



Archivage et conformité grâce à la technologie SnapLock

ONTAP 9

NetApp
September 12, 2024

Sommaire

- Archivage et conformité grâce à la technologie SnapLock 1
 - Qu'est-ce que SnapLock 1
 - Configurez SnapLock 6
 - Gérer les fichiers WORM 22
 - Déplacer un volume SnapLock 36
 - Verrouiller une copie Snapshot pour assurer la protection contre les attaques par ransomware 38
 - Les API SnapLock 46

Archivage et conformité grâce à la technologie SnapLock

Qu'est-ce que SnapLock

SnapLock est une solution de conformité hautes performances pour les entreprises qui utilisent le stockage WORM pour conserver les fichiers sous une forme non modifiée à des fins réglementaires et de gouvernance.

SnapLock empêche la suppression, la modification ou la modification des données pour répondre aux réglementations SEC 17a-4, HIPAA, FINRA, CFTC et le RGPD. SnapLock vous permet de créer des volumes spéciaux dans lesquels les fichiers peuvent être stockés et archivés dans un état non effaçable et non inscriptible pour une période de conservation définie ou indéfiniment. SnapLock permet cette conservation au niveau fichier via des protocoles de fichiers ouverts standard tels que CIFS et NFS. Les protocoles de fichier ouvert pris en charge pour SnapLock sont les suivants : NFS (versions 2, 3 et 4) et CIFS (SMB 1.0, 2.0 et 3.0).

Avec SnapLock, vous archivez des fichiers et des copies Snapshot sur le stockage WORM et définissez des périodes de conservation pour les données protégées WORM. Le stockage WORM SnapLock utilise la technologie NetApp Snapshot et peut exploiter la réplication SnapMirror ainsi que les sauvegardes SnapVault comme technologie de base pour offrir une protection des données de restauration de sauvegarde. En savoir plus sur le stockage WORM : ["Conformité du stockage WORM avec NetApp SnapLock - TR-4526"](#).

Vous pouvez utiliser une application pour valider les fichiers en mode WORM sur NFS ou CIFS, ou utiliser la fonctionnalité d'autovalidation de SnapLock pour allouer automatiquement les fichiers en mode WORM. Vous pouvez utiliser un fichier *WORM applicable* pour conserver les données écrites de manière incrémentielle, comme les informations de journal. Pour plus d'informations, voir ["Utilisez le mode d'ajout de volumes pour créer des fichiers d'ajout WORM"](#).

SnapLock prend en charge les méthodes de protection des données qui doivent répondre à la plupart des exigences de conformité :

- Vous pouvez utiliser SnapLock pour SnapVault pour protéger les copies Snapshot WORM sur le stockage secondaire. Voir ["Archivage des copies Snapshot en mode WORM"](#).
- Vous pouvez utiliser SnapMirror pour répliquer des fichiers WORM dans un autre emplacement géographique à des fins de reprise après incident. Voir ["Fichiers WORM en miroir"](#).

SnapLock est une fonctionnalité sous licence de NetApp ONTAP. Une seule licence vous donne le droit d'utiliser SnapLock en mode strict conformité, afin de répondre aux exigences externes telles que la règle SEC 17a-4 et un mode perte de l'entreprise, afin de respecter les réglementations internes régissant la protection des ressources numériques. Les licences SnapLock font partie du ["ONTAP One"](#) suite logicielle.

SnapLock est pris en charge sur tous les systèmes AFF, FAS et ONTAP Select. SnapLock n'est pas une solution exclusivement logicielle ; il s'agit d'une solution matérielle et logicielle intégrée. Cette distinction est importante pour les réglementations WORM strictes, telles que la norme SEC 17a-4, qui requièrent une solution matérielle et logicielle intégrée. Pour plus d'informations, reportez-vous à la section ["SEC interprétation : stockage électronique des dossiers des courtiers-concessionnaires"](#).

Les avantages de SnapLock

Une fois SnapLock configuré, vous pouvez effectuer les tâches suivantes :

- "Archivage des fichiers en mode WORM"
- "Archivage des copies Snapshot sur le stockage WORM pour le stockage secondaire"
- "Mise en miroir des fichiers WORM pour la reprise après incident"
- "Conservation des fichiers WORM en cas de litiges avec la conservation légale"
- "Supprimez des fichiers WORM à l'aide de la fonction de suppression privilégiée"
- "Définissez la période de rétention des fichiers"
- "Déplacer un volume SnapLock"
- "Verrouiller une copie Snapshot pour assurer la protection contre les attaques par ransomware"
- "Vérifiez l'utilisation de SnapLock avec le journal d'audit"
- "Utilisez les API SnapLock"

SnapLock Compliance et Enterprise modes

Les modes SnapLock Compliance et Enterprise diffèrent principalement du niveau auquel chaque mode protège les fichiers WORM :

| Mode SnapLock | Niveau de protection | Suppression du fichier WORM pendant la conservation |
|--------------------|----------------------|--|
| Mode de conformité | Au niveau du disque | Ne peut pas être supprimé |
| Mode entreprise | Au niveau fichier | Peut être supprimé par l'administrateur de conformité à l'aide d'une procédure audité de "suppression privilégiée" |

Une fois la période de rétention écoulée, vous êtes responsable de la suppression des fichiers dont vous n'avez plus besoin. Une fois qu'un fichier a été engagé en mode WORM, qu'il soit en mode conformité ou entreprise, il ne peut pas être modifié, même après l'expiration de la période de conservation.

Vous ne pouvez pas déplacer un fichier WORM pendant ou après la période de conservation. Vous pouvez copier un fichier WORM, mais la copie ne conserve pas ses caractéristiques WORM.

Le tableau suivant présente les différences de capacités prises en charge par les modes SnapLock Compliance et Enterprise :

| Fonctionnalité | Conformité SnapLock | SnapLock Enterprise |
|---|---------------------|---|
| Activer et supprimer des fichiers à l'aide de la suppression privilégiée | Non | Oui. |
| Réinitialiser les disques | Non | Oui. |
| Destruction des agrégats et des volumes SnapLock pendant la période de conservation | Non | Oui, à l'exception du volume du journal d'audit de SnapLock |

| | | |
|--|------|---|
| Renommer les agrégats ou les volumes | Non | Oui. |
| Utiliser des disques non NetApp | Non | Oui (avec " Virtualisation FlexArray ") |
| Utilisation du volume SnapLock pour la journalisation des audits | Oui. | Oui, à partir de ONTAP 9.5 |

Fonctionnalités prises en charge et non prises en charge avec SnapLock

Le tableau suivant présente les fonctionnalités prises en charge avec le mode SnapLock Compliance, le mode SnapLock Enterprise ou les deux :

| Fonction | Prise en charge par SnapLock Compliance | Pris en charge par SnapLock Enterprise |
|--------------------------------------|--|--|
| Groupes de cohérence | Non | Non |
| Volumes chiffrés | Oui, à partir de ONTAP 9.2. En savoir plus sur Cryptage et SnapLock . | Oui, à partir de ONTAP 9.2. En savoir plus sur Cryptage et SnapLock . |
| FabricPool sur les agrégats SnapLock | Non | Oui, à partir de ONTAP 9.8. En savoir plus sur FabricPool sur les agrégats SnapLock Enterprise . |
| Les agrégats Flash Pool | Oui, à partir de ONTAP 9.1. | Oui, à partir de ONTAP 9.1. |
| FlexClone | Vous pouvez cloner des volumes SnapLock, mais vous ne pouvez pas cloner des fichiers sur un volume SnapLock. | Vous pouvez cloner des volumes SnapLock, mais vous ne pouvez pas cloner des fichiers sur un volume SnapLock. |
| Volumes FlexGroup | Oui, à partir de ONTAP 9.11.1. En savoir plus sur [flexgroup] . | Oui, à partir de ONTAP 9.11.1. En savoir plus sur [flexgroup] . |
| LUN | Non En savoir plus sur Prise en charge LUN Avec SnapLock. | Non En savoir plus sur Prise en charge LUN Avec SnapLock. |
| Configurations MetroCluster | Oui, à partir de ONTAP 9.3. En savoir plus sur Prise en charge de MetroCluster . | Oui, à partir de ONTAP 9.3. En savoir plus sur Prise en charge de MetroCluster . |
| Vérification multiadministrateur | Oui, à partir de ONTAP 9.13.1. En savoir plus sur Prise en charge MAV . | Oui, à partir de ONTAP 9.13.1. En savoir plus sur Prise en charge MAV . |

| | | |
|--|---|---|
| SAN | Non | Non |
| SnapRestore pour un seul fichier | Non | Oui. |
| Synchronisation active SnapMirror | Non | Non |
| SnapRestore | Non | Oui. |
| SMTape | Non | Non |
| SnapMirror synchrone | Non | Non |
| SSD | Oui, à partir de ONTAP 9.1. | Oui, à partir de ONTAP 9.1. |
| Fonctionnalités d'efficacité du stockage | Oui, depuis ONTAP 9.9.1. En savoir plus sur prise en charge de l'efficacité du stockage . | Oui, depuis ONTAP 9.9.1. En savoir plus sur prise en charge de l'efficacité du stockage . |

FabricPool sur les agrégats SnapLock Enterprise

FabricPool est pris en charge sur les agrégats SnapLock Enterprise à partir de ONTAP 9.8. Toutefois, votre équipe de compte doit ouvrir une demande de modification des produits afin de documenter que les données FabricPool hiérarchisées vers un cloud public ou privé ne sont plus protégées par SnapLock, car les administrateurs cloud peuvent les supprimer.



