



# **Configurez la gestion externe des clés**

## **ONTAP 9**

NetApp  
February 13, 2026

# Sommaire

Configurez la gestion externe des clés .....	1
En savoir plus sur la configuration de la gestion des clés externes ONTAP .....	1
Installer des certificats SSL sur le cluster ONTAP .....	1
Activer la gestion des clés externes pour le chiffrement matériel dans ONTAP 9.6 et versions ultérieures ..	2
Activer la gestion des clés externes pour le chiffrement matériel dans ONTAP 9.5 et versions antérieures ..	4
Configurez des serveurs de clés externes en cluster dans ONTAP .....	5
Créer un serveur de clés mis en cluster .....	6
Modifier les serveurs de clés en cluster .....	8
Créez des clés d'authentification dans ONTAP 9.6 et versions ultérieures .....	9
Création de clés d'authentification dans ONTAP 9.5 et versions antérieures .....	12
Attribuer une clé d'authentification de données à un lecteur FIPS ou SED avec la gestion des clés externes ONTAP .....	14

# Configurez la gestion externe des clés

## En savoir plus sur la configuration de la gestion des clés externes ONTAP

Vous pouvez utiliser un ou plusieurs serveurs externes de gestion des clés pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Un serveur externe de gestion des clés est un système tiers de votre environnement de stockage qui transmet des clés aux nœuds à l'aide du protocole KMIP (Key Management Interoperability Protocol).

NVE (NetApp Volume Encryption) peut être implémenté avec le gestionnaire de clés intégré. Dans ONTAP 9.3 et versions ultérieures, NVE peut être implémenté avec une gestion des clés externe (KMIP) et un gestionnaire de clés intégré. Depuis la version ONTAP 9.11.1, vous pouvez configurer plusieurs gestionnaires de clés externes dans un cluster. Voir [Configurez les serveurs de clés en cluster](#).

## Installer des certificats SSL sur le cluster ONTAP

Le cluster et le serveur KMIP utilisent des certificats SSL KMIP pour vérifier l'identité de l'autre et établir une connexion SSL. Avant de configurer la connexion SSL avec le serveur KMIP, vous devez installer les certificats SSL du client KMIP pour le cluster et le certificat public SSL pour l'autorité de certification racine (CA) du serveur KMIP.

### Description de la tâche

Dans une paire haute disponibilité, les deux nœuds doivent utiliser les mêmes certificats SSL publics et privés KMIP. Si vous connectez plusieurs paires haute disponibilité au même serveur KMIP, tous les nœuds des paires haute disponibilité doivent utiliser les mêmes certificats SSL publics et privés.

### Avant de commencer

- L'heure doit être synchronisée sur le serveur qui crée les certificats, le serveur KMIP et le cluster.
- Vous devez avoir obtenu le certificat public du client SSL KMIP pour le cluster.
- Vous devez avoir obtenu la clé privée associée au certificat client SSL KMIP pour le cluster.
- Le certificat client SSL KMIP ne doit pas être protégé par un mot de passe.
- Vous devez avoir obtenu le certificat public SSL pour l'autorité de certification racine (CA) du serveur KMIP.
- Dans un environnement MetroCluster, vous devez installer les mêmes certificats SSL KMIP sur les deux clusters.



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

### Étapes

1. Installez les certificats client SSL KMIP pour le cluster :

```
security certificate install -vserver admin_svm_name -type client
```

Vous êtes invité à entrer les certificats SSL KMIP publics et privés.

```
cluster1::> security certificate install -vserver cluster1 -type client
```

2. Installez le certificat public SSL pour l'autorité de certification racine (CA) du serveur KMIP :

```
security certificate install -vserver admin_svm_name -type server-ca
```

```
cluster1::> security certificate install -vserver cluster1 -type server-ca
```

#### Informations associées

- ["Installation du certificat de sécurité"](#)

## Activer la gestion des clés externes pour le chiffrement matériel dans ONTAP 9.6 et versions ultérieures

Vous pouvez utiliser un ou plusieurs serveurs KMIP pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Vous pouvez connecter jusqu'à quatre serveurs KMIP à un nœud. Un minimum de deux serveurs est recommandé pour la redondance et la reprise après sinistre.

À partir de ONTAP 9.11.1, vous pouvez ajouter jusqu'à 3 serveurs de clés secondaires par serveur de clés principal pour créer un serveur de clés en cluster. Pour plus d'informations, voir [Configurez les serveurs de clés externes en cluster](#).

