Configurez SnapLock

ONTAP 9

NetApp
April 01, 2023

Table des matières

Configurez SnapLock

Configurez SnapLock

Avant d'utiliser SnapLock, vous devez configurer SnapLock en exécutant diverses tâches telles que l'installation de la licence SnapLock, l'initialisation de l'horloge de conformité, la création d'un agrégat SnapLock, etc.

Installez la licence

Une licence SnapLock vous permet d'utiliser à la fois le mode SnapLock Compliance et le mode SnapLock Enterprise. Les licences SnapLock sont émises selon les nœuds. Vous devez installer une licence pour chaque nœud qui héberge un agrégat SnapLock.

Pour plus d'informations sur le mode conformité et le mode entreprise, reportez-vous à la section "Qu'est-ce que SnapLock".

Ce dont vous avez besoin

Vous devez être un administrateur de cluster pour effectuer cette tâche.

Description de la tâche

Vous devez avoir reçu les clés de licence SnapLock de votre ingénieur commercial.

Effectuez cette tâche à l'aide de ONTAP System Manager ou de l'interface de ligne de commandes de ONTAP.

System Manager

1. Accédez à **Cluster > Paramètres > licences > Ajouter une licence**.
2. Cliquez sur **+Ajouter**.
3. Cliquez sur **Browse** et recherchez le fichier de licence NetApp.
4. Cliquez sur **Ajouter**.

CLI

1. Installez la licence SnapLock pour un nœud :

   `system license add -license-code` *`license_key`*

   La commande suivante installe la licence avec la clé `AAAAAAAAAAAAAAAAAAAAAAAAAAAA`.

   ```
   cluster1::> system license add -license-code
   AAAAAAAAAAAAAAAAAAAAAAAAAAAA
   ```

2. Répétez l'étape précédente pour chaque licence de nœud.

Initialiser l’horloge de conformité

La fonctionnalité SnapLock ComplanceClock évite toute altération susceptible de modifier la période de conservation des fichiers WORM. Vous devez initialiser *system ComplanceClock* sur chaque nœud hébergeant un agrégat SnapLock. Une fois que vous avez initialisé la ComplianceClock sur un noeud, vous ne pouvez pas l’initialiser à nouveau.

Ce dont vous avez besoin

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- La licence SnapLock doit être installée sur le nœud.

Description de la tâche

L’heure sur le système ComplanceClock est héritée par le *volume CombianceClock*, qui contrôle la période de rétention des fichiers WORM sur le volume. Le réveil complet du volume est initialisé automatiquement lorsque vous créez un volume SnapLock.

Le réglage initial de l’horloge de conformité est basé sur l’horloge actuelle du système. Pour cette raison, vous devez vérifier que l’heure et le fuseau horaire du système sont corrects avant d’initialiser la ComplanceClock. Une fois que vous avez initialisé la ComplianceClock sur un noeud, vous ne pouvez pas l’initialiser à nouveau.

System Manager

Depuis ONTAP 9.12.1, vous pouvez utiliser System Manager pour initialiser l'horloge de conformité SnapLock.

Étapes

1. Accédez à **Cluster > Présentation**.
2. Dans la section **noeuds**, cliquez sur **Initialize SnapLock Compliance Clock**.
3. Pour afficher la colonne horloge de conformité et vérifier que l'horloge de conformité est initialisée, dans la section **Cluster > Présentation > nœuds**, cliquez sur **Afficher/Masquer** et sélectionnez **horloge de conformité SnapLock**.

