SnapLockの設定

ONTAP 9

NetApp
December 20, 2024

目次

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。

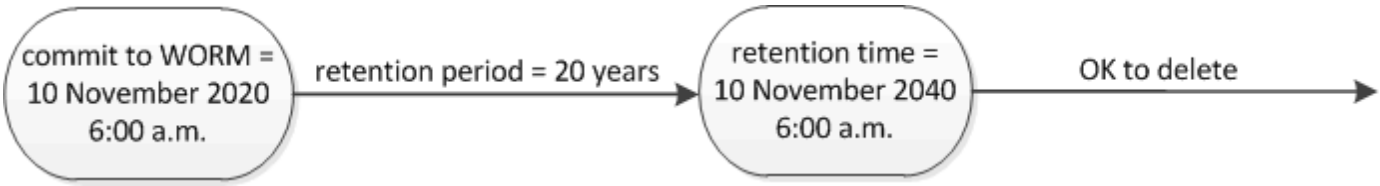
   ```
   cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path /sales
   ```

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	

値	単位	脚注
0 ~ 24	時間	
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
```

著作権に関する情報

商標に関する情報