Gestion du cryptage NetApp

ONTAP 9

NetApp
March 24, 2023

Table des matières

Gestion du cryptage NetApp . . . 1
- Déchiffrement des données de volume . . . 1
- Déplacement d'un volume chiffré . . . 1
- Autorité déléguée pour exécuter la commande volume Move . . . 3
- Modifiez la clé de chiffrement d'un volume à l'aide de la commande Volume Encryption rekey start . . . 3
- Modifiez la clé de chiffrement d'un volume à l'aide de la commande volume Move start . . . 4
- Rotation des clés d'authentification pour NetApp Storage Encryption . . . 5
- Supprimez un volume chiffré . . . 6
- Supprimez les données de façon sécurisée sur un volume chiffré . . . 7
- Modifiez la phrase secrète intégrée pour la gestion des clés . . . 13
- Sauvegardez manuellement les informations intégrées de gestion des clés . . . 14
- Restaurez les clés de chiffrement intégrées de gestion des clés . . . 15
- Restaurez les clés de chiffrement externes pour la gestion des clés . . . 17
- Remplacer les certificats SSL . . . 18
- Remplacez un lecteur FIPS ou SED . . . 19
- Rendre les données d'un lecteur FIPS ou SED inaccessibles . . . 21
- Renvoyez un lecteur FIPS ou SED au service en cas de perte de clés d'authentification . . . 28
- Retournez un lecteur FIPS ou SED en mode non protégé . . . 30
- Supprimez une connexion externe au gestionnaire de clés . . . 32
- Modifiez les propriétés du serveur de gestion externe des clés . . . 33
- Transition vers la gestion externe des clés à partir de la gestion intégrée des clés . . . 34
- Transition vers la gestion intégrée des clés à partir d'une gestion externe des clés . . . 35
- Que se passe-t-il lorsque les serveurs de gestion des clés ne sont pas accessibles lors du processus de démarrage . . . 35
- Désactivez le chiffrement par défaut avec ONTAP 9.7 et versions ultérieures . . . 37

Gestion du cryptage NetApp

Déchiffrement des données de volume

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

Ce dont vous avez besoin

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.

"Délégation d'autorité pour exécuter la commande de déplacement de volume"

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 connaître la syntaxe complète de la commande, reportez-vous à la page man.

   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 connaître la syntaxe complète de la commande, reportez-vous à la page man.

   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

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.

Ce dont vous avez besoin

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.

"Délégation d'autorité pour exécuter la commande de déplacement de volume"

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. Vous devez spécifier explicitement que vous ne voulez pas que le volume de destination soit chiffré afin de vous assurer que vous ne déchiffrez pas par inadvertance les données du volume.

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 connaître la syntaxe complète de la commande, reportez-vous à la page man.

   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 connaître la syntaxe complète de la commande, reportez-vous à la page man.

   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%
   ```

Autorité déléguée pour exécuter la commande volume Move

Vous pouvez utiliser le `volume move` commande pour chiffrer un volume existant, déplacer un volume chiffré ou annuler le chiffrement d'un volume. Les administrateurs du cluster peuvent exécuter `volume move` Ils peuvent se passer eux-mêmes de la commande ou déléguer à l'autorité pour qu'elle exécute la commande aux administrateurs du SVM.

Description de la tâche

Par défaut, les administrateurs du SVM sont affectés au système `vsadmin` rôle, qui ne comprend pas l'autorité nécessaire pour déplacer les volumes. Vous devez affecter le `vsadmin-volume` Rôle aux administrateurs SVM afin de leur permettre d'exécuter les `volume move` commande.

Étape

1. Déléguer l'autorité pour exécuter le `volume move` commande :

   `security login modify -vserver` *`SVM_name`* `-user-or-group-name` *`user_or_group_name`* `-application` *`application`* `-authmethod` *`authentication_method`* `-role` *`vsadmin-volume`*

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   La commande suivante permet à l'administrateur du SVM d'exécuter le `volume move` commande.

   ```
   cluster1::>security login modify -vserver engData -user-or-group-name
   SVM-admin -application ssh -authmethod domain -role vsadmin-volume
   ```

Modifiez la clé de chiffrement d'un volume à l'aide de la commande Volume Encryption rekey start

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 SVM`vs1`:

   ```
   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 connaître la syntaxe complète de la commande, reportez-vous à la page man.

