Configuration du chiffrement matériel NetApp

ONTAP 9

NetApp
February 13, 2026

Sommaire

Configuration du chiffrement matériel NetApp

En savoir plus sur le chiffrement matériel ONTAP

Le chiffrement matériel NetApp prend en charge le chiffrement de disque intégral (FDE) des données au fur et à mesure de leur écriture. Les données ne peuvent pas être lues si une clé de chiffrement est stockée sur le micrologiciel. La clé de chiffrement, à son tour, n'est accessible qu'à un nœud authentifié.

Présentation du cryptage matériel NetApp

Un nœud s'authentifie auprès d'un disque auto-chiffré à l'aide d'une clé d'authentification extraite d'un serveur de gestion externe des clés ou d'un gestionnaire de clés intégré :

- Le 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). Il est recommandé de configurer des serveurs de gestion externe des clés sur un système de stockage différent de vos données.
- Le gestionnaire de clés intégré est un outil intégré qui sert des clés d'authentification aux nœuds du même système de stockage que vos données.

Vous pouvez utiliser NetApp Volume Encryption avec chiffrement matériel pour « paramétrer la fonctionnalité de chiffrement » des données sur des disques à autochiffrement.

Lorsque les disques à chiffrement automatique sont activés, le « core dump » est également chiffré.

> Si une paire haute disponibilité utilise des disques avec cryptage SAS ou 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.

Types de disques à autocryptage pris en charge

Deux types de disques à autocryptage sont pris en charge :

- Tous les systèmes FAS et AFF prennent en charge les disques SAS ou NVMe certifiés FIPS avec le chiffrement automatique. Ces unités, appelées unités *FIPS,* sont conformes aux exigences de la publication 140-2 de la norme fédérale de traitement des informations, niveau 2. Les fonctionnalités certifiées permettent d'ajouter des protections au chiffrement, comme la prévention d'attaques par déni de service sur le disque. Les disques FIPS ne peuvent pas être combinés avec d'autres types de disques sur le même nœud ou la même paire HA.
- Depuis ONTAP 9.6, les disques NVMe à autocryptage n'ayant pas encore été testés FIPS sont pris en charge sur des systèmes AFF A800, A320 et versions ultérieures. Ces disques, appelés *SED*, offrent les mêmes fonctionnalités de cryptage que les disques FIPS, mais peuvent être combinés avec des disques sans cryptage sur un même nœud ou une paire haute disponibilité.
- Tous les disques validés FIPS utilisent un module cryptographique de firmware qui a été validé par FIPS. Le module cryptographique du lecteur FIPS n'utilise aucune clé générée en dehors du disque (la phrase de passe d'authentification entrée dans le lecteur est utilisée par le module cryptographique du firmware du disque pour obtenir une clé de chiffrement).

Les disques sans chiffrement sont des disques qui ne sont pas des disques SED ou FIPS.

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

Quand utiliser la gestion externe des clés

Le gestionnaire de clés intégré est moins coûteux et généralement plus pratique, mais vous devez utiliser une gestion externe des clés si l'un des éléments suivants est vrai :

- La stratégie de votre entreprise nécessite une solution de gestion des clés qui utilise un module cryptographique FIPS 140-2 de niveau 2 (ou supérieur).
- Vous avez besoin d'une solution à plusieurs clusters et d'une gestion centralisée des clés de chiffrement.
- Votre entreprise exige que les clés d'authentification soient sécurisées sur un système ou à un emplacement différent de celui des données.