Les données FabricPool placées dans un cloud public ou privé n'sont plus protégées par SnapLock, car les administrateurs cloud peuvent les supprimer.

Volumes FlexGroup

SnapLock prend en charge les volumes FlexGroup depuis ONTAP 9.11.1, mais les fonctionnalités suivantes ne sont pas prises en charge :

- Obligation légale
- Conservation basée sur les événements
- SnapLock pour SnapVault (prise en charge à partir de ONTAP 9.12.1)

Vous devez également connaître les comportements suivants :

- L'horloge de conformité de volume (VCC) d'un volume FlexGroup est déterminée par le VCC du composant racine. Tous les composants non racines auront leur VCC étroitement synchronisé avec le VCC racine.
- Les propriétés de configuration de SnapLock sont définies uniquement sur la FlexGroup dans son ensemble. Les composants individuels ne peuvent pas avoir des propriétés de configuration différentes, telles que le temps de rétention par défaut et la période de validation automatique.

Prise en charge LUN

Les LUN ne sont prises en charge dans les volumes SnapLock que dans les cas où les copies Snapshot créées sur un volume non SnapLock sont transférées vers un volume SnapLock pour être protégées dans le cadre de la relation de copie SnapLock. Les LUN ne sont pas prises en charge dans les volumes SnapLock en lecture/écriture. Toutefois, les copies Snapshot inviolables sont prises en charge à la fois sur les volumes source SnapMirror et les volumes de destination qui contiennent des LUN.

Prise en charge de MetroCluster

La prise en charge de SnapLock dans les configurations MetroCluster diffère entre le mode SnapLock Compliance et le mode SnapLock Enterprise.

Conformité SnapLock

- Depuis ONTAP 9.3, la conformité SnapLock est prise en charge sur les agrégats MetroCluster sans miroir.
- Depuis ONTAP 9.3, la conformité SnapLock est prise en charge sur les agrégats en miroir, mais uniquement si l'agrégat est utilisé pour héberger les volumes du journal d'audit SnapLock.
- Les configurations SnapLock spécifiques à SVM peuvent être répliquées sur les sites principal et secondaire à l'aide de MetroCluster.

SnapLock Enterprise

- Les agrégats SnapLock Enterprise sont pris en charge depuis la version ONTAP 9.
- Depuis ONTAP 9.3, les agrégats SnapLock Enterprise avec suppression privilégiée sont pris en charge.
- Les configurations SnapLock spécifiques à SVM peuvent être répliquées vers les deux sites à l'aide de MetroCluster.

Configurations MetroCluster et horloges de conformité

Les configurations MetroCluster utilisent deux mécanismes d'horloge de conformité, l'horloge de conformité du volume (VCC) et l'horloge de conformité du système (SCC). Les VCC et SCC sont disponibles dans toutes les configurations SnapLock. Lorsque vous créez un nouveau volume sur un noeud, son VCC est initialisé avec la valeur actuelle du SCC sur ce noeud. Une fois le volume créé, la durée de rétention du volume et du fichier est toujours suivie avec le VCC.

Lorsqu'un volume est répliqué vers un autre site, son VCC est également répliqué. Lors d'un basculement de volume, du site A vers le site B, par exemple, le VCC continue d'être mis à jour sur le site B pendant que le SCC sur le site A s'arrête lorsque le site A passe hors ligne.

Lorsque le site A est remis en ligne et que le rétablissement du volume est effectué, l'horloge du site A SCC redémarre alors que le VCC du volume continue d'être mis à jour. Étant donné que le VCC est mis à jour en permanence, indépendamment des opérations de basculement et de rétablissement, les délais de conservation des fichiers ne dépendent pas des horloges SCC et ne sont pas extensibles.

Prise en charge de la vérification multiadministrateur

Depuis la version ONTAP 9.13.1, un administrateur de cluster peut explicitement activer la vérification multiadministrateur sur un cluster afin de demander l'approbation du quorum avant l'exécution de certaines opérations SnapLock. Lorsque MAV est activé, les propriétés du volume SnapLock telles que temps-conservation-défaut, temps-conservation-minimum, temps-conservation-maximum, mode-ajout-volume, période-allocation-auto et suppression-privilégiée requièrent l'approbation du quorum. En savoir plus sur ["VAM"](#).

Efficacité du stockage

Depuis la version ONTAP 9.9.1, SnapLock prend en charge les fonctionnalités d'efficacité du stockage, telles que la compaction des données, la déduplication entre les volumes et la compression adaptative pour les volumes et les agrégats SnapLock. Pour plus d'informations sur l'efficacité du stockage, voir ["Présentation de l'efficacité du stockage ONTAP"](#).

Le cryptage

ONTAP propose des technologies de cryptage logicielles et matérielles qui permettent de garantir que les données au repos ne peuvent pas être lues si le support de stockage est requalifié, perdu ou volé.

Avertissement : NetApp ne peut pas garantir que les fichiers WORM protégés par SnapLock sur des disques ou volumes à autochiffrement seront récupérables en cas de perte de la clé d'authentification ou si le nombre de tentatives d'authentification échouées dépasse la limite spécifiée et entraîne le verrouillage permanent du disque. Vous êtes responsable de vous assurer contre les échecs d'authentification.



Depuis ONTAP 9.2, les volumes chiffrés sont pris en charge sur les agrégats SnapLock.

Transition depuis la version 7-mode

Vous pouvez migrer des volumes SnapLock de 7-mode vers ONTAP à l'aide de la fonctionnalité de transition basée sur la copie de l'outil de transition 7-mode. Le mode SnapLock du volume de destination, conformité ou entreprise doit correspondre au mode SnapLock du volume source. Vous ne pouvez pas utiliser la transition sans copie pour migrer des volumes SnapLock.

Configurez SnapLock

Configurez SnapLock

Avant d'utiliser SnapLock, vous devez configurer SnapLock en exécutant diverses tâches telles que ["Installez la licence SnapLock"](#). Pour chaque nœud qui héberge un agrégat avec un volume SnapLock, initialisez le ["Horloge de conformité"](#), Créez un agrégat SnapLock pour les clusters exécutant des versions ONTAP antérieures à ONTAP 9.10.1, ["Créez et montez un volume SnapLock"](#), et plus encore.

Initialiser l'horloge de conformité

SnapLock utilise le *volume Compliance Clock* pour éviter toute altération susceptible de modifier la période de conservation des fichiers WORM. Vous devez d'abord initialiser le *système CompléanceClock* sur chaque nœud hébergeant un agrégat SnapLock.

Depuis ONTAP 9.14.1, vous pouvez initialiser ou réinitialiser l'horloge de conformité du système en l'absence de volumes SnapLock ou de volumes sur lesquels le verrouillage des copies Snapshot est activé. La possibilité de réinitialiser permet aux administrateurs système de réinitialiser l'horloge de conformité du système dans les cas où elle a été mal initialisée ou de corriger la dérive de l'horloge sur le système. Dans ONTAP 9.13.1 et les versions antérieures, une fois que vous avez initialisé l'horloge de conformité sur un nœud, vous ne pouvez pas l'initialiser à nouveau.

Avant de commencer

Pour réinitialiser l'horloge de conformité :

- Tous les nœuds du cluster doivent être en état de santé.
- Tous les volumes doivent être en ligne.
- Aucun volume ne peut être présent dans la file d'attente de récupération.
- Aucun volume SnapLock ne peut être présent.
- Aucun volume sur lequel le verrouillage des copies Snapshot est activé ne peut être présent.

Exigences générales pour l'initialisation de l'horloge de conformité :

- 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 de l'horloge de conformité du système est héritée par le *volume Compliance Clock*, qui contrôle la période de conservation des fichiers WORM sur le volume. L'horloge de conformité du volume est initialisée automatiquement lorsque vous créez un nouveau volume SnapLock.



Le réglage initial de l'horloge de conformité du système est basé sur l'horloge du système matériel actuel. C'est pourquoi vous devez vérifier que l'heure et le fuseau horaire du système sont corrects avant d'initialiser l'horloge de conformité du système sur chaque nœud. Une fois que vous avez initialisé l'horloge de conformité du système sur un nœud, vous ne pouvez plus l'initialiser lorsque des volumes SnapLock ou des volumes dont le verrouillage est activé sont présents.

Étapes

Vous pouvez utiliser l'interface de ligne de commande ONTAP pour initialiser l'horloge de conformité ou, à partir de ONTAP 9.12.1, vous pouvez utiliser System Manager pour initialiser l'horloge de conformité.

