Supprimez les données de façon sécurisée sur un volume chiffré

ONTAP 9

NetApp
April 24, 2024

Sommaire

Supprimez les données de façon sécurisée sur un volume chiffré

Supprimez les données de façon sécurisée dans une vue d'ensemble du volume chiffré

Depuis ONTAP 9.4, vous pouvez utiliser la suppression sécurisée pour nettoyer les données sans interruption sur les volumes NVE. La suppression des données sur un volume chiffré garantit qu'elles ne peuvent pas être récupérées depuis le support physique, par exemple en cas de « pillage », où les traces de données peuvent être laissées derrière lors de l'écrasement des blocs ou pour supprimer en toute sécurité les données d'un locataire vide.

La suppression sécurisée fonctionne uniquement pour les fichiers précédemment supprimés sur les volumes NVE. Vous ne pouvez pas nettoyer un volume non chiffré. Vous devez utiliser des serveurs KMIP pour fournir des clés, et non le gestionnaire de clés intégré.

Considérations relatives à l'utilisation de la suppression sécurisée

- Les volumes créés dans un agrégat pour NetApp Aggregate Encryption (NAE) ne prennent pas en charge la suppression sécurisée.
- La suppression sécurisée fonctionne uniquement pour les fichiers précédemment supprimés sur les volumes NVE.
- Vous ne pouvez pas nettoyer un volume non chiffré.
- Vous devez utiliser des serveurs KMIP pour fournir des clés, et non le gestionnaire de clés intégré.

Les fonctions de purge sécurisée varient en fonction de votre version de ONTAP.

ONTAP 9.8 et versions ultérieures

- La suppression sécurisée est prise en charge par MetroCluster et FlexGroup.
- Si le volume en cours de purge est à l'origine d'une relation SnapMirror, il n'est pas nécessaire de rompre la relation SnapMirror pour effectuer une purge sécurisée.
- La méthode de rechiffrement est différente pour les volumes qui utilisent la protection des données SnapMirror, contre les volumes qui n'utilisent pas la protection des données SnapMirror (DP) ou ceux qui utilisent la protection étendue des données SnapMirror.
  - Par défaut, les volumes utilisant le mode de protection des données SnapMirror (DP) recryptent les données à l'aide de la méthode de chiffrement du déplacement de volume.
  - Par défaut, les volumes qui n'utilisent pas la protection des données SnapMirror ou les volumes en utilisant le mode XDP (SnapMirror Extended Data protection) utilisent la méthode de rechiffrement sur place.
  - Ces valeurs par défaut peuvent être modifiées à l'aide de l' `secure purge re-encryption-method [volume-move|in-place-rekey]` commande.
- Par défaut toutes les copies Snapshot des volumes FlexVol sont automatiquement supprimées lors de l'opération de suppression sécurisée. Par défaut, les copies Snapshot des volumes FlexGroup et les volumes qui utilisent la protection des données SnapMirror ne sont pas automatiquement supprimées lors de l'opération de suppression sécurisée. Ces valeurs par défaut peuvent être modifiées à l'aide de l' `secure purge delete-all-snapshots [true|false]` commande.

ONTAP 9.7 et versions antérieures :

- La purge sécurisée ne prend pas en charge les éléments suivants :
  - FlexClone
  - SnapVault
  - FabricPool
- Si le volume en cours de purge est la source d'une relation SnapMirror, vous devez interrompre la relation SnapMirror avant de pouvoir purger le volume.

  Si des copies Snapshot sont occupées dans le volume, vous devez libérer les copies Snapshot avant de pouvoir purger le volume. Par exemple, vous devrez peut-être séparer un volume FlexClone de son volume parent.

- L'appel réussi de la fonction de suppression sécurisée déclenche un déplacement de volume qui recrypte les données restantes non supprimées avec une nouvelle clé.

  Le volume déplacé reste sur l'agrégat actuel. L'ancienne clé est automatiquement détruite, ce qui permet de s'assurer que les données supprimées ne peuvent pas être récupérées du support de stockage.

