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
December 20, 2024

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

SnapLockとは

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。

SnapLockは、SEC 17a-4（f）、HIPAA、FINRA、CFTC、GDPRなどの規制に準拠するために、データの削除、変更、名前変更を防止するのに役立ちます。SnapLockを使用すると、指定した保持期間または無期限のいずれかで、ファイルを消去および書き込み不可の状態で保存およびコミットできる専用ボリュームを作成できます。SnapLockでは、CIFSやNFSなどの標準オープンファイルプロトコルを使用して、ファイルレベルでこの保持を実行できます。SnapLockで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、ファイルやSnapshotコピーをWORMストレージにコミットし、WORMで保護されたデータの保持期間を設定できます。SnapLock WORMストレージでは、NetApp Snapshotテクノロジを使用し、SnapMirrorレプリケーションとSnapVaultバックアップをベーステクノロジとして活用して、データのバックアップリカバリ保護を実現できます。WORMストレージの詳細については、を参照してください"NetApp SnapLock - TR-4526を使用して準拠したWORMストレージを実現します"。

ファイルをWORM状態にコミットするには、アプリケーションを使用してNFSまたはCIFS経由でコミットできます。ファイルをWORM状態に自動的にコミットするには、SnapLockの自動コミット機能を使用します。追記可能 WORM ファイル _ を使用すると、ログ情報のように段階的に書き込まれるデータを保持できます。詳細については、を参照してください "ボリュームアペンドモードを使用して追記可能WORMファイルを作成する"。

SnapLockは、ほとんどのコンプライアンス要件を満たすデータ保護方法をサポートしています。

- SnapLock for SnapVaultを使用すると、セカンダリストレージ上のSnapshotコピーをWORM方式で保護できます。を参照して "SnapshotコピーのWORM状態へのコミット"
- SnapMirrorを使用すると、ディザスタリカバリ用に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。を参照して "WORMファイルのミラーリング"

SnapLockは、NetApp 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を厳格なコンプライアンスモードで使用してSECルール17a-4（f）などの外部の要件を満たし、より緩やかなエンタープライズモードで使用して、デジタル資産の保護に関する社内で義務付けられている規制を満たすことができます。SnapLockライセンスはソフトウェアスイートの一部"ONTAP One"です。

SnapLockは、すべてのAFFシステムとFASシステム、および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。SEC 17a-4（f）など、ハードウェアとソフトウェアの統合ソリューションを必要とする厳しいWORM規制には、この区別が重要です。詳細については、を参照してください "ブローカーへのSECガイダンス-電子記憶媒体の使用に関するディーラー"。

SnapLockの機能

SnapLockを設定したら、次のタスクを実行できます。

- "ファイルをWORM状態にコミット"
- "セカンダリストレージのSnapshotコピーをWORM状態にコミット"
- "ディザスタリカバリ用にWORMファイルをミラーリング"
- "訴訟時にリーガルホールドを使用してWORMファイルを保持"
- "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を設定する"
- "SnapLockボリュームを移動する"
- "Snapshotコピーをロックしてランサムウェア攻撃から保護"
- "監査ログを使用したSnapLockの使用状況の確認"
- "SnapLock APIの使用"

SnapLock Complianceモードとエンタープライズモード

SnapLock ComplianceモードとEnterpriseモードでは、主に各モードでWORMファイルが保護されるレベルが異なります。

SnapLock モード	保護レベル	保持中のWORMファイル削除
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は、監査対象の「privileged delete」手順を使用して削除できます。

保持期間の経過後、不要になったファイルはユーザが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、保持期間が過ぎたあとも変更することはできません。

保持期間中または保持期間後にWORMファイルを移動することはできません。WORMファイルはコピーできますが、コピーしたファイルのWORM特性は保持されません。

次の表に、SnapLock 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	○
ディスクの再初期化	いいえ	○
保持期間中のSnapLockアグリゲートおよびボリュームの削除	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	○
NetApp以外のディスクを使用する	いいえ	○（あり）"FlexArray仮想化"
監査ログにSnapLockボリュームを使用する	○	はい（ONTAP 9 .5以降）

SnapLockでサポートされる機能とサポートされない機能

次の表に、SnapLock Complianceモード、SnapLock Enterpriseモード、またはその両方でサポートされる機能を示します。

機能	SnapLock Complianceでサポートされます	SnapLock Enterpriseでサポートされます
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、ONTAP 9から始まります。2.詳細については、をご覧ください 暗号化とSnapLock。	はい、ONTAP 9から始まります。2.詳細については、をご覧ください 暗号化とSnapLock。
SnapLockアグリゲートでのFabricPoolの使用	いいえ	はい、ONTAP 9から始まります。8.詳細については、をご覧ください SnapLock Enterpriseアグリゲート上のFabricPool。
Flash Poolアグリゲート	はい、ONTAP 9 .1から始まります。	はい、ONTAP 9 .1から始まります。
FlexClone	SnapLockボリュームはクローニングできますが、SnapLockボリューム上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ボリューム上のファイルはクローニングできません。
FlexGroupホリユウム	はい、ONTAP 9 .11.1以降。詳細については、をご覧ください [flexgroup]。	はい、ONTAP 9 .11.1以降。詳細については、をご覧ください [flexgroup]。
LUN	いいえ。SnapLockの詳細については、こちらをご覧くださいLUNのサポート。	いいえ。SnapLockの詳細については、こちらをご覧くださいLUNのサポート。
MetroClusterコウセイ	はい、ONTAP 9から始まります。3.詳細については、をご覧ください MetroClusterのサポート。	はい、ONTAP 9から始まります。3.詳細については、をご覧ください MetroClusterのサポート。

マルチ管理者認証（MAV）	はい。ONTAP 9 13.1以降。詳細については、をご覧ください MAVサポート。	はい。ONTAP 9 13.1以降。詳細については、をご覧ください MAVサポート。
SAN	いいえ	いいえ
シングルファイルSnapRestore	いいえ	○
SnapMirrorアクティブ同期	いいえ	いいえ
SnapRestore	いいえ	○
SMTape	いいえ	いいえ
SnapMirror Synchronous	いいえ	いいえ
SSD	はい、ONTAP 9 .1から始まります。	はい、ONTAP 9 .1から始まります。
Storage Efficiency機能	○（ONTAP 9 .9.1以降）詳細については、をご覧ください Storage Efficiencyのサポート。	○（ONTAP 9 .9.1以降）詳細については、をご覧ください Storage Efficiencyのサポート。

SnapLock Enterpriseアグリゲート上のFabricPool

FabricPoolは、ONTAP 9以降のSnapLock Enterpriseアグリゲートでサポートされます。8.ただし、アカウントチームは、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データは、クラウド管理者が削除できるためSnapLockで保護されなくなったことを理解していることを記載した製品差異申請を行う必要があります。

FabricPoolが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するデータは、クラウド管理者が削除できるため、SnapLockで保護されなくなります。

FlexGroupボリュウム

SnapLockでは、ONTAP 9 .11.1以降で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、次の動作にも注意してください。

- 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。ルート以外のすべてのコンスティチュエントのVCCは、ルートVCCと密接に

同期されます。

- SnapLock構成プロパティは、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間や自動コミット期間など、異なる設定プロパティを設定することはできません。

LUNのサポート

SnapLockでは、SnapLock以外のボリュームで作成されたSnapshotコピーをSnapLockバックアップ関係の一部として保護するためにSnapLockに転送する場合にのみ、LUNがサポートされます。読み取り/書き込みSnapLockボリュームではLUNはサポートされません。ただし、改ざん防止Snapshotコピーは、SnapMirrorのソースボリュームと、LUNを含むデスティネーションボリュームの両方でサポートされます。

