Rendre les données d'un lecteur FIPS ou SED inaccessibles

ONTAP 9

NetApp
April 24, 2024

Sommaire

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.

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`*

   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.

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.
```

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.

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`

   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.
```

Données d'urgence déchirées 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.

Avant de commencer

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

Étape

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

Si…	Alors…

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

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

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

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