#### Avant de commencer

- Les certificats client SSL KMIP et serveur doivent avoir été installés.
- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Dans un environnement MetroCluster :
  - Vous devez configurer l'environnement MetroCluster avant de configurer un gestionnaire de clés externe.
  - Vous devez installer le même certificat SSL KMIP sur les deux clusters.

#### Étapes

1. Configurer la connectivité du gestionnaire de clés pour le cluster :

```
security key-manager external enable -vserver admin_SVM -key-servers  
host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert  
server_CA_certificates
```



- **security key-manager external enable** La commande remplace `security key-manager setup la commande. Vous pouvez exécuter **security key-manager external modify** la commande pour modifier la configuration de la gestion externe des clés. Pour en savoir plus, **security key-manager external enable** consultez le ["Référence de commande ONTAP"](#).
- Dans un environnement MetroCluster, si vous configurez une gestion externe des clés pour le SVM admin, vous devez répéter l'opération **security key-manager external enable** commande sur le cluster partenaire.

La commande suivante active la gestion externe des clés pour cluster1 avec trois serveurs de clés externes. Le premier serveur de clés est spécifié à l'aide de son nom d'hôte et de son port, le second est spécifié à l'aide d'une adresse IP et du port par défaut, et le troisième est spécifié à l'aide d'une adresse et d'un port IPv6 :

```
cluster1::> security key-manager external enable -key-servers  
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234  
-client-cert AdminVserverClientCert -server-ca-certs  
AdminVserverServerCaCert
```

## 2. Vérifiez que tous les serveurs KMIP configurés sont connectés :

```
security key-manager external show-status -node node_name -vserver SVM -key  
-server host_name|IP_address:port -key-server-status available|not-  
responding|unknown
```

 `security key-manager external show-status` La commande remplace `security key-manager show -status` la commande. Pour en savoir plus, `security key-manager external show-status` consultez le link:<https://docs.netapp.com/us-en/ontap-cli/security-key-manager-external-show-status.html>["Référence de commande ONTAP"].

```
cluster1::> security key-manager external show-status
```

Node	Vserver	Key Server	Status
node1	cluster1	10.0.0.10:5696	available
		fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234	available
		ks1.local:15696	available
node2	cluster1	10.0.0.10:5696	available
		fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234	available
		ks1.local:15696	available

6 entries were displayed.

## Informations associées

- [Configurez les serveurs de clés externes en cluster](#)

- "[gestionnaire-de-clés-de-sécurité-activation-externe](#)"
- "[gestionnaire-de-clés-de-sécurité-externe-afficher-l'état](#)"

## Activer la gestion des clés externes pour le chiffrement matériel dans ONTAP 9.5 et versions antérieures

Vous pouvez utiliser un ou plusieurs serveurs KMIP pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Vous pouvez connecter jusqu'à quatre serveurs KMIP à un nœud. Un minimum de deux serveurs est recommandé pour la redondance et la reprise après sinistre.

### Description de la tâche

ONTAP configure la connectivité du serveur KMIP pour tous les nœuds du cluster.

### Avant de commencer

- Les certificats client SSL KMIP et serveur doivent avoir été installés.
- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Vous devez configurer l'environnement MetroCluster avant de configurer un gestionnaire de clés externe.
- Dans un environnement MetroCluster, vous devez installer le même certificat SSL KMIP sur les deux clusters.

### Étapes

1. Configurer la connectivité du gestionnaire de clés pour les nœuds du cluster :

```
security key-manager setup
```

La configuration du gestionnaire de clés démarre.



Dans un environnement MetroCluster, vous devez exécuter cette commande sur les deux clusters. En savoir plus sur `security key-manager setup` dans le "[Référence de commande ONTAP](#)".

2. Entrez la réponse appropriée à chaque invite.

3. Ajoutez un serveur KMIP :

```
security key-manager add -address key_management_server_ipaddress
```

```
cluster1::> security key-manager add -address 20.1.1.1
```



Dans un environnement MetroCluster, vous devez exécuter cette commande sur les deux clusters.

4. Ajoutez un serveur KMIP supplémentaire pour la redondance :

```
security key-manager add -address key_management_server_ipaddress
```

```
cluster1::> security key-manager add -address 20.1.1.2
```



Dans un environnement MetroCluster, vous devez exécuter cette commande sur les deux clusters.

