



Etapas 7. Complete la actualización

Upgrade controllers

NetApp

February 19, 2026

This PDF was generated from <https://docs.netapp.com/es-es/ontap-systems-upgrade/upgrade-arl-auto-in-chassis/manage-authentication-using-kmip-servers.html> on February 19, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

- Etapa 7. Complete la actualización 1
 - Gestionar la autenticación mediante servidores KMIP 1
 - Confirmar que las nuevas controladoras están configuradas correctamente 1
 - 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 7
 - Reanudar las operaciones de SnapMirror 7

Etapa 7. Complete la actualización

Gestionar la autenticación mediante servidores KMIP

A partir de ONTAP 9.10.1, se pueden 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. Añadir 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 verificar que el par de alta disponibilidad está habilitado. También debe verificar que node1 y node2 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, se debe verificar que todos los agregados de datos se encuentran en los nodos iniciales correctos y que los volúmenes de ambos nodos estén en línea. Si uno de los nodos nuevos tiene un adaptador de destino unificado, debe restaurar cualquier configuración de puerto y es posible que deba cambiar el uso del adaptador.

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
```

Node	Partner	Takeover Possible	State Description
node1	node2	true	Connected to node2
node2	node1	true	Connected to node1

3. Compruebe que los nodos 1 y 2 pertenecen al mismo clúster mediante el siguiente comando y examine el resultado:

```
cluster show
```

4. Compruebe que los nodos 1 y 2 pueden acceder al almacenamiento de los demás mediante el siguiente comando y examine el resultado:

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

5. Compruebe que ni el nodo 1 ni el nodo 2 tienen las LIF de datos propias del hogar de otros nodos del clúster mediante el siguiente comando y examine el resultado:

```
network interface show
```

Si ni el nodo 1 ni el nodo 2 tienen LIF de datos propias del hogar de otros nodos del clúster, revierte las LIF de los datos a su propietario raíz:

```
network interface revert
```

6. Confirmar que los agregados son propiedad de sus respectivos nodos principales.

```
storage aggregate show -owner-name <node1>
```

```
storage aggregate show -owner-name <node2>
```

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

```
volume show -node <node1> -state offline
```

```
volume show -node <node2> -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 su resultado:

```
system license show
```

Puede comparar la salida con la que ha capturado en "[Prepare los nodos para la actualización](#)" sección.

12. Si se utilizan unidades de autocifrado en la configuración y se ha configurado el `kmip.init.maxwait` variable a `off` (Por ejemplo, en *Boot node2 con los módulos del sistema de reemplazo*, "[Paso 1](#)"), 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: 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 Storage Encryption está habilitado en los nodos 1 y 2, 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](#)

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.

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 vsilver_name
```

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.