Configurez NVE

ONTAP 9

NetApp
January 08, 2026

Sommaire

Configurez NVE

Déterminez si votre version de cluster ONTAP prend en charge NVE

Vous devez déterminer si votre version de cluster prend en charge NVE avant d'installer la licence. Vous pouvez utiliser le `version` pour déterminer la version du cluster.

Description de la tâche

La version en cluster est la version la plus basse d'ONTAP s'exécutant sur n'importe quel nœud du cluster.

Étapes

1. Déterminez si votre version de cluster prend en charge NVE :

   ```
   version -v
   ```

   NVE n'est pas pris en charge si le texte affiché dans le résultat de la commande `1Ono-DARE` (pour « pas de chiffrement des données au repos ») ou si vous utilisez une plateforme non répertoriée dans le "Détails du support".

Installer la licence de chiffrement de volume sur un cluster ONTAP

Une licence VE vous permet d'utiliser cette fonctionnalité sur tous les nœuds du cluster. Cette licence est requise avant de pouvoir chiffrer les données avec NVE. Il est inclus avec "ONTAP One".

Avant ONTAP One, la licence VE était incluse avec le pack de chiffrement. Le pack de chiffrement n'est plus proposé, mais reste valide. Bien qu'il ne soit pas actuellement requis, les clients existants peuvent choisir de "Passez à ONTAP One".

Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Vous devez avoir reçu la clé de licence VE de votre représentant commercial ou avoir installé ONTAP One.

Étapes

1. "Vérifiez que la licence VE est installée".

   Le nom du package de licences VE est `VE`.

2. Si la licence n'est pas installée, "Utilisez System Manager ou l'interface de ligne de commandes ONTAP pour l'installer".

Configurez la gestion externe des clés

En savoir plus sur la configuration de la gestion des clés externes avec ONTAP NetApp Volume Encryption

Vous pouvez utiliser un ou plusieurs serveurs de gestion de clés externes pour sécuriser les clés utilisées par le cluster pour accéder aux données chiffrées. Un serveur de gestion de clés externe est un système tiers de votre environnement de stockage qui fournit des clés aux nœuds via le protocole KMIP (Key Management Interoperability Protocol). Outre le gestionnaire de clés intégré, ONTAP prend en charge plusieurs serveurs de gestion de clés externes.

À partir d' ONTAP 9.10.1, vous pouvez utiliser Azure Key Vault ou Google Cloud Key Manager pour protéger vos clés NVE pour les SVM de données. À partir d' ONTAP 9.11.1, vous pouvez configurer plusieurs gestionnaires de clés externes dans un cluster. VoirConfigurer les serveurs de clés en cluster . À partir d' ONTAP 9.12.0, vous pouvez utiliser "KMS D'AWS" pour protéger vos clés NVE pour les SVM de données. À partir d' ONTAP 9.17.1, vous pouvez utiliser OpenStack Barbican KMS pour protéger vos clés NVE pour les SVM de données.

Gérez les gestionnaires de clés externes avec ONTAP System Manager

À partir de la version ONTAP 9.7, vous pouvez stocker et gérer les clés d'authentification et de chiffrement à l'aide du gestionnaire de clés intégré. À partir de ONTAP 9.13.1, vous pouvez également utiliser des gestionnaires de clés externes pour stocker et gérer ces clés.

Le gestionnaire de clés intégré stocke et gère les clés dans une base de données sécurisée interne au cluster. L'étendue du cluster est celle-ci. Un gestionnaire de clés externe stocke et gère les clés à l'extérieur du cluster. Il peut s'agir du cluster ou de la VM de stockage. Un ou plusieurs gestionnaires de clés externes peuvent être utilisés. Les conditions suivantes s'appliquent :

- Si le gestionnaire de clés intégré est activé, un gestionnaire de clés externe ne peut pas être activé au niveau du cluster, mais il peut être activé au niveau de la VM de stockage.
- Si un gestionnaire de clés externe est activé au niveau du cluster, le gestionnaire de clés intégré ne peut pas être activé.

Lorsque vous utilisez des gestionnaires de clés externes, vous pouvez enregistrer jusqu'à quatre serveurs de clés principaux par machine virtuelle de stockage et par cluster. Chaque serveur de clés principal peut être mis en cluster avec jusqu'à trois serveurs de clés secondaires.

