



Configuración del cifrado basado en hardware de NetApp

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from <https://docs.netapp.com/es-es/ontap/encryption-at-rest/support-storage-encryption-concept.html> on February 12, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

Configuración del cifrado basado en hardware de NetApp	1
Obtenga más información sobre el cifrado basado en hardware de ONTAP	1
Cifrado basado en hardware de NetApp	1
Tipos de unidades de autocifrado compatibles	1
Cuándo utilizar la gestión de claves externas	2
Detalles de soporte	2
Flujo de trabajo de cifrado basado en hardware	3
Configure la gestión de claves externas	4
Obtenga información sobre cómo configurar la administración de claves externas de ONTAP	4
Instalar certificados SSL en el clúster ONTAP	4
Habilitar la administración de claves externas para el cifrado basado en hardware en ONTAP 9.6 y versiones posteriores	5
Habilitar la administración de claves externas para el cifrado basado en hardware en ONTAP 9.5 y versiones anteriores	6
Configure servidores de claves externas en clúster en ONTAP	8
Cree claves de autenticación en ONTAP 9.6 y versiones posteriores	11
Cree claves de autenticación en ONTAP 9.5 y versiones anteriores	13
Asignar una clave de autenticación de datos a una unidad FIPS o SED con la administración de claves externas ONTAP	15
Configure la gestión de claves incorporada	16
Habilite la gestión de claves incorporada en ONTAP 9.6 y versiones posteriores	17
Habilite la gestión de claves incorporada en ONTAP 9.5 y versiones anteriores	19
Asignar una clave de autenticación de datos a una unidad FIPS o SED con administración de claves integrada de ONTAP	21
Asignar una clave de autenticación FIPS 140-2 a una unidad FIPS de ONTAP	23
Habilite el modo conforme a FIPS para todo el clúster para las conexiones del servidor KMIP en ONTAP ..	24

Configuración del cifrado basado en hardware de NetApp

Obtenga más información sobre el cifrado basado en hardware de ONTAP

El cifrado basado en hardware de NetApp admite el cifrado de disco completo (FDE) de los datos mientras se escriben. No se pueden leer los datos sin una clave de cifrado almacenada en el firmware. La clave de cifrado, a su vez, sólo es accesible a un nodo autenticado.

Cifrado basado en hardware de NetApp

Un nodo se autentica a una unidad de autocifrado mediante una clave de autenticación recuperada de un servidor de gestión de claves externo o Onboard Key Manager:

- El servidor de gestión de claves externo es un sistema de terceros en el entorno de almacenamiento que proporciona claves a los nodos mediante el protocolo de interoperabilidad de gestión de claves (KMIP). Se recomienda configurar servidores de gestión de claves externos a partir de sus datos en un sistema de almacenamiento diferente.
- El gestor de claves incorporado es una herramienta integrada que proporciona claves de autenticación a nodos del mismo sistema de almacenamiento que los datos.

Puede utilizar el cifrado de volúmenes de NetApp con cifrado basado en hardware para «cifrar doble» los datos de unidades con autocifrado.

Cuando se habilitan unidades de autocifrado, también se cifra el volcado de memoria.



Si una pareja de alta disponibilidad utiliza cifrado de unidades SAS o NVMe (SED, NSE, FIPS), debe seguir las instrucciones del tema [Devolver una unidad FIPS o SED al modo sin protección](#) para todas las unidades de la pareja de alta disponibilidad antes de inicializar el sistema (opciones de arranque 4 o 9). Si las unidades se reasignan, es posible que no se produzcan pérdidas de datos futuras.

Tipos de unidades de autocifrado compatibles

Se admiten dos tipos de unidades de autocifrado:

- Las unidades SAS o NVMe con certificación FIPS de autocifrado son compatibles con todos los sistemas FAS y AFF. Estas unidades, denominadas *_unidades FIPS*, cumplen con los requisitos del nivel 2 de la publicación estándar de procesamiento de información federal 140-2. Las capacidades certificadas ofrecen protecciones además del cifrado, como la prevención de ataques de denegación de servicio en la unidad. Las unidades FIPS no pueden combinarse con otros tipos de unidades en el mismo nodo o en la pareja de alta disponibilidad.
- A partir de ONTAP 9.6, las unidades NVMe de autocifrado que no se han sometido a pruebas FIPS son compatibles con los sistemas AFF A800, A320 y posteriores. Estas unidades, denominadas *SED*, ofrecen las mismas funcionalidades de cifrado que las unidades FIPS, pero se pueden combinar con unidades sin cifrado en el mismo nodo o par de alta disponibilidad.

- Todas las unidades validadas con FIPS utilizan un módulo criptográfico de firmware que se ha realizado mediante la validación FIPS. El módulo criptográfico de la unidad FIPS no utiliza ninguna clave generada fuera de la unidad (el módulo criptográfico del firmware de la unidad utiliza la frase de acceso de autenticación que se introduce en la unidad para obtener una clave de cifrado).



Las unidades sin cifrado son unidades que no están de SED o FIPS.



Si utiliza NSE en un sistema con un módulo Flash Cache, también debe habilitar NVE o NAE. NSe no cifra los datos que residen en el módulo de Flash Cache.

Cuándo utilizar la gestión de claves externas

Aunque resulta menos caro y, por lo general, más práctico, utilizar el gestor de claves incorporado, se debe utilizar la gestión de claves externa si se da alguna de las siguientes situaciones:

- La política de su organización requiere una solución de gestión de claves que utilice un módulo criptográfico FIPS 140-2 de nivel 2 (o superior).
- Necesita una solución de varios clústeres con gestión centralizada de las claves de cifrado.
- Su empresa requiere una seguridad añadida para almacenar claves de autenticación en un sistema o en una ubicación distinta de los datos.