CLI

1. Initialisez le système ComplanceClock :

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

   La commande suivante permet d'initialiser la ComplanceClock du système `node1`:

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

2. Lorsque vous y êtes invité, vérifiez que l'horloge système est correcte et que vous souhaitez initialiser la ComplanceClock :

   ```
   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. Répétez cette procédure pour chaque nœud qui héberge un agrégat SnapLock.

Activez la resynchronisation ComplanceClock pour un système configuré en NTP

Vous pouvez activer la fonction de synchronisation de l'heure de la conformité SnapLock lorsqu'un serveur NTP est configuré.

Ce dont vous avez besoin

- Cette fonction est disponible uniquement au niveau de privilège avancé.
- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- La licence SnapLock doit être installée sur le nœud.

- Cette fonction est disponible uniquement sur les plates-formes Cloud Volumes ONTAP, ONTAP Select et VSIM.

Description de la tâche

Lorsque le démon d'horloge sécurisée SnapLock détecte une inclinaison au-delà du seuil, ONTAP utilise l'heure système pour réinitialiser à la fois le verrouillage complet du système et du volume. Une période de 24 heures est définie comme seuil d'inclinaison. Cela signifie que la fonction ComplanceClock du système est synchronisée avec l'horloge du système uniquement si l'inclinaison est plus d'un jour.

Le démon d'horloge sécurisée SnapLock détecte une inclinaison et modifie la conformité à l'heure système. Toute tentative de modification de l'heure système pour forcer la synchronisation de la ComplanceClock avec l'heure système échoue, car la ComplanceClock se synchronise à l'heure système uniquement si l'heure système est synchronisée avec l'heure NTP.

Étapes

1. Activez la fonction de synchronisation de l'heure de fin d'horloge SnapLock lorsqu'un serveur NTP est configuré :

   `snaplock compliance-clock ntp`

   La commande suivante active la fonction de synchronisation de l'heure de la ComplanceClock du système :

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

2. Lorsque vous y êtes invité, vérifiez que les serveurs NTP configurés sont approuvés et que le canal de communication est sécurisé pour activer la fonction :
3. Vérifiez que la fonction est activée :

   `snaplock compliance-clock ntp show`

   La commande suivante vérifie que la fonction de synchronisation de l'heure de la ComplanceClock du système est activée :

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

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

Créer un agrégat SnapLock

Vous utilisez le volume `-snaplock-type` Pour spécifier un type de volume Compliance ou Enterprise SnapLock. Pour les versions antérieures à ONTAP 9.10.1, vous devez créer un agrégat SnapLock distinct. Depuis ONTAP 9.10.1, les volumes SnapLock et non SnapLock peuvent exister sur le même agrégat. Ainsi, vous n'avez plus besoin de créer un agrégat SnapLock distinct si vous utilisez ONTAP 9.10.1.

Ce dont vous avez besoin

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- La licence SnapLock doit être installée sur le nœud.
- La ComplanceClock du nœud doit être initialisée.
- Si vous avez partitionné les disques comme « root », « data1 » et « data2 », vous devez vous assurer que les disques de secours sont disponibles.

Mise à niveau

Lors de la mise à niveau vers ONTAP 9.10.1, les agrégats SnapLock et non SnapLock existants sont mis à niveau pour prendre en charge la présence de volumes SnapLock et non SnapLock. Cependant, les attributs des volumes SnapLock existants ne sont pas automatiquement mis à jour. Par exemple, les champs de compaction des données, de déduplication entre les volumes et de déduplication entre les volumes en arrière-plan restent inchangés. Les nouveaux volumes SnapLock créés sur des agrégats existants ont les mêmes valeurs par défaut que les volumes qui ne sont pas SnapLock. Les valeurs par défaut des nouveaux volumes et des agrégats dépendent de la plateforme.

Ne tenez pas compte des considérations