Configurez un gestionnaire de clés externe

Pour ajouter un gestionnaire de clés externe à une VM de stockage, il est conseillé d'ajouter une passerelle en option lors de la configuration de l'interface réseau de la VM de stockage. Si la machine virtuelle de stockage a été créée sans la route réseau, vous devrez créer la route explicitement pour le gestionnaire de clés externe. Voir "Créer une LIF (interface réseau)".

Étapes

Vous pouvez configurer un gestionnaire de clés externe à partir de différents emplacements dans System Manager.

1. Pour configurer un gestionnaire de clés externe, effectuez l'une des étapes de démarrage suivantes.

Flux de travail	Navigation	Étape de départ
Configurer le gestionnaire de clés	**Cluster** > **Paramètres**	Accédez à la section **sécurité**. Sous **cryptage**, sélectionnez ⚙. Sélectionnez **Gestionnaire de clés externe**.
Ajouter un niveau local	**Stockage** > **niveaux**	Sélectionnez **+ Ajouter un niveau local**. Cochez la case « configurer le gestionnaire de clés ». Sélectionnez **Gestionnaire de clés externe**.
Préparez le stockage	**Tableau de bord**	Dans la section **capacité**, sélectionnez **préparer le stockage**. Sélectionnez ensuite « configurer le gestionnaire de clés ». Sélectionnez **Gestionnaire de clés externe**.
Configuration du chiffrement (gestionnaire de clés dans le périmètre de la VM de stockage uniquement)	**Stockage** > **machines virtuelles de stockage**	Sélectionnez la VM de stockage. Sélectionnez l'onglet **Paramètres**. Dans la section **cryptage** sous **sécurité**, sélectionnez ⚙.

2. Pour ajouter un serveur de clés principal, sélectionnez + Add et renseignez les champs **adresse IP ou Nom d'hôte** et **Port**.
3. Les certificats installés existants sont répertoriés dans les champs **KMIP Server CA Certificates** et **KMIP client Certificate**. Vous pouvez effectuer l'une des actions suivantes :
   - Sélectionnez ⌄ cette option pour sélectionner les certificats installés que vous souhaitez mapper au gestionnaire de clés. (Plusieurs certificats d'autorité de certification de service peuvent être sélectionnés, mais un seul certificat client peut être sélectionné.)
   - Sélectionnez **Ajouter un nouveau certificat** pour ajouter un certificat qui n'a pas encore été installé et le mapper au gestionnaire de clés externe.
   - Sélectionnez × en regard du nom du certificat pour supprimer les certificats installés que vous ne souhaitez pas mapper au gestionnaire de clés externe.
4. Pour ajouter un serveur de clés secondaire, sélectionnez **Ajouter** dans la colonne **Secondary Key Servers** et fournissez ses détails.
5. Sélectionnez **Enregistrer** pour terminer la configuration.

Modifier un gestionnaire de clés externe existant

Si vous avez déjà configuré un gestionnaire de clés externe, vous pouvez modifier ses paramètres.

Étapes

1. Pour modifier la configuration d'un gestionnaire de clés externe, effectuez l'une des étapes de démarrage suivantes.

Portée	Navigation	Étape de départ

Gestionnaire de clés externe de l'étendue du cluster	**Cluster** > **Paramètres**	Accédez à la section **sécurité**. Sous **Encryption**, sélectionnez ⋮, puis **Edit External Key Manager**.
Périmètre de l'ordinateur virtuel de stockage gestionnaire de clés externe	**Stockage** > **machines virtuelles de stockage**	Sélectionnez la VM de stockage. Sélectionnez l'onglet **Paramètres**. Dans la section **Encryption** sous **Security**, sélectionnez ⋮, puis **Edit External Key Manager**.

2. Les serveurs de clés existants sont répertoriés dans le tableau **Key Servers**. Vous pouvez effectuer les opérations suivantes :
   - Ajoutez un nouveau serveur de clés en sélectionnant + Add .
   - Supprimez un serveur de clés en sélectionnant ⋮ à la fin de la cellule de table contenant le nom du serveur de clés. Les serveurs de clés secondaires associés à ce serveur de clés principal sont également supprimés de la configuration.

Supprimez un gestionnaire de clés externe

Un gestionnaire de clés externe peut être supprimé si les volumes sont non chiffrés.