Detalles de soporte

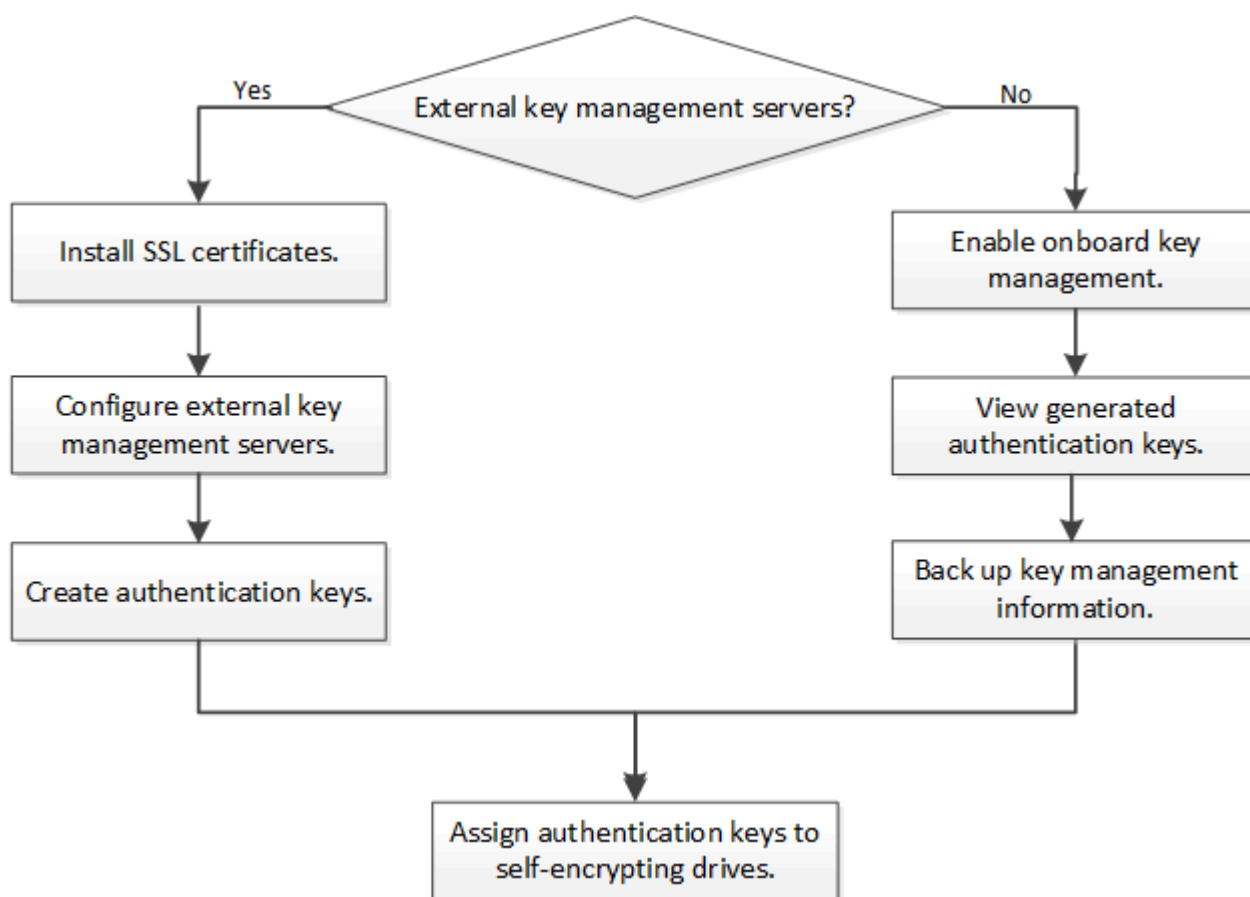
En la siguiente tabla se muestran detalles importantes de compatibilidad con el cifrado de hardware. Consulte la matriz de interoperabilidad para obtener la información más reciente sobre servidores KMIP, sistemas de almacenamiento y bandejas de discos compatibles.

Recurso o característica	Detalles de soporte
Conjuntos de discos no homogéneos	<ul style="list-style-type: none"> • Las unidades FIPS no pueden combinarse con otros tipos de unidades en el mismo nodo o en la pareja de alta disponibilidad. Las parejas de alta disponibilidad conformes pueden coexistir con parejas de alta disponibilidad no conformes en el mismo clúster. • SEDS puede combinarse con unidades sin cifrado en el mismo nodo o en la pareja de alta disponibilidad.
Tipo de unidad	<ul style="list-style-type: none"> • Las unidades FIPS pueden ser SAS o NVMe. • SEDS debe ser unidades NVMe.
Interfaces de red de 10 GB	A partir de ONTAP 9.3, las configuraciones de gestión de claves KMIP admiten interfaces de red de 10 GB para las comunicaciones con servidores de gestión de claves externos.

Puertos para la comunicación con el servidor de gestión de claves	A partir de ONTAP 9.3, es posible usar cualquier puerto de la controladora de almacenamiento para la comunicación con el servidor de gestión de claves. De lo contrario, debe utilizar el puerto e0M para la comunicación con los servidores de gestión de claves. Según el modelo de controladora de almacenamiento, es posible que ciertas interfaces de red no estén disponibles durante el proceso de arranque para establecer la comunicación con los servidores de gestión de claves.
MetroCluster (MCC) (en inglés)	<ul style="list-style-type: none"> Las unidades NVMe admiten MCC. Las unidades SAS no son compatibles con MCC.

Flujo de trabajo de cifrado basado en hardware

Debe configurar los servicios de gestión de claves para que el clúster pueda autenticarse en la unidad de autocifrado. Es posible usar un servidor de gestión de claves externo o un administrador de claves incorporado.



Información relacionada

- ["NetApp Hardware Universe"](#)
- ["Cifrado de volúmenes de NetApp y cifrado de agregados de NetApp"](#)

Configure la gestión de claves externas

Obtenga información sobre cómo configurar la administración de claves externas de ONTAP

Puede usar uno o varios servidores de gestión de claves externos para proteger las claves que utiliza el clúster para acceder a los datos cifrados. Un servidor de gestión de claves externo es un sistema de terceros en el entorno de almacenamiento que proporciona claves a los nodos mediante el protocolo de interoperabilidad de gestión de claves (KMIP).

