



# Configurez NVE

## ONTAP 9

NetApp  
April 24, 2024

# Sommaire

- Configurez NVE ..... 1
  - Déterminez si votre version de cluster prend en charge NVE ..... 1
  - Installez la licence ..... 1
  - Configurez la gestion externe des clés ..... 2
  - Intégrez la gestion des clés dans ONTAP 9.6 et versions ultérieures (NVE). .... 13
  - Gestion intégrée des clés dans ONTAP 9.5 et versions antérieures (NVE) ..... 16
  - Activez la gestion intégrée des clés dans les nouveaux nœuds ajoutés ..... 19

# Configurez NVE

## Déterminez si votre version de cluster 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.

### Étape

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

```
version -v
```

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

La commande suivante détermine si NVE est pris en charge sur `cluster1`.

```
cluster1::> version -v
NetApp Release 9.1.0: Tue May 10 19:30:23 UTC 2016 <1Ono-DARE>
```

La sortie de `1Ono-DARE` indique que NVE n'est pas pris en charge sur la version du cluster.

## Installez la licence

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'ils ne soient pas encore requis, les clients existants peuvent choisir de le faire ["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

## Configurer la gestion externe des clés en vue d'ensemble

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).



Pour ONTAP 9.1 et les versions antérieures, les LIFs de node-management doivent être attribuées à des ports configurés avec le rôle de node-management avant de pouvoir utiliser le gestionnaire de clés externe.

NetApp Volume Encryption (NVE) prend en charge le gestionnaire de clés intégré dans ONTAP 9.1 et les versions ultérieures. Depuis la version ONTAP 9.3, NVE prend en charge le protocole KMIP (externe Key Management) et le gestionnaire de clés intégré. À partir de ONTAP 9.10.1, vous pouvez l'utiliser [Azure Key Vault](#) ou [Google Cloud Key Manager Service](#) Pour protéger vos clés NVE. À partir de ONTAP 9.11.1, vous pouvez configurer plusieurs gestionnaires de clés externes dans un cluster. Voir [Configurez les serveurs de clés en cluster](#).

## Gérez des gestionnaires de clés externes avec 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	<b>Cluster &gt; Paramètres</b>	Accédez à la section <b>sécurité</b> . Sous <b>cryptage</b> , sélectionnez  . Sélectionnez <b>Gestionnaire de clés externe</b> .
Ajouter un niveau local	<b>Stockage &gt; niveaux</b>	Sélectionnez <b>+ Ajouter un niveau local</b> . Cochez la case « configurer le gestionnaire de clés ». Sélectionnez <b>Gestionnaire de clés externe</b> .
Préparez le stockage	<b>Tableau de bord</b>	Dans la section <b>capacité</b> , sélectionnez <b>préparer le stockage</b> . Sélectionnez ensuite « configurer le gestionnaire de clés ». Sélectionnez <b>Gestionnaire de clés externe</b> .
Configuration du chiffrement (gestionnaire de clés dans le périmètre de la VM de stockage uniquement)	<b>Stockage &gt; machines virtuelles de stockage</b>	Sélectionnez la VM de stockage. Sélectionnez l'onglet <b>Paramètres</b> . Dans la section <b>cryptage</b> sous <b>sécurité</b> , 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  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 **x** 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	<b>Cluster &gt; Paramètres</b>	Accédez à la section <b>sécurité</b> . Sous <b>cryptage</b> , sélectionnez  , Puis sélectionnez <b>Modifier le gestionnaire de clés externe</b> .
Périmètre de l'ordinateur virtuel de stockage gestionnaire de clés externe	<b>Stockage &gt; machines virtuelles de stockage</b>	Sélectionnez la VM de stockage. Sélectionnez l'onglet <b>Paramètres</b> . Dans la section <b>cryptage</b> sous <b>sécurité</b> , sélectionnez  , Puis sélectionnez <b>Modifier le gestionnaire de clés externe</b> .



- 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 la table qui contient 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

- 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	<b>Cluster &gt; Paramètres</b>	Accédez à la section <b>sécurité</b> . Sous <b>cryptage</b> , sélectionnez <b>SELECT</b>  , Puis sélectionnez <b>Supprimer le gestionnaire de clés externe</b> .
Périmètre de l'ordinateur virtuel de stockage gestionnaire de clés externe	<b>Stockage &gt; machines virtuelles de stockage</b>	Sélectionnez la VM de stockage. Sélectionnez l'onglet <b>Paramètres</b> . Dans la section <b>cryptage</b> sous <b>sécurité</b> , sélectionnez  , Puis sélectionnez <b>Supprimer le gestionnaire de clés externe</b> .

