Rendre les données d'un lecteur FIPS ou SED inaccessibles

ONTAP 9

NetApp
February 13, 2026

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

Sommaire

Rendre les données d'un lecteur FIPS ou SED inaccessibles 1
Découvrez comment rendre les données ONTAP sur un lecteur FIPS ou SED inaccessibles 1
Procédez à la désinfection d'un disque FIPS ou SED dans ONTAP 1
Détruisez un disque FIPS ou SED dans ONTAP 3
Données d'urgence déchirées sur un lecteur FIPS ou SED dans ONTAP 5

Rendre les données d’un lecteur FIPS ou SED inaccessibles

Découvrez comment rendre les données ONTAP sur un lecteur FIPS ou SED inaccessibles

Si vous souhaitez rendre les données stockées sur un lecteur FIPS ou SED définitivement inaccessibles, mais que l’espace inutilisé du lecteur reste disponible pour les nouvelles données, vous pouvez désinfecter le disque. Si vous souhaitez rendre les données définitivement inaccessibles et que vous n’avez pas besoin de réutiliser le lecteur, vous pouvez le détruire.

- Nettoyage de disque

  Lorsque vous procédez à la suppression d’un disque à auto-cryptage, le système modifie la clé de cryptage sur disque en une nouvelle valeur aléatoire, réinitialise l’état de verrouillage à la mise sous tension sur FALSE et définit l’ID de clé sur une valeur par défaut, soit l’ID sécurisé du fabricant 0x0 (disques SAS), soit une clé nulle (disques NVMe). Cela rend les données sur le disque inaccessibles et impossible à récupérer. Vous pouvez réutiliser des disques aseptisés comme disques de rechange non remis à zéro.

- Destruction du disque

  Lorsque vous détruisez un lecteur FIPS ou SED, le système définit la clé de cryptage sur une valeur aléatoire inconnue et verrouille le disque de façon irréversible. Le disque devient ainsi définitivement inutilisable et les données qu’il y a définitivement inaccessibles.

Vous pouvez supprimer ou détruire des disques auto-cryptés ou tous les disques auto-cryptés d’un nœud.

Procédez à la désinfection d’un disque FIPS ou SED dans ONTAP

Si vous voulez rendre les données sur un lecteur FIPS ou SED définitivement inaccessibles et utiliser le lecteur pour les nouvelles données, vous pouvez utiliser le `storage encryption disk sanitize` commande de nettoyage du disque.

Description de la tâche

Lorsque vous procédez à la suppression d’un disque à auto-cryptage, le système modifie la clé de cryptage sur disque en une nouvelle valeur aléatoire, réinitialise l’état de verrouillage à la mise sous tension sur FALSE et définit l’ID de clé sur une valeur par défaut, soit l’ID sécurisé du fabricant 0x0 (disques SAS), soit une clé nulle (disques NVMe). Cela rend les données sur le disque inaccessibles et impossible à récupérer. Vous pouvez réutiliser des disques aseptisés comme disques de rechange non remis à zéro.

Avant de commencer

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

Étapes

1. Migrer toutes les données qui doivent être conservées vers un agrégat sur un autre disque.
2. Supprimez l'agrégat du lecteur FIPS ou SED pour les désinfecter :

   `storage aggregate delete -aggregate aggregate_name`

   ```
   cluster1::> storage aggregate delete -aggregate aggr1
   ```

   Pour en savoir plus, `storage aggregate delete` consultez le "Référence de commande ONTAP".

3. Identifiez l'ID du disque pour le lecteur FIPS ou SED à désinfecter :

   `storage encryption disk show -fields data-key-id,fips-key-id,owner`

   Pour en savoir plus, `storage encryption disk show` consultez le "Référence de commande ONTAP".

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   ------------------------------------------------------------------
   0.0.0   data <id_value>
   0.0.1   data <id_value>
   1.10.2  data <id_value>
   [...]
   ```

4. Si un lecteur FIPS est exécuté en mode FIPS-Compliance, définissez l'ID de clé d'authentification FIPS du nœud sur le MSID 0x0 par défaut :

   `storage encryption disk modify -disk disk_id -fips-key-id 0x0`

   Vous pouvez utiliser le `security key-manager query` Commande permettant d'afficher les ID de clés.

   ```
   cluster1::> storage encryption disk modify -disk 1.10.2 -fips-key-id 0x0

   Info: Starting modify on 1 disk.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

5. Désinfectez le lecteur :

   `storage encryption disk sanitize -disk disk_id`

   Vous pouvez utiliser cette commande pour désinfecter uniquement les disques de rechange à chaud ou endommagés. Pour nettoyer tous les disques, quel que soit leur type, utilisez `-force-all-state` l'option. Pour en savoir plus, `storage encryption disk sanitize` consultez le "Référence de commande ONTAP".