System Manager

1. Accédez à **Cluster > Présentation**.
2. Dans la section **nœuds**, 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. Initialiser l'horloge de conformité du système :

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

La commande suivante initialise l'horloge de conformité du système node1:

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

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

```
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 Compliance Clock pour un système configuré en NTP

Vous pouvez activer la fonction de synchronisation de l'heure de l'horloge de 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 les horloges de conformité du système et du volume. Une période de 24 heures est définie comme seuil d'inclinaison. Cela signifie que l'horloge de conformité du système est synchronisée sur l'horloge du système uniquement si l'inclinaison a plus d'un jour.

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

Étapes

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

```
snaplock compliance-clock ntp
```

La commande suivante active la fonction de synchronisation de l'horloge de conformité 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'horloge de conformité 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.

Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Le SnapLock ["la licence doit être installée"](#) sur le nœud. Cette licence est incluse dans ["ONTAP One"](#).
- ["L'horloge de conformité sur le 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`.

Avant de commencer

- L'agrégat SnapLock doit être en ligne.
- Vous devriez "[Vérifiez qu'une licence SnapLock est installée](#)". Si aucune licence SnapLock n'est installée sur le nœud, vous devez "[installer](#)" il. Cette licence est incluse avec "[ONTAP One](#)". Avant ONTAP One, la licence SnapLock était incluse dans le bundle sécurité et conformité. Le bundle sécurité et conformité n'est plus proposé, mais reste valide. Bien qu'ils ne soient pas encore requis, les clients existants peuvent choisir de le faire "[Passez à ONTAP One](#)".
- "[L'horloge de conformité sur le 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 dans les volumes SnapLock. Les LUN ne sont prises en charge dans les volumes SnapLock que dans les cas où les copies Snapshot créées sur un volume non SnapLock sont transférées vers un volume SnapLock pour être protégées dans le cadre de la relation de copie SnapLock. Les LUN ne sont pas prises en charge dans les volumes SnapLock en lecture/écriture. Toutefois, les copies Snapshot inviolables sont prises en charge à la fois sur les volumes source SnapMirror et les volumes de destination qui contiennent des LUN.

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 :

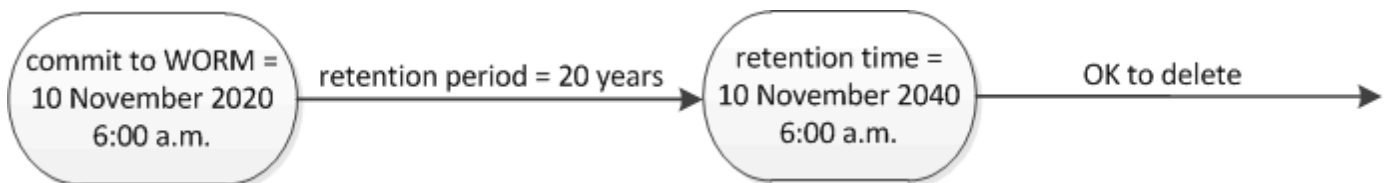
```
cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path /sales
```

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 ».

Comprendre les périodes de conservation

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 (\geq) la période de rétention minimale et inférieure ou égale à (\leq) 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

Si vous utilisez ONTAP 9.9.1 ou une version antérieure, vous devez d'abord créer un agrégat SnapLock, puis 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.

Depuis ONTAP 9.10.1, vous ne créez plus d'agrégat SnapLock. Vous devez utiliser l'option `-snaplock-type`

pour "Créer un volume SnapLock de manière explicite" En spécifiant soit conformité, soit entreprise comme type SnapLock.

Avant de commencer

Si vous utilisez ONTAP 9.9.1 ou une version antérieure, vous devez être administrateur du cluster pour créer un agrégat SnapLock.

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-log
-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-log-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 applicable), la date d'expiration du volume, etc.

Étapes

1. Générer une empreinte de fichier :

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

```
svml1::> volume file fingerprint start -vserver svml -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*

```
svml:> volume file fingerprint dump -session-id 33619976
Vserver:svml
Session-ID:33619976
Volume:slc_vol
Path:/vol/slc_vol/fl
Data
Fingerprint:MOFJVEvxNSJm3C/4Bn5oEEYH51CrudOzZYK4r5Cfylg=Metadata

Fingerprint:8iMjqJXiNcqqXT5XuRhLiEwIrJEihDmwS0hrexnjgmc=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
```

Gérer les fichiers WORM

Gérer les fichiers WORM

Vous pouvez gérer les fichiers WORM de l'une des manières suivantes :

- ["Archivage des fichiers en mode WORM"](#)
- ["Archivage des copies Snapshot sur WORM sur une destination d'archivage sécurisé"](#)
- ["Mise en miroir des fichiers WORM pour la reprise après incident"](#)
- ["Conservation des fichiers WORM en cas de litige"](#)
- ["Supprimez les fichiers WORM"](#)

Archivage des fichiers en mode WORM

Vous pouvez archiver les fichiers en mode WORM (write once, read many) manuellement ou automatiquement. Vous pouvez également créer des fichiers modifiables WORM.

Archivage manuel des fichiers en mode WORM

Vous devez valider manuellement un fichier en mode WORM en le rendant en lecture seule. Vous pouvez utiliser n'importe quelle commande ou programme approprié sur NFS ou CIFS pour changer l'attribut lecture-écriture d'un fichier en lecture seule. Vous pouvez choisir de valider manuellement les fichiers si vous voulez vous assurer qu'une application a terminé l'écriture dans un fichier de sorte que le fichier n'est pas validé prématurément ou qu'il existe des problèmes de mise à l'échelle pour le scanner à validation automatique en raison d'un nombre élevé de volumes.

Ce dont vous avez besoin

- Le fichier à valider doit résider sur un volume SnapLock.
- Le fichier doit être accessible en écriture.

Description de la tâche

L'heure de la durée de la période de conformité du volume est écrite sur le `ctime` champ du fichier lors de l'exécution de la commande ou du programme. L'heure de la fin de l'horloge détermine quand la durée de conservation du fichier a été atteinte.

Étapes

1. Utilisez une commande ou un programme approprié pour modifier l'attribut lecture-écriture d'un fichier en lecture seule.

Dans un shell UNIX, utilisez la commande suivante pour créer un fichier nommé `document.txt` lecture seule :

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

Dans un shell Windows, utilisez la commande suivante pour créer un fichier nommé `document.txt` lecture seule :

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

Archivage automatique des fichiers sur WORM

La fonctionnalité d'autovalidation de SnapLock vous permet d'allouer automatiquement les fichiers en mode WORM. La fonction `autocommit` valide un fichier à l'état WORM sur un volume SnapLock si le fichier n'a pas été modifié pendant la période `autocommit` durée. La fonction de validation automatique est désactivée par défaut.

Ce dont vous avez besoin

- Les fichiers que vous souhaitez effectuer une validation automatique doivent résider sur un volume SnapLock.
- Le volume SnapLock doit être en ligne.
- Le volume SnapLock doit être un volume en lecture/écriture.



La fonction SnapLock `autocommit` analyse tous les fichiers du volume et valide un fichier s'il répond à l'exigence d'`autocommit`. Il peut y avoir un intervalle de temps entre le moment où le fichier est prêt pour la validation automatique et celui où il est réellement engagé par le scanner SnapLock `autocommit`. Cependant, le fichier est toujours protégé contre les modifications et la suppression par le système de fichiers dès qu'il est éligible à l'auto-validation.

Description de la tâche

Le paramètre *autocommit Period* spécifie le temps pendant lequel les fichiers doivent rester inchangés avant leur validation automatique. La modification d'un fichier avant que la période de validation automatique ne soit écoulée entraîne le redémarrage de la période de validation automatique du fichier.

Le tableau suivant présente les valeurs possibles pour la période de validation automatique :

| Valeur | Unité | Remarques |
|-------------|------------------|-----------------------|
| Aucune | - | La valeur par défaut. |
| 5 - 5256000 | quelques minutes | - |
| 1 - 87600 | heures | - |
| 1 - 3650 | jours | - |

| Valeur | Unité | Remarques |
|---------|--------|-----------|
| 1 - 120 | mois | - |
| 1 - 10 | années | - |



La valeur minimale est de 5 minutes et la valeur maximale est de 10 ans.

Étapes

1. Validation automatique des fichiers sur un volume SnapLock vers WORM :

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

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

La commande suivante valide automatiquement les fichiers sur le volume `vol1` Du SVM `vs1`, tant que les fichiers restent inchangés pendant 5 heures :

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

Créez un fichier d'ajout WORM

Un fichier WORM fiable conserve les données écrites de manière incrémentielle, comme les entrées de journal. Vous pouvez utiliser n'importe quelle commande ou programme approprié pour créer un fichier compatible WORM, ou vous pouvez utiliser la fonction SnapLock *volume append mode* pour créer des fichiers compatibles WORM par défaut.

Utilisez une commande ou un programme pour créer un fichier inscriptible WORM

Vous pouvez utiliser n'importe quelle commande ou programme appropriée sur NFS ou CIFS pour créer un fichier compatible WORM. Un fichier WORM fiable conserve les données écrites de manière incrémentielle, comme les entrées de journal. Les données sont ajoutées au fichier par blocs de 256 Ko. Au fur et à mesure que chaque bloc est écrit, le bloc précédent devient protégé par WORM. Vous ne pouvez pas supprimer le fichier tant que la période de conservation n'est pas écoulée.

Ce dont vous avez besoin

Le fichier fiable WORM doit résider sur un volume SnapLock.

Description de la tâche

Les données n'ont pas besoin d'être écrites de manière séquentielle dans le bloc actif de 256 Ko. Lorsque les données sont écrites sur l'octet $n \times 256 \text{ Ko} + 1$ du fichier, le segment 256 Ko précédent devient protégé par WORM.

Toute écriture non ordonnée au-delà du bloc actif actuel de 256 Ko entraînera la réinitialisation du bloc actif de 256 Ko au dernier décalage et entraînera l'échec des écritures sur les décalages plus anciens avec une erreur du système de fichiers en lecture seule (ROFS). Les décalages d'écriture dépendent de l'application client. Un client qui n'est pas conforme à la sémantique d'écriture du fichier d'ajout WORM peut entraîner une

interruption incorrecte du contenu d'écriture. Par conséquent, il est recommandé de s'assurer que le client respecte les restrictions de décalage pour les écritures non ordonnées, ou de garantir les écritures synchrones en montant le système de fichiers en mode synchrone.

