



# Gérer les fichiers WORM

## ONTAP 9

NetApp  
April 24, 2024

# Sommaire

- Gérer les fichiers WORM ..... 1
  - Gérer les fichiers WORM ..... 1
  - Archivage des fichiers en mode WORM ..... 1
  - Archivage des copies Snapshot sur WORM sur une destination d'archivage sécurisé..... 5
  - Mise en miroir des fichiers WORM pour la reprise après incident..... 8
  - Conservation des fichiers WORM en cas de litiges avec la conservation légale..... 12
  - Vue d'ensemble de la suppression des fichiers WORM ..... 13

# 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	-
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.

### 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

- Le cluster source doit exécuter ONTAP 8.2.2 ou version ultérieure.
- Les agrégats source et de destination doivent être de 64 bits.
- Le volume source ne peut pas être un volume SnapLock.
- Les volumes source et destination doivent être créés dans des clusters associés avec des SVM peering.

Pour plus d'informations, voir "[Peering de clusters](#)".

- Si la croissance automatique du volume est désactivée, l'espace disponible sur le volume de destination doit être au moins cinq pour cent supérieur à l'espace utilisé sur le volume source.

### 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 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

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, 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.



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 cluster de destination, définissez la période de conservation par défaut, comme décrit dans [Définir la période de conservation par défaut](#).



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](#).

5. [Créer une nouvelle relation de réplication](#) Entre la source non SnapLock et la nouvelle destination SnapLock que vous avez créée à l'étape 3.

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.

6. Sur le SVM destination, initialiser la relation SnapVault créée à l'étape 5 :

**`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
```

7. Une fois la relation initialisée et inactive, utilisez le `snapshot show` Commande de la destination pour vérifier que la durée d'expiration du SnapLock est 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 dispose de mises en attente légales, la période d'expiration du volume réel est masquée et apparaît comme « indéfinie », mais l'instantané est verrouillé pendant la durée de la période d'expiration du volume réel.

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 `vol1`:

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



## 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.