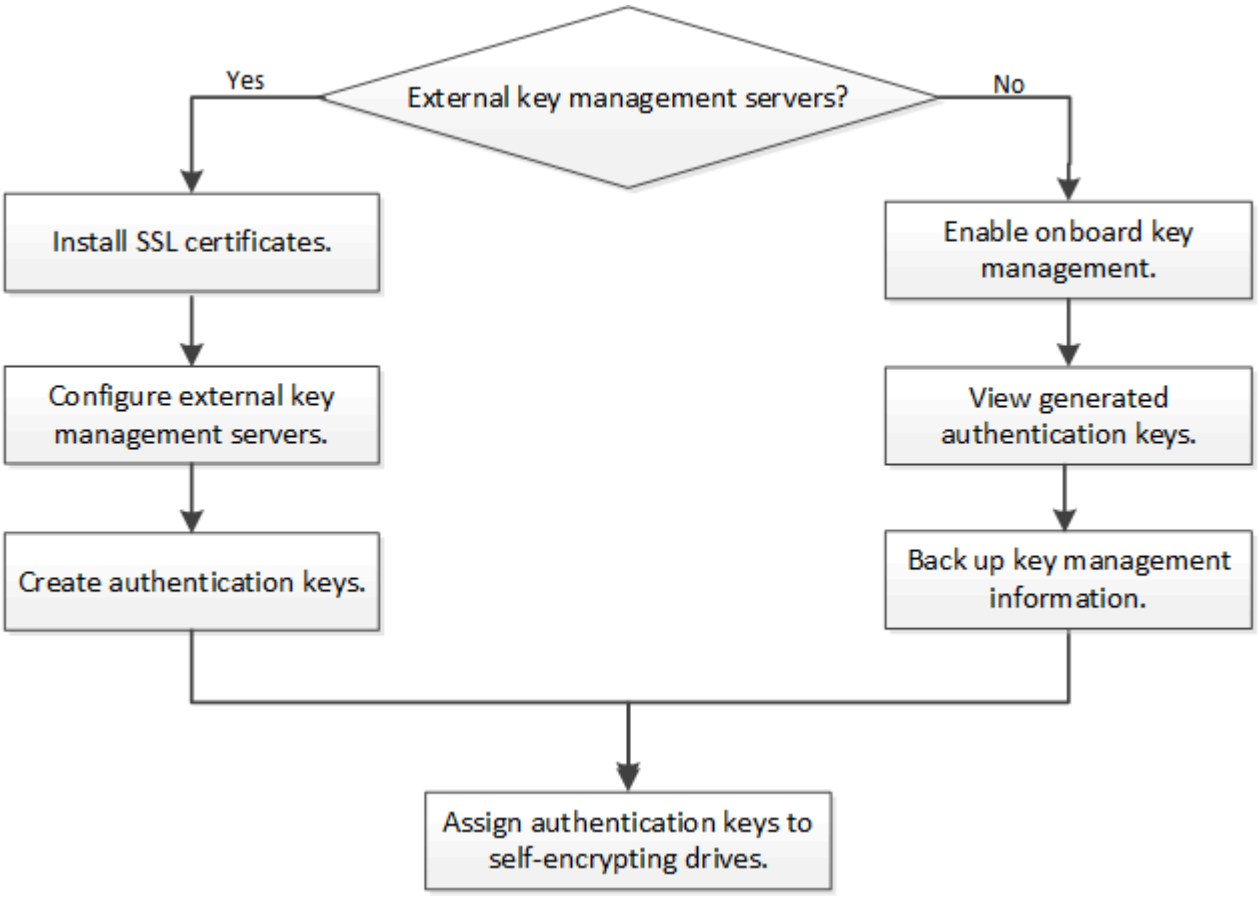
Détails du support

Le tableau suivant présente des détails importants sur la prise en charge du chiffrement matériel. Consultez la matrice d'interopérabilité pour obtenir les dernières informations sur les serveurs, les systèmes de stockage et les tiroirs disques KMIP pris en charge.