Étapes

1. Pour supprimer un gestionnaire de clés externe, effectuez l'une des opérations suivantes.

Portée	Navigation	Étape de départ
Gestionnaire de clés externe de l'étendue du cluster	**Cluster** > **Paramètres**	Accédez à la section **sécurité**. Sous **Encryption**, sélectionnez SELECT ⋮, puis **Delete External Key Manager**.
Périmètre de l'ordinateur virtuel de stockage gestionnaire de clés externe	**Stockage** > **machines virtuelles de stockage**	Sélectionnez la VM de stockage. Sélectionnez l'onglet **Paramètres**. Dans la section **Encryption** sous **Security**, sélectionnez ⋮, puis **Delete External Key Manager**.

Migration des clés entre les gestionnaires de clés

Lorsque plusieurs gestionnaires de clés sont activés sur un cluster, les clés doivent être migrées d'un gestionnaire de clés vers un autre. System Manager effectue automatiquement ce processus.

- Si le gestionnaire de clés intégré ou un gestionnaire de clés externe est activé au niveau du cluster et que certains volumes sont chiffrés, Ensuite, lorsque vous configurez un gestionnaire de clés externe au niveau de la VM de stockage, les clés doivent être migrées du gestionnaire de clés intégré ou du gestionnaire de clés externe au niveau du cluster vers le gestionnaire de clés externe au niveau de la VM de stockage. System Manager effectue automatiquement ce processus.
- Si les volumes ont été créés sans chiffrement sur une machine virtuelle de stockage, les clés n'ont pas besoin d'être migrées.

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 NVE dans ONTAP 9.6 et versions ultérieures

Utilisez les serveurs KMIP pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. À partir d' ONTAP 9.6, vous avez la possibilité de configurer un gestionnaire de clés externe distinct pour sécuriser les clés qu'un SVM de données utilise

pour accéder aux données chiffrées.

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.

Description de la tâche

Vous pouvez connecter jusqu'à quatre serveurs KMIP à un cluster ou à un SVM. Utilisez au moins deux serveurs pour la redondance et la reprise après sinistre.

Le périmètre de la gestion externe des clés détermine si les serveurs de gestion des clés sécurisent tous les SVM dans le cluster ou bien uniquement les SVM sélectionnés :

- Vous pouvez utiliser une *cluster scope* pour configurer la gestion des clés externe pour tous les SVM du cluster. L'administrateur du cluster a accès à chaque clé stockée sur les serveurs.
- Depuis ONTAP 9.6, vous pouvez utiliser une *SVM scope* pour configurer la gestion externe des clés pour une SVM de données dans le cluster. C'est le mieux adapté aux environnements mutualisés dans lesquels chaque locataire utilise un autre SVM (ou ensemble de SVM) pour transmettre les données. Seul l'administrateur du SVM pour un locataire donné peut accéder aux clés pour ce locataire.
- Pour les environnements mutualisés, installez une licence pour *MT_EK_MGMT* à l'aide de la commande suivante :

  ```
  system license add -license-code <MT_EK_MGMT license code>
  ```

  Pour en savoir plus, `system license add` consultez le "Référence de commande ONTAP".

Vous pouvez utiliser les deux étendues du même cluster. Si les serveurs de gestion des clés ont été configurés pour un SVM, ONTAP utilise uniquement ces serveurs pour sécuriser les clés. Sinon, ONTAP sécurise les clés avec les serveurs de gestion des clés configurés pour le cluster.

Vous pouvez configurer la gestion intégrée des clés au niveau du cluster et la gestion externe des clés au niveau de SVM. Vous pouvez utiliser le `security key-manager key migrate` Commande pour migrer les clés de la gestion intégrée des clés au périmètre du cluster vers des gestionnaires de clés externes au périmètre des SVM

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

Avant de commencer

- Les certificats client SSL KMIP et serveur doivent avoir été installés.
- Le serveur KMIP doit être accessible depuis l'interface LIF de gestion des nœuds de chaque nœud.
- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.
- Dans un environnement MetroCluster :
  - MetroCluster doit être entièrement configuré avant d'activer la gestion des clés externes.
  - Vous devez installer le même certificat SSL KMIP sur les deux clusters.
  - Un gestionnaire de clés externe doit être configuré 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
```

> Le `security key-manager external enable` commande remplace le `security key-manager setup` commande. Si vous exécutez la commande à l'invite de connexion du cluster, *`admin_SVM`* par défaut, il s'agit du SVM d'administration du cluster actuel. Vous pouvez exécuter le `security key-manager external modify` commande pour modifier la configuration de la gestion des clés externes.

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 :

```
clusterl::> security key-manager external enable -vserver cluster1 -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. Configurer un SVM gestionnaire de clés :

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

> - Si vous exécutez la commande à l'invite de connexion SVM, `SVM` par défaut, le SVM actuel. Vous pouvez exécuter le `security key-manager external modify` commande pour modifier la configuration de la gestion des clés externes.
> - Dans un environnement MetroCluster, si vous configurez une gestion externe des clés pour une SVM de données, vous n'avez pas besoin de répéter le `security key-manager external enable` commande sur le cluster partenaire.

