Gestion du chiffrement via l'interface de ligne de commandes

ONTAP 9

NetApp
September 12, 2024

Sommaire

Gestion du chiffrement via l'interface de ligne de commandes

Présentation du chiffrement NetApp

NetApp propose des technologies de cryptage logicielles et matérielles qui permettent de garantir que les données au repos ne peuvent pas être lues si le support de stockage est requalifié, perdu ou volé.

- Le chiffrement logiciel associé à NetApp Volume Encryption (NVE) prend en charge le chiffrement des données sur un volume à la fois
- Le chiffrement matériel utilisant NetApp Storage Encryption (NSE) prend en charge le chiffrement de disque intégral (FDE) des données au moment de leur écriture.

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

Avec NVE, les métadonnées et les données (y compris les copies Snapshot) 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 (OKM) sert les clés pour les 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. La licence VE est incluse avec "ONTAP One". 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. À partir de ONTAP 9.14.1, vous pouvez Activez NVE sur les volumes root du SVM existant.

> 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.

Lorsque NVE est activé, 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 Protection des clés NVE uniquement pour les SVM de données. Ce dernier est disponible pour le KMS d'AWS à partir de la version 9.12.0.

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 trouver cette liste, entrez le terme « gestionnaires de clés » dans la fonction de recherche de l'IMT.

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 SVM existants. Il n'est pas possible de chiffrer des données sur des volumes de métadonnées MetroCluster. Dans les versions de ONTAP antérieures à 9.14.1, vous ne pouvez pas chiffrer les données sur le volume racine du SVM avec NVE. À partir de ONTAP 9.14.1, ONTAP prend en charge NVE sur les volumes root du SVM.
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 devez effectuer une `volume move` sur un clone divisé, après quoi le clone divisé aura une clé différente.
La réplication	• Pour la réplication de volume, les volumes source et de destination peuvent avoir des paramètres de chiffrement différents. 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.

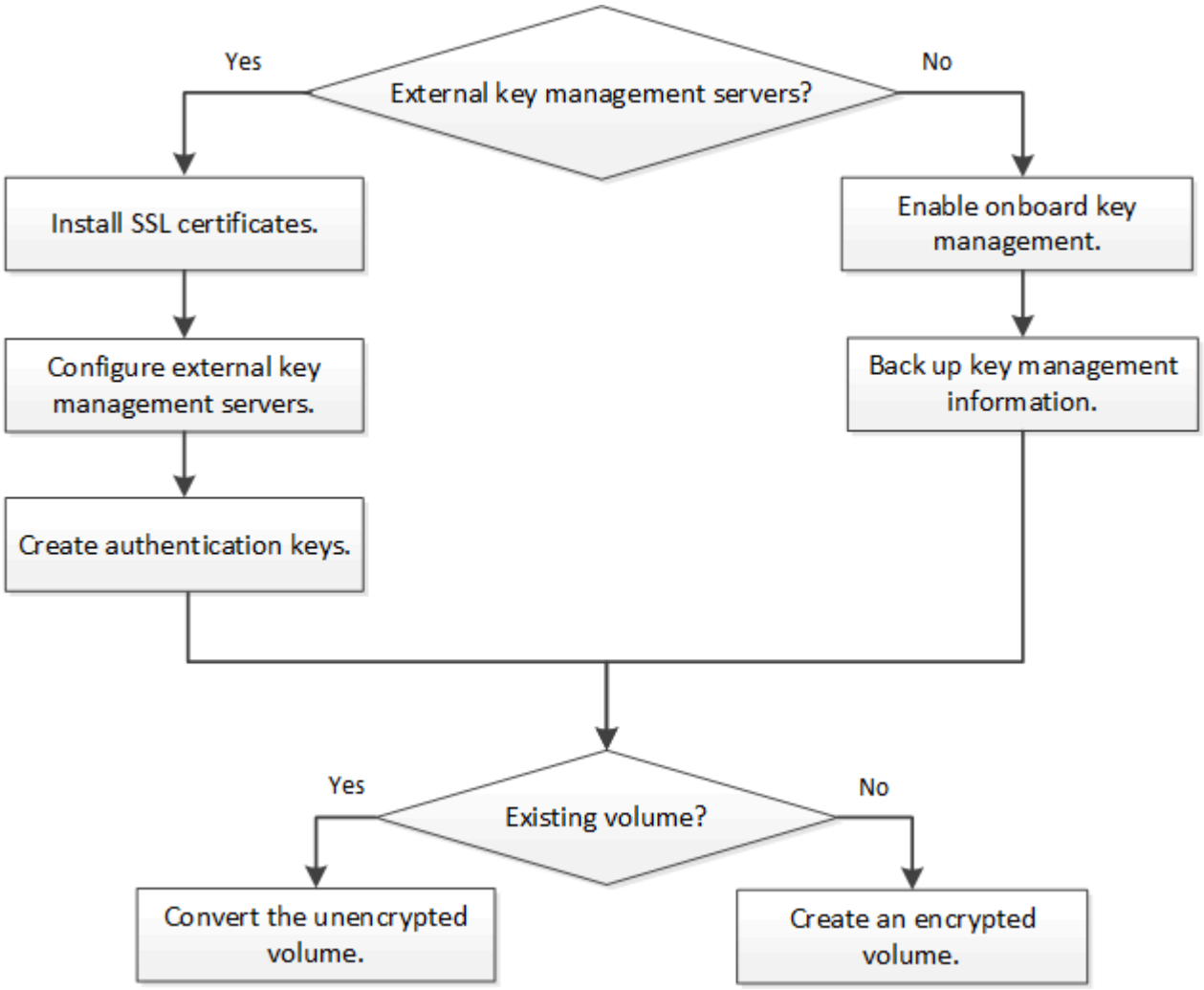
FlexGroups	FlexGroups est pris en charge à partir de ONTAP 9.2. Les agrégats de destination doivent être du même type que les agrégats source, au niveau des volumes ou de l'agrégat. ONTAP 9.5 prend en charge le renouvellement de clés des volumes FlexGroup sur place,
Transition depuis la version 7-mode	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 configurez les services de gestion des clés avant de chiffrer les données avec NVE. Avant d'installer la licence, vous devez "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. Cette licence est requise avant de pouvoir chiffrer les données avec NVE. Il est inclus avec "ONTAP One".

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

Avant de commencer

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

Étapes

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

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

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

Configurez la gestion externe des clés

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

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

Modifier un gestionnaire de clés externe existant

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

Étapes

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

Portée	Navigation	Étape de départ

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

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

Supprimez un gestionnaire de clés externe

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

Étapes

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

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

Migration des clés entre les gestionnaires de clés

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

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

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 :

```
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.
   ```

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
   ```

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

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

4. Ajoutez un serveur KMIP supplémentaire pour la redondance :

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

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

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

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

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

   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 KMV sur un SVM ONTAP

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

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:
00000000000000000200000000000100056178fc6ace6d91472df8a9286daacc00000000
00000000

node1                                 NSE-AK   AES-256      true

    Key ID:
00000000000000000200000000000100df1689a148fdfbf9c2b198ef974d0baa00000000
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 :

```
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
-----------------------------------------------------------------------
--------
000000000000000002000000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                                   Used By
-----------------------------------------------------------------------
--------
000000000000000002000000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

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.

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 la version ONTAP 9.7, les agrégats et volumes nouvellement créés sont chiffrés par défaut lorsque vous disposez de "Licence VE"et de la 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.

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.

Avant de commencer

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

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 la version ONTAP 9.7, les nouveaux volumes créés sont chiffrés par défaut lorsque vous disposez de "Licence VE"et de la gestion des clés intégrée ou externe. 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 obtenir 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/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 ONTAP".

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.

=
:allow-uri-read:

Activez le chiffrement sur un volume existant

Vous pouvez utiliser le `volume move start` ou le `volume encryption conversion start` commande permettant d'activer le chiffrement sur un volume existant.

Description de la tâche

- 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. Vous pouvez également utiliser le `volume move start` commande.
- Pour ONTAP 9.2 et les versions antérieures, vous pouvez utiliser uniquement le `volume move start` commande permettant d'activer le chiffrement en déplaçant un volume existant.

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.

Une fois que vous avez lancé 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 la syntaxe complète de la commande, reportez-vous à la page man de la commande.

La commande suivante active le chiffrement sur un 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 la syntaxe complète de la commande, reportez-vous à la page man de la commande.

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

   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.

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 *volume NVE* (ce qui signifie qu'il utilise le chiffrement de volume NetApp). 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.
- À partir de ONTAP 9.14.1, vous pouvez chiffrer un volume root SVM avec NVE. Pour plus d'informations, voir Configurer le chiffrement de volume NetApp sur un volume root SVM.

Avant de commencer

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"

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

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

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

   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 chiffrement d'un nœud, ONTAP transmet automatiquement une clé de chiffrement au serveur lorsque vous chiffrez un volume.

Configurer le chiffrement de volume NetApp sur un volume root SVM

À partir de la version ONTAP 9.14.1, vous pouvez activer NetApp Volume Encryption (NVE) sur un volume racine de machine virtuelle de stockage (SVM). Avec NVE, le volume racine est chiffré avec une clé unique, pour renforcer la sécurité au niveau du SVM.

Description de la tâche

NVE sur un volume root SVM ne peut être activé qu'une fois le SVM créé.

Avant de commencer

- Le volume racine du SVM ne doit pas se trouver sur un agrégat chiffré avec le chiffrement d'agrégat NetApp (NAE).
- Vous devez avoir activé le chiffrement avec Onboard Key Manager ou un gestionnaire de clés externe.
- Vous devez exécuter ONTAP 9.14.1 ou une version ultérieure.
- Pour migrer un SVM contenant un volume racine chiffré avec NVE, vous devez convertir le volume racine du SVM en volume texte brut une fois la migration terminée, puis re-chiffrer le volume racine du SVM.
  - Si l'agrégat de destination de la migration du SVM utilise NAE, le volume racine hérite de NAE par défaut.

- Si la SVM est dans une relation de SVM DR :
  - Les paramètres de chiffrement d'un SVM en miroir ne sont pas copiés vers la destination. Si vous activez NVE sur la source ou la destination, vous devez activer NVE séparément sur le volume racine du SVM en miroir.
  - Si tous les agrégats du cluster de destination utilisent NAE, le volume racine du SVM utilisera NAE.

Étapes

Vous pouvez activer NVE sur un volume root SVM via l'interface de ligne de commandes ONTAP ou System Manager.

CLI

Vous pouvez activer NVE sur le volume racine du SVM sans déplacement ou en déplaçant le volume entre les agrégats.

Chiffrez le volume racine sur place

1. Convertir le volume root en volume chiffré :

   ```
   volume encryption conversion start -vserver svm_name -volume volume
   ```

2. Confirmez que le chiffrement a réussi. Le `volume show -encryption-type volume` Affiche la liste de tous les volumes qui utilisent NVE.

Chiffrer le volume root du SVM en le déplaçant

1. Lancer un déplacement de volume :

   ```
   volume move start -vserver svm_name -volume volume -destination-aggregate
   aggregate -encrypt-with-aggr-key false -encrypt-destination true
   ```

   Pour plus d'informations sur `volume move`, voir Déplacer un volume.

2. Confirmez le `volume move` l'opération a réussi avec le `volume move show` commande. Le `volume show -encryption-type volume` Affiche la liste de tous les volumes qui utilisent NVE.

System Manager

1. Accédez à **stockage** > **volumes**.
2. À côté du nom du volume root du SVM à crypter, sélectionner ⋮ puis **Edit**.
3. Sous l'en-tête **stockage et optimisation**, sélectionnez **Activer le cryptage**.
4. Sélectionnez **Enregistrer**.