Ressource ou fonctionnalité	Détails du support
Jeux de disques non homogènes	• Les disques FIPS ne peuvent pas être combinés avec d'autres types de disques sur le même nœud ou la même paire HA. Les paires haute disponibilité conformes peuvent coexister avec des paires haute disponibilité non conformes dans le même cluster. • Les disques SED peuvent être combinés avec des disques sans cryptage sur un même nœud ou une même paire haute disponibilité.
Type de disque	• Les disques FIPS peuvent être des disques SAS ou NVMe. • Les disques SED doivent être des disques NVMe.
Interfaces réseau de 10 Go	Depuis ONTAP 9.3, les configurations de gestion des clés KMIP prennent en charge des interfaces réseau de 10 Gbit pour les communications avec des serveurs de gestion des clés externes.
Ports de communication avec le serveur de gestion des clés	Depuis ONTAP 9.3, vous pouvez utiliser n'importe quel port du contrôleur de stockage pour la communication avec le serveur de gestion des clés. Dans le cas contraire, vous devez utiliser le port e0M pour la communication avec les serveurs de gestion des clés. Selon le modèle du contrôleur de stockage, certaines interfaces réseau peuvent ne pas être disponibles durant le processus de démarrage pour la communication avec les serveurs de gestion des clés.
MetroCluster (MCC)	• Les disques NVMe prennent en charge MCC. • Les disques SAS ne prennent pas en charge MCC.

Flux de production de cryptage matériel

Vous devez configurer les services de gestion des clés pour que le cluster puisse s'authentifier sur le disque auto-chiffré. Vous pouvez utiliser un serveur de gestion externe des clés ou un gestionnaire de clés intégré.



Informations associées

- "NetApp Hardware Universe"
- "NetApp Volume Encryption et chiffrement d'agrégat NetApp"

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`

   ```
   clusterl::> 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`

   ```
   clusterl::> 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` paramétrez 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 leCréer 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 leCréer 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 utilisiez 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                                  Key Type  Restored
---------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID: <id_value>
node1                                    NSE-AK    yes
    Key ID: <id_value>

       Vserver: cluster1
   Key Manager: external
          Node: node2

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node2                                    NSE-AK    yes
    Key ID: <id_value>
node2                                    NSE-AK    yes
    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 le `security key-manager create-key` 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 utilisiez 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 le "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 le `security key-manager query -key-type NSE-AK` Commande permettant d'afficher les ID de clés.