Pour restaurer une version ONTAP antérieure à la version 9.10.1, vous devez déplacer les volumes SnapLock Compliance, SnapLock Enterprise et SnapLock vers leurs propres agrégats SnapLock.

Description de la tâche

- Vous ne pouvez pas créer d'agrégats de conformité pour les LUN FlexArray, mais les agrégats de conformité SnapLock sont pris en charge avec les LUN FlexArray.
- L'option SyncMirror ne permet pas de créer des agrégats de conformité.
- Vous pouvez créer des agrégats de conformité en miroir dans une configuration MetroCluster uniquement si l'agrégat est utilisé pour héberger des volumes du journal d'audit SnapLock.

> Dans une configuration MetroCluster, SnapLock Enterprise est pris en charge sur des agrégats en miroir ou non mis en miroir. La conformité SnapLock est prise en charge uniquement sur les agrégats sans miroir.

Étapes

1. Créer un agrégat SnapLock :

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

   La page man de la commande contient une liste complète d'options.

   La commande suivante crée une SnapLock `Compliance` agrégat nommé `aggr1` avec trois disques sur `node1`:

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

Création et montage de volumes SnapLock

Vous devez créer un volume SnapLock pour les fichiers ou les copies Snapshot que vous

souhaitez valider en état WORM. Depuis ONTAP 9.10.1, tout volume que vous créez, quel que soit le type d'agrégat, est créé par défaut en tant que volume non SnapLock. Vous devez utiliser le `-snaplock-type` Option permettant de créer explicitement un volume SnapLock en spécifiant Compliance ou Enterprise comme type SnapLock. Par défaut, le type de SnapLock est défini sur `non-snaplock`.

Ce dont vous avez besoin

- L'agrégat SnapLock doit être en ligne.
- La licence SnapLock doit être installée sur le nœud.
- La ComplanceClock du nœud doit être initialisée.

Description de la tâche

Avec les autorisations SnapLock appropriées, vous pouvez détruire ou renommer un volume d'entreprise à tout moment. Vous ne pouvez pas détruire un volume Compliance tant que la période de conservation n'est pas écoulée. Vous ne pouvez jamais renommer un volume Compliance.

Vous pouvez cloner des volumes SnapLock, mais vous ne pouvez pas cloner des fichiers sur un volume SnapLock. Le volume clone sera du même type SnapLock que le volume parent.

> Les LUN ne sont pas prises en charge sur les volumes SnapLock. S'il est possible de déplacer des LUN vers un volume SnapLock avec la technologie existante, il ne s'agit pas d'une opération prise en charge, ni de toute autre opération impliquant des LUN dans un volume SnapLock.

Effectuez cette tâche à l'aide de ONTAP System Manager ou de l'interface de ligne de commandes de ONTAP.

System Manager

Depuis ONTAP 9.12.1, vous pouvez utiliser System Manager pour créer un volume SnapLock.

Étapes

1. Accédez à **Storage > volumes** et cliquez sur **Add**.
2. Dans la fenêtre **Ajouter un volume**, cliquez sur **plus d'options**.
3. Entrez les informations du nouveau volume, notamment le nom et la taille du volume.
4. Sélectionnez **Activer SnapLock** et choisissez le type SnapLock, conformité ou entreprise.
5. Dans la section **Auto-commit Files**, sélectionnez **Modified** et entrez la durée pendant laquelle un fichier doit rester inchangé avant qu'il ne soit automatiquement engagé. La valeur minimale est de 5 minutes et la valeur maximale est de 10 ans.
6. Dans la section **Data Retention**, sélectionnez la période de rétention minimale et maximale.
7. Sélectionnez la période de rétention par défaut.
8. Cliquez sur **Enregistrer**.
9. Sélectionnez le nouveau volume dans la page **volumes** pour vérifier les paramètres SnapLock.

CLI

1. Créer un volume SnapLock :

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

   Pour obtenir la liste complète des options, consultez la page man de la commande. Les options suivantes ne sont pas disponibles pour les volumes SnapLock : `-nvfail`, `-atime-update`, `-is -autobalance-eligible`, `-space-mgmt-try-first`, et `vmalign`.

   La commande suivante crée une SnapLock `Compliance` volume nommé `vol1` marche `aggr1` marche `vs1`:

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