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.

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 des SVM peuvent être protégés via le chiffrement au niveau des agrégats et À partir de ONTAP 9.14.1, NVE.

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.

Avant de commencer

- Votre système doit utiliser une configuration haute disponibilité.
- 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).

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
   ```

Configuration du chiffrement matériel NetApp

Configuration de la présentation de NetApp Hardware-based Encryption

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

Présentation du cryptage matériel NetApp

Un nœud s'authentifie auprès d'un disque auto-chiffré à l'aide d'une clé d'authentification extraite d'un serveur

de gestion externe des clés ou d'un gestionnaire de clés intégré :

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

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

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

> Si une paire haute disponibilité utilise des disques avec cryptage SAS ou NVMe (SED, NSE, FIPS), vous devez suivre les instructions de la rubrique Retour d'un lecteur FIPS ou SED en mode non protégé Pour tous les disques de la paire HA avant d'initialiser le système (options de démarrage 4 ou 9). Si vous ne le faites pas, vous risquez de subir des pertes de données si les disques sont requalifiés.

Types de disques à autocryptage pris en charge

Deux types de disques à autocryptage sont pris en charge :

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

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

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

Quand utiliser la gestion externe des clés

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

- La stratégie de votre entreprise nécessite une solution de gestion des clés qui utilise un module cryptographique FIPS 140-2 de niveau 2 (ou supérieur).

- Vous avez besoin d'une solution à plusieurs clusters et d'une gestion centralisée des clés de chiffrement.
- Votre entreprise exige que les clés d'authentification soient sécurisées sur un système ou à un emplacement différent de celui des données.

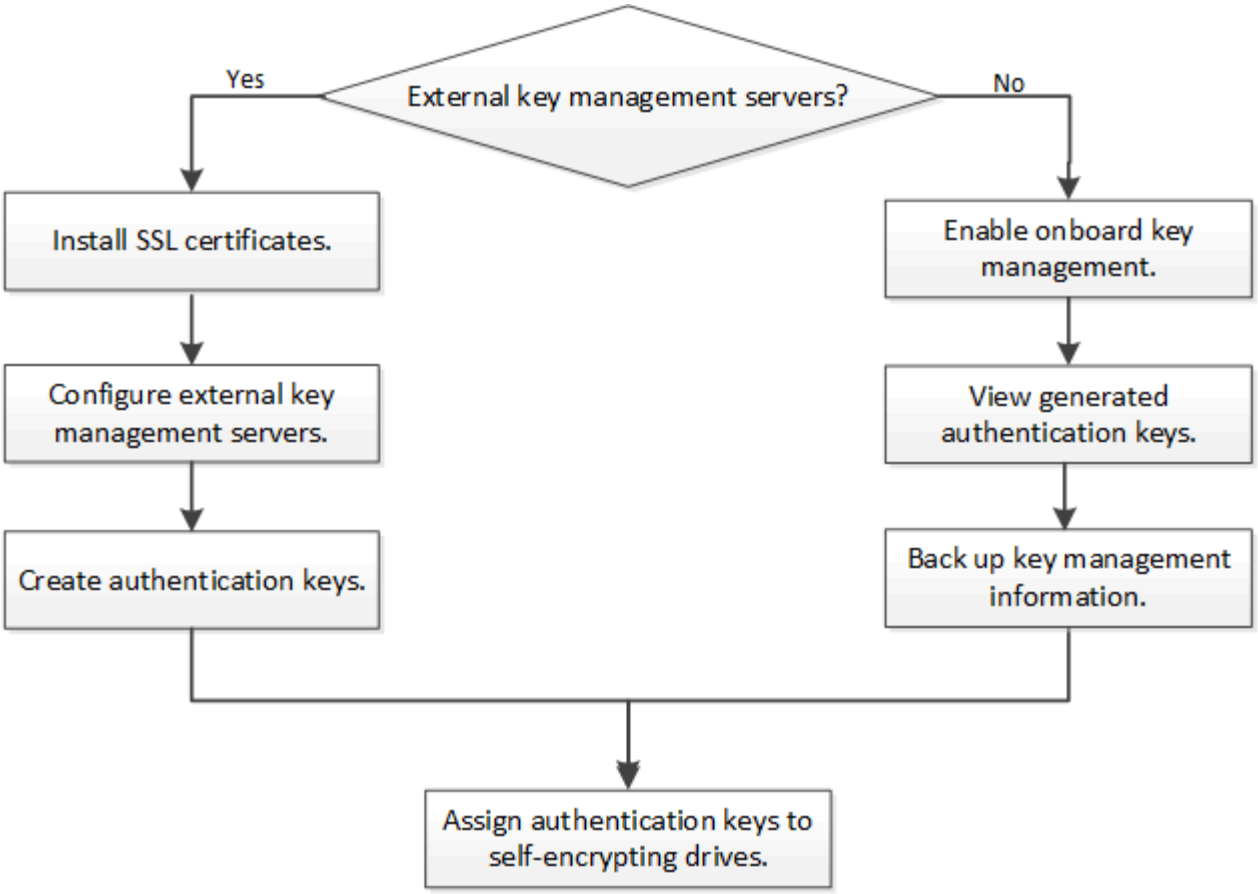
Détails du support

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

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

Flux de production de cryptage matériel

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



Informations associées

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

Configurez la gestion externe des clés

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) peut être implémenté avec le gestionnaire de clés intégré dans ONTAP 9.1 et les versions ultérieures. Dans ONTAP 9.3 et versions ultérieures, NVE peut être implémenté avec une gestion des clés externe (KMIP) et un gestionnaire de clés intégré. 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.

Collectez des informations réseau dans ONTAP 9.2 et versions antérieures

Si vous utilisez ONTAP 9.2 ou une version antérieure, vous devez remplir la fiche de configuration du réseau avant d'activer la gestion externe des clés.

> Depuis ONTAP 9.3, le système détecte automatiquement toutes les informations réseau nécessaires.

Élément	Remarques	Valeur
Nom de l'interface réseau de gestion des clés		
Adresse IP de l'interface réseau de gestion des clés	Adresse IP de la LIF de node management, au format IPv4 ou IPv6	
Longueur du préfixe réseau IPv6 de gestion des clés	Si vous utilisez IPv6, la longueur du préfixe réseau IPv6	
Masque de sous-réseau de l'interface réseau de gestion des clés		
Adresse IP de la passerelle d'interface réseau de gestion des clés		
Adresse IPv6 pour l'interface réseau du cluster	Requis uniquement si vous utilisez IPv6 pour l'interface réseau de gestion des clés	
Numéro de port pour chaque serveur KMIP	Facultatif. Le numéro de port doit être le même pour tous les serveurs KMIP. Si vous ne fournissez pas de numéro de port, il prend par défaut le port 5696, qui est le port attribué par Internet Numbers Authority (IANA) pour KMIP.	
Nom de la balise clé	Facultatif. Le nom de la balise clé est utilisé pour identifier toutes les clés appartenant à un nœud. Le nom de la balise par défaut est le nom du nœud.	

Informations associées

"Rapport technique NetApp 3954 : exigences et procédures de préinstallation pour IBM Tivoli Lifetime Key Manager pour NetApp Storage Encryption"

"Rapport technique NetApp 4074 : exigences et procédures de préinstallation pour NetApp Storage Encryption pour SafeNet KeySecure"

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
   ```

Activation de la gestion externe des clés dans ONTAP 9.6 et versions ultérieures (basée sur le matériel)

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

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

Avant de commencer

- Les certificats client SSL KMIP et serveur doivent avoir été installés.
- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- 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 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. Vous pouvez exécuter le `security key-manager external modify` commande pour modifier la configuration de la gestion externe des clés. Pour connaître la syntaxe complète des commandes, consultez les pages de manuels.
   > - 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 -key-servers
   ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
   -client-cert AdminVserverClientCert -server-ca-certs
   AdminVserverServerCaCert
   ```

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

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

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

6 entries were displayed.
```

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.

Configurez les serveurs de clés externes en cluster

À partir de ONTAP 9.11.1, il est possible de configurer la connectivité aux serveurs de gestion externe des clés en cluster sur un SVM. Avec des serveurs de clés en cluster, vous pouvez désigner des serveurs de clés principaux et secondaires sur une SVM. Lors

de l'enregistrement des clés, ONTAP essaie d'abord d'accéder à un serveur de clés principal avant de tenter d'accéder aux serveurs secondaires de manière séquentielle jusqu'à ce que l'opération s'effectue correctement, ce qui évite la duplication des clés.

Les serveurs de clés externes peuvent être utilisés pour les clés NSE, NVE, NAE et SED. Un SVM peut prendre en charge jusqu'à quatre principaux serveurs KMIP externes. Chaque serveur principal peut prendre en charge jusqu'à trois serveurs de clés secondaires.

Avant de commencer

- "La gestion des clés KMIP doit être activée pour le SVM".
- Ce processus prend uniquement en charge les serveurs de clés qui utilisent KMIP. Pour obtenir la liste des serveurs de clés pris en charge, reportez-vous à la "Matrice d'interopérabilité NetApp".
- Tous les nœuds du cluster doivent exécuter ONTAP 9.11.1 ou une version ultérieure.
- L'ordre des serveurs répertorie les arguments dans `-secondary-key-servers` Paramètre correspond à l'ordre d'accès des serveurs de gestion externe des clés (KMIP).

Créer un serveur de clés mis en cluster

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

Ajout de serveurs de clés primaires et secondaires à un SVM

1. Vérifier qu'aucune gestion des clés n'a été activée pour le cluster :
   `security key-manager external show -vserver` *`svm_name`*
   Si le SVM possède déjà le maximum de quatre serveurs de clés principaux activés, vous devez supprimer l'un des serveurs de clés principaux existants avant d'en ajouter un nouveau.
2. Activez le gestionnaire de clés principal :
   `security key-manager external enable -vserver` *`svm_name`* `-key-servers` *`server_ip`* `-client-cert` *`client_cert_name`* `-server-ca-certs` *`server_ca_cert_names`*
3. Modifiez le serveur de clés principal pour ajouter des serveurs de clés secondaires. Le `-secondary-key-servers` paramètre accepte une liste séparée par des virgules de trois serveurs de clés au maximum.
   `security key-manager external modify-server -vserver` *`svm_name`* `-key-servers` *`primary_key_server`* `-secondary-key-servers` *`list_of_key_servers`*

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

1. Modifiez le serveur de clés principal pour ajouter des serveurs de clés secondaires. Le `-secondary-key-servers` paramètre accepte une liste séparée par des virgules de trois serveurs de clés au maximum.
   `security key-manager external modify-server -vserver` *`svm_name`* `-key-servers` *`primary_key_server`* `-secondary-key-servers` *`list_of_key_servers`*
   Pour plus d'informations sur les serveurs de clés secondaires, reportez-vous à la section [mod-secondary].

Modifier les serveurs de clés en cluster

Vous pouvez modifier les clusters de serveurs de clés externes en modifiant l'état (principal ou secondaire) de serveurs de clés spécifiques, en ajoutant et en supprimant des serveurs de clés secondaires ou en modifiant

l'ordre d'accès des serveurs de clés secondaires.

Conversion des serveurs de clés principaux et secondaires

Pour convertir un serveur de clés principal en serveur de clés secondaire, vous devez d'abord le supprimer de la SVM avec le `security key-manager external remove-servers` commande.

Pour convertir un serveur de clés secondaire en serveur de clés principal, vous devez d'abord supprimer le serveur de clés secondaire de son serveur de clés principal existant. Voir [mod-secondary]. Si vous convertissez un serveur de clés secondaire en serveur principal lors de la suppression d'une clé existante, toute tentative d'ajout d'un nouveau serveur avant la suppression et la conversion peut entraîner la duplication des clés.