ONTAP vous invite à saisir une phrase de confirmation avant de continuer. Saisissez la phrase exactement comme indiqué à l'écran.

```
cluster1::> storage encryption disk sanitize -disk 1.10.2

Warning: This operation will cryptographically sanitize 1 spare or
broken self-encrypting disk on 1 node.
         To continue, enter sanitize disk: sanitize disk

Info: Starting sanitize on 1 disk.
      View the status of the operation using the
      storage encryption disk show-status command.
```

6. Éliminez la panne du disque désinfecté : `storage disk unfail -spare true -disk disk_id`
7. Vérifiez si le disque est propriétaire : `storage disk show -disk disk_id`
   Si le disque ne possède pas de propriétaire, attribuez-en un. `storage disk assign -owner node -disk disk_id`
8. Entrez le nodeshell pour le nœud qui possède les disques à désinfecter :

   `system node run -node node_name`

   Exécutez le `disk sanitize release` commande.

9. Quittez le nodeshell. Éliminez à nouveau la panne du disque : `storage disk unfail -spare true -disk disk_id`
10. Vérifier que le disque est désormais une pièce de rechange et prêt à être réutilisé dans un agrégat : `storage disk show -disk disk_id`

Informations associées

- "affectation de disque de stockage"
- "affichage du disque de stockage"
- "disque de stockage non défaillant"
- "modification du disque de cryptage de stockage"
- "stockage cryptage disque nettoyage"
- "disque de chiffrement de stockage afficher-état"

Détruisez un disque FIPS ou SED dans ONTAP

Si vous voulez rendre les données sur un lecteur FIPS ou SED définitivement inaccessibles et que vous n'avez pas besoin de réutiliser le lecteur, vous pouvez utiliser `storage encryption disk destroy` commande de destruction du disque.

Description de la tâche

Lorsque vous détruisez un lecteur FIPS ou SED, le système définit la clé de cryptage sur une valeur aléatoire

inconnue et verrouille le disque de façon irréversible. Le disque devient ainsi pratiquement inutilisable et les données qu'il y a définitivement inaccessibles. Cependant, vous pouvez réinitialiser le disque à ses paramètres configurés en usine à l'aide de l'ID de sécurité physique (PSID) imprimé sur l'étiquette du disque. Pour plus d'informations, voir "Remise en service d'un lecteur FIPS ou SED en cas de perte de clés d'authentification".

> Vous ne devez pas détruire un disque FIPS ou SED sauf si vous disposez du service NRD plus (non-Returnable Disk plus). La destruction d'un disque annule sa garantie.

Avant de commencer

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

Étapes

1. Migrer toutes les données qui doivent être conservées vers un agrégat sur un autre disque.
2. Supprimez l'agrégat du disque FIPS ou SED à détruire :

   `storage aggregate delete -aggregate aggregate_name`

   ```
   cluster1::> storage aggregate delete -aggregate aggr1
   ```

   Pour en savoir plus, `storage aggregate delete` consultez le "Référence de commande ONTAP".

3. Identifiez l'ID de disque pour le lecteur FIPS ou SED à détruire :

   `storage encryption disk show`

   Pour en savoir plus, `storage encryption disk show` consultez le "Référence de commande ONTAP".

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   ------------------------------------------------------------------
   0.0.0   data <id_value>
   0.0.1   data <id_value>
   1.10.2  data <id_value>
   [...]
   ```

4. Détruire le disque :

   `storage encryption disk destroy -disk disk_id`

   Pour en savoir plus, `storage encryption disk destroy` consultez le "Référence de commande ONTAP".

   > Vous êtes invité à entrer une phrase de confirmation avant de continuer. Saisissez la phrase exactement comme indiqué à l'écran.