Montez un volume SnapLock

Vous pouvez monter un volume SnapLock sur une Junction path dans le SVM namespace pour accéder au client NAS.

Ce dont vous avez besoin

Le volume SnapLock doit être en ligne.

Description de la tâche

- Vous pouvez monter un volume SnapLock uniquement sous la racine de la SVM.
- Vous ne pouvez pas monter un volume normal sous un volume SnapLock.

Étapes

1. Monter un volume SnapLock :

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

   Pour obtenir la liste complète des options, consultez la page man de la commande.

   La commande suivante monte un volume SnapLock nommé `vol1` au chemin de jonction `/sales` dans le `vs1` espace de noms :

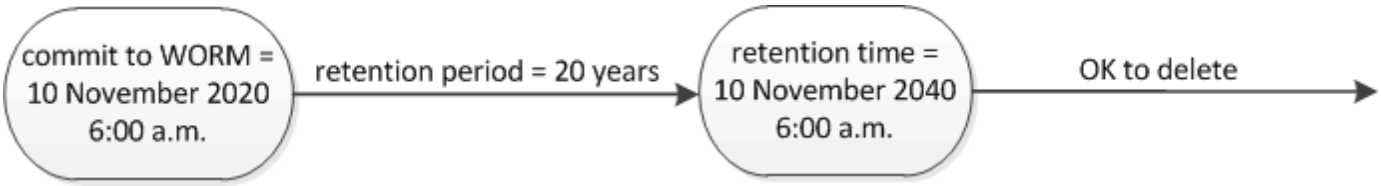
   ```
   cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path /sales
   ```

Définissez la durée de rétention

Vous pouvez définir explicitement la durée de conservation d'un fichier ou utiliser la période de rétention par défaut pour le volume afin de définir la durée de conservation. Sauf si vous définissez explicitement la durée de conservation, SnapLock utilise la période de conservation par défaut pour calculer la durée de conservation. Vous pouvez également définir la conservation des fichiers après un événement.

À propos de la période de conservation et de la durée de conservation

Le paramètre *rétention_période* pour un fichier WORM spécifie la durée pendant laquelle le fichier doit être conservé après son activation à l'état WORM. Le *temps de rétention* pour un fichier WORM est le temps après lequel le fichier n'a plus besoin d'être conservé. Une période de conservation de 20 ans pour un dossier engagé à l'état WORM le 10 novembre 2020 6 h 00, par exemple, entraînerait un temps de rétention de 10 novembre 2040 6 h 00



> Depuis ONTAP 9.10.1, vous pouvez définir une durée de conservation allant jusqu'au 26 octobre 3058 et une période de conservation pouvant aller jusqu'à 100 ans. Lorsque vous prolongez les dates de conservation, les anciennes règles sont automatiquement converties. Dans ONTAP 9.9.1 et versions antérieures, sauf si vous avez défini la période de conservation par défaut sur infinie, la durée maximale de conservation prise en charge est de janvier 19 2071 (GMT).

Considérations importantes relatives à la réplication

Lorsque vous définissez une relation SnapMirror avec un volume source SnapLock à une date de conservation postérieure au 19 janvier 2071 (GMT), le cluster de destination doit exécuter ONTAP 9.10.1 ou version ultérieure, sinon le transfert SnapMirror échoue.

Considérations importantes concernant la restauration

ONTAP vous empêche de restaurer un cluster depuis ONTAP 9.10.1 vers une version antérieure de ONTAP lorsqu'il y a des fichiers avec une période de conservation postérieure à « janvier 19, 2071 8:44:07 ».

Compréhension des périodes de conservation par défaut

Un volume SnapLock Compliance ou Enterprise a quatre périodes de conservation :

- Durée de conservation minimale (`min`), avec une valeur par défaut de 0
- Durée de conservation maximale (`max`), avec une valeur par défaut de 30 ans
- Période de rétention par défaut, avec une valeur par défaut égale à `min` Pour le mode conformité et le mode entreprise à partir de ONTAP 9.10.1. Dans les versions ONTAP antérieures à ONTAP 9.10.1, la période de conservation par défaut dépend du mode :
  - Pour le mode conformité, la valeur par défaut est égale à `max`.
  - Pour le mode entreprise, la valeur par défaut est égale à `min`.
- Période de conservation non spécifiée.

  Depuis ONTAP 9.8, vous pouvez définir la période de conservation des fichiers d'un volume sur `unspecified`, pour activer le fichier à conserver jusqu'à ce que vous ayez défini une durée de conservation absolue. Vous pouvez définir un fichier avec un temps de conservation absolu sur une rétention non spécifiée et revenir à une conservation absolue tant que la nouvelle durée de conservation absolue est postérieure à la durée absolue que vous avez définie précédemment.

