Configurez la gestion intégrée des clés

ONTAP 9

NetApp
September 12, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/ontap/encryption-at-rest/enable-onboard-key-management-96-later-nse-task.html on September 12, 2024. Always check docs.netapp.com for the latest.

Sommaire

Configurez la gestion intégrée des clés 1
Activez la gestion intégrée des clés dans ONTAP 9.6 et versions ultérieures 1
Activez la gestion intégrée des clés dans ONTAP 9.5 et versions antérieures 4
Attribution d'une clé d'authentification des données à un lecteur FIPS ou SED (gestion des clés intégrée) . 6

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

       Vserver: cluster1
   Key Manager: onboard
          Node: node2

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001006f4e2513353a674305872a4c9f3bf79700000000
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
   00000000000000000200000000000010019215b9738bc7b43d4698c80246db1f4

   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
   00000000000000000200000000000010019215b9738bc7b43d4698c80246db1f4
   0.0.1   data
   00000000000000000200000000000010059851742AF2703FC91369B7DB47C4722
   [...]
   ```

Informations sur le copyright

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

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

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

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

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

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

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

Informations sur les marques commerciales

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