5. Vérifiez que tous les serveurs KMIP configurés sont connectés :

```
security key-manager show -status
```

Apprenez-en plus sur les commandes décrites dans cette procédure dans le "[Référence de commande ONTAP](#)" .

```
cluster1::> security key-manager show -status
```

Node	Port	Registered Key Manager	Status
cluster1-01	5696	20.1.1.1	available
cluster1-01	5696	20.1.1.2	available
cluster1-02	5696	20.1.1.1	available
cluster1-02	5696	20.1.1.2	available

6. Vous pouvez également convertir des volumes en texte brut en volumes chiffrés.

```
volume encryption conversion start
```

Un gestionnaire de clés externe doit être entièrement configuré avant la conversion des volumes. Dans un environnement MetroCluster, un gestionnaire de clés externe doit être configuré sur les deux sites.

## Configurez des serveurs de clés externes en cluster dans ONTAP

À partir d'ONTAP 9.11.1, vous pouvez configurer la connectivité aux serveurs de gestion de clés externes en cluster sur une SVM. Avec les serveurs de clés en cluster, vous pouvez désigner des serveurs de clés primaires et secondaires sur une SVM. Lors de l'enregistrement ou de la récupération de clés, ONTAP tente d'abord d'accéder au serveur de clés principal avant de tenter successivement d'accéder aux serveurs secondaires jusqu'à ce que l'opération se termine avec succès.

Vous pouvez utiliser des serveurs de clés externes pour les clés NetApp Storage Encryption (NSE), NetApp Volume Encryption (NVE) et NetApp Aggregate Encryption (NAE). Un SVM peut prendre en charge jusqu'à quatre serveurs KMIP externes principaux. Chaque serveur principal peut prendre en charge jusqu'à trois serveurs de clés secondaires.

### Description de la tâche

- Ce processus prend uniquement en charge les serveurs de clés qui utilisent KMIP. Pour obtenir la liste des serveurs de clés pris en charge, reportez-vous à la "[Matrice d'interopérabilité NetApp](#)".

## **Avant de commencer**

- "La gestion des clés KMIP doit être activée pour le SVM".
- Tous les nœuds du cluster doivent exécuter ONTAP 9.11.1 ou une version ultérieure.
- L'ordre des serveurs listés dans le -secondary-key-servers Ce paramètre reflète l'ordre d'accès des serveurs de gestion de clés externes (KMIP).

## **Créer un serveur de clés mis en cluster**

La procédure de configuration varie selon que vous avez configuré ou non un serveur de clés principal.

## Ajout de serveurs de clés primaires et secondaires à un SVM

### Étapes

1. Vérifiez qu'aucune gestion de clés n'a été activée pour le cluster (SVM d'administration) :

```
security key-manager external show -vserver <svm_name>
```

Si le SVM a déjà le maximum de quatre serveurs de clés primaires activés, vous devez supprimer l'un des serveurs de clés primaires existants avant d'en ajouter un nouveau.

2. Activez le gestionnaire de clés primaires :

```
security key-manager external enable -vserver <svm_name> -key-servers  
<primary_key_server_ip> -client-cert <client_cert_name> -server-ca-certs  
<server_ca_cert_names>
```

- Si vous ne spécifiez pas de port dans le `-key-servers` Ce paramètre indique que le port par défaut 5696 est utilisé.



Si vous exécutez le `security key-manager external enable` Pour exécuter la commande relative à la SVM d'administration dans une configuration MetroCluster , vous devez la réaliser sur les deux clusters. Si vous exécutez la commande pour une SVM de données individuelle, vous n'avez pas besoin de l'exécuter sur les deux clusters. NetApp recommande fortement d'utiliser les mêmes serveurs clés sur les deux clusters.

3. Modifiez le serveur de clé primaire pour ajouter des serveurs de clé secondaires. Le `-secondary-key-servers` Ce paramètre accepte une liste de trois serveurs clés maximum, séparés par des virgules :

```
security key-manager external modify-server -vserver <svm_name> -key  
-servers <primary_key_server> -secondary-key-servers <list_of_key_servers>
```

- N'incluez pas de numéro de port pour les serveurs de clés secondaires dans le `-secondary-key-servers` paramètre. Il utilise le même numéro de port que le serveur de clé primaire.



