Configurez NetApp Volume Encryption

ONTAP 9

NetApp
April 01, 2023

Table des matières

Configurez NetApp Volume Encryption

Configurer la présentation de NetApp Volume Encryption

NetApp Volume Encryption (NVE) est une technologie logicielle de chiffrement des données au repos d'un volume à la fois. Une clé de chiffrement accessible uniquement au système de stockage garantit que les données du volume ne peuvent pas être lues si l'appareil sous-jacent est requalifié, perdu ou volé.

Présentation de NVE

Les données, y compris les copies Snapshot, et les métadonnées sont chiffrées. L'accès aux données est donné par une clé XTS-AES-256 unique, une par volume. Un serveur de gestion externe des clés ou un gestionnaire de clés intégré sert des clés aux nœuds :

- Le serveur externe de gestion des clés est un système tiers de votre environnement de stockage qui transmet des clés aux nœuds à l'aide du protocole KMIP (Key Management Interoperability Protocol). Il est recommandé de configurer des serveurs de gestion externe des clés sur un système de stockage différent de vos données.
- Le gestionnaire de clés intégré est un outil intégré qui sert des clés aux nœuds du même système de stockage que vos données.

Depuis ONTAP 9.7, le chiffrement d'agrégat et de volume est activé par défaut si vous disposez d'une licence VE (Volume Encryption) et utilisez un gestionnaire de clés intégré ou externe. Lorsqu'un gestionnaire de clés externe ou intégré est configuré, la configuration du chiffrement des données au repos est modifiée pour les nouveaux agrégats et les nouveaux volumes. Par défaut, NetApp Aggregate Encryption (NAE) sera activé dans les nouveaux agrégats. Par défaut, les nouveaux volumes qui ne font pas partie d'un agrégat NAE ont sur lequel le chiffrement de volume NetApp (NVE) est activé. Lorsqu'un serveur SVM (Data Storage Virtual machine) est configuré avec son propre gestionnaire de clés à l'aide d'une gestion mutualisée des clés, alors le volume créé pour ce SVM est automatiquement configuré avec NVE.

Vous pouvez activer le chiffrement sur un volume nouveau ou existant. NVE prend en charge la gamme complète de fonctionnalités d'efficacité du stockage, notamment la déduplication et la compression.

> Si vous utilisez SnapLock, vous pouvez activer le chiffrement uniquement sur les nouveaux volumes SnapLock vides. Vous ne pouvez pas activer le chiffrement sur un volume SnapLock existant.

Vous pouvez utiliser NVE sur n'importe quel type d'agrégat (HDD, SSD, hybride, LUN de baie), avec n'importe quel type RAID et dans n'importe quelle implémentation ONTAP prise en charge, y compris ONTAP Select. Vous pouvez également utiliser NVE avec le chiffrement matériel pour « chiffrer » les données sur des disques à autochiffrement.

> AFF A220, AFF A800, FAS2720, FAS2750 et versions ultérieures stockent les core dumps sur leur périphérique de démarrage. Lorsque NVE est activé sur ces systèmes, le « core dump » est également chiffré.

Chiffrement d'agrégat

En général, une clé unique est attribuée à chaque volume chiffré. Lorsque le volume est supprimé, la clé est

supprimée.

Depuis ONTAP 9.6, il est possible d'utiliser *NetApp Aggregate Encryption (NAE)* pour attribuer des clés à l'agrégat contenant pour le chiffrement des volumes. Lors de la suppression d'un volume chiffré, les clés de l'agrégat sont préservées. Les clés sont supprimées si l'agrégat entier est supprimé.

Vous devez utiliser le chiffrement au niveau de l'agrégat pour procéder à la déduplication à la volée ou en arrière-plan au niveau de l'agrégat. NVE ne prend cependant pas en charge la déduplication au niveau de l'agrégat.

Depuis ONTAP 9.7, le chiffrement d'agrégat et de volume est activé par défaut si vous disposez d'une licence VE (Volume Encryption) et utilisez un gestionnaire de clés intégré ou externe.

Les volumes NVE et NAE peuvent coexister sur un même agrégat. Par défaut, les volumes NAE sont chiffrés avec un chiffrement au niveau des agrégats. Vous pouvez remplacer la valeur par défaut lorsque vous chiffrez le volume.

