Etapa 6. Complete la actualización

Upgrade controllers

NetApp
July 05, 2024

Tabla de contenidos

Etapa 6. Complete la actualización

Descripción general de la etapa 6

Durante la fase 6, el usuario confirma que los nodos nuevos están configurados correctamente y, si los nodos nuevos tienen la función de cifrado habilitada, se configuran y se configuran el cifrado de almacenamiento o el cifrado de volúmenes de NetApp. También debe retirar los nodos antiguos y reanudar las operaciones de SnapMirror.

Pasos

1. "Gestionar la autenticación mediante servidores KMIP"
2. "Confirmar que las nuevas controladoras están configuradas correctamente"
3. "Configure Storage Encryption en el nuevo módulo de la controladora"
4. "Configure el cifrado de volúmenes de NetApp o el cifrado de agregados en el nuevo módulo de la controladora"
5. "Retire el sistema antiguo"
6. "Reanudar las operaciones de SnapMirror"

Gestionar la autenticación mediante servidores KMIP

Es posible usar servidores de protocolo de interoperabilidad de gestión de claves (KMIP) para gestionar las claves de autenticación.

Pasos

1. Añadir una nueva controladora:

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

2. Añada el gestor de claves:

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

3. Verifique que los servidores de gestión de claves estén configurados y disponibles para todos los nodos del clúster:

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

4. Restaure las claves de autenticación de todos los servidores de gestión de claves vinculados al nuevo nodo:

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

Confirmar que las nuevas controladoras están configuradas correctamente

Para confirmar la configuración correcta, debe habilitar la pareja de ha. También es necesario verificar que los nodos 3 y 4 pueden acceder al almacenamiento de cada uno de los demás y que ninguno de los dos posee LIF de datos que pertenecen a otros nodos del clúster. Además, debe confirmar que el nodo 3 tiene agregados del nodo 1 y que el nodo 4 tiene agregados del nodo 2, y que los volúmenes de ambos nodos están en línea.

Pasos

1. Después de las comprobaciones posteriores al nodo 2, se habilitan la conmutación por error de almacenamiento y la pareja de alta disponibilidad de clúster para el clúster 2. Una vez finalizada la operación, ambos nodos muestran como completados y el sistema realiza algunas operaciones de limpieza.
2. Compruebe que la recuperación tras fallos del almacenamiento está activada:

   ```
   storage failover show
   ```

   En el ejemplo siguiente se muestra el resultado del comando cuando la conmutación por error del almacenamiento está habilitada:

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

3. Verifique que los nodos 3 y 4 pertenezcan al mismo clúster mediante el siguiente comando y examinando el resultado:

   ```
   cluster show
   ```

4. Verifique que los nodos 3 y 4 puedan acceder al almacenamiento de los demás mediante el siguiente comando y examinando el resultado:

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

5. Verifique que ni el nodo 3 ni el nodo 4 sean propiedad de las LIF de datos propias del hogar de otros nodos del clúster. Para ello, utilice el siguiente comando y examine la salida:

   ```
   network interface show
   ```

   Si ni el nodo 3 ni el nodo 4 son propiedad de los LIF de datos propiedad del hogar de otros nodos del clúster, revierte las LIF de datos a su propietario doméstico:

   ```
   network interface revert
   ```

6. Verifique que el nodo 3 tenga los agregados del nodo 1 y que el nodo 4 sea propietario de los agregados del nodo 2:

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

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

7. Determine si alguno de los volúmenes está sin conexión:

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

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

8. Si alguno de los volúmenes se encuentra sin conexión, compárelo con la lista de volúmenes sin conexión que ha capturado en la sección "Prepare los nodos para la actualización", y conectar cualquiera de los volúmenes sin conexión, según sea necesario, mediante el siguiente comando, una vez para cada volumen:

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

9. Instale licencias nuevas para los nodos nuevos mediante el siguiente comando para cada nodo:

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

   El parámetro license-code acepta una lista de 28 claves de caracteres alfabéticos en mayúsculas. Puede añadir una licencia cada vez, o bien puede añadir varias licencias a la vez, separando cada clave de licencia por una coma.

10. Quite todas las licencias antiguas de los nodos originales mediante uno de los siguientes comandos:

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

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

    - Eliminar todas las licencias caducadas:

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

    - Elimine todas las licencias no utilizadas:

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

    - Elimine una licencia específica de un clúster mediante los siguientes comandos en los nodos:

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

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

    Se muestra la siguiente salida:

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

Introduzca `y` para eliminar todos los paquetes.

11. Compruebe que las licencias se han instalado correctamente mediante el siguiente comando y examine el resultado:

    `system license show`

    Puede comparar la salida con la que ha capturado en la sección "Prepare los nodos para la actualización".

12. Si se están utilizando unidades de autocifrado en la configuración y se ha establecido la `kmip.init.maxwait` variable en `off` (por ejemplo, en "Instale y arranque el nodo 4, Paso 24"), debe anular la definición de la variable:

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

13. Configure los SPS utilizando el siguiente comando en ambos nodos:

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

    Consulte "Referencias" Para establecer un vínculo a la *referencia de administración del sistema* para obtener información sobre los SPS y los comandos *ONTAP 9.8: Referencia de página del manual* para obtener información detallada sobre el sistema `service-processor network modify` comando.

14. Si desea configurar un clúster sin switches en los nuevos nodos, consulte "Referencias" Para establecer un enlace al *sitio de soporte de NetApp* y siga las instrucciones que se indican en *Cambiar a un clúster sin switch de dos nodos*.