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以降では、ミラーされたアグリゲートでSnapLock Complianceがサポートされますが、アグリゲートを使用してSnapLock監査ログボリュームをホストする場合にのみサポートされます。
- SVM固有のSnapLock設定は、MetroClusterを使用してプライマリサイトとセカンダリサイトにレプリケートできます。

SnapLock Enterprise

- ONTAP 9以降では、SnapLock Enterpriseアグリゲートがサポートされます。
- 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。
- SVM固有のSnapLock設定は、MetroClusterを使用して両方のサイトに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を使用します。VCCおよび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、そのVCCはそのノードの現在のSCCの値で初期化されます。ボリュームの作成後は、ボリュームとファイルの保持期限が常にVCCで追跡されます。

ボリュームを別のサイトにレプリケートすると、そのVCCもレプリケートされます。たとえば、サイトAからサイトBへのボリュームのスイッチオーバーが発生した場合、VCCの更新はサイトBで継続され、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、ファイルの保持期間はSCCのクロックに依存せず、長くなりません。

Multi-Admin Verification（MAV）のサポート

ONTAP 9 .13.1以降では、クラスタ管理者が明示的にマルチ管理者検証を有効にして、一部のSnapLock処理を実行する前にクォーラムの承認が必要になるようにすることができます。MAVが有効な場合は、default-retention-time、minimum-retention-time、maximum-retention-time、volume-append-mode、自動コミット期間、privileged-deleteなどのSnapLockボリュームプロパティでクォーラムの承認が必要になります。詳細については、をご覧ください "MAV"。

Storage Efficiency

ONTAP 9 .9.1以降では、SnapLockでSnapLockおよびアグリゲートのデータコンパクション、ボリューム間重複排除、適応圧縮などのStorage Efficiency機能がサポートされます。Storage Efficiencyの詳細については、を参照してください"ONTAPのStorage Efficiencyの概要"。

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： * 認証キーが紛失した場合や、認証に失敗した回数が指定した制限を超えたためにドライブが永続的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 で保護された WORM ファイルを取得できるかどうかは、ネットアップでは保証できません。認証エラーが発生しないようにする責任はユーザにあります。

ONTAP 9 .2以降では、SnapLockアグリゲートで暗号化されたボリュームがサポートされます。

7-Modeからの移行

7-Mode Transition ToolのCopy-Based Transition（CBT）機能を使用して、SnapLockボリュームを7-ModeからONTAPにマイグレートできます。デスティネーションボリュームのSnapLockモード（ComplianceまたはEnterprise）がソースボリュームのSnapLockモードと一致している必要があります。コピーフリーの移行（CFT）を使用してSnapLockボリュームを移行することはできません。

SnapLockの設定

SnapLockの設定

SnapLockを使用する前に、SnapLockを設定する必要があります。たとえば、"SnapLockライセンスをインストールする"SnapLockボリュームを含むアグリゲートをホストするノードごとに、を初期化し"コンプライアンスクロック"、ONTAP 9 10.1より前のリリースのONTAPを実行するクラスタ用にSnapLockアグリゲートを作成します。"SnapLockボリュームの作成とマウント"

コンプライアンスクロックの初期化

SnapLockでは、_volumeコンプライアンスクロック_を使用して、改ざんによるWORMファイルの保持期間の変更を防止します。最初に、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、Snapshotコピーロックが有効になっているSnapLockボリュームがない場合やボリュームがない場合に、システムコンプライアンスクロックを初期化または再初期化できます。再初期化機能を使用すると、システム管理者は、システムコンプライアンスクロックが誤って初期化されたり、システムのクロックドリフトが修正されたりした場合に、システムコンプライアンスクロックをリセットできます。ONTAP 9 .13.1以前のリリースでは、ノードでコンプライアンスクロックを初期化すると、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手順は、次のとおりです。

- クラスタ内のすべてのノードが正常な状態である必要があります。
- すべてのボリュームがオンラインである必要があります。
- どのボリュームもリカバリキューに含めることができません。
- SnapLockボリュームが存在できません。
- Snapshotコピー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。
- "ノードにSnapLockライセンスがインストールされている必要があります。"です。

タスクの内容

システムのコンプライアンスクロックの時間は_volumeコンプライアンスクロック_に継承され、ボリューム上のWORMファイルの保持期間はボリューム側で制御されます。ボリュームコンプライアンスクロックは、新しいSnapLock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いています。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すると、ロックが有効なSnapLockボリュームまたは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。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、[Initialize SnapLock Compliance Clock*]をクリックします。
3. コンプライアンスクロック*列を表示してコンプライアンスクロックが初期化された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、のシステムコンプライアンスクロックを初期化し `node1`ます。

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

2. プロンプトが表示されたら、システムクロックが正しいこと、およびコンプライアンスクロックを初期化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ノードごとに、この手順を繰り返します。

NTPが設定されたシステムでコンプライアンスクロックの再同期を有効にする

サーバが設定されている場合は、SnapLock Complianceクロック時間同期機能をイネーブルにできます。

必要なもの

- 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。
- "ノードにSnapLockライセンスがインストールされている必要があります。"です。
- この機能は、Cloud Volumes ONTAP、ONTAP Select、vsimの各プラットフォームでのみ使用できます。

タスクの内容

SnapLockセキュアクロックデーモンがしきい値を超えたスキューを検出すると、ONTAPはシステム時間を使

用してシステムクロックとボリュームコンプライアンスクロックの両方をリセットします。スキューしきい値として24時間の期間が設定されています。つまり、スキューが1日以上経過した場合にのみ、システムコンプライアンスクロックがシステムクロックに同期されます。

SnapLockセキュアクロックデーモンはスキューを検出し、コンプライアンスクロックをシステム時間に変更します。コンプライアンスクロックはシステム時間がNTP時間と同期されている場合にのみシステム時間と同期されるため、コンプライアンスクロックを強制的にシステム時間に変更しようとすると失敗します。

手順

1. サーバが設定されている場合は、SnapLock Complianceクロック時刻同期機能をイネーブルにします。

   snaplock compliance-clock ntp

   次のコマンドは、システムコンプライアンスクロック時間同期機能を有効にします。

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

2. プロンプトが表示されたら、設定したNTPサーバが信頼できること、および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、システムのコンプライアンス クロック時間同期機能が有効になっていることを確認します。

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

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

SnapLockアグリゲートを作成する

volumeオプションを使用 `-snaplock-type`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より前のリリースでは、独立した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SnapLock以外のボリュームを同じアグリゲート上に配置できます。そのため、ONTAP 9 .10.1を使用している場合は、SnapLockアグリゲートを別途作成する必要はありません。

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。
- "ライセンスをインストールする必要があります"ノードのSnapLock。このライセンスはに含まれて い"ONTAP One"ます。
- "ノード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"です。

- ディスクを「 root 」、「 data1 」、および「 d ata2 」としてパーティショニングした場合、スペアディスクが利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アグリゲートとSnapLock以外のアグリゲートは、SnapLockボリュームとSnapLock以外の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る新しいSnapLockボリュームのデフォルト値は、SnapLock以外のボリュームと同じです。また、新しいボリュームおよびアグリゲートのデフォルト値はプラットフォームによって異なります。