Si vous exécutez le `security key-manager external` Pour exécuter la commande relative à la SVM d'administration dans une configuration MetroCluster , vous devez la réaliser sur les deux clusters. Si vous exécutez la commande pour une SVM de données individuelle, vous n'avez pas besoin de l'exécuter sur les deux clusters. NetApp recommande fortement d'utiliser les mêmes serveurs clés sur les deux clusters.

## Ajoutez des serveurs de clés secondaires à un serveur de clés principal existant

### Étapes

1. Modifiez le serveur de clé primaire pour ajouter des serveurs de clé secondaires. Le `-secondary-key-servers` Ce paramètre accepte une liste de trois serveurs clés maximum, séparés par des virgules :

```
security key-manager external modify-server -vserver <svm_name> -key  
-servers <primary_key_server> -secondary-key-servers <list_of_key_servers>
```

- N'incluez pas de numéro de port pour les serveurs de clés secondaires dans le `-secondary-key-servers` paramètre. Il utilise le même numéro de port que les serveurs de clés primaires.



Si vous exécutez le `security key-manager external modify-server` Pour exécuter la commande relative à la SVM d'administration dans une configuration MetroCluster , vous devez la réaliser sur les deux clusters. Si vous exécutez la commande pour une SVM de données individuelle, vous n'avez pas besoin de l'exécuter sur les deux clusters. NetApp recommande fortement d'utiliser les mêmes serveurs clés sur les deux clusters.

Pour plus d'informations sur les serveurs de clés secondaires, consultez [\[mod-secondary\]](#).

## Modifier les serveurs de clés en cluster

Vous pouvez modifier les serveurs de clés externes en cluster en ajoutant et en supprimant des serveurs de clés secondaires, en modifiant l'ordre d'accès des serveurs de clés secondaires ou en modifiant la désignation ( primaire ou secondaire) de certains serveurs de clés. Si vous modifiez des serveurs de clés externes en cluster dans une configuration MetroCluster , NetApp recommande fortement d'utiliser les mêmes serveurs de clés sur les deux clusters.

### Modifier les serveurs de clés secondaires

Utilisez le paramètre `-secondary-key-servers` de la commande `security key-manager external modify-server` pour gérer les serveurs de clés secondaires. Le `-secondary-key-servers` Ce paramètre accepte une liste séparée par des virgules. L'ordre spécifié des serveurs de clés secondaires dans la liste détermine la séquence d'accès pour ces serveurs. Vous pouvez modifier l'ordre d'accès en exécutant la commande `security key-manager external modify-server` avec les serveurs de clés secondaires saisis dans un ordre différent. N'indiquez pas de numéro de port pour les serveurs de clés secondaires.



Si vous exécutez le `security key-manager external modify-server` Pour exécuter la commande relative à la SVM d'administration dans une configuration MetroCluster , vous devez la réaliser sur les deux clusters. Si vous exécutez la commande pour une SVM de données individuelle, vous n'avez pas besoin de l'exécuter sur les deux clusters.

Pour supprimer un serveur de clés secondaire, incluez les serveurs de clés que vous souhaitez conserver dans le `-secondary-key-servers` paramètre et omettez celui que vous souhaitez supprimer. Pour supprimer tous les serveurs de clés secondaires, utilisez l'argument `-`, signifiant aucun.

### Conversion des serveurs de clés principaux et secondaires

Vous pouvez utiliser les étapes suivantes pour modifier la désignation ( primaire ou secondaire) de certains serveurs clés.

## Convertir un serveur de clé primaire en serveur de clé secondaire

### Étapes

1. Supprimez le serveur de clé primaire du SVM :

```
security key-manager external remove-servers
```



Si vous exécutez le `security key-manager external remove-servers` Pour exécuter la commande relative à la SVM d'administration dans une configuration MetroCluster , vous devez la réaliser sur les deux clusters. Si vous exécutez la commande pour une SVM de données individuelle, vous n'avez pas besoin de l'exécuter sur les deux clusters.

2. Effectuez le[Créer un serveur de clés mis en cluster](#) procédure utilisant l'ancien serveur de clé primaire comme serveur de clé secondaire.