  Depuis ONTAP 9.12.1, les fichiers WORM dont la période de conservation est définie sur `unspecified` Est garanti que la période de conservation est définie sur la période minimale de conservation configurée pour le volume SnapLock. Lorsque vous modifiez la période de rétention des fichiers de `unspecified` pour une durée de conservation absolue, la nouvelle durée de rétention spécifiée doit être supérieure à la durée de conservation minimale déjà définie sur le fichier.

Ainsi, si vous ne définissez pas explicitement la durée de rétention avant de valider un fichier en mode conformité à l'état WORM et que vous ne modifiez pas les valeurs par défaut, le fichier sera conservé pendant 30 ans. De même, si vous ne définissez pas explicitement la durée de rétention avant de valider un fichier Enterprise-mode à l'état WORM et que vous ne modifiez pas les valeurs par défaut, le fichier sera conservé pendant 0 ans, ou, de manière efficace, pas du tout.

Définir la période de conservation par défaut

Vous pouvez utiliser le `volume snaplock modify` Commande pour définir la période de conservation par défaut pour les fichiers d'un volume SnapLock.

Ce dont vous avez besoin

Le volume SnapLock doit être en ligne.

Description de la tâche

Le tableau suivant indique les valeurs possibles pour l'option de période de conservation par défaut :

> La période de conservation par défaut doit être supérieure ou égale à (>=) la période de rétention minimale et inférieure ou égale à (<=) la période de rétention maximale.

Valeur	Unité	Remarques
0 - 65535	secondes	

Valeur	Unité	Remarques
0 - 24	heures	
0 - 365	jours	
0 - 12	mois	
0 - 100	années	À partir d'ONTAP 9.10.1. Pour les versions antérieures de ONTAP, la valeur est comprise entre 0 et 70.
capacité	-	Utilisez la période de rétention maximale.
minimum	-	Utilisez la période de rétention minimale.
illimitée	-	Conservez toujours les fichiers.
non spécifié	-	Conservez les fichiers jusqu'à ce qu'une période de conservation absolue soit définie.

Les valeurs et les plages des périodes de rétention maximale et minimale sont identiques, sauf pour `max` et `min`, qui ne sont pas applicables. Pour plus d'informations sur cette tâche, voir "Définissez l'aperçu de la durée de conservation".

Vous pouvez utiliser le `volume snaplock show` commande pour afficher les paramètres de la période de rétention du volume. Pour plus d'informations, consultez la page man de la commande

> Une fois qu'un fichier a été engagé à l'état WORM, vous pouvez prolonger mais pas raccourcir la période de rétention.

Étapes

1. Définissez la période de conservation par défaut pour les fichiers d'un volume SnapLock :

   ```
   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
   ```

   Pour obtenir la liste complète des options, consultez la page man de la commande.

   > Les exemples suivants supposent que les périodes de rétention minimale et maximale n'ont pas été modifiées auparavant.

   La commande suivante définit la période de conservation par défaut pour un volume Compliance ou Enterprise sur 20 jours :

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

La commande suivante définit la période de conservation par défaut pour un volume Compliance sur 70 ans :

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

La commande suivante définit la période de conservation par défaut pour un volume entreprise sur 10 ans :

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

Les commandes suivantes définissent la période de conservation par défaut pour un volume entreprise sur 10 jours :

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

La commande suivante définit la période de conservation par défaut d'un volume Compliance sur infinie :

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

Définissez explicitement la durée de rétention d'un fichier

Vous pouvez définir explicitement la durée de conservation d'un fichier en modifiant son heure de dernier accès. Vous pouvez utiliser n'importe quelle commande ou programme approprié via NFS ou CIFS pour modifier l'heure du dernier accès.

Description de la tâche

Une fois qu'un fichier a été enregistré sur WORM, vous pouvez prolonger mais pas réduire la durée de conservation. La durée de rétention est stockée dans le `atime` champ du fichier.