Supprimez en toute sécurité les données d'un volume chiffré sans une relation SnapMirror

Depuis ONTAP 9.4, vous pouvez utiliser la suppression sécurisée vers les données « ``cribs'' sans interruption sur les volumes NVE.

Description de la tâche

La suppression sécurisée peut prendre de plusieurs minutes à plusieurs heures, selon la quantité de données contenues dans les fichiers supprimés. Vous pouvez utiliser le `volume encryption secure-purge show` commande permettant d'afficher le statut de l'opération. Vous pouvez utiliser le `volume encryption secure-purge abort` commande pour mettre fin à l'opération.

> Pour effectuer une purge sécurisée sur un hôte SAN, vous devez supprimer la LUN entière contenant les fichiers à purger, ou vous devez pouvoir perforer les trous dans la LUN pour les blocs appartenant aux fichiers à purger. Si vous ne pouvez pas supprimer la LUN ou si votre système d'exploitation hôte ne prend pas en charge la perforation dans la LUN, vous ne pouvez pas effectuer de purge sécurisée.

Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Des privilèges avancés sont requis pour cette tâche.

Étapes

1. Supprimez les fichiers ou la LUN que vous souhaitez supprimer en toute sécurité.
   - Sur un client NAS, supprimez les fichiers que vous souhaitez purger en toute sécurité.
   - Sur un hôte SAN, supprimez le LUN que vous souhaitez purger ou perforer en toute sécurité les blocs appartenant aux fichiers à supprimer.
2. Sur le système de stockage, passez au niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

3. Si les fichiers que vous souhaitez purger en toute sécurité sont dans les instantanés, supprimez-les :

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

4. Supprimez les fichiers supprimés de manière sécurisée :

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   ```

   La commande suivante supprime de manière sécurisée les fichiers supprimés sur `vol1` Sur SVM`vs1`:

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

5. Vérifier l'état de l'opération de purge sécurisée :

   ```
   volume encryption secure-purge show
   ```

Supprimez en toute sécurité les données d'un volume chiffré avec une relation SnapMirror asynchrone

Depuis ONTAP 9.8, vous pouvez utiliser une suppression sécurisée des données « `réplication```ss" sans interruption sur les volumes NVE avec une relation SnapMirror

asynchrone.

Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Des privilèges avancés sont requis pour cette tâche.

Description de la tâche

La suppression sécurisée peut prendre de plusieurs minutes à plusieurs heures, selon la quantité de données contenues dans les fichiers supprimés. Vous pouvez utiliser le `volume encryption secure-purge show` commande permettant d'afficher le statut de l'opération. Vous pouvez utiliser le `volume encryption secure-purge abort` commande pour mettre fin à l'opération.

> Pour effectuer une purge sécurisée sur un hôte SAN, vous devez supprimer la LUN entière contenant les fichiers à purger, ou vous devez pouvoir perforer les trous dans la LUN pour les blocs appartenant aux fichiers à purger. Si vous ne pouvez pas supprimer la LUN ou si votre système d'exploitation hôte ne prend pas en charge la perforation dans la LUN, vous ne pouvez pas effectuer de purge sécurisée.

Étapes

1. Sur le système de stockage, basculer sur le niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

2. Supprimez les fichiers ou la LUN que vous souhaitez supprimer en toute sécurité.
   - Sur un client NAS, supprimez les fichiers que vous souhaitez purger en toute sécurité.
   - Sur un hôte SAN, supprimez le LUN que vous souhaitez purger ou perforer en toute sécurité les blocs appartenant aux fichiers à supprimer.
3. Préparez le volume de destination dans la relation asynchrone à supprimer de manière sécurisée :