La commande suivante active la gestion externe des clés pour `svm1` avec un serveur à une seule clé qui écoute le port par défaut 5696 :

```
svm1l::> security key-manager external enable -vserver svm1 -key-servers
keyserver.svm1.com -client-cert SVM1ClientCert -server-ca-certs
SVM1ServerCaCert
```

3. Répétez la dernière étape pour tout SVM supplémentaire.

Vous pouvez également utiliser `security key-manager external add-servers` la commande pour configurer des SVM supplémentaires. `security key-manager external add-servers`La commande remplace `security key-manager add` la commande. Pour en savoir plus, `security key-manager external add-servers` consultez le "Référence de commande ONTAP".

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

   `security key-manager external show-status -node node_name`

   `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
      svm1
               keyserver.svm1.com:5696                         available
      cluster1
               10.0.0.10:5696                                  available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234    available
               ks1.local:15696                                 available
node2
      svm1
               keyserver.svm1.com:5696                         available
      cluster1
               10.0.0.10:5696                                  available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234    available
               ks1.local:15696                                 available

8 entries were displayed.
```

5. 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 de convertir les volumes.

Informations associées

- Configurez les serveurs de clés externes en cluster
- "ajout de licence système"
- "migration de clés du gestionnaire de clés de sécurité"
- "gestionnaire de clés de sécurité serveurs d'ajout externes"
- "gestionnaire de clés de sécurité externe show-status"

Activer la gestion des clés externes pour NVE 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`

   ```
   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.

Gérer les clés NVE pour les SVM de données ONTAP avec un fournisseur de cloud

Depuis la version ONTAP 9.10.1, vous pouvez utiliser "Azure Key Vault (AKV)" et "Service de gestion des clés (KMS cloud) de Google Cloud Platform"protéger vos clés de chiffrement ONTAP dans une application hébergée dans le cloud. Depuis la version ONTAP 9.12.0, vous pouvez également protéger les clés NVE avec "KMS D'AWS".

Vous pouvez utiliser AWS KMS, AKV et Cloud KMS pour protéger les données "Clés NetApp Volume Encryption (NVE)" Uniquement pour les SVM de données.

Description de la tâche

La gestion des clés avec un fournisseur cloud peut être activée via l'interface de ligne de commandes ou l'API REST ONTAP.

Lorsque vous utilisez un fournisseur cloud pour protéger vos clés, sachez que par défaut, une LIF de SVM de

données communique avec le terminal de gestion des clés cloud. Un réseau de gestion de nœuds est utilisé pour communiquer avec les services d'authentification du fournisseur cloud (login.microsoftonline.com pour Azure ; oauth2.googleapis.com pour le Cloud KMS). Si le réseau de cluster n'est pas configuré correctement, le cluster n'utilisera pas correctement le service de gestion des clés.

Lorsque vous utilisez un service de gestion des clés de fournisseur cloud, vous devez connaître les limites suivantes :

- La gestion des clés du fournisseur cloud n'est pas disponible pour le chiffrement du stockage NetApp (NSE) et le chiffrement d'agrégat NetApp (NAE). "KMIP externes" peut être utilisé à la place.
- La gestion des clés du fournisseur cloud n'est pas disponible pour les configurations MetroCluster.
- La gestion des clés du fournisseur cloud peut uniquement être configurée sur un SVM de données.

Avant de commencer

- Vous devez avoir configuré le KMS sur le fournisseur cloud approprié.
- Les nœuds du cluster ONTAP doivent prendre en charge NVE.
- "Vous devez avoir installé les licences Volume Encryption (VE) et MTEKM (Encryption Key Management) multitenant". Ces licences sont incluses avec "ONTAP One".
- Vous devez être administrateur du cluster ou du SVM.
- La SVM de données ne doit pas inclure de volumes chiffrés ni utiliser un gestionnaire de clés. Si le SVM de données inclut des volumes chiffrés, vous devez les migrer avant de configurer le KMS.