Vous pouvez utiliser le `volume move` Commande de conversion d'un volume NVE en volume NAE, et inversement. Vous pouvez répliquer un volume NAE sur un volume NVE.

Vous ne pouvez pas utiliser `secure purge` Commandes sur un volume NAE.

Quand utiliser des serveurs externes de gestion des clés

Bien qu'il soit moins coûteux et généralement plus pratique d'utiliser le gestionnaire de clés intégré, vous devez configurer des serveurs KMIP si les conditions suivantes sont vraies :

- Votre solution de gestion des clés de chiffrement doit être conforme à la norme FIPS 140-2 (Federal information Processing Standards) ou OASIS KMIP.
- Vous avez besoin d'une solution à plusieurs clusters et d'une gestion centralisée des clés de chiffrement.
- Votre entreprise exige que les clés d'authentification soient sécurisées sur un système ou à un emplacement différent de celui des données.

Champ d'application de la gestion externe des clés

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 nommée 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.
- Vous pouvez utiliser ONTAP 9.10.1 depuis Azure Key Vault et Google Cloud KMS Pour protéger les clés NVE uniquement pour les serveurs vServer de données.

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.

Une liste de gestionnaires de clés externes validés est disponible dans le "Matrice d'interopérabilité NetApp (IMT)". Pour accéder à cette liste, saisissez le terme « gestionnaires de clés » dans la fonctionnalité de

recherche de la matrice d'interopérabilité.

Détails du support

Le tableau suivant présente les détails de la prise en charge de NVE :

Ressource ou fonctionnalité	Détails du support
Plateformes	Une fonctionnalité de déchargement AES-ni est requise. Consultez la page Hardware Universe (HWU) pour vérifier que NVE et NAE sont pris en charge pour votre plateforme.

Le cryptage	Depuis ONTAP 9.7, les volumes et les agrégats nouvellement créés sont chiffrés par défaut lorsque vous ajoutez une licence VE (Volume Encryption) et qu'un gestionnaire de clés intégré ou externe est configuré. Si vous devez créer un agrégat non chiffré, utilisez la commande suivante :
	
	`storage aggregate create -encrypt-with-aggr-key false`
	
	Si vous avez besoin de créer un volume de texte brut, utilisez la commande suivante :
	
	`volume create -encrypt false`
	
	Le chiffrement n'est pas activé par défaut lorsque :
	• La licence VE n'est pas installée.
	• Le gestionnaire de clés n'est pas configuré.
	• La plateforme ou le logiciel ne prend pas en charge le chiffrement.
	• Le chiffrement matériel est activé.

ONTAP	Toutes les implémentations de ONTAP. La prise en charge de ONTAP Cloud est disponible dans ONTAP 9.5 et versions ultérieures.
Périphériques	HDD, SSD, hybride, LUN de baie.
RAID	RAID0, RAID4, RAID-DP, RAID-TEC.
Volumes	Volumes de données et volumes root existants. Vous ne pouvez pas chiffrer les données d'un volume root SVM ou de volumes de métadonnées MetroCluster.