リバートに関する考慮事項

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

タスクの内容

- FlexArray LUN用にComplianceアグリゲートを作成することはできませんが、SnapLock ComplianceアグリゲートはFlexArray LUNでサポートされています。
- SyncMirrorオプションを使用して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構成で作成できるのは、そのアグリゲートを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>
```

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

次のコマンドでは、3本のディスクを含む `node1`という名前のSnapLockアグリゲートが `aggr1`作成され`Compliance`ます。

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

SnapLockボリュームの作成とマウント

WORM状態にコミットするファイルまたはSnapshotコピー用に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、アグリゲートタイプに関係なく、

作成するすべてのボリュームがデフォルトでSnapLock以外のボリュームとして作成されます。SnapLockタイプとしてComplianceまたはEnterpriseを指定してSnapLockボリュームを明示的に作成するには、オプションを使用する必要があります `-snaplock -type`。デフォルトでは、SnapLockタイプはに設定されてい `non-snaplock`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。
- そうするべきだ"SnapLockライセンスがインストールされていることの確認"ノードにSnapLockライセンスがインストールされていない場合は"インストール"、ライセンスが必要です。このライセンスはに含まれてい"ONTAP One"ます。ONTAP Oneよりも前のリリースでは、SnapLockライセンスはSecurity and Compliance Bundleに含まれていました。Security and Compliance Bundleの提供は終了しましたが、引き続き有効です。現在は必須ではありませんが、既存のお客様は選択できます"ONTAP Oneへのアップグレード"。
- "ノード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"です。

タスクの内容

適切なSnapLock権限があれば、エンタープライズボリュームの削除や名前変更はいつでも実行できます。Complianceボリュームは保持期間が経過するまで削除できません。Complianceボリュームの名前は変更できません。

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

> SnapLockボリュームではLUNはサポートされません。SnapLockでは、SnapLock以外のボリュームで作成されたSnapshotコピーをSnapLockバックアップ関係の一部として保護するためにSnapLockに転送する場合にのみ、LUNがサポートされます。読み取り/書き込みSnapLockボリュームではLUNはサポートされません。ただし、改ざん防止Snapshotコピーは、SnapMirrorのソースボリュームと、LUNを含むデスティネーションボリュームの両方でサポートされます。

このタスクは、ONTAPシステムマネージャまたは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. [*Storage]>[Volumes]に移動し、[*Add]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. ボリュームの名前とサイズなど、新しいボリューム情報を入力します。
4. 「* SnapLock を有効にする*」を選択し、SnapLock タイプとして「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、ファイルが自動的にコミットされるまでに変更されないようにする時間を入力します。最小値は5分、最大値は10年です。
6. [*データ保持期間]セクションで、最小保持期間と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（ Save ）] をクリックします。
9. [* Volumes]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>
```

すべてのオプションの一覧については、コマンドのマニュアルページを参照してください。SnapLockボリュームには、、 `-atime-update` `-is-autobalance-eligible`、、 `-space-mgmt-try-first`および `vmalign`使用できません `-nvfail`。

次のコマンドは、 `aggr1`on `vs1`という名前のSnapLockボリュームを `vol1`作成し `Compliance`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できます。

必要なもの

SnapLockボリュームはオンラインである必要があります。

タスクの内容

- SnapLockボリュームはSVMのルートにのみマウントできます。
- 通常のボリュームをSnapLockボリュームの下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*

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

   次のコマンドは、という名前のSnapLockをネームスペースの `vs1`ジャンクションパスに `/sales`マウントし `vol1`ます。

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

保持期限を設定する

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かぎり、SnapLockではデフォルトの保持期間を使用して保持期限が計算されます。イベント発生後にファイルの保持期間を設定することもできます。

ホシキカントホシキケンニツイテ

WORM ファイルの *retention period* は、 WORM 状態にコミットされたファイルを保持する必要がある期間を指定します。WORM ファイルの _ retention time_ は、その時点までファイルを保持する必要がなくなった時間です。たとえば、2020年11月10日の午前6時にWORM状態にコミットされたファイルの保持期間を20年とすると、保持期限は2040年11月10日の午前6時になります。

ONTAP 9 .10.1以降では、保持期限を3058年10月26日まで、保持期間を100年まで設定できます。保持期限を延長すると、古いポリシーが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infiniteに設定しないかぎり、サポートされる最大保持期間は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

2071年1月19日（GMT）よりもあとの保持期限を使用して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。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「 January 19 、 2071 8:44:07 AM 」よりもあとのファイルがある場合、 ONTAP 9.10.1 から以前の ONTAP バージョンにクラスタを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Enterpriseボリュームには、次の4つの保持期間があります。

- 最小保持期間(`min`）（デフォルトは0）
- 最大保持期間(`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となります。 `min`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、デフォルトはと同じです `max`。
  - エンタープライズモードの場合、デフォルトはと同じです `min`。
- 未指定の保持期間。

  ONTAP 9 .8以降では、ボリューム内のファイルの保持期間をに設定して、絶対的な保持期限を設定するまでファイルが保持されるようにすることができ `unspecified`ます。絶対保持期間が設定されたファイルの保持期間を未指定に設定し、再度絶対保持期間に設定することができます。ただし、新しい保持期間が以前に設定した絶対保持期間よりもあとである必要があります。

  ONTAP 9 12.1以降では、保持期間がに設定されたWORMファイルの `unspecified`保持期間は、SnapLockボリュームに設定された最小保持期間に設定されます。ファイルの保持期間をから絶対的な保持期間に変更する場合 `unspecified`は、ファイルにすでに設定されている最小保持期間よりも長い新しい保持期間を指定する必要があります。

そのため、Complianceモードのファイルを WORM状態にコミットする前に保持期限を明示的に設定していない場合、デフォルトを変更しないとファイルが30年間保持されます。同様に、Enterpriseモードのファイルを WORM状態にコミットする前に保持期限を明示的に設定していない場合、デフォルトを変更しないとファイルの保持期間は0年になります。つまり、ファイルは保持されなくなります。

デフォルトの保持期間を設定する

コマンドを使用して、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できます `volume snaplock modify`。

必要なもの

SnapLockボリュームはオンラインである必要があります。

タスクの内容

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。

値	単位	脚注
0 ~ 65535	秒	
0 ~ 24	時間	

値	単位	脚注
0 ~ 365	日	
0 ~ 12	月	
0 ~ 100	年	ONTAP 9 .10.1以降。以前のONTAPリリースでは、値は0~70です。
最大	-	最大保持期間を使用します。
最小	-	最小保持期間を使用します。
インフィニット	-	ファイルを無期限に保持します。
未指定	-	絶対的な保持期間が設定されるまでファイルを保持します。

最大保持期間と最小保持期間の値と範囲は同じですが、と `min`は `max`該当しません。このタスクの詳細については、を参照してください"保持期間の概要の設定"。

コマンドを使用して、ボリュームの保持期間の設定を表示できます `volume snaplock show`。詳細については、コマンドのマニュアルページを参照してください。