Étapes

1. Utilisez une commande ou un programme approprié pour créer un fichier de longueur nulle avec le temps de rétention souhaité.

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

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

2. Utilisez une commande ou un programme approprié pour modifier l'attribut lecture-écriture du fichier en lecture seule.

Dans un shell UNIX, utilisez la commande suivante pour créer un fichier nommé `document.txt` lecture seule :

```
chmod 444 document.txt
```

3. Utilisez une commande ou un programme approprié pour remettre l'attribut de lecture-écriture du fichier en inscriptible.



Cette étape n'est pas considérée comme un risque de conformité, car aucune donnée n'est présente dans le fichier.

Dans un shell UNIX, utilisez la commande suivante pour créer un fichier nommé `document.txt` inscriptible :

```
chmod 777 document.txt
```

4. Utilisez une commande ou un programme approprié pour commencer à écrire des données dans le fichier.

Dans un shell UNIX, utiliser la commande suivante pour écrire des données sur `document.txt`:

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



Rétablissez les autorisations de fichier en lecture seule lorsque vous n'avez plus besoin d'ajouter des données au fichier.

Utilisez le mode d'ajout de volumes pour créer des fichiers d'ajout WORM

Depuis ONTAP 9.3, vous pouvez utiliser la fonctionnalité SnapLock *volume append mode* (VAM) pour créer par défaut des fichiers WORM utilisables. Un fichier WORM fiable conserve les données écrites de manière incrémentielle, comme les entrées de journal. Les données sont ajoutées au fichier par blocs de 256 Ko. Au fur

et à mesure que chaque bloc est écrit, le bloc précédent devient protégé par WORM. Vous ne pouvez pas supprimer le fichier tant que la période de conservation n'est pas écoulée.

Ce dont vous avez besoin

- Le fichier fiable WORM doit résider sur un volume SnapLock.
- Le volume SnapLock doit être démonté et vide des copies Snapshot et des fichiers créés par l'utilisateur.

Description de la tâche

Les données n'ont pas besoin d'être écrites de manière séquentielle dans le bloc actif de 256 Ko. Lorsque les données sont écrites sur l'octet $n \times 256 \text{ Ko} + 1$ du fichier, le segment 256 Ko précédent devient protégé par WORM.

Si vous spécifiez une période de validation automatique pour le volume, les fichiers modifiables WORM qui ne sont pas modifiés pour une période supérieure à la période de validation automatique sont validés en mode WORM.



Le mode VAM n'est pas pris en charge sur les volumes des journaux d'audit SnapLock.

Étapes

1. Activer VAM :

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

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

La commande suivante active le mode VAM sur le volume `vol1` de SVM `vs1`:

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

2. Utilisez une commande ou un programme approprié pour créer des fichiers avec des autorisations d'écriture.

Les fichiers sont par défaut modifiables.

Archivage des copies Snapshot sur WORM sur une destination d'archivage sécurisé

Vous pouvez utiliser SnapLock pour SnapVault pour protéger les copies Snapshot WORM sur le stockage secondaire. Vous exécutez toutes les tâches SnapLock de base sur la destination du coffre-fort. Le volume de destination est automatiquement monté en lecture seule. Il est donc inutile de valider de manière explicite les copies Snapshot sur WORM. Ainsi, la création de copies Snapshot planifiées sur le volume de destination à l'aide des règles SnapMirror n'est pas prise en charge.

Avant de commencer

- Si vous souhaitez utiliser System Manager pour configurer la relation, les clusters source et cible doivent exécuter ONTAP 9.15.1 ou une version ultérieure.

- Sur le cluster de destination :
 - ["Installez la licence SnapLock"](#).
 - ["Initialiser l'horloge de conformité"](#).
 - Si vous utilisez l'interface de ligne de commandes avec une version de ONTAP antérieure à la version 9.10.1, ["Créer un agrégat SnapLock"](#).
- La règle de protection doit être de type « coffre-fort ».
- Les agrégats source et de destination doivent être de 64 bits.
- Le volume source ne peut pas être un volume SnapLock.
- Si vous utilisez l'interface de ligne de commandes de ONTAP, les volumes source et de destination doivent être créés dans le ["clusters de peering"](#) et ["SVM"](#).

Description de la tâche

Le volume source peut utiliser le stockage NetApp ou autre. Pour le stockage non NetApp, vous devez utiliser la virtualisation FlexArray.



Vous ne pouvez pas renommer une copie Snapshot engagée en état WORM.

Vous pouvez cloner des volumes SnapLock, mais vous ne pouvez pas cloner des fichiers sur un volume SnapLock.



Les LUN ne sont pas prises en charge dans les volumes SnapLock. Les LUN ne sont prises en charge dans les volumes SnapLock que dans les cas où les copies Snapshot créées sur un volume non SnapLock sont transférées vers un volume SnapLock pour être protégées dans le cadre de la relation de copie SnapLock. Les LUN ne sont pas prises en charge dans les volumes SnapLock en lecture/écriture. Toutefois, les copies Snapshot inviolables sont prises en charge à la fois sur les volumes source SnapMirror et les volumes de destination qui contiennent des LUN.

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. Vous pouvez utiliser l'option '-snaplock-type' du volume pour spécifier un type de volume Compliance ou Enterprise SnapLock. Dans les versions ONTAP antérieures à ONTAP 9.10.1, le mode SnapLock, conformité ou entreprise, est hérité de l'agrégat. Les volumes de destination flexibles de la version ne sont pas pris en charge. Le paramètre de langue du volume de destination doit correspondre au paramètre de langue du volume source.

Une période de conservation par défaut est affectée à un volume SnapLock cible du coffre-fort. La valeur pour cette période est initialement définie sur un minimum de 0 ans pour les volumes SnapLock Enterprise et un maximum de 30 ans pour les volumes SnapLock Compliance. À chaque copie NetApp Snapshot, toutes les copies NetApp Snapshot sont conservées pendant cette période de conservation par défaut. La période de conservation peut être prolongée ultérieurement, si nécessaire. Pour plus d'informations, voir ["Aperçu de la durée de conservation"](#).

Depuis la version ONTAP 9.14.1, vous pouvez spécifier des périodes de conservation pour des étiquettes SnapMirror spécifiques dans la règle SnapMirror de la relation SnapMirror de sorte que les copies Snapshot répliquées du volume source vers le volume de destination soient conservées pendant la période de conservation spécifiée dans la règle. Si aucune période de conservation n'est spécifiée, la période de rétention par défaut du volume de destination est utilisée.

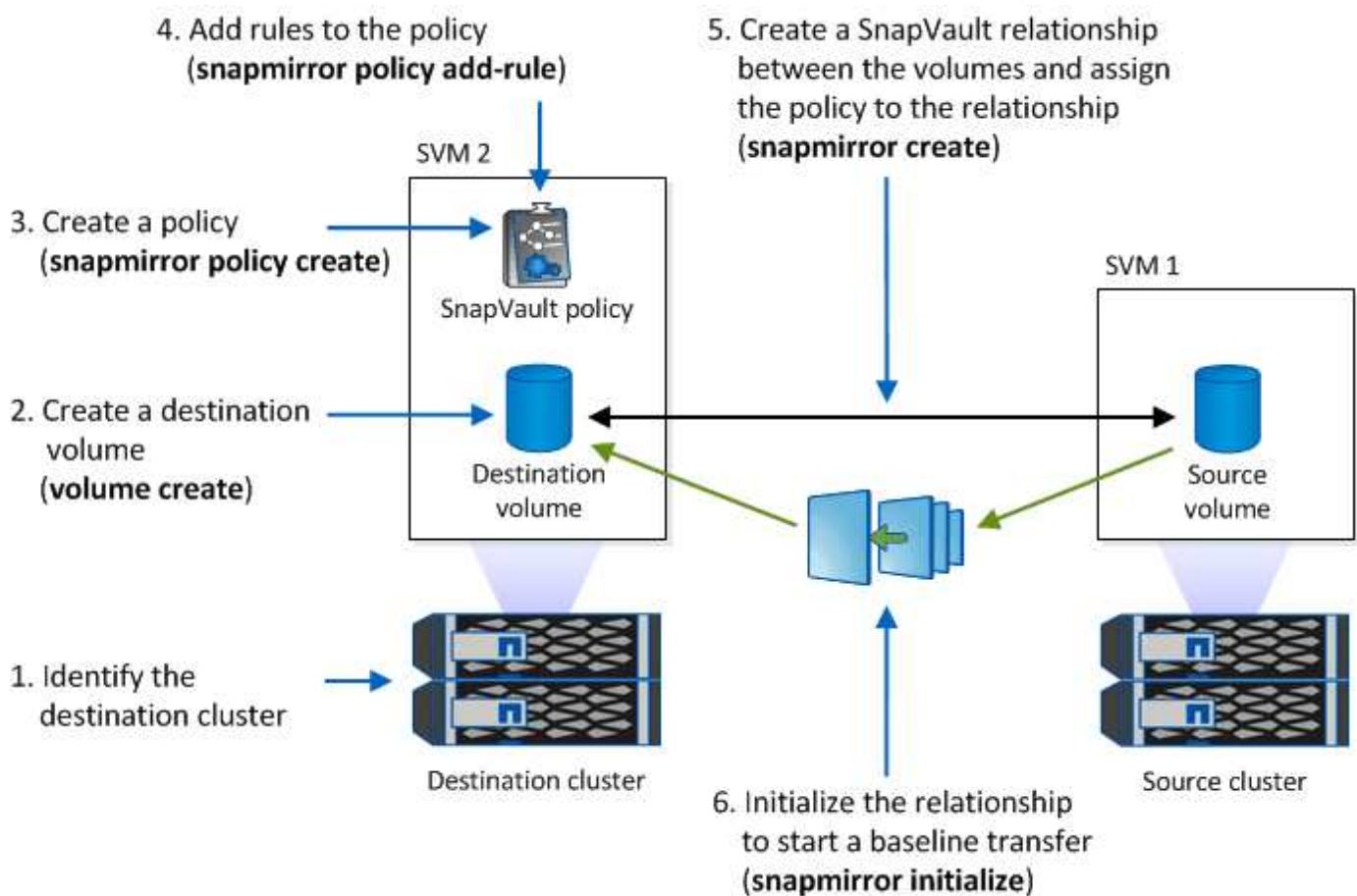
À partir de ONTAP 9.13.1, vous pouvez restaurer instantanément une copie Snapshot verrouillée sur le volume

