



# **Gestion du cryptage NetApp**

## **ONTAP 9**

NetApp  
January 08, 2026

This PDF was generated from <https://docs.netapp.com/fr-fr/ontap/encryption-at-rest/unencrypt-volume-data-task.html> on January 08, 2026. Always check docs.netapp.com for the latest.

# Sommaire

Gestion du cryptage NetApp .....	1
Annulez le chiffrement des données de volume dans ONTAP .....	1
Déplacement d'un volume chiffré dans ONTAP .....	1
Modifiez la clé de chiffrement d'un volume à l'aide de la commande volume Encryption reskey start dans ONTAP .....	2
Modifier la clé de chiffrement d'un volume avec la commande ONTAP volume move start .....	4
Rotation des clés d'authentification pour le chiffrement du stockage ONTAP NetApp .....	5
Supprime un volume chiffré dans ONTAP .....	5
Supprimez les données de façon sécurisée sur un volume chiffré .....	6
En savoir plus sur la purge sécurisée des données d'un volume ONTAP chiffré .....	6
Nettoyer les données d'un volume ONTAP chiffré sans relation SnapMirror .....	7
Nettoyer les données d'un volume ONTAP chiffré avec une relation asynchrone SnapMirror .....	8
Nettoyer les données d'un volume ONTAP chiffré avec une relation synchrone SnapMirror .....	10
Modifier la phrase secrète de gestion des clés intégrées ONTAP .....	12
Sauvegarder manuellement les informations de gestion des clés intégrées ONTAP .....	13
Restaurez les clés de chiffrement dans ONTAP pour la gestion intégrée des clés .....	15
ONTAP 9.6 et versions ultérieures .....	15
ONTAP 9.8 ou version ultérieure avec volume racine chiffré .....	15
ONTAP 9.5 et versions antérieures .....	16
Restaurer les clés de chiffrement de gestion des clés externes ONTAP .....	16
Remplacer les certificats SSL KMIP sur le cluster ONTAP .....	17
Remplacez un lecteur FIPS ou SED dans ONTAP .....	18
Rendre les données d'un lecteur FIPS ou SED inaccessibles .....	20
Découvrez comment rendre les données ONTAP sur un lecteur FIPS ou SED inaccessibles .....	20
Procédez à la désinfection d'un disque FIPS ou SED dans ONTAP .....	21
Détruisez un disque FIPS ou SED dans ONTAP .....	23
Données d'urgence déchirées sur un lecteur FIPS ou SED dans ONTAP .....	24
Remettre en service un lecteur FIPS ou SED lorsque les clés d'authentification sont perdues dans ONTAP .....	28
Remettre un lecteur FIPS ou SED en mode non protégé dans ONTAP .....	30
Mode Maintenance .....	32
Supprimez une connexion de gestionnaire de clés externe dans ONTAP .....	33
Modifier les propriétés du serveur de gestion de clés externes ONTAP .....	34
Passez à la gestion externe des clés grâce à la gestion intégrée des clés dans ONTAP .....	35
Passer de la gestion des clés externes à la gestion des clés intégrée ONTAP .....	36
Que se passe-t-il lorsque les serveurs de gestion de clés ne sont pas accessibles pendant le processus de démarrage ONTAP .....	37
Désactiver le cryptage ONTAP par défaut .....	39

# Gestion du cryptage NetApp

## Annulez le chiffrement des données de volume dans ONTAP

Vous pouvez utiliser le `volume move start` commande pour déplacer et annuler le chiffrement des données de volume.

### Avant de commencer

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

### Étapes

1. Déplacer un volume chiffré existant sans chiffrer les données sur le volume :

```
volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false
```

Pour en savoir plus, `volume move start` consultez le ["Référence de commande ONTAP"](#).

La commande suivante déplace un volume existant nommé `vol1` vers l'agrégat de destination `aggr3` et déchiffre les données sur le volume :

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination-aggregate aggr3 -encrypt-destination false
```

Le système supprime la clé de cryptage du volume. Les données du volume sont non chiffrées.

2. Vérifiez que le volume est désactivé pour le chiffrement :

```
volume show -encryption
```

Pour en savoir plus, `volume show` consultez le ["Référence de commande ONTAP"](#).

La commande suivante indique si les volumes sont présents `cluster1` sont chiffrées :

```
cluster1::> volume show -encryption
```

Vserver	Volume	Aggregate	State	Encryption State
-----	-----	-----	-----	-----
vs1	vol1	aggr1	online	none

## Déplacement d'un volume chiffré dans ONTAP

Vous pouvez utiliser le `volume move start` commande permettant de déplacer un volume chiffré. Le volume déplacé peut résider sur le même agrégat ou sur un autre agrégat.

## Description de la tâche

Le déplacement échoue si le nœud de destination ou le volume de destination ne prend pas en charge le chiffrement de volume.

Le `-encrypt-destination` option pour `volume move start` la valeur par défaut est `true` pour les volumes chiffrés. La nécessité de spécifier que vous ne souhaitez pas que le volume de destination soit chiffré garantit que vous ne déchiffrez pas par inadvertance les données sur le volume.

## Avant de commencer

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

## Étapes

1. Déplacez un volume chiffré et laissez les données sur le volume chiffré :

```
volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name
```

Pour en savoir plus, `volume move start` consultez le ["Référence de commande ONTAP"](#).

La commande suivante déplace un volume existant nommé `vol1` vers l'agrégat de destination `aggr3` et conserve les données sur le volume chiffrées :

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination -aggregate aggr3
```

2. Vérifiez que le volume est activé pour le chiffrement :

```
volume show -is-encrypted true
```

Pour en savoir plus, `volume show` consultez le ["Référence de commande ONTAP"](#).