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*

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

   次の例は、最小保持期間と最大保持期間が以前に変更されていないことを前提としています。

   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
```

ファイルの保持期限を明示的に設定する

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。最終アクセス日時は、NFSまたはCIFS経由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。

タスクの内容

ファイルがWORM状態にコミットされたあとは、保持期限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。保持期限は、ファイルのフィールドに保存され `atime`ます。

ファイルの保持期限をに明示的に設定することはできません `infinite`。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日時を変更します。

   UNIXシェルで、次のコマンドを使用して、という名前のファイルの保持期限を2020年11月21日午前6時に設定し `document.txt`ます。

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

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間を変更できます。

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 のイベントベースの保持（EBR）機能を使用して、イベントの発生後にファイルを保持する期間を定義できます。

必要なもの

- このタスクを実行するには、SnapLock管理者である必要があります。

  "SnapLock管理者アカウントの作成"

- セキュアな接続（SSH、コンソール、またはZAPI）でログインしておく必要があります。

タスクの内容

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、単一のファイルに適用することも、ディレクトリ内のすべてのファイルに適用することもできます。

- WORMファイルでないファイルは、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、リーガルホールドの対象となる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、を参照してください"NetApp SnapLock を使用して WORM ストレージに準拠"。

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、従業員が源泉徴収票を変更した後、3年間、従業員のW-4レコードを変更されていない形式で保持することが会社のポリシーである可能性があります。別の企業ポリシーでは、従業員が解雇された後、W-4レコードを5年間保持することが義務付けられている場合があります。 その場合は、保持期間を5年に設定したEBRポリシーを作成できます。従業員が退職した後（「イベント」）、 EBR ポリシーを従業員の W-4 レコードに適用すると、保持期間が延長されます。これは通常、保持期間を手動で延長するよりも簡単です。特に、多数のファイルが含まれている場合に便利です。

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、保持期間が10年のEBRポリシーをに `vs1`作成し `employee_exit`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`、ディレクトリ内のすべてのファイルに `d1`EBRポリシーを適用し `employee_exit` ます。

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

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、SnapLockアグリゲートを作成してから、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する必要があります。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が記録されます。

ONTAP 9 .10.1以降では、SnapLockアグリゲートの作成は廃止されました。SnapLock "SnapLockボリュームの明示的な作成" SnapLockタイプとしてComplianceまたはEnterpriseのいずれかを指定して、に-replace-typeオプションを使用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は、クラスタ管理者でSnapLockアグリゲートを作成する必要があります。

タスクの内容

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 ComplianceモードとEnterpriseモードの両方に当てはまります。

> ONTAP 9 .4以前では、SnapLock Enterpriseボリュームを監査ログに使用できません。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にマウントする必要があります `/snaplock_audit_log`。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の下のディレクトリのサブディレクトリ（privileged delete処理）および `system_log`（それ以外のすべて）に `privdel_log`あり `/snaplock_log`ます。監査ログのファイル名には最初にログに記録された処理のタイムスタンプが含まれているため、処理が実行されたおおよ

その時間で簡単にレコードを検索できます。

- コマンドを使用すると、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 show`。
- 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て新しいログファイルを作成できます `snaplock log file archive`。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。

詳細については、コマンドのマニュアルページを参照してください。

データ保護ボリュームをSnapLock監査ログボリュームとして使用することはできません。

手順

1. SnapLockアグリゲートを作成します。

   SnapLockアグリゲートを作成する

2. 監査ログを設定するSVMで、SnapLockボリュームを作成します。

   SnapLockボリュームを作成する

3. SVMの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カ月です。該当す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、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、privileged deleteを使用して削除されたファイルの保持期間が10カ月で、監査ログの保持期間が8カ月の場合、ログの保持期間は10カ月に延長されます。保持期間とデフォルトの保持期間の詳細については、を参照してください"保持期限を設定する"。

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

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

4. 監査ログを設定したSVMで、ジャンクションパスにSnapLockボリュームをマウントします `/snaplock_audit_log`。

   SnapLockボリュームのマウント

SnapLock設定の確認

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、追記可能WORM）、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 `volume file fingerprint start。

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.
   ```

   コマンドを実行すると、コマンドの入力として使用できるSession IDが生成され `volume file fingerprint dump`ます。

   > コマンドでSession IDを指定すると、フィンガープリント処理の進捗状況を監視できます `volume file fingerprint show`。フィンガープリントを表示する前に、処理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ファイルを管理します。

WORMファイルを管理します。

WORMファイルは次の方法で管理できます。

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

ファイルを**WORM**状態にコミット

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

ファイルを**WORM**状態に手動でコミット

ファイルを手動でWORM状態にコミットするには、ファイルを読み取り専用にします。ファイルの読み取り/書き込み属性は、NFSまたはCIFSで適切なコマンドやプログラムを使用して読み取り専用に変更できます。ファイルの書き込みが完了してファイルが途中でコミットされないようにする場合や、ボリューム数が多いために自動コミットスキャナの拡張に問題がある場合は、ファイルを手動でコミットすることを選択できます。

必要なもの

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

タスクの内容

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

手順

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

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

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

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

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

ファイルを**WORM**状態に自動的にコミット

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

必要なもの

- 自動コミットするファイルがSnapLockボリューム上に存在している必要があります。
- SnapLockボリュームはオンラインである必要があります。
- SnapLockボリュームは読み書き可能ボリュームである必要があります。

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

タスクの内容

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

自動コミット期間に指定できる値は次のとおりです。

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

最小値は5分、最大値は10年です。

手順

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

   volume snaplock modify -vserver *SVM_name* -volume *volume_name* -autocommit -period *autocommit_period*

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

   次のコマンドは、5時間変更がないかぎり、SVM vs1のボリューム上のファイルを自動コミットし `vol1`ます。

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

追記可能**WORM**ファイルの作成

追記可能WORMファイルには、ログエントリと同様に段階的に書き込まれたデータが保持されます。追記可能 WORM ファイルは、適切なコマンドやプログラムを使用して作成するか、 SnapLock のボリュームアペンドモード機能を使用してデフォルトで作成できます。

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

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

必要なもの

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

タスクの内容

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

現在アクティブな256KBチャンクを超える順序付けされていない書き込みは、アクティブな256KBチャンクが最新のオフセットにリセットされ、古いオフセットへの書き込みが「読み取り専用ファイルシステム（ROFS）」エラーで失敗します。書き込みオフセットは、クライアントアプリケーションによって異なります。追記可能WORMファイル書き込みセマンティクスに準拠していないクライアントが原因で、書き込み内容が誤って終了する可能性があります。したがって、順序付けされていない書き込みのオフセット制限に従うか、ファイルシステムを同期モードでマウントして同期書き込みを確保することを推奨します。

手順

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

   UNIXシェルで、次のコマンドを使用して、という名前のゼロ長ファイルに保持期限を2020年11月21日午前6時に設定し `document.txt`ます。

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

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

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

   ```
   chmod 444 document.txt
   ```

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

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

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

```
chmod 777 document.txt
```

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

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

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

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

ボリュームアペンドモードを使用して追記可能**WORM**ファイルを作成する

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

必要なもの

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

タスクの内容

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

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

VAMはSnapLock監査ログボリュームではサポートされません。

手順

1. VAMを有効にします。

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

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

   次のコマンドは、SVM`vs1`のボリュームでVAMを有効にし `vol1`ます。

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

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

   ファイルはデフォルトで追記可能WORMです。

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

SnapLock for SnapVaultを使用すると、セカンダリストレージ上のSnapshotをWORM方式で保護できます。SnapLockの基本タスクはすべてSnapVaultデスティネーションで実行します。デスティネーションボリュームは自動的に読み取り専用でマウントされるため、SnapshotをWORM状態に明示的にコミットする必要はありません。

開始する前に

- System Managerを使用して関係を設定する場合は、ソースとデスティネーションの両方のクラスタでONTAP 9.15.1以降が実行されている必要があります。
- デスティネーション クラスタ：
  - "SnapLock ライセンスをインストール"です。
  - "コンプライアンスクロックの初期化"です。
  - 9.10.1より前のONTAPリリースでCLIを使用している場合は、"SnapLockアグリゲートを作成する"
- 保護ポリシーのタイプは「vault」である必要があります。
- ソースアグリゲートとデスティネーションアグリゲートは64ビットである必要があります。
- ソースボリュームをSnapLockボリュームにすることはできません。
- ONTAP CLIを使用している場合は、およびにソースボリュームとデスティネーションボリュームを作成する必要があります"ピアリングクラスタ""SVM"。

タスクの内容

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

WORM状態にコミットされたSnapshotの名前は変更できません。

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

SnapLockボリュームではLUNはサポートされません。SnapLockでは、SnapLock以外のボリュームで作成されたSnapshotをSnapLockバックアップ関係の一部として保護するためにSnapLockに転送する場合にのみ、LUNがサポートされます。読み取り/書き込みSnapLockボリュームではLUNはサポートされません。ただし、改ざん防止Snapshotは、SnapMirrorのソースボリュームと、LUNを含むデスティネーションボリュームの両方でサポートされます。

