロールを持つユーザの作成
- privileged-deleteの有効化
- SnapLock監査ログボリュームの設定

通常、既存の設定の変更は、SnapLockライセンスが有効になっていない場合でも可能です。次の処理では、SnapLockライセンスを有効にする必要はありません。

- SnapLockアグリゲートの削除
- SnapLockボリュームの削除
- 自動コミットスキャナの電源をオフにする
- vsadmin-snaplockロールを持つユーザの削除
- privileged-deleteの無効化または永続的な無効化
- SnapLock監査ログボリューム設定の削除

SnapLock ComplianceClockの初期化

データコンプライアンス環境では、システムクロックは管理者が任意に変更でき、WORMファイルおよびNetApp Snapshot™コピーの保持期間が損なわれる可能性があるため、システムクロックに依存することはできません。そのため、SnapLockは、改ざん防止機能を備えたソフトウェアベースのクロックであるONTAPのComplianceClockサービスに依存しています。ComplianceClockはすべてのノードで管理者が1回だけ初期化でき、初期化後はハードウェアティックに基づいて処理されます。ComplianceClockを初期化する前に、タイムゾーンを適切にメモし、ストレージシステムの時間ができるだけ正確であることを確認する必要があります。ComplianceClockの初期化後は、管理者はクロックを調整する操作を実行できません。この機能により、リファレンス・クロックを順方向に調整してもWORMファイルの保持期間が短縮されないようにします。

ComplianceClockには次の2つのタイプがあります。

- **ボリュームComplianceClock（VCC）：**ボリュームComplianceClockは、ボリュームごとの改ざん防止の参照時間です。VCCはSnapLockボリュームにのみ格納され、そのボリューム内のWORMファイルおよびWORM Snapshotコピーの有効期限を判断するために使用されます。VCCはボリューム単位であるため、ボリュームXのVCCスキューイングはボリュームYのVCCには影響しません。SnapLockボリュームのVCCは、クライアントの書き込みやその他のONTAP処理が原因で、整合ポイントにある場合にのみ遅延して更新されます。長時間（24時間）後にVCCが強制的に更新されます。
- **System ComplianceClock（SCC；システムComplianceClock）：**システムComplianceClockはノードごとに1つ保持されます。SCCは、VCC値を更新し、新しいボリュームのベースVCC値を提供するために使用されます。SCCはノードのルートボリュームに格納されます。ハードウェアティックに基づいて、メモリおよびノードのルートボリュームで15秒ごとに更新されます。

各SnapLockボリュームは、VCCの次のディスク上のメタデータを保持します。

- VCC時間：64ビットVCCタイムスタンプ
- SCC時間：64ビットSCCタイムスタンプ（最終更新時のSCC時間）
- Node ID：ノードの一意の識別子（SCC-VCCアソシエーションに使用）
- SCC ID：SCCの一意の識別子（SCC-VCCアソシエーションに使用）

VCCは（作成時またはアップグレード時に）1回だけ初期化され、それ以降は再初期化できません。VCCは、ボリュームの作成時にSCCから開始値を取得します。更新の参照時間ベースとしてSCCを使用します。VCCは次のように更新されます。

```
time elapsed since last update (delta) = current SCC time - SCC time at last VCC update new VCC
time = stored VCC time + delta
```

ボリュームがオンラインになると、最後の更新からの経過時間が計算されます。ノードIDとSCC IDが一致すると、ボリュームのオンディスクVCCが更新されます。したがって、同じシステムでボリュームがオンラインに戻っても、ボリュームがオフラインになっていた期間に関係なく、VCCスキューは発生しません。

ComplianceClockは、次のコマンドを実行してノードで1回だけ初期化できます。

```
snaplock compliance-clock initialize -node <nodename>
```

ComplianceClockを表示するには、次のコマンドを実行します。

```
snaplock compliance-clock show
```

SnapLockボリュームとアグリゲートの作成

SnapLockライセンスをインストールしてストレージシステムでComplianceClockを初期化したあとの手順では、作成と破棄の試行、WORMコミットなどの処理、削除または変更の試行、全体的な使いやすさなど、SnapLockボリュームのさまざまな側面が表示されます。信頼性とパフォーマンスを最適化するには、いくつかの検討と計画が必要です。この情報は、本ドキュメントで後述するベストプラクティスのガイドラインに記載されています。

volume `-snaplock-type` オプションを使用して、ComplianceまたはEnterprise SnapLockボリュームのタイプを指定します。ONTAP 9.10.1よりも前のリリースでは、SnapLockアグリゲートを別々に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。SnapLockボリュームの作成方法は、SnapLock以外のボリュームの作成方法と同じです。

注： 混在アグリゲートには、ホストされているすべてのボリュームのうち最も厳密なSnapLockタイプが反映されます。たとえば、1つのSnapLock Complianceボリューム、1つのSnapLock Enterpriseボリューム、および複数のSnapLock以外のボリュームを含むアグリゲートでは、アグリゲートに複数のタイプのボリュームがある場合でも、SnapLock Complianceアグリゲートとして表示されます。

ONTAP 9.11.1以降では、SnapLockでFlexGroupボリュームがサポートされます。FlexGroupボリュームは1つ以上のFlexVolで構成され、クラスタの複数のノードでホストされた複数のアグリゲートに分散され、単一の拡張性に優れたファイルシステムにまとめられます。FlexGroupボリュームにより、パフォーマンスとストレージをスケールアウトできます。FlexGroupボリュームの詳細については、『NetApp ONTAP FlexGroupVolumes Best Practices and Implementation Guide』を参照してください。

SnapLock向けのFlexGroupボリュームのサポートには、SnapLockのコア機能、ボリュームアペンドモード、未指定の保持期間、保持期間の延長（2、038を超える）、監査ログボリュームのサポート、自動コミットスキャナなどがあります。ONTAP 9.11.1では、リーガルホールド、イベントベースの保持、およびLockVaultはまだサポートされていませんFlexGroup SnapLock。ONTAP 9.12.1以降では、FlexGroupボリュームでLockVaultがサポートされます。

注： ONTAP 9.11.1より前のバージョンにリバートすると、クラスタにFlexGroup SnapLockボリュームがある場合はブロックされます。

SnapLock準拠の制限事項

SnapLock Complianceボリュームで通常の処理が実行されないようにするために、次のコマンドが変更されています。

- **ボリュームの削除。** SnapLock Complianceボリューム上のすべてのレコードとファイルの保持期間が満了する前に削除を許可すると、特に規制対象のデータのアーカイブスペースにおいて、WORMストレージの原則に違反します。SnapLock Complianceボリュームでdeleteコマンドを実行できるのは、指定した保持期間に一致するWORMレコードとファイルがすべて期限切れになっている場合だけです。

SnapLockボリュームの使用状況

SnapLockでは、個々のファイルレベルで保存期間をきめ細かく設定できます。SnapLockボリュームでファイルをWORM状態にコミットするには、いくつかの方法があります。以下に2つについて説明します。

注： Event Based Retention（EBR；イベントベースの保持）もファイルをWORM状態にコミットする方法の1つです。「イベントベースの保持」を参照してください。

手動コミット

1つ目は、SnapLockボリュームにファイルをコピーまたは作成してから、ファイル属性をNFSまたはCIFSオープンプロトコルを使用して読み取り専用に変更する方法です。読み取り専用に変更されると、ファイルはSnapLockボリューム上で変更不可の状態にコミットされます。SnapLockボリュームでファイルをWORM状態にコミットするには、次の2つの手順を実行します。

1. 最終アクセス日をファイルの保持期限に変更します。ボリュームにデフォルトの保持期間を使用する場合は、この手順を省略します。具体的な処理は、ファイルプロトコル（CIFS、NFSなど）とクライアントのオペレーティングシステムによって異なります。UNIXシェル環境での操作の例を次に示します。

```
touch -a -t [retention date] [file]
```

2. ファイルの属性を書き込み可能な状態から読み取り専用状態に移行します。具体的な処理はファイルプロトコル（CIFS、NFSなど）とクライアントオペレーティングシステムによって異なりますが、この処理は常に簡単です。この移行は、スクリプトを使用して手動で、またはプログラムによって簡単に実行できます。さまざまな環境の例を次に示します。

   UNIXシェル環境：

```
chmod -w [file]
```

   Windowsシェル環境：

```
attrib +r [file]
```

ファイルをWORM状態にコミットすると、ファイルのctimeフィールドにボリュームComplianceClock時間が書き込まれます。ボリュームComplianceClockは、ファイルの保持期間の計算に使用されます。

注： WORM状態へのコミットを実行するには、ファイルが書き込み可能な状態から読み取り専用状態に移行する必要があることに注意してください。読み取り専用で作成されたファイルではこの移行は行われないため、WORM状態にコミットされません。アプリケーションは、ファイルをWORM状態にコミットするために読み取り専用にする前に、必ずSnapLockボリューム上で最初に書き込み可能であることを確認する必要があります。

自動コミット

2つ目の方法は、SnapLockボリュームで変更不可の状態にファイルをコミットする方法です。autocommitオプションはSnapLockボリュームで設定できます。この場合、アプリケーションは読み取り専用ファイル属性を設定する必要はありません。自動コミット機能を使用すると、自動コミット期間中にファイルが変更されなかった場合に、SnapLockボリュームでファイルをWORM状態に自動コミットできます。ボリュームごとに自動コミット期間のボリュームオプションがあり、管理者はボリュームごとに異なるWORMポリシーを柔軟に設定できます。デフォルトでは、SnapLockボリュームの自動コミットは無効になっています。設定可能な最小値は5分、最大値は10年です。

注: アプリケーションがいつファイルへの書き込みを完了したかを知ることは非常に困難であるため、自動コミットはすべてのケースに適しているとは限りません。WORM状態へのコミットが途中で実行されると、変更不可のファイルが残され、アプリケーションが許可しない可能性があります。自動コミットスキャナは、ボリュームごとにスレッドを実行して、ボリューム内のすべてのファイルをスキャンします。ノードのボリューム数が多い場合や、WAFL® がクライアントI/Oでビジー状態の場合は、拡張の問題が発生する可能性があります。