La commande suivante affiche les volumes chiffrés sur `cluster1`:

```
cluster1::> volume show -is-encrypted true
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used
-----	-----	-----	-----	----	-----	-----	-----
vs1	vol1	aggr3	online	RW	200GB	160.0GB	20%

## Modifiez la clé de chiffrement d'un volume à l'aide de la commande `volume Encryption reskey start` dans ONTAP

Il est recommandé de modifier régulièrement la clé de chiffrement d'un volume. Vous pouvez utiliser ONTAP 9.3 à partir de `volume encryption rekey start` commande pour changer la clé de chiffrement.

## Description de la tâche

Une fois que vous avez démarré une opération de recontact, elle doit être terminée. Il n'y a pas de retour à l'ancienne clé. Si vous rencontrez un problème de performances pendant l'opération, vous pouvez exécuter le `volume encryption rekey pause` commande pour mettre l'opération en pause, et le `volume encryption rekey resume` commande pour reprendre l'opération.

Jusqu'à la fin de l'opération de renouvellement de clé, le volume est composé de deux touches. Les nouvelles écritures et les lectures correspondantes utiliseront la nouvelle clé. Sinon, les lectures utilisent l'ancienne clé.



Vous ne pouvez pas utiliser `volume encryption rekey start` Pour rétablir un volume SnapLock.

## Étapes

1. Modifier une clé de chiffrement :

```
volume encryption rekey start -vserver SVM_name -volume volume_name
```

La commande suivante modifie la clé de chiffrement pour `vol1` Sur `SVMvs1`:

```
cluster1::> volume encryption rekey start -vserver vs1 -volume vol1
```

2. Vérifier l'état de l'opération de renouvellement de clé :

```
volume encryption rekey show
```

Pour en savoir plus, `volume encryption rekey show` consultez le ["Référence de commande ONTAP"](#).

La commande suivante affiche l'état de l'opération de renouvellement de clés :

```
cluster1::> volume encryption rekey show
```

Vserver	Volume	Start Time	Status
-----	-----	-----	-----
vs1	vol1	9/18/2017 17:51:41	Phase 2 of 2 is in progress.

3. Une fois l'opération de renouvellement de clés terminée, vérifiez que le volume est activé pour le chiffrement :

```
volume show -is-encrypted true
```

Pour en savoir plus, `volume show` consultez le ["Référence de commande ONTAP"](#).

La commande suivante affiche les volumes chiffrés sur `cluster1`:

```
cluster1::> volume show -is-encrypted true
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used
-----	-----	-----	-----	-----	-----	-----	-----
vs1	vol1	aggr2	online	RW	200GB	160.0GB	20%

## Modifier la clé de chiffrement d'un volume avec la commande ONTAP volume move start

Il est recommandé de modifier régulièrement la clé de chiffrement d'un volume. Vous pouvez utiliser `volume move start` la commande pour modifier la clé de chiffrement. Le volume déplacé peut résider sur le même agrégat ou sur un autre agrégat.

### Description de la tâche

Vous ne pouvez pas utiliser `volume move start` Pour reKey un volume SnapLock ou FlexGroup.

### Avant de commencer

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

### Étapes

1. Déplacer un volume existant et modifier la clé de chiffrement :

```
volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -generate-destination-key true
```

Pour en savoir plus, `volume move start` consultez le ["Référence de commande ONTAP"](#).

La commande suivante déplace un volume existant nommé **vol1** vers l'agrégat de destination **aggr2** et modifie la clé de chiffrement :

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination -aggregate aggr2 -generate-destination-key true
```

Une nouvelle clé de chiffrement est créée pour le volume. Les données du volume restent chiffrées.

2. Vérifiez que le volume est activé pour le chiffrement :

```
volume show -is-encrypted true
```

Pour en savoir plus, `volume show` consultez le ["Référence de commande ONTAP"](#).

La commande suivante affiche les volumes chiffrés sur `cluster1`:

```
cluster1::> volume show -is-encrypted true
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used
-----	-----	-----	-----	-----	-----	-----	-----
vs1	vol1	aggr2	online	RW	200GB	160.0GB	20%

## Rotation des clés d'authentification pour le chiffrement du stockage ONTAP NetApp

Vous pouvez faire tourner les clés d'authentification lorsque vous utilisez NetApp Storage Encryption (NSE).

### Description de la tâche

La rotation des clés d'authentification dans un environnement NSE est prise en charge si vous utilisez External Key Manager (KMIP).



La rotation des clés d'authentification dans un environnement NSE n'est pas prise en charge pour Onboard Key Manager (OKM).

### Étapes

1. Utilisez le `security key-manager create-key` commande permettant de générer de nouvelles clés d'authentification.

Vous devez générer de nouvelles clés d'authentification avant de pouvoir modifier les clés d'authentification.

2. Utilisez le `storage encryption disk modify -disk * -data-key-id` commande pour modifier les clés d'authentification.

### Informations associées

- ["modification du disque de cryptage de stockage"](#)

## Supprime un volume chiffré dans ONTAP

Vous pouvez utiliser le `volume delete` commande de suppression d'un volume chiffré.

### Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Le volume doit être hors ligne.

### Étape

1. Supprimez un volume chiffré :

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

Pour en savoir plus, `volume delete` consultez le ["Référence de commande ONTAP"](#).

La commande suivante supprime un volume chiffré nommé `vol1`:

```
cluster1::> volume delete -vserver vs1 -volume vol1
```

Entrez `yes` lorsque vous êtes invité à confirmer la suppression.

Le système supprime la clé de cryptage du volume au bout de 24 heures.

À utiliser `volume delete` avec la `-force true` possibilité de supprimer un volume et de détruire immédiatement la clé de chiffrement correspondante. Cette commande nécessite des privilèges avancés. Pour en savoir plus, `volume delete` consultez le ["Référence de commande ONTAP"](#).

### Une fois que vous avez terminé

Vous pouvez utiliser le `volume recovery-queue` pour restaurer un volume supprimé pendant la période de rétention après l'émission du `volume delete` commande :

```
volume recovery-queue SVM_name -volume volume_name
```

["Comment utiliser la fonction de récupération de volume"](#)

## 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 supprimés 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 `SVMvs1`:

```
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"](#)

# Modifier la phrase secrète de gestion des clés intégrées ONTAP

NetApp recommande de modifier régulièrement la phrase de passe de gestion des clés intégrées. Vous devez stocker la nouvelle phrase de passe dans un endroit sécurisé, en dehors du système de stockage.

## Avant de commencer

- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.
- Des privilèges avancés sont requis pour cette tâche.
- Dans un environnement MetroCluster , après avoir mis à jour la phrase secrète sur le cluster local, synchronisez la mise à jour de la phrase secrète sur le cluster partenaire.

## Étapes

1. Changement au niveau de privilège avancé :

```
set -privilege advanced
```

2. Modifiez la phrase de passe de gestion des clés intégrées. La commande à utiliser dépend de la version ONTAP que vous utilisez.

### ONTAP 9.6 et versions ultérieures

```
security key-manager onboard update-passphrase
```

### ONTAP 9.5 et versions antérieures