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
<id_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 <id_value>
0.0.1   data <id_value>
[...]
```

Informations associées

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

Configurez la gestion intégrée des clés

Activez la gestion intégrée des clés dans ONTAP 9.6 et versions ultérieures

Vous pouvez utiliser le gestionnaire de clés intégré pour authentifier les nœuds de cluster sur un lecteur FIPS ou SED. Le gestionnaire de clés intégré est un outil intégré qui sert des clés d'authentification aux nœuds du même système de stockage que vos données. Le gestionnaire de clés intégré est conforme à la norme FIPS-140-2 de niveau 1.

Vous pouvez utiliser le gestionnaire de clés intégré pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Vous devez activer le gestionnaire de clés intégré sur chaque cluster qui accède à un

volume chiffré ou à un disque auto-chiffré.

Description de la tâche

Vous devez exécuter le `security key-manager onboard enable` commande à chaque ajout d'un nœud au cluster. Dans les configurations MetroCluster, vous devez exécuter `security key-manager onboard enable` sur le cluster local, puis s'exécute `security key-manager onboard sync` sur le cluster distant, en utilisant la même phrase de passe sur chacun d'eux.

En savoir plus sur `security key-manager onboard enable` et `security key-manager onboard sync` dans le"Référence de commande ONTAP" .

Par défaut, vous n'êtes pas tenu de saisir la phrase de passe du gestionnaire de clés lors du redémarrage d'un nœud. Sauf dans MetroCluster, vous pouvez utiliser `cc-mode-enabled=yes` option pour exiger que les utilisateurs saisissent la phrase de passe après un redémarrage.

Lorsque le gestionnaire de clés intégré est activé en mode critères communs (`cc-mode-enabled=yes`), le comportement du système est modifié de l'une des manières suivantes :

- Le système surveille les tentatives consécutives de mot de passe de cluster ayant échoué lorsqu'il fonctionne en mode critères communs.

  Si NetApp Storage Encryption (NSE) est activé et que vous ne saisissez pas la phrase secrète appropriée au démarrage, le système ne peut pas s'authentifier sur ses disques et redémarre automatiquement. Pour corriger ce problème, vous devez saisir la phrase secrète correcte du cluster à l'invite de démarrage. Une fois démarré, le système peut saisir jusqu'à 5 tentatives consécutives de saisie de la phrase secrète du cluster dans une période de 24 heures pour toute commande nécessitant une phrase secrète comme paramètre. Si la limite est atteinte (par exemple, vous n'avez pas saisi correctement la phrase de passe du cluster 5 fois de suite) alors vous devez attendre l'expiration du délai de 24 heures ou redémarrer le nœud pour réinitialiser la limite.

- Les mises à jour d'images système utilisent le certificat de signature de code NetApp RSA-3072 avec des digests signés SHA-384 pour vérifier l'intégrité de l'image au lieu du certificat de signature de code RSA-2048 NetApp habituel et des digests signés par code SHA-256.

  La commande de mise à niveau vérifie que le contenu de l'image n'a pas été modifié ou corrompu en vérifiant diverses signatures numériques. Si la validation fonctionne, la mise à jour de l'image passe à l'étape suivante. Si la validation ne fonctionne pas, la mise à jour de l'image échoue. En savoir plus sur `cluster image` dans le"Référence de commande ONTAP" .

Le gestionnaire de clés intégré stocke les clés dans la mémoire volatile. Le contenu de la mémoire volatile est effacé lors du redémarrage ou de l'arrêt du système. Dans des conditions de fonctionnement normales, le contenu de la mémoire volatile est effacé dans les 30 secondes lorsqu'un système est arrêté.

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.
- Vous devez configurer l'environnement MetroCluster avant de configurer le gestionnaire de clés intégré.

Étapes

1. Lancez la commande de configuration du gestionnaire de clés :

   `security key-manager onboard enable -cc-mode-enabled yes|no`

   > Défini `cc-mode-enabled=yes` pour exiger que les utilisateurs saisissent la phrase de passe du gestionnaire de clés après un redémarrage. L' `- cc-mode-enabled`option n'est pas prise en charge dans les configurations MetroCluster. `security key-manager onboard enable`La commande remplace `security key-manager setup` la commande.

   L'exemple suivant démarre la commande Key Manager setup sur cluster1 sans exiger la saisie de la phrase de passe après chaque redémarrage :

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

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

3. À l'invite de confirmation de la phrase de passe, saisissez à nouveau la phrase de passe.