Después de terminar

Si el cifrado del almacenamiento está habilitado en los nodos 3 y 4, complete la sección "Configure Storage Encryption en el nuevo módulo de la controladora". De lo contrario, complete la sección "Retire el sistema antiguo".

Configure Storage Encryption en el nuevo módulo de la controladora

Si la controladora reemplazada o el asociado de alta disponibilidad de la nueva controladora utilizan Storage Encryption, debe configurar el nuevo módulo de controlador para Storage Encryption, que incluye la instalación de certificados SSL y la configuración de servidores de administración de claves.

Acerca de esta tarea

Este procedimiento incluye los pasos que se realizan en el nuevo módulo del controlador. Debe introducir el comando en el nodo correcto.

Pasos

1. Compruebe que los servidores de gestión de claves aún estén disponibles, su estado y la información de la clave de autenticación:

   ```
   security key-manager external show-status

   security key-manager onboard show-backup
   ```

2. Añada los servidores de gestión de claves que se enumeran en el paso anterior a la lista del servidor de gestión de claves de la nueva controladora.
   a. Añada el servidor de gestión de claves:

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

   b. Repita el paso anterior para cada servidor de gestión de claves enumerado. Puede vincular hasta cuatro servidores de gestión de claves.
   c. Compruebe que los servidores de gestión de claves se han añadido correctamente:

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

3. En el nuevo módulo de controlador, ejecute el asistente de configuración de gestión de claves para configurar e instalar los servidores de gestión de claves.

   Debe instalar los mismos servidores de gestión de claves que se instalan en el módulo de controladora existente.

   a. Inicie el asistente de configuración del servidor de gestión de claves en el nuevo nodo:

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

   b. Complete los pasos del asistente para configurar los servidores de gestión de claves.
4. Restaure las claves de autenticación de todos los servidores de gestión de claves vinculados al nuevo nodo:

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

Configure el cifrado de volúmenes de NetApp o el cifrado de agregados en el nuevo módulo de la controladora

Si la controladora reemplazada o el partner de alta disponibilidad (ha) de la nueva controladora utilizan el cifrado de volúmenes de NetApp (NVE) o el cifrado de agregados de NetApp (NAE), debe configurar el nuevo módulo de controladoras para NVE o NAE.

Acerca de esta tarea

Este procedimiento incluye los pasos que se realizan en el nuevo módulo del controlador. Debe introducir el comando en el nodo correcto.

Gestión de claves incorporada

Configure NVE o NAE con el gestor de claves incorporado.

Pasos

1. Restaure las claves de autenticación de todos los servidores de gestión de claves vinculados al nuevo nodo:

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

Gestión de claves externas

Configure NVE o NAE mediante la gestión de claves externa.

Pasos

1. Compruebe que los servidores de gestión de claves aún estén disponibles, su estado y la información de la clave de autenticación:

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

2. Añada los servidores de gestión de claves que se enumeran en el paso anterior a la lista del servidor de gestión de claves de la nueva controladora:

   a. Añada el servidor de gestión de claves:

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

   b. Repita el paso anterior para cada servidor de gestión de claves enumerado. Puede vincular hasta cuatro servidores de gestión de claves.

   c. Compruebe que los servidores de gestión de claves se han añadido correctamente:

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

3. En el nuevo módulo de controlador, ejecute el asistente de configuración de gestión de claves para configurar e instalar los servidores de gestión de claves.

   Debe instalar los mismos servidores de gestión de claves que se instalan en el módulo de controladora existente.

   a. Inicie el asistente de configuración del servidor de gestión de claves en el nuevo nodo:

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

   b. Complete los pasos del asistente para configurar los servidores de gestión de claves.

4. Restaure las claves de autenticación de todos los servidores de gestión de claves vinculados al nuevo nodo:

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

   Este comando necesita la clave de acceso de OKM

   Para obtener más información, vea el artículo de la base de conocimientos "Cómo restaurar la configuración del servidor del administrador de claves externo desde el menú de arranque de

ONTAP".

Después de terminar

Compruebe si algún volumen se desconectó debido a que no había claves de autenticación disponibles o a que no se pudo acceder a los servidores EKM. Vuelva a conectar esos volúmenes en línea mediante el `volume online` comando.

Retire el sistema antiguo

Tras la actualización, puede retirar el sistema antiguo a través del sitio de soporte de NetApp. Decomisionando el sistema indica a NetApp que el sistema ya no está en funcionamiento y lo elimina de las bases de datos de soporte.

Pasos

1. Consulte "Referencias" Para enlazar con el *sitio de soporte de NetApp* e iniciar sesión.
2. Seleccione **Productos > Mis productos** en el menú.
3. En la página **Ver sistemas instalados**, elija los **criterios de selección** que desea utilizar para mostrar información sobre su sistema.

   Puede elegir una de las siguientes opciones para localizar su sistema:

   - Número de serie (situado en la parte posterior de la unidad)
   - Números de serie para Mi ubicación
4. Seleccione **Go!**

   Una tabla muestra información del clúster, incluidos los números de serie.
5. Localice el clúster en la tabla y seleccione **DECOMmission este sistema** en el menú desplegable Product Tool Set (conjunto de herramientas del producto).

Reanudar las operaciones de SnapMirror

Puede reanudar las transferencias de SnapMirror que se pusieron en modo inactivo antes de la actualización y reanudar las relaciones de SnapMirror. Las actualizaciones se programan una vez finalizada la actualización.

Pasos

1. Compruebe el estado de SnapMirror en el destino:

   ```
   snapmirror show
   ```
2. Reanude la relación de SnapMirror:

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

Información de copyright

Información de la marca comercial