SnapLock de destination d'une relation de copie SnapLock en créant une copie FlexClone avec `snaplock-type` Défini sur non `snaplock` et spécifiant la copie Snapshot comme « snapshot-parent » lors de l'exécution de l'opération de création du clone de volume. En savoir plus sur "[Création d'un volume FlexClone avec un type SnapLock](#)".

Pour les configurations MetroCluster, il est important de connaître les éléments suivants :

- Vous pouvez créer une relation SnapVault uniquement entre des SVM source synchrone, et non entre un SVM source synchrone et une SVM de destination synchrone.
- Vous pouvez créer une relation SnapVault depuis un volume d'un SVM source synchrone vers une SVM transmettant les données.
- Vous pouvez créer une relation SnapVault depuis un volume d'une SVM diffusant les données vers un volume DP au sein d'un SVM source synchrone.

L'illustration suivante montre la procédure d'initialisation d'une relation de coffre-fort SnapLock :



Étapes

Vous pouvez utiliser l'interface de ligne de commandes ONTAP pour créer une relation de copie SnapLock ou, à partir de ONTAP 9.15.1, vous pouvez utiliser System Manager pour créer une relation de copie SnapLock.

System Manager

1. Naviguez jusqu'à **stockage > volumes** et sélectionnez **Ajouter**.
2. Dans la fenêtre **Ajouter un volume**, choisissez **plus d'options**.
3. Entrez le nom du volume, sa taille, la règle d'export et le nom du partage.
4. Sélectionnez **Verrouiller les instantanés de destination pour empêcher la suppression**, et dans la section **méthode de verrouillage**, choisissez **SnapLock pour SnapVault**. Cette sélection ne s'affiche pas si le type de stratégie sélectionné n'est pas de type « coffre-fort », si la licence SnapLock n'est pas installée ou si l'horloge de conformité n'est pas initialisée.
5. S'il n'est pas déjà activé, sélectionnez **initialiser horloge de conformité SnapLock**.
6. Enregistrez les modifications.

CLI

1. Sur le cluster de destination, créez un volume de destination SnapLock de type DP taille identique ou supérieure à celle du volume source :

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

La commande suivante crée un volume SnapLock Compliance de 2 Go nommé `dstvolB` dans `SVM2` sur l'agrégat `node01_aggr`:

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

2. Sur le cluster de destination, "[définissez la période de conservation par défaut](#)".
3. "[Créer une nouvelle relation de réplication](#)" Entre la source non SnapLock et la nouvelle destination SnapLock que vous avez créée.

Dans cet exemple, une nouvelle relation SnapMirror est créée avec un volume SnapLock de destination `dstvolB` à l'aide d'une règle de `XDPDefault` Pour archiver les copies Snapshot étiquetées tous les jours et toutes les semaines selon une planification horaire :

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



"[Création d'une règle de réplication personnalisée](#)" ou un "[planification personnalisée](#)" si les valeurs par défaut disponibles ne sont pas appropriées.

4. Sur le SVM de destination, initialiser la relation SnapVault créée :

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

La commande suivante initialise la relation entre le volume source `srcvolA` marche SVM1 et le volume de destination `dstvolB` marche SVM2:

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

5. Une fois la relation initialisée et inactive, utilisez le `snapshot show` Sur le volume de destination afin de vérifier l'heure d'expiration du SnapLock appliquée aux copies Snapshot répliquées.

Cet exemple répertorie les copies Snapshot sur le volume `dstvolB` Étiquette SnapMirror et date d'expiration du SnapLock :

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

Informations associées

["Cluster et SVM peering"](#)

["Sauvegarde de volume avec SnapVault"](#)

Mise en miroir des fichiers WORM pour la reprise après incident

Vous pouvez utiliser SnapMirror pour répliquer des fichiers WORM dans un autre emplacement géographique à des fins autres que la reprise après incident. Le volume source et le volume de destination doivent être configurés pour SnapLock et les deux volumes doivent disposer du même mode SnapLock, Compliance ou Enterprise. Toutes les propriétés SnapLock clés du volume et les fichiers sont répliqués.

Prérequis

Les volumes source et destination doivent être créés dans des clusters associés avec des SVM peering. Pour plus d'informations, voir ["Cluster et SVM peering"](#).

Description de la tâche

- Depuis ONTAP 9.5, vous pouvez répliquer les fichiers WORM avec la relation SnapMirror de type XDP (protection étendue des données) plutôt qu'avec la relation de type DP (protection des données). Le mode XDP ne dépend pas de la version d'ONTAP. Il peut donc différencier les fichiers stockés dans le même bloc, ce qui facilite la resynchronisation des volumes du mode Compliance répliqué. Pour plus d'informations sur la conversion d'une relation de type DP existante en relation de type XDP, reportez-vous à ["La protection des données"](#).
- Une opération de resynchronisation dans une relation SnapMirror de type DP échoue pour un volume en mode conformité si SnapLock détermine qu'elle entraînera une perte de données. Si une opération de resynchronisation échoue, vous pouvez utiliser le `volume clone create` commande pour créer un clone du volume de destination. Vous pouvez ensuite resynchroniser le volume source avec le clone.
- Une relation SnapMirror de type XDP entre des volumes compatibles SnapLock prend en charge une resynchronisation après une interruption, même si les données de la destination ont divergé de la source après l'arrêt.

Lors d'une resynchronisation, lorsque des divergences de données sont détectées entre la source et la destination au-delà du snapshot commun, un nouvel instantané est coupé sur la destination pour capturer cette divergence. Le nouvel instantané et le snapshot commun sont tous deux verrouillés avec un temps de rétention comme suit :

- Heure d'expiration du volume de la destination
- Si le délai d'expiration du volume est passé ou n'a pas été défini, le snapshot est verrouillé pendant une période de 30 jours
- Si la destination a des raisons juridiques, la période d'expiration réelle du volume est masquée et apparaît comme « indéfinie » ; cependant, l'instantané est verrouillé pendant la durée de la période d'expiration réelle du volume.

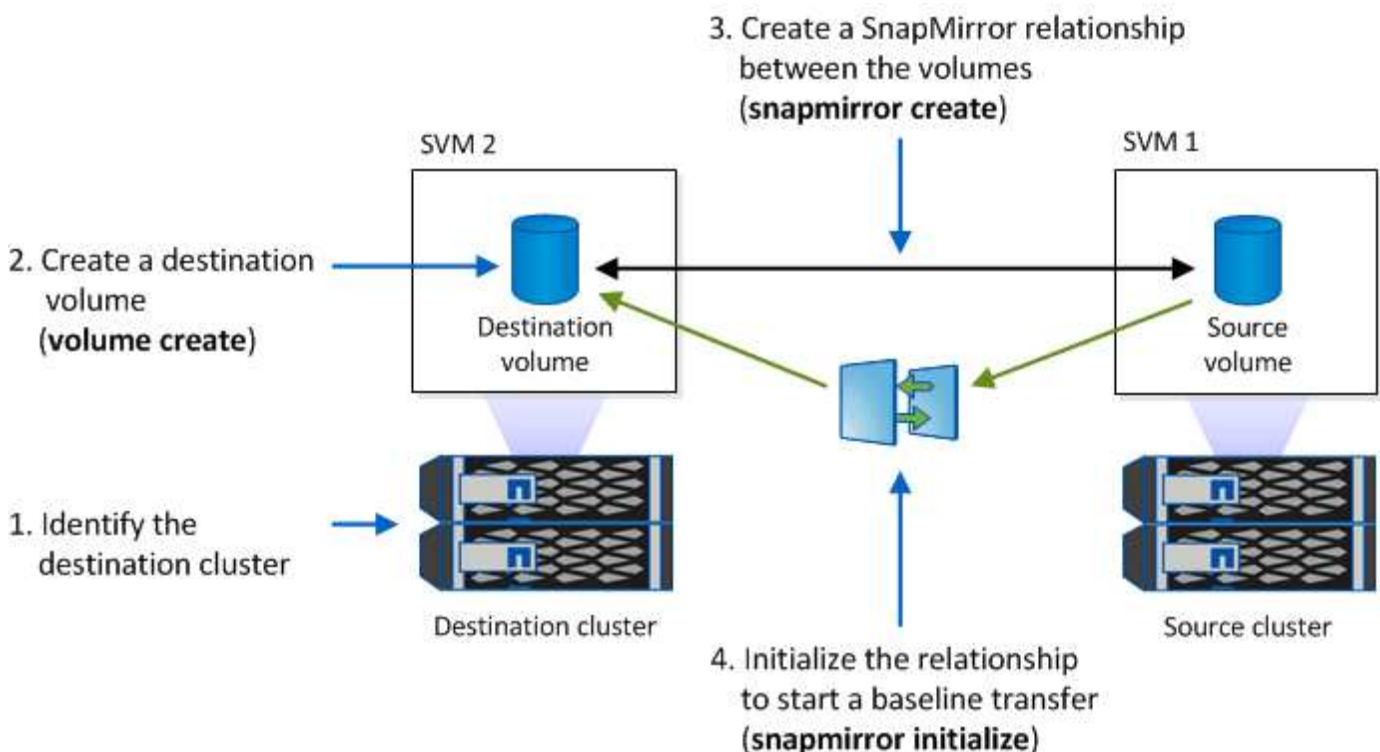
Si le volume de destination a une période d'expiration postérieure à la source, la période d'expiration de destination est conservée et ne sera pas écrasée par la période d'expiration du volume source après la resynchronisation.