```
security key-manager update-passphrase
```

3. Saisissez une phrase secrète entre 32 et 256 caractères, ou pour « cc-mode », une phrase secrète entre 64 et 256 caractères.

Si la phrase de passe « CC-mode » spécifiée est inférieure à 64 caractères, il y a un délai de cinq secondes avant que l'opération de configuration du gestionnaire de clés n'affiche à nouveau l'invite de phrase de passe.

4. À l'invite de confirmation de la phrase de passe, saisissez à nouveau la phrase de passe.
5. Si vous utilisez une configuration MetroCluster , synchronisez la phrase secrète mise à jour sur le cluster partenaire.
  - a. Synchronisez la phrase secrète sur le cluster partenaire en choisissant la commande appropriée pour votre version ONTAP :

#### ONTAP 9.6 et versions ultérieures

```
security key-manager onboard sync
```

#### ONTAP 9.5 et versions antérieures

- Dans ONTAP 9.5, exécutez :

```
security key-manager setup -sync-metrocluster-config
```

- Dans ONTAP 9.4 et versions antérieures, après avoir mis à jour la phrase secrète sur le cluster local, attendez 20 secondes, puis exécutez la commande suivante sur le cluster partenaire :

```
security key-manager setup
```

- b. Saisissez la nouvelle phrase secrète lorsque vous y êtes invité.

La même phrase secrète doit être utilisée sur les deux clusters.

#### Une fois que vous avez terminé

Copiez la phrase secrète de gestion des clés intégrée dans un emplacement sécurisé en dehors du système de stockage pour une utilisation ultérieure.

Sauvegardez manuellement les informations de gestion des clés chaque fois que vous modifiez la phrase de passe de gestion des clés intégrée.

#### Informations associées

- ["Sauvegardez manuellement les informations intégrées de gestion des clés"](#)
- ["mot de passe de mise à jour intégré du gestionnaire de clés de sécurité"](#)

## Sauvegarder manuellement les informations de gestion des clés intégrées ONTAP

Vous devez copier les informations de gestion intégrée des clés dans un emplacement sécurisé en dehors du système de stockage dès que vous configurez la phrase secrète Onboard Key Manager.

#### 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

Toutes les informations de gestion des clés sont automatiquement sauvegardées dans la base de données répliquée (RDB) pour le cluster. Vous devez également sauvegarder manuellement les informations de gestion des clés pour une utilisation en cas d'incident.

#### Étapes

1. Changement au niveau de privilège avancé :

```
set -privilege advanced
```

2. Afficher les informations de gestion des clés du cluster :

Pour cette version ONTAP...	Utilisez cette commande...
ONTAP 9.6 et versions ultérieures	<code>security key-manager onboard show-backup</code>
ONTAP 9.5 et versions antérieures	<code>security key-manager backup show</code>

La commande 9.6 suivante affiche les informations de sauvegarde de la gestion des clés pour `cluster1` :

```
cluster1::> security key-manager onboard show-backup
```

[illegible]



3. Copiez les informations de sauvegarde dans un emplacement sécurisé en dehors du système de stockage afin de les utiliser en cas d'incident.

#### Informations associées

- ["gestionnaire de clés de sécurité embarqué show-backup"](#)
- ["affichage de sauvegarde du gestionnaire de clés de sécurité"](#)

## Restaurez les clés de chiffrement dans ONTAP pour la gestion intégrée des clés

Parfois, vous devrez peut-être restaurer une clé de chiffrement de gestion de clés intégrée. Une fois que vous avez vérifié qu'une clé doit être restaurée, vous pouvez configurer le gestionnaire de clés intégré pour restaurer la clé. La procédure à suivre pour restaurer vos clés de chiffrement de gestion de clés intégrées varie en fonction de votre version d' ONTAP.

#### Avant de commencer

- Supprimez la base de données du gestionnaire de clés externe si vous utilisez NSE avec un serveur KMIP externe. Pour plus de détails, voir ["Transition de la gestion des clés externes vers la gestion des clés intégrée ONTAP"](#).
- Vous devez être un administrateur de cluster pour effectuer cette tâche.



Si vous utilisez NSE sur un système doté d'un module Flash cache, vous devez également activer NVE ou NAE. NSE ne chiffre pas les données qui résident sur le module Flash cache.

### ONTAP 9.6 et versions ultérieures



Si vous exécutez ONTAP 9.8 ou une version ultérieure et que votre volume racine est chiffré, suivez la procédure de [\[ontap-9-8\]](#).

1. Vérifiez que la clé doit être restaurée :

```
security key-manager key query -node node
```

Pour en savoir plus, `security key-manager key query` consultez le ["Référence de commande ONTAP"](#).

2. Restaurer la clé :

```
security key-manager onboard sync
```

Pour en savoir plus, `security key-manager onboard sync` consultez le ["Référence de commande ONTAP"](#).

3. À l'invite de phrase secrète, entrez la phrase secrète intégrée pour la gestion des clés du cluster.

### ONTAP 9.8 ou version ultérieure avec volume racine chiffré

Si vous exécutez ONTAP 9.8 ou une version ultérieure et que votre volume racine est chiffré, vous devez définir une phrase de passe de récupération de la gestion des clés intégrée à l'aide du menu de démarrage. Ce processus est également nécessaire si vous effectuez un remplacement de support de démarrage.

1. Démarrez le nœud sur le menu de démarrage et sélectionnez option (10) `Set onboard key management recovery secrets`.
2. Entrez `y` pour utiliser cette option.
3. Entrez à l'invite la phrase secrète de gestion intégrée des clés pour le cluster.
4. À l'invite, entrez les données de la clé de sauvegarde.

Après avoir saisi les données de la clé de sauvegarde, le nœud revient au menu de démarrage.

5. Dans le menu de démarrage, sélectionnez option (1) `Normal Boot`.

## ONTAP 9.5 et versions antérieures

1. Vérifiez que la clé doit être restaurée :  
`security key-manager key show`
2. Restaurer la clé :  
`security key-manager setup -node node`

En savoir plus sur `security key-manager setup` dans le ["Référence de commande ONTAP"](#).

3. À l'invite de phrase secrète, entrez la phrase secrète intégrée pour la gestion des clés du cluster.

## Restaurer les clés de chiffrement de gestion des clés externes ONTAP

Vous pouvez restaurer manuellement des clés de chiffrement de gestion externe des clés et les transférer vers un autre nœud. Vous pouvez le faire si vous redémarrez un nœud qui était temporairement arrêté lorsque vous avez créé les clés du cluster.

### Description de la tâche

Dans ONTAP 9.6 et versions ultérieures, vous pouvez utiliser le `security key-manager key query -node node_name` commande pour vérifier si votre clé doit être restaurée.

Dans ONTAP 9.5 et les versions antérieures, vous pouvez utiliser le `security key-manager key show` commande pour vérifier si votre clé doit être restaurée.



Si vous utilisez NSE sur un système doté d'un module Flash cache, vous devez également activer NVE ou NAE. NSE ne chiffre pas les données qui résident sur le module Flash cache.

Pour en savoir plus, `security key-manager key query` consultez le ["Référence de commande ONTAP"](#).

### Avant de commencer

Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

### Étapes

1. Si vous exécutez ONTAP 9.8 ou version ultérieure et que le volume racine est chiffré, procédez comme suit :

Si vous exécutez ONTAP 9.7 ou une version antérieure, ou si vous exécutez ONTAP 9.8 ou une version

ultérieure et que votre volume racine n'est pas chiffré, ignorez cette étape.

a. Définissez les bootargs :

