Étape 6. Terminez la mise à niveau

Upgrade controllers

NetApp
July 05, 2024

Sommaire

Étape 6. Terminez la mise à niveau

Présentation de la phase 6

Lors de la phase 6, vous vérifiez que les nouveaux nœuds sont correctement configurés et que, si les nouveaux nœuds sont activés pour le chiffrement, vous configurez et configurez Storage Encryption ou NetApp Volume Encryption. Vous devez également désaffecter les anciens nœuds et reprendre les opérations SnapMirror.

Étapes

1. "Gérez l'authentification à l'aide de serveurs KMIP"
2. "Vérifiez que les nouveaux contrôleurs sont correctement configurés"
3. "Configurez Storage Encryption sur le nouveau module de contrôleur"
4. "Configurez NetApp Volume Encryption ou Aggregate Encryption sur le nouveau module de contrôleur"
5. "Désaffectation de l'ancien système"
6. "Reprendre les opérations SnapMirror"

Gérez l'authentification à l'aide de serveurs KMIP

Vous pouvez utiliser les serveurs KMIP (Key Management Interoperability Protocol) pour gérer les clés d'authentification.

Étapes

1. Ajout d'un nouveau contrôleur :

   ```
   security key-manager external enable
   ```

2. Ajouter le gestionnaire de clés :

   ```
   security key-manager external add-servers -key-servers
   key_management_server_ip_address
   ```

3. Vérifier que les serveurs de gestion des clés sont configurés et disponibles pour tous les nœuds du cluster :

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

4. Restaurez les clés d'authentification de tous les serveurs de gestion de clés liés vers le nouveau nœud :

   ```
   security key-manager external restore -node new_controller_name
   ```

Vérifiez que les nouveaux contrôleurs sont correctement configurés

Pour confirmer la configuration correcte, vous devez activer la paire HA. Vous devez également vérifier que les nœuds 3 et Node4 ne sont pas en mesure d'accéder aux

systèmes de stockage des autres et que les LIF de données ne sont pas membres du cluster. Vous devez également confirmer que le nœud 3 est propriétaire des agrégats du nœud 1 et que le nœud 4 est propriétaire des agrégats du nœud 2, et que les volumes des deux nœuds sont en ligne.

Étapes

1. Après la vérification du post-nœud 2, le basculement du stockage et la paire HA du cluster pour le cluster node 2 sont activés. Lorsque l'opération est effectuée, les deux nœuds indiquent que l'opération est terminée et le système effectue certaines opérations de nettoyage.
2. Vérifiez que le basculement du stockage est activé :

   ```
   storage failover show
   ```

   L'exemple suivant montre la sortie de la commande lorsque le basculement du stockage est activé :

   ```
   cluster::> storage failover show
                       Takeover
   Node     Partner  Possible   State Description
   -------- -----    -------    ------------------
   node3    node4    true       Connected to node4
   node4    node3    true       Connected to node3
   ```

3. Vérifiez que les nœuds 3 et 4 appartiennent au même cluster à l'aide de la commande suivante et en examinant le résultat :

   ```
   cluster show
   ```

4. Vérifiez que les nœuds 3 et Node4 peuvent accéder mutuellement au stockage, à l'aide de la commande suivante et en examinant le résultat :

   ```
   storage failover show -fields local-missing-disks, partner-missing-disks
   ```

5. Vérifiez que les nœuds 3 et NODE4 ne possèdent pas de LIF de données détenues par d'autres nœuds du cluster à l'aide de la commande suivante et en examinant la sortie.

   ```
   network interface show
   ```

   Si les LIF de données des nœuds 3 ou 4 ne sont pas propriétaires de LIF de données détenues par d'autres nœuds du cluster, restaurez-les au propriétaire de leur domicile :

   ```
   network interface revert
   ```

6. Vérifiez que le nœud 3 possède les agrégats du nœud 1 et que le nœud 4 est propriétaire des agrégats du nœud 2 :

   ```
   storage aggregate show -owner-name <node3>
   ```

   ```
   storage aggregate show -owner-name <node4>
   ```

7. Déterminez si des volumes sont hors ligne :

```
volume show -node <node3> -state offline

volume show -node <node4> -state offline
```

8. Si des volumes sont hors ligne, comparez-les avec la liste des volumes hors ligne que vous avez capturés dans la section "Préparer les nœuds pour une mise à niveau", et de mettre en ligne l'un des volumes hors ligne, si nécessaire, à l'aide de la commande suivante, une fois pour chaque volume :

   ```
   volume online -vserver <vserver_name> -volume <volume_name>
   ```

9. Installez les nouvelles licences pour les nouveaux nœuds à l'aide de la commande suivante pour chaque nœud :

   ```
   system license add -license-code <license_code,license_code,license_code…>
   ```

   Le paramètre License-code accepte une liste de 28 clés de caractères alphabétiques majuscules. Vous pouvez ajouter une licence à la fois ou ajouter plusieurs licences à la fois, en séparant chaque clé de licence par une virgule.