El cifrado de volúmenes de NetApp (NVE) se puede implementar con el gestor de claves incorporado. En ONTAP 9.3 y versiones posteriores, el NVE puede implementarse con gestión de claves externa (KMIP) y el gestor de claves incorporado. A partir de ONTAP 9.11.1, es posible configurar varios administradores de claves externos en un clúster. Consulte [Configurar servidores de claves en cluster](#).

Instalar certificados SSL en el clúster ONTAP

El clúster y el servidor KMIP utilizan certificados SSL KMIP para verificar la identidad de las otras y establecer una conexión SSL. Antes de configurar la conexión SSL con el servidor KMIP, debe instalar los certificados SSL de cliente KMIP para el clúster y el certificado público SSL para la entidad de certificación (CA) raíz del servidor KMIP.

Acerca de esta tarea

En una pareja de alta disponibilidad, ambos nodos deben usar los mismos certificados KMIP públicos y privados. Si conecta varias parejas de alta disponibilidad con el mismo servidor KMIP, todos los nodos de las parejas de alta disponibilidad deben utilizar los mismos certificados KMIP públicos y privados.

Antes de empezar

- La hora debe sincronizarse en el servidor que crea los certificados, el servidor KMIP y el clúster.
- Debe haber obtenido el certificado de cliente SSL KMIP público para el clúster.
- Debe haber obtenido la clave privada asociada con el certificado de cliente SSL KMIP para el clúster.
- El certificado de cliente SSL KMIP no debe estar protegido por contraseña.
- Debe haber obtenido el certificado público de SSL para la entidad de certificación (CA) raíz del servidor KMIP.
- En un entorno de MetroCluster, debe instalar los mismos certificados SSL KMIP en ambos clústeres.



Es posible instalar los certificados de cliente y de servidor en el servidor KMIP antes o después de instalar los certificados en el clúster.

Pasos

1. Instale los certificados de cliente SSL KMIP para el clúster:

```
security certificate install -vserver admin_svm_name -type client
```

Se le solicita que introduzca los certificados públicos y privados de SSL KMIP.

```
cluster1::> security certificate install -vserver cluster1 -type client
```

2. Instale el certificado público SSL para la entidad de certificación (CA) raíz del servidor KMIP:

```
security certificate install -vserver admin_svm_name -type server-ca  
  
cluster1::> security certificate install -vserver cluster1 -type server-ca
```

Información relacionada

- ["instalación del certificado de seguridad"](#)

Habilitar la administración de claves externas para el cifrado basado en hardware en ONTAP 9.6 y versiones posteriores

Puede utilizar uno o varios servidores KMIP para proteger las claves que utiliza el clúster para acceder a los datos cifrados. Se pueden conectar hasta cuatro servidores KMIP a un nodo. Se recomienda un mínimo de dos servidores para la redundancia y la recuperación ante desastres.

A partir de ONTAP 9.11.1, puede agregar hasta 3 servidores de claves secundarios por servidor de claves primario para crear un servidor de claves en clúster. Para obtener más información, consulte [Configurar servidores de claves externas en cluster](#).

Antes de empezar

- Deben haberse instalado el cliente KMIP SSL y los certificados de servidor.
- Para realizar esta tarea, debe ser un administrador de clústeres.
- En un entorno MetroCluster :
 - Debe configurar el entorno de MetroCluster antes de configurar un gestor de claves externo.
 - Debe instalar el mismo certificado SSL KMIP en ambos clústeres.

Pasos

1. Configure la conectividad del gestor de claves para el clúster:

```
security key-manager external enable -vserver admin_SVM -key-servers  
host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert  
server_CA_certificates
```



- El `security key-manager external enable` comando reemplaza `security key-manager setup` el comando. Es posible ejecutar `security key-manager external modify` el comando para cambiar la configuración de gestión de claves externas. Obtenga más información sobre `security key-manager external enable` en el ["Referencia de comandos del ONTAP"](#).
- En un entorno MetroCluster, si se configura la gestión de claves externa para la SVM de administrador, debe repetir `security key-manager external enable` el comando en el clúster de socios.

El siguiente comando habilita la gestión de claves externas `cluster1` con tres servidores de claves externos. El primer servidor de claves se especifica mediante su nombre de host y puerto, el segundo se especifica mediante una dirección IP y el puerto predeterminado, y el tercero se especifica mediante una dirección IPv6 y un puerto:

```
cluster1::> security key-manager external enable -key-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

2. Compruebe que todos los servidores KMIP configurados están conectados:

```
security key-manager external show-status -node node_name -vserver SVM -key
-server host_name|IP_address:port -key-server-status available|not-
responding|unknown
```



El `security key-manager external show-status` comando reemplaza `security key-manager show -status` el comando. Obtenga más información sobre `security key-manager external show-status` en el ["Referencia de comandos del ONTAP"](#).

```
cluster1::> security key-manager external show-status
```

Node	Vserver	Key Server	Status

node1			
	cluster1	10.0.0.10:5696	available
		fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234	available
		ks1.local:15696	available
node2			
	cluster1	10.0.0.10:5696	available
		fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234	available
		ks1.local:15696	available

6 entries were displayed.

Información relacionada

- [Configurar servidores de claves externas en cluster](#)
- ["administrador de claves de seguridad habilitado externamente"](#)
- ["administrador de claves de seguridad externo para mostrar el estado"](#)

Habilitar la administración de claves externas para el cifrado basado en hardware en ONTAP 9.5 y versiones anteriores

Puede utilizar uno o varios servidores KMIP para proteger las claves que utiliza el clúster para acceder a los datos cifrados. Se pueden conectar hasta cuatro servidores KMIP a un nodo. Se recomienda un mínimo de dos servidores para la redundancia y la

recuperación ante desastres.

Acerca de esta tarea

ONTAP configura la conectividad de los servidores KMIP para todos los nodos del clúster.

Antes de empezar

- Deben haberse instalado el cliente KMIP SSL y los certificados de servidor.
- Para realizar esta tarea, debe ser un administrador de clústeres.
- Debe configurar el entorno de MetroCluster antes de configurar un gestor de claves externo.
- En un entorno MetroCluster, debe instalar el mismo certificado SSL KMIP en ambos clústeres.

Pasos

1. Configure la conectividad de Key Manager para los nodos del clúster:

```
security key-manager setup
```

Se inicia la configuración del gestor de claves.



En un entorno MetroCluster, debe ejecutar este comando en ambos clústeres. Obtenga más información sobre `security key-manager setup` en el ["Referencia de comandos del ONTAP"](#).

2. Introduzca la respuesta adecuada en cada solicitud.
3. Añadir un servidor KMIP:

```
security key-manager add -address key_management_server_ipaddress
```

```
cluster1::> security key-manager add -address 20.1.1.1
```



En un entorno de MetroCluster, debe ejecutar este comando en ambos clústeres.

4. Añada un servidor KMIP adicional para redundancia:

```
security key-manager add -address key_management_server_ipaddress
```

```
cluster1::> security key-manager add -address 20.1.1.2
```



En un entorno de MetroCluster, debe ejecutar este comando en ambos clústeres.

5. Compruebe que todos los servidores KMIP configurados están conectados:

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

Obtenga más información sobre los comandos descritos en este procedimiento en el ["Referencia de comandos del ONTAP"](#).

```
cluster1::> security key-manager show -status
```

Node	Port	Registered Key Manager	Status
-----	----	-----	-----
cluster1-01	5696	20.1.1.1	available
cluster1-01	5696	20.1.1.2	available
cluster1-02	5696	20.1.1.1	available
cluster1-02	5696	20.1.1.2	available

6. Opcionalmente, convierta volúmenes de texto sin formato en volúmenes cifrados.

```
volume encryption conversion start
```

Debe haber configurado completamente un gestor de claves externo para poder convertir los volúmenes. En un entorno MetroCluster, debe configurarse un gestor de claves externo en ambos sitios.

Configure servidores de claves externas en clúster en ONTAP

A partir de ONTAP 9.11.1, puede configurar la conectividad a servidores de administración de claves externos agrupados en un SVM. Con servidores de claves agrupados, puede designar servidores de claves principales y secundarios en una SVM. Al registrar o recuperar claves, ONTAP primero intenta acceder al servidor de clave principal antes de intentar acceder secuencialmente a los servidores secundarios hasta que la operación se complete exitosamente.

Puede utilizar servidores de claves externos para claves NetApp Storage Encryption (NSE), NetApp Volume Encryption (NVE) y NetApp Aggregate Encryption (NAE). Una SVM puede admitir hasta cuatro servidores KMIP externos primarios. Cada servidor principal puede admitir hasta tres servidores clave secundarios.

Acerca de esta tarea

- Este proceso solo admite servidores de claves que utilizan KMIP. Para obtener una lista de los servidores de claves compatibles, compruebe el ["Herramienta de matriz de interoperabilidad de NetApp"](#).

Antes de empezar

- ["La gestión de claves KMIP debe estar habilitada para la SVM"](#).
- Todos los nodos del clúster deben ejecutar ONTAP 9.11.1 o una versión posterior.
- El orden de los servidores enumerados en el `-secondary-key-servers` El parámetro refleja el orden de acceso de los servidores de administración de claves externas (KMIP).

Cree un servidor de claves en clúster

El procedimiento de configuración depende de si se ha configurado o no un servidor de claves primario.

Añada servidores de claves primarios y secundarios a una SVM

Pasos

1. Confirme que no se ha habilitado ninguna administración de claves para el clúster (SVM de administrador):

```
security key-manager external show -vserver <svm_name>
```

Si la SVM ya tiene habilitado el máximo de cuatro servidores de clave principal, debe eliminar uno de los servidores de clave principal existentes antes de agregar uno nuevo.

2. Habilitar el administrador de claves principal:

```
security key-manager external enable -vserver <svm_name> -key-servers  
<primary_key_server_ip> -client-cert <client_cert_name> -server-ca-certs  
<server_ca_cert_names>
```

- Si no especifica un puerto en el `-key-servers` parámetro, se utiliza el puerto predeterminado 5696.



Si está ejecutando el `security key-manager external enable` comando para el SVM de administrador en una configuración de MetroCluster, debe ejecutar el comando en ambos clústeres. Si está ejecutando el comando para un SVM de datos individual, no necesita ejecutar el comando en ambos clústeres. NetApp recomienda encarecidamente utilizar los mismos servidores clave en ambos clústeres.

3. Modifique el servidor de clave principal para agregar servidores de clave secundaria. El `-secondary -key-servers` El parámetro acepta una lista separada por comas de hasta tres servidores clave:

```
security key-manager external modify-server -vserver <svm_name> -key  
-servers <primary_key_server> -secondary-key-servers <list_of_key_servers>
```

- No incluya un número de puerto para servidores de clave secundaria en el `-secondary-key -servers` parámetro. Utiliza el mismo número de puerto que el servidor de clave principal.



Si está ejecutando el `security key-manager external` comando para el SVM de administrador en una configuración de MetroCluster, debe ejecutar el comando en ambos clústeres. Si está ejecutando el comando para un SVM de datos individual, no necesita ejecutar el comando en ambos clústeres. NetApp recomienda encarecidamente utilizar los mismos servidores clave en ambos clústeres.

Añadir servidores de claves secundarios a un servidor de claves primario existente

Pasos

1. Modifique el servidor de clave principal para agregar servidores de clave secundaria. El `-secondary -key-servers` El parámetro acepta una lista separada por comas de hasta tres servidores clave:

```
security key-manager external modify-server -vserver <svm_name> -key  
-servers <primary_key_server> -secondary-key-servers <list_of_key_servers>
```

- No incluya un número de puerto para servidores de clave secundaria en el `-secondary-key-servers` parámetro. Utiliza el mismo número de puerto que los servidores de clave principal.



Si está ejecutando el `security key-manager external modify-server` comando para el SVM de administrador en una configuración de MetroCluster , debe ejecutar el comando en ambos clústeres. Si está ejecutando el comando para un SVM de datos individual, no necesita ejecutar el comando en ambos clústeres. NetApp recomienda encarecidamente utilizar los mismos servidores clave en ambos clústeres.

Para obtener más información sobre los servidores de claves secundarias, consulte [\[mod-secondary\]](#).

Modifique los servidores de claves en cluster

Puede modificar servidores de claves externos agrupados agregando y eliminando servidores de claves secundarios, cambiando el orden de acceso de los servidores de claves secundarios o cambiando la designación (principal o secundaria) de servidores de claves particulares. Si modifica servidores de clave externos agrupados en una configuración de MetroCluster , NetApp recomienda enfáticamente utilizar los mismos servidores de clave en ambos clústeres.

Modificar servidores de claves secundarios

Utilice el parámetro `-secondary-key-servers` del comando `security key-manager external modify-server` para gestionar servidores de claves secundarios. El `-secondary-key-servers` El parámetro acepta una lista separada por comas. El orden especificado de los servidores de clave secundaria en la lista determina la secuencia de acceso para los servidores de clave secundaria. Puede modificar el orden de acceso ejecutando el comando `security key-manager external modify-server` con los servidores de claves secundarios introducidos en una secuencia diferente. No incluya un número de puerto para servidores de clave secundaria.



Si está ejecutando el `security key-manager external modify-server` comando para el SVM de administrador en una configuración de MetroCluster , debe ejecutar el comando en ambos clústeres. Si está ejecutando el comando para un SVM de datos individual, no necesita ejecutar el comando en ambos clústeres.

Para eliminar un servidor de clave secundaria, incluya los servidores de clave que desea conservar en el `-secondary-key-servers` parámetro y omita el que desea eliminar. Para eliminar todos los servidores de claves secundarias, utilice el argumento `-` , que significa ninguno.

Convertir servidores de claves primarios y secundarios

Puede utilizar los siguientes pasos para cambiar la designación (principal o secundaria) de servidores de claves particulares.

Convertir un servidor de clave principal en un servidor de clave secundaria

Pasos

1. Eliminar el servidor de clave principal de la SVM:

```
security key-manager external remove-servers
```



Si está ejecutando el `security key-manager external remove-servers` comando para el SVM de administrador en una configuración de MetroCluster , debe ejecutar el comando en ambos clústeres. Si está ejecutando el comando para un SVM de datos individual, no necesita ejecutar el comando en ambos clústeres.

2. Realizar el [Cree un servidor de claves en clúster](#) procedimiento que utiliza el antiguo servidor de clave principal como servidor de clave secundaria.

Convertir un servidor de clave secundaria en un servidor de clave principal

Pasos

1. Eliminar el servidor de clave secundaria de su servidor de clave principal existente:

```
security key-manager external modify-server -secondary-key-servers
```

- Si está ejecutando el `security key-manager external modify-server -secondary-key -servers` comando para el SVM de administrador en una configuración de MetroCluster , debe ejecutar el comando en ambos clústeres. Si está ejecutando el comando para un SVM de datos individual, no necesita ejecutar el comando en ambos clústeres.
- Si convierte un servidor de clave secundario en un servidor de clave principal mientras elimina un servidor de clave existente, intentar agregar un nuevo servidor de clave antes de completar la eliminación y la conversión puede generar la duplicación de claves.

1. Realizar el [Cree un servidor de claves en clúster](#) procedimiento que utiliza el antiguo servidor de clave secundaria como servidor de clave principal del nuevo servidor de clave agrupado.

Referirse a [\[mod-secondary\]](#) Para más información.

Información relacionada

- Obtenga más información sobre `security key-manager external` en el ["Referencia de comandos del ONTAP"](#)

Cree claves de autenticación en ONTAP 9.6 y versiones posteriores

Puede usar el `security key-manager key create` comando para crear las claves de autenticación de un nodo y almacenarlas en los servidores KMIP configurados.

Acerca de esta tarea

Si la configuración de seguridad requiere el uso de claves diferentes para la autenticación de datos y la autenticación FIPS 140-2-2, debe crear una clave independiente para cada una. Si este no es el caso, puede usar la misma clave de autenticación para el cumplimiento de FIPS que utiliza para el acceso a los datos.

ONTAP crea claves de autenticación para todos los nodos del clúster.

- Este comando no es compatible cuando el gestor de claves incorporado está habilitado. Sin embargo, se crean automáticamente dos claves de autenticación cuando se habilita el gestor de claves incorporado. Las teclas se pueden ver con el siguiente comando:

```
security key-manager key query -key-type NSE-AK
```

- Recibe una advertencia si los servidores de gestión de claves configurados ya almacenan más de 128 claves de autenticación.
- Puede usar el `security key-manager key delete` comando para eliminar las claves no utilizadas. El `security key-manager key delete` comando falla si la clave dada está actualmente en uso en ONTAP. (Para utilizar este comando, debe tener un Privileges mayor que admin).



En un entorno de MetroCluster, antes de eliminar una clave, debe asegurarse de que la clave no se esté utilizando en el clúster de partners. Puede utilizar los siguientes comandos en el clúster de partners para comprobar que la clave no esté en uso:

- ° `storage encryption disk show -data-key-id <key-id>`
- ° `storage encryption disk show -fips-key-id <key-id>`

Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

Pasos

1. Cree las claves de autenticación para los nodos del clúster:

```
security key-manager key create -key-tag <passphrase_label> -prompt-for  
-key true|false
```



Al establecer esta configuración `prompt-for-key=true`, el sistema solicita al administrador del clúster que la clave de acceso se use al autenticar las unidades cifradas. De lo contrario, el sistema genera automáticamente una frase de acceso de 32 bytes. El `security key-manager key create` comando reemplaza `security key-manager create-key` el comando. Obtenga más información sobre `security key-manager key create` en el ["Referencia de comandos del ONTAP"](#).

En el siguiente ejemplo se crean las claves de autenticación para `cluster1`, generar automáticamente una frase de contraseña de 32 bytes:

```
cluster1::> security key-manager key create  
Key ID: <id_value>
```

2. Compruebe que se han creado las claves de autenticación:

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



El `security key-manager key query` comando reemplaza `security key-manager query key` el comando.

El ID de clave que se muestra en el resultado es un identificador que se utiliza para hacer referencia a la clave de autenticación. No es la clave de autenticación real ni la clave de cifrado de datos.

En el siguiente ejemplo se verifica que se han creado claves de autenticación para `cluster1`:

```
cluster1::> security key-manager key query
Vserver: cluster1
Key Manager: external
Node: node1
```

Key Tag	Key Type	Restored
node1	NSE-AK	yes
Key ID: <id_value>		
node1	NSE-AK	yes
Key ID: <id_value>		

```
Vserver: cluster1
Key Manager: external
Node: node2
```

Key Tag	Key Type	Restored
node2	NSE-AK	yes
Key ID: <id_value>		
node2	NSE-AK	yes
Key ID: <id_value>		

Obtenga más información sobre `security key-manager key query` en el ["Referencia de comandos del ONTAP"](#).

Información relacionada

- ["Mostrar disco de cifrado de almacenamiento"](#)

Cree claves de autenticación en ONTAP 9.5 y versiones anteriores

Puede usar el `security key-manager create-key` comando para crear las claves de autenticación de un nodo y almacenarlas en los servidores KMIP configurados.

Acerca de esta tarea

Si la configuración de seguridad requiere el uso de claves diferentes para la autenticación de datos y la autenticación FIPS 140-2-2, debe crear una clave independiente para cada una. Si no es así, puede usar la misma clave de autenticación para el cumplimiento de FIPS que se usa para acceder a los datos.

ONTAP crea claves de autenticación para todos los nodos del clúster.

- Este comando no es compatible cuando la gestión de claves incorporada está habilitada.
- Recibe una advertencia si los servidores de gestión de claves configurados ya almacenan más de 128 claves de autenticación.

Se puede usar el software del servidor de gestión de claves para eliminar las claves sin usar y, a continuación, ejecutar el comando de nuevo.

Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

Pasos

1. Cree las claves de autenticación para los nodos del clúster:

```
security key-manager create-key
```

Obtenga más información sobre `security key-manager create-key` en el ["Referencia de comandos del ONTAP"](#).



El ID de clave que se muestra en el resultado es un identificador que se utiliza para hacer referencia a la clave de autenticación. No es la clave de autenticación real ni la clave de cifrado de datos.

En el siguiente ejemplo se crean las claves de autenticación para `cluster1`:

```
cluster1::> security key-manager create-key
(security key-manager create-key)
Verifying requirements...

Node: cluster1-01
Creating authentication key...
Authentication key creation successful.
Key ID: <id_value>

Node: cluster1-01
Key manager restore operation initialized.
Successfully restored key information.

Node: cluster1-02
Key manager restore operation initialized.
Successfully restored key information.
```


2. Compruebe que se han creado las claves de autenticación:

```
security key-manager query
```

Obtenga más información sobre `security key-manager query` en el ["Referencia de comandos del ONTAP"](#).

En el siguiente ejemplo se verifica que se han creado claves de autenticación para `cluster1`:

```
cluster1::> security key-manager query
```

```
(security key-manager query)
```

```
Node: cluster1-01
```

```
Key Manager: 20.1.1.1
```

```
Server Status: available
```

Key Tag	Key Type	Restored
cluster1-01	NSE-AK	yes
Key ID: <id_value>		

```
Node: cluster1-02
```

```
Key Manager: 20.1.1.1
```

```
Server Status: available
```

Key Tag	Key Type	Restored
cluster1-02	NSE-AK	yes
Key ID: <id_value>		

Asignar una clave de autenticación de datos a una unidad FIPS o SED con la administración de claves externas ONTAP

Puede utilizar `storage encryption disk modify` el comando para asignar una clave de autenticación de datos a una unidad FIPS o SED. Los nodos de clúster utilizan esta clave para bloquear o desbloquear los datos cifrados en la unidad.

Acerca de esta tarea

Una unidad de autocifrado está protegida contra el acceso no autorizado solo si su ID de clave de autenticación se configura como un valor no predeterminado. El ID seguro del fabricante (MSID), que tiene el ID de clave 0x0, es el valor predeterminado estándar para las unidades SAS. Para las unidades NVMe, el valor predeterminado estándar es una clave nula, que se representa como un ID de clave en blanco. Cuando se asigna el ID de clave a una unidad de autocifrado, el sistema cambia el ID de clave de autenticación por un valor no predeterminado.

Este procedimiento no causa interrupciones.

Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

Pasos

1. Asigne una clave de autenticación de datos a una unidad FIPS o SED:

```
storage encryption disk modify -disk disk_ID -data-key-id key_ID
```

Obtenga más información sobre `storage encryption disk modify` en el ["Referencia de comandos del ONTAP"](#).



Puede usar el `security key-manager query -key-type NSE-AK` comando para ver ID de claves.

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id  
<id_value>
```

```
Info: Starting modify on 14 disks.  
View the status of the operation by using the  
storage encryption disk show-status command.
```

2. Compruebe que se han asignado las claves de autenticación:

```
storage encryption disk show
```

Obtenga más información sobre `storage encryption disk show` en el ["Referencia de comandos del ONTAP"](#).

```
cluster1::> storage encryption disk show  
Disk      Mode Data Key ID  
-----  
-----  
0.0.0     data <id_value>  
0.0.1     data <id_value>  
[...]
```

Información relacionada

- ["Mostrar disco de cifrado de almacenamiento"](#)
- ["estado del disco de cifrado de almacenamiento"](#)

Configure la gestión de claves incorporada

Habilite la gestión de claves incorporada en ONTAP 9.6 y versiones posteriores

Puede usar el gestor de claves incorporado para autenticar nodos de clúster en una unidad FIPS o SED. El gestor de claves incorporado es una herramienta integrada que proporciona claves de autenticación a nodos del mismo sistema de almacenamiento que los datos. El gestor de claves incorporado es conforme a la normativa FIPS-140-2 de nivel 1.