```
setenv kmip.init.ipaddr <ip-address>
setenv kmip.init.netmask <netmask>
setenv kmip.init.gateway <gateway>
setenv kmip.init.interface e0M
boot_ontap
```

b. Démarrez le nœud sur le menu de démarrage et sélectionnez option (11) Configure node for external key management.

c. Suivez les invites pour saisir le certificat de gestion.

Une fois toutes les informations relatives au certificat de gestion saisies, le système revient au menu de démarrage.

d. Dans le menu de démarrage, sélectionnez option (1) Normal Boot.

2. Restaurer la clé :

Pour cette version ONTAP...	Utilisez cette commande...
ONTAP 9.6 et versions ultérieures	`security key-manager external restore -vserver SVM -node node -key-server host_name`
IP_address:port -key-id key_id -key -tag key_tag`	ONTAP 9.5 et versions antérieures



node tous les nœuds sont par défaut.

Cette commande n'est pas prise en charge lorsque la gestion intégrée des clés est activée.

La commande ONTAP 9.6 suivante restaure les clés d'authentification externes de gestion des clés vers tous les nœuds de `cluster1`:

```
cluster1::> security key-manager external restore
```

### Informations associées

- ["restauration externe du gestionnaire de clés de sécurité"](#)

## Remplacer les certificats SSL KMIP sur le cluster ONTAP

Tous les certificats SSL ont une date d'expiration. Vous devez mettre à jour vos certificats avant qu'ils n'expirent pour éviter toute perte d'accès aux clés d'authentification.

### Avant de commencer

- Vous devez avoir obtenu le certificat public et la clé privée de remplacement pour le cluster (certificat client KMIP).
- Vous devez avoir obtenu le certificat public de remplacement pour le serveur KMIP (certificat KMIP Server-)

CA).

- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.
- Si vous remplacez les certificats SSL KMIP dans un environnement MetroCluster, vous devez installer le même certificat SSL KMIP de remplacement sur les deux clusters.



Vous pouvez installer les certificats client et serveur de remplacement sur le serveur KMIP avant ou après l'installation des certificats sur le cluster.

## Étapes

1. Installez le nouveau certificat KMIP Server-ca :

```
security certificate install -type server-ca -vserver <>
```

2. Installez le nouveau certificat client KMIP :

```
security certificate install -type client -vserver <>
```

3. Mettez à jour la configuration du gestionnaire de clés pour utiliser les certificats nouvellement installés :

```
security key-manager external modify -vserver <> -client-cert <> -server-ca  
-certs <>
```

Si vous exécutez ONTAP 9.6 ou version ultérieure dans un environnement MetroCluster et que vous souhaitez modifier la configuration du gestionnaire de clés sur le SVM admin, vous devez exécuter la commande sur les deux clusters de la configuration.



La mise à jour de la configuration du gestionnaire de clés pour utiliser les certificats nouvellement installés renverra une erreur si les clés publiques/privées du nouveau certificat client sont différentes des clés précédemment installées. Voir le ["Base de connaissances NetApp : Les clés publiques ou privées du nouveau certificat client sont différentes du certificat client existant"](#) pour obtenir des instructions sur la façon de contourner cette erreur.

## Informations associées

- ["installation du certificat de sécurité"](#)
- ["modification externe du gestionnaire de clés de sécurité"](#)

# Remplacez un lecteur FIPS ou SED dans ONTAP

Vous pouvez remplacer un lecteur FIPS ou SED de la même façon que vous remplacez un disque ordinaire. Veillez à attribuer de nouvelles clés d'authentification des données au disque de remplacement. Pour un lecteur FIPS, vous pouvez également attribuer une nouvelle clé d'authentification FIPS 140-2.



Si une paire haute disponibilité est utilisée ["Cryptage SAS ou disques NVMe \(SED, NSE, FIPS\)"](#), vous devez suivre les instructions de la rubrique ["Retour d'un lecteur FIPS ou SED en mode non protégé"](#) Pour tous les disques de la paire HA avant d'initialiser le système (options de démarrage 4 ou 9). Si vous ne le faites pas, vous risquez de subir des pertes de données si les disques sont requalifiés.

## Avant de commencer

- Vous devez connaître l'ID de clé pour la clé d'authentification utilisée par le lecteur.
- Vous devez être un administrateur de cluster pour effectuer cette tâche.

## Étapes

1. Vérifiez que le disque a été marqué défectueux :

```
storage disk show -broken
```

Pour en savoir plus, `storage disk show` consultez le ["Référence de commande ONTAP"](#).

```
cluster1::> storage disk show -broken
Original Owner: cluster1-01
Checksum Compatibility: block
```

Physical											Usable
Disk	Outage	Reason	HA	Shelf	Bay	Chan	Pool	Type	RPM	Size	
Size											
-----	----	-----	----	----	----	-----	-----	-----	-----	-----	-----
0.0.0	admin	failed	0b	1	0	A	Pool0	FCAL	10000	132.8GB	
133.9GB											
0.0.7	admin	removed	0b	2	6	A	Pool1	FCAL	10000	132.8GB	
134.2GB											
[...]											

2. Retirez le disque défectueux et remplacez-le par un nouveau lecteur FIPS ou SED, en suivant les instructions du guide matériel de votre modèle de tiroir disque.
3. Attribuez la propriété du disque récemment remplacé :

```
storage disk assign -disk disk_name -owner node
```

Pour en savoir plus, `storage disk assign` consultez le ["Référence de commande ONTAP"](#).