Activez la gestion externe des clés

L'activation de la gestion externe des clés dépend du gestionnaire de clés que vous utilisez. Choisissez l'onglet du gestionnaire de clés et de l'environnement appropriés.

AWS

Avant de commencer

- Vous devez créer un octroi pour la clé KMS AWS qui sera utilisée par le rôle IAM gérant le chiffrement. Le rôle IAM doit inclure une politique permettant les opérations suivantes :
  - `DescribeKey`
  - `Encrypt`
  - `Decrypt`

  Pour plus d'informations, consultez la documentation AWS pour "subventions".

Activez AWS KMV sur un SVM ONTAP

1. Avant de commencer, procurez-vous l'ID de clé d'accès et la clé secrète sur votre serveur KMS AWS.
2. Définissez le niveau de privilège sur avancé : `set -priv advanced`
3. Activer AWS KMS : `security key-manager external aws enable -vserver` *`svm_name`* `-region` *`AWS_region`* `-key-id` *`key_ID`* `-encryption-context` *`encryption_context`*
4. Lorsque vous y êtes invité, entrez la clé secrète.
5. Vérifiez que le KMS AWS a été correctement configuré : `security key-manager external aws show -vserver` *`svm_name`*

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

Azure

Activez Azure Key Vault sur un SVM ONTAP

1. Avant de commencer, vous devez obtenir les informations d'authentification appropriées à partir de votre compte Azure, soit un secret client, soit un certificat. Vous devez également vous assurer que tous les nœuds du cluster fonctionnent correctement. Vous pouvez le vérifier à l'aide de la commande `cluster show`. Pour en savoir plus, `cluster show` consultez le "Référence de commande ONTAP".
2. Définissez le niveau privilégié sur avancé `set -priv advanced`
3. Activation de AKV sur le SVM `security key-manager external azure enable -client -id` *`client_id`* `-tenant-id` *`tenant_id`* `-name -key-id` *`key_id`* `-authentication -method {certificate|client-secret}` Lorsque vous y êtes invité, entrez le certificat client ou le secret client de votre compte Azure.
4. Vérifiez que la fonction AKV est activée correctement : `security key-manager external azure show vserver` *`svm_name`* Si l'accessibilité du service n'est pas OK, établir la connectivité au service de gestion des clés AKV via la LIF du SVM de données.

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

Google Cloud

Activez le serveur KMS cloud sur une SVM ONTAP

1. Avant de commencer, procurez-vous la clé privée du fichier de clé de compte Google Cloud KMS au

format JSON. Elles sont disponibles dans votre compte GCP. Vous devez également vous assurer que tous les nœuds du cluster fonctionnent correctement. Vous pouvez le vérifier à l'aide de la commande `cluster show`. Pour en savoir plus, `cluster show` consultez le "Référence de commande ONTAP".

2. Définir le niveau privilégié sur avancé : `set -priv advanced`
3. Activation du KMS cloud sur le SVM `security key-manager external gcp enable -vserver svm_name -project-id project_id-key-ring-name key_ring_name -key -ring-location key_ring_location -key-name key_name` Lorsque vous y êtes invité, entrez le contenu du fichier JSON avec la clé privée du compte de service
4. Vérifiez que Cloud KMS est configuré avec les paramètres corrects : `security key-manager external gcp show vserver svm_name` Le statut de `kms_wrapped_key_status` sera `"UNKNOWN"` si aucun volume chiffré n'a été créé. Si l'accessibilité du service n'est pas correcte, établissez la connectivité au service de gestion des clés GCP via les données SVM LIF.

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

Si un ou plusieurs volumes chiffrés sont déjà configurés pour un SVM de données et que les clés NVE correspondantes sont gérées par le gestionnaire de clés intégré des SVM d'administration, ces clés doivent être migrées vers le service externe de gestion des clés. Pour ce faire via l'interface de ligne de commandes, lancer la commande : `security key-manager key migrate -from-Vserver admin_SVM -to -Vserver data_SVM` Il n'est pas possible de créer de nouveaux volumes chiffrés pour le SVM de données du locataire tant que toutes les clés NVE du SVM de données ne sont pas migrées correctement.