   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 connaître la syntaxe complète de la commande, reportez-vous à la page man.

   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%
   ```

Modifiez la clé de chiffrement d'un volume à l'aide de la commande volume Move start

Il est recommandé de modifier régulièrement la clé de chiffrement d'un volume. Vous pouvez utiliser le `volume move start` commande pour changer la clé de chiffrement. Vous devez utiliser `volume move start` Dans ONTAP 9.2 et versions antérieures. Le volume déplacé peut résider sur le même agrégat ou sur un autre agrégat.

Ce dont vous avez besoin

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.

"Délégation d'autorité pour exécuter la commande de déplacement de volume"

Description de la tâche

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

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 connaître la syntaxe complète de la commande, reportez-vous à la page man.

   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 connaître la syntaxe complète de la commande, reportez-vous à la page man.

   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 NetApp Storage Encryption

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.

Supprimez un volume chiffré

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

Ce dont vous avez besoin

- 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.

  "Délégation d'autorité pour exécuter la commande de déplacement de volume"

- Le volume doit être hors ligne.

Étape

1. Supprimez un volume chiffré :

   `volume delete -vserver SVM_name -volume volume_name`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   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.

   Utiliser `volume delete` avec le `-force true` option permettant de supprimer un volume et de détruire immédiatement la clé de chiffrement correspondante. Cette commande nécessite des privilèges avancés. Pour plus d'informations, consultez la page man.

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

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

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

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

Considérations relatives à l'utilisation de la suppression sécurisée

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

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

ONTAP 9.8 et versions ultérieures

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

ONTAP 9.7 et versions antérieures :

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

  Si des copies Snapshot sont occupées dans le volume, vous devez libérer les copies Snapshot avant de pouvoir purger le volume. Par exemple, vous devrez peut-être séparer un volume FlexClone de son volume parent.
- L'appel réussi de la fonction de suppression sécurisée déclenche un déplacement de volume qui recrypte les données restantes non supprimées avec une nouvelle clé.

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

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

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

Ce dont vous avez besoin

- 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. 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 vol_name -snapshot
   ```

4. Supprimez les fichiers supprimés de manière sécurisée :

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

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

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

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

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

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

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

Ce dont vous avez besoin

- 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, 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 chaque volume de la relation SnapMirror asynchrone.

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

   ```
   snapshot delete -vserver SVM_name -volume vol_name -snapshot
   ```

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

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

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

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

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

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

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

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

b. Vérifiez que la copie Snapshot de base est présente :
   `snapshot show -vserver SVM_name -volume vol_name`

c. Supprimez la copie Snapshot de base :
   `snapshot delete -vserver SVM_name -volume vol_name -snapshot snapshot`

6. Supprimez les fichiers supprimés de manière sécurisée :

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

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

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

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

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

   `volume encryption secure-purge show`

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

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

Ce dont vous avez besoin

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

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.

Étapes

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

```
set -privilege advanced
```

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

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

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

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

   ```
   snapshot delete -vserver SVM_name -volume vol_A -snapshot snapshot
   ```

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

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

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

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

   ```
   snapshot delete -vserver SVM_name -volume vol_name -snapshot snapshot
   ```

   Effectuer cette étape sur les deux volumes.

7. Supprimez les fichiers supprimés de manière sécurisée :

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

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

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

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

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

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

Modifiez la phrase secrète intégrée pour la gestion des clés

Il est recommandé d'appliquer régulièrement une meilleure pratique de sécurité à la modification de la phrase secrète intégrée pour la gestion des clés. Copiez la nouvelle phrase secrète intégrée pour la gestion des clés dans un emplacement sécurisé en dehors du système de stockage pour une utilisation ultérieure.

Ce dont vous avez besoin

- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.
- Des privilèges avancés sont requis pour cette tâche.

Étapes

1. Changement au niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

2. Modifiez la phrase secrète intégrée pour la gestion des clés :

Pour cette version ONTAP…	Utilisez cette commande…
ONTAP 9.6 et versions ultérieures	`security key-manager onboard update-passphrase`
ONTAP 9.5 et versions antérieures	`security key-manager update-passphrase`

   Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.