10. Supprimez toutes les anciennes licences des nœuds d'origine à l'aide de l'une des commandes suivantes :

    ```
    system license clean-up -unused -expired

    system license delete -serial-number <node_serial_number> -package
    <licensable_package>
    ```

    - Supprimer toutes les licences expirées :

      ```
      system license clean-up -expired
      ```

    - Supprimer toutes les licences inutilisées :

      ```
      system license clean-up -unused
      ```

    - Supprimez une licence spécifique d'un cluster à l'aide des commandes suivantes sur les nœuds :

      ```
      system license delete -serial-number <node1_serial_number> -package *

      system license delete -serial-number <node2_serial_number> -package *
      ```

    Les valeurs de sortie suivantes sont affichées :

    ```
    Warning: The following licenses will be removed:
    <list of each installed package>
    Do you want to continue? {y|n}: y
    ```

    Entrez `y` pour supprimer tous les paquets.

11. Vérifiez que les licences sont correctement installées à l'aide de la commande suivante et en examinant le résultat :

```
system license show
```

Vous pouvez comparer la sortie avec la sortie capturée dans la section "Préparer les nœuds pour une mise à niveau".

12. si des lecteurs auto-cryptés sont utilisés dans la configuration et que vous avez défini la `kmip.init.maxwait` variable sur `off` (par exemple, dans "Installez et démarrez node4, étape 24"), vous devez annuler la définition de la variable :

```
set diag; systemshell -node <node_name> -command sudo kenv -u -p
kmip.init.maxwait
```

13. [[étape 13]]configurez les SP à l'aide de la commande suivante sur les deux nœuds :

```
system service-processor network modify -node <node_name>
```

Reportez-vous à la section "Références" Pour accéder à *System Administration Reference* pour obtenir des informations sur les processeurs de stockage et les *ONTAP 9.8 Commands: Manual page Reference* pour obtenir des informations détaillées sur le système `service-processor network modify` commande.

14. Pour configurer un cluster sans commutateur sur les nouveaux nœuds, reportez-vous à la section "Références" Pour établir un lien vers le site de support *NetApp* et suivre les instructions de la section *transition vers un cluster* sans commutateur à deux nœuds_.

Une fois que vous avez terminé

Si le cryptage du stockage est activé sur les nœuds 3 et 4, complétez la section "Configurez Storage Encryption sur le nouveau module de contrôleur". Sinon, complétez la section "Désaffectation de l'ancien système".

Configurez Storage Encryption sur le nouveau module de contrôleur

Si le contrôleur remplacé ou le partenaire de haute disponibilité du nouveau contrôleur utilise Storage Encryption, vous devez configurer le nouveau module de contrôleur pour Storage Encryption, y compris l'installation de certificats SSL et la configuration de serveurs de gestion des clés.

Description de la tâche

Cette procédure comprend les étapes réalisées sur le nouveau module de contrôleur. Vous devez saisir la commande sur le nœud approprié.

Étapes

1. Vérifier que les serveurs de gestion des clés sont toujours disponibles, leur état et leurs informations de clé d'authentification :

```
security key-manager external show-status

security key-manager onboard show-backup
```

2. Ajoutez les serveurs de gestion des clés répertoriés à l'étape précédente à la liste des serveurs de gestion des clés du nouveau contrôleur.

a. Ajouter le serveur de gestion des clés :

```
security key-manager external add-servers -key-servers
key_management_server_ip_address
```

b. Répétez l'étape précédente pour chaque serveur de gestion des clés répertorié. Vous pouvez lier jusqu'à quatre serveurs de gestion des clés.

c. Vérifiez que les serveurs de gestion des clés ont été ajoutés correctement :

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

3. Sur le nouveau module de contrôleur, exécutez l'assistant de configuration de la gestion des clés pour configurer et installer les serveurs de gestion des clés.

   Vous devez installer les mêmes serveurs de gestion des clés que ceux installés sur le module de contrôleur existant.

   a. Lancez l'assistant de configuration du serveur de gestion des clés sur le nouveau nœud :

   ```
   security key-manager external enable
   ```

   b. Suivez les étapes de l'assistant pour configurer les serveurs de gestion des clés.