Modifier les serveurs de clés secondaires

Les serveurs de clés secondaires sont gérés à l'aide du `-secondary-key-servers` paramètre du `security key-manager external modify-server` commande. Le `-secondary-key-servers` le paramètre accepte une liste séparée par des virgules. L'ordre spécifié des serveurs de clés secondaires dans la liste détermine la séquence d'accès des serveurs de clés secondaires. L'ordre d'accès peut être modifié en exécutant la commande `security key-manager external modify-server` les serveurs de clés secondaires étant entrés dans une séquence différente.

Pour supprimer un serveur de clés secondaire, le `-secondary-key-servers` les arguments doivent inclure les serveurs clés que vous voulez conserver lors de l'omission de celui à supprimer. Pour supprimer tous les serveurs de clés secondaires, utilisez l'argument `-`, indiquant aucun.

Pour plus d'informations, reportez-vous au `security key-manager external` dans le "Référence de commande ONTAP".

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

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

Description de la tâche

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

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

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

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

- Vous recevez un avertissement si les serveurs de gestion des clés configurés stockent déjà plus de 128 clés d'authentification.
- Vous pouvez utiliser le `security key-manager key delete` commande permettant de supprimer les clés inutilisées. Le `security key-manager key delete` La commande échoue si la clé donnée est

actuellement utilisée par ONTAP. (Vous devez avoir des privilèges supérieurs à « admin » pour utiliser cette commande.)

> Dans un environnement MetroCluster, avant de supprimer une clé, veillez à ce que cette clé ne soit pas utilisée sur le cluster partenaire. Vous pouvez utiliser les commandes suivantes sur le cluster partenaire pour vérifier que la clé n'est pas utilisée :
>
> - `storage encryption disk show -data-key-id` *`key-id`*
> - `storage encryption disk show -fips-key-id` *`key-id`*

Avant de commencer

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

Étapes

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

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

   > Réglage `prompt-for-key=true` provoque l'invite de l'administrateur de cluster à utiliser la phrase secrète lors de l'authentification de disques cryptés. Dans le cas contraire, le système génère automatiquement une phrase de passe de 32 octets. Le `security key-manager key create` la commande remplace le `security key-manager create-key` commande. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

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

   ```
   cluster1::> security key-manager key create
   Key ID:
   00000000000000000200000000000001006268333f870860128fbe17d393e5083b00000000
   00000000
   ```

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

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

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

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

```
cluster1::> security key-manager key query
       Vserver: cluster1
   Key Manager: external
          Node: node1

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

       Vserver: cluster1
   Key Manager: external
          Node: node2

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node2                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

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

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

Description de la tâche

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

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

- Cette commande n'est pas prise en charge lorsque la gestion intégrée des clés est activée.

- Vous recevez un avertissement si les serveurs de gestion des clés configurés stockent déjà plus de 128 clés d'authentification.

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

Avant de commencer

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

Étapes

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

   `security key-manager create-key`

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

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

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

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

   Node: cluster1-01
   Creating authentication key...
   Authentication key creation successful.
   Key ID: F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

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

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

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

   `security key-manager query`

   Pour 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 query

  (security key-manager query)

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

Key Tag        Key Type  Restored
-------------  --------  --------
cluster1-01    NSE-AK    yes
       Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C


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

Key Tag        Key Type  Restored
-------------  --------  --------
cluster1-02    NSE-AK    yes
       Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
```

Attribution d'une clé d'authentification de données à un lecteur FIPS ou SED (gestion de clés externe)

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

Description de la tâche

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

Cette procédure n'est pas perturbatrice.

Avant de commencer

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

Étapes

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

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

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

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

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

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

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

   `storage encryption disk show`

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

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   ------------------------------------------------------------------
   0.0.0   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   [...]
   ```

Configurez la gestion intégrée des clés

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

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

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

Description de la tâche

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

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

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

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

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

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

  La commande de mise à niveau vérifie que le contenu de l'image n'a pas été modifié ou corrompu en vérifiant diverses signatures numériques. 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.

Avant de commencer

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

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

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

Étapes

1. Lancez la commande de 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. 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 -node node
```

> 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
       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: cluster1
   Key Manager: onboard
          Node: node2

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
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.

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

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

Vous pouvez utiliser le gestionnaire de clés intégré pour sécuriser les clés que le cluster utilise pour accéder aux données chiffrées. 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 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 que le gestionnaire de clés intégré ne soit configuré.

Étapes

1. Lancez la configuration du gestionnaire de clés :

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

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

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

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

...

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

2. Entrez `yes` à l'invite, configurez la gestion intégrée des clés.
3. À l'invite de phrase de passe, entrez une phrase de passe comprise entre 32 et 256 caractères, ou une phrase de passe entre 64 et 256 caractères pour « mode CC ».

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

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

   `security key-manager 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
-----------------------------------------------------------------------
--------
000000000000000002000000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                                   Used By
-----------------------------------------------------------------------
--------
000000000000000002000000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

Une fois que vous avez terminé

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".

Attribution d'une clé d'authentification des données à un lecteur FIPS ou SED (gestion des clés intégrée)

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

Description de la tâche

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

Avant de commencer

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

Étapes

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

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

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

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

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   0000000000000000020000000000010019215b9738bc7b43d4698c80246db1f4

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

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

   `storage encryption disk show`

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

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
--------------------------------------------------------------
0.0.0   data
000000000000000002000000000010019215b9738bc7b43d4698c80246db1f4
0.0.1   data
000000000000000002000000000010059851742AF2703FC91369B7DB47C4722
[...]
```

Attribuez une clé d'authentification FIPS 140-2 à un disque FIPS

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

Description de la tâche

Votre configuration de sécurité peut nécessiter l'utilisation de clés différentes pour l'authentification des données et l'authentification FIPS 140-2-2. Si ce n'est pas le cas, vous pouvez utiliser la même clé d'authentification pour la conformité FIPS que celle utilisée pour l'accès aux données.

Cette procédure n'est pas perturbatrice.

Avant de commencer

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

Étapes

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

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

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

```
cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A

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

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

   `storage encryption disk show -fips`

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

```
cluster1::> storage encryption disk show -fips
Disk    Mode FIPS-Compliance Key ID
------  ----
-------------------------------------------------------------------
2.10.0  full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
2.10.1  full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
[...]
```

Activez le mode compatible FIPS au niveau du cluster pour les connexions de serveurs KMIP

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

Description de la tâche

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

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

Avant de commencer

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

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

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

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

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

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

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

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

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

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

   ```
   security config show
   ```

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

Gestion du cryptage NetApp

Déchiffrement des données de volume

Vous pouvez utiliser le `volume move start` commande pour déplacer et annuler le chiffrement des données de volume.

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche. Vous pouvez également être un administrateur SVM auquel l'administrateur du cluster a délégué des pouvoirs. Pour plus d'informations, voir "Autorité déléguée pour exécuter la commande volume Move".

Étapes

1. Déplacer un volume chiffré existant sans chiffrer les données sur le volume :

   `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 déplace un volume existant nommé `vol1` vers l'agrégat de destination `aggr3` et déchiffre les données sur le volume :

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3 -encrypt-destination false
   ```

   Le système supprime la clé de cryptage du volume. Les données du volume sont non chiffrées.

2. Vérifiez que le volume est désactivé pour le chiffrement :

   `volume show -encryption`

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

   La commande suivante indique si les volumes sont présents `cluster1` sont chiffrées :

   ```
   cluster1::> volume show -encryption

   Vserver  Volume   Aggregate   State    Encryption State
   -------  ------   ---------   -----    ----------------
   vs1      vol1     aggr1       online   none
   ```

Déplacement d'un volume chiffré

Vous pouvez utiliser le `volume move start` commande permettant de déplacer un volume chiffré. Le volume déplacé peut résider sur le même agrégat ou sur un autre agrégat.

Description de la tâche

Le déplacement échoue si le nœud de destination ou le volume de destination ne prend pas en charge le chiffrement de volume.

Le `-encrypt-destination` option pour `volume move start` la valeur par défaut est true pour les volumes chiffrés. La nécessité de spécifier que vous ne souhaitez pas que le volume de destination soit chiffré garantit que vous ne déchiffrez pas par inadvertance les données sur le volume.

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche. Vous pouvez également être un administrateur SVM auquel l'administrateur du cluster a délégué des pouvoirs. Pour plus d'informations, voir "autorité déléguée pour exécuter la commande de déplacement de volume".

Étapes

1. Déplacez un volume chiffré et laissez les données sur le volume chiffré :

   `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`*

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

   La commande suivante déplace un volume existant nommé `vol1` vers l'agrégat de destination `aggr3` et conserve les données sur le volume chiffrées :

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3
   ```

2. 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    aggr3     online    RW  200GB    160.0GB  20%
   ```

Autorité déléguée pour exécuter la commande volume Move

Vous pouvez utiliser le `volume move` commande pour chiffrer un volume existant, déplacer un volume chiffré ou annuler le chiffrement d'un volume. Les administrateurs du cluster peuvent exécuter `volume move` Ils peuvent se passer eux-mêmes de la commande ou déléguer à l'autorité pour qu'elle exécute la commande aux

administrateurs du SVM.

Description de la tâche

Par défaut, les administrateurs du SVM sont affectés au système `vsadmin` rôle, qui ne comprend pas l'autorité nécessaire pour déplacer les volumes. Vous devez affecter le `vsadmin-volume` Rôle aux administrateurs SVM afin de leur permettre d'exécuter les `volume move` commande.

Étape

1. Déléguer l'autorité pour exécuter le `volume move` commande :

   ```
   security login modify -vserver SVM_name -user-or-group-name user_or_group_name
   -application application -authmethod authentication_method -role vsadmin-
   volume
   ```

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

   La commande suivante permet à l'administrateur du SVM d'exécuter le `volume move` commande.

   ```
   cluster1::>security login modify -vserver engData -user-or-group-name
   SVM-admin -application ssh -authmethod domain -role vsadmin-volume
   ```

Modifiez la clé de chiffrement d'un volume à l'aide de la commande Volume Encryption rekey start

Il est recommandé de modifier régulièrement la clé de chiffrement d'un volume. Vous pouvez utiliser ONTAP 9.3 à partir de `volume encryption rekey start` commande pour changer la clé de chiffrement.

Description de la tâche

Une fois que vous avez démarré une opération de recontact, elle doit être terminée. Il n'y a pas de retour à l'ancienne clé. Si vous rencontrez un problème de performances pendant l'opération, vous pouvez exécuter le `volume encryption rekey pause` commande pour mettre l'opération en pause, et le `volume encryption rekey resume` commande pour reprendre l'opération.

Jusqu'à la fin de l'opération de renouvellement de clé, le volume est composé de deux touches. Les nouvelles écritures et les lectures correspondantes utiliseront la nouvelle clé. Sinon, les lectures utilisent l'ancienne clé.

> Vous ne pouvez pas utiliser `volume encryption rekey start` Pour rétablir un volume SnapLock.

Étapes

1. Modifier une clé de chiffrement :

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

   La commande suivante modifie la clé de chiffrement pour `vol1` Sur SVM`vs1`:

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

2. Vérifier l'état de l'opération de renouvellement de clé :

   `volume encryption rekey show`

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

   La commande suivante affiche l'état de l'opération de renouvellement de clés :

```
cluster1::> volume encryption rekey 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 renouvellement de clés 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%
```

Modifiez la clé de chiffrement d'un volume à l'aide de la commande volume Move start

Il est recommandé de modifier régulièrement la clé de chiffrement d'un volume. Vous pouvez utiliser le `volume move start` commande pour changer la clé de chiffrement. Vous devez utiliser `volume move start` Dans ONTAP 9.2 et versions antérieures. Le volume déplacé peut résider sur le même agrégat ou sur un autre agrégat.

Description de la tâche

Vous ne pouvez pas utiliser `volume move start` Pour reKey un volume SnapLock ou FlexGroup.

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche. Vous pouvez également être un administrateur SVM auquel l'administrateur du cluster a délégué des pouvoirs. Pour plus d'informations, voir

"autorité déléguée pour exécuter la commande de déplacement de volume".

Étapes

1. Déplacer un volume existant et modifier la clé de chiffrement :

   `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-generate-destination-key true`

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

   La commande suivante déplace un volume existant nommé **`vol1`** vers l'agrégat de destination **`aggr2`** et modifie la clé de chiffrement :

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

   Une nouvelle clé de chiffrement est créée pour le volume. Les données du volume restent chiffrées.

2. 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%
   ```

Rotation des clés d'authentification pour NetApp Storage Encryption

Vous pouvez faire tourner les clés d'authentification lorsque vous utilisez NetApp Storage Encryption (NSE).