Si la destination dispose de mentions légales qui diffèrent de la source, une resynchronisation n'est pas autorisée. La source et la destination doivent disposer de mentions légales identiques ou toutes les mentions légales de la destination doivent être libérées avant toute tentative de resynchronisation.

Une copie Snapshot verrouillée sur le volume de destination créé pour capturer les données divergentes peut être copiée vers la source à l'aide de la CLI en exécutant le `snapmirror update -s snapshot` commande. Une fois copié, le snapshot reste également verrouillé à la source.

- Les relations de protection des données des SVM ne sont pas prises en charge.
- Les relations de protection des données de partage de charge ne sont pas prises en charge.


L'illustration suivante montre la procédure d'initialisation d'une relation SnapMirror :



System Manager

Depuis ONTAP 9.12.1, System Manager vous permet de configurer la réplication SnapMirror des fichiers WORM.

Étapes

1. Accédez à **Storage > volumes**.
2. Cliquez sur **Afficher/Masquer** et sélectionnez **Type SnapLock** pour afficher la colonne dans la fenêtre **volumes**.
3. Recherchez un volume SnapLock.
4. Cliquez sur  et sélectionnez **protéger**.
5. Choisir le cluster de destination et la VM de stockage de destination
6. Cliquez sur **plus d'options**.
7. Sélectionnez **Afficher les règles héritées** et **DPDefault (TDA/TDE/s)**.
8. Dans la section **Détails de configuration de destination**, sélectionnez **remplacer le programme de transfert** et sélectionnez **horaire**.
9. Cliquez sur **Enregistrer**.
10. À gauche du nom du volume source, cliquez sur la flèche pour développer les détails du volume, puis, à droite de la page, consultez les informations relatives à la protection SnapMirror distante.
11. Sur le cluster distant, accédez à **protection relations**.
12. Localisez la relation et cliquez sur le nom du volume de destination pour afficher les détails de la relation.
13. Vérifiez que le type de SnapLock du volume de destination et d'autres informations SnapLock.

CLI

1. Identifier le cluster de destination
2. Sur le cluster de destination, "[Installez la licence SnapLock](#)", "[Initialiser l'horloge de conformité](#)", Et, si vous utilisez une version de ONTAP antérieure à 9.10.1, "[Créer un agrégat SnapLock](#)".
3. Sur le cluster de destination, créez un volume de destination SnapLock de type DP taille identique ou supérieure à celle du volume source :

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



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. Utilisez l'option `volume -snaplock-type` pour spécifier un type de volume Compliance ou Enterprise SnapLock. Dans les versions ONTAP antérieures à ONTAP 9.10.1, le mode SnapLock—Compliance ou Enterprise—est hérité de l'agrégat. Les volumes de destination flexibles de la version ne sont pas pris en charge. Le paramètre de langue du volume de destination doit correspondre au paramètre de langue du volume source.

La commande suivante crée un SnapLock de 2 Go Compliance volume nommé `dstvolB` dans SVM2 sur l'agrégat `node01_aggr`:

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

4. Sur le SVM de destination, créer une règle SnapMirror :

```
snapmirror policy create -vserver SVM_name -policy policy_name
```

La commande suivante crée la politique au niveau du SVM SVM1-mirror:

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

5. Sur le SVM de destination, créer une planification SnapMirror :

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

La commande suivante crée une planification SnapMirror nommée weekendcron:

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

6. Sur le SVM de destination, créer une relation SnapMirror :

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

La commande suivante crée une relation SnapMirror entre le volume source srcvolA marche SVM1 et le volume de destination dstvolB marche SVM2, et affecte la stratégie SVM1-mirror et le planning weekendcron:

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



Le type XDP est disponible dans ONTAP 9.5 et versions ultérieures. Vous devez utiliser le type DP dans ONTAP 9.4 et versions antérieures.

7. Sur le SVM de destination, initialiser la relation SnapMirror :

```
snapmirror initialize -destination-path destination_path
```

Le processus d'initialisation effectue un transfert *baseline* vers le volume de destination. SnapMirror effectue une copie Snapshot du volume source, puis transfère la copie ainsi que tous les blocs de données qu'il renvoie au volume de destination. Il transfère également toutes les autres copies Snapshot du volume source vers le volume de destination.

La commande suivante initialise la relation entre le volume source `srcvolA` marche SVM1 et le volume de destination `dstvolB` marche SVM2:

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

Informations associées

["Cluster et SVM peering"](#)

["Préparation de la reprise après incident de volume"](#)

["Protection des données"](#)

Conservation des fichiers WORM en cas de litiges avec la conservation légale

À partir de ONTAP 9.3, vous pouvez conserver des fichiers WORM en mode conformité pendant la durée d'un litige en utilisant la fonction *Legal Hold*.

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

Un fichier placé dans une mise en attente légale se comporte comme un fichier WORM ayant une période de conservation indéfinie. Il est de votre responsabilité de préciser à quel moment la période de conservation légale prend fin.

Le nombre de fichiers que vous pouvez placer sous conservation légale dépend de l'espace disponible sur le volume.

Étapes

1. Démarrer une mise en garde légale :

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

La commande suivante démarre une mise en attente légale pour tous les fichiers dans `vol1`:

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

2. Mettre fin à l'attente légale :

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

La commande suivante met fin à la mise en attente légale de tous les fichiers dans voll:

```
cluster1::>snaplock legal-hold end -litigation-name litigation1 -volume  
voll1 -path /
```

Vue d'ensemble de la suppression des fichiers WORM

Vous pouvez supprimer des fichiers WORM en mode entreprise pendant la période de conservation à l'aide de la fonction de suppression privilégiée. Avant de pouvoir utiliser cette fonction, vous devez créer un compte administrateur SnapLock, puis activer la fonction à l'aide du compte.

Créez un compte d'administrateur SnapLock

Vous devez disposer des privilèges d'administrateur SnapLock pour effectuer une suppression privilégiée. Ces privilèges sont définis dans le rôle vsadmin-snaplock. Si ce rôle n'est pas encore attribué, vous pouvez demander à l'administrateur du cluster de créer un compte d'administrateur SVM avec le rôle d'administrateur SnapLock.

Ce dont vous avez besoin

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Vous devez vous connecter à une connexion sécurisée (SSH, console ou ZAPI).

Étapes

1. Créer un compte administrateur SVM avec le rôle d'administrateur SnapLock :

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

La commande suivante active le compte d'administrateur du SVM SnapLockAdmin avec le prédéfini vsadmin-snaplock rôle d'accès SVM1 utilisation d'un mot de passe :

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

Activer la fonction de suppression privilégiée

Vous devez activer explicitement la fonction de suppression privilégiée sur le volume entreprise contenant les fichiers WORM que vous souhaitez supprimer.

Description de la tâche

La valeur du `-privileged-delete` détermine si la suppression privilégiée est activée. Les valeurs possibles sont `enabled`, `disabled`, et `permanently-disabled`.



`permanently-disabled` est l'état du terminal. Vous ne pouvez pas activer la suppression privilégiée sur le volume après avoir défini l'état sur `permanently-disabled`.

Étapes

1. Activer la suppression privilégiée pour un volume SnapLock Enterprise :

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

La commande suivante active la fonction de suppression privilégiée pour le volume entreprise dataVol marche SVM1:

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

Supprimez les fichiers WORM en mode entreprise

Vous pouvez utiliser la fonction de suppression privilégiée pour supprimer des fichiers WORM en mode entreprise pendant la période de conservation.

Ce dont vous avez besoin

- Vous devez être un administrateur SnapLock pour effectuer cette tâche.
- Vous devez avoir créé un journal d'audit SnapLock et activé la fonctionnalité de suppression privilégiée sur le volume entreprise.

Description de la tâche

Vous ne pouvez pas utiliser une opération de suppression privilégiée pour supprimer un fichier WORM expiré. Vous pouvez utiliser le `volume file retention show` Commande pour afficher la durée de conservation du fichier WORM que vous souhaitez supprimer. Pour plus d'informations, consultez la page man de la commande

Étape

1. Supprimez un fichier WORM sur un volume d'entreprise :

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

La commande suivante supprime le fichier /vol/dataVol/f1 Sur le SVM SVM1:

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

Déplacer un volume SnapLock

Depuis ONTAP 9.8, vous pouvez déplacer un volume SnapLock vers un agrégat de

destination du même type (entreprise vers entreprise ou conformité vers conformité). Vous devez avoir le rôle de sécurité SnapLock pour déplacer un volume SnapLock.