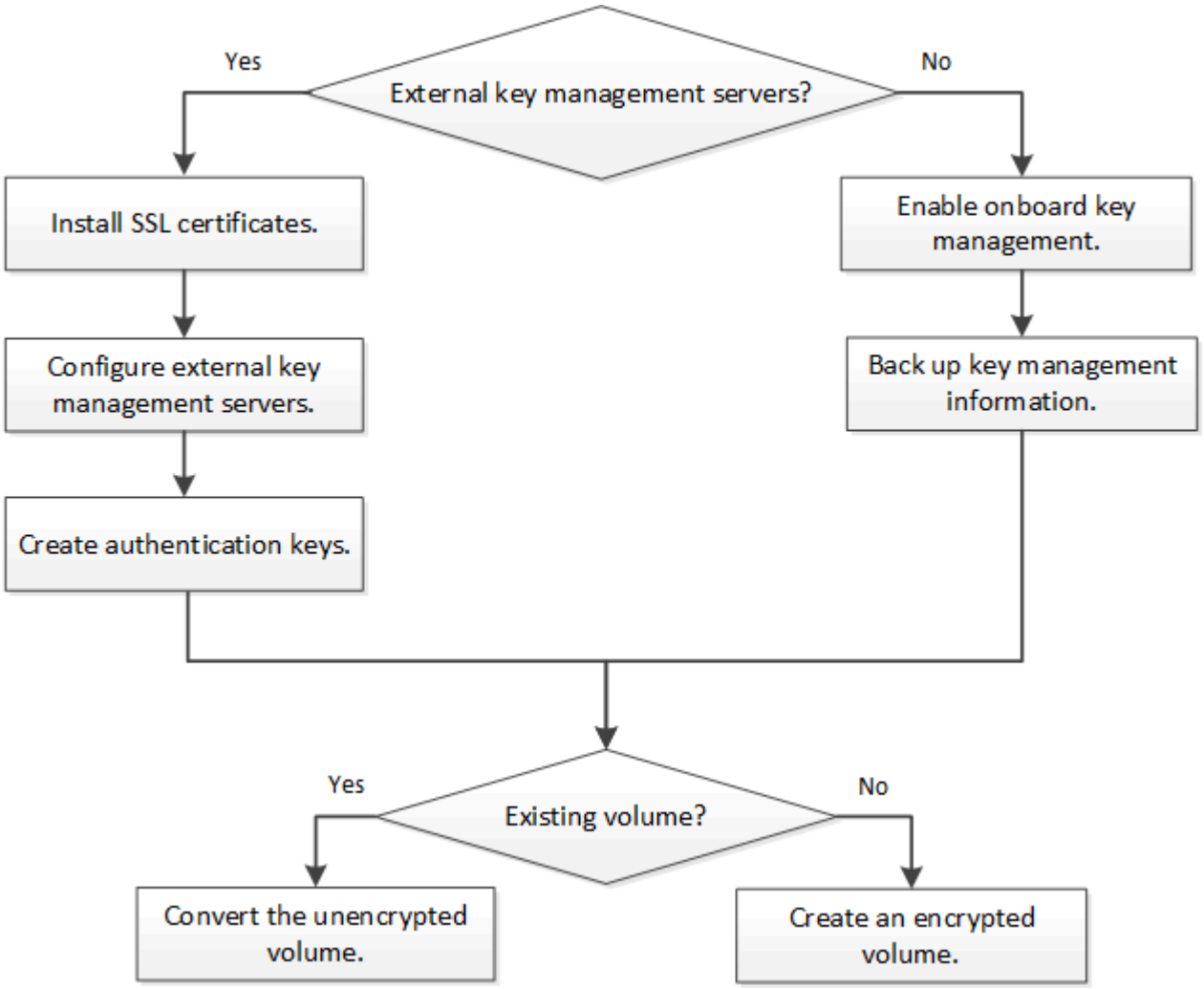
Chiffrement d'agrégat	Depuis la version ONTAP 9.6, NVE prend en charge le chiffrement au niveau des agrégats (NAE) : • Vous devez utiliser le chiffrement au niveau de l'agrégat pour procéder à la déduplication à la volée ou en arrière-plan au niveau de l'agrégat. • Vous ne pouvez pas reKey un volume de chiffrement au niveau de l'agrégat. • La suppression sécurisée n'est pas prise en charge sur les volumes de chiffrement au niveau des agrégats. • Outre les volumes de données, NAE prend en charge le chiffrement des volumes root du SVM et du volume de métadonnées MetroCluster. NAE ne prend pas en charge le chiffrement du volume racine.
Étendue des SVM	Depuis ONTAP 9.6, NVE prend en charge le périmètre des SVM pour la gestion externe des clés uniquement, et non pour le gestionnaire de clés intégré. MetroCluster est pris en charge à partir de ONTAP 9.8.
Efficacité du stockage	Déduplication, compression, compaction, FlexClone. Les clones utilisent la même clé que le parent, même après le fractionnement du clone. Vous êtes averti de ressaisir le clone fractionné.
La réplication	• Pour la réplication de volume, le volume de destination doit avoir été activé pour le chiffrement. Le chiffrement peut être configuré pour la source et non configuré pour la destination, et inversement. • Pour la réplication SVM, le volume de destination est automatiquement chiffré, sauf si le nœud de destination ne contient pas de nœud qui prend en charge le chiffrement de volume, dans ce cas la réplication réussit, mais le volume de destination n'est pas chiffré. • Dans le cas de configurations MetroCluster, chaque cluster extrait les clés de gestion externes des serveurs de clés configurés. Les clés OKM sont répliquées vers le site partenaire par le service de réplication de la configuration.
La conformité	Depuis ONTAP 9.2, SnapLock est pris en charge en mode conformité et entreprise pour les nouveaux volumes uniquement. Vous ne pouvez pas activer le chiffrement sur un volume SnapLock existant.
FlexGroups	FlexGroups est pris en charge à partir de ONTAP 9.2. Les agrégats de destination doivent être du même type que les agrégats source, au niveau des volumes ou de l'agrégat. ONTAP 9.5 prend en charge le renouvellement de clés des volumes FlexGroup sur place,
Transition depuis la version 7-mode	À partir de 7-mode transition Tool 3.3, vous pouvez utiliser l'interface de ligne de commandes de l'outil 7-mode transition Tool pour effectuer une transition basée sur les copies vers les volumes de destination NVE sur le système en cluster.