> Vous ne pouvez pas définir explicitement la durée de conservation d'un fichier sur `infinite`. Cette valeur n'est disponible que lorsque vous utilisez la période de rétention par défaut pour calculer la durée de rétention.

Étapes

1. Utilisez une commande ou un programme approprié pour modifier l'heure du dernier accès pour le fichier dont vous souhaitez définir la durée de rétention.

   Dans un shell UNIX, utilisez la commande suivante pour définir un temps de rétention de 21 novembre 2020 6 h 00 sur un fichier nommé `document.txt`:

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

   Vous pouvez utiliser n'importe quelle commande ou programme approprié pour modifier l'heure du dernier accès dans Windows.

Définissez la période de rétention des fichiers après un événement

À partir de ONTAP 9.3, vous pouvez définir la durée de conservation d'un fichier après un événement en utilisant la fonction SnapLock *Event Based Retention (EBR)*.

Ce dont vous avez besoin

- Vous devez être un administrateur SnapLock pour effectuer cette tâche.

  "Créez un compte d'administrateur SnapLock"

- Vous devez vous connecter à une connexion sécurisée (SSH, console ou ZAPI).

Description de la tâche

La stratégie *Event Retention* définit la période de rétention du fichier après l'événement. La règle peut être appliquée à un seul fichier ou à tous les fichiers d'un répertoire.

- Si un fichier n'est pas un fichier WORM, il est mis à l'état WORM pour la période de conservation définie dans la stratégie.
- Si un fichier est un fichier WORM ou un fichier inscriptible WORM, sa période de conservation sera prolongée par la période de conservation définie dans la stratégie.

Vous pouvez utiliser un volume Compliance-mode ou Enterprise-mode.

Les politiques EBR ne peuvent pas être appliquées aux fichiers en attente légale.

Pour une utilisation avancée, voir "Stockage WORM conforme avec NetApp SnapLock".

utilisation d'EBR pour prolonger la période de conservation des fichiers WORM déjà existants

EBR est pratique lorsque vous souhaitez prolonger la période de conservation des fichiers WORM existants. Par exemple, votre entreprise a peut-être pour politique de conserver les enregistrements W-4 des employés sous forme non modifiée pendant trois ans après que l'employé change de retenue d'impôt. Une autre politique de l'entreprise pourrait exiger que les enregistrements W-4 soient conservés pendant cinq ans après la cessation d'emploi de l'employé.

Dans ce cas, vous pouvez créer une police EBR avec une période de rétention de cinq ans. Une fois l'employé résilié (l'« événement »), vous appliqueriez la politique de l'EBR au registre W-4 de l'employé, ce qui entraînerait la prolongation de sa période de conservation. Ce processus est généralement plus simple que de prolonger manuellement la période de conservation, en particulier lorsqu'un grand nombre de fichiers sont impliqués.

Étapes

1. Créer une règle EBR :

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

   La commande suivante crée la règle EBR `employee_exit` marche `vs1` avec une période de rétention de dix ans :

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

2. Appliquer une politique EBR :

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

   La commande suivante applique la règle EBR `employee_exit` marche `vs1` à tous les fichiers du répertoire `d1`:

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

Créer un journal d'audit

Vous devez créer un journal d'audit protégé par SnapLock avant d'effectuer une suppression privilégiée ou un déplacement de volume SnapLock. Le journal d'audit enregistre la création et la suppression de comptes administrateur SnapLock, les modifications du volume du journal, si la suppression privilégiée est activée, les opérations de suppression privilégiée et les opérations de déplacement de volume SnapLock.

Ce dont vous avez besoin

Pour créer un agrégat SnapLock, vous devez être un administrateur de cluster.

Description de la tâche