WORM状態へのファイルのコミット

ファイルは、いくつかの方法でWORM状態にコミットできます。

- SnapLockボリュームにファイルを作成します。
  - アプリケーションによって読み取り/書き込み（rw）として作成される、自動コミット期間が指定されていないSnapLockボリューム内のファイル。準備が完了すると、最終的にファイルが読み取り専用に設定され、ファイルがWORM状態にコミットされます。
  - 自動コミット期間が指定されているSnapLock内にアプリケーションによってrwとして作成されるファイル。自動コミット期間が終了すると、自動コミットスキャナによってファイルが読み取り専用に自動的に設定されます。アプリケーションがファイルを明示的に読み取り専用にする必要はありません。
- RWファイルをSnapLockボリュームにコピーします。
  - どのコピーアプリケーションを使用してSnapLockボリュームにコピーする場合でも、最終的にはWORMにコミットされないRWファイルになります。ファイルを読み取り専用に変更して手動でWORM状態にコミットするか、自動コミット機能を使用してファイルを自動的にコミットする必要があります。
- 読み取り専用ファイルをSnapLockボリュームにコピーします。
  - NFSv3を使用する場合：

- NFS（UNIX形式）のcopyコマンドを実行すると、読み取り専用ファイルがSnapLockボリュームに作成され、そのボリュームへのデータのコピーが試行されます。これは失敗します。ファイルをコピーする前に、ファイルをrwに変更する必要があります。

- CIFS / SMBを使用：
  - copyコマンドでRWファイルが生成された場合の結果は、RWファイルをSnapLockボリュームにコピーした場合と同じです。ファイルをWORM状態に手動でコミットするか、自動コミットを有効にする必要があります。（`copy` コマンドラインからコマンドを実行すると、読み取り専用ファイルはRWファイルとして書き込まれます）。
  - copyコマンドで読み取り専用ファイルが作成されると、ファイルは自動的にWORM状態にコミットされます。たとえば、Windowsのドラッグアンドドロップまたはコピー/貼り付けを使用すると、最初にRWファイルが作成され、そのファイルにデータがコピーされ、ファイルが読み取り専用になります（WORM状態にコミットされます）。

疑問がある場合は、実装前にコピー方法をテストすることをお勧めします。

WORMファイルをコミットするための手順の詳細については、ONTAP 9ドキュメントセンターを参照してください。

SnapLockノホシキカン

SnapLockボリュームでファイルが変更不可の状態にコミットされる方法に関係なく、保持期間の設定を理解しておくことが重要です。SnapLockボリュームでWORM状態にコミットされたすべてのレコードには、個別の保持期間を関連付けることができます。ONTAPデータ管理ソフトウェアでは、保持期間が終了するまでこれらのレコードが保持されます。保持期間が終了したレコードは削除できますが、変更することはできません。

各SnapLockには、最小、最大、およびデフォルトの保持期間を制御するオプションがあります。指定できる値は、それぞれ最小保持期間、最大保持期間、およびデフォルト保持期間です。default-retention-periodは、最小保持期間と最大保持期間の間の任意の値に設定できます。ファイルのコミット時に保持期間が指定されていない場合は、default-retention-periodが使用されます。アプリケーションが最小保持期間よりも短い保持期間を設定しようとすると、代わりに最小保持期間が使用されます。アプリケーションが最大保持期間を超える保持期間を設定しようとすると、最大保持期間が使用されます。これらの設定は、新しいアプリケーションを評価する際に、ファイルを長期間コミットしたくない場合に便利です。ファイルの保持期間を延長しても、最大保持期間のチェックは実行されません。

SnapLockボリュームアペンドモード

ユーザがSnapLockボリューム内のファイルをWORM状態にコミットすると、ファイルの保持期限が切れるまでファイルを削除できません。有効期限の前後であっても、ファイルの内容を変更することはできません。ファイルの保存期間は延長のみ可能で、短縮はできません。ログを記録するために、このWORMファイルに追記することが必要になる場合があります。

ONTAP 9では、SnapLockで追記可能WORMファイルと呼ばれる別のタイプのファイルを作成できます。WORMアペンド機能を使用すると、WORMファイルを作成してデータを追加できます。ファイルに追加されたデータは、256K単位で自動的にWORM状態にコミットされます。ブロックは、特別に定義された追記可能WORMファイルに書き込まれるときにロックされます。ユーザはこのファイルにログを追加できますが、ファイルの既存の内容を変更したり、期限切れになるまでファイルを削除したりすることはできません。これは、ログファイルに追加できるが、変更や削除はできない場合に特に便利です。たとえば、このアプローチは、オーディオ、ビデオ、またはロギングアプリケーションが自動的に、またはNFS共有またはCIFS共有にファイルを作成する場合に使用します。

SnapLockボリュームに追記可能WORMファイルを作成する手順は次のとおりです。

1. 0バイトのファイルを作成します。
2. ファイルのatimeフィールドで必要な保持期限を設定します（オプション）。
3. ファイルに対する書き込み権限を削除してWORM状態にします。
4. 書き込み権限を追加して、ファイルを書き込み可能にします（この場合は追記可能のみ）。

5. ロギングが完了したら、ファイルの書き込み権限を削除することで、そのファイルをWORM読み取り専用ファイルにすることができます。

ONTAP 9.3では、SnapLockボリューム用の新しいボリュームオプションが導入され、SnapLockボリュームアペンドモード（VAM）を有効または無効にできます。vamオプションを有効にすると、書き込み権限を持つ新規作成されたすべてのファイルが、デフォルトで追記可能WORMファイルになります。このオプションは、空のボリューム（ユーザデータやSnapshotコピーがないボリューム）でのみ切り替えて、すでにボリュームを使用しているアプリケーションの停止を回避できます。

空のボリュームでVAMを有効にするコマンド：

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

VAMが有効なボリュームの自動コミットスキャナコードでは、通常のWORM以外のファイルに加え、前回の自動コミット期間に書き込みがない追記可能WORMファイルが検索されます。これらのファイルはWORMのみのステータスに変換されます（書き込みアクセスが削除されます）。

要約すると、ファイルがアペンドモードで書き込まれている場合、たとえば256KBのセグメントがいっぱいになるたびに、データはWORM状態にコミットされるなど、256KBのセグメントごとに上書きや削除から保護されます。不完全な（つまりコミットされていない）256KBセグメント内のデータは、a）セグメントがいっぱいになるか、b）ファイルが手動でWORM状態にコミットされるまで、書き込み可能または削除可能なままです。VAMボリュームに追加モードのファイルがある場合は、ボリュームのデフォルト値を使用してファイルをWORM状態に自動コミットすることもできます（5分~10年の間で1分刻み）。

アプリケーションの統合

SnapLockでは、標準のオープンプロトコル（NFSおよびCIFS）を使用してWORMデータを設定および管理できるため、他のアプリケーションとの統合が非常に簡単です。これは、atime（最終アクセスタイムスタンプ）ファイル属性を使用してファイルの保持期間を表します。また、ファイルに対する書き込みアクセスが解除されてWORM状態へのコミットがトリガーされます。アプリケーションは、次の2つの基本的な方法のいずれかを使用することで、SnapLock機能と統合できます。

- **NFSまたはCIFSによる統合**このアプローチにより、クライアントはファイルをWORM状態にコミットするために必要な次の処理を実行できます。
  a. 一定期間保持する必要があるファイルを選択します。
  b. 保持期間を選択します（通常は規制によって規定されています）。保持期間はファイル単位で設定できます（ファイル単位で設定可能）。またはボリュームレベルのデフォルトを使用して、保持期間を指定せずにボリューム上に存在するファイルに保持期間を設定できます。
  c. ファイルをWORM状態にコミットします。これは、個 々 のファイルレベルで（ファイルに対する書き込み権限を削除することで）実行することも、自動コミット機能を使用して、指定した期間変更されていないWORMファイルに自動的にコミットすることもできます。
  d. 保持期間が経過すると（ComplianceClockの値がatimeの値を超えた場合）、それらのファイルは削除できます。
- **ONTAP REST APIによる統合**ONTAP REST APIに機能を実装することで、このドキュメントで説明するSnapLock機能をアプリケーションで実行できるようになります。SnapLock APIの詳細なリストについては、ONTAP 9ドキュメントセンターを参照してください。

アプリケーションでは、SnapLockの自動コミット機能を利用して、SnapLockボリュームのファイルをWORM状態に自動的に移行できます。自動コミット機能は、アプリケーションがファイルをSnapLockボリュームにコピーするだけで、プログラムでWORM状態に移行できない場合に特に便利です。

SnapLockを使用したファイルの保持期限の設定

SnapLockオープンプロトコルの設計に合わせて、ファイル保持期間のサポートが実装され、独自のAPIやプロトコルを使用する必要はありませんでした。ファイル保持期限は、ほとんどのオペレーティングシステムで提供されている標準のシステムコールインターフェイスを使用してプログラムで設定および照会できます。また、標準

のコマンドラインツールを使用して対話的に照会することもできます。ONTAP REST APIを使用して設定することもできます。SnapLock処理と同様に、保持期限を設定する処理は、NFSやCIFSなどの標準的なネットワークファイルシステムインターフェイスで実行されます。この柔軟性により、アプリケーションはコンパイルされたコードやスクリプトからSnapLockを利用でき、クライアントシステムにライブラリやソフトウェアをインストールする必要はありません。

SnapLockボリューム上のWORMファイルの保持期限は、ファイルメタデータの最終アクセスタイムスタンプに保存されます。WORMファイルの保持期限を設定するには、ファイルを読み取り専用に設定してWORMコミット処理を実行する前に、アプリケーションでファイルの最終アクセス日時を目的の保持期限に明示的に設定する必要があります。WORM状態にコミットされると、ファイルのアクセス時間は変更できません。ただし、ファイルの保持期間の延長は例外です。

保持期間前のファイル削除

SnapLockのprivileged-delete機能を使用すると、vsadmin-snaplockロールの権限を持つユーザは、SnapLock Enterpriseボリューム上の期限切れ前のWORMファイルを削除できます。ただし、privileged-delete機能を使用して、期限切れのWORMファイルを削除することはできません。削除はSnapLock Compliance監査ログボリューム上の監査ファイルに記録されるため、ファイルが以前存在したか早期削除されたかを消去できないレコードが保持されます。SnapLock監査ログファイルでは、WORMファイルのprivileged deleteに関連する詳細（ファイルが削除されたかどうか、削除日時、ファイルを削除したユーザ、ファイルのフィンガープリント情報など）を確認できます。そのため、privileged-delete機能は監査可能な削除とも呼ばれます。