Informations associées

- "Chiffrez les volumes avec les solutions de chiffrement NetApp pour Cloud Volumes ONTAP"
- "gestionnaire de clés de sécurité externe"

Gérer les clés ONTAP avec Barbican KMS

À partir d' ONTAP 9.17.1, vous pouvez utiliser OpenStack "Barbican KMS" Pour protéger les clés de chiffrement ONTAP . Barbican KMS est un service de stockage et d'accès sécurisé aux clés. Barbican KMS peut être utilisé pour protéger les clés NetApp Volume Encryption (NVE) des SVM de données. Barbican s'appuie sur "Keystone OpenStack" , Service d'identité d'OpenStack, pour l'authentification.

Description de la tâche

Vous pouvez configurer la gestion des clés avec Barbican KMS via l'interface de ligne de commande (CLI) ou l'API REST ONTAP . Avec la version 9.17.1, la prise en charge de Barbican KMS présente les limitations suivantes :

- Barbican KMS n'est pas compatible avec NetApp Storage Encryption (NSE) et NetApp Aggregate Encryption (NAE). Vous pouvez également utiliser "KMIP externes" ou le "Gestionnaire de clés embarqué (OKM)" pour les clés NSE et NVE.
- Barbican KMS n'est pas pris en charge pour les configurations MetroCluster .
- Barbican KMS ne peut être configuré que pour un SVM de données. Il n'est pas disponible pour le SVM d'administration.

Sauf indication contraire, les administrateurs du `admin` le niveau de privilège peut effectuer les procédures suivantes.

Avant de commencer

- Barbican KMS et OpenStack Keystone doivent être configurés. La SVM utilisée avec Barbican doit avoir accès au réseau des serveurs Barbican et OpenStack Keystone .
- Si vous utilisez une autorité de certification (CA) personnalisée pour les serveurs Barbican et OpenStack Keystone , vous devez installer le certificat CA avec `security certificate install -type server-ca -vserver <admin_svm>` .

Créer et activer une configuration Barbican KMS

Vous pouvez créer une nouvelle configuration Barbican KMS pour une SVM et l'activer. Une SVM peut avoir plusieurs configurations Barbican KMS inactives, mais une seule peut être active à la fois.

Étapes

1. Créez une nouvelle configuration Barbican KMS inactive pour un SVM :

```
security key-manager external barbican create-config -vserver <svm_name>
-config-name <unique_config_name> -key-id <key_id> -keystone-url
<keystone_url> -application-cred-id
<keystone_applications_credentials_id>
```

   - `-key-id` est l'identifiant de la clé de chiffrement Barbican (KEK). Saisissez une URL complète, incluant `https://` .

     Certaines URL contiennent un point d'interrogation (?). Ce point active l'aide active de la ligne de commande ONTAP . Pour saisir une URL avec un point d'interrogation, vous devez d'abord désactiver l'aide active avec la commande. `set -active-help false` . L'aide active peut être réactivée ultérieurement avec la commande `set -active -help true` . En savoir plus dans le "Référence de commande ONTAP" .

   - `-keystone-url` est l'URL de l'hôte d'autorisation OpenStack Keystone . Saisissez une URL complète, y compris `https://` .
   - `-application-cred-id` est l'ID d'identification de l'application.

     Après avoir saisi cette commande, vous serez invité à saisir la clé secrète des informations d'identification de l'application. Cette commande crée une configuration Barbican KMS inactive.

     L'exemple suivant crée une nouvelle configuration Barbican KMS inactive nommée `config1` pour le SVM `svm1` :

```
cluster1::> security key-manager external barbican create-config
-vserver svm1 -config-name config1 -keystone-url
https://172.21.76.152:5000/v3 -application-cred-id app123 -key-id
https://172.21.76.153:9311/v1/secrets/<id_value>

Enter the Application Credentials Secret for authentication with
Keystone: <key_value>
```

2. Activer la nouvelle configuration Barbican KMS :

```
security key-manager keystore enable -vserver <svm_name> -config-name
<unique_config_name> -keystore barbican
```

Vous pouvez utiliser cette commande pour basculer entre les configurations Barbican KMS. Si une configuration Barbican KMS est déjà active sur la SVM, elle sera désactivée et la nouvelle configuration sera activée.

