SnapLockの設定

ONTAP 9

NetApp
January 23, 2026

目次

SnapLockの設定

ONTAP SnapLockの設定について学ぶ

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

ONTAP Compliance Clockを初期化する

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

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

開始する前に

コンプライアンス クロックを再初期化するには：

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

コンプライアンス クロックを初期化するための一般的な要件：

- このタスクを実行するには、クラスタ管理者である必要があります。
- "SnapLock ライセンスはノードにインストールする必要があります"。

タスク概要

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

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

手順

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

System Manager

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

CLI

1. システム コンプライアンス クロックを初期化します。

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

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

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

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

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

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

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

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

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

NTPが設定されたシステムのコンプライアンス クロック再同期の有効化

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

開始する前に

- この機能は、advanced権限レベルでのみ使用できます。

- このタスクを実行するには、クラスタ管理者である必要があります。
- "SnapLock ライセンスはノードにインストールする必要があります"。
- この機能は、Cloud Volumes ONTAP、ONTAP Select、およびVSIMのプラットフォームでのみ使用できます。

タスク概要

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

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

手順

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

   `snaplock compliance-clock ntp`

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

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

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

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

   `snaplock compliance-clock ntp show`

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

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

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

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

ONTAP SnapLockアグリゲートを作成する

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

開始する前に

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

アップグレード時の考慮事項

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

リバートに関する考慮事項

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

タスク概要

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

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

手順

1. SnapLockアグリゲートを作成します。

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

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

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

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

ONTAP SnapLockボリュームを作成してマウントする

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

開始する前に

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

タスク概要

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

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

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

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

System Manager

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

手順

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

CLI

1. SnapLockボリュームを作成します。

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

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

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

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

SnapLockボリュームのマウント

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

開始する前に

SnapLockがオンラインである必要があります。

タスク概要

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

手順

1. SnapLockボリュームをマウントします。

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

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

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

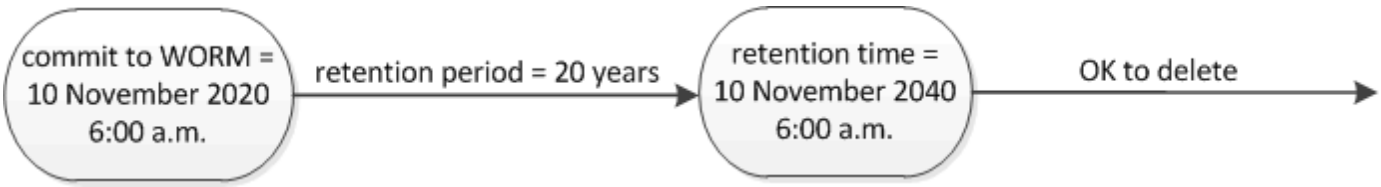
   ```
   cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path /sales
   ```

ONTAP SnapLock保持期間を設定する

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

保持期間と保持期限について

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



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

レプリケーションに関する重要な考慮事項

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

リバートに関する重要な考慮事項

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

保持期間について

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

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

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

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

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

デフォルトの保持期間の設定

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

開始する前に

SnapLockがオンラインである必要があります。

タスク概要

次の表に、デフォルトの保持期間に指定できる値を示します。

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

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

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

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

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

手順

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ファイルに対する保持期限の明示的な設定

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

タスク概要

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

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

手順

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

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

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

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

イベント発生後のファイル保持期間の設定

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

開始する前に

- このタスクを実行するには、SnapLock管理者である必要があります。

  "SnapLock管理者アカウントの作成"

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

タスク概要

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

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

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

EBRポリシーは、リーガル ホールド中のファイルには適用できません。

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

EBRを使用して既存の***WORM***ファイルの保持期間を延長する

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

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

手順

1. EBRポリシーを作成します。

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

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

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

2. EBRポリシーを適用します。

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

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

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

関連情報

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

ONTAP SnapLockで保護された監査ログを作成する

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

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

開始する前に

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

タスク概要

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

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

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

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

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

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

手順

1. SnapLockアグリゲートを作成します。

   SnapLockアグリゲートの作成

2. 監査ログを設定するSVMにSnapLockボリュームを作成します。

   SnapLockボリュームの作成

3. SVMに監査ログを設定します。

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

`-size size -retention-period default_retention_period`

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

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

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

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

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

   SnapLockボリュームのマウント

ONTAP SnapLock設定を確認する

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

手順

1. ファイル フィンガープリントを生成します。

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

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

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

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

2. ファイルのフィンガープリントを表示します。

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

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

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

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