   La commande suivante de ONTAP 9.6 vous permet de modifier la phrase secrète de gestion intégrée des clés pour `cluster1`:

   ```
   cluster1::> security key-manager onboard update-passphrase
   Warning: This command will reconfigure the cluster passphrase for
   onboard key management for Vserver "cluster1".
   Do you want to continue? {y|n}: y
   Enter current passphrase:
   Enter new passphrase:
   ```

3. Entrez `y` à l'invite, vous pouvez modifier la phrase secrète intégrée pour la gestion des clés.
4. Saisissez la phrase de passe actuelle à l'invite de phrase de passe actuelle.
5. À l'invite de la nouvelle phrase de passe, entrez une phrase de passe comprise entre 32 et 256 caractères, ou une phrase de passe entre 64 et 256 caractères pour « mode CC ».

   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.

6. À l'invite de confirmation de la phrase de passe, saisissez à nouveau la phrase de passe.

Une fois que vous avez terminé

Dans un environnement MetroCluster, vous devez mettre à jour la phrase secrète sur le cluster partenaire :

- Dans ONTAP 9.5 et les versions antérieures, vous devez exécuter `security key-manager update-passphrase` avec la même phrase secrète sur le cluster partenaire.
- Dans ONTAP 9.6 et versions ultérieures, vous êtes invité à exécuter `security key-manager onboard sync` avec la même phrase secrète sur le cluster partenaire.

Copiez le mot de passe de gestion des clés intégré vers un emplacement sécurisé en dehors du système de stockage pour une utilisation ultérieure.

Vous devez sauvegarder manuellement les informations de gestion des clés chaque fois que vous modifiez la phrase secrète de gestion intégrée des clés.

"Sauvegarde manuelle des informations de gestion intégrée des clés"

Sauvegardez manuellement les informations intégrées de gestion des clés

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.

Ce dont vous avez besoin

- 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	`security key-manager onboard show-backup`
ONTAP 9.5 et versions antérieures	`security key-manager backup show`

Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.

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

+

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

     --------------------------BEGIN BACKUP--------------------------
     TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
     QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
     dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
     3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
     IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
     QRHwv+1aWvAAAAAAAAAAACQAAAAAAAAAgAAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
     BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
     AQAAAAMAAAAYAQAAAAAAADA5/ccAAAAAIgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAA
     AAAAAAAAAAACAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAACIAAAAAAAAA
     KAAAAAAAAACI8z/bAAAAAAAAAAAAAAAAAgAAAAAAAQAbxMcI4qiaMS4Uts5tTUnU
     AAAAAAAAAAAkAAAAAAAAAIAAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5Smyj
     LSgoK/qc8FAmMMcrRXY6uriulnL0WPB/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAwAAABgBAAAAAAAA
     1cNLLwAAAAAiAAAAAAAAAACgAAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAAIAAAAAAAAkA
     ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAAIgAAAAAAAAAoAAAAAAAAAJ4/cQsAAAAA
     AAAAAAAAAAACAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAAAACQAAAAAAAAA
     gAAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rrH4nPQM0n
     rDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     ---------------------------END BACKUP---------------------------
```

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

Restaurez les clés de chiffrement intégrées de gestion des clés

Si vous devez restaurer une clé de chiffrement intégrée de gestion des clés, vérifiez d’abord qu’une clé doit être restaurée, vous pouvez configurer le gestionnaire de clés

intégré pour restaurer la clé.

Avant de commencer

- Si vous utilisez NSE avec un serveur de gestion externe des clés (KMIP), vous devez avoir supprimé la base de données de gestionnaire de clés externe.

  "Transition vers la gestion intégrée des clés à partir d'une gestion externe des clés"

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

Étapes pour ONTAP 9.6 et versions ultérieures

1. Vérifiez que la clé doit être restaurée :
   `security key-manager key query -node node`
2. Si vous exécutez ONTAP 9.8 ou version ultérieure et que le volume racine est chiffré, procédez comme oui [root_volume_encrypted].

   Si vous exécutez ONTAP 9.6 ou 9.7, ou si vous utilisez ONTAP 9.8 ou une version ultérieure et que votre volume racine n'est pas chiffré, ignorez cette étape.

3. Restaurer la clé :
   `security key-manager onboard sync`

   Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.

   La commande ONTAP 9.6 suivante synchronise les clés dans la hiérarchie de clés intégrée :

   ```
   cluster1::> security key-manager onboard sync