4. Vérifiez que le système crée les clés d'authentification :

   `security key-manager key query -node node`

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

   Pour en savoir plus, `security key-manager key query` consultez le "Référence de commande ONTAP".

Une fois que vous avez terminé

Copiez la phrase secrète dans un emplacement sécurisé à l'extérieur du système de stockage pour une utilisation ultérieure.

Le système sauvegarde automatiquement les informations de gestion des clés dans la base de données répliquée (RDB) du cluster. Vous devez également sauvegarder ces informations manuellement pour la reprise après sinistre.

Informations associées

- "commandes d'image de cluster"
- "activation externe du gestionnaire de clés de sécurité"
- "requête de clé du gestionnaire de clés de sécurité"
- "activation du gestionnaire de clés de sécurité intégré"

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

Activez la gestion intégrée des clés dans ONTAP 9.5 et versions antérieures

Vous pouvez utiliser le gestionnaire de clés intégré pour authentifier les nœuds de cluster sur un lecteur FIPS ou SED. Le gestionnaire de clés intégré est un outil intégré qui sert des clés d'authentification aux nœuds du même système de stockage que vos données. Le gestionnaire de clés intégré est conforme à la norme FIPS-140-2 de niveau 1.

Vous pouvez utiliser le gestionnaire de clés intégré pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Activez Onboard Key Manager sur chaque cluster qui accède aux volumes chiffrés ou aux disques à chiffrement automatique.

Description de la tâche

Vous devez exécuter le `security key-manager setup` commande à chaque ajout d'un nœud au cluster.

Si vous disposez d'une configuration MetroCluster, consultez les consignes suivantes :

- Dans ONTAP 9.5, vous devez exécuter `security key-manager setup` sur le cluster local et `security key-manager setup -sync-metrocluster-config yes` sur le cluster distant, en utilisant la même phrase de passe sur chacun d'eux.
- Avant ONTAP 9.5, vous devez exécuter `security key-manager setup` sur le cluster local, attendez environ 20 secondes, puis exécutez `security key-manager setup` sur le cluster distant, en utilisant la même phrase de passe sur chacun d'eux.

Par défaut, vous n'êtes pas tenu de saisir la phrase de passe du gestionnaire de clés lors du redémarrage d'un nœud. À partir de ONTAP 9.4, vous pouvez utiliser le `-enable-cc-mode yes` option pour exiger que les utilisateurs saisissent la phrase de passe après un redémarrage.

Pour NVE, si vous définissez `-enable-cc-mode yes`, volumes que vous créez avec `volume create` et `volume move start` les commandes sont automatiquement chiffrées. Pour `volume create`, vous n'avez pas besoin de spécifier `-encrypt true`. Pour `volume move start`, vous n'avez pas besoin de spécifier `-encrypt-destination true`.

Après une tentative de phrase de passe, vous devez redémarrer le nœud.

Avant de commencer

- Si vous utilisez NSE avec un serveur de gestion de clés externe (KMIP), supprimez la base de données du 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.
- Configurez l'environnement MetroCluster avant de configurer le gestionnaire de clés intégré.

Étapes

1. Lancez la configuration du gestionnaire de clés :

   ```
   security key-manager setup -enable-cc-mode yes|no
   ```

À partir de ONTAP 9.4, vous pouvez utiliser le `-enable-cc-mode yes` option permettant aux utilisateurs de saisir la phrase de passe du gestionnaire de clés après un redémarrage. Pour NVE, si vous définissez `-enable-cc-mode yes`, volumes que vous créez avec `volume create` et `volume move start` les commandes sont automatiquement chiffrées.

L'exemple suivant commence à configurer le gestionnaire de clés sur le cluster 1 sans que la phrase de passe ne soit saisie après chaque redémarrage :

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. Entrez `yes` à l'invite, configurez la gestion intégrée des clés.
3. À l'invite de 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.

4. À l'invite de confirmation de la phrase de passe, saisissez à nouveau la phrase de passe.
5. Vérifier que les clés sont configurées pour tous les nœuds :

   `security key-manager show-key-store`

   En savoir plus sur `security key-manager show-key-store` dans le"Référence de commande ONTAP" .

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

Node: node1
Key Store: onboard
Key ID                                                               Used By
-----------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK

Node: node2
Key Store: onboard
Key ID                                                               Used By
-----------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK
```