保持期間後のファイル削除

ONTAPでは、保持期限に達したファイルや保持期限を過ぎたファイルも含め、ファイルは自動的に削除されません。代わりに、このようなファイルのすべての削除は、アプリケーションまたはスクリプトやバッチジョブなどの他のプロセスで処理する必要があります。WORMファイルの保持期限に達すると、ONTAPはアプリケーションがファイル権限を読み取り専用から書き込み可能に戻し、ファイルを削除できるようにします。ONTAPでは、書き込み可能な状態に戻ったSnapLockファイルの変更や変更は許可されていません。この時点で実行できる操作は、ファイルを削除するか新しい保持期限を設定し、ファイルを読み取り専用に変更してSnapLock WORM保護を再度有効にすることだけです。

SnapLockのベストプラクティス

このセクションでは、SnapLockのベストプラクティスについて説明します。

ComplianceClockノヘストフラクテイス

ComplianceClockは、システムクロックから独立したソフトウェアベースのクロックであり、ハードウェアティックに基づいて更新されます。ComplianceClockが有効になっているNetAppシステムで、SnapLock以外のすべてのSnapLockボリュームとボリュームが短時間だけオフライン（または制限）になるようにします。初期化したComplianceClockは、どのような状況であっても変更できません。これは、保持期限の改ざんを防ぐためです。ComplianceClockはソフトウェアクロックであるため、システム停止中は実行されませんが、最後の状態はシャットダウン前に永続的に保存されます。システムが再起動されると、ComplianceClockはリアルタイムで実行されなくなります。その結果、期限切れのファイルを削除するために、システムの電源がオフになっていた時間によっては、数時間または数日待たなければならない場合があります。ただし、これはコンプライアンスの観点から安全な実装であり、SnapLockで保護されているファイルを早期に削除することはできません。

また、ボリュームComplianceClock（VCC）は、ボリュームのシステムComplianceClock（SCC）の関連付けがシステムと一致する場合にのみ更新されます。これは、SCC IDとノードIDを使用して決定されます。関連付けを確立するには、SnapLockボリュームのノードIDとSCC IDの両方が対応する値と一致している必要があります。VCCを更新する前に、VCCとSCCの間の関連付けを確立して、現在のSCCと最後に更新されたSCCが同じ時間ベースのものであることを確認する必要があります。

ノードIDは、ボリュームコピーやディスクの物理的な移動によるノードの変更を検出するために必要です。SCC IDは、SCCの再初期化によるSCCアソシエーションの変更を検出するために必要です。SCCの関連付けが変更された場合、ボリュームに保存されているSCC時間がシステムのSCC時間に対応していません。したがって、ボリュームのSCC時間は破棄され、VCCデルタはゼロと見なされます。

SCCの関連付けが変更されると、ボリュームのComplianceClockメタデータが更新され、新しいSCCとの関連付けが確立されます。これにより、VCCスキューが原因される可能性があります。このようなスキューを最小限に抑えるために、SCCアソシエーション（SCC /ノードID）に対する原因変更が可能なすべての処理は、続行する前にVCCを更新する必要があります。次に、そのようなシナリオを示します（このリストはすべてを網羅しているわけではありません）。

- ボリュームの制限
- ボリュームはオフライン
- アグリゲートがオフライン
- アグリゲートの再配置
- 停止/リブート

SnapLock準拠テスト

SnapLock Complianceボリューム上のアプリケーションソフトウェアとストレージを含む新しい包括的なアーカイブソリューションを実装しているIT組織では、多くの場合、コンセプトの実証段階から最終承認までのテストが必要です。承認マイルストーンが達成された後でも、アーカイブインフラのアップグレード作業の一環として、追加のテストが自然に発生する可能性があります。SnapLockコンプライアンスボリュームを使用するアプリケーションをテストすると、危険が発生する可能性があります。SnapLock Complianceトラディショナル・ボリュームまたはアグリゲートは、設計上、格納されているすべてのファイルの保持期間が終了するまで削除できません。誤って保持期間が長期間設定されている場合、すべての変更不可ファイルがそれぞれの保持期間の終わりに達するまで、SnapLock Complianceアグリゲートを構成するディスクを再利用できません。

物理ボリュームの使用

初期テストと継続的テストの両方で、ストレージ管理者は、最小限のドライブ数で構成される、永続的な専用テストボリュームを作成することを推奨します。SnapLock Complianceボリュームでアーカイブをテストする場合は、各ファイルまたはレコードに保持期限が設定されていることを確認してください。保持期限が設定されていない状態でSnapLockにコミットされたファイルは、デフォルトで最大保持期間（30年）に設定され、SnapLockボリュームのデフォルトまたは最大保持期限オプションで指定されていないかぎり、それより前に削除することはできません。ボリュームのSnapLockのデフォルトの保持期間は、ボリューム作成時のデフォルト以外の値に設定する必要があります。ファイルの保持期間が終了すると、そのボリュームを含むSnapLock Complianceテストボリュームを破棄してスペースを再生できます。

NetAppアプライアンスシミュレータの使用

SnapLockコンプライアンスプロセスをテストするもう1つの方法は、NetApp Support Siteで利用可能なONTAPシミュレータを使用することです。シミュレータはVMware仮想マシン（VM）内で実行され、NetAppストレージシステム上のONTAPと同等の機能をすべて備えています。ComplianceClockの値はシミュレータで設定できます。テストと統合のアクティビティ用に、どちらのタイプのSnapLockボリュームも作成できます。テストが完了すると、SnapLock準拠テストの場合でも、シミュレータを削除してすべてのディスクスペースを解放できます。ONTAPシミュレータの使用方法の詳細については、付属のドキュメントを参照してください。

本番SnapLockボリュームの作成と拡張

SnapLockストレージでは、ディレクトリがどのように扱われるかを考慮することが重要です。SnapLockボリュームに作成されたディレクトリは、アクセス権限に関係なく名前を変更できません。これは、Microsoft Windowsエクスプローラを使用して新しいフォルダを作成するときに覚えておくことが重要です。Windowsエ

クスプローラでは、最初にNew Folderというディレクトリが作成されます。SnapLockでは、このディレクトリの名前をより便利な名前に変更することはできません。SnapLock以外のボリュームでフォルダを作成して名前を変更し、正しく名前が付けられてSnapLockボリュームにコピーすることができます。Microsoft環境またはUNIX環境のSnapLockボリュームに手動でディレクトリを作成する場合は `mkdir` 、CLIでコマンドを使用して実行することを推奨します。ディレクトリの名前は変更できませんが、WORM状態にコミットされたファイルが階層内に含まれていなければ削除できます。

SnapLockボリュームの最小保持期間、最大保持期間、およびデフォルトの保持期間の値

SnapLockボリュームを作成すると、ボリューム上に存在するファイルについて、ボリュームの最小保持期間、最大保持期間、およびデフォルト保持期間にデフォルト値が設定されます。表1 にデフォルト値を示します。

表1）SnapLockボリュームのデフォルト値

オプション	SnapLock Enterprise	SnapLock Compliance
`minimum-retention-period`（最小）	0	0
`maximum-retention-period`（最大）	30 years	30 years
`default-retention-period`	最小	最大
`autocommit_period`	なし	なし

これらの値は保守的な値であり、会社の基準を反映していない可能性があります。NetAppでは、これらの値を見直し、会社のビジネス要件および法的要件に関連する値にリセットすることを推奨しています。

minimum-retention-period値を指定すると、ボリューム上にあるファイルの保持期間を最小期間よりも短い値に設定できなくなります。最小保持期間は、要求した保持期間がこの値よりも短い場合に使用されます。maximum-retention-periodは、ファイルが変更不可になる可能性がある最も遠い期間を表します。要求されたファイル保持期間が最大値を超えている場合は、最大保持期間が使用されます。[retention period]フィールドに値を指定しない場合は、default-retention-periodが使用されます。

未指定の保持

新たに作成されたデータに適用する保持期間を把握しているとは限りませんが、すぐに保護する必要があります。Unspecified Retention Time（URT；未指定の保持期限）を使用すると、作成後にデータをロックしたり、あとで保持期間を指定したりできます。

URTが設定されたファイルは、ファイルに絶対的な保持期限が設定されるまで保持

されます。ファイルにURTを設定するには、次の手順を実行します。

- ファイル保持CLI、NetApp Manageability SDK、REST APIを使用
- 保持期間が指定されていないEBRを使用する
- SnapLockボリュームのデフォルトの保持期間を指定せずに自動コミットを有効にする
- SnapLockボリュームのデフォルトの保持期間が指定されていない場合にNFSクライアントおよびCIFSクライアントから書き込み権限を削除する

絶対保持期限（ART）をURTからARTに変換できるのは、新しい保持期限が以前の保持期限よりも早い場合のみです。

URTを使用する場合は、明示的な保持期間を設定してベースライン（最小）の保持制御を確立することを推奨します。初期保持が適用されたら、ARTをURTに変更できます。これにより、アートが後で設定されたときに、最初に設定された値よりも低い値に設定することはできません。

データ保護

ONTAPには、データ保護と高可用性を促進するための多数の機能が組み込まれているか、アドオンオプションとして利用できます。ただし、規制機関で義務付けられているレベルのデータ保護を実現するには、より包括的なエンタープライズ戦略が必要です。NetAppでは、堅牢なアーカイブ解決策で考慮すべき少なくとも次のデータ保護戦略を推奨しています。NetAppプロフェッショナルサービスまたは認定テクノロジパートナーと連携して、お客様固有のビジネスニーズやテクノロジニーズに最も適したデータ保護戦略を特定できます。

リモートサイトへのレプリケーション

データ保持ルールの要件として、アーカイブ データのコピーをリモート サイトに保管するように規制機関から求められることがあります。この要件を満たすための最も簡単な方法は、プライマリNetAppシステムから別の場所にあるセカンダリNetAppシステムにデータをレプリケートすることです。