ONTAP 9 .10.1以降では、SnapLockボリュームとSnapLock以外のボリュームを同じアグリゲート上に配置で

きます。そのため、ONTAP 9 .10.1を使用している場合は、SnapLockアグリゲートを別途作成する必要はありません。Compliance SnapLockまたはEnterprise SnapLockのボリュームタイプを指定するには、ボリューム「-Enterprise-type」オプションを使用します。ONTAP 9 10.1より前のONTAPリリースでは、SnapLockモード（ComplianceまたはEnterprise）がアグリゲートから継承されます。バージョンに依存しないデスティネーションボリュームはサポートされません。デスティネーションボリュームの言語設定は、ソースボリュームの言語設定と一致している必要があります。

バックアップデスティネーションであるSnapLockには、デフォルトの保持期間が割り当てられています。この期間の最初の値は、SnapLock Enterpriseボリュームの場合は最小0年、SnapLock Complianceボリュームの場合は最大30年です。各NetApp Snapshotは、最初はこのデフォルトの保持期間でコミットされます。保持期間は、必要に応じてあとから延長できます。詳細については、を参照してください "保持期限の設定の概要を確認します"。

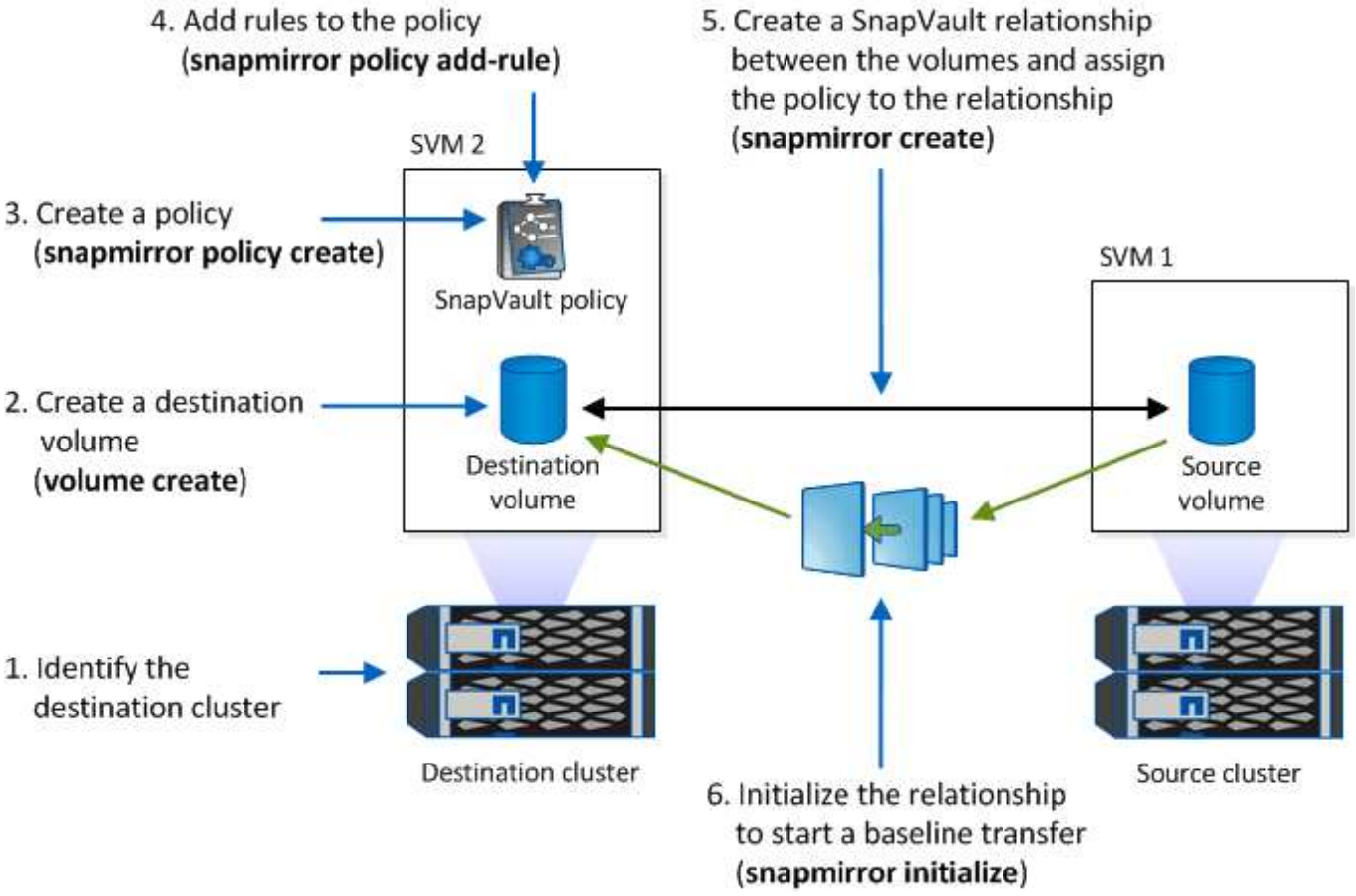
ONTAP 9.14.1以降では、SnapMirror関係のSnapMirrorポリシーに特定のSnapMirrorラベルの保持期間を指定できます。これにより、ソースボリュームからデスティネーションボリュームにレプリケートされたSnapshotが、ルールで指定された保持期間に保持されます。保持期間を指定しない場合は、デスティネーションボリュームのデフォルトの保持期間が使用されます。

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

MetroCluster構成の場合は、次の点に注意してください。

- SnapVault関係は同期元のSVM間でのみ作成でき、同期元のSVMと同期先のSVM間では作成できません。
- 同期元のSVMのボリュームからデータ提供用のSVMへのSnapVault関係を作成できます。
- データ提供用のSVMから同期元のSVMのDPボリュームへのSnapVault関係を作成できます。

次の図は、SnapLockバックアップ関係を初期化する手順を示しています。



手順

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

System Manager

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

CLI

1. デスティネーションクラスタで、ソースボリュームと同じサイズ以上のタイプのSnapLockデスティネーションボリュームを作成し `DP`ます。

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

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

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

2. デスティネーションクラスタで、"デフォルトの保持期間を設定する"を実行します。
3. "新しいレプリケーション関係を作成"SnapLock以外のソースと作成した新しいSnapLockデスティネーション間。

この例では、ポリシーを使用して、dailyおよびweeklyというラベルのSnapshotを毎時スケジュールでバックアップするように、 `XDPDefault`デスティネーションSnapLockボリュームとの新しいSnapMirror関係を作成し `dstvolB`ます。

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

"カスタムレプリケーションポリシーを作成します。"または"カスタムスケジュール"、使用可能なデフォルト値が適切でない場合に使用します。

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

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

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

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

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

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

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

関連情報

"クラスタとSVMのピアリング"

"SnapVaultによるボリュームのバックアップ"

ディザスタリカバリ用に**WORM**ファイルをミラーリング

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

前提条件

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

タスクの内容

- .5以降では、ONTAP 9（データ保護）タイプの関係ではなくXDP（拡張データ保護）タイプのSnapMirror関係を使用してWORMファイルをレプリケートできます。XDPモードはONTAPのバージョンに依存せず、同じブロックに格納されているファイルを区別できるため、レプリケートされたComplianceモードのボリュームの再同期がはるかに簡単になります。既存のDPタイプの関係をXDPタイプの関係に変換する方法については、を参照してください"データ保護"。
- ComplianceモードのボリュームでDPタイプのSnapMirror関係を再同期する場合、再同期によってデータが失われるとSnapLockで判断されると処理は失敗します。再同期処理に失敗した場合は、コマンドを使用してデスティネーションボリュームのクローンを作成でき `volume clone create`ます。その後、ソースボリュームとクローンを再同期できます。