Une fois que vous avez terminé

ONTAP sauvegarde automatiquement les informations de gestion des clés dans la base de données répliquée (RDB) du cluster.

Après avoir configuré la phrase secrète du gestionnaire de clés embarquées, sauvegardez manuellement les informations dans un emplacement sécurisé en dehors du système de stockage. Voir"Sauvegardez manuellement les informations intégrées de gestion des clés" .

Informations associées

- "Sauvegardez manuellement les informations intégrées de gestion des clés"
- "configuration du gestionnaire de clés de sécurité"
- "gestionnaire de clés de sécurité show-key-store"
- "Transition vers la gestion intégrée des clés à partir d'une gestion externe des clés"

Attribuer une clé d'authentification de données à un lecteur FIPS ou SED avec la gestion des clés intégrée 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 accéder aux données du 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.

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 le `security key-manager key query -key-type NSE-AK` Commande permettant d'afficher les ID de clés.

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

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

   Pour en savoir plus, `security key-manager key query` consultez le "Référence de commande ONTAP".

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

Informations associées

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

Attribuer une clé d'authentification FIPS 140-2 à un lecteur ONTAP FIPS

Vous pouvez utiliser le `storage encryption disk modify` commande avec `-fips-key-id` Option permettant d'attribuer une clé d'authentification FIPS 140-2 à un disque FIPS. Les nœuds de cluster utilisent cette clé pour des opérations autres que l'accès aux données, comme empêcher les attaques de déni de service sur le disque.

Description de la tâche

Votre configuration de sécurité peut nécessiter l'utilisation de clés différentes pour l'authentification des données et l'authentification FIPS 140-2-2. 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.

Cette procédure n'est pas perturbatrice.

Avant de commencer

Le firmware du disque doit prendre en charge la conformité à la norme FIPS 140-2-2. Le "Matrice d'interopérabilité NetApp" contient des informations sur les versions de micrologiciel de lecteur prises en charge.

Étapes

1. Vous devez d'abord vous assurer que vous avez attribué une clé d'authentification des données. Pour ce faire, utilisez un gestionnaire de clés externe ou un gestionnaire de clés intégré. Vérifiez que la clé est affectée à la commande `storage encryption disk show`.
2. Attribution d'une clé d'authentification FIPS 140-2 aux disques SED :

   `storage encryption disk modify -disk` *`disk_id`* `-fips-key-id` *`fips_authentication_key_id`*

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

   ```
   cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
   <id_value>

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

3. Vérifiez que la clé d'authentification a été attribuée :

   `storage encryption disk show -fips`

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

```
cluster1::> storage encryption disk show -fips
Disk    Mode FIPS-Compliance Key ID
------  ----
--------------------------------------------------------------------
2.10.0  full <id_value>
2.10.1  full <id_value>
[...]
```

Informations associées

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

Activez le mode conforme FIPS à l'échelle du cluster pour les connexions de serveurs KMIP dans ONTAP

Vous pouvez utiliser le `security config modify` commande avec `-is-fips-enabled` Option permettant d'activer le mode conforme à la norme FIPS au niveau du cluster pour les données en transit. Cela force le cluster à utiliser OpenSSL en mode FIPS lors de la connexion à des serveurs KMIP.

Description de la tâche

Lorsque vous activez le mode cluster compatible FIPS, le cluster n'utilise automatiquement que les suites de chiffrement conformes à la norme TLS1.2 et FIPS. Le mode conforme à la norme FIPS à l'échelle du cluster est désactivé par défaut.

Vous devez redémarrer manuellement les nœuds du cluster après avoir modifié la configuration de sécurité à l'échelle du cluster.

Avant de commencer

- Le contrôleur de stockage doit être configuré en mode conforme à la norme FIPS.
- Tous les serveurs KMIP doivent prendre en charge TLSv1.2. Le système nécessite TLSv1.2 pour terminer la connexion au serveur KMIP lorsque le mode conforme FIPS à l'échelle du cluster est activé.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Vérifiez que TLSv1.2 est pris en charge :

   ```
   security config show -supported-protocols
   ```

   Pour en savoir plus, `security config show` consultez le "Référence de commande ONTAP".

```
cluster1::> security config show
          Cluster                                                  Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       false      TLSv1.2, TLSv1.1, TLSv1 ALL:!LOW:         yes
                                             !aNULL:!EXP:
                                             !eNULL
```

3. Activer le mode compatible FIPS à l'échelle du cluster :

   `security config modify -is-fips-enabled true -interface SSL`

   Pour en savoir plus, `security config modify` consultez le "Référence de commande ONTAP".

4. Redémarrez les nœuds du cluster manuellement.
5. Vérifiez que le mode compatible FIPS à l'échelle du cluster est activé :

   `security config show`

```
cluster1::> security config show
          Cluster                                                  Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       true       TLSv1.2, TLSv1.1        ALL:!LOW:         yes
                                             !aNULL:!EXP:
                                             !eNULL:!RC4
```