データレプリケーションをシームレスに実行できる統合NetAppソリューションには、次の3つがあります。

- 最も簡単で堅牢な解決策は、非同期モードでNetApp SnapMirror®機能を使用してリモートサイトにデータをレプリケートする方法です。非同期SnapMirrorは、すべてのWORM属性を維持したまま、SnapLockデータをリモートNetApp SnapLockボリュームにレプリケートします。SnapMirrorは、ONTAPで利用できるアドオンライセンス製品です。
- 2つ目の解決策であるndmpcopyは無償のユーティリティで、すでにONTAPにバンドルされています。ndmpcopyは、SnapMirrorと同様に、レプリケートコピー内で元のファイルのWORM状態を維持します。
- 3番目の解決策はNetApp MetroClusterです。ONTAP 9.0のMetroClusterでは、SnapLockエンタープライズアグリゲートのみがサポートされます。ONTAP 9.3では、privileged deleteを使用したSnapLock EnterpriseアグリゲートがMetroClusterでサポートされます。ONTAP 9.3以降では、MetroClusterのミラーされていないアグリゲートでもSnapLock準拠がサポートされます。MetroClusterミラーされたアグリゲートでのSnapLock準拠は、アグリゲートがSnapLock監査ログボリュームのホストにのみ使用される場合にのみサポートされます。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。

  注： 3つのレプリケーションケースすべてで、SnapLockファイルおよびボリュームの保持期限などのWORM属性が保持され、ソースからデスティネーションにミラーリングされます。

レプリケーションでの**ComplianceClock**の動作

SnapLock間でSnapMirror関係を作成する場合は、SnapLockのソースボリュームとデスティネーションボリュームのタイプが同じである必要があります。Volume SnapMirrorは、ソースからデスティネーションにブロックレベルのコピーを実行します。ソースからデスティネーションに、算出されたコア内ボリューム ComplianceClock（VCC）時間が送信されます。その結果、デスティネーションVCC時間はソースVCC時間と同じになります。デスティネーションVCCの時間は、SnapMirrorが更新されるたびに更新されます。ミラーリング関係が解除されると、デスティネーションボリュームは読み書き可能にマウントされ、デスティネーションシステムのComplianceClock（SCC）時間を参照としてVCCソフトウェアの動作が開始されます。したがって、休憩の結果として歪みは導入されません。

ディスクツーディスクバックアップ

NetAppは、NetApp SnapVault®と呼ばれる効率的なディスクベースのバックアップ解決策を提供します。ブロックレベルの増分処理を活用して、あらゆる環境に適した信頼性の高い低オーバーヘッドのバックアップとリカバリを実現します。ストレージ効率に優れた（ブロック差分のみ）毎日（またはそれ以上の頻度で）Snapshotコピーをセカンダリストレージにバックアップし（SnapVaultテクノロジを使用）、指定した保持期限まで変更や削除から保護します（SnapLockテクノロジを使用）。SnapLockボリュームのバックアップはサポートされていません。SnapVault関係のソースがSnapLockボリュームの場合、SnapVault転送は失敗します。

これらのWORM Snapshotコピーの保持期間は、ボリュームのデフォルトの保持期間を通じて指定できます。WORM Snapshotコピーの保持期間は延長できますが、短縮することはできません。ONTAP 9では、この機能はSnapLock with SnapVaultと呼ばれています。

WORM以外のSnapshotコピーでは、保持するSnapshotコピーの最大数に達すると、新しいSnapshotコピーが追加されると、最も古い保持Snapshotコピーが削除されます。ただし、古いWORM Snapshotコピーは保持期間が終了するまで削除できません。最大許容数を超えるWORM Snapshotコピーを保持する必要がある場合は、ボリュームクローンを使用してこの制限を克服する必要があります。

テープ バックアップ

NetAppは、光ディスクまたはテープベースのストレージに比べてニアラインデータストレージのパフォーマンスとストレージ機能が大幅に向上しますが、多くの企業にとって、テープバックアップは依然として全体的なデータ保護戦略において重要な役割を果たしています。SnapLockボリュームが別のサイトにミラーリングされていない場合、NetAppでは、SnapLockボリュームにアーカイブされた規制対象データを、テープかディスクかにかかわらず、NDMP開始のダンプおよびリストアを使用して、ソースファイルのWORM特性を維持することを推奨します。冗長なリカバリシナリオに備えて、規制対象データのコピーを複数作成するのが賢明です。これらの機能のデータストリームが強化され、データのバックアップ、リストア、またはコピーを行う際に、SnapLockボリューム上のファイルのWORM属性を保持できるようになりました。ただし、WORM属性を適切に適用するには、SnapLockボリュームへのリストアも実行する必要があります。SnapLockボリュームのバックアップをSnapLock以外のボリュームにリストアした場合、WORM属性は維持されますが、ONTAPデータ管理ソフトウェアでは無視され、適用されません。

物理的なセキュリティ

SnapLockは、データを変更不可の状態で完全に保持するように設計されています。SnapLockでは、ディスクが物理的に破壊された場合のデータ損失を防ぐことができません。光メディアプラッタや紙のドキュメントを物理的に破壊できるのと同じ意味で、SnapLockアグリゲート内のディスクを取り外して破壊することができます。いずれのシナリオでも、ストレージメディアの耐障害性は、その場所の物理的なセキュリティと同等です。SnapLockボリュームを備えたNetAppストレージシステムは、物理的な改ざんのリスクを最小限に抑えるために、制限された場所にあるロックされたキャビネットに収納する必要があります。

セキュリティの強化

データが組織のセキュリティ目標を確実に達成できるようにすることが非常に重要です。ONTAPには、インストールの耐障害性と生産性を高めるSnapLockに加えて、多数のセキュリティ機能が含まれています。TR-4569：『Security Hardening Guide for NetApp ONTAP 9』このテクニカルレポートでは、組織が情報システムの機密性、整合性、可用性について規定されたセキュリティ目標を達成するのに役立つ、ONTAP 9のガイダンスと構成設定について説明します。NetApp暗号化とSnapLock

お客様は、コンプライアンス保持要件がプライバシー規制と競合する場合など、重複する規制に準拠するためにデータを暗号化したいと考える場合があります。また、期限切れのコンプライアンスデータや削除されたコンプライアンスデータを保護するレイヤを追加したいと考えている場合もあります。ONTAP 9以降では、SnapLock ComplianceとSnapLock Enterpriseの両方がNetApp Storage Encryption（NSE）ドライブと組み合わせてサポートされます。NetAppボリューム暗号化（NVE）では、SnapLock ComplianceとSnapLock Enterpriseの両方もサポートされています。

注： NVEを使用している場合は、新しい空のSnapLockでのみ暗号化を有効にできます。既存のSnapLockボリュームで暗号化を有効にすることはできません。

暗号化では、暗号化キーを削除してデータを暗号化し、暗号化されたデータを読み取り不能にする機能も提供されます。

注意： 準拠したデータを（意図的または偶発的に）電子的にシュレッディングすると、お客様が訴訟を起こす可能性があります。災害発生時に暗号化キーが保護され、リカバリ可能であることを確認するのは、お客様の責任です。これを怠ると、SnapLockデータが永続的に破棄され、コンプライアンス違反になる可能性があります。

イベントベースの保持

イベントベースの保存は、指定されたイベントの後に一定期間ファイルを破棄することを指定する命令として定義されます。つまり、保持ポリシーは、このようなイベントが発生した時点（ファイルがWORM状態にコミットされたあとの未決定の期間）から開始されます。

イベントベースの保持（EBR）はONTAP 9.3で導入され、任意のSnapLockボリューム（SnapLock ComplianceまたはSnapLock Enterprise）に適用できます。EBRは、ファイルに対する無制限の保持とprivileged delete（特別なユーザが保持期限が切れる前にWORMファイルを削除できるSnapLock Enterpriseの機能）をアプリケーションレベルのブックキーピングと組み合わせて使用することで、SnapLock Enterpriseボリュームで実行できます。具体的には、SnapLock Enterpriseボリュームの保持期間のデフォルト値をinfiniteに設定し、ボリュームにファイルをコピーして、コピーしたすべてのファイルを追跡するアプリケーションをセットアップします。 その後、ファイルに無期限の保持期間を設定してファイルをWORM状態に移行します（この手順は自動コミットを使用して省略します）。

イベントが発生すると（通常はファイルごとに1つのイベント）、ファイルの保持ポリシーが適用されます。アプリケーションは個 々 のファイルを追跡するため'イベントが発生した後'アプリケーションは保存ポリシーで指定されている将来の特定の時点でファイルを削除するようにメモを作成するだけですこの時間が経過すると、アプリケーションはprivileged deleteを使用してこの削除を実行します。

ユーザは、保持ポリシーを作成してSnapLockボリュームに適用する必要があります。

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

ユーザは、SVM全体のイベント保持ポリシーを作成、変更、削除、および一覧表示できます。このポリシーは、単一のファイルまたはディレクトリ全体に適用できます。EBRポリシーをWORM状態でないファイルに適用すると、そのファイルはWORM状態にコミットされます。EBRポリシーをWORMファイルに適用した場合、EBRポリシーを適用した場合にのみ、そのファイルの保持期限を延長できます（短縮することはできません）。

1つのシンプルで現実的な例として、医療機関では、IBM FileNetなどのエンタープライズコンテンツ管理（ECM）解決策を使用してSnapLock Enterpriseボリューム上の患者記録を管理しています。HIPAAは、患者の死亡後7年間、患者記録の不変コピーを保持することを求めています。FileNetはSnapLockと統合されていますが、このタイプのビジネスプロセスでは、ONTAP REST APIを使用した拡張統合が必要です。死亡日が事前に判明していないため、すべての患者記録は最初に無制限の保持で設定されます。イベント発生から7年後、FileNetは、SnapLockボリュームから患者データを削除するコードを含む削除前処理を実行します。FileNet内では、これは監査可能なイベントとして登録されます。同様に、NetAppストレージシステム内では、privileged delete処理がSnapLock Complianceボリュームに記録されます。この処理は、ストレージ管理者であっても変更または削除することはできません。FileNetなどのECMアプリケーションとSnapLockやprivileged deleteを統合することで、企業は柔軟でコスト効率の高いストレージプラットフォームで規制の記録保持要件を満たすことができます。

privileged delete処理およびこの機能を公開するONTAP REST APIの詳細については、NetApp Support SiteのONTAP 9ドキュメントセンターを参照してください。