Description de la tâche

La rotation des clés d'authentification dans un environnement NSE est prise en charge si vous utilisez External Key Manager (KMIP).

> La rotation des clés d'authentification dans un environnement NSE n'est pas prise en charge pour Onboard Key Manager (OKM).

Étapes

1. Utilisez le `security key-manager create-key` commande permettant de générer de nouvelles clés d'authentification.

Vous devez générer de nouvelles clés d'authentification avant de pouvoir modifier les clés d'authentification.

2. Utilisez le `storage encryption disk modify -disk * -data-key-id` commande pour modifier les clés d'authentification.

Supprimez un volume chiffré

Vous pouvez utiliser le `volume delete` commande de suppression d'un volume chiffré.

Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche. Vous pouvez également être un administrateur SVM auquel l'administrateur du cluster a délégué des pouvoirs. Pour plus d'informations, voir "autorité déléguée pour exécuter la commande de déplacement de volume".
- Le volume doit être hors ligne.

Étape

1. Supprimez un volume chiffré :

   `volume delete -vserver` *`SVM_name`* `-volume` *`volume_name`*

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

   La commande suivante supprime un volume chiffré nommé `vol1`:

   ```
   cluster1::> volume delete -vserver vs1 -volume vol1
   ```

   Entrez `yes` lorsque vous êtes invité à confirmer la suppression.

   Le système supprime la clé de cryptage du volume au bout de 24 heures.

   Utiliser `volume delete` avec le `-force true` option permettant de supprimer un volume et de détruire immédiatement la clé de chiffrement correspondante. Cette commande nécessite des privilèges avancés. Pour plus d'informations, consultez la page man.

Une fois que vous avez terminé

Vous pouvez utiliser le `volume recovery-queue` pour restaurer un volume supprimé pendant la période de rétention après l'émission du `volume delete` commande :

`volume recovery-queue` *`SVM_name`* `-volume` *`volume_name`*

"Comment utiliser la fonction de récupération de volume"

Supprimez les données de façon sécurisée sur un volume chiffré

Supprimez les données de façon sécurisée dans une vue d'ensemble du volume chiffré

Depuis ONTAP 9.4, vous pouvez utiliser la suppression sécurisée pour nettoyer les données sans interruption sur les volumes NVE. La suppression des données sur un

volume chiffré garantit qu'elles ne peuvent pas être récupérées depuis le support physique, par exemple en cas de « pillage », où les traces de données peuvent être laissées derrière lors de l'écrasement des blocs ou pour supprimer en toute sécurité les données d'un locataire vide.

La suppression sécurisée fonctionne uniquement pour les fichiers précédemment supprimés sur les volumes NVE. Vous ne pouvez pas nettoyer un volume non chiffré. Vous devez utiliser des serveurs KMIP pour fournir des clés, et non le gestionnaire de clés intégré.

Considérations relatives à l'utilisation de la suppression sécurisée

- Les volumes créés dans un agrégat pour NetApp Aggregate Encryption (NAE) ne prennent pas en charge la suppression sécurisée.
- La suppression sécurisée fonctionne uniquement pour les fichiers précédemment supprimés sur les volumes NVE.
- Vous ne pouvez pas nettoyer un volume non chiffré.
- Vous devez utiliser des serveurs KMIP pour fournir des clés, et non le gestionnaire de clés intégré.

Les fonctions de purge sécurisée varient en fonction de votre version de ONTAP.

ONTAP 9.8 et versions ultérieures

- La suppression sécurisée est prise en charge par MetroCluster et FlexGroup.
- Si le volume en cours de purge est à l'origine d'une relation SnapMirror, il n'est pas nécessaire de rompre la relation SnapMirror pour effectuer une purge sécurisée.
- La méthode de rechiffrement est différente pour les volumes qui utilisent la protection des données SnapMirror, contre les volumes qui n'utilisent pas la protection des données SnapMirror (DP) ou ceux qui utilisent la protection étendue des données SnapMirror.
  - Par défaut, les volumes utilisant le mode de protection des données SnapMirror (DP) recryptent les données à l'aide de la méthode de chiffrement du déplacement de volume.
  - Par défaut, les volumes qui n'utilisent pas la protection des données SnapMirror ou les volumes en utilisant le mode XDP (SnapMirror Extended Data protection) utilisent la méthode de rechiffrement sur place.
  - Ces valeurs par défaut peuvent être modifiées à l'aide de l' `secure purge re-encryption-method [volume-move|in-place-rekey]` commande.
- Par défaut toutes les copies Snapshot des volumes FlexVol sont automatiquement supprimées lors de l'opération de suppression sécurisée. Par défaut, les copies Snapshot des volumes FlexGroup et les volumes qui utilisent la protection des données SnapMirror ne sont pas automatiquement supprimées lors de l'opération de suppression sécurisée. Ces valeurs par défaut peuvent être modifiées à l'aide de l' `secure purge delete-all-snapshots [true|false]` commande.

ONTAP 9.7 et versions antérieures :

- La purge sécurisée ne prend pas en charge les éléments suivants :
  - FlexClone
  - SnapVault
  - FabricPool
- Si le volume en cours de purge est la source d'une relation SnapMirror, vous devez interrompre la relation SnapMirror avant de pouvoir purger le volume.

  Si des copies Snapshot sont occupées dans le volume, vous devez libérer les copies Snapshot avant de pouvoir purger le volume. Par exemple, vous devrez peut-être séparer un volume FlexClone de son volume parent.

- L'appel réussi de la fonction de suppression sécurisée déclenche un déplacement de volume qui recrypte les données restantes non supprimées avec une nouvelle clé.

  Le volume déplacé reste sur l'agrégat actuel. L'ancienne clé est automatiquement détruite, ce qui permet de s'assurer que les données supprimées ne peuvent pas être récupérées du support de stockage.

Supprimez en toute sécurité les données d'un volume chiffré sans une relation SnapMirror

Depuis ONTAP 9.4, vous pouvez utiliser la suppression sécurisée vers les données « ``cribs'' sans interruption sur les volumes NVE.

Description de la tâche

La suppression sécurisée peut prendre de plusieurs minutes à plusieurs heures, selon la quantité de données

contenues dans les fichiers supprimés. Vous pouvez utiliser le `volume encryption secure-purge show` commande permettant d'afficher le statut de l'opération. Vous pouvez utiliser le `volume encryption secure-purge abort` commande pour mettre fin à l'opération.

> Pour effectuer une purge sécurisée sur un hôte SAN, vous devez supprimer la LUN entière contenant les fichiers à purger, ou vous devez pouvoir perforer les trous dans la LUN pour les blocs appartenant aux fichiers à purger. Si vous ne pouvez pas supprimer la LUN ou si votre système d'exploitation hôte ne prend pas en charge la perforation dans la LUN, vous ne pouvez pas effectuer de purge sécurisée.

Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Des privilèges avancés sont requis pour cette tâche.

Étapes

1. Supprimez les fichiers ou la LUN que vous souhaitez supprimer en toute sécurité.
   - Sur un client NAS, supprimez les fichiers que vous souhaitez purger en toute sécurité.
   - Sur un hôte SAN, supprimez le LUN que vous souhaitez purger ou perforer en toute sécurité les blocs appartenant aux fichiers à supprimer.
2. Sur le système de stockage, passez au niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

3. Si les fichiers que vous souhaitez purger en toute sécurité sont dans les instantanés, supprimez-les :

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

4. Supprimez les fichiers supprimés de manière sécurisée :

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   ```

   La commande suivante supprime de manière sécurisée les fichiers supprimés sur `vol1` Sur SVM`vs1`:

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

5. Vérifier l'état de l'opération de purge sécurisée :

   ```
   volume encryption secure-purge show
   ```

Supprimez en toute sécurité les données sur un volume chiffré avec une relation asynchrone SnapMirror

À partir de ONTAP 9.8, vous pouvez appliquer une suppression sécurisée aux données « crub » sans interruption sur les volumes NVE avec une relation asynchrone SnapMirror.

Avant de commencer

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

- Des privilèges avancés sont requis pour cette tâche.

Description de la tâche

La suppression sécurisée peut prendre de plusieurs minutes à plusieurs heures, selon la quantité de données contenues dans les fichiers supprimés. Vous pouvez utiliser le `volume encryption secure-purge show` commande permettant d'afficher le statut de l'opération. Vous pouvez utiliser le `volume encryption secure-purge abort` commande pour mettre fin à l'opération.

> Pour effectuer une purge sécurisée sur un hôte SAN, vous devez supprimer la LUN entière contenant les fichiers à purger, ou vous devez pouvoir perforer les trous dans la LUN pour les blocs appartenant aux fichiers à purger. Si vous ne pouvez pas supprimer la LUN ou si votre système d'exploitation hôte ne prend pas en charge la perforation dans la LUN, vous ne pouvez pas effectuer de purge sécurisée.

Étapes

1. Sur le système de stockage, basculer sur le niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

2. Supprimez les fichiers ou la LUN que vous souhaitez supprimer en toute sécurité.
   - Sur un client NAS, supprimez les fichiers que vous souhaitez purger en toute sécurité.
   - Sur un hôte SAN, supprimez le LUN que vous souhaitez purger ou perforer en toute sécurité les blocs appartenant aux fichiers à supprimer.
3. Préparez le volume de destination dans la relation asynchrone à supprimer de manière sécurisée :

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   -prepare true
   ```

   Répétez cette étape pour chaque volume de votre relation SnapMirror asynchrone.

4. Si les fichiers que vous souhaitez supprimer de manière sécurisée se trouvent dans des copies Snapshot, supprimez les copies Snapshot :

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

5. Si les fichiers que vous souhaitez supprimer de manière sécurisée se trouvent dans les copies Snapshot de base, procédez comme suit :

   a. Créer une copie Snapshot sur le volume de destination dans la relation asynchrone SnapMirror :

      ```
      volume snapshot create -snapshot snapshot_name -vserver SVM_name -volume
      volume_name
      ```

   b. Mettre à jour SnapMirror pour transférer la copie Snapshot de base :

      ```
      snapmirror update -source-snapshot snapshot_name -destination-path
      destination_path
      ```

   Répétez cette étape pour chaque volume de la relation asynchrone SnapMirror.

   a. Les étapes de répétition (a) et (b) sont égales au nombre de copies Snapshot de base plus une.

Par exemple, si vous avez deux copies Snapshot de base, vous devez répéter les étapes (a) et (b) trois fois.

b. Vérifier la présence de la copie Snapshot de base :

```
snapshot show -vserver SVM_name -volume volume_name
```

c. Supprimer la copie Snapshot de base :

```
snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot
```

6. Supprimez les fichiers supprimés de manière sécurisée :

```
volume encryption secure-purge start -vserver svm_name -volume volume_name
```

Répétez cette étape pour chaque volume de la relation asynchrone SnapMirror.

La commande suivante purge de manière sécurisée les fichiers supprimés sur « 'vol1' » du SVM « vs1 » :

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume
vol1
```

7. Vérifier l'état de l'opération de purge sécurisée :

```
volume encryption secure-purge show
```

Nettoyer les données sur un volume chiffré avec une relation synchrone SnapMirror

À partir de ONTAP 9.8, vous pouvez utiliser une suppression sécurisée pour « nettoyer » les données de volumes NVE avec une relation synchrone SnapMirror, sans interruption.