4. Restaurer les clés d'authentification de tous les serveurs de gestion des clés liés vers le nouveau nœud :

   ```
   security key-manager external restore -node new_controller_name
   ```

Configurez NetApp Volume Encryption ou Aggregate Encryption sur le nouveau module de contrôleur

Si le remplacement du contrôleur ou du partenaire HA (haute disponibilité) du nouveau contrôleur utilise NetApp Volume Encryption (NVE) ou NetApp Aggregate Encryption (NAE), il faut configurer le nouveau module de contrôleur pour NVE ou NAE.

Description de la tâche

Cette procédure comprend les étapes réalisées sur le nouveau module de contrôleur. Vous devez saisir la commande sur le nœud approprié.

Gestionnaire de clés intégré

Configurez NVE ou NAE à l'aide du Gestionnaire de clés intégré.

Étapes

1. Restaurer les clés d'authentification de tous les serveurs de gestion des clés liés vers le nouveau nœud :

   ```
   security key-manager onboard sync
   ```

Gestion externe des clés

Configurez NVE ou NAE à l'aide de la gestion externe des clés.

Étapes

1. Vérifier que les serveurs de gestion des clés sont toujours disponibles, leur état et leurs informations de clé d'authentification :

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

2. Ajoutez les serveurs de gestion des clés répertoriés à l'étape précédente à la liste des serveurs de gestion des clés du nouveau contrôleur :

   a. Ajouter le serveur de gestion des clés :

      ```
      security key-manager external add-servers -key-servers
      key_management_server_ip_address
      ```

   b. Répétez l'étape précédente pour chaque serveur de gestion des clés répertorié. Vous pouvez lier jusqu'à quatre serveurs de gestion des clés.

   c. Vérifiez que les serveurs de gestion des clés ont été ajoutés correctement :

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

3. Sur le nouveau module de contrôleur, exécutez l'assistant de configuration de la gestion des clés pour configurer et installer les serveurs de gestion des clés.

   Vous devez installer les mêmes serveurs de gestion des clés que ceux installés sur le module de contrôleur existant.

   a. Lancez l'assistant de configuration du serveur de gestion des clés sur le nouveau nœud :

      ```
      security key-manager external enable
      ```

   b. Suivez les étapes de l'assistant pour configurer les serveurs de gestion des clés.

4. Restaurer les clés d'authentification de tous les serveurs de gestion des clés liés vers le nouveau nœud :

   ```
   security key-manager external restore
   ```

   Cette commande a besoin de la phrase de passe OKM

   Pour plus d'informations, consultez l'article de la base de connaissances "Restauration de la configuration du serveur de gestionnaire de clés externe à partir du menu de démarrage ONTAP".

Une fois que vous avez terminé

Vérifiez si des volumes ont été mis hors ligne car les clés d'authentification n'étaient pas disponibles ou si les serveurs EKM n'ont pas pu être atteints. Remettre ces volumes en ligne à l'aide du `volume online` commande.

Désaffectation de l'ancien système

Une fois la mise à niveau effectuée, vous pouvez désaffecter l'ancien système via le site de support NetApp. Hors fonctionnement du système dit à NetApp que le système n'est plus opérationnel et qu'il l'supprime des bases de données de prise en charge.

Étapes

1. Reportez-vous à la section "Références" Pour accéder au *site de support NetApp* et connectez-vous.
2. Sélectionnez **produits > Mes produits** dans le menu.
3. Sur la page **Afficher les systèmes installés**, choisissez les **critères de sélection** que vous souhaitez utiliser pour afficher des informations sur votre système.

   Vous pouvez choisir l'une des options suivantes pour localiser votre système :

   - Numéro de série (situé à l'arrière de l'appareil)
   - Numéros de série pour mon emplacement
4. Sélectionnez **Go!**

   Un tableau affiche les informations sur le cluster, y compris les numéros de série.
5. Localisez le cluster dans le tableau et sélectionnez **Decommission This system** dans le menu déroulant Product Tool Set.

Reprendre les opérations SnapMirror

Vous pouvez reprendre les transferts SnapMirror suspendus avant de mettre à niveau et reprendre les relations SnapMirror. Les mises à jour sont planifiées une fois la mise à niveau terminée.

Étapes

1. Vérifier le statut SnapMirror sur la destination :

   ```
   snapmirror show
   ```
2. Reprendre la relation SnapMirror :

   ```
   snapmirror resume -destination-vserver vserver_name
   ```

Informations sur le copyright

Informations sur les marques commerciales