3. Vérifiez que la nouvelle configuration Barbican KMS est active :

```
security key-manager external barbican check -vserver <svm_name> -node
<node_name>
```

Cette commande fournit l'état de la configuration active de Barbican KMS sur la SVM ou le nœud. Par exemple, si la SVM `svm1` sur le nœud `node1` dispose d'une configuration Barbican KMS active, la commande suivante renverra l'état de cette configuration :

```
cluster1::> security key-manager external barbican check -node node1

Vserver: svm1
Node: node1

Category: service_reachability
             Status: OK

Category: kms_wrapped_key_status
             Status: OK
```

Mettre à jour les informations d'identification et les paramètres d'une configuration Barbican KMS

Vous pouvez afficher et mettre à jour les paramètres actuels d'une configuration Barbican KMS active ou inactive.

Étapes

1. Afficher les configurations KMS Barbican actuelles pour un SVM :

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

L'ID de clé, l'URL OpenStack Keystone et l'ID d'identification de l'application sont affichés pour chaque configuration Barbican KMS sur le SVM.

2. Mettre à jour les paramètres d'une configuration Barbican KMS :

```
security key-manager external barbican update-config -vserver <svm_name>
-config-name <unique_config_name> -timeout <timeout> -verify
<true|false> -verify-host <true|false>
```

Cette commande met à jour les paramètres de délai d'expiration et de vérification de la configuration Barbican KMS spécifiée. `timeout` Détermine le temps en secondes pendant lequel ONTAP attend la réponse de Barbican avant l'échec de la connexion . `timeout` c'est dix secondes. `verify` et `verify-host` Déterminer si l'identité et le nom d'hôte de l'hôte Barbican doivent être vérifiés avant la connexion. Par défaut, ces paramètres sont définis sur `true` . Le `vserver` et `config-name` Les paramètres sont obligatoires. Les autres paramètres sont facultatifs.

3. Si nécessaire, mettez à jour les informations d'identification d'une configuration Barbican KMS active ou inactive :

```
security key-manager external barbican update-credentials -vserver
<svm_name> -config-name <unique_config_name> -application-cred-id
<keystone_applications_credentials_id>
```

Après avoir entré cette commande, vous serez invité à saisir la nouvelle clé secrète des informations d'identification de l'application.

4. Si nécessaire, restaurez une clé de chiffrement de clé SVM manquante (KEK) pour une configuration Barbican KMS active :
   a. Restaurer une clé KEK SVM manquante avec `security key-manager external barbican restore` :

```
security key-manager external barbican restore -vserver <svm_name>
```

Cette commande restaurera le SVM KEK pour la configuration Barbican KMS active en communiquant avec le serveur Barbican.

5. Si nécessaire, recréez la clé SVM KEK pour une configuration Barbican KMS :
   a. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

b. Renouveler la clé SVM KEK avec `security key-manager external barbican rekey-internal` :

```
security key-manager external barbican rekey-internal -vserver
<svm_name>
```

Cette commande génère une nouvelle clé KEK SVM pour la SVM spécifiée et réencapsule les clés de chiffrement du volume avec cette nouvelle clé KEK. Cette dernière sera protégée par la configuration active de Barbican KMS.

Migrer les clés entre Barbican KMS et le gestionnaire de clés embarqué

Vous pouvez migrer des clés de Barbican KMS vers le gestionnaire de clés embarqué (OKM), et inversement. Pour en savoir plus sur OKM, consultez la page "Activez la gestion intégrée des clés dans ONTAP 9.6 et versions ultérieures" .

Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Si nécessaire, migrez les clés de Barbican KMS vers OKM :

```
security key-manager key migrate -from-vserver <svm_name> -to-vserver
<admin_svm_name>
```

`svm_name` est le nom du SVM avec la configuration Barbican KMS.

3. Si nécessaire, migrez les clés de l'OKM vers Barbican KMS :

```
security key-manager key migrate -from-vserver <admin_svm_name> -to
-vserver <svm_name>
```

Désactiver et supprimer une configuration Barbican KMS

Vous pouvez désactiver une configuration Barbican KMS active sans volumes chiffrés et supprimer une configuration Barbican KMS inactive.

Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Désactiver une configuration Barbican KMS active :

```
security key-manager keystore disable -vserver <svm_name>
```

Si des volumes chiffrés NVE existent sur la SVM, vous devez les déchiffrer ou migrer les clés Avant de désactiver la configuration Barbican KMS. L'activation d'une nouvelle configuration Barbican KMS ne nécessite pas le déchiffrement des volumes NVE ni la migration des clés, et désactivera la configuration Barbican KMS active actuelle.

3. Supprimer une configuration Barbican KMS inactive :

```
security key-manager keystore delete -vserver <svm_name> -config-name
<unique_config_name> -type barbican
```

Activer la gestion des clés intégrées pour NVE dans ONTAP 9.6 et versions ultérieures

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 à chiffrement automatique.