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

  再同期では、共通のSnapshotを超えてソースとデスティネーションの間でデータの相違が検出されると、この相違をキャプチャするためにデスティネーションで新しいSnapshotがカットされます。新しいSnapshotと共通のSnapshotの両方が次の保持期間でロックされます。

  - デスティネーションのボリューム有効期限
  - ボリューム有効期限が過ぎているか設定されていない場合、Snapshotは30日間ロックされます。
  - デスティネーションにリーガルホールドが設定されている場合、実際のボリューム有効期限はマスクされて「無期限」と表示されますが、Snapshotは実際のボリューム有効期限内はロックされます。

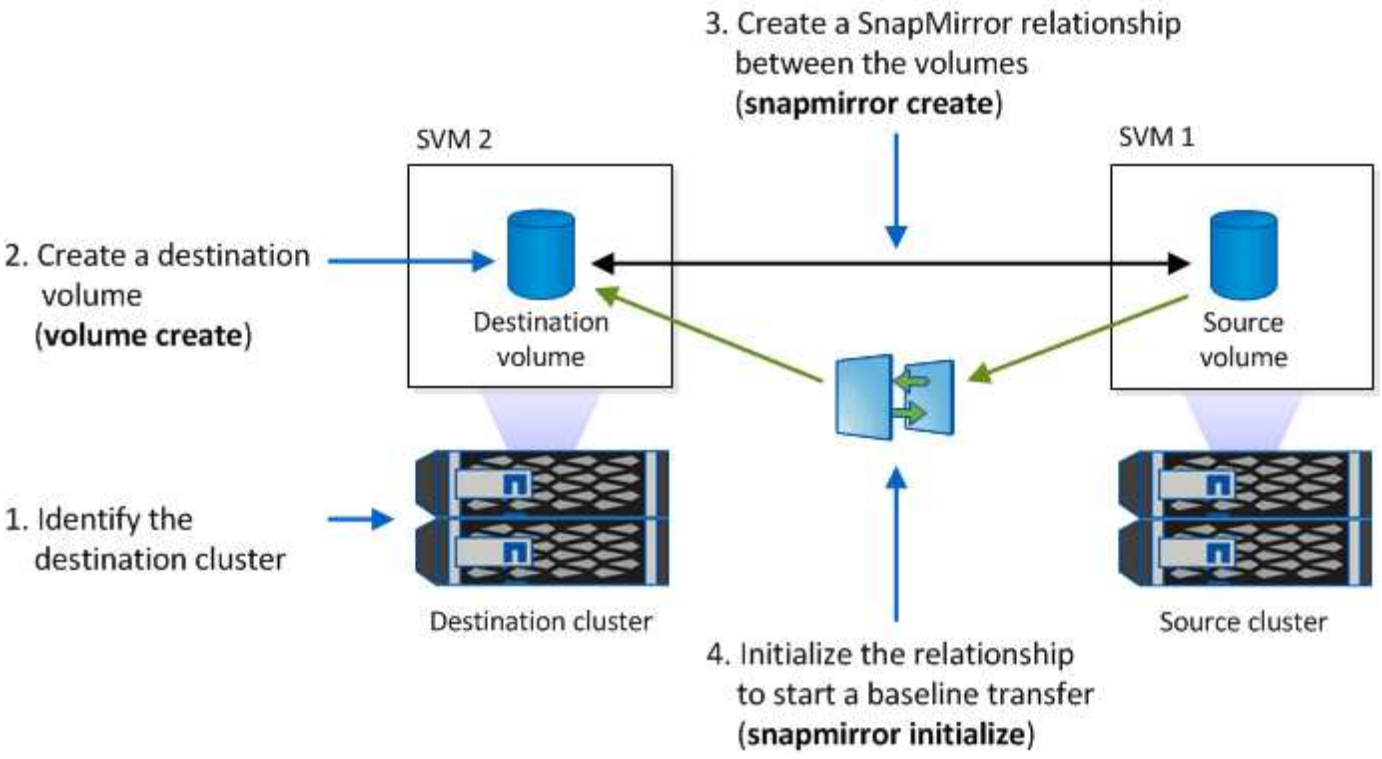
デスティネーションボリュームの有効期限がソースよりもあとの場合、デスティネーションの有効期限が保持され、再同期後にソースボリュームの有効期限で上書きされることはありません。

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

異なるデータをキャプチャするために作成されたデスティネーションボリューム上のロックされたSnapshotコピーは、CLIでコマンドを実行してソースにコピーできます `snapmirror update -s snapshot`。コピーされたSnapshotは、ソースでも引き続きロックされます。

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

次の図は、SnapMirror関係を初期化する手順を示しています。



System Manager

ONTAP 9 .12.1以降では、System Managerを使用してWORMファイルのSnapMirrorレプリケーションを設定できます。

手順

1. [ストレージ]>[ボリューム]に移動します。
2. 表示/非表示*をクリックし、 SnapLock タイプ*を選択して、*ボリューム*ウィンドウに列を表示します。
3. SnapLockボリュームを探します。
4. をクリックし、*[保護]*を選択します。
5. デスティネーションクラスタとデスティネーションStorage VMを選択
6. [* その他のオプション *] をクリックします。
7. [Show legacy policies*]を選択し、[**DPDefault (legacy)**]を選択します。
8. 「接続先設定の詳細」セクションで「転送スケジュールの上書き」を選択し、「*時間単位」を選択します。
9. [保存（ Save ）] をクリックします。
10. ソースボリューム名の左側にある矢印をクリックしてボリュームの詳細を展開し、ページの右側でリモートSnapMirror保護の詳細を確認します。
11. リモートクラスタで、「保護関係」に移動します。
12. 関係を検索し、デスティネーションボリューム名をクリックして関係の詳細を表示します。
13. デスティネーションボリュームのSnapLockタイプやその他のSnapLock情報を確認します。

CLI

1. デスティネーションクラスタを特定
2. デスティネーションクラスタ、"SnapLockライセンスをインストールする"、"コンプライアンスクロックの初期化"、および9.10.1より前のONTAPリリースを使用している場合は、"SnapLockアグリゲートを作成する"。
3. デスティネーションクラスタで、ソースボリュームと同じサイズ以上のSnapLockデスティネーションボリュームを作成し `DP`ます。

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

> ONTAP 9 .10.1以降では、SnapLockボリュームとSnapLock以外のボリュームを同じアグリゲート上に配置できます。そのため、ONTAP 9 .10.1を使用している場合は、SnapLockアグリゲートを別途作成する必要はありません。ComplianceまたはEnterprise SnapLockのボリュームタイプを指定するには、volume SnapLock -typeオプションを使用します。ONTAP 9 10.1より前のONTAPリリースでは、SnapLockモード（ComplianceまたはEnterprise）がアグリゲートから継承されます。バージョンに依存しないデスティネーションボリュームはサポートされません。デスティネーションボリュームの言語設定は、ソースボリュームの言語設定と一致している必要があります。

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

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

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

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

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

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

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

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

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

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

6. デスティネーションSVMで、SnapMirror関係を作成します。

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

   次のコマンドでは、の `SVM1`ソースボリュームとの `SVM2`デスティネーションボリューム `dstvolB`の間にSnapMirror関係を作成し `srcvolA`、ポリシーとスケジュールを `weekendcron`割り当て `SVM1-mirror`ます。

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

   XDPタイプはONTAP 9 .5以降で使用できます。ONTAP 9 .4以前ではDPタイプを使用する必要があります。

7. デスティネーションSVMで、SnapMirror関係を初期化します。

   snapmirror initialize -destination-path *destination_path*

   初期化プロセスでは、デスティネーションボリュームへの _ ベースライン転送 _ が実行されま

す。SnapMirrorはソースボリュームのSnapshotコピーを作成して、そのコピーおよびコピーが参照するすべてのデータブロックをデスティネーションボリュームに転送します。また、ソースボリューム上のその他のSnapshotコピーもデスティネーションボリュームに転送します。