リーガル ホールド

ONTAP 9.3ではリーガルホールドの機能が導入されました。リーガルホールドは、訴訟目的で無期限に改ざんを防止した状態でファイル、フォルダ、ボリューム、またはボリュームリストを保持する機能です。この保留により、リーガルホールドが解除されるまで、指定したオブジェクトが削除されることはありません。このリーガルホールドはいつでも解除できます。リーガルホールドを解除しても、以前の保持期間または元の保持期間が経過していない場合は、元の保持期間または以前の保持期間が有効なままになります。

リーガルホールドは、SnapLock Complianceボリュームでのみ許可されます。ファイルあたり最大255件のリーガルホールド、ボリュームあたり65,535件の訴訟を適用できます。訴訟ごとのファイル数に制限はありません。ボリューム内の使用可能なスペースのみによって異なります。リーガルホールドの対象となるボリュームには無期限の保持が設定されています。すべてのリーガルホールドがボリュームから削除されると、以前の保持期間に戻ります。訴訟関連のメタデータはすべて、ボリュームのパブリックinodeスペースに格納されます。ユーザはこのデータを変更することはできません。リーガルホールドの開始処理と終了処理は、パスの下に監査ログが記録されます `/snaplock_log/legal_hold_logs/`。

ボリュームの言語設定でUTF文字セットが許可されている場合は、訴訟名にASCII以外の文字セット（UTF8）を使用できます。訴訟名の先頭を「」にすることはできません。 またはを使用できます。スペースは使用できません。また、訴訟名の最大長は80文字に制限されています。

ブロックレベルのレプリケーションを実行するSnapMirrorでは、リーガルホールドのメタデータをレプリケートします。リーガルホールド情報のバックアップとリストアは、ボリューム全体のバックアップとリストアでのみサポートされます。サブボリュームのきめ細かなバックアップやリストア（qtree、ディレクトリ、ファイルなど）では、リーガルホールド情報は保持されません。

リーガルホールドを適用または削除するコマンドインターフェイスは次のようになります。

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

さまざまなCLIオプションを使用してステータスを表示することもできます。

```
show’ command displays the holds on a particular volume. vserver::> snaplock legal-hold show -
volume vol1
Operation

hold    16842755       vs1     vol1 Completed
hold    16842757       vs1     vol1 Completed
‘dump-litigations’ command displays the litigation within a given SVM.
vserver::> snaplock legal-hold dump-litigations -output-volume out -output-directory-path /d1
```

SnapLockとSnapVault

ONTAPを使用すると、SnapLockボリューム以外のフレキシブルボリュームをSnapLock Enterpriseボリュームまたは SnapLock Complianceボリュームにバックアップできます。つまり、ソースとしてのFlexVolボリュームとデスティネーションとしてのSnapLockボリュームの間にSnapVault関係を作成できます。Snapshotコピーは（SnapVaultテクノロジを使用して）セカンダリストレージにバックアップされ、（SnapLockテクノロジを使用して）指定した保持期限まで変更や削除から保護されます。

関係に関連付けられたSnapMirrorポリシーは、特定のSnapMirrorラベルのSnapshotコピーをデスティネーションSnapLockボリュームで保持する数を定義します。SnapLockボリュームのデフォルトの保持期間は、このボリューム（デスティネーション）までにバックアップ（転送）されたSnapshotコピーの保持期間です。その結果、Snapshotコピーにsnaplock-expiry-timeが設定されます。Snapshotコピーのsnaplock-expiry-timeをデフォルトの有効期限よりも長くすることもできます。スケジュールされた転送（または手動更新）処理のたびに、SnapMirrorラベルに対応する古いSnapshotコピーの削除が試行され、保持数が維持されます。ただし、これらのSnapshotコピーの有効期限があとの場合、Snapshotコピーは削除されません。SnapLockデスティネーションボリュームでは、SnapMirrorポリシーで指定された数を超えた場合でも、保持/バックアップするSnapshotコピーの数が増え続けます。たとえば、デフォルトの保持期間が1カ月（30日）のSnapLockデスティネーションボリュームで、日単位のSnapshotコピーを15個保持する必要がある場合などです。SnapVault転送スケジュールが毎日に設定されています。有効期限は30日後に設定されるため、16番目のSnapshotコピーが転送されても、最も古いSnapshotコピーは削除されません。31日目にのみ、31日目にSnapshotコピーが転送されると、最も古いSnapshotコピーが削除されます（保持期間が期限切れになるため）。

retention-periodまたはretention-countを設定するCLIコマンド：

```
snapmirror policy add-rule -vserver verver -policy test_lv -snapmirror-label sle
-keep 15

volume snaplock modify -volume test_dst -default-retention-period "30days"
```

注： デスティネーションがSnapLock Complianceボリュームの場合、デフォルトの保持期間は30年です。SnapLock ComplianceボリュームへのSnapVault Snapshotコピーの転送を開始する前に、デスティネーションボリュームでデフォルトの保持期限を設定することを推奨します。

リストア

SnapLockボリューム内のデータをリストアする場合、手順は、SnapLock Complianceの場合を除き、他のNetApp Snapshotコピーをリストアする場合と同じです。SnapLockエンタープライズデータ、NetApp FlexClone®、 `snapmirror restore` 処理、およびNetApp SnapRestore® All for SnapLockエンタープライズデータの場合は、NetApp Snapshotデータの場合と同じです。SnapRestore処理は、ファイルおよびデータのリカバリや以前の正常な状態へのリバートに非常に役立ちます。ただし、SnapLock Complianceボリュームの場合、SnapRestoreまたはFlexCloneを以前の状態にリカバリすると、Snapshotコピーの作成後に書き込まれたすべてのデータが失われる可能性があります。これを許可すると、データのWORM整合性とコンプライアンスに違反します。

SnapLock Complianceボリュームからデータをリストアする場合は `ndmp copy`、の `ndmp restoresnapmirror restore` 各処理を実行できます。LUNデータを含むSnapshotコピーでLUNがSnapLockボリューム上のSnapshotコピーでロックされている場合は、 `snapmirror restore` その処理を通じてSnapLock以外のボリュームにLUNをリストアする必要があります。

SnapLockコンプライアンスデータのFlexCloneボリュームを作成することもできますが、ただし注意事項があります。クローンは元のプロパティを継承します。作成されたFlexCloneは読み取り専用で、元のSnapshotコピーの保持を継承します。元のSnapshotコピーの保持期限まではFlexCloneボリュームを削除できません。保持期間が短い場合は問題にならない可能性がありますが、保持期間が長い場合は、FlexCloneボリュームに削除できない問題が発生する可能性があります。

SnapLockコンプライアンスデータをリストアする最良の方法は引き続き `snapmirror restore`使用できます。

ONTAP 9.13.1以降では、RWボリュームのFlexCloneを作成する際に、3つのSnapLockタイプ（Compliance、Enterprise、non-SnapLock）のいずれかを指定できます。デフォルトでは、FlexCloneボリュームは親ボリュームと同じSnapLockタイプで作成されます。ただし、FlexCloneボリュームの作成時にsnaplock-typeオプションを使用すると、デフォルトの設定を上書きできます。詳細については 、ONTAPのドキュメントを参照してください。

その他

SnapLockボリュームのハードリンクの動作は、フレキシブルボリュームの場合とまったく同じです。ファイルへのハードリンクは、同じディレクトリ内に作成することも、複数のディレクトリにまたがって作成することもできます。デスティネーションファイルには、RW、WORM、またはWORM_APPEND（VAMまたは非VAM）を指定できます。WORMファイルへのハードリンクは、そのハードリンクもWORMになります。その場合、基盤となるinodeが期限切れになるまでハードリンクを削除できません。

まとめ

SnapLockコンプライアンスとSnapLockエンタープライズは'WORMストレージ機能に優れたパフォーマンスと低いTCOを必要とする企業向けに'包括的なデータ・アーカイブ解決策の重要な要素として設計されていますSnapLockには、従来のWORMストレージよりも優れている点として、パフォーマンスの向上や高度なデータ保護などのメリットがあり、同時にストレージ管理コストを大幅に削減できます。これらのSnapLockのメリットは、コンプライアンスや規制に準拠するためにストレージ要件を変更できない企業のニーズに対応します。SnapLockを使用すると、競合製品よりも複雑さを軽減しながら、厳格なデータ保護と改ざん防止の基準を組織全体に適用できます。

SnapLockの強力なデータ永続性とデータ整合性機能は、既存のONTAPデータ管理ソフトウェアとストレージ製品ラインを活用することでTCOを削減し、ストレージ効率に優れたレプリケーションテクノロジを使用して運用コストを継続的に削減します。 また、オープンで業界標準のプロトコルを使用して、データアクセスとアプリケーション統合を簡易化します。これらを組み合わせることで、WORMデータストレージ領域で比類のない解決策を実現できます。

NetAppのソリューションベース製品の詳細については、www.netapp.com/productsを参照してください。

付録A：7-ModeからONTAP 9への移行

ONTAP 9.0は、クラスタ環境にSnapLockを導入した最初のリリースです。7-Modeストレージシステムを使用しているNetAppの既存のお客様は、ONTAP 9のclustered環境の機能を利用するには、既存の7-Mode環境を移行する必要があります。クラスタ環境への移行では、現在の環境を確認し、移行対象を定義し、デスティネーションシステムの最適な構成を設計し、データと構成のマイグレート方法を計画し、必要に応じて環境を更新します。

このセクションでは、7-ModeシステムからONTAP 9システムにSnapLockデータを移動するために必要な主な知識について説明します。このセクションでは、SnapLockに固有の推奨事項についてのみ説明します。7-Modeからクラスタ環境への移行の基本事項については、TR-4052『Successfully Transitioning to Clustered Data ONTAP』を参照してください。このテクニカルレポートには、7-Modeストレージ環境の範囲を設定、設計、およびクラスタ環境に移行するためのガイダンスが記載されています。また、NetApp SnapMirror®、qtree、NetApp FlexClone® ボリュームなど、移動に関するONTAPの主な考慮事項についても説明します。また、NetApp Universityでは、移行の基礎をカバーするONTAPクラスも多数用意されています。

- NetApp Transition Fundamentals（Webベース）
- Planning and Implementing Transition Using the 7-Mode Transition Tool（Webベース）
- Transitioning to clustered Data ONTAP（Webベース）

基本的な理解を得たら、移行の計画を開始できます。

注： SnapLockボリュームにLUNが含まれている場合、7-Mode SnapLockボリュームの移行はサポートされません。

ベスト プラクティス

ここで説明する手順に従うことは、法的コンプライアンスを意味するものではありません。重要な手順が移行計画全体に含まれるように、計画の出発点として使用することを目的としています。固有のコンプライアンス要件を確実に満たすために、法務部門と相談することを強くお勧めします。