```
cluster1::> storage disk assign -disk 2.1.1 -owner cluster1-01
```

4. Vérifiez que le nouveau disque a été affecté :

```
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>		
-------	------	------------	--	--

1.10.0	data	<id_value>		
--------	------	------------	--	--

1.10.1	data	<id_value>		
--------	------	------------	--	--

2.1.1	open	0x0		
-------	------	-----	--	--

[...]				
-------	--	--	--	--

5. Attribuez les clés d'authentification des données au lecteur FIPS ou SED.

"Attribution d'une clé d'authentification de données à un lecteur FIPS ou SED (gestion de clés externe)"

6. Si nécessaire, attribuez une clé d'authentification FIPS 140-2 au lecteur FIPS.

"Attribution d'une clé d'authentification FIPS 140-2 à un lecteur FIPS"

#### Informations associées

- "affectation de disque de stockage"
- "affichage du disque de stockage"
- "affichage du disque de cryptage de stockage"

## 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...
-------	----------

<p>L'alimentation est disponible pour le système de stockage et vous avez le temps de mettre celui-ci hors ligne aisément</p>	<ol style="list-style-type: none"> <li>Si le système de stockage est configuré en tant que paire haute disponibilité, désactivez le basculement.</li> <li>Mettre tous les agrégats hors ligne et les supprimer</li> <li>Définissez le niveau de privilège sur avancé :  <pre>set -privilege advanced</pre> </li> <li>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 :   <pre>storage encryption disk modify -disk * -fips-key-id 0x0</pre> </li> <li>Arrêter le système de stockage.</li> <li>Démarre en mode de maintenance.</li> <li>Procédez à la suppression ou à la destruction des disques : <ol style="list-style-type: none"> <li>Pour rendre les données sur les disques inaccessibles et continuer à réutiliser les disques, procédez comme suit :  <pre>disk encrypt sanitize -all</pre> </li> <li>Si vous souhaitez rendre les données sur les disques inaccessibles et que vous n'avez pas besoin d'enregistrer les disques, détruisez les disques :  <pre>disk encrypt destroy disk_id1 disk_id2 ...</pre> </li> </ol> </li> </ol>	<p>Le système de stockage est sous tension et vous devez immédiatement détruire les données</p>
---	--	---

<p>a. <b>Si vous souhaitez rendre les données sur les disques inaccessibles et que vous pourrez toujours les réutiliser, désinfectez les disques :</b></p> <p>b. Si le système de stockage est configuré en tant que paire haute disponibilité, désactivez le basculement.</p> <p>c. Définissez le niveau de privilège sur avancé :</p> <pre>set -privilege advanced</pre> <p>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 :</p> <pre>storage encryption disk modify -disk * -fips-key-id 0x0</pre> <p>e. Procédez à la suppression du disque :</p> <pre>storage encryption disk sanitize -disk * -force-all-states true</pre>	<p>a. <b>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></p> <p>b. Si le système de stockage est configuré en tant que paire haute disponibilité, désactivez le basculement.</p> <p>c. Définissez le niveau de privilège sur avancé :</p> <pre>set -privilege advanced</pre> <p>d. Détruire les disques :</p> <pre>storage encryption disk destroy -disk * -force-all-states true</pre>	<p>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.</p>
<p>L'alimentation est disponible pour le serveur KMIP, mais pas pour le système de stockage</p>	<p>a. Connectez-vous au serveur KMIP.</p> <p>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.</p>	<p>L'alimentation n'est pas disponible pour le serveur KMIP ou le système de stockage</p>

#### Informations associées

- ["destruction du disque de cryptage de stockage"](#)
- ["modification du disque de cryptage de stockage"](#)
- ["stockage cryptage disque nettoyage"](#)

# Remettre en service un lecteur FIPS ou SED lorsque les clés d'authentification sont perdues dans ONTAP

Le système traite un lecteur FIPS ou SED comme étant rompu si vous perdez définitivement les clés d'authentification pour lui et que vous ne pouvez pas les récupérer du serveur KMIP. Bien que vous ne puissiez pas accéder ou récupérer les données sur le disque, vous pouvez prendre des mesures pour rendre à nouveau disponible l'espace inutilisé de SED pour les données.

## Avant de commencer

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

## Description de la tâche

Vous ne devez utiliser ce processus que si vous êtes certain que les clés d'authentification du lecteur FIPS ou SED sont définitivement perdues et que vous ne pouvez pas les récupérer.

Si les disques sont partitionnés, ils doivent d'abord être départitionnés avant que vous ne puissiez démarrer ce processus.



La commande permettant de départitionner un disque n'est disponible qu'au niveau du diagnostic et doit être exécutée uniquement sous la supervision du support NetApp . **Il est fortement recommandé de contacter le support NetApp avant de continuer.** Vous pouvez également vous référer à la "[Base de connaissances NetApp : Comment départitionner un disque de secours dans ONTAP](#)".

## Étapes

1. Renvoyez un lecteur FIPS ou SED au service :

Si le SEDS est...	Procédez comme suit...
-------------------	------------------------

<p>Pas en mode de conformité FIPS, ni en mode de conformité FIPS et la clé FIPS est disponible</p>	<ol style="list-style-type: none"> <li>a. Définissez le niveau de privilège sur avancé :  <code>set -privilege advanced</code></li> <li>b. Réinitialisez la clé FIPS sur l'ID sécurisé de fabrication par défaut 0x0 :  <code>storage encryption disk modify -fips-key-id 0x0 -disk <i>disk_id</i></code></li> <li>c. Vérifiez que l'opération a réussi :  <code>storage encryption disk show-status</code>            Si l'opération a échoué, utilisez le processus PSID dans cette rubrique.</li> <li>d. Procédez au nettoyage du disque défaillant :  <code>storage encryption disk sanitize -disk <i>disk_id</i></code>            Vérifiez que l'opération a réussi avec la commande <code>storage encryption disk show-status</code> avant de passer à l'étape suivante.</li> <li>e. Éliminez la panne du disque désinfecté :  <code>storage disk unfail -spare true -disk <i>disk_id</i></code></li> <li>f. Vérifiez si le disque est propriétaire :  <code>storage disk show -disk <i>disk_id</i></code>             Si le disque ne possède pas de propriétaire, attribuez-en un.  <code>storage disk assign -owner node -disk <i>disk_id</i></code>   <ol style="list-style-type: none"> <li>i. Entrez le nodeshell pour le nœud qui possède les disques à désinfecter :   <code>system node run -node <i>node_name</i></code></li> </ol>           Exécutez le <code>disk sanitize release</code> commande.</li> <li>g. Quittez le nodeshell. Éliminez à nouveau la panne du disque :  <code>storage disk unfail -spare true -disk <i>disk_id</i></code></li> <li>h. Vérifier que le disque est désormais une pièce de rechange et prêt à être réutilisé dans un agrégat :  <code>storage disk show -disk <i>disk_id</i></code></li> </ol>
--	--