Description de la tâche

Une purge sécurisée peut prendre plusieurs minutes à plusieurs heures, selon la quantité de données contenues dans les fichiers supprimés. Vous pouvez utiliser le `volume encryption secure-purge show` commande permettant d'afficher le statut de l'opération. Vous pouvez utiliser le `volume encryption secure-purge abort` commande pour mettre fin à l'opération.

> Pour effectuer une purge sécurisée sur un hôte SAN, vous devez supprimer la LUN entière contenant les fichiers à purger, ou vous devez pouvoir perforer les trous dans la LUN pour les blocs appartenant aux fichiers à purger. Si vous ne pouvez pas supprimer la LUN ou si votre système d'exploitation hôte ne prend pas en charge la perforation dans la LUN, vous ne pouvez pas effectuer de purge sécurisée.

Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Des privilèges avancés sont requis pour cette tâche.

Étapes

1. Sur le système de stockage, passez au niveau de privilège avancé :

```
set -privilege advanced
```

2. Supprimez les fichiers ou la LUN que vous souhaitez supprimer en toute sécurité.
   - Sur un client NAS, supprimez les fichiers que vous souhaitez purger en toute sécurité.
   - Sur un hôte SAN, supprimez le LUN que vous souhaitez purger ou perforer en toute sécurité les blocs appartenant aux fichiers à supprimer.
3. Préparez le volume de destination dans la relation asynchrone à supprimer de manière sécurisée :

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   -prepare true
   ```

   Répétez cette étape pour l'autre volume de votre relation synchrone SnapMirror.

4. Si les fichiers que vous souhaitez supprimer de manière sécurisée se trouvent dans des copies Snapshot, supprimez les copies Snapshot :

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot snapshot
   ```

5. Si le fichier de suppression sécurisée se trouve dans les copies Snapshot de base ou communes, mettez à jour SnapMirror pour déplacer la copie Snapshot commune :

   ```
   snapmirror update -source-snapshot snapshot_name -destination-path
   destination_path
   ```

   Il existe deux copies Snapshot communes. Cette commande doit donc être émise deux fois.

6. Si le fichier de suppression sécurisée se trouve dans la copie Snapshot cohérente au niveau des applications, supprimez la copie Snapshot sur les deux volumes de la relation synchrone SnapMirror :

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot snapshot
   ```

   Effectuer cette étape sur les deux volumes.

7. Supprimez les fichiers supprimés de manière sécurisée :

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   ```

   Répétez cette étape pour chaque volume de la relation synchrone SnapMirror.

   La commande suivante supprime en toute sécurité les fichiers supprimés sur « vol1 » sur le SMV « vs1 ».

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

8. Vérifier l'état de l'opération de purge sécurisée :

   ```
   volume encryption secure-purge show
   ```

Modifiez la phrase secrète intégrée pour la gestion des clés

Il est recommandé d'appliquer régulièrement une meilleure pratique de sécurité à la modification de la phrase secrète intégrée pour la gestion des clés. Copiez la nouvelle phrase secrète intégrée pour la gestion des clés dans un emplacement sécurisé en dehors du système de stockage pour une utilisation ultérieure.

Avant de commencer

- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.
- Des privilèges avancés sont requis pour cette tâche.

Étapes

1. Changement au niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

2. Modifiez la phrase secrète intégrée pour la gestion des clés :

Pour cette version ONTAP…	Utilisez cette commande…
ONTAP 9.6 et versions ultérieures	`security key-manager onboard update-passphrase`
ONTAP 9.5 et versions antérieures	`security key-manager update-passphrase`

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

   La commande suivante de ONTAP 9.6 vous permet de modifier la phrase secrète de gestion intégrée des clés pour `cluster1`:

   ```
   cluster1::> security key-manager onboard update-passphrase
   Warning: This command will reconfigure the cluster passphrase for
   onboard key management for Vserver "cluster1".
   Do you want to continue? {y|n}: y
   Enter current passphrase:
   Enter new passphrase:
   ```

3. Entrez `y` à l'invite, vous pouvez modifier la phrase secrète intégrée pour la gestion des clés.
4. Saisissez la phrase de passe actuelle à l'invite de phrase de passe actuelle.
5. À l'invite de la nouvelle 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.

6. À l'invite de confirmation de la phrase de passe, saisissez à nouveau la phrase de passe.

Une fois que vous avez terminé

Dans un environnement MetroCluster, vous devez mettre à jour la phrase secrète sur le cluster partenaire :

- Dans ONTAP 9.5 et les versions antérieures, vous devez exécuter `security key-manager update-passphrase` avec la même phrase secrète sur le cluster partenaire.
- Dans ONTAP 9.6 et versions ultérieures, vous êtes invité à exécuter `security key-manager onboard sync` avec la même phrase secrète sur le cluster partenaire.

Copiez le mot de passe de gestion des clés intégré vers un emplacement sécurisé en dehors du système de stockage pour une utilisation ultérieure.

Vous devez sauvegarder manuellement les informations de gestion des clés chaque fois que vous modifiez la phrase secrète de gestion intégrée des clés.

"Sauvegarde manuelle des informations de gestion intégrée des clés"

Sauvegardez manuellement les informations intégrées de gestion des clés

Vous devez copier les informations de gestion intégrée des clés dans un emplacement sécurisé en dehors du système de stockage dès que vous configurez la phrase secrète Onboard Key Manager.

Ce dont vous avez besoin

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Des privilèges avancés sont requis pour cette tâche.

Description de la tâche

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

Étapes

1. Changement au niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

2. Afficher les informations de gestion des clés du cluster :

Pour cette version ONTAP…	Utilisez cette commande…
ONTAP 9.6 et versions ultérieures	`security key-manager onboard show-backup`
ONTAP 9.5 et versions antérieures	`security key-manager backup show`

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

+

La commande 9.6 suivante affiche les informations de sauvegarde de la gestion des clés pour `cluster1`:

+

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

     --------------------------BEGIN BACKUP--------------------------
     TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
     QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
     dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAAACgAAAAAAAAAAA
     3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAAAA
     IgAAAAAAAAAAoAAAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
     QRHwv+1aWvAAAAAAAAAAAACQAAAAAAAAAAgAAAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
     BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
     AQAAAAMAAAAYAQAAAAAAADA5/ccAAAAAIgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAA
     AAAAAAAAAACAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAAACIAAAAAAAAAAA
     KAAAAAAAAACI8z/bAAAAAAAAAAAAAAAAAgAAAAAAAAQAbxMcI4qiaMS4Uts5tTUnU
     AAAAAAAAAAAkAAAAAAAAAAIAAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5Smyj
     LSgoK/qc8FAmMMcrRXY6uriulnL0WPB/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAAwAAABgBAAAAAAAAAA
     1cNLLwAAAAAiAAAAAAAAAACgAAAAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAIAAAAAAAkA
     ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAAIgAAAAAAAAAAoAAAAAAAAAAAJ4/cQsAAAAA
     AAAAAAAAAACAAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAAAAACQAAAAAAAAAAA
     gAAAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rrH4nPQM0n
     rDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     ---------------------------END BACKUP---------------------------
```

1. Copiez les informations de sauvegarde dans un emplacement sécurisé en dehors du système de stockage afin de les utiliser en cas d’incident.

Restaurez les clés de chiffrement intégrées de gestion des clés

La procédure à suivre pour restaurer vos clés de chiffrement de gestion intégrée des clés varie en fonction de votre version d’ONTAP.

Avant de commencer

- Si vous utilisez NSE avec un serveur de gestion externe des clés (KMIP), vous devez avoir supprimé la base de données de gestionnaire de clés externe. Pour plus d'informations, voir "passez à la gestion intégrée des clés grâce à la gestion externe des clés"
- Vous devez être un administrateur de cluster pour effectuer cette tâche.

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

ONTAP 9.6 et versions ultérieures

> Si vous exécutez ONTAP 9.8 ou une version ultérieure et que votre volume racine est chiffré, suivez la procédure de [ontap-9-8].

1. Vérifiez que la clé doit être restaurée :
   `security key-manager key query -node node`
2. Restaurer la clé :
   `security key-manager onboard sync`

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

   La commande ONTAP 9.6 suivante synchronise les clés dans la hiérarchie de clés intégrée :

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

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

3. À l'invite de phrase secrète, entrez la phrase secrète intégrée pour la gestion des clés du cluster.

ONTAP 9.8 ou version ultérieure avec volume racine chiffré

Si vous exécutez ONTAP 9.8 ou une version ultérieure et que votre volume racine est chiffré, vous devez définir une phrase de passe de récupération de la gestion des clés intégrée à l'aide du menu de démarrage. Ce processus est également nécessaire si vous effectuez un remplacement de support de démarrage.

1. Démarrez le nœud sur le menu de démarrage et sélectionnez option `(10) Set onboard key management recovery secrets`.
2. Entrez `y` pour utiliser cette option.
3. Entrez à l'invite le phrase secrète de gestion intégrée des clés pour le cluster.
4. À l'invite, entrez les données de la clé de sauvegarde.

   Le nœud revient au menu de démarrage.

5. Dans le menu de démarrage, sélectionnez option `(1) Normal Boot`.

ONTAP 9.5 et versions antérieures

1. Vérifiez que la clé doit être restaurée :

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

2. Si vous exécutez ONTAP 9.8 ou version ultérieure et que votre volume racine est chiffré, procédez comme suit :

   Si vous exécutez ONTAP 9.6 ou 9.7, ou si vous utilisez ONTAP 9.8 ou une version ultérieure et que votre volume racine n'est pas chiffré, ignorez cette étape.

3. Restaurer la clé :
   `security key-manager setup -node node`

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

4. À l'invite de phrase secrète, entrez la phrase secrète intégrée pour la gestion des clés du cluster.

Restaurez les clés de chiffrement externes pour la gestion des clés

Vous pouvez restaurer manuellement des clés de chiffrement de gestion externe des clés et les transférer vers un autre nœud. Vous pouvez le faire si vous redémarrez un nœud qui était temporairement arrêté lorsque vous avez créé les clés du cluster.

Description de la tâche

Dans ONTAP 9.6 et versions ultérieures, vous pouvez utiliser le `security key-manager key query -node node_name` commande pour vérifier si votre clé doit être restaurée.

Dans ONTAP 9.5 et les versions antérieures, vous pouvez utiliser le `security key-manager key show` commande pour vérifier si votre clé doit être restaurée.

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

Avant de commencer

Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

Étapes

1. Si vous exécutez ONTAP 9.8 ou version ultérieure et que le volume racine est chiffré, procédez comme suit :

   Si vous exécutez ONTAP 9.7 ou une version antérieure, ou si vous exécutez ONTAP 9.8 ou une version ultérieure et que votre volume racine n'est pas chiffré, ignorez cette étape.

   a. Définissez les bootargs :

   ```
   setenv kmip.init.ipaddr <ip-address>

   setenv kmip.init.netmask <netmask>

   setenv kmip.init.gateway <gateway>

   setenv kmip.init.interface e0M

   boot_ontap
   ```

b. Démarrez le nœud sur le menu de démarrage et sélectionnez option `(11) Configure node for external key management`.

c. Suivez les invites pour saisir le certificat de gestion.