## Convertir un serveur de clés secondaires en serveur de clés primaires

### Étapes

1. Supprimez le serveur de clé secondaire de son serveur de clé primaire existant :

```
security key-manager external modify-server -secondary-key-servers
```

- Si vous exécutez le `security key-manager external modify-server -secondary-key -servers` Pour exécuter la commande relative à la SVM d'administration dans une configuration MetroCluster , vous devez la réaliser sur les deux clusters. Si vous exécutez la commande pour une SVM de données individuelle, vous n'avez pas besoin de l'exécuter sur les deux clusters.
- Si vous convertissez un serveur de clés secondaire en serveur de clés primaire tout en supprimant un serveur de clés existant, toute tentative d'ajout d'un nouveau serveur de clés avant la fin de la suppression et de la conversion peut entraîner la duplication des clés.

1. Effectuez le[Créer un serveur de clés mis en cluster](#) procédure utilisant l'ancien serveur de clés secondaires comme serveur de clés primaires du nouveau serveur de clés en cluster.

Se référer à[\[mod-secondary\]](#) pour plus d'informations.

### Informations associées

- Apprenez-en davantage sur `security key-manager external` dans le["Référence de commande ONTAP"](#)

## Créez des clés d'authentification dans ONTAP 9.6 et versions ultérieures

Vous pouvez utiliser le `security key-manager key create` Commande permettant de créer les clés d'authentification d'un nœud et de les stocker sur les serveurs KMIP configurés.

### Description de la tâche

Si votre configuration de sécurité exige que vous utilisez des clés différentes pour l'authentification des données et l'authentification FIPS 140-2, vous devez créer une clé distincte pour chacune d'elles. Si ce n'est pas le cas, vous pouvez utiliser la même clé d'authentification pour la conformité FIPS que pour l'accès aux données.

ONTAP crée des clés d'authentification pour tous les nœuds du cluster.

- Cette commande n'est pas prise en charge lorsque le gestionnaire de clés intégré est activé. Toutefois, deux clés d'authentification sont créées automatiquement lorsque le gestionnaire de clés intégré est activé. Les clés peuvent être affichées à l'aide de la commande suivante :

```
security key-manager key query -key-type NSE-AK
```

- Vous recevez un avertissement si les serveurs de gestion des clés configurés stockent déjà plus de 128 clés d'authentification.
- Vous pouvez utiliser `security key-manager key delete` la commande pour supprimer toutes les clés inutilisées. La `security key-manager key delete` commande échoue si la clé indiquée est actuellement utilisée par ONTAP. (Privileges doit être supérieur à `admin` pour utiliser cette commande.)

Dans un environnement MetroCluster, avant de supprimer une clé, veillez à ce que cette clé ne soit pas utilisée sur le cluster partenaire. Vous pouvez utiliser les commandes suivantes sur le cluster partenaire pour vérifier que la clé n'est pas utilisée :



- `storage encryption disk show -data-key-id <key-id>`
- `storage encryption disk show -fips-key-id <key-id>`

## Avant de commencer

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

## Étapes

1. Créer les clés d'authentification pour les nœuds du cluster :

```
security key-manager key create -key-tag <passphrase_label> -prompt-for-key true|false
```



Si ce paramètre est défini `prompt-for-key=true`, le système invite l'administrateur du cluster à indiquer la phrase de passe à utiliser lors de l'authentification des disques cryptés. Dans le cas contraire, le système génère automatiquement une phrase de passe de 32 octets. `security key-manager key create``La commande remplace ``security key-manager create-key`` la commande. Pour en savoir plus, `security key-manager key create` consultez le "[Référence de commande ONTAP](#)".

L'exemple suivant crée les clés d'authentification pour `cluster1`, génération automatique d'une phrase de passe de 32 octets :

```
cluster1::> security key-manager key create  
Key ID: <id_value>
```

2. Vérifiez que les clés d'authentification ont été créées :

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

 `security key-manager key query` La commande remplace `security key-manager query key` la commande.

L'ID de clé affiché dans la sortie est un identificateur utilisé pour faire référence à la clé d'authentification. Ce n'est pas la clé d'authentification ou la clé de chiffrement des données.

L'exemple suivant vérifie que les clés d'authentification ont été créées pour cluster1:

```
cluster1::> security key-manager key query  
Vserver: cluster1  
Key Manager: external  
Node: node1  
  
Key Tag  
-----  
node1  
    Key ID: <id_value>  
node1  
    Key ID: <id_value>  
  
Vserver: cluster1  
Key Manager: external  
Node: node2  
  
Key Tag  
-----  
node2  
    Key ID: <id_value>  
node2  
    Key ID: <id_value>
```

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

## Informations associées

- "affichage du disque de cryptage de stockage"

## Création de clés d'authentification dans ONTAP 9.5 et versions antérieures

Vous pouvez utiliser la commande `security key-manager create-key` pour créer les clés d'authentification d'un nœud et les stocker sur les serveurs KMIP configurés.