<p>En mode FIPS-compliance, la clé FIPS n'est pas disponible et les disques SED ont un PSID imprimé sur l'étiquette</p>	<ol style="list-style-type: none"> <li>a. Procurez-vous le PSID du disque à partir de l'étiquette du disque.</li> <li>b. Définissez le niveau de privilège sur avancé :  <pre>set -privilege advanced</pre> </li> <li>c. Réinitialise le disque en fonction des paramètres configurés en usine :  <pre>storage encryption disk revert-to-original-state -disk <i>disk_id</i> -psid <i>disk_physical_secure_id</i></pre> Vérifiez que l'opération a réussi avec la commande <code>storage encryption disk show-status</code> avant de passer à l'étape suivante. </li> <li>d. Si vous utilisez ONTAP 9.8P5 ou une version antérieure, passez à l'étape suivante. Si vous exécutez ONTAP 9.8P6 ou une version ultérieure, éliminez la panne du disque désinfecté.  <pre>storage disk unfail -disk <i>disk_id</i></pre> </li> <li>e. Vérifiez si le disque est propriétaire :  <pre>storage disk show -disk <i>disk_id</i></pre> <p>Si le disque ne possède pas de propriétaire, attribuez-en un.  <pre>storage disk assign -owner node -disk <i>disk_id</i></pre> </p> <ol style="list-style-type: none"> <li>i. Entrez le nodeshell pour le nœud qui possède les disques à désinfecter :  <pre>system node run -node <i>node_name</i></pre> </li> </ol> <p>Exécutez le <code>disk sanitize release</code> commande.</p> </li> <li>f. Quittez le nodeshell. Éliminez à nouveau la panne du disque :  <pre>storage disk unfail -spare true -disk <i>disk_id</i></pre> </li> <li>g. Vérifier que le disque est désormais une pièce de rechange et prêt à être réutilisé dans un agrégat :  <pre>storage disk show -disk <i>disk_id</i></pre> </li> </ol>
---	--

#### Informations associées

- ["modification du disque de cryptage de stockage"](#)
- ["disque de cryptage de stockage retour à l'état d'origine"](#)
- ["stockage cryptage disque nettoyage"](#)
- ["disque de chiffrement de stockage afficher-état"](#)

## Remettre un lecteur FIPS ou SED en mode non protégé dans ONTAP

Un lecteur FIPS ou SED est protégé contre les accès non autorisés uniquement si l'ID de clé d'authentification du nœud est défini sur une valeur autre que la valeur par défaut. Vous pouvez rétablir un lecteur FIPS ou SED en mode non protégé à l'aide de la `storage encryption disk modify` commande pour définir l'ID de clé sur la valeur par défaut. Un lecteur FIPS ou SED en mode non protégé utilise les clés de cryptage par



défaut, tandis qu'un lecteur FIPS ou SED en mode protégé utilise les clés de cryptage secrètes fournies. Si des données chiffrées sont présentes sur le disque et que le disque est réinitialisé en mode non protégé, les données sont toujours chiffrées et ne sont pas exposées.



Suivez cette procédure pour garantir que toutes les données chiffrées deviennent inaccessibles une fois que le lecteur FIPS ou SED est remis en mode non protégé. Une fois les identifiants FIPS et de clé de données réinitialisés, les données existantes ne peuvent plus être déchiffrées et deviennent inaccessibles à moins que les clés d'origine ne soient restaurées.

Si une paire haute disponibilité utilise des disques avec cryptage SAS ou NVMe (SED, NSE, FIPS), vous devez suivre cette procédure pour tous les disques de la paire haute disponibilité avant d'initialiser le système (options de démarrage 4 ou 9). Si vous ne le faites pas, vous risquez de subir des pertes de données si les disques sont requalifiés.

### Avant de commencer

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

### Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. 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 2.10.11 -fips-key-id 0x0
```

```
Info: Starting modify on 14 disks.  
View the status of the operation by using the  
storage encryption disk show-status command.
```

Confirmer la réussite de l'opération à l'aide de la commande :

```
storage encryption disk show-status
```

Répétez la commande `show-status` jusqu'à ce que les nombres dans « Disques commencés » et « Disques terminés » soient identiques.

```
cluster1:: storage encryption disk show-status
```

	FIPS	Latest	Start		Execution	Disks
Disks	Disks					
Node	Support	Request	Timestamp		Time (sec)	Begun
Done	Successful					
-----	-----	-----	-----	-----	-----	-----
-----	-----					
cluster1	true	modify	1/18/2022 15:29:38	3	14	5

1 entry was displayed.

3. Définissez à nouveau l'ID de clé d'authentification des données du nœud sur le MSID 0x0 par défaut :

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

La valeur de `-data-key-id` Doit être défini sur 0x0 si vous retournez un disque SAS ou NVMe en mode non protégé.

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

```
cluster1::> storage encryption disk modify -disk 2.10.11 -data-key-id 0x0
```

```
Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

Confirmer la réussite de l'opération à l'aide de la commande :

```
storage encryption disk show-status
```

Répétez la commande `show-status` jusqu'à ce que les chiffres soient identiques. L'opération est terminée lorsque les nombres dans « disques commencés » et « disques terminés » sont les mêmes.

## Mode Maintenance

Depuis ONTAP 9.7, vous pouvez ressaisir un disque FIPS à partir du mode de maintenance. Si vous ne pouvez pas utiliser les instructions de l'interface de ligne de commandes ONTAP décrites dans la section précédente, vous devez utiliser le mode de maintenance.