データマイグレーション方式

クラスタ環境へのデータマイグレーションを開始する前に、アプリケーションタイプ、アプリケーション環境、その他の要因に基づいて推奨されるマイグレーション方式を特定します。現在利用可能な移行ツールはいくつかあり、それぞれにメリットと考慮事項があります。これらのツールは、次の2つのカテゴリに分類できます。

レプリケーションベースの移動

このマイグレーション方式はNetApp SnapMirrorテクノロジを使用しており、7-Mode Transition Tool（7MTT）SnapMirrorと移行データ保護（TDP）SnapMirrorの両方で使用できます。ONTAPによって報告されるTDP SnapMirror関係とは、ソースが7-Modeでデスティネーションがの SnapMirror関係のタイプを指します。レプリケーションベースのマイグレーションの主なメリットは、マイグレーションアクティビティを通じてSnapshotコピーとストレージ効率に優れたレプリケーションによる削減効果が維持されることです。

SnapLockボリュームの移動は、手動のTDP SnapMirrorまたは7MTT v3.3.3を使用して実行できます。ただし、NetAppでは、7MTTを使用して7-Modeボリュームを移行することを推奨しています。これは、移動プロセスのすべてのステップで7-Modeとクラスタ環境の両方が事前チェックされ、多数の潜在的な問題を回避できるためです。このツールを使用すると、データ移行に加えて、すべてのプロトコル、ネットワーク、サービス構成の移行が大幅に簡易化されます。

注： 7MTTではCopy-Based Transition（CBT；コピーベースの移行）のみがサポートされ、SnapLockボリュームに対してCopy-Free Transition（CFT；コピーフリーの移行）はサポートされません。

コピーベースマイグレーション

ホストベースおよびアプリケーションベースのマイグレーション方式では、NetAppで直接提供またはサポートされていないツール（NetApp製品ではないため）を使用します。

データ マイグレーションに多く使用されるホストベースのツールは次のとおりです。

- さまざまなベンダーが提供する論理ボリューム マネージャ（LVM）
- ScriptLogic Secure Copy
- Rsync
- Robocopy / Richcopy
- PEER Software PeerSync
- Data Dynamics StorageX

前述のツールには、一般的なデータマイグレーションツールもあれば、7-Modeからクラスタ環境への移行に対応するためにNetAppパートナーが自社製品に特定の機能を組み込んだツールもあります。アプリケーションベースとホストベースのマイグレーション方式はどちらもコピーベースであり、レプリケーションベースではありません。そのため、SnapshotコピーとStorage Efficiencyによるレプリケーションによる削減効果は、データマイグレーションアクティビティによって維持されません。

注： NetAppは、サードパーティ製ツールを直接サポートしていません。データ移行にサードパーティのツールを使用していて、ONTAPや他のNetApp製品とは関係のないツールで問題が発生した場合は、ベンダーのカスタマーサポート部門に問い合わせる必要があります。

移行を実行する前に、ONTAP 9への移行がサポートされるONTAP 7-Modeのバージョンを確認しておく必要があります。ソースの7-Modeシステムに64ビットのアグリゲートとボリュームしかない場合は、それらをONTAP 9に移行できます。ただし、ソースの7-Modeシステムに32ビットのアグリゲートまたは32ビットのSnapshotコピーを含むボリュームがある場合は、最初にONTAP 8.1.4 P4または8.2.1にアップグレードする必要があります。アップグレードが完了したら、32ビットアグリゲートを64ビットに拡張してから、Snapshotを含む32ビットデータを検出して削除する必要があります。

コピーベースのマイグレーション方式では、移行元と移行先のアグリゲート タイプにかかわらず、データをマイグレートできます。ただし、レプリケーションベースのマイグレーション方式では、ソースの7-Modeストレージシステムから ONTAP 9の64ビットアグリゲートに32ビットアグリゲートを移行することはできません。64ビットアグリゲートに32ビットSnapshotコピーがあるかどうか不明な場合は、NetAppのサポートにお問い合わせください。

準備

SnapLockボリュームを7-ModeからONTAP 9に移行する前に、7-Modeストレージシステムとクラスタを準備し、7-ModeシステムとStorage Virtual Machine（SVM）の間に移行ピア関係を作成する必要があります。

また、7-ModeストレージシステムにSnapMirrorのライセンスがあり、デスティネーションクラスタにSnapLockのライセンスがあることも確認する必要があります。SnapLockボリューム間の7-Mode VSM関係を移行する場合は、デスティネーションクラスタにSnapLockライセンスとSnapMirrorライセンスが必要です。

データコピー

次に、SnapLockシステムに関連する最も一般的なマイグレーションシナリオで推奨されるマイグレーションアプローチを示します。

シナリオ1：スタンドアロンボリューム

スタンドアロンボリュームの移行は、7MTT（推奨）または手動のTDP SnapMirrorを使用して簡単に実行できます。このプロセスでは、7-ModeソースとONTAP 9デスティネーション間にSnapMirror関係を作成し、ベースライン転送を実行し、差分更新を実行し、データコピー処理を監視し、SnapMirror関係を解除して、7-ModeボリュームからONTAP 9ボリュームにクライアントアクセスを移動します。

7-ModeのComplianceボリュームはONTAP 9のSnapLock SnapLockボリュームにのみ、SnapLock Enterpriseボリュームは SnapLock Enterpriseボリュームにのみ移行できます。表2 に、SnapLockボリュームの移行でサポートされる組み合わせを示します。

表2）SnapLockボリューム移行の組み合わせ

SnapMirrorデスティネーション			
	SnapLock Compliance	SnapLock Enterprise	通常のFlexVolボリューム
SnapLock Compliance	✓	✘	✘
SnapLock Enterprise	✘	✓	✘
通常のFlexVolボリューム	✘	✘	✓

注： 7-Modeの監査ログボリュームはノードに固有ですが、ONTAP 9の監査ログボリュームはSVMに固有です。

移行中に、SnapLock監査ログボリュームをONTAP 9デスティネーション内のどこに配置するかをユーザが決定する必要があります。ログボリュームは管理者が信頼できるSnapLock Enterpriseボリューム上の処理によってのみ生成されるため、この動作は許容可能です。

シナリオ2：SnapMirrorを使用した基本的なディザスタリカバリ

基本的なディザスタ リカバリのシナリオで扱うのは、単一のソース ボリュームとデスティネーション ボリュームがVolume SnapMirror関係にある、最も一般的なケースです。ボリューム、関連するSnapshotコピー、およびSnapMirror関係のマイグレーションは、7MTT（推奨）または手動のTDP SnapMirrorを使用して簡単に実行できます。

SnapLock Complianceボリュームの並行移行

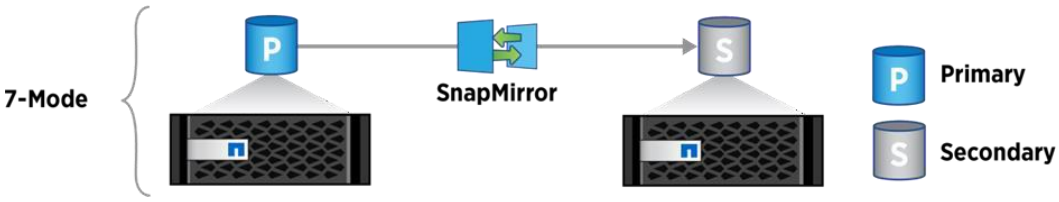
SnapLock Complianceボリュームの場合は、7-Mode SnapMirror関係のプライマリボリュームとセカンダリボリュームを、同じカットオーバー期間内に並行して移行できます。移行後に、ONTAPでVolume SnapMirror関係を手動で設定する必要があります。

SnapLock Complianceボリューム間の7-Mode SnapMirror関係は、並行して移行する必要があります。SnapLock ComplianceボリュームとのTDP関係のSnapMirror再同期は、データが失われる可能性があるためサポートされていません。そのため、SnapLock Complianceボリュームを使用する7-Modeプライマリボリュームと ONTAPセカンダリボリュームの間にSnapMirrorディザスタリカバリ関係を確立することはできません。

SnapLock Enterpriseボリュームの段階的移行

7-ModeのVolume SnapMirror関係を移行する場合は、SnapLock Enterpriseボリュームに対してのみ段階的移行（セカンダリを移行してからプライマリを移行）を使用できます。7-Modeプライマリボリュームと ONTAP セカンダリボリュームの間のSnapMirrorディザスタリカバリ関係は、SnapLock Enterpriseボリュームでのみサポートされ、SnapLock Complianceボリュームではサポートされません。

図1）7-Modeにおける基本的なディザスタリカバリ



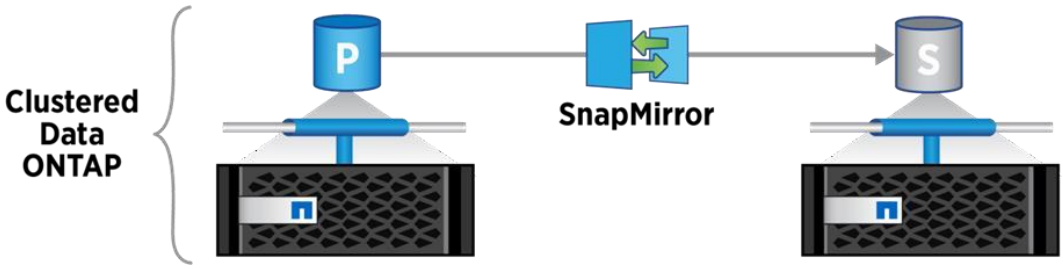
移行手順

SnapLockボリュームを含むディザスタリカバリ関係は、次の手順でCBTを使用して7-ModeからONTAP 9に移行できます。

1. デスティネーションボリュームは別々に移行します。
2. 7-ModeソースボリュームとONTAP 9で移行したデスティネーションボリュームの間の関係を作成して、移行したボリュームをディザスタリカバリ関係のデスティネーションボリュームにします。SnapLock準拠の場合、この手順はスキップしてください。SnapLock準拠の場合、データが失われる可能性があるため、SnapMirrorの再同期は実行できません。
3. ソースボリュームを移行
4. SnapLock Enterpriseの場合は、7-ModeソースとONTAP 9デスティネーションの間のディザスタリカバリ関係を解除します。SnapLock Complianceの場合は、SnapMirrorが解除されたあとに、ソースボリュームとデスティネーションボリューム間のSnapMirrorが再確立されます。
5. 移行元ボリュームとデスティネーションボリュームの間でSnapMirrorの再同期を実行します。

