Etapa 6. Complete la actualización

Upgrade controllers

NetApp
March 11, 2026

Tabla de contenidos

Etapa 6. Complete la actualización

Gestionar la autenticación mediante servidores KMIP

Con ONTAP 9.5 y versiones posteriores, se pueden utilizar 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 setup -node new_controller_name
   ```

2. Añada el gestor de claves:

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

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

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

Confirmar que las nuevas controladoras están configuradas correctamente

Para confirmar la configuración correcta, tiene que habilitar el par de alta disponibilidad. También debe verificar que node3 y node4 pueden acceder entre sí al almacenamiento de otro y que ninguno de sus propietarios son LIF de datos que pertenecen a otros nodos del clúster. Además, usted confirma que node3 posee los agregados de node1 y que node4 es propietario de los agregados de node2 y que los volúmenes de ambos nodos están en línea.

Pasos

1. Habilite la conmutación al nodo de respaldo del almacenamiento introduciendo el siguiente comando en uno de los nodos:

   ```
   storage failover modify -enabled true -node <node3>
   ```

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. Realice una de las siguientes acciones:

Si el clúster es un…	Descripción
Clúster de dos nodos	Habilite la alta disponibilidad del clúster introduciendo el comando siguiente en cualquiera de los nodos: `cluster ha modify -configured true`
Clúster con más de dos nodos	Vaya a. Paso 4.

4. Compruebe que los nodos 3 y no4 pertenecen al mismo clúster introduciendo el siguiente comando y examinando el resultado:

   ```
   cluster show
   ```

5. Verifique que los nodos 3 y 4 puedan acceder al almacenamiento de los demás. Para ello, introduzca el siguiente comando y examine el resultado:

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

6. 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, introduzca el siguiente comando y examine el resultado:

   ```
   network interface show
   ```

   Si el nodo 3 o el nodo 4 son propiedad de los LIF de datos que pertenecen a otros nodos del clúster, use el `network interface revert` Comando para devolver las LIF de datos a su propietario raíz.

7. 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>
   ```

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

   ```
   volume show -node <node3> -state offline
   volume show -node <node4> -state offline
   ```

9. Si alguno de los volúmenes se encuentra sin conexión, compártalos con la lista de volúmenes sin conexión en los que se haya capturado "Paso 19 (d)" En *prepare los nodos para la actualización* y active cualquiera de los volúmenes sin conexión, según sea necesario, introduzca el comando siguiente, una vez para cada volumen:

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

10. Instale licencias nuevas para los nodos nuevos introduciendo 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 agregar una licencia cada vez, o puede agregar varias licencias a la vez, cada clave de licencia separada por una coma.

11. Si se utilizan unidades de autocifrado en la configuración y se ha configurado el `kmip.init.maxwait` variable a. `off` (por ejemplo, en "Paso 16" De *Install and boot node3*), debe anular la definición de la variable:

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

12. Para quitar todas las licencias antiguas de los nodos originales, escriba uno de los siguientes comandos:

    ```
    system license clean-up -unused -expired
    system license delete -serial-number <node_serial_number> -package
    <licensable_package>
    ```

    - Para eliminar todas las licencias caducadas, introduzca:

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

    - Para eliminar todas las licencias no utilizadas, introduzca:

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

    - Para eliminar una licencia específica de un clúster, introduzca 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.

13. Compruebe que las licencias se han instalado correctamente introduciendo el comando siguiente y examinando su resultado:

    ```
    system license show
    ```

    Puedes comparar la salida con la salida que capturaste en"Paso 29" de *Preparar los nodos para la actualización*.

14. Configure los SPS realizando el siguiente comando en ambos nodos:

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

    Ve a "Referencias" para enlazar con la *System Administration Reference* para información sobre los SP y la *ONTAP 9 Command reference* para información detallada sobre el comando `system service-processor network modify`.

15. Si desea configurar un clúster sin switches en los nuevos nodos, vaya a. "Referencias" Para establecer un enlace al *sitio de soporte de red* y siga las instrucciones de *transición 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 los pasos de "Configure Storage Encryption en el nuevo módulo de la controladora". De lo contrario, complete los pasos de "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 show -status

    security key-manager query
    ```

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 -add 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 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 setup -node new_controller_name
```

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 restore -node new_controller_name
```

Configure el cifrado de volumen de NetApp o el cifrado agregante en el nuevo módulo del controlador

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.

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 mediante el siguiente comando:

```
security key-manager -add 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 mediante el siguiente comando:

```
security key-manager 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 mediante el siguiente comando:

   `security key-manager setup -node new_controller_name`

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:

Durante…	Se usa este comando…
Gestor de claves externas	`security key-manager external restore`Este comando necesita la clave de acceso de OKM
Gestión de claves incorporada (OKM)	`security key-manager onboard sync`

   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 alguno de los volúmenes se desconectó debido a que no existían claves de autenticación o porque no se pudo acceder a los servidores de gestión de claves externos. Vuelva a poner en línea esos volúmenes mediante el uso de `volume online` dominio.

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
   ```