Vous ne pouvez pas supprimer un journal d'audit tant que la période de conservation du fichier journal n'est pas écoulée. Vous ne pouvez pas modifier un journal d'audit même après la période de conservation écoulée. Ceci est vrai pour les modes SnapLock Compliance et Enterprise.

> Dans ONTAP 9.4 et versions antérieures, vous ne pouvez pas utiliser un volume SnapLock Enterprise pour la journalisation des audits. Vous devez utiliser un volume SnapLock Compliance. Dans ONTAP 9.5 et versions ultérieures, vous pouvez utiliser un volume SnapLock Enterprise ou un volume SnapLock Compliance pour la journalisation des audits. Dans tous les cas, le volume du journal d'audit doit être monté sur le Junction path `/snaplock_audit_log`. Aucun autre volume ne peut utiliser cette Junction path

Les journaux d'audit SnapLock sont disponibles dans le `/snaplock_log` répertoire sous la racine du volume du journal de vérification, dans les sous-répertoires nommés `privdel_log` (opérations de suppression privilégiée) et `system_log` (autres). Les noms des fichiers journaux d'audit contiennent l'horodatage de la première opération consignée, ce qui facilite la recherche des enregistrements en fonction de l'heure approximative d'exécution des opérations.

- Vous pouvez utiliser le `snaplock log file show` commande pour afficher les fichiers journaux sur le volume du journal d'audit.
- Vous pouvez utiliser le `snaplock log file archive` commande pour archiver le fichier journal actuel et en créer un nouveau, ce qui est utile dans les cas où vous devez enregistrer les informations du journal d'audit dans un fichier distinct.

Pour plus d'informations, consultez les pages de manuels des commandes.

> Un volume de protection des données ne peut pas être utilisé comme volume de journal d'audit SnapLock.

Étapes

1. Créer un agrégat SnapLock.

   Créer un agrégat SnapLock

2. Sur le SVM que vous voulez configurer pour la journalisation d'audit, créez un volume SnapLock.

   Créer un volume SnapLock

3. Configuration du SVM pour la journalisation d'audit :

   ```
   snaplock log create -vserver SVM_name -volume snaplock_volume_name -max-file
   -size size -retention-period default_retention_period
   ```

   > La période de conservation minimale par défaut des fichiers journaux d'audit est de six mois. Si la période de conservation d'un fichier affecté est supérieure à la période de conservation du journal d'audit, la période de conservation du journal hérite de la période de conservation du fichier. Ainsi, si la période de conservation d'un fichier supprimé avec suppression privilégiée est de 10 mois et que la période de conservation du journal d'audit est de 8 mois, la période de conservation du journal est étendue à 10 mois. Pour plus d'informations sur la durée de conservation et la période de rétention par défaut, reportez-vous à la section "Définissez la durée de rétention".

La commande suivante configure `SVM1` Pour la journalisation des audits à l'aide du volume SnapLock `logVol`. Le journal d'audit a une taille maximale de 20 Go et est conservé pendant huit mois.

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

4. Sur le SVM que vous avez configuré pour la journalisation d'audit, montez le volume SnapLock sur la Junction path `/snaplock_audit_log`.

   Montez un volume SnapLock

Vérifiez les paramètres SnapLock

Vous pouvez utiliser le `volume file fingerprint start` et `volume file fingerprint dump` Commandes permettant d'afficher des informations clés sur les fichiers et volumes, y compris le type de fichier (standard, WORM ou WORM appliable), la date d'expiration du volume, etc.

Étapes

1. Générer une empreinte de fichier :

   `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.
```

   La commande génère un ID de session que vous pouvez utiliser comme entrée dans `volume file fingerprint dump` commande.

   Vous pouvez utiliser le `volume file fingerprint show` Commande avec l'ID de session pour contrôler la progression de l'opération d'empreinte digitale. Assurez-vous que l'opération est terminée avant d'essayer d'afficher l'empreinte digitale.

2. Afficher l'empreinte du fichier :

   `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
```

Informations sur le copyright

Informations sur les marques commerciales