要約すると、SnapLockコンプライアンスディザスタリカバリ関係の移行では並行移行のみがサポートされますが、SnapLockエンタープライズディザスタリカバリ関係では段階的移行と並行移行の両方がサポートされます。

図2）クラスタモードにおける基本的なディザスタリカバリ



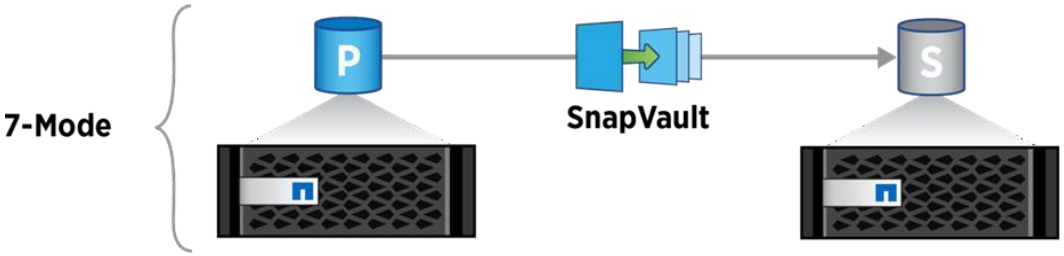
シナリオ3：SnapVaultを使用したSnapLock（LockVault）

SnapLock with SnapVaultは、7-Modeの非構造化データを対象としたディスクベースのコンプライアンス解決策です。ONTAP 9では、この機能はSnapLock with SnapVault®と呼ばれて**います。**バックアップをコンプライアンスに準拠させ（データの1つのコピーを2つの目的に使用）、ブロックレベルの増分変更のみを保存することで、容量効率に優れた規制解決策を実現します。ストレージ効率に優れた（差分ブロックのSnapshotコピー）Snapshotコピーをセカンダリストレージにバックアップし（SnapVaultテクノロジを使用）、指定した保持期

限まで変更や削除から保護します（SnapLockテクノロジを使用）。

この機能には、7-Modeとの違いが1つあります。7-Modeでは、Snapshotコピー間の変更を追跡してWORMボリュームに格納するコンプライアンスジャーナル（ファイルログ）がサポートされているため、ログも変更できません。ONTAP 9では、転送ごとにファイルの変更を追跡するコンプライアンスジャーナルの作成はサポートされていません。

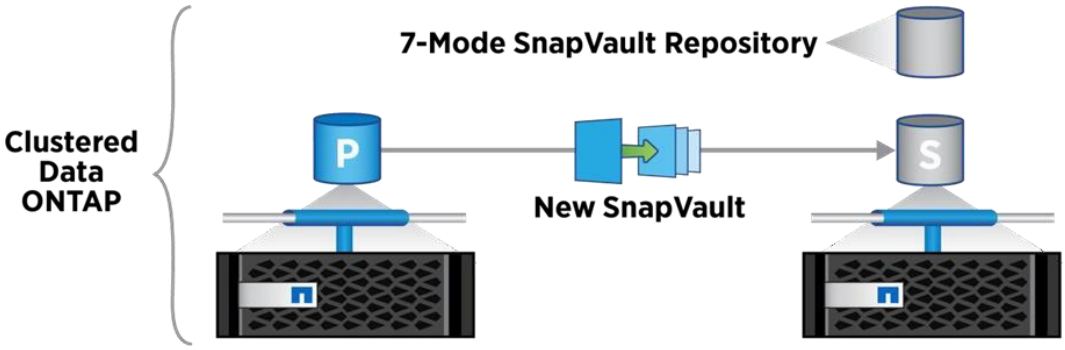
図3）7-ModeにおけるSnapLockとSnapVault



7-ModeからLockVault関係をONTAP 9に移行することはできません。バックアップデスティネーションはスタンドアロンボリュームとして移行できます。ボリューム移行の一環として、LockVaultデスティネーションに32ビットのWORM Snapshotコピーがある場合は移行できません。7-ModeのSnapVaultはqtreeベースですが、clustered環境のSnapVaultはボリュームベースです。そのため、ONTAPで新しいSnapVault関係を作成し、7-Mode SnapVaultリポジトリに最適な対処方法を決定する必要があります。プライマリ ボリュームは、7MTTまたは手動のTDP SnapMirror関係を使用して、通常の方法でマイグレートできます。セカンダリボリュームの移動は、日次バックアップを想定したリポジトリの保持期間によって異なります。

- 保持期間が3カ月を超える場合は、リポジトリを（ONTAPでの新しいSnapVault関係のセカンダリボリュームとしてではなく）アーカイブ用のONTAPボリュームに移行する必要があります。
- 保持期間が3カ月以内の場合は、7-Modeのリポジトリをそのまま残し、期間が過ぎたら廃棄します。

図4）clusteredモードでのSnapVaultを使用したSnapLock



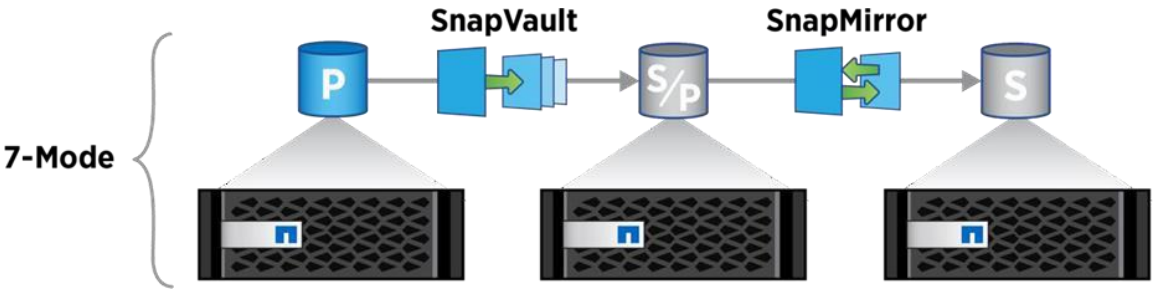
プライマリボリュームのONTAPへの移動と新しいSnapVault関係の確立は、7-Modeのセカンダリボリュームには依存しません（ONTAP SnapVault関係は新規であるため）。ONTAPで新しいSnapVault関係を作成するには、ベースライン転送を完了する必要があります。

注： この `snap restore` コマンドはSnapVaultデスティネーションでは使用できません。

シナリオ4：SnapVaultからディザスタリカバリへのカスケード

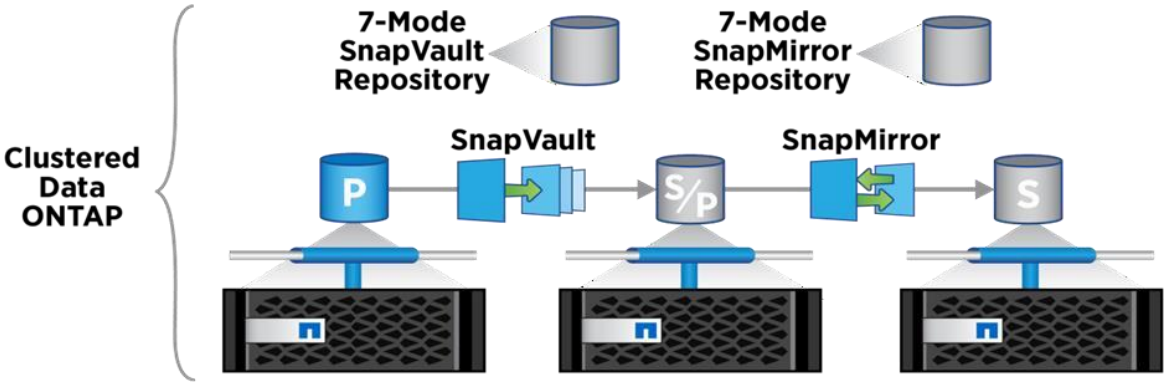
SnapVaultからディザスタリカバリへのカスケードのシナリオで扱うのは、SnapVaultのプライマリボリュームとセカンダリボリュームがあり、SnapVaultのセカンダリボリュームがSnapMirror関係のプライマリボリューム（別のセカンダリボリュームを使用）であるケースです。

図5）7-ModeにおけるSnapVaultからディザスタリカバリへのカスケード



このアプローチでは、SnapVaultのセカンダリボリューム、およびSnapMirrorのプライマリボリュームとセカンダリボリュームには、クラスタ環境で直接リストアできないSnapshotコピーのデータが含まれています。最初に、7MTTまたは手動のTDP SnapMirrorを使用して、プライマリSnapVaultボリュームをクラスタ環境にマイグレートします。プライマリSnapVaultボリュームをカットオーバーする前に、SnapVault関係を解除する必要があります。プライマリSnapVaultボリュームをクラスタ環境に配置したら、新しいSnapVault関係を作成します（新しいデスティネーションボリュームを使用）。SnapVaultボリュームが確立されたら、SnapVaultセカンダリボリュームと新しいSnapMirrorデスティネーションボリュームの間に新しいSnapMirror関係を作成できます。7-ModeのSnapVaultセカンダリボリュームとSnapMirrorセカンダリボリュームは、どちらも「シナリオ3：SnapLock with SnapVault（LockVault）」で説明した保持アプローチの対象となります（7-Modeに保持するか、保持期間に基づいて別のクラスタ環境ボリュームに移動します）。Snapshotコピーの保持期間が短い場合（数週間または最大で数か月）は、Snapshotコピーが期限切れになるまでSnapMirrorセカンダリボリュームを7-Modeに残した方が簡単です。クラスタ環境で新しいSnapVault関係と新しいSnapMirror関係を確立するには、どちらもベースライン転送を完了する必要があります。

図6）ONTAP 9におけるSnapVaultからディザスタリカバリへのカスケード



移行中の7-Modeサイトでの災害からの復旧

7-ModeプライマリボリュームとONTAPセカンダリボリュームの間のSnapMirrorディザスタリカバリ（DR）関係は、SnapLock Enterpriseボリュームでのみサポートされます。