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

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

関連情報

"クラスタとSVMのピアリング"

"ボリュームのディザスタリカバリの準備"

"データ保護"

訴訟時にリーガルホールドを使用して**WORM**ファイルを保持

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

開始する前に

- このタスクを実行するには、SnapLock管理者である必要があります。

  "SnapLock管理者アカウントの作成"

- セキュアな接続（SSH、コンソール、またはZAPI）でログインしておく必要があります。

タスクの内容

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

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

手順

1. リーガルホールドを開始します。

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

   次のコマンドは、のすべてのファイルに対してリーガルホールドを開始し `vol1`ます。

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

2. リーガルホールドの終了：

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

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

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

WORMファイルの削除の概要

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

SnapLock管理者アカウントの作成

privileged deleteを実行するには、SnapLock管理者Privilegesが必要です。これらのPrivilegesは、SnapLockロールで定義されます。このロールが割り当てられていない場合は、クラスタ管理者に依頼して、 SnapLock 管理者ロールを持つ SVM 管理者アカウントを作成してもらいます。

必要なもの

- このタスクを実行するには、クラスタ管理者である必要があります。
- セキュアな接続（SSH、コンソール、またはZAPI）でログインしておく必要があります。

手順

1. SnapLock管理者ロールを持つSVM管理者アカウントを作成します。

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

   次のコマンドは、事前定義されたロールが割り当てられた `vsadmin-snaplock`SVM管理者アカウントにパスワードを使用したアクセスを `SVM1`許可し `SnapLockAdmin`ます。

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

privileged delete機能を有効にする

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

タスクの内容

オプションの値 `-privileged-delete`によって、`privileged delete`が有効かどうかが決まります。指

定できる値は `enabled、 disabled、および `permanently-disabled`です。

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

手順

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

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

   次のコマンドは、の `SVM1`Enterpriseボリュームに対してprivileged delete機能を有効にし `dataVol`ます。

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

EnterpriseモードのWORMファイルの削除

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

必要なもの

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

タスクの内容

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

ステップ

1. EnterpriseボリュームのWORMファイルを削除します。

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

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

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

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（エンタープライズからエンタープライズ、コンプライアンスからコンプライアンス）に移動できます。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を作成する

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Privilegesが必要です。この権限は、 ONTAP 9.8 で導入された _ SnapLock _ ロールで付与されます。このロールが割り当てられていない場合は、クラスタ管理者に依頼して、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の作成を依頼できます。

必要なもの

- このタスクを実行するには、クラスタ管理者である必要があります。
- セキュアな接続（SSH、コンソール、またはZAPI）でログインしておく必要があります。

タスクの内容

SnapLockロールは管理SVMに関連付けられますが、vsadmin-SVM SnapLockロールはデータSVMに関連付けられます。

ステップ

1. SnapLock管理者ロールを持つSVM管理者アカウントを作成します。

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

   次のコマンドは、事前定義のロールが割り当てられた `snaplock`SVM管理者アカウントが、パスワードを使用した管理SVMへのアクセスを `cluster1`許可し `SnapLockAdmin`ます。

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

SnapLockボリュームを移動する

コマンドを使用すると、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 `volume move`。

必要なもの

- 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。

  "監査ログを作成する"です。

- ONTAP 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と同じである必要があります（ComplianceからComplianceへ、またはEnterpriseからEnterpriseへ）。ONTAP 9 .10.1以降では、この制限が解除され、アグリゲートにComplianceボリュームとEnterprise SnapLockボリュームの両方を含めることができるようになりました。また、SnapLock以外のボリュームも含めることができます。
- SnapLockのセキュリティロールを持つユーザである必要があります。

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
   ```

Snapshotコピーをロックしてランサムウェア攻撃から保護

ONTAP 9 12.1以降では、SnapLock以外のボリュームにSnapshotコピーをロックして、ランサムウェア攻撃から保護できます。Snapshotコピーをロックすることで、誤って削除したり悪意を持って削除したりすることがなくなります。

SnapLock Complianceクロック機能を使用すると、Snapshotコピーを指定した期間ロックして、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。Snapshotコピーをロックすると改ざんが防止され、ランサムウェアの脅威から保護されます。ロックされたSnapshotコピーを使用して、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にデータをリカバリできます。

ONTAP 9 14.1以降では、Snapshotコピーロックで、SnapLockヴォールトデスティネーションおよびSnapLock SnapMirror以外のデスティネーションボリュームでのSnapshotコピーの長期保持がサポートされます。Snapshotコピーロックを有効にするには、に関連付けられたSnapMirrorポリシールールを使用して保持期間を設定し既存のポリシーラベルます。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持期間よりも優先されます。SnapMirrorラベルに保持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持期間が使用されます。

Snapshotコピーの改ざん防止の要件と考慮事項

- 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ライセンスがクラスタにインストールされている必要があります。"です。このライセンスはに含まれてい"ONTAP One"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ります。"です。
- ボリュームでSnapshotロックが有効になっている場合は、クラスタをONTAP 9より新しいバージョン

のONTAPにアップグレードできます。12.1ただし、ロックされたすべてのSnapshotコピーが有効期限に達して削除され、Snapshotコピーロックが無効になるまで、ONTAPを以前のバージョンにリバートすることはできません。

- Snapshotがロックされている場合、ボリューム有効時間はSnapshotコピーの有効期限に設定されます。複数のSnapshotコピーがロックされている場合、ボリューム有効期限はすべてのSnapshotコピーの最大有効期限を反映します。
- ロックされたSnapshotコピーの保持期間はSnapshotコピーの保持数よりも優先されます。つまり、ロックされたSnapshotコピーのSnapshotコピーの保持期間が経過していない場合、保持数の制限は適用されません。
- SnapMirror関係では、ミラーバックアップポリシールールに保持期間を設定できます。デスティネーションボリュームでSnapshotコピーロックが有効になっている場合は、デスティネーションにレプリケートされたSnapshotコピー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、保持数を超えていても、有効期限を過ぎていないSnapshotコピーは保持されます。
- SnapLock以外のボリューム上のSnapshotコピーの名前は変更できます。SnapMirror関係のプライマリボリュームでのSnapshot名変更処理は、ポリシーがMirrorAllSnapshotsの場合にのみセカンダリボリュームに反映されます。それ以外のポリシータイプの場合、名前を変更したSnapshotコピーは更新時に伝播されません。
- ONTAP CLIを使用している場合は、ロックされたSnapshotコピーが最新のものである場合にのみ、コマンドを使用してロックされたSnapshotコピーをリストアでき `volume snapshot restore`ます。リストア対象のSnapshotコピーよりもあとのSnapshotコピーがある場合、Snapshotコピーのリストア処理は失敗します。

改ざん防止**Snapshot**コピーでサポートされる機能

- "Cloud Volumes ONTAP"
- FlexGroupホリユウム

  SnapshotコピーロックはFlexGroupボリュームでサポートされます。Snapshotロックは、ルートコンスティチュエントのSnapshotコピーに対してのみ実行されます。FlexGroupボリュームを削除できるのは、ルートコンスティチュエントの有効期限が過ぎている場合のみです。

- FlexVolからFlexGroupへの変換

  ロックされたSnapshotコピーがあるFlexVol volumeをFlexGroupボリュームに変換できます。変換後もSnapshotコピーはロックされたままです。

- ボリューム クローンとファイル クローン

  ロックされたSnapshotコピーからボリューム クローンとファイル クローンを作成できます。

サポートされない機能

現在、改ざん防止Snapshotコピーでは、次の機能はサポートされていません。

- 整合グループ
- FabricPool
- FlexCacheホリユウム
- SMTape
- SnapMirrorアクティブ同期

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

ボリューム作成時に**Snapshot**コピーロックを有効にする

ONTAP 9 12.1以降では、新しいボリュームを作成するとき、またはCLIのコマンドと `volume modify`コマンドでオプションを `volume create`使用して既存のボリュームを変更するときに、Snapshotコピーロックを有効にでき `-snapshot-locking-enabled`ます。ONTAP 9 .13.1以降では、System Managerを使用してSnapshotコピー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. ウィンドウで、[その他のオプション]*を選択します。
3. ボリューム名、サイズ、エクスポートポリシー、および共有名を入力します。
4. [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. SnapLockコンプライアンスクロックがまだ有効になっていない場合は、*[Initialize Compliance Clock]*を選択します。
6. 変更を保存します。
7. 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コピーのロック*が「有効」*と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、Snapshotコピー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Snapshotコピーロックを有効にします。

   ```
   > volume create -volume vol1 -aggregate aggr1 -size 100m -snapshot
   -locking-enabled true
   Warning: Snapshot copy locking is being enabled on volume “vol1” in
   Vserver “vs1”. It cannot be disabled until all locked Snapshot
   copies are past their expiry time. A volume with unexpired locked
   Snapshot copies 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**コピーロックを有効にする