### Description de la tâche

Si votre configuration de sécurité exige que vous utilisez des clés différentes pour l'authentification des données et l'authentification FIPS 140-2, vous devez créer une clé distincte pour chacune d'elles. Si ce n'est pas le cas, vous pouvez utiliser la même clé d'authentification pour la conformité FIPS que celle utilisée pour l'accès aux données.

ONTAP crée des clés d'authentification pour tous les nœuds du cluster.

- Cette commande n'est pas prise en charge lorsque la gestion intégrée des clés est activée.
- Vous recevez un avertissement si les serveurs de gestion des clés configurés stockent déjà plus de 128 clés d'authentification.

Vous pouvez utiliser le logiciel du serveur de gestion des clés pour supprimer toutes les clés inutilisées, puis exécuter de nouveau la commande.

### Avant de commencer

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

### Étapes

1. Créer les clés d'authentification pour les nœuds du cluster :

```
security key-manager create-key
```

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



L'ID de clé affiché dans la sortie est un identificateur utilisé pour faire référence à la clé d'authentification. Ce n'est pas la clé d'authentification ou la clé de chiffrement des données.

L'exemple suivant crée les clés d'authentification pour `cluster1`:

```
cluster1::> security key-manager create-key
    (security key-manager create-key)
Verifying requirements...

Node: cluster1-01
Creating authentication key...
Authentication key creation successful.
Key ID: <id_value>

Node: cluster1-01
Key manager restore operation initialized.
Successfully restored key information.

Node: cluster1-02
Key manager restore operation initialized.
Successfully restored key information.
```

2. Vérifiez que les clés d'authentification ont été créées :

```
security key-manager query
```

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

L'exemple suivant vérifie que les clés d'authentification ont été créées pour cluster1:

```

cluster1::> security key-manager query

(security key-manager query)

      Node: cluster1-01
      Key Manager: 20.1.1.1
      Server Status: available

      Key Tag          Key Type  Restored
      -----          -----  -----
cluster1-01      NSE-AK    yes
      Key ID: <id_value>

      Node: cluster1-02
      Key Manager: 20.1.1.1
      Server Status: available

      Key Tag          Key Type  Restored
      -----          -----  -----
cluster1-02      NSE-AK    yes
      Key ID: <id_value>

```

## Attribuer une clé d'authentification de données à un lecteur FIPS ou SED avec la gestion des clés externes ONTAP

Vous pouvez utiliser le `storage encryption disk modify` Commande permettant d'attribuer une clé d'authentification de données à un lecteur FIPS ou SED. Les nœuds de cluster utilisent cette clé pour verrouiller ou déverrouiller des données chiffrées sur le disque.

### Description de la tâche

Un disque à chiffrement automatique est protégé contre tout accès non autorisé uniquement si son ID de clé d'authentification est défini sur une valeur autre que celle par défaut. L'ID sécurisé du fabricant (MSID), qui possède l'ID de clé 0x0, est la valeur par défaut standard des lecteurs SAS. Pour les disques NVMe, la valeur standard par défaut est une clé nulle, représentée sous forme d'ID de clé vierge. Lorsque vous attribuez l'ID de clé à un disque auto-crypté, le système remplace son ID de clé d'authentification par une valeur autre que celle par défaut.

Cette procédure n'est pas perturbatrice.

### Avant de commencer

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

### Étapes

## 1. Attribuez une clé d'authentification de données à un lecteur FIPS ou SED :

```
storage encryption disk modify -disk disk_ID -data-key-id key_ID
```

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



Vous pouvez utiliser la commande `security key-manager query -key-type NSE-AK` pour afficher les ID de clés.

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id  
<iid_value>
```

Info: Starting modify on 14 disks.

View the status of the operation by using the `storage encryption disk show-status` command.

## 2. Vérifiez que les clés d'authentification ont été attribuées :

```
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 <iid_value>
0.0.1    data <iid_value>
[...]
```

### Informations associées

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

## **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 JOUSSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

## **Informations sur les marques commerciales**

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.