   Une fois toutes les informations relatives au certificat de gestion saisies, le système revient au menu de démarrage.

d. Dans le menu de démarrage, sélectionnez option `(1) Normal Boot`.

2. Restaurer la clé :

Pour cette version ONTAP…	Utilisez cette commande…
ONTAP 9.6 et versions ultérieures	`security key-manager external restore -vserver SVM -node node -key-server host_name
IP_address:port -key-id key_id -key -tag key_tag`	ONTAP 9.5 et versions antérieures

> `node` tous les nœuds par défaut. Pour connaître la syntaxe complète des commandes, consultez les pages de manuels. Cette commande n'est pas prise en charge lorsque la gestion intégrée des clés est activée.

La commande ONTAP 9.6 suivante restaure les clés d'authentification externes de gestion des clés vers tous les nœuds de `cluster1`:

```
clusterl::> security key-manager external restore
```

Remplacer les certificats SSL

Tous les certificats SSL ont une date d'expiration. Vous devez mettre à jour vos certificats avant qu'ils n'expirent pour éviter toute perte d'accès aux clés d'authentification.

Avant de commencer

- Vous devez avoir obtenu le certificat public et la clé privée de remplacement pour le cluster (certificat client KMIP).
- Vous devez avoir obtenu le certificat public de remplacement pour le serveur KMIP (certificat KMIP Server-CA).
- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.
- Dans un environnement MetroCluster, vous devez remplacer le certificat SSL KMIP sur les deux clusters.

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

Étapes

1. Installez le nouveau certificat KMIP Server-ca :

```
security certificate install -type server-ca -vserver <>
```

2. Installez le nouveau certificat client KMIP :

   ```
   security certificate install -type client -vserver <>
   ```

3. Mettez à jour la configuration du gestionnaire de clés pour utiliser les certificats nouvellement installés :

   ```
   security key-manager external modify -vserver <> -client-cert <> -server-ca
   -certs <>
   ```

   Si vous exécutez ONTAP 9.6 ou version ultérieure dans un environnement MetroCluster et que vous souhaitez modifier la configuration du gestionnaire de clés sur le SVM admin, vous devez exécuter la commande sur les deux clusters de la configuration.

> La mise à jour de la configuration du gestionnaire de clés pour utiliser les certificats nouvellement installés renvoie une erreur si les clés publiques/privées du nouveau certificat client sont différentes des clés installées précédemment. Consultez l'article de la base de connaissances "Le nouveau certificat client les clés publiques ou privées sont différentes du certificat client existant" pour obtenir des instructions sur la manière de neutraliser cette erreur.

Remplacez un lecteur FIPS ou SED

Vous pouvez remplacer un lecteur FIPS ou SED de la même façon que vous remplacez un disque ordinaire. Veillez à attribuer de nouvelles clés d'authentification des données au disque de remplacement. Pour un lecteur FIPS, vous pouvez également attribuer une nouvelle clé d'authentification FIPS 140-2.

> Si une paire haute disponibilité est utilisée "Cryptage SAS ou disques NVMe (SED, NSE, FIPS)", vous devez suivre les instructions de la rubrique "Retour d'un lecteur FIPS ou SED en mode non protégé" Pour tous les disques de la paire HA avant d'initialiser le système (options de démarrage 4 ou 9). Si vous ne le faites pas, vous risquez de subir des pertes de données si les disques sont requalifiés.

Avant de commencer

- Vous devez connaître l'ID de clé pour la clé d'authentification utilisée par le lecteur.
- Vous devez être un administrateur de cluster pour effectuer cette tâche.

Étapes

1. Vérifiez que le disque a été marqué défectueux :

   ```
   storage disk show -broken
   ```

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

```
cluster1::> storage disk show -broken
Original Owner: cluster1-01
  Checksum Compatibility: block
                                                                    Usable
Physical
    Disk   Outage Reason HA Shelf Bay Chan   Pool  Type    RPM     Size
Size
    ------ ---- ------------ ---- --- ---- ------ -----  -----  -------
-------
    0.0.0  admin  failed  0b    1   0    A  Pool0  FCAL  10000  132.8GB
133.9GB
    0.0.7  admin  removed 0b    2   6    A  Pool1  FCAL  10000  132.8GB
134.2GB
[...]
```

2. Retirez le disque défectueux et remplacez-le par un nouveau lecteur FIPS ou SED, en suivant les instructions du guide matériel de votre modèle de tiroir disque.
3. Attribuez la propriété du disque récemment remplacé :

   ```
   storage disk assign -disk disk_name -owner node
   ```

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

   ```
   cluster1::> storage disk assign -disk 2.1.1 -owner cluster1-01
   ```

4. Vérifiez que le nouveau disque a été affecté :

   ```
   storage encryption disk show
   ```

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

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
--------------------------------------------------------------
0.0.0   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
0.0.1   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
1.10.0  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
1.10.1  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
2.1.1   open 0x0
[...]
```

5. Attribuez les clés d'authentification des données au lecteur FIPS ou SED.

   "Attribution d'une clé d'authentification de données à un lecteur FIPS ou SED (gestion de clés externe)"

6. Si nécessaire, attribuez une clé d'authentification FIPS 140-2 au lecteur FIPS.

   "Attribution d'une clé d'authentification FIPS 140-2 à un lecteur FIPS"

Rendre les données d'un lecteur FIPS ou SED inaccessibles

Rendre les données sur un lecteur FIPS ou SED inaccessibles

Si vous souhaitez rendre les données stockées sur un lecteur FIPS ou SED définitivement inaccessibles, mais que l'espace inutilisé du lecteur reste disponible pour les nouvelles données, vous pouvez désinfecter le disque. Si vous souhaitez rendre les données définitivement inaccessibles et que vous n'avez pas besoin de réutiliser le lecteur, vous pouvez le détruire.

- Nettoyage de disque

  Lorsque vous procédez à la suppression d'un disque à auto-cryptage, le système modifie la clé de cryptage sur disque en une nouvelle valeur aléatoire, réinitialise l'état de verrouillage à la mise sous tension sur FALSE et définit l'ID de clé sur une valeur par défaut, soit l'ID sécurisé du fabricant 0x0 (disques SAS), soit une clé nulle (disques NVMe). Cela rend les données sur le disque inaccessibles et impossible à récupérer. Vous pouvez réutiliser des disques aseptisés comme disques de rechange non remis à zéro.

- Destruction du disque

  Lorsque vous détruisez un lecteur FIPS ou SED, le système définit la clé de cryptage sur une valeur aléatoire inconnue et verrouille le disque de façon irréversible. Le disque devient ainsi définitivement inutilisable et les données qu'il y a définitivement inaccessibles.

Vous pouvez supprimer ou détruire des disques auto-cryptés ou tous les disques auto-cryptés d'un nœud.

Désinfectez un lecteur FIPS ou SED

Si vous voulez rendre les données sur un lecteur FIPS ou SED définitivement inaccessibles et utiliser le lecteur pour les nouvelles données, vous pouvez utiliser le `storage encryption disk sanitize` commande de nettoyage du disque.

Description de la tâche

Lorsque vous procédez à la suppression d'un disque à auto-cryptage, le système modifie la clé de cryptage sur disque en une nouvelle valeur aléatoire, réinitialise l'état de verrouillage à la mise sous tension sur FALSE et définit l'ID de clé sur une valeur par défaut, soit l'ID sécurisé du fabricant 0x0 (disques SAS), soit une clé nulle (disques NVMe). Cela rend les données sur le disque inaccessibles et impossible à récupérer. Vous pouvez réutiliser des disques aseptisés comme disques de rechange non remis à zéro.

Avant de commencer

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

Étapes

1. Migrer toutes les données qui doivent être conservées vers un agrégat sur un autre disque.
2. Supprimez l'agrégat du lecteur FIPS ou SED pour les désinfecter :

   `storage aggregate delete -aggregate` *`aggregate_name`*

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

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

3. Identifiez l'ID du disque pour le lecteur FIPS ou SED à désinfecter :

   `storage encryption disk show -fields data-key-id,fips-key-id,owner`

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

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   --------------------------------------------------------------------
   0.0.0   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   1.10.2  data
   F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
   [...]
   ```

4. Si un lecteur FIPS est exécuté en mode FIPS-Compliance, définissez l'ID de clé d'authentification FIPS du

nœud sur le MSID 0x0 par défaut :

`storage encryption disk modify -disk disk_id -fips-key-id 0x0`

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

```
cluster1::> storage encryption disk modify -disk 1.10.2 -fips-key-id 0x0

Info: Starting modify on 1 disk.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

5. Désinfectez le lecteur :

   `storage encryption disk sanitize -disk disk_id`

   Vous pouvez utiliser cette commande pour désinfecter uniquement les disques de rechange à chaud ou endommagés. Pour désinfecter tous les disques, quel que soit leur type, utilisez le `-force-all-state` option. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   > ONTAP vous invite à saisir une phrase de confirmation avant de continuer. Saisissez la phrase exactement comme indiqué à l'écran.

```
cluster1::> storage encryption disk sanitize -disk 1.10.2

Warning: This operation will cryptographically sanitize 1 spare or
broken self-encrypting disk on 1 node.
         To continue, enter sanitize disk: sanitize disk

Info: Starting sanitize on 1 disk.
      View the status of the operation using the
      storage encryption disk show-status command.
```

6. Éliminez la panne du disque désinfecté :
   `storage disk unfail -spare true -disk disk_id`
7. Vérifiez si le disque est propriétaire :
   `storage disk show -disk disk_id`

   Si le disque ne possède pas de propriétaire, attribuez-en un.
   `storage disk assign -owner node -disk disk_id`
8. Entrez le nodeshell pour le nœud qui possède les disques à désinfecter :

   `system node run -node node_name`

   Exécutez le `disk sanitize release` commande.

9. Quittez le nodeshell. Éliminez à nouveau la panne du disque :
   `storage disk unfail -spare true -disk disk_id`
10. Vérifier que le disque est désormais une pièce de rechange et prêt à être réutilisé dans un agrégat :
   `storage disk show -disk disk_id`

Détruire un lecteur FIPS ou SED

Si vous voulez rendre les données sur un lecteur FIPS ou SED définitivement inaccessibles et que vous n'avez pas besoin de réutiliser le lecteur, vous pouvez utiliser `storage encryption disk destroy` commande de destruction du disque.

Description de la tâche

Lorsque vous détruisez un lecteur FIPS ou SED, le système définit la clé de cryptage sur une valeur aléatoire inconnue et verrouille le disque de façon irréversible. Le disque devient ainsi pratiquement inutilisable et les données qu'il y a définitivement inaccessibles. Cependant, vous pouvez réinitialiser le disque à ses paramètres configurés en usine à l'aide de l'ID de sécurité physique (PSID) imprimé sur l'étiquette du disque. Pour plus d'informations, voir "Remise en service d'un lecteur FIPS ou SED en cas de perte de clés d'authentification".

> Vous ne devez pas détruire un disque FIPS ou SED sauf si vous disposez du service NRD plus (non-Returnable Disk plus). La destruction d'un disque annule sa garantie.

Avant de commencer

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

Étapes

1. Migrer toutes les données qui doivent être conservées vers un agrégat sur un autre disque.
2. Supprimez l'agrégat du disque FIPS ou SED à détruire :

   `storage aggregate delete -aggregate aggregate_name`

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

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

3. Identifiez l'ID de disque pour le lecteur FIPS ou SED à détruire :

   `storage encryption disk show`

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

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
--------------------------------------------------------------------
0.0.0   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
0.0.1   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
1.10.2  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
[...]
```

4. Détruire le disque :

   ```
   storage encryption disk destroy -disk disk_id
   ```

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

   > Vous êtes invité à entrer une phrase de confirmation avant de continuer. Saisissez la phrase exactement comme indiqué à l'écran.