### 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.

## Installez les certificats SSL sur le cluster

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
```

## Gestion externe des clés dans ONTAP 9.6 et versions ultérieures (NVE)

Vous pouvez utiliser un ou plusieurs serveurs KMIP pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. Depuis ONTAP 9.6, il est possible de configurer un gestionnaire de clés externe distinct pour sécuriser les clés utilisées par un SVM de données 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 un SVM. Un minimum de deux serveurs est recommandé 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 connaître la syntaxe complète de la commande, reportez-vous à la page man.

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

## Avant de commencer

- Les certificats client SSL KMIP et serveur doivent avoir été installés.
- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.
- Si vous souhaitez activer la gestion externe des clés dans un environnement MetroCluster, MetroCluster doit être entièrement configuré avant d'activer la gestion externe des clés.
- Dans un environnement MetroCluster, vous devez installer le 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
```





- Le `security key-manager external enable` la commande remplace le `security key-manager setup` commande. Si vous exécutez la commande à l'invite de connexion du cluster, *admin\_SVM* Par défaut au SVM admin du cluster actuel. Vous devez être l'administrateur du cluster pour configurer le périmètre du cluster. Vous pouvez exécuter le `security key-manager external modify` commande pour modifier la configuration de la gestion externe des clés.
- 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 -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 du SVM, *SVM* Par défaut au SVM actuel On doit être un administrateur de cluster ou de SVM pour configurer le cadre de la SVM. Vous pouvez exécuter le `security key-manager external modify` commande pour modifier la configuration de la gestion externe des clés.
- 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 :

```
svm11::> 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 le `security key-manager external add-servers` Commande permettant de configurer des SVM supplémentaires Le `security key-manager external add-servers` la commande remplace le `security key-manager add` commande. Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

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

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



Le `security key-manager external show-status` la commande remplace le `security key-manager show -status` commande. Pour connaître la syntaxe complète de la commande, reportez-vous à la page `man`.

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

## Activez la gestion externe des clés 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 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.

2. Entrez la réponse appropriée à chaque invite.
3. Ajoutez un serveur KMIP :

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

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



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

4. Ajoutez un serveur KMIP supplémentaire pour la redondance :

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

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



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

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

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

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

```
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 avec un fournisseur cloud

À partir de ONTAP 9.10.1, vous pouvez l'utiliser "[Azure Key Vault \(AKV\)](#)" et "[Service de gestion des clés \(KMS cloud\) de Google Cloud Platform](#)" Pour protéger vos clés de chiffrement ONTAP dans une application hébergée dans le cloud. À partir de 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 KMS 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`

## 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`.
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.

## 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`.

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 appropriés :

```
security key-manager external gcp show vserver svm_name
```

Le statut de `kms_wrapped_key_status` sera le cas "UNKNOWN" si aucun volume chiffré n'a été créé.

Si la accessibilité du service n'est pas satisfaisante, établissez la connectivité au service de gestion des clés GCP via LIF du SVM de données.

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"](#)

## Intégrez la gestion des clés dans ONTAP 9.6 et versions ultérieures (NVE)

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.

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 relatives aux solutions commerciales pour les données classées (CSfC), vous devez utiliser NSE avec NVE et vous assurer que le gestionnaire de clés intégré est activé en mode critères communs. Reportez-vous à la ["Description de la solution CSfC"](#) Pour en savoir plus sur 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 saisissez pas la phrase secrète appropriée au démarrage, les volumes chiffrés ne sont pas montés. Pour corriger cette situation, vous devez redémarrer le nœud et saisir la phrase secrète correcte du cluster. 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. Le processus de mise à jour de l'image passe à l'étape suivante si la validation réussit ; sinon, la mise à jour de l'image échoue. Voir la `cluster image` pour plus d'informations sur les mises à jour système.

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

- 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.

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

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

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

2. 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.

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
```



Le `security key-manager key query` la commande remplace le `security key-manager query key` commande. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

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

```
cluster1::> security key-manager key query -key-type NSE-AK
Node: node1
Vserver: cluster1
Key Manager: onboard
Key Manager Type: OKM
Key Manager Policy: -
```

Key Tag	Key Type	Encryption	Restored
node1	NSE-AK	AES-256	true
Key ID: 00000000000000000000200000000000100056178fc6ace6d91472df8a9286daacc00000000 00000000			
node1	NSE-AK	AES-256	true
Key ID: 00000000000000000000200000000000100df1689a148fdfbf9c2b198ef974d0baa00000000 00000000			

2 entries were displayed.

5. Vous pouvez également convertir des volumes en 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.

Chaque fois que vous configurez la phrase secrète Onboard Key Manager, vous devez également sauvegarder les informations manuellement dans un emplacement sécurisé en dehors du système de stockage afin de les utiliser en cas d'incident. Voir ["Sauvegardez manuellement les informations intégrées de gestion des clés"](#).

## Gestion intégrée des clés dans ONTAP 9.5 et versions antérieures (NVE)

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 externe des clés (KMIP), vous devez avoir supprimé 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.
- 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 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 :

• • •

- 



- 



6. Vous pouvez également convertir des volumes en 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.

Chaque fois que vous configurez la phrase secrète Onboard Key Manager, vous devez également sauvegarder les informations manuellement dans un emplacement sécurisé en dehors du système de stockage afin de les utiliser en cas d'incident. Voir ["Sauvegardez manuellement les informations intégrées de gestion des clés"](#).

## Activez la gestion intégrée des clés dans les nouveaux nœuds 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 9.5 et les versions antérieures, vous devez exécuter le `security key-manager setup` commande à chaque ajout d'un nœud au cluster.

Pour ONTAP 9.6 et versions ultérieures, vous devez exécuter le `security key-manager sync` commande à chaque ajout d'un nœud au cluster.

Si vous ajoutez un nœud à un cluster dont la gestion intégrée des clés est configurée, vous 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.
- 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.

## Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

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

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

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

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

## Informations sur les marques commerciales

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