Supprimez les données de façon sécurisée sur un volume chiffré

ONTAP 9

NetApp
February 13, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/ontap/encryption-at-rest/secure-purge-data-encrypted-volume-concept.html on February 13, 2026. Always check docs.netapp.com for the latest.

Sommaire

Supprimez les données de façon sécurisée sur un volume chiffré 1
En savoir plus sur la purge sécurisée des données d'un volume ONTAP chiffré 1
Considérations relatives à l'utilisation de la suppression sécurisée 1
Nettoyer les données d'un volume ONTAP chiffré sans relation SnapMirror 2
Nettoyer les données d'un volume ONTAP chiffré avec une relation asynchrone SnapMirror 3
Nettoyer les données d'un volume ONTAP chiffré avec une relation synchrone SnapMirror 5

Supprimez les données de façon sécurisée sur un volume chiffré

En savoir plus sur la purge sécurisée des données d'un volume ONTAP 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, tous les snapshots des volumes FlexVol sont automatiquement supprimés lors de l'opération de purge 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 la `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 le volume contient des snapshots occupés, vous devez les libérer 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.

Nettoyer les données d'un volume ONTAP chiffré sans 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
   ```

Nettoyer les données d'un volume ONTAP chiffré avec une relation asynchrone SnapMirror

À partir de ONTAP 9.8, vous pouvez appliquer une suppression sécurisée aux données « crub » sans interruption sur les volumes NVE avec une relation asynchrone SnapMirror.

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 votre relation SnapMirror asynchrone.

4. 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
   ```

5. Si les fichiers que vous souhaitez supprimer en toute sécurité se trouvent dans les instantanés de base, procédez comme suit :

   a. Créer un snapshot sur le volume de destination dans la relation asynchrone SnapMirror :

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

   b. Mettre à jour SnapMirror pour déplacer le snapshot de base vers l'avant :

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

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

a. Répéter les étapes (a) et (b) correspondant au nombre d'instantanés de base plus un.

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

b. Vérifiez que l'instantané de base est présent :
   `snapshot show -vserver SVM_name -volume volume_name`

c. Supprimer l'instantané 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 asynchrone SnapMirror.

   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`

Informations associées

- "mise à jour de SnapMirror"

Nettoyer les données d'un volume ONTAP chiffré avec une relation synchrone SnapMirror

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

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 synchrone SnapMirror.

4. 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 <snapshot>
   ```

5. Si le fichier de purge sécurisée se trouve dans les instantanés de base ou courants, mettez à jour SnapMirror pour déplacer le snapshot commun vers l'avant :

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

   Il existe deux instantanés courants. Cette commande doit donc être exécutée deux fois.

6. Si le fichier de suppression sécurisée se trouve dans le snapshot cohérent avec l'application, supprimez le snapshot sur les deux volumes de la relation synchrone SnapMirror :

   ```
   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 synchrone SnapMirror.

   La commande suivante supprime en toute sécurité les fichiers supprimés sur « vol1 » sur le SVM « 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
   ```

Informations associées

- "mise à jour de SnapMirror"

Informations sur le copyright

Copyright © 2026 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 DÉLICTUELLE (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.