7-Modeのプライマリボリュームとクラスタ環境のセカンダリボリュームの間にSnapMirrorディザスタリカバリ関係が確立されていて、7-Modeのプライマリサイトで災害が発生した場合は、クラスタ環境のセカンダリボリュームにクライアントアクセスを転送できます。災害後に7-Modeのプライマリ ボリュームがオンラインに復帰したら、7-Modeのプライマリ ボリュームを移行する必要があります。この時点では、7-Modeのプラ

イマリボリュームに対するSnapMirror関係はすべて解除されて削除されているため、このタイプの移行ではスタンドアロンボリュームを移行します。ONTAPプライマリボリュームへの移行が完了したら、ONTAPプライマリボリュームを再同期して、ONTAPセカンダリボリュームに書き込まれたデータを取得できます。その後、クラスタ環境のプライマリボリュームにクライアントをリダイレクトします。

警告

クラスタ環境のボリュームから7-ModeボリュームへのSnapMirror再同期はサポートされていません。そのため、災害後に7-Modeのプライマリボリュームとクラスタ環境のセカンダリボリュームの間にディザスタリカバリ関係を再確立すると、セカンダリクラスタ環境のボリュームに書き込まれたデータはすべて失われます。

検証

前の手順で作成されたデータコピーは同一であり、処理中にすべてのSnapLockメタデータが保持されます。ただし、この検証手順は、SnapLockデータのソースコピーとデスティネーションコピーの両方で、すべてのファイルとその内容の永続的なレコードを生成するために必要です。このレコードは、コピーの処理中にWORMデータの内容や保持期間などのプロパティが変更されていないことをあとで確認するのに役立ちます。検証結果は、コピー後にソースが破棄または破棄された場合に特に役立ちます（そのため、後日内容を検証することはできません）。

7MTT v3.3.3には、移行したSnapLockボリューム内のファイルに対して移行後のデータ検証を実行するSnapLockのCoC機能が用意されています。移行の完了後に、7MTTプロジェクト内のSnapLockボリュームに対してCoC処理をトリガーできます。この処理は、プロジェクト内のすべてのSnapLockボリュームに対して実行することも、一部のSnapLockボリュームに対して実行することもできます。CoC検証は、ComplianceボリュームとEnterprise SnapLockボリュームの両方でサポートされます。CoC検証は、読み書き可能なSnapLockボリュームでのみサポートされ、読み取り専用SnapLockボリュームではサポートされません。

7MTTのCoCの詳細については、ONTAP 9ドキュメントセンターおよび特定のCoCのドキュメントを参照してください。

7MTTのCoC機能を使用していない場合は、検証タスクを手動で実行できます。WORMデータがデスティネーションにコピーされたら、チェックを実行して次の条件をテストできます。

- コピーされたファイルの関連するメタデータとコンテンツは、ソースと同じです。
- ソースとデスティネーションで有効な保持期間が同じです。
- SnapLockに関連するオプション（ボリュームレベルとシステム全体の両方）は、両側で同じです。

絶えず変化するデータに対処しないように、データの最新のSnapshotコピーに基づいて比較を行うことを推奨します。

テスト1：コピーされたファイルの関連メタデータとコンテンツがソースと同じである

そのためには、ソースとデスティネーションのファイルの「フィンガープリント」を生成して比較するか、コンテンツとメタデータを1バイトずつ比較します。フィンガープリント処理では、MD5またはSHA-256のいずれかのハッシュアルゴリズムを使用して、ファイル単位でフィンガープリントを生成できます。NetAppではSHA-256の使用を推奨しています。これにより、ユーザーは任意の時点でファイルの整合性を検証できます。ファイルフィンガープリントは、ユーザおよびパートナーアプリケーション用のCLIおよびNetApp Manageability SDKを使用して、ONTAPの外部にエクスポートされます。SnapLockは、システム内の任意の場所にファイルフィンガープリントをディスクに格納しません。ファイルフィンガープリントは、CLIまたはNetApp Manageability SDKを介してユーザから要求されたファイルのハッシュダイジェストをオンザフライで計算します。ファイルフィンガープリントを問題するには、次のコマンドを使用します。

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

上記のコマンドを使用してファイルフィンガープリントが発行されると、セッションIDが生成されます。このセッションIDを使用すると、次のコマンドを使用してステータスを確認できます。

```
volume file fingerprint show -session-id <session-id>
```

ステータスがcompletedになったら、前のコマンドと同じsession-idを使用し、次のコマンドを問題してフィンガープリント出力を取得します。

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

FILEタイプは、`worm` SnapLockファイルの場合、 `worm_appendable` 追記可能WORMファイルの場合 `worm_active_log worm_log`、アクティブなWORMログファイルの場合、閉じたWORMログファイルの場合です。`regular` 通常のファイルやSnapLock以外のファイルの場合も同様です。

NetAppでは、ファイルメタデータを比較する際に、次のファイル属性を使用することを推奨しています。

- ファイル タイプ
- ファイル サイズ
- ファイル所有者のユーザID
- ファイル所有者のグループID
- 所有者のセキュリティID（SID）（CIFSからのみ表示）
- 最終変更時刻（mtime）
- 最終アクセス日時（atime）：SnapLockでは、ファイルのファイル保持期間を表します。
- ファイル作成時間（CIFSクライアントからのみ表示され、NFSクライアントからは表示されません）
- ステータスが最後に変更された時刻（ctime：NFSクライアントにのみ表示され、CIFSクライアントには表示されない）
- ファイル権限とその他のセキュリティ属性

注： コピーの直後に検証を実行せずに、新しいシステムをしばらく使用したあとに検証を実行すると、ファイルのメタデータが完全に一致しない場合があります。たとえば、WORMファイルの保持期間が延長された可能性があります（短縮することはできません）。さらに、新しいWORMコンテンツやWORM以外のコンテンツが作成されている可能性があります。期限切れのWORMファイルも削除されている可能性があります。このような場合、状況に応じて、検証を緩和してこれを考慮することができます。

テスト2：ソースとデスティネーションで有効な保持期間がほぼ同じ

両端で有効な保持期間が同じであることを確認する必要があります。最終アクセス日時（前に実行）を照合すると、いずれのエンドでも保持タイムスタンプが同じになります。

ただし、絶対タイムスタンプを意味するためには、ComplianceClockの値も両端で比較する必要があります。新しいシステムのComplianceClockは同期されているか、ソースよりも遅れている必要があります。新しいシステムのComplianceClockが遅れている場合は、保持期間がはるかに長くなります。

テスト3：ソースとデスティネーションでSnapLockオプションが同じ

最後に、SnapLockに関連するボリュームオプションとシステムオプションを比較して、ソースとデスティネーションの両方で同じにする必要があります。関連するSnapLockオプションは次のとおりです。

- ボリューム名
- SnapLockタイプ：エンタープライズまたはコンプライアンス

- 最小保持期間
- デフォルト保持期間
- 最大保持期間
- 自動コミット期間
- 有効期限
- ComplianceClock時間
- privileged deleteオプション：enabled、disabled、またはpermanently disabled

これらの詳細情報は、次のコマンドを使用して取得できます。

```
volume snaplock show -vserver <vserver name> -volume <volume name>
```

レポート

これは、監査の観点から関連する詳細とともに実行されたアクションの概要です。レポートには検証フェーズの情報が含まれている必要があります。レポートは、ボリューム内のすべてのレコードの最大保持期間と同じ保持期間を持つWORMレコードとして格納する必要があります。

移行のレポートに関連する可能性のある項目のチェックリストを次に示します。

- データ移行を実行する理由。
- 移動を実行する個人の詳細。
- ソースノードとデスティネーションノードのシステム情報。次のコマンドを使用して取得できます。`system node show -node <nodename>`
- ソースとデスティネーションのマイグレートされたSnapLockボリュームのボリューム情報。
- 処理の開始時と終了時のソースとデスティネーションのComplianceClockの値。

詳細情報の入手方法

このドキュメントに記載されている情報の詳細については、次のドキュメントやWebサイトを参照してください。

- TR-4052『Successfully Transitioning to Clustered Data ONTAP』
  http://www.netapp.com/us/media/tr-4052.pdf
- ONTAP 9ドキュメント
  https://docs.netapp.com/us-en/ontap/index.html

お問い合わせ

本テクニカル レポートの品質向上について、ご意見をお寄せください。doccomments@netapp.com

までお問い合わせください。件名に「TECHNICAL REPORT 4526」と添えてください。

バージョン履歴

バージョン	日付	ドキュメントの改訂履歴
バージョン1.0	2016年7月	Siddharth Agrawal：本テクニカルレポートの最初の一般公開版です。
バージョン2.0	2018年3月	Arpan Merchant: ONTAP 9.3のアップデート。

バージョン	日付	ドキュメントの改訂履歴
バージョン3.0	2021年5月	Jeannine Walter：ONTAP 9.9.1の更新
バージョン3.1	2021年9月	追加の更新が追加されました：保持とリストアが未指定です。
バージョン3.2	2021年12月	Jeannine Walter：ONTAP 9.10.1のアップデート。
バージョン3.3	2022年2月	Dan Tulledge：ONTAP 9.10.1に関する追加アップデート
バージョン3.4	2022年5月	Dan Tulledge：ONTAP 9.11.1のアップデート
バージョン3.5	2023年1月	Dan Tulledge：ONTAP 9.12.1のアップデート
バージョン3.6	2023年7月	ONTAP 9.13.1のDan Tulledgeアップデート

本ドキュメントに記載されている製品や機能のバージョンがお客様の環境でサポートされるかどうかについては、NetApp サポート サイトで Interoperability Matrix Tool (IMT)を参照してください。NetApp IMT には、NetApp がサポートする構成を構築するために使用できる製品コンポーネントやバージョンが定義されています。サポートの可否は、お客様の実際のインストール環境が公表されている仕様に従っているかどうかによって異なります。

機械翻訳に関する免責事項

原文は英語で作成されました。英語と日本語訳の間に不一致がある場合には、英語の内容が優先されます。公式な情報については、本資料の英語版を参照してください。翻訳によって生じた矛盾や不一致は、法令の順守や施行に対していかなる拘束力も法的な効力も持ちません。

著作権に関する情報

商標に関する情報

TR-4526-0123-JP

NetApp