Créez un compte administrateur de sécurité SnapLock

Pour effectuer un déplacement de volume SnapLock, vous devez disposer des privilèges administrateur de sécurité SnapLock. Ce privilège vous est accordé avec le rôle *SnapLock*, introduit dans ONTAP 9.8. Si ce rôle n'est pas encore attribué, vous pouvez demander à votre administrateur de cluster de créer un utilisateur de sécurité SnapLock avec ce rôle de sécurité SnapLock.

Ce dont vous avez besoin

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Vous devez vous connecter à une connexion sécurisée (SSH, console ou ZAPI).

Description de la tâche

Le rôle SnapLock est associé au SVM admin, contrairement au rôle vsadmin-snaplock, qui est associé au SVM de données.

Étape

1. Créer un compte administrateur SVM avec le rôle d'administrateur SnapLock :

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

La commande suivante active le compte d'administrateur du SVM SnapLockAdmin avec le prédéfini snaplock Rôle permettant d'accéder à la SVM d'admin cluster1 utilisation d'un mot de passe :

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

Déplacer un volume SnapLock

Vous pouvez utiliser le `volume move` Commande de déplacement d'un volume SnapLock vers un agrégat de destination.

Ce dont vous avez besoin

- Vous devez avoir créé un journal d'audit protégé SnapLock avant d'effectuer le déplacement de volume SnapLock.

["Créer un journal d'audit"](#).

- Si vous utilisez une version de ONTAP antérieure à ONTAP 9.10.1, l'agrégat de destination doit être du même type SnapLock que le volume SnapLock que vous souhaitez déplacer : conformité à la conformité ou entreprise à la norme. Depuis ONTAP 9.10.1, cette restriction est supprimée et un agrégat peut inclure des volumes Compliance et Enterprise SnapLock, ainsi que des volumes non SnapLock.
- Vous devez être un utilisateur ayant le rôle de sécurité SnapLock.

Étapes

1. Via une connexion sécurisée, connectez-vous à la LIF de gestion du cluster ONTAP :

```
ssh snaplock_user@cluster_mgmt_ip
```

2. Déplacer un volume SnapLock :

```
volume move start -vserver SVM_name -volume SnapLock_volume_name -destination  
-aggregate destination_aggregate_name
```

3. Vérifier l'état de l'opération de déplacement de volume :

```
volume move show -volume SnapLock_volume_name -vserver SVM_name -fields  
volume,phase,vserver
```

Verrouiller une copie Snapshot pour assurer la protection contre les attaques par ransomware

Depuis ONTAP 9.12.1, vous pouvez verrouiller une copie Snapshot sur un volume non SnapLock pour vous protéger des attaques par ransomware. Le verrouillage des copies Snapshot permet de ne pas les supprimer accidentellement ou accidentellement.

La fonction horloge de conformité de SnapLock vous permet de verrouiller les copies Snapshot pendant une période spécifiée, de sorte qu'elles ne puissent pas être supprimées tant que l'heure d'expiration n'est pas atteinte. Le verrouillage des copies Snapshot est inviolable, ce qui les protège contre les menaces de ransomware. Vous pouvez utiliser des copies Snapshot verrouillées pour récupérer des données si un volume est compromis par une attaque par ransomware.

À partir de la version ONTAP 9.14.1, le verrouillage des copies Snapshot prend en charge les copies Snapshot à conservation à long terme sur les destinations des coffres-forts SnapLock et sur les volumes de destination SnapMirror non SnapLock. Le verrouillage des copies Snapshot est activé en définissant la période de conservation à l'aide des règles de règles SnapMirror associées à un [libellé de police existant](#). La règle remplace la période de rétention par défaut définie sur le volume. Si aucune période de conservation n'est associée au label SnapMirror, la période de conservation par défaut du volume est utilisée.

Exigences et considérations relatives à la non-conformité des copies Snapshot

- Si vous utilisez l'interface de ligne de commandes ONTAP, tous les nœuds du cluster doivent exécuter ONTAP 9.12.1 ou une version ultérieure. Si vous utilisez System Manager, tous les nœuds doivent exécuter ONTAP 9.13.1 ou une version ultérieure.
- ["La licence SnapLock doit être installée sur le cluster"](#). Cette licence est incluse dans ["ONTAP One"](#).
- ["L'horloge de conformité du cluster doit être initialisée"](#).
- Lorsque le verrouillage Snapshot est activé sur un volume, vous pouvez mettre à niveau les clusters vers une version d'ONTAP ultérieure à ONTAP 9.12.1 ; Cependant, vous ne pouvez pas revenir à une version antérieure de ONTAP tant que toutes les copies Snapshot verrouillées n'ont pas atteint leur date d'expiration. Elles sont supprimées et le verrouillage des copies Snapshot est désactivé.
- Lorsqu'un snapshot est verrouillé, la durée d'expiration du volume est définie sur la date d'expiration de la copie Snapshot. Si plusieurs copies Snapshot sont verrouillées, la date d'expiration du volume reflète la date d'expiration la plus élevée parmi toutes les copies Snapshot.
- La période de conservation des copies Snapshot verrouillées est prioritaire sur le nombre de copies Snapshot conservées. En d'autres termes, la limite de conservation des copies Snapshot n'est pas

respectée si la période de conservation des copies Snapshot verrouillées n'a pas expiré.

- Dans une relation SnapMirror, vous pouvez définir une période de conservation sur une règle de stratégie de copie en miroir et la période de conservation est appliquée aux copies Snapshot répliquées vers la destination si le volume de destination est activé pour le verrouillage des copies Snapshot. La période de conservation est prioritaire sur le nombre de copies. Par exemple, les copies Snapshot qui n'ont pas dépassé leur expiration seront conservées même si le nombre de copies à conserver est dépassé.
- Vous pouvez renommer une copie Snapshot sur un volume non SnapLock. Les opérations de renommage de snapshot sur le volume principal d'une relation SnapMirror sont reflétées sur le volume secondaire uniquement si la règle est MirrorAllsnapshots. Pour les autres types de règles, la copie Snapshot renommée n'est pas propagée lors des mises à jour.
- Si vous utilisez l'interface de ligne de commandes de ONTAP, vous pouvez restaurer une copie Snapshot verrouillée avec `volume snapshot restore` Commande uniquement si la copie Snapshot verrouillée est la plus récente. Si des copies Snapshot non expirées sont présentes dans la suite de la restauration, l'opération de restauration de copie Snapshot échoue.

Fonctionnalités prises en charge par les copies Snapshot inviolables

- ["Cloud Volumes ONTAP"](#)
- Volumes FlexGroup

Le verrouillage des copies Snapshot est pris en charge sur les volumes FlexGroup. Le verrouillage des snapshots n'a lieu que sur la copie Snapshot du composant racine. La suppression du volume FlexGroup n'est autorisée que si la durée d'expiration du composant racine est passée.

- Conversion FlexVol en FlexGroup

Vous pouvez convertir un volume FlexVol avec des copies Snapshot verrouillées en un volume FlexGroup. Les copies Snapshot restent verrouillées après la conversion.

- Clone de volume et de fichiers

Vous pouvez créer des clones de volumes et de fichiers à partir d'une copie Snapshot verrouillée.

Fonctions non prises en charge

Les fonctionnalités suivantes ne sont actuellement pas prises en charge par les copies Snapshot inviolables :

- Groupes de cohérence
- FabricPool
- Volumes FlexCache
- Bande SMtape
- Synchronisation active SnapMirror
- Règle SnapMirror utilisant le `-schedule` paramètre
- SnapMirror synchrone
- Mobilité des données des SVM (utilisé pour la migration ou le déplacement d'un SVM d'un cluster source vers un cluster destination)

Activez le verrouillage des copies Snapshot lors de la création d'un volume

Depuis ONTAP 9.12.1, vous pouvez activer le verrouillage des copies Snapshot lorsque vous créez un

nouveau volume ou que vous modifiez un volume existant à l'aide du `-snapshot-locking-enabled` avec le `volume create` et `volume modify` Dans l'interface de ligne de commande. Depuis la version ONTAP 9.13.1, System Manager permet le verrouillage des copies Snapshot.

System Manager

1. Naviguez jusqu'à **stockage > volumes** et sélectionnez **Ajouter**.
2. Dans la fenêtre **Ajouter un volume**, choisissez **plus d'options**.
3. Entrez le nom du volume, sa taille, la règle d'export et le nom du partage.
4. Sélectionnez **Activer le verrouillage des instantanés**. Cette sélection ne s'affiche pas si la licence SnapLock n'est pas installée.
5. S'il n'est pas déjà activé, sélectionnez **initialiser horloge de conformité SnapLock**.
6. Enregistrez les modifications.
7. Dans la fenêtre **volumes**, sélectionnez le volume que vous avez mis à jour et choisissez **vue d'ensemble**.
8. Vérifiez que **SnapLock snapshot Copy Locking** affiche **enabled**.

CLI

1. Pour créer un nouveau volume et activer le verrouillage des copies Snapshot, entrez la commande suivante :

```
volume create -vserver vs1 -volume vol1 -snapshot-locking-enabled true
```

La commande suivante permet de verrouiller les copies Snapshot sur un nouveau volume nommé vol1 :

```
> 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
```

Activez le verrouillage des copies Snapshot sur un volume existant

Depuis la version ONTAP 9.12.1, vous pouvez activer le verrouillage des copies Snapshot sur un volume existant à l'aide de l'interface de ligne de commande ONTAP. Depuis ONTAP 9.13.1, vous pouvez utiliser System Manager pour activer le verrouillage des copies Snapshot sur un volume existant.