   ```
   cluster1::> storage encryption disk destroy -disk 1.10.2

   Warning: This operation will cryptographically destroy 1 spare or broken
            self-encrypting disks on 1 node.
            You cannot reuse destroyed disks unless you revert
            them to their original state using the PSID value.
            To continue, enter
             destroy disk
            :destroy disk

   Info: Starting destroy on 1 disk.
         View the status of the operation by using the
         "storage encryption disk show-status" command.
   ```

Données d'urgence déchirées sur un lecteur FIPS ou SED

En cas d'urgence en matière de sécurité, vous pouvez instantanément empêcher l'accès à un disque FIPS ou SED, même si l'alimentation n'est pas disponible pour le système de stockage ou le serveur KMIP.

Avant de commencer

- Si vous utilisez un serveur KMIP qui n'est pas alimenté, vous devez configurer le serveur KMIP avec un élément d'authentification facilement détruit (par exemple, une carte à puce ou un lecteur USB).

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

Étape

1. Exécutez la suppression d’urgence des données sur un lecteur FIPS ou SED :

Si…	Alors…

L'alimentation est disponible pour le système de stockage et vous avez le temps de mettre celui-ci hors ligne aisément	a. Si le système de stockage est configuré en tant que paire haute disponibilité, désactivez le basculement.
	b. Mettre tous les agrégats hors ligne et les supprimer
	c. Définissez le niveau de privilège sur avancé :
	`set -privilege advanced`
	d. Si le lecteur est en mode FIPS-compliance, définissez à nouveau l'ID de clé d'authentification FIPS du nœud sur le MSID par défaut :
	`storage encryption disk modify -disk * -fips-key-id 0x0`
	e. Arrêter le système de stockage.
	f. Démarre en mode de maintenance.
	g. Procédez à la suppression ou à la destruction des disques :
	◦ Pour rendre les données sur les disques inaccessibles et continuer à réutiliser les disques, procédez comme suit :
	`disk encrypt sanitize -all`
	◦ Si vous souhaitez rendre les données sur les disques inaccessibles et que vous n'avez pas besoin d'enregistrer les disques, détruisez les disques :
	`disk encrypt destroy disk_id1 disk_id2 …`
		Le système de stockage est sous tension et vous devez immédiatement détruire les données

a. **Si vous souhaitez rendre les données sur les disques inaccessibles et que vous pourrez toujours les réutiliser, désinfectez les disques :**
b. Si le système de stockage est configuré en tant que paire haute disponibilité, désactivez le basculement.
c. Définissez le niveau de privilège sur avancé :
`set -privilege advanced`
d. Si le lecteur est en mode FIPS-compliance, définissez à nouveau l'ID de clé d'authentification FIPS du nœud sur le MSID par défaut :
`storage encryption disk modify -disk * -fips-key-id 0x0`
e. Procédez à la suppression du disque :
`storage encryption disk sanitize -disk * -force-all-states true`
	a. **Si vous souhaitez rendre les données sur les disques inaccessibles et que vous n'avez pas besoin d'enregistrer les disques, détruisez les disques :**
	b. Si le système de stockage est configuré en tant que paire haute disponibilité, désactivez le basculement.
	c. Définissez le niveau de privilège sur avancé :
	`set -privilege advanced`
	d. Détruire les disques :
	`storage encryption disk destroy -disk * -force-all-states true`
		Le système de stockage fonctionne de façon incohérente, laissant le système se trouve dans un état désactivé en permanence et toutes les données sont effacées. Pour réutiliser le système, vous devez le reconfigurer.

L'alimentation est disponible pour le serveur KMIP, mais pas pour le système de stockage	a. Connectez-vous au serveur KMIP. b. Détruire toutes les clés associées aux lecteurs FIPS ou les disques SED qui contiennent les données auxquelles vous souhaitez empêcher l'accès. Cela empêche l'accès aux clés de cryptage du disque par le système de stockage.	L'alimentation n'est pas disponible pour le serveur KMIP ou le système de stockage

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

Renvoyez un lecteur FIPS ou SED au service en cas de perte de clés d'authentification

Le système traite un lecteur FIPS ou SED comme étant rompu si vous perdez définitivement les clés d'authentification pour lui et que vous ne pouvez pas les récupérer du serveur KMIP. Bien que vous ne puissiez pas accéder ou récupérer les données sur le disque, vous pouvez prendre des mesures pour rendre à nouveau disponible l'espace inutilisé de SED pour les données.

Avant de commencer

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

Description de la tâche

Vous ne devez utiliser ce processus que si vous êtes certain que les clés d'authentification du lecteur FIPS ou SED sont définitivement perdues et que vous ne pouvez pas les récupérer.

Si les disques sont partitionnés, ils doivent d'abord être départitionnés avant que vous ne puissiez démarrer ce processus.

> La commande permettant de départitionner un disque est uniquement disponible au niveau diagnostic et ne doit être effectuée qu'avec NetApp support supervision. **Il est fortement recommandé de contacter le support NetApp avant de continuer.** vous pouvez également consulter l'article de la base de connaissances "Comment départitionner un lecteur de réserve dans ONTAP".

Étapes

1. Renvoyez un lecteur FIPS ou SED au service :

Si le SEDS est…	Procédez comme suit…

Pas en mode de conformité FIPS, ni en mode de conformité FIPS et la clé FIPS est disponible	a. Définissez le niveau de privilège sur avancé :
	`set -privilege advanced`
	b. Réinitialisez la clé FIPS sur l'ID sécurisé de fabrication par défaut 0x0 :
	`storage encryption disk modify -fips-key-id 0x0 -disk` *`disk_id`*
	c. Vérifiez que l'opération a réussi :
	`storage encryption disk show-status`
	Si l'opération a échoué, utilisez le processus PSID dans cette rubrique.
	d. Procédez au nettoyage du disque défaillant :
	`storage encryption disk sanitize -disk` *`disk_id`*
	Vérifiez que l'opération a réussi avec la commande `storage encryption disk show-status` avant de passer à l'étape suivante.
	e. Éliminez la panne du disque désinfecté :
	`storage disk unfail -spare true -disk` *`disk_id`*
	f. Vérifiez si le disque est propriétaire :
	`storage disk show -disk` *`disk_id`*
	
	Si le disque ne possède pas de propriétaire, attribuez-en un.
	`storage disk assign -owner node -disk` *`disk_id`*
	
	i. Entrez le nodeshell pour le nœud qui possède les disques à désinfecter :
	
	`system node run -node` *`node_name`*
	
	Exécutez le `disk sanitize release` commande.
	g. Quittez le nodeshell. Éliminez à nouveau la panne du disque :
	`storage disk unfail -spare true -disk` *`disk_id`*
	h. Vérifier que le disque est désormais une pièce de rechange et prêt à être réutilisé dans un agrégat :
	`storage disk show -disk` *`disk_id`*

En mode FIPS-compliance, la clé FIPS n'est pas disponible et les disques SED ont un PSID imprimé sur l'étiquette	a. Procurez-vous le PSID du disque à partir de l'étiquette du disque. b. Définissez le niveau de privilège sur avancé : `set -privilege advanced` c. Réinitialise le disque en fonction des paramètres configurés en usine : `storage encryption disk revert-to-original-state -disk` *`disk_id`* `-psid` *`disk_physical_secure_id`* Vérifiez que l'opération a réussi avec la commande `storage encryption disk show-status` avant de passer à l'étape suivante. d. Si vous utilisez ONTAP 9.8P5 ou une version antérieure, passez à l'étape suivante. Si vous exécutez ONTAP 9.8P6 ou une version ultérieure, éliminez la panne du disque désinfecté. `storage disk unfail -disk` *`disk_id`* e. Vérifiez si le disque est propriétaire : `storage disk show -disk` *`disk_id`* Si le disque ne possède pas de propriétaire, attribuez-en un. `storage disk assign -owner node -disk` *`disk_id`* i. Entrez le nodeshell pour le nœud qui possède les disques à désinfecter : `system node run -node` *`node_name`* Exécutez le `disk sanitize release` commande. f. Quittez le nodeshell. Éliminez à nouveau la panne du disque : `storage disk unfail -spare true -disk` *`disk_id`* g. Vérifier que le disque est désormais une pièce de rechange et prêt à être réutilisé dans un agrégat : `storage disk show -disk` *`disk_id`*

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

Retournez un lecteur FIPS ou SED en mode non protégé

Un lecteur FIPS ou SED est protégé contre les accès non autorisés uniquement si l'ID de clé d'authentification du nœud est défini sur une valeur autre que la valeur par défaut. Vous pouvez rétablir un lecteur FIPS ou SED en mode non protégé à l'aide de la `storage encryption disk modify` Commande pour définir l'ID de clé sur la valeur par défaut.

Si une paire haute disponibilité utilise des disques avec cryptage SAS ou NVMe (SED, NSE, FIPS), vous devez suivre cette procédure pour tous les disques de la paire haute disponibilité avant d'initialiser le système (options de démarrage 4 ou 9). Si vous ne le faites pas, vous risquez de subir des pertes de données si les disques sont requalifiés.

Avant de commencer

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

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Si un lecteur FIPS est exécuté en mode FIPS-Compliance, définissez l'ID de clé d'authentification FIPS du nœud sur le MSID 0x0 par défaut :

   ```
   storage encryption disk modify -disk disk_id -fips-key-id 0x0
   ```

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

   ```
   cluster1::> storage encryption disk modify -disk 2.10.11 -fips-key-id
   0x0

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

   Confirmer la réussite de l'opération à l'aide de la commande :

   ```
   storage encryption disk show-status
   ```

   Répétez la commande show-status jusqu'à ce que les chiffres de "disques commencés" et de "disques réalisés" soient identiques.

   ```
   cluster1:: storage encryption disk show-status

               FIPS    Latest   Start                Execution   Disks
   Disks Disks
   Node        Support Request  Timestamp            Time (sec)  Begun
   Done  Successful
   -------     ------- -------- ------------------   ---------- ------
   ------  ----------
   cluster1    true    modify   1/18/2022 15:29:38    3           14     5
   5
   1 entry was displayed.
   ```

3. Définissez à nouveau l'ID de clé d'authentification des données du nœud sur le MSID 0x0 par défaut :

   ```
   storage encryption disk modify -disk disk_id -data-key-id 0x0
   ```

   La valeur de `-data-key-id` Doit être défini sur 0x0 si vous retournez un disque SAS ou NVMe en mode non protégé.

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

```
cluster1::> storage encryption disk modify -disk 2.10.11 -data-key-id
0x0

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

Confirmer la réussite de l'opération à l'aide de la commande :

```
storage encryption disk show-status
```

Répétez la commande show-status jusqu'à ce que les chiffres soient identiques. L'opération est terminée lorsque les numéros dans "disques commencés" et "disques terminés" sont les mêmes.

Mode Maintenance

Depuis ONTAP 9.7, vous pouvez ressaisir un disque FIPS à partir du mode de maintenance. Si vous ne pouvez pas utiliser les instructions de l'interface de ligne de commandes ONTAP décrites dans la section précédente, vous devez utiliser le mode de maintenance.