Informations associées

"FAQ : NetApp Volume Encryption et NetApp Aggregate Encryption"

Flux de travail NetApp Volume Encryption

Vous devez configurer les services de gestion des clés avant d'activer le chiffrement de volume. Vous pouvez activer le chiffrement sur un nouveau volume ou sur un volume existant.



Vous devez installer la licence VE et configurer les services de gestion des clés avant de pouvoir chiffrer les données avec NVE. Avant d'installer la licence, vous devriez "Déterminez si votre version de ONTAP prend en charge NVE".

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. Vous devez installer la licence pour pouvoir chiffrer les données avec NVE.

Ce dont vous avez besoin

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

Description de la tâche

Vous devriez avoir reçu la clé de licence VE de votre représentant commercial.

Étapes

1. Installez la licence VE pour un noeud :

   `system license add -license-code license_key`

   La commande suivante installe la licence avec la clé `AAAAAAAAAAAAAAAAAAAAAAAAAAAA`.

   ```
   cluster1::> system license add -license-code
   AAAAAAAAAAAAAAAAAAAAAAAAAAAA
   ```

2. Vérifiez que la licence est installée en affichant toutes les licences sur le cluster :

   `system license show`

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

   La commande suivante affiche toutes les licences sur `cluster1`:

   ```
   cluster1::> system license show
   ```

Le nom du paquet de licence VE est "VE".

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.

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.

Ce dont vous avez besoin

- 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 le certificat 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.

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.

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.

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.

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

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 :

   ```
   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 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 :

```
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 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.
```

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.

Ce dont vous avez besoin

- 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.

Description de la tâche

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

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
```

Gérez les clés avec Azure Key Vault ou Google Cloud KMS

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 déployée dans Azure ou Google Cloud Platform.

Les clés AKV et Cloud KMS peuvent être utilisées pour la protection "Clés NetApp Volume Encryption (NVE)" Uniquement pour les SVM de données.

La gestion des clés via AKV ou Cloud KMS peut être activée via l'interface de ligne de commande ou l'API REST de ONTAP.

Si vous utilisez AKV ou Cloud KMS, notez que, par défaut, une LIF de SVM de données est utilisée pour communiquer 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.

Prérequis

- Les nœuds du cluster ONTAP doivent prendre en charge NVE
- Licence VE (Volume Encryption) installée
- Licence MTEKM (Multi-tenant Encryption Key Management) installée
- Vous devez être un administrateur de cluster ou de SVM

Limites

- Les AKV et Cloud KMS ne sont pas disponibles pour NSE et NAE. "KMIP externes" peut être utilisé à la place
- Les AKV et Cloud KMS ne sont pas disponibles pour les configurations MetroCluster.
- Les AKV et Cloud KMS ne peuvent être configurés que sur les SVM de données

Activez la gestion externe des clés à l'aide de l'interface de ligne de commandes

L'activation de la gestion externe des clés dépend du gestionnaire de clés que vous utilisez. Si vous activez AKV dans un Cloud Volumes ONTAP, notez qu'il existe une procédure distincte. Choisissez l'onglet du gestionnaire de clés et de l'environnement qui correspond à vos besoins :

Azure

Activez le coffre-fort de clés Azure pour 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 la accessibilité du service n'est pas satisfaisante, établir la connectivité au service de gestion des clés AKV via LIF SVM de données.