System Manager

1. Accédez à **Storage > volumes**.
2. Sélectionnez  et choisissez **Modifier > Volume**.
3. Dans la fenêtre **Modifier le volume**, localisez la section Paramètres des copies Snapshot (local) et sélectionnez **Activer le verrouillage des instantanés**.

Cette sélection ne s'affiche pas si la licence SnapLock n'est pas installée.

4. S'il n'est pas déjà activé, sélectionnez **initialiser horloge de conformité SnapLock**.
5. Enregistrez les modifications.
6. Dans la fenêtre **volumes**, sélectionnez le volume que vous avez mis à jour et choisissez **vue d'ensemble**.
7. Vérifiez que **SnapLock snapshot Copy Locking** affiche **enabled**.

CLI

1. Pour modifier un volume existant afin d'activer le verrouillage des copies Snapshot, entrez la commande suivante :

```
volume modify -vserver vserver_name -volume volume_name -snapshot-locking  
-enabled true
```

Créez une règle de copie Snapshot verrouillée et appliquez la conservation

Depuis ONTAP 9.12.1, vous pouvez créer des règles de copie Snapshot pour appliquer une période de conservation de copies Snapshot et appliquer la règle à un volume afin de verrouiller les copies Snapshot pour la période spécifiée. Vous pouvez également verrouiller une copie Snapshot en définissant manuellement une période de conservation. Depuis ONTAP 9.13.1, System Manager permet de créer des règles de verrouillage des copies Snapshot et de les appliquer à un volume.

Créer une règle de verrouillage des copies Snapshot

System Manager

1. Accédez à **Storage > Storage VM** et sélectionnez une VM de stockage.
2. Sélectionnez **Paramètres**.
3. Localisez **stratégies d'instantanés** et sélectionnez ➔.
4. Dans la fenêtre **Ajouter une stratégie d'instantanés**, entrez le nom de la stratégie.
5. Sélectionnez **+ Add**.
6. Fournissez les détails de la planification de la copie Snapshot, notamment le nom de la planification, le nombre maximal de copies Snapshot à conserver et la période de conservation SnapLock.
7. Dans la colonne **SnapLock Retention Period**, entrez le nombre d'heures, de jours, de mois ou d'années pour conserver les copies instantanées. Par exemple, une règle de copie Snapshot avec une période de conservation de 5 jours verrouille une copie Snapshot pendant 5 jours à compter de sa création. Elle ne peut pas être supprimée pendant cette période. Les périodes de conservation suivantes sont prises en charge :
 - Années: 0 - 100
 - Mois: 0 - 1200
 - Jours: 0 - 36500
 - Heures: 0 - 24
8. Enregistrez les modifications.

CLI

1. Pour créer une règle de copie Snapshot, entrez la commande suivante :

```
volume snapshot policy create -policy policy_name -enabled true -schedule1  
schedule1_name -count1 maximum_Snapshot_copies -retention-period1  
_retention_period
```


La commande suivante crée une règle de verrouillage des copies Snapshot :

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

Une copie Snapshot n'est pas remplacée si la conservation est active ; autrement dit, le nombre de conservation n'est pas respecté si des copies Snapshot verrouillées n'ont pas encore expiré.

Application d'une politique de verrouillage à un volume

System Manager

1. Accédez à **Storage > volumes**.
2. Sélectionnez  et choisissez **Modifier > Volume**.
3. Dans la fenêtre **Edit Volume**, sélectionnez **Schedule Snapshot copies**.
4. Sélectionnez la règle de verrouillage des copies Snapshot dans la liste.
5. Si le verrouillage des copies Snapshot n'est pas déjà activé, sélectionnez **Activer le verrouillage des instantanés**.
6. Enregistrez les modifications.

CLI

1. Pour appliquer une règle de verrouillage des copies Snapshot à un volume existant, entrez la commande suivante :

```
volume modify -volume volume_name -vserver vserver_name -snapshot-policy  
policy_name
```

Appliquez une période de conservation à la création manuelle de copies Snapshot

Vous pouvez appliquer une période de conservation des copies Snapshot lorsque vous créez manuellement une copie Snapshot. Le verrouillage des copies Snapshot doit être activé sur le volume ; sinon, le paramètre de période de conservation est ignoré.

System Manager

1. Accédez à **stockage > volumes** et sélectionnez un volume.
2. Dans la page de détails du volume, sélectionnez l'onglet **copies Snapshot**.
3. Sélectionnez **+ Add**.
4. Indiquez le nom de la copie Snapshot et la date d'expiration du SnapLock. Vous pouvez sélectionner le calendrier pour choisir la date et l'heure d'expiration de la conservation.
5. Enregistrez les modifications.
6. Sur la page **volumes > copies instantanées**, sélectionnez **Afficher/Masquer** et choisissez **SnapLock expiration Time** pour afficher la colonne **SnapLock expiration Time** et vérifier que la durée de conservation est définie.

CLI

1. Pour créer une copie Snapshot manuellement et appliquer une période de conservation de verrouillage, entrez la commande suivante :


```
volume snapshot create -volume volume_name -snapshot snapshot_copy_name
-snaplock-expiry-time expiration_date_time
```

La commande suivante crée une nouvelle copie Snapshot et définit la période de conservation :

```
cluster1> volume snapshot create -vserver vs1 -volume voll -snapshot
snap1 -snaplock-expiry-time "11/10/2022 09:00:00"
```

Appliquez une période de conservation à une copie Snapshot existante

System Manager

1. Accédez à **stockage > volumes** et sélectionnez un volume.
2. Dans la page de détails du volume, sélectionnez l'onglet **copies Snapshot**.
3. Sélectionnez la copie snapshot, sélectionnez , puis choisissez **Modifier le délai d'expiration SnapLock**. Vous pouvez sélectionner le calendrier pour choisir la date et l'heure d'expiration de la conservation.
4. Enregistrez les modifications.
5. Sur la page **volumes > copies instantanées**, sélectionnez **Afficher/Masquer** et choisissez **SnapLock expiration Time** pour afficher la colonne **SnapLock expiration Time** et vérifier que la durée de conservation est définie.

CLI

1. Pour appliquer manuellement une période de conservation à une copie Snapshot existante, entrez la commande suivante :

```
volume snapshot modify-snaplock-expiry-time -volume volume_name -snapshot snapshot_copy_name -expiry-time expiration_date_time
```

L'exemple suivant applique une période de conservation à une copie Snapshot existante :

```
cluster1> volume snapshot modify-snaplock-expiry-time -volume vol1  
-snapshot snap2 -expiry-time "11/10/2022 09:00:00"
```

Modifiez une stratégie existante pour appliquer la conservation à long terme

Depuis la version ONTAP 9.14.1, vous pouvez modifier une règle SnapMirror existante en ajoutant une règle afin de définir la conservation à long terme des copies Snapshot. La règle permet de remplacer la période de conservation par défaut du volume sur les destinations du coffre-fort SnapLock et sur les volumes de destination non SnapLock SnapMirror.

1. Ajouter une règle à une règle SnapMirror existante :

```
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]
```

L'exemple suivant crée une règle qui applique une période de rétention de 6 mois à la stratégie existante appelée « lockvault » :

```
snapmirror policy add-rule -vserver vs1 -policy lockvault -snapmirror  
-label test1 -keep 10 -retention-period "6 months"
```

Les API SnapLock

Vous pouvez utiliser les API Zephyr pour intégrer la fonctionnalité SnapLock dans les scripts ou l'automatisation des flux de travail. Les API utilisent la messagerie XML via HTTP, HTTPS et Windows DCE/RPC. Pour plus d'informations, voir "[Documentation sur l'automatisation ONTAP](#)".

abandon-empreinte-fichier

Annuler une opération d'empreinte digitale de fichier.

fichier-empreinte-dump

Affiche les informations relatives aux empreintes digitales du fichier.

fichier-empreinte-get-iter

Affiche l'état des opérations d'empreinte des fichiers.

démarrage de fichier-empreinte-fichier

Générez une empreinte de fichier.

snaplock-archive-vserver-log

Archivez le fichier journal d'audit actif.

snaplock-create-vserver-log

Créer une configuration de journal d'audit pour un SVM.

snaplock-delete-vserver-log

Supprime une configuration du journal d'audit pour une SVM.

snaplock-file-privileged-delete

Exécutez une opération de suppression privilégiée.

snaplock-get-file-retention

Obtenir la période de conservation d'un fichier.

snaplock-get-node-conformité-clock

Obtenir la date et l'heure de la fin de l'horloge du nœud.

snaplock-get-vserver-active-log-files-iter

Affiche l'état des fichiers journaux actifs.

snaplock-get-vserver-log-iter

Afficher la configuration du journal d'audit.

snaplock-modify-vserver-log

Modifier la configuration du journal d'audit d'un SVM

snaplock-set-file-conservation

Définissez la durée de conservation d'un fichier.

snaplock-set-node-compliance-clock

Définissez la date et l'heure de la fin de l'horloge du nœud.

snaplock-volume-set-privileged-delete

Définissez l'option Privileged-delete sur un volume SnapLock Enterprise.

volumes-get-snaplock-attrs

Obtenir les attributs d'un volume SnapLock.

volume-set-snaplock-attrs

Définissez les attributs d'un volume SnapLock.

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.