   Enter the cluster-wide passphrase for onboard key management in Vserver
   "cluster1"::    <32..256 ASCII characters long text>
   ```

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

Étapes pour ONTAP 9.5 et versions antérieures

1. Vérifiez que la clé doit être restaurée :
   `security key-manager key show`
2. Si vous exécutez ONTAP 9.8 ou version ultérieure et que votre volume racine est chiffré, procédez comme suit :

   Si vous exécutez ONTAP 9.6 ou 9.7, ou si vous utilisez ONTAP 9.8 ou une version ultérieure et que votre volume racine n'est pas chiffré, ignorez cette étape.

3. Restaurer la clé :
   `security key-manager setup -node node`

   Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.

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

Étapes si le volume racine est 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 le phrase secrète de gestion intégrée des clés pour le cluster.
4. À l'invite, entrez 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`.

Restaurez les clés de chiffrement externes pour la gestion des clés

Vous pouvez restaurer manuellement les clés de cryptage externes de gestion des clés et les « pousser » vers un nœud différent. Vous pouvez le faire si vous redémarrez un nœud qui était temporairement arrêté lorsque vous avez créé les clés du cluster.

Ce dont vous avez besoin

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

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.

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 par défaut. Pour connaître la syntaxe complète des commandes, consultez les pages de manuels. 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`:

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

Remplacer les certificats SSL

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.
- Dans un environnement MetroCluster, vous devez remplacer le certificat SSL KMIP 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 renvoie une erreur si les clés publiques/privées du nouveau certificat client sont différentes des clés installées précédemment. Consultez l'article de la base de connaissances "Le nouveau certificat client les clés publiques ou privées sont différentes du certificat client existant" pour obtenir des instructions sur la manière de neutraliser cette erreur.

Remplacez un lecteur FIPS ou SED

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.

Ce dont vous avez besoin

- 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 connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster1::> storage disk show -broken
Original Owner: cluster1-01
  Checksum Compatibility: block
                                                                    Usable
Physical
    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 connaître la syntaxe complète de la commande, reportez-vous à la page man.

   ```
   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 connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
------------------------------------------------------------------
0.0.0   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
0.0.1   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
1.10.0  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
1.10.1  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
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"

Rendre les données d'un lecteur FIPS ou SED inaccessibles

Rendre les données 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.

Désinfectez un lecteur FIPS ou SED

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.

Ce dont vous avez besoin

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

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.

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`*

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

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

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 connaître la syntaxe complète de la commande, reportez-vous à la page man.

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   ------------------------------------------------------------------
   0.0.0   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   1.10.2  data
   F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
   [...]
   ```

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 désinfecter tous les disques, quel que soit leur type, utilisez le `-force-all-state` option. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

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 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.
```

Détruire un lecteur FIPS ou SED

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.

Ce dont vous avez besoin

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

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.

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`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

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

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

   `storage encryption disk show`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   ------------------------------------------------------------------
   0.0.0   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   1.10.2  data
   F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
   [...]
   ```

4. Détruire le disque :

   `storage encryption disk destroy -disk disk_id`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   > 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.
```

Suppression d’urgence des données sur un lecteur FIPS ou SED

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.

Ce dont vous avez besoin

- 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 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 : ◦ Si vous souhaitez rendre les données sur les disques inaccessibles et que vous pouvez encore les réutiliser, procédez à leur nettoyage : `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, détruire 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

Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.