Puede usar el administrador de claves incorporado para proteger las claves que el clúster utiliza para acceder a los datos cifrados. Debe habilitar el gestor de claves incorporado en cada clúster que acceda a un volumen cifrado o un disco de autocifrado.

Acerca de esta tarea

Debe ejecutar `security key-manager onboard enable` el comando cada vez que añade un nodo al clúster. En configuraciones de MetroCluster, `security key-manager onboard enable` primero debe ejecutar en el clúster local y luego ejecutar `security key-manager onboard sync` en el clúster remoto, con la misma clave de acceso en cada uno.

Obtenga más información sobre `security key-manager onboard enable` y `security key-manager onboard sync` en el ["Referencia de comandos del ONTAP"](#).

De forma predeterminada, no es necesario introducir la clave de acceso del administrador de claves cuando se reinicia un nodo. Excepto en MetroCluster, puede usar `cc-mode-enabled=yes` la opción para requerir que los usuarios introduzcan la clave de acceso después de un reinicio.

Cuando Onboard Key Manager está activado en el modo Common Criteria (`cc-mode-enabled=yes`), el comportamiento del sistema se cambia de las siguientes formas:

- El sistema supervisa los intentos fallidos consecutivos de acceso al clúster cuando funciona en modo de criterios comunes.

Si se habilitó el cifrado en almacenamiento de NetApp (NSE) y no se puede introducir la clave de acceso del clúster correcta en el arranque, el sistema no puede autenticarse en sus unidades y se reinicia automáticamente. Para corregir esto, debe introducir la clave de acceso correcta del clúster en el símbolo del sistema de arranque. Una vez arrancado, el sistema permite 5 introducir correctamente la clave de acceso del clúster en un periodo de 24 horas para cualquier comando que requiera la clave de acceso del clúster como parámetro. Si se alcanza el límite (por ejemplo, no ha podido introducir correctamente la clave de acceso del clúster 5 veces en una fila), debe esperar al tiempo de espera de 24 horas o reiniciar el nodo para restablecer el límite.

- Las actualizaciones de imágenes del sistema utilizan el certificado de firma de código RSA-3072 de NetApp junto con los resúmenes firmados con código SHA-384 para comprobar la integridad de la imagen en lugar del certificado de firma de código RSA-2048 de NetApp habitual y los resúmenes firmados con código SHA-256.

El comando de actualización verifica que el contenido de la imagen no haya sido alterado o dañado comprobando varias firmas digitales. Si la validación funciona, la actualización de la imagen pasa al siguiente paso. Si la validación no funciona, la actualización de la imagen falla. Obtenga más información sobre `cluster image` en el ["Referencia de comandos del ONTAP"](#).





El gestor de claves incorporado almacena claves en la memoria volátil. El contenido de la memoria volátil se borra al reiniciar o detener el sistema. En condiciones normales de funcionamiento, el contenido de la memoria volátil se borrará en un plazo de 30 segundos cuando se pare un sistema.

Antes de empezar

- Si utiliza NSE con un servidor de gestión de claves externa (KMIP), debe haber eliminado la base de datos de gestor de claves externo.

["Transición a la gestión de claves incorporada desde la gestión de claves externas"](#)

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Debe configurar el entorno de MetroCluster antes de configurar el gestor de claves incorporado.

Pasos

1. Inicie el comando de configuración del gestor de claves:

```
security key-manager onboard enable -cc-mode-enabled yes|no
```



Establezca esta opción `cc-mode-enabled=yes` para que los usuarios introduzcan la frase de contraseña del gestor de claves después de reiniciar. - `cc-mode-enabled`La opción no es compatible con las configuraciones de MetroCluster. El `security key-manager onboard enable comando reemplaza security key-manager setup el comando.`

En el siguiente ejemplo, se inicia el comando `key Manager setup` en `cluster1` sin necesidad de introducir la frase de contraseña después de cada reinicio:

2. Introduzca una frase de contraseña entre 32 y 256 caracteres, o para "cc-mode", una frase de contraseña entre 64 y 256 caracteres.



Si la frase de paso "cc-mode" especificada es menor de 64 caracteres, hay un retraso de cinco segundos antes de que la operación de configuración del gestor de claves vuelva a mostrar la indicación de contraseña.

3. En la solicitud de confirmación de contraseña, vuelva a introducir la frase de contraseña.
4. Verifique que el sistema cree las claves de autenticación:

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



El `security key-manager key query` comando reemplaza `security key-manager query key` el comando.

Obtenga más información sobre `security key-manager key query` en el ["Referencia de comandos del ONTAP"](#).

Después de terminar

Copie la clave de acceso en una ubicación segura fuera del sistema de almacenamiento para usarla en el futuro.

El sistema realiza automáticamente una copia de seguridad de la información de administración de claves en la base de datos replicada (RDB) del clúster. También debe realizar una copia de seguridad de esta información manualmente para la recuperación ante desastres.

Información relacionada

- ["comandos de imagen de clúster"](#)
- ["Habilitación externa del administrador de claves de seguridad"](#)
- ["consulta de claves del administrador de claves de seguridad"](#)
- ["Habilitación integrada del administrador de claves de seguridad"](#)
- ["Transición a la gestión de claves incorporada desde la gestión de claves externas"](#)

Habilite la gestión de claves incorporada en ONTAP 9.5 y versiones anteriores

Puede usar el gestor de claves incorporado para autenticar nodos de clúster en una unidad FIPS o SED. El gestor de claves incorporado es una herramienta integrada que proporciona claves de autenticación a nodos del mismo sistema de almacenamiento que los datos. El gestor de claves incorporado es conforme a la normativa FIPS-140-2 de nivel 1.

Puede utilizar el Administrador de claves integrado para proteger las claves que utiliza el clúster para acceder a datos cifrados. Habilite el Administrador de claves integrado en cada clúster que acceda a volúmenes cifrados o discos con cifrado automático.

Acerca de esta tarea

Debe ejecutar `security key-manager setup` el comando cada vez que añade un nodo al clúster.