### Étapes

1. Définissez à nouveau l'ID de clé d'authentification FIPS du nœud sur le MSID 0x0 par défaut :

```
disk encrypt rekey_fips 0x0 disklist
```

2. Définissez à nouveau l'ID de clé d'authentification des données du nœud sur le MSID 0x0 par défaut :

```
disk encrypt rekey 0x0 disklist
```

3. Vérifiez que la clé d'authentification FIPS a bien été reclés :

```
disk encrypt show_fips
```

4. Confirmer que la clé d'authentification des données a bien été reclés avec :

```
disk encrypt show
```

Votre sortie affichera probablement soit l'ID de clé MSID 0x0 par défaut, soit la valeur de 64 caractères détenue par le serveur de clés. Le `Locked?` ce champ fait référence au verrouillage des données.

Disk	FIPS Key ID	Locked?
0a.01.0	0x0	Yes

#### Informations associées

- ["modification du disque de cryptage de stockage"](#)
- ["disque de chiffrement de stockage afficher-état"](#)

## Supprimez une connexion de gestionnaire de clés externe dans ONTAP

Si vous n'avez plus besoin du serveur, vous pouvez déconnecter un serveur KMIP d'un nœud. Par exemple, vous pouvez déconnecter un serveur KMIP lorsque vous passez au chiffrement de volume.

#### Description de la tâche

Lorsque vous déconnectez un serveur KMIP d'un nœud d'une paire haute disponibilité, le système déconnecte automatiquement le serveur de tous les nœuds du cluster.



Si vous prévoyez de continuer à utiliser la gestion externe des clés après la déconnexion d'un serveur KMIP, assurez-vous qu'un autre serveur KMIP est disponible pour assurer le service des clés d'authentification.

#### Avant de commencer

Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

#### Étape

1. Déconnectez un serveur KMIP du nœud actuel :

Pour cette version ONTAP...	Utilisez cette commande...
ONTAP 9.6 et versions ultérieures	<code>`security key-manager external remove-servers -vserver SVM -key -servers host_name`</code>

IP\_address:port,...`

ONTAP 9.5 et versions antérieures

Dans un environnement MetroCluster, il faut répéter ces commandes sur les deux clusters pour le SVM admin.

La commande ONTAP 9.6 suivante désactive les connexions à deux serveurs de gestion des clés externes pour `cluster1`, le premier nommé `ks1`, Écoute sur le port par défaut 5696, le second avec l'adresse IP 10.0.0.20, écoute sur le port 24482 :

```
cluster1::> security key-manager external remove-servers -vserver  
cluster-1 -key-servers ks1,10.0.0.20:24482
```

Pour en savoir plus sur `security key-manager external remove-servers` et `security key-manager delete` dans le ["Référence de commande ONTAP"](#).

## Modifier les propriétés du serveur de gestion de clés externes ONTAP

À partir de ONTAP 9.6, vous pouvez utiliser le `security key-manager external modify-server` Commande permettant de modifier le délai d'attente d'E/S et le nom d'utilisateur d'un serveur de gestion de clés externe.

### Avant de commencer

- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.
- Des privilèges avancés sont requis pour cette tâche.
- Dans un environnement MetroCluster, vous devez répéter ces étapes sur les deux clusters pour la SVM d'administration.

### Étapes

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

```
set -privilege advanced
```

2. Modifiez les propriétés externes du serveur du gestionnaire de clés pour le cluster :

```
security key-manager external modify-server -vserver admin_SVM -key-server  
host_name|IP_address:port,... -timeout 1...60 -username user_name
```



La valeur de temporisation est exprimée en secondes. Si vous modifiez le nom d'utilisateur, vous êtes invité à entrer un nouveau mot de passe. Si vous exécutez la commande à l'invite de connexion du cluster, `admin_SVM` Par défaut au SVM admin du cluster actuel. Vous devez être l'administrateur de cluster pour modifier les propriétés du serveur du gestionnaire de clés externe.

La commande suivante remplace la valeur de temporisation par 45 secondes pour le `cluster1` serveur de gestion externe des clés à l'écoute sur le port par défaut 5696 :

```
cluster1::> security key-manager external modify-server -vserver  
cluster1 -key-server ks1.local -timeout 45
```

### 3. Modifier les propriétés du serveur gestionnaire de clés externe pour un SVM (NVE uniquement) :

```
security key-manager external modify-server -vserver SVM -key-server  
host_name|IP_address:port,... -timeout 1...60 -username user_name
```



La valeur de temporisation est exprimée en secondes. Si vous modifiez le nom d'utilisateur, vous êtes invité à entrer un nouveau mot de passe. Si vous exécutez la commande à l'invite de connexion du SVM, *SVM* Par défaut au SVM actuel Vous devez être l'administrateur du cluster ou de SVM pour modifier les propriétés du serveur externe Key Manager.

La commande suivante modifie le nom d'utilisateur et le mot de passe de *svm1* serveur de gestion externe des clés à l'écoute sur le port par défaut 5696 :

```
svm1::> security key-manager external modify-server -vserver svm11 -key  
-server ks1.local -username svm1user  
Enter the password:  
Reenter the password:
```

### 4. Répétez la dernière étape pour tout SVM supplémentaire.

#### Informations associées

- ["gestionnaire de clés de sécurité serveur de modification externe"](#)

## Passez à la gestion externe des clés grâce à la gestion intégrée des clés dans ONTAP

Pour basculer de la gestion externe des clés à partir de la gestion intégrée des clés, vous devez supprimer la configuration intégrée de la gestion des clés avant de pouvoir activer la gestion externe des clés.

#### Avant de commencer

- Pour le chiffrement matériel, vous devez réinitialiser les clés de données de tous les lecteurs FIPS ou SED à la valeur par défaut.

["Retour d'un lecteur FIPS ou SED en mode non protégé"](#)

- Pour le chiffrement logiciel, vous devez déchiffrer tous les volumes.

["Sans chiffrement des données de volume"](#)

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

#### Étape

1. Supprimez la configuration intégrée de gestion des clés d'un cluster :

Pour cette version ONTAP...	Utilisez cette commande...
ONTAP 9.6 et versions ultérieures	<code>security key-manager onboard disable -vserver SVM</code>
ONTAP 9.5 et versions antérieures	<code>security key-manager delete-key-database</code>

Pour en savoir plus sur `security key-manager onboard disable` et `security key-manager delete-key-database` dans le ["Référence de commande ONTAP"](#).

## Passer de la gestion des clés externes à la gestion des clés intégrée ONTAP

Pour passer à la gestion des clés intégrée, supprimez la configuration de gestion des clés externes avant d'activer la gestion des clés intégrée.