Google Cloud

Activation du KMS cloud à l'aide de l'interface de ligne de commande pour ONTAP

1. Avant de commencer, vous devez obtenir la clé privée du fichier de clé de compte KMS Google Cloud 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. Définissez le niveau privilégié sur avancé
   `set -priv advanced`
3. Activation du KMS cloud sur le SVM
   `security key-manager external gcp enable -vserver *data_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 est impossible de créer de nouveaux volumes chiffrés pour le vServer de données du locataire tant que toutes les clés NVE du SVM de données ne sont pas migrées correctement.

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 auto-chiffré.

Ce dont vous avez besoin

- 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.

Description de la tâche

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

Si vous disposez d'une configuration MetroCluster, vous devez exécuter `security key-manager onboard enable` sur le cluster local, puis s'exécute `security key-manager onboard sync` sur le cluster distant, en utilisant la même phrase de passe sur chacun d'eux.

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. Pour plus d'informations sur les mises à jour du système, reportez-vous à la page de manuel « image du cluster ».

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.

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
   ```

```
       Vserver: cluster1
   Key Manager: onboard
          Node: node1

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

       Vserver: svm1
   Key Manager: onboard
          Node: node1
    Key Server: keyserver.svm1.com:5965

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
eb9f8311-e8d8-487e-9663-7642d7788a75     VEK       yes
    Key ID:
000000000000000002000000000004001cb18336f7c8223743d3e75c6a7726e00000000
00000000
9d09cbbf-0da9-4696-87a1-8e083d8261bb     VEK       yes
    Key ID:
000000000000000002000000000004064f2e1533356a470385274a9c3ffb97700000000
00000000

       Vserver: cluster1
   Key Manager: onboard
          Node: node2

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

```
        Vserver: svm1
    Key Manager: onboard
           Node: node2
     Key Server: keyserver.svm1.com:5965

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
eb9f8311-e8d8-487e-9663-7642d7788a75  VEK       yes
    Key ID:
000000000000000002000000000004001cb18336f7c8223743d3e75c6a7726e00000000
00000000
9d09cbbf-0da9-4696-87a1-8e083d8261bb  VEK       yes
    Key ID:
000000000000000002000000000004064f2e1533356a470385274a9c3ffb97700000000
00000000
```

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.

Toutes les informations de gestion des clés sont automatiquement sauvegardées dans la base de données répliquée (RDB) pour le cluster. Vous devez également sauvegarder les informations manuellement pour les utiliser en cas d'incident.

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.

Ce dont vous avez besoin

- Si vous utilisez NSE avec un serveur de gestion externe des clés (KMIP), vous devez avoir supprimé la base de données de gestionnaire de clés externe.

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

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Vous devez configurer l'environnement MetroCluster avant de configurer le gestionnaire de clés intégré.

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. Vous pouvez utiliser ONTAP 9.4 à partir de `-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.

Étapes

1. Lancez la configuration du gestionnaire de clés :

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

   Vous pouvez utiliser ONTAP 9.4 à partir de `-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 key show`

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

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

Node: node1
Key Store: onboard
Key ID                                                               Used By
-------------------------------------------------------------------------
--------
000000000000000002000000000000100598517 42AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000000100 8C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                               Used By
-------------------------------------------------------------------------
--------
000000000000000002000000000000100598517 42AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000000100 8C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

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.

Toutes les informations de gestion des clés sont automatiquement sauvegardées dans la base de données répliquée (RDB) pour le cluster.

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. Vous pouvez utiliser ONTAP 9.4 à partir de `-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.

Chiffrement des données de volume avec NVE

Chiffrement des données de volume avec NVE

Depuis ONTAP 9.7, le chiffrement de l'agrégat et du volume est activé par défaut lorsque vous disposez de la licence VE et de la gestion intégrée ou externe des clés. Pour ONTAP 9.6 et version antérieure, vous pouvez activer le chiffrement sur un nouveau volume ou sur un volume existant. Vous devez avoir installé la licence VE et activé la gestion des clés avant de pouvoir activer le chiffrement de volume. NVE est conforme à la norme FIPS-140-2 de niveau 1.

Chiffrement au niveau de l'agrégat avec licence VE

Depuis ONTAP 9.7, les agrégats et volumes nouvellement créés sont chiffrés par défaut lorsque vous disposez de la licence VE et d'une gestion des clés intégrée ou externe. Depuis ONTAP 9.6, vous pouvez utiliser le chiffrement au niveau de l'agrégat pour

attribuer des clés à l'agrégat contenant afin de chiffrer les volumes.

Ce dont vous avez besoin

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

Description de la tâche

Vous devez utiliser le chiffrement au niveau de l'agrégat pour procéder à la déduplication à la volée ou en arrière-plan au niveau de l'agrégat. NVE ne prend cependant pas en charge la déduplication au niveau de l'agrégat.

Un agrégat activé pour le chiffrement au niveau de l'agrégat est appelé agrégat *NAE* (pour le chiffrement d'agrégat NetApp). Tous les volumes d'un agrégat NAE doivent être chiffrés avec un chiffrement NAE ou NVE. Grâce au chiffrement au niveau des agrégats, les volumes que vous créez dans l'agrégat sont chiffrés avec un chiffrement NAE par défaut. Vous pouvez remplacer le par défaut pour utiliser le chiffrement NVE.

Les volumes en texte brut ne sont pas pris en charge dans les agrégats NAE.

Étapes

1. Activer ou désactiver le chiffrement au niveau des agrégats :

Pour…	Utilisez cette commande…
Créez un agrégat NAE avec ONTAP 9.7 ou version ultérieure	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`*
Créez un agrégat NAE avec ONTAP 9.6	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
Conversion d'un agrégat non-NAE en agrégat NAE	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
Conversion d'un agrégat NAE en agrégat non-NAE	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key false`

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

La commande suivante active le chiffrement au niveau de l'agrégat sur `aggr1`:

- ONTAP 9.7 ou version ultérieure :

```
cluster1::> storage aggregate create -aggregate aggr1
```

- ONTAP 9.6 ou version antérieure :

```
cluster1::> storage aggregate create -aggregate aggr1 -encrypt-with
-aggr-key true
```

2. Vérifier que l'agrégat est activé pour le chiffrement :

   `storage aggregate show -fields encrypt-with-aggr-key`

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

   La commande suivante vérifie que `aggr1` est activé pour le chiffrement :

```
cluster1::> storage aggregate show -fields encrypt-with-aggr-key
aggregate            encrypt-aggr-key
-------------------- ----------------
aggr0_vsim4          false
aggr1                true
2 entries were displayed.
```

Une fois que vous avez terminé

Exécutez le `volume create` commande permettant de créer les volumes chiffrés.

Si vous utilisez un serveur KMIP pour stocker les clés de cryptage d'un nœud, ONTAP « transfère » automatiquement une clé de cryptage vers le serveur lorsque vous chiffrez un volume.

Activer le chiffrement sur un nouveau volume

Vous pouvez utiliser le `volume create` commande permettant d'activer le chiffrement sur un nouveau volume.

Description de la tâche

Vous pouvez chiffrer les volumes à l'aide de NetApp Volume Encryption (NVE) et, à partir de ONTAP 9.6, NetApp Aggregate Encryption (NAE). Pour en savoir plus sur NAE et NVE, consultez le présentation du chiffrement de volume.

La procédure d'activation du chiffrement sur un nouveau volume dans ONTAP varie en fonction de la version de ONTAP que vous utilisez et de votre configuration spécifique :

- À partir de ONTAP 9.4, si vous l'activez `cc-mode` Lorsque vous configurez le gestionnaire de clés intégré, les volumes que vous créez avec le `volume create` la commande est automatiquement chiffrée, que vous spécifiez ou non `-encrypt true`.
- Dans ONTAP 9.6 et les versions antérieures, vous devez utiliser `-encrypt true` avec `volume create` commandes permettant d'activer le chiffrement (à condition que vous n'ayez pas activé `cc-mode`).
- Si vous voulez créer un volume NAE dans ONTAP 9.6, vous devez activer NAE au niveau des agrégats. Reportez-vous à la section Activation du chiffrement au niveau de l'agrégat avec la licence VE pour plus de détails sur cette tâche.
- Depuis ONTAP 9.7, les volumes nouvellement créés sont cryptés par défaut lorsque vous disposez de la

licence VE et de la gestion intégrée ou externe des clés. Par défaut, les nouveaux volumes créés dans un agrégat NAE seront de type NAE plutôt que NVE.

- Dans ONTAP 9.7 et versions ultérieures, si vous ajoutez `-encrypt true` à la `volume create` Commande de création d'un volume dans un agrégat NAE, au lieu de NAE pour le volume le chiffrement NVE. Tous les volumes d'un agrégat NAE doivent être chiffrés avec NVE ou NAE.

Les volumes en texte brut ne sont pas pris en charge dans les agrégats NAE.

Étapes

1. Créez un nouveau volume et spécifiez si le chiffrement est activé sur le volume. Si le nouveau volume se trouve dans un agrégat NAE, le volume en est par défaut un volume NAE :

Pour créer…	Utilisez cette commande…
Volume NAE	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`*
Un volume NVE	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt true` + Dans les versions ONTAP 9.6 et antérieures, où NAE n'est pas pris en charge, `-encrypt true` Spécifie que le volume doit être chiffré avec NVE. Dans ONTAP 9.7 et versions ultérieures, où les volumes sont créés dans des agrégats NAE, `-encrypt true` Remplace le type de chiffrement par défaut de NAE pour créer un volume NVE.
Volume de texte brut	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt false`

Pour connaître la syntaxe complète de la commande, reportez-vous à la page de référence de la commande LINK:https://docs.netapp.com/us-en/ontap-cli-9121/volume-create.html[`volume create`^].

2. Vérifiez que les volumes sont activés pour le chiffrement :

```
volume show -is-encrypted true
```

Pour connaître la syntaxe complète de la commande, reportez-vous au "référence de commande".

Résultat

Si vous utilisez un serveur KMIP pour stocker les clés de chiffrement d'un nœud, ONTAP « transmet automatiquement » une clé de chiffrement au serveur lorsque vous chiffrez un volume.

Activez le chiffrement sur un volume existant à l'aide de la commande Volume Encryption conversion start

Vous pouvez utiliser ONTAP 9.3 à partir de `volume encryption conversion start` commande permettant de chiffrer un volume existant « à la place », sans avoir à déplacer le volume vers un autre emplacement.

Description de la tâche

Une fois que vous avez démarré une opération de conversion, elle doit être terminée. Si vous rencontrez un problème de performances pendant l'opération, vous pouvez exécuter le `volume encryption conversion pause` commande pour mettre l'opération en pause, et le `volume encryption conversion resume` commande pour reprendre l'opération.

> Vous ne pouvez pas utiliser `volume encryption conversion start` Pour convertir un volume SnapLock.

Étapes

1. Activer le chiffrement sur un volume existant :

   `volume encryption conversion start -vserver SVM_name -volume volume_name`

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

   La commande suivante permet le chiffrement sur le volume existant `vol1`:

   ```
   cluster1::> volume encryption conversion start -vserver vs1 -volume vol1
   ```

   Le système crée une clé de chiffrement pour le volume. Les données du volume sont chiffrées.

2. Vérifiez l'état de l'opération de conversion :

   `volume encryption conversion show`

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

   La commande suivante affiche le statut de l'opération de conversion :

   ```
   cluster1::> volume encryption conversion show

   Vserver   Volume   Start Time           Status
   -------   ------   ------------------   --------------------------
   vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
   ```

3. Une fois l'opération de conversion terminée, vérifiez que le volume est activé pour le chiffrement :

   `volume show -is-encrypted true`

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

   La commande suivante affiche les volumes chiffrés sur `cluster1`:

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Résultat

Si vous utilisez un serveur KMIP pour stocker les clés de cryptage d'un nœud, ONTAP « transfère » automatiquement une clé de cryptage vers le serveur lorsque vous chiffrez un volume.

Activez le chiffrement sur un volume existant à l'aide de la commande volume Move start

Vous pouvez utiliser le `volume move start` commande permettant d'activer le chiffrement en déplaçant un volume existant. Vous devez utiliser `volume move start` Dans ONTAP 9.2 et versions antérieures. Vous pouvez utiliser le même agrégat ou un autre agrégat.

Ce dont vous avez besoin

Vous devez être un administrateur de cluster pour effectuer cette tâche, ou un administrateur de SVM à qui l'administrateur du cluster a délégué des pouvoirs.

"Délégation d'autorité pour exécuter la commande de déplacement de volume"

Description de la tâche

Vous pouvez utiliser ONTAP 9.8 depuis `volume move start` Pour activer le chiffrement sur un volume SnapLock ou FlexGroup.

Depuis ONTAP 9.4, si vous activez « cc-mode » lors de la configuration du gestionnaire de clés intégré, les volumes que vous créez avec le système `volume move start` la commande est automatiquement chiffrée. Vous n'avez pas besoin de spécifier `-encrypt-destination true`.

Depuis ONTAP 9.6, il est possible d'utiliser le chiffrement au niveau de l'agrégat pour attribuer des clés à l'agrégat contenant afin de déplacer les volumes. Un volume chiffré avec une clé unique est appelé un *volume NVE*. Un volume chiffré avec une clé au niveau de l'agrégat est appelé un volume NAE_ (pour le chiffrement d'agrégat NetApp). Les volumes en texte brut ne sont pas pris en charge dans les agrégats NAE.

Étapes

1. Déplacez un volume existant et spécifiez si le chiffrement est activé sur le volume :

Pour convertir…	Utilisez cette commande…
Volume en texte brut vers un volume NVE	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination true`

Un volume NVE ou en texte clair vers un volume NAE (en supposant que le chiffrement au niveau de l'agrégat est activé sur la destination)	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key true`
Un volume NAE vers un volume NVE	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key false`
Volume NAE en volume en texte brut	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false -encrypt-with-aggr-key false`
Un volume NVE vers un volume en texte brut	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false`

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

La commande suivante convertit un volume en texte brut nommé `vol1` Vers un volume NVE :

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-destination true
```

En supposant que le chiffrement au niveau de l'agrégat soit activé sur la destination, la commande suivante convertit un volume NVE ou en texte brut nommé `vol1` Vers un volume NAE :

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-with-aggr-key true
```

La commande suivante convertit un volume NAE nommé `vol2` Vers un volume NVE :

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-with-aggr-key false
```

La commande suivante convertit un volume NAE nommé `vol2` vers un volume en texte clair :

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false -encrypt-with-aggr-key false
```

La commande suivante convertit un volume NVE nommé `vol2` vers un volume en texte clair :

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false
```

2. Afficher le type de chiffrement des volumes du cluster :

   `volume show -fields encryption-type none|volume|aggregate`

   Le `encryption-type` Ce champ est disponible dans ONTAP 9.6 et versions ultérieures.

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

   La commande suivante affiche le type de cryptage des volumes dans `cluster2`:

```
cluster2::> volume show -fields encryption-type

vserver  volume  encryption-type
-------  ------  ---------------
vs1      vol1    none
vs2      vol2    volume
vs3      vol3    aggregate
```

3. Vérifiez que les volumes sont activés pour le chiffrement :

   `volume show -is-encrypted true`

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

   La commande suivante affiche les volumes chiffrés sur `cluster2`:

```
cluster2::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Résultat

Si vous utilisez un serveur KMIP pour stocker les clés de cryptage d'un nœud, ONTAP « transfère » automatiquement une clé de cryptage vers le serveur lorsque vous chiffrez un volume.

Activer le chiffrement de volume racine de nœud

Depuis ONTAP 9.8, vous pouvez utiliser NetApp Volume Encryption pour protéger le volume racine de votre nœud.

Ce dont vous avez besoin

- Votre système doit utiliser une configuration haute disponibilité.

  Le chiffrement de volume racine n'est pas pris en charge dans les configurations à un seul nœud.

- Le volume racine du nœud doit déjà être créé.
- Votre système doit disposer d'un gestionnaire de clés intégré ou d'un serveur de gestion des clés externe à l'aide du protocole KMIP (Key Management Interoperability Protocol).

Description de la tâche

Cette procédure s'applique au volume racine du nœud. Elle ne s'applique pas aux volumes root du SVM. Les volumes root du SVM peuvent être protégés par le chiffrement au niveau des agrégats.

Une fois le chiffrement du volume racine démarré, il doit être terminé. Vous ne pouvez pas interrompre l'opération. Une fois le cryptage terminé, vous ne pouvez pas attribuer de nouvelle clé au volume racine et vous ne pouvez pas effectuer de suppression sécurisée.

Étapes

1. Chiffrer le volume root :

   ```
   volume encryption conversion start -vserver SVM_name -volume root_vol_name
   ```

2. Vérifiez l'état de l'opération de conversion :

   ```
   volume encryption conversion show
   ```

3. Une fois l'opération de conversion terminée, vérifiez que le volume est crypté :

   ```
   volume show -fields
   ```

   Voici un exemple de sortie pour un volume chiffré.

   ```
   ::> volume show -vserver xyz  -volume vol0 -fields is-encrypted
   vserver    volume is-encrypted
   ---------- ------ ------------
   xyz        vol0   true
   ```