Si tiene una configuración de MetroCluster, revise las siguientes directrices:

- En ONTAP 9.5, debe ejecutarse `security key-manager setup` en el clúster local y `security key-manager setup -sync-metrocluster-config yes` en el clúster remoto, con la misma clave de acceso en cada uno.
- Antes de usar ONTAP 9.5, debe ejecutarse `security key-manager setup` en el clúster local, esperar aproximadamente 20 segundos y, luego, ejecutarse `security key-manager setup` en el clúster remoto, usando la misma clave de acceso en cada uno.

De forma predeterminada, no es necesario introducir la clave de acceso del administrador de claves cuando se reinicia un nodo. A partir de ONTAP 9.4, puede usar la `-enable-cc-mode yes` opción para solicitar que los usuarios introduzcan la frase de acceso después de reiniciar.

Para NVE, si establece `-enable-cc-mode yes`, los volúmenes que cree con los `volume create volume move start` comandos y se cifran automáticamente. Para `volume create`, no es necesario especificar `-encrypt true`. Para `volume move start`, no es necesario especificar `-encrypt-destination true`.



Después de un intento de clave de acceso con errores, debe reiniciar el nodo de nuevo.

Antes de empezar

- Si está utilizando NSE con un servidor de administración de claves externo (KMIP), elimine la base de datos del administrador de claves externo.

"Transición a la gestión de claves incorporada desde la gestión de claves externas"

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Configure el entorno MetroCluster antes de configurar el Administrador de claves integrado.

Pasos

1. Inicie la configuración del gestor de claves:

```
security key-manager setup -enable-cc-mode yes|no
```



A partir de ONTAP 9.4, puede usar la `-enable-cc-mode yes` opción para solicitar que los usuarios introduzcan la frase de contraseña del administrador de claves después de un reinicio. Para NVE, si establece `-enable-cc-mode yes`, los volúmenes que cree con los `volume create volume move start` comandos y se cifran automáticamente.

En el siguiente ejemplo, se inicia la configuración del gestor de claves en `cluster1` sin necesidad de introducir la clave de acceso después de cada reinicio:

```
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. Introduzca `yes` en el aviso para configurar la gestión de claves incorporada.
3. En el indicador de frase de contraseña, introduzca una frase de paso entre 32 y 256 caracteres, o bien, para `"cc-mode"`, una frase de paso entre 64 y 256 caracteres.



Si la frase de paso `"cc-mode"` especificada es menor de 64 caracteres, hay un retraso de cinco segundos antes de que la operación de configuración del gestor de claves vuelva a mostrar la indicación de contraseña.

4. En la solicitud de confirmación de contraseña, vuelva a introducir la frase de contraseña.
5. Compruebe que las claves estén configuradas para todos los nodos:

```
security key-manager show-key-store
```

Obtenga más información sobre `security key-manager show-key-store` en el ["Referencia de comandos del ONTAP"](#).

```
cluster1::> security key-manager show-key-store

Node: node1
Key Store: onboard
Key ID                                     Used By
-----
-----
<id_value> NSE-AK
<id_value> NSE-AK

Node: node2
Key Store: onboard
Key ID                                     Used By
-----
-----
<id_value> NSE-AK
<id_value> NSE-AK
```

Después de terminar

ONTAP realiza automáticamente una copia de seguridad de la información de administración de claves en la base de datos replicada (RDB) del clúster.

Después de configurar la contraseña del Onboard Key Manager, realice manualmente una copia de seguridad de la información en una ubicación segura fuera del sistema de almacenamiento. Ver ["Realice un backup manual de la información de gestión de claves incorporada"](#).

Información relacionada

- ["Realice un backup manual de la información de gestión de claves incorporada"](#)
- ["configuración del administrador de claves de seguridad"](#)
- ["administrador de claves de seguridad mostrar almacén de claves"](#)
- ["Transición a la gestión de claves incorporada desde la gestión de claves externas"](#)

Asignar una clave de autenticación de datos a una unidad FIPS o SED con administración de claves integrada de ONTAP

Puede utilizar `storage encryption disk modify` el comando para asignar una clave de autenticación de datos a una unidad FIPS o SED. Los nodos de clúster usan esta clave para acceder a los datos de la unidad.

Acerca de esta tarea

Una unidad de autocifrado está protegida contra el acceso no autorizado solo si su ID de clave de autenticación se configura como un valor no predeterminado. El ID seguro del fabricante (MSID), que tiene el ID de clave 0x0, es el valor predeterminado estándar para las unidades SAS. Para las unidades NVMe, el valor predeterminado estándar es una clave nula, que se representa como un ID de clave en blanco. Cuando se asigna el ID de clave a una unidad de autocifrado, el sistema cambia el ID de clave de autenticación por un valor no predeterminado.

Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

Pasos

1. Asigne una clave de autenticación de datos a una unidad FIPS o SED:

```
storage encryption disk modify -disk disk_ID -data-key-id key_ID
```

Obtenga más información sobre `storage encryption disk modify` en el ["Referencia de comandos del ONTAP"](#).



Puede usar el `security key-manager key query -key-type NSE-AK` comando para ver ID de claves.

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id  
<id_value>
```

```
Info: Starting modify on 14 disks.  
View the status of the operation by using the  
storage encryption disk show-status command.
```

Obtenga más información sobre `security key-manager key query` en el ["Referencia de comandos del ONTAP"](#).

2. Compruebe que se han asignado las claves de autenticación:

```
storage encryption disk show
```

Obtenga más información sobre `storage encryption disk show` en el ["Referencia de comandos del ONTAP"](#).

```
cluster1::> storage encryption disk show  
Disk      Mode Data Key ID  
-----  
-----  
0.0.0     data <id_value>  
0.0.1     data <id_value>  
[...]
```

Información relacionada

- ["Mostrar disco de cifrado de almacenamiento"](#)
- ["estado del disco de cifrado de almacenamiento"](#)

Asignar una clave de autenticación FIPS 140-2 a una unidad FIPS de ONTAP

Puede usar `storage encryption disk modify` el comando con `-fips-key-id` la opción para asignar una clave de autenticación FIPS 140-2 a una unidad FIPS. Los nodos de clúster utilizan esta clave para las operaciones de unidad distintas del acceso