### Avant de commencer

- Pour le chiffrement matériel, vous devez réinitialiser les clés de données de tous les lecteurs FIPS ou SED à la valeur par défaut.

["Retour d'un lecteur FIPS ou SED en mode non protégé"](#)

- Vous devez avoir supprimé toutes les connexions externes du gestionnaire de clés.

["Suppression d'une connexion externe au gestionnaire de clés"](#)

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

### Étapes

La procédure de transition de la gestion des clés dépend de la version de ONTAP que vous utilisez.

### ONTAP 9.6 et versions ultérieures

1. Changement au niveau de privilège avancé :

```
set -privilege advanced
```

2. Utiliser la commande :

```
security key-manager external disable -vserver admin_SVM
```



Dans un environnement MetroCluster, il faut répéter la commande sur les deux clusters pour la SVM admin.

En savoir plus sur `security key-manager external disable` dans le ["Référence de commande ONTAP"](#).

### ONTAP 9.5 et versions antérieures

Utiliser la commande :

```
security key-manager delete-kmip-config
```

En savoir plus sur `security key-manager delete-kmip-config` dans le ["Référence de commande ONTAP"](#).

### Informations associées

- ["désactivation externe du gestionnaire de clés de sécurité"](#)

## Que se passe-t-il lorsque les serveurs de gestion de clés ne sont pas accessibles pendant le processus de démarrage ONTAP

ONTAP prend certaines précautions afin d'éviter tout comportement indésirable dans l'éventualité où un système de stockage configuré pour NSE ne puisse pas atteindre l'un des serveurs de gestion des clés spécifiés lors du processus de démarrage.

Si le système de stockage est configuré pour NSE, les disques SED sont de nouveau et verrouillés, et les disques SED sont sous tension, le système de stockage doit récupérer les clés d'authentification requises à partir des serveurs de gestion des clés pour s'authentifier auprès des disques SED avant qu'ils puissent accéder aux données.

Le système de stockage tente de contacter les serveurs de gestion des clés spécifiés pendant jusqu'à trois heures. Si le système de stockage ne peut pas atteindre l'un d'eux après ce délai, le processus d'amorçage s'arrête et le système de stockage s'arrête.

Si le système de stockage contacte avec succès un serveur de gestion de clés spécifié, il tente alors d'établir une connexion SSL pendant 15 minutes. Si le système de stockage ne parvient pas à établir de connexion SSL avec un serveur de gestion de clés spécifié, le processus d'amorçage s'arrête et le système de stockage s'arrête.

Pendant que le système de stockage tente de contacter et de se connecter aux serveurs de gestion des clés, il

affiche des informations détaillées sur les tentatives de contact ayant échoué au niveau de l'interface de ligne de commande. Vous pouvez interrompre les tentatives de contact à tout moment en appuyant sur Ctrl-C.

Par mesure de sécurité, les disques SED ne permettent qu'un nombre limité de tentatives d'accès non autorisées, après quoi ils désactivent l'accès aux données existantes. Si le système de stockage ne peut pas contacter les serveurs de gestion des clés spécifiés pour obtenir les clés d'authentification appropriées, il peut uniquement tenter de s'authentifier auprès de la clé par défaut, ce qui entraîne une tentative d'échec et un incident. Si le système de stockage est configuré pour redémarrer automatiquement en cas de panique, il entre dans une boucle d'amorçage qui entraîne des tentatives d'authentification continues sur les disques SED ayant échoué.

Dans ces scénarios, l'arrêt du système de stockage a été conçu pour éviter que le système de stockage ne pénétre dans une boucle d'amorçage et qu'il puisse y avoir des pertes de données inattendues suite au verrouillage permanent des disques SED, raison du dépassement de la limite de sécurité d'un certain nombre de tentatives d'authentification consécutives ayant échoué. La limite et le type de protection de verrouillage dépendent des spécifications de fabrication et du type de SED :

Type SED	Nombre de tentatives d'authentification consécutives ayant échoué entraînant un blocage	Type de protection de verrouillage lorsque la limite de sécurité est atteinte
DISQUES DURS	1024	Permanent. Les données ne peuvent pas être restaurées, même si la clé d'authentification appropriée est à nouveau disponible.
X440_PHM2800MCTO SSD NSE 800 Go avec révisions du firmware NA00 ou NA01	5	Temporaire. Le verrouillage est activé uniquement jusqu'à ce que le disque soit mis hors/sous tension.
X577_PHM2800MNA00 SSD NSE 800 Go avec révisions de firmware ou NA01	5	Temporaire. Le verrouillage est activé uniquement jusqu'à ce que le disque soit mis hors/sous tension.
X440_PHM2800MCTO SSD NSE 800 Go avec révisions de firmware plus élevées	1024	Permanent. Les données ne peuvent pas être restaurées, même si la clé d'authentification appropriée est à nouveau disponible.
X577_PHM2800MCTO SSD NSE 800 Go avec révisions de micrologiciel plus élevées	1024	Permanent. Les données ne peuvent pas être restaurées, même si la clé d'authentification appropriée est à nouveau disponible.
Tous les autres modèles de SSD	1024	Permanent. Les données ne peuvent pas être restaurées, même si la clé d'authentification appropriée est à nouveau disponible.

Pour tous les types SED, une authentification réussie réinitialise le nombre d'essayer à zéro.



Si vous rencontrez ce scénario lorsque le système de stockage est arrêté en raison d'un échec d'accès aux serveurs de gestion de clés spécifiés, vous devez d'abord identifier et corriger la cause de l'échec de communication avant de poursuivre le démarrage du système de stockage.

## Désactiver le cryptage ONTAP par défaut

Depuis ONTAP 9.7, le chiffrement d'agrégat et de volume est activé par défaut si vous disposez d'une licence VE (Volume Encryption) et utilisez un gestionnaire de clés intégré ou externe. Si nécessaire, vous pouvez désactiver le chiffrement par défaut pour l'ensemble du cluster.

### Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche, ou un administrateur de SVM à qui l'administrateur du cluster a délégué des pouvoirs.

### Étape

1. Pour désactiver le chiffrement par défaut pour l'ensemble du cluster dans ONTAP 9.7 ou version ultérieure, exécutez la commande suivante :

```
options -option-name encryption.data_at_rest_encryption.disable_by_default  
-option-value on
```

## 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 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.