Renvoyez un lecteur FIPS ou SED au service en cas de perte de clés d'authentification

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. inclus :./_include/unpartition-disk.adoc[]

Étapes

1. Renvoyez un lecteur FIPS ou SED au service :

Si le SEDS est…	Procédez comme suit…

Pas en mode de conformité FIPS, ni en mode de conformité FIPS et la clé FIPS est disponible	a. Définissez le niveau de privilège sur avancé :
	`set -privilege advanced`
	b. Réinitialisez la clé FIPS sur l'ID sécurisé de fabrication par défaut 0x0 :
	`storage encryption disk modify -fips-key-id 0x0 -disk disk_id`
	c. Vérifiez que l'opération a réussi :
	`storage encryption disk show-status`Si l'opération a échoué, utilisez le processus PSID dans cette rubrique.
	d. Procédez au nettoyage du disque défaillant :
	`storage encryption disk sanitize -disk disk_id`Vérifiez que l'opération a réussi avec la commande `storage encryption disk show-status` avant de passer à l'étape suivante.
	e. Éliminez la panne du disque désinfecté :
	`storage disk unfail -spare true -disk disk_id`
	f. Vérifiez si le disque est propriétaire :
	`storage disk show -disk disk_id`
	g. Si le disque ne dispose pas d'un propriétaire, affectez-en un, puis annulez de nouveau l'échec du disque :
	`storage disk assign -owner node -disk disk_id`
	`storage disk unfail -spare true -disk disk_id`
	h. Vérifier que le disque est désormais une pièce de rechange et prêt à être réutilisé dans un agrégat :
	`storage disk show -disk disk_id`

En mode FIPS-compliance, la clé FIPS n'est pas disponible et les disques SED ont un PSID imprimé sur l'étiquette	a. Procurez-vous le PSID du disque à partir de l'étiquette du disque.
	b. Définissez le niveau de privilège sur avancé :
	`set -privilege advanced`
	c. Réinitialise le disque en fonction des paramètres configurés en usine :
	`storage encryption disk revert-to-original-state -disk disk_id -psid disk_physical_secure_id`Vérifiez que l'opération a réussi avec la commande `storage encryption disk show-status` avant de passer à l'étape suivante.
	d. Éliminez la panne du disque désinfecté :
	`storage disk unfail -spare true -disk disk_id`
	e. Vérifiez si le disque est propriétaire :
	`storage disk show -disk disk_id`
	f. Si le disque ne dispose pas d'un propriétaire, affectez-en un, puis annulez de nouveau l'échec du disque :
	`storage disk assign -owner node -disk disk_id`
	`storage disk unfail -spare true -disk disk_id`
	g. Vérifier que le disque est désormais une pièce de rechange et prêt à être réutilisé dans un agrégat :
	`storage disk show -disk disk_id`

Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.

Retournez un lecteur FIPS ou SED en mode non protégé

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.

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.

Ce dont vous avez besoin

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 chiffres de "disques commencés" et de "disques réalisés" 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
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 réalisés" sont identiques.

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
```

Supprimez une connexion externe au gestionnaire de clés

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.

Ce dont vous avez besoin

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

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.

Étape

1. Déconnectez un serveur KMIP du nœud actuel :

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

Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.

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 :

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

Modifiez les propriétés du serveur de gestion externe des clés

Vous pouvez utiliser ONTAP 9.6 à partir de `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 :

   ```
   clusterl::> 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.

Transition vers la gestion externe des clés à partir de la gestion intégrée des clés

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.

Ce dont vous avez besoin

- 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	`security key-manager onboard disable -vserver SVM`
ONTAP 9.5 et versions antérieures	`security key-manager delete-key-database`

Pour connaître la syntaxe complète de la commande, reportez-vous au "Pages de manuel ONTAP".

Transition vers la gestion intégrée des clés à partir d'une gestion externe des clés

Pour basculer vers la gestion intégrée des clés à partir d'une gestion externe des clés, vous devez supprimer la configuration de gestion externe des clés pour pouvoir activer la gestion intégrée 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"

- 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.

Procédure

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.

ONTAP 9.5 et versions antérieures

Utiliser la commande :
`security key-manager delete-kmip-config`

Que se passe-t-il lorsque les serveurs de gestion des clés ne sont pas accessibles lors du processus de démarrage

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 pénètre 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.

Désactivez le chiffrement par défaut avec ONTAP 9.7 et versions ultérieures

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. Vous pouvez désactiver le cryptage par défaut pour l'ensemble du cluster, si nécessaire.

Ce dont vous avez besoin

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
   ```