Description de la tâche

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

Si vous avez une configuration MetroCluster, vous devez exécuter `security key-manager onboard enable` d'abord sur le cluster local, puis exécutez le `security key-manager onboard sync` sur le cluster distant, en utilisant la même phrase de passe sur chacun d'entre eux. Lorsque vous exécutez le `security key-manager onboard enable` à partir du cluster local, puis effectuez une synchronisation sur le cluster distant. vous n'avez pas besoin d'exécuter le `enable` commandez à nouveau à partir du cluster distant.

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. Vous pouvez utiliser le `cc-mode-enabled=yes` option pour exiger que les utilisateurs saisissent la phrase de passe après un redémarrage.

Pour NVE, si vous définissez `cc-mode-enabled=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`.

Lors de la configuration du chiffrement des données ONTAP au repos, pour répondre aux exigences des solutions commerciales classifiées (CSfC), vous devez utiliser NSE avec NVE et vous assurer que le gestionnaire de clés embarqué est activé en mode Critères communs. Voir"Description de la solution CSFC" .

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 vous ne parvenez pas à saisir la phrase secrète du cluster 5 fois, attendez 24 heures ou redémarrez 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. Le système passe à l'étape suivante du processus de mise à jour de l'image si la validation réussit ; sinon, la mise à jour de l'image échoue. En savoir plus sur `cluster image` dans le"Référence de commande ONTAP" .

Le gestionnaire de clés embarqué stocke les clés dans une mémoire volatile. Le contenu de la mémoire volatile est effacé lorsque le système est redémarré ou arrêté. Le système efface la mémoire volatile dans les 30 secondes lorsqu'il est arrêté.

Avant de commencer

- 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 configuration du gestionnaire de clés :

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

   Réglez `cc-mode-enabled=yes` pour demander aux utilisateurs de saisir la phrase de passe du gestionnaire de clés après un redémarrage. Pour NVE, si vous définissez `cc-mode-enabled=yes`, volumes que vous créez avec `volume create` et `volume move start` les commandes sont automatiquement chiffrées. Le `- cc-mode-enabled` Cette option n'est pas prise en charge dans les configurations MetroCluster. Le `security key-manager onboard enable` la commande remplace le `security key-manager setup` commande.

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 les clés d'authentification ont été créées :

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

> `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".

5. En option, vous pouvez convertir des volumes de texte brut en volumes chiffrés.

   ```
   volume encryption conversion start
   ```

   Le gestionnaire de clés intégré doit être entièrement configuré avant de convertir les volumes. Dans un environnement MetroCluster, le gestionnaire de clés intégré doit être configuré sur les deux sites.

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.

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

- "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"

Activer la gestion des clés intégrées pour NVE dans ONTAP 9.5 et versions antérieures

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 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 ou NVE 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 embarqué.

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`

   ```
   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
   ```

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

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

   `volume encryption conversion start`

   Configurez le gestionnaire de clés intégré avant de convertir les volumes. Dans les environnements MetroCluster , configurez-le sur les deux sites.

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.

Lorsque vous configurez la phrase secrète du gestionnaire de clés embarquées, sauvegardez les informations dans un emplacement sécurisé en dehors du système de stockage en cas de sinistre. Voir"Sauvegardez manuellement les informations intégrées de gestion des clés" .

Informations associées

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

Activer la gestion des clés intégrées dans les nœuds ONTAP nouvellement ajoutés

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.

Pour ONTAP 9.6 et versions ultérieures, vous devez exécuter le `security key-manager onboard sync` commande à exécuter chaque fois que vous ajoutez un nœud au cluster.

Pour ONTAP 9.5 et les versions antérieures, vous devez exécuter le `security key-manager setup` commande à chaque ajout d'un nœud au cluster.

Si vous ajoutez un nœud à un cluster avec gestion des clés intégrée, exécutez cette commande pour actualiser les clés manquantes.

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

- Avec ONTAP 9.6, 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.

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

- 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`.

Si la tentative de saisie du mot de passe échoue, redémarrez le nœud. Après le redémarrage, vous pouvez essayer de saisir à nouveau la phrase de passe.

Informations associées

- "commandes d’image de cluster"
- "activation externe du gestionnaire de clés de sécurité"
- "activation du gestionnaire de clés de sécurité intégré"