ONTAP 9 12.1以降では、ONTAP CLIを使用して、既存のボリュームでSnapshotコピー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に対してSnapshotコピーロックを有効にできます。

System Manager

1. [ストレージ]>[ボリューム]に移動します。
2. を選択 ⋮ し、*[編集]>[ボリューム]*を選択します。
3. ウィンドウで、**[Snapshot**コピー（ローカル）設定**]**セクションを探し、[Snapshotロックの有効化]*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。
4. SnapLockコンプライアンスクロックがまだ有効になっていない場合は、*[Initialize Compliance Clock]*を選択します。
5. 変更を保存します。
6. 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コピーのロック*が「有効」*と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Snapshotコピー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**コピーポリシーを作成して保持を適用する

12.1以降では、ONTAP 9コピーポリシーを作成して、Snapshotコピーの保持期間を適用し、ポリシーをボリュームに適用して、指定した期間にわたってSnapshotコピーをロックできます。保持期間を手動で設定して、Snapshotコピー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Snapshotコピー ロック ポリシーを作成し、ボリュームに適用できます。

Snapshotコピー ロック ポリシーの作成

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]*に移動し、を選択します →。
4. [Snapshotポリシーの追加]*ウィンドウで、ポリシー名を入力します。
5. を選択します + Add 。
6. スケジュール名、保持するSnapshotコピーの最大数、SnapLockの保持期間など、Snapshotコピースケジュールの詳細を指定します。
7. [Snapshot保持期間]列にSnapLock 、Snapshotコピーを保持する時間数、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日間のSnapshotコピーポリシーでは、Snapshotコピーが作成されてから5日間はロックされ、その間は削除できません。サポートされる保持期間は次のとおりです。
   - 年：0～100
   - 月：0～1200
   - 日数：0～36500
   - 営業時間：0～24
8. 変更を保存します。

CLI

1. Snapshotコピー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_Snapshot_copies -retention-period1
   _retention_period
   ```

   次のコマンドは、Snapshotコピーロックポリシーを作成します。

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

   アクティブな保持期間にあるSnapshotコピーは置き換えられません。つまり、期限切れになっていないロックされたSnapshotコピーがある場合、保持数は反映されません。

ボリュームへのロックポリシーの適用

System Manager

1. [ストレージ]>[ボリューム]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. ウィンドウで、[Snapshotコピーのスケジュール設定]*を選択します。
4. リストからSnapshotコピーロックポリシーを選択します。
5. Snapshotコピーのロックがまだ有効になっていない場合は、*[Snapshotロックを有効にする]*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Snapshotコピー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
   ```

Snapshotコピーの手動作成時に保持期間を適用

Snapshotコピーの保持期間は、Snapshotコピーを手動で作成するときに適用できます。ボリュームでSnapshotコピー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. [ストレージ]>[ボリューム]*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、*[Snapshotコピー]*タブを選択します。
3. を選択します ＋ Add 。
4. Snapshotコピー名とSnapLockの有効期限を入力します。カレンダーから日付と時刻を選択できます。
5. 変更を保存します。
6. [ボリューム]>[Snapshotコピー]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、保持期限が設定されていることを確認します。

CLI

1. Snapshotコピーを手動で作成して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_copy_name
   -snaplock-expiry-time expiration_date_time
   ```

   次のコマンドでは、新しいSnapshotコピーを作成して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**コピーに保持期間を適用する

System Manager

1. [ストレージ]>[ボリューム]*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、*[Snapshotコピー]*タブを選択します。
3. Snapshotコピーを選択し、を選択して *[Modify SnapLock Expiration Time]*を選択します。カレンダーを選択して、保持期限の日付と時刻を選択できます。
4. 変更を保存します。
5. [ボリューム]>[Snapshotコピー]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、保持期限が設定されていることを確認します。

CLI

1. 既存のSnapshotコピー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_copy_name -expiry-time expiration_date_time
   ```

   次の例は、既存のSnapshotコピーに保持期間を適用します。

   ```
   cluster1> volume snapshot modify-snaplock-expiry-time -volume vol1
   -snapshot snap2 -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、ミラーバックアップポリシールールに保持期間を設定できます。デスティネーションボリュームでSnapshotコピーロックが有効になっている場合は、デスティネーションにレプリケートされたSnapshotコピー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、保持数を超えていても、有効期限を過ぎていないSnapshotコピーは保持されます。

ONTAP 9.14.1以降では、Snapshotコピー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バックアップ デスティネーションや非SnapLockのSnapMirrorデスティネーション ボリュームでのデフォルトのボリューム保持期間を上書きするために使用します。

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 Snapshot copies> -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"
   ```

SnapLock API

Zephyr APIを使用して、スクリプトやワークフロー自動化のSnapLock機能と統合することができます。APIは、HTTP、HTTPS、およびWindows DCE/RPC経由のXMLメッセージングを使用します。詳細については、を "ONTAP自動化に関するドキュメント"参照してください。

ファイル-フィンガープリント-中止

ファイルフィンガープリント処理を中止します。

ファイルフィンガープリントダンプ

ファイルのフィンガープリント情報を表示します。

file-fingerprint-get-iter

ファイルフィンガープリント処理のステータスを表示します。

file-fingerprint-start

ファイルフィンガープリントを生成します。

snaplock-archive-vserver-log

アクティブな監査ログファイルをアーカイブします。

SnapLock - create-vserver-log

SVM の監査ログ設定を作成します。

network-delete-vserver-log SnapLock

SVM の監査ログ設定を削除します。

SnapLock - file-privileged-delete

privileged delete処理を実行します。

snaplock-get-file-retention

ファイルの保持期間を取得します。

SnapLock - get-node-compliance-clock

ノードのComplianceClockの日付と時刻を取得します。

network-get-vserver -active-log-files-iter SnapLock

アクティブなログファイルのステータスを表示します。

vlan-get-vserver -log-iter SnapLock

監査ログ設定を表示します。

network-modify-vserver-log SnapLock

SVM の監査ログ設定を変更します。

snaplock-set-file-retention

ファイルの保持期限を設定します。

SnapLock set-node-compliance-clock

ノードのComplianceClockの日時を設定します。

snaplock-volume-set-privileged-delete

SnapLock Enterpriseボリュームに対してprivileged-deleteオプションを設定します。

volume-get-snaplock-attrs

SnapLockボリュームの属性を取得します。

volume-set-snaplock-attrs

SnapLockボリュームの属性を設定します。

著作権に関する情報

商標に関する情報