```
cluster1::> storage encryption disk destroy -disk 1.10.2

Warning: This operation will cryptographically destroy 1 spare or broken
         self-encrypting disks on 1 node.
         You cannot reuse destroyed disks unless you revert
         them to their original state using the PSID value.
         To continue, enter
          destroy disk
         :destroy disk

Info: Starting destroy on 1 disk.
      View the status of the operation by using the
      "storage encryption disk show-status" command.
```

Informations associées

- "destruction du disque de cryptage de stockage"
- "affichage du disque de cryptage de stockage"
- "disque de chiffrement de stockage afficher-état"

Données d'urgence déchirées sur un lecteur FIPS ou SED dans ONTAP

En cas d'urgence en matière de sécurité, vous pouvez instantanément empêcher l'accès à un disque FIPS ou SED, même si l'alimentation n'est pas disponible pour le système de stockage ou le serveur KMIP.

Avant de commencer

- Si vous utilisez un serveur KMIP qui n'est pas alimenté, vous devez configurer le serveur KMIP avec un élément d'authentification facilement détruit (par exemple, une carte à puce ou un lecteur USB).
- Vous devez être un administrateur de cluster pour effectuer cette tâche.

Étape

1. Exécutez la suppression d'urgence des données sur un lecteur FIPS ou SED :

Si…	Alors…

L’alimentation est disponible pour le système de stockage et vous avez le temps de mettre celui-ci hors ligne aisément	a. Si le système de stockage est configuré en tant que paire haute disponibilité, désactivez le basculement. b. Mettre tous les agrégats hors ligne et les supprimer c. Définissez le niveau de privilège sur avancé : `set -privilege advanced` d. Si le lecteur est en mode FIPS-compliance, définissez à nouveau l’ID de clé d’authentification FIPS du nœud sur le MSID par défaut : `storage encryption disk modify -disk * -fips-key-id 0x0` e. Arrêter le système de stockage. f. Démarre en mode de maintenance. g. Procédez à la suppression ou à la destruction des disques : ◦ Pour rendre les données sur les disques inaccessibles et continuer à réutiliser les disques, procédez comme suit : `disk encrypt sanitize -all` ◦ Si vous souhaitez rendre les données sur les disques inaccessibles et que vous n’avez pas besoin d’enregistrer les disques, détruisez les disques : `disk encrypt destroy disk_id1 disk_id2 …`	Le système de stockage est sous tension et vous devez immédiatement détruire les données

a. **Si vous souhaitez rendre les données sur les disques inaccessibles et que vous pourrez toujours les réutiliser, désinfectez les disques :**
b. Si le système de stockage est configuré en tant que paire haute disponibilité, désactivez le basculement.
c. Définissez le niveau de privilège sur avancé :
`set -privilege advanced`
d. Si le lecteur est en mode FIPS-compliance, définissez à nouveau l'ID de clé d'authentification FIPS du nœud sur le MSID par défaut :
`storage encryption disk modify -disk * -fips-key-id 0x0`
e. Procédez à la suppression du disque :
`storage encryption disk sanitize -disk * -force-all-states true`
	a. **Si vous souhaitez rendre les données sur les disques inaccessibles et que vous n'avez pas besoin d'enregistrer les disques, détruisez les disques :**
	b. Si le système de stockage est configuré en tant que paire haute disponibilité, désactivez le basculement.
	c. Définissez le niveau de privilège sur avancé :
	`set -privilege advanced`
	d. Détruire les disques :
	`storage encryption disk destroy -disk * -force-all-states true`
		Le système de stockage fonctionne de façon incohérente, laissant le système se trouve dans un état désactivé en permanence et toutes les données sont effacées. Pour réutiliser le système, vous devez le reconfigurer.

L'alimentation est disponible pour le serveur KMIP, mais pas pour le système de stockage	a. Connectez-vous au serveur KMIP. b. Détruire toutes les clés associées aux lecteurs FIPS ou les disques SED qui contiennent les données auxquelles vous souhaitez empêcher l'accès. Cela empêche l'accès aux clés de cryptage du disque par le système de stockage.	L'alimentation n'est pas disponible pour le serveur KMIP ou le système de stockage

Informations associées

- "destruction du disque de cryptage de stockage"
- "modification du disque de cryptage de stockage"
- "stockage cryptage disque nettoyage"

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.