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   -prepare true
   ```

   Répétez cette étape pour chaque volume de la relation SnapMirror asynchrone.

4. Si les fichiers que vous souhaitez supprimer de manière sécurisée se trouvent dans des copies Snapshot, supprimez les copies Snapshot :

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

5. Si les fichiers que vous souhaitez supprimer de manière sécurisée se trouvent dans les copies Snapshot de base, procédez comme suit :

   a. Créez une copie Snapshot sur le volume de destination dans la relation SnapMirror asynchrone :

      ```
      volume snapshot create -snapshot snapshot_name -vserver SVM_name -volume
      volume_name
      ```

   b. Mettre à jour SnapMirror pour transférer la copie Snapshot de base :

      ```
      snapmirror update -source-snapshot snapshot_name -destination-path
      destination_path
      ```

Répétez cette étape pour chaque volume de la relation SnapMirror asynchrone.

a. Les étapes de répétition (a) et (b) sont égales au nombre de copies Snapshot de base plus une.

   Par exemple, si vous avez deux copies Snapshot de base, vous devez répéter les étapes (a) et (b) trois fois.

b. Vérifier la présence de la copie Snapshot de base :
   `snapshot show -vserver SVM_name -volume volume_name`

c. Supprimer la copie Snapshot de base :
   `snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot`

6. Supprimez les fichiers supprimés de manière sécurisée :

   `volume encryption secure-purge start -vserver svm_name -volume volume_name`

   Répétez cette étape pour chaque volume de la relation SnapMirror asynchrone.

   La commande suivante purge de manière sécurisée les fichiers supprimés sur « 'vol1' » du SVM « vs1 » :

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

7. Vérifier l'état de l'opération de purge sécurisée :

   `volume encryption secure-purge show`

Frottez les données sur un volume chiffré avec une relation SnapMirror synchrone

À partir de ONTAP 9.8, vous pouvez utiliser une suppression sécurisée pour « nettoyer » les données de volumes NVE sans interruption avec une relation SnapMirror synchrone.

Description de la tâche

Une purge sécurisée peut prendre plusieurs minutes à plusieurs heures, selon la quantité de données contenues dans les fichiers supprimés. Vous pouvez utiliser le `volume encryption secure-purge show` commande permettant d'afficher le statut de l'opération. Vous pouvez utiliser le `volume encryption secure-purge abort` commande pour mettre fin à l'opération.

> Pour effectuer une purge sécurisée sur un hôte SAN, vous devez supprimer la LUN entière contenant les fichiers à purger, ou vous devez pouvoir perforer les trous dans la LUN pour les blocs appartenant aux fichiers à purger. Si vous ne pouvez pas supprimer la LUN ou si votre système d'exploitation hôte ne prend pas en charge la perforation dans la LUN, vous ne pouvez pas effectuer de purge sécurisée.

Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Des privilèges avancés sont requis pour cette tâche.

Étapes

1. Sur le système de stockage, passez au niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

2. Supprimez les fichiers ou la LUN que vous souhaitez supprimer en toute sécurité.
   - Sur un client NAS, supprimez les fichiers que vous souhaitez purger en toute sécurité.
   - Sur un hôte SAN, supprimez le LUN que vous souhaitez purger ou perforer en toute sécurité les blocs appartenant aux fichiers à supprimer.

3. Préparez le volume de destination dans la relation asynchrone à supprimer de manière sécurisée :

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   -prepare true
   ```

   Répétez cette étape pour l'autre volume de votre relation SnapMirror synchrone.

4. Si les fichiers que vous souhaitez supprimer de manière sécurisée se trouvent dans des copies Snapshot, supprimez les copies Snapshot :

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot snapshot
   ```

5. Si le fichier de suppression sécurisée se trouve dans les copies Snapshot de base ou communes, mettez à jour SnapMirror pour déplacer la copie Snapshot commune :

   ```
   snapmirror update -source-snapshot snapshot_name -destination-path
   destination_path
   ```

   Il existe deux copies Snapshot communes. Cette commande doit donc être émise deux fois.

6. Si le fichier de suppression sécurisée se trouve dans la copie Snapshot cohérente au niveau des applications, supprimez la copie Snapshot sur les deux volumes de la relation SnapMirror synchrone :

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot snapshot
   ```

   Effectuer cette étape sur les deux volumes.

7. Supprimez les fichiers supprimés de manière sécurisée :

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   ```

   Répétez cette étape pour chaque volume de la relation SnapMirror synchrone.

   La commande suivante supprime en toute sécurité les fichiers supprimés sur « vol1 » sur le SMV « vs1 ».

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

8. Vérifier l'état de l'opération de purge sécurisée :

   ```
   volume encryption secure-purge show
   ```