Étapes

1. Définissez à nouveau l'ID de clé d'authentification FIPS du nœud sur le MSID 0x0 par défaut :

   `disk encrypt rekey_fips 0x0 *disklist*`

2. Définissez à nouveau l'ID de clé d'authentification des données du nœud sur le MSID 0x0 par défaut :

   `disk encrypt rekey 0x0 *disklist*`

3. Vérifiez que la clé d'authentification FIPS a bien été reclés :

   `disk encrypt show_fips`

4. Confirmer que la clé d'authentification des données a bien été reclés avec :

   `disk encrypt show`

   Votre sortie affichera probablement soit l'ID de clé MSID 0x0 par défaut, soit la valeur de 64 caractères détenue par le serveur de clés. Le `Locked?` ce champ fait référence au verrouillage des données.

```
Disk       FIPS Key ID                 Locked?
---------- --------------------------- -------
0a.01.0    0x0                          Yes
```

Supprimez une connexion externe au gestionnaire de clés

Si vous n'avez plus besoin du serveur, vous pouvez déconnecter un serveur KMIP d'un

nœud. Par exemple, vous pouvez déconnecter un serveur KMIP lorsque vous passez au chiffrement de volume.

Description de la tâche

Lorsque vous déconnectez un serveur KMIP d'un nœud d'une paire haute disponibilité, le système déconnecte automatiquement le serveur de tous les nœuds du cluster.

> Si vous prévoyez de continuer à utiliser la gestion externe des clés après la déconnexion d'un serveur KMIP, assurez-vous qu'un autre serveur KMIP est disponible pour assurer le service des clés d'authentification.

Avant de commencer

Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.

Étape

1. Déconnectez un serveur KMIP du nœud actuel :

Pour cette version ONTAP…	Utilisez cette commande…
ONTAP 9.6 et versions ultérieures	`security key-manager external remove-servers -vserver SVM -key -servers host_name
IP_address:port,…`	ONTAP 9.5 et versions antérieures

   Dans un environnement MetroCluster, il faut répéter ces commandes sur les deux clusters pour le SVM admin.

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

   La commande ONTAP 9.6 suivante désactive les connexions à deux serveurs de gestion des clés externes pour `cluster1`, le premier nommé `ks1`, Écoute sur le port par défaut 5696, le second avec l'adresse IP 10.0.0.20, écoute sur le port 24482 :

```
clusterl::> security key-manager external remove-servers -vserver
cluster-1 -key-servers ks1,10.0.0.20:24482
```

Modifiez les propriétés du serveur de gestion externe des clés

À partir de ONTAP 9.6, vous pouvez utiliser le `security key-manager external modify-server` Commande permettant de modifier le délai d'attente d'E/S et le nom d'utilisateur d'un serveur de gestion de clés externe.

Avant de commencer

- Pour effectuer cette tâche, vous devez être un administrateur de cluster ou de SVM.
- Des privilèges avancés sont requis pour cette tâche.
- Dans un environnement MetroCluster, vous devez répéter ces étapes sur les deux clusters pour la SVM d'administration.

Étapes

1. Sur le système de stockage, passez au niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

2. Modifiez les propriétés externes du serveur du gestionnaire de clés pour le cluster :

   ```
   security key-manager external modify-server -vserver admin_SVM -key-server
   host_name|IP_address:port,… -timeout 1…60 -username user_name
   ```

   > La valeur de temporisation est exprimée en secondes. Si vous modifiez le nom d'utilisateur, vous êtes invité à entrer un nouveau mot de passe. 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 de cluster pour modifier les propriétés du serveur du gestionnaire de clés externe.

   La commande suivante remplace la valeur de temporisation par 45 secondes pour le `cluster1` serveur de gestion externe des clés à l'écoute sur le port par défaut 5696 :

   ```
   clusterl::> security key-manager external modify-server -vserver
   cluster1 -key-server ks1.local -timeout 45
   ```

3. Modifier les propriétés du serveur gestionnaire de clés externe pour un SVM (NVE uniquement) :

   ```
   security key-manager external modify-server -vserver SVM -key-server
   host_name|IP_address:port,… -timeout 1…60 -username user_name
   ```

   > La valeur de temporisation est exprimée en secondes. Si vous modifiez le nom d'utilisateur, vous êtes invité à entrer un nouveau mot de passe. Si vous exécutez la commande à l'invite de connexion du SVM, *`SVM`* Par défaut au SVM actuel Vous devez être l'administrateur du cluster ou de SVM pour modifier les propriétés du serveur externe Key Manager.

   La commande suivante modifie le nom d'utilisateur et le mot de passe de `svm1` serveur de gestion externe des clés à l'écoute sur le port par défaut 5696 :

   ```
   svml::> security key-manager external modify-server -vserver svm11 -key
   -server ks1.local -username svm1user
   Enter the password:
   Reenter the password:
   ```

4. Répétez la dernière étape pour tout SVM supplémentaire.

Transition vers la gestion externe des clés à partir de la gestion intégrée des clés

Pour basculer de la gestion externe des clés à partir de la gestion intégrée des clés, vous devez supprimer la configuration intégrée de la gestion des clés avant de pouvoir activer la gestion externe des clés.

Avant de commencer

- Pour le chiffrement matériel, vous devez réinitialiser les clés de données de tous les lecteurs FIPS ou SED à la valeur par défaut.

  "Retour d'un lecteur FIPS ou SED en mode non protégé"

- Pour le chiffrement logiciel, vous devez déchiffrer tous les volumes.

  "Sans chiffrement des données de volume"

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

Étape

1. Supprimez la configuration intégrée de gestion des clés d'un cluster :

Pour cette version ONTAP…	Utilisez cette commande…
ONTAP 9.6 et versions ultérieures	`security key-manager onboard disable -vserver SVM`
ONTAP 9.5 et versions antérieures	`security key-manager delete-key-database`

Pour obtenir la syntaxe complète de la commande, reportez-vous à la "Référence de commande ONTAP".

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

Pour basculer vers la gestion intégrée des clés à partir d'une gestion externe des clés, vous devez supprimer la configuration de gestion externe des clés pour pouvoir activer la gestion intégrée des clés.

Avant de commencer

- Pour le chiffrement matériel, vous devez réinitialiser les clés de données de tous les lecteurs FIPS ou SED à la valeur par défaut.

  "Retour d'un lecteur FIPS ou SED en mode non protégé"

- Vous devez avoir supprimé toutes les connexions externes du gestionnaire de clés.

  "Suppression d'une connexion externe au gestionnaire de clés"

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

Procédure

La procédure de transition de la gestion des clés dépend de la version de ONTAP que vous utilisez.

ONTAP 9.6 et versions ultérieures

1. Changement au niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

2. Utiliser la commande :

   ```
   security key-manager external disable -vserver admin_SVM
   ```

   > Dans un environnement MetroCluster, il faut répéter la commande sur les deux clusters pour la SVM admin.

ONTAP 9.5 et versions antérieures

Utiliser la commande :
`security key-manager delete-kmip-config`

Que se passe-t-il lorsque les serveurs de gestion des clés ne sont pas accessibles lors du processus de démarrage

ONTAP prend certaines précautions afin d'éviter tout comportement indésirable dans l'éventualité où un système de stockage configuré pour NSE ne puisse pas atteindre l'un des serveurs de gestion des clés spécifiés lors du processus de démarrage.

Si le système de stockage est configuré pour NSE, les disques SED sont de nouveau et verrouillés, et les disques SED sont sous tension, le système de stockage doit récupérer les clés d'authentification requises à partir des serveurs de gestion des clés pour s'authentifier auprès des disques SED avant qu'ils puissent accéder aux données.

Le système de stockage tente de contacter les serveurs de gestion des clés spécifiés pendant jusqu'à trois heures. Si le système de stockage ne peut pas atteindre l'un d'eux après ce délai, le processus d'amorçage s'arrête et le système de stockage s'arrête.

Si le système de stockage contacte avec succès un serveur de gestion de clés spécifié, il tente alors d'établir une connexion SSL pendant 15 minutes. Si le système de stockage ne parvient pas à établir de connexion SSL avec un serveur de gestion de clés spécifié, le processus d'amorçage s'arrête et le système de stockage s'arrête.

Pendant que le système de stockage tente de contacter et de se connecter aux serveurs de gestion des clés, il affiche des informations détaillées sur les tentatives de contact ayant échoué au niveau de l'interface de ligne de commande. Vous pouvez interrompre les tentatives de contact à tout moment en appuyant sur Ctrl-C.

Par mesure de sécurité, les disques SED ne permettent qu'un nombre limité de tentatives d'accès non autorisées, après quoi ils désactivent l'accès aux données existantes. Si le système de stockage ne peut pas contacter les serveurs de gestion des clés spécifiés pour obtenir les clés d'authentification appropriées, il peut uniquement tenter de s'authentifier auprès de la clé par défaut, ce qui entraîne une tentative d'échec et un incident. Si le système de stockage est configuré pour redémarrer automatiquement en cas de panique, il entre dans une boucle d'amorçage qui entraîne des tentatives d'authentification continues sur les disques SED ayant échoué.

Dans ces scénarios, l'arrêt du système de stockage a été conçu pour éviter que le système de stockage ne

pénètre dans une boucle d'amorçage et qu'il puisse y avoir des pertes de données inattendues suite au verrouillage permanent des disques SED, raison du dépassement de la limite de sécurité d'un certain nombre de tentatives d'authentification consécutives ayant échoué. La limite et le type de protection de verrouillage dépendent des spécifications de fabrication et du type de SED :

Type SED	Nombre de tentatives d'authentification consécutives ayant échoué entraînant un blocage	Type de protection de verrouillage lorsque la limite de sécurité est atteinte
DISQUES DURS	1024	Permanent. Les données ne peuvent pas être restaurées, même si la clé d'authentification appropriée est à nouveau disponible.
X440_PHM2800MCTO SSD NSE 800 Go avec révisions du firmware NA00 ou NA01	5	Temporaire. Le verrouillage est activé uniquement jusqu'à ce que le disque soit mis hors/sous tension.
X577_PHM2800MNA00 SSD NSE 800 Go avec révisions de firmware ou NA01	5	Temporaire. Le verrouillage est activé uniquement jusqu'à ce que le disque soit mis hors/sous tension.
X440_PHM2800MCTO SSD NSE 800 Go avec révisions de firmware plus élevées	1024	Permanent. Les données ne peuvent pas être restaurées, même si la clé d'authentification appropriée est à nouveau disponible.
X577_PHM2800MCTO SSD NSE 800 Go avec révisions de micrologiciel plus élevées	1024	Permanent. Les données ne peuvent pas être restaurées, même si la clé d'authentification appropriée est à nouveau disponible.
Tous les autres modèles de SSD	1024	Permanent. Les données ne peuvent pas être restaurées, même si la clé d'authentification appropriée est à nouveau disponible.

Pour tous les types SED, une authentification réussie réinitialise le nombre d'essayer à zéro.

Si vous rencontrez ce scénario lorsque le système de stockage est arrêté en raison d'un échec d'accès aux serveurs de gestion de clés spécifiés, vous devez d'abord identifier et corriger la cause de l'échec de communication avant de poursuivre le démarrage du système de stockage.

Désactiver le chiffrement par défaut

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. Si nécessaire, vous pouvez désactiver le chiffrement par défaut pour l'ensemble du cluster.

Avant de commencer

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.

Étape

1. Pour désactiver le chiffrement par défaut pour l'ensemble du cluster dans ONTAP 9.7 ou version ultérieure, exécutez la commande suivante :

   ```
   options -option-name encryption.data_at_rest_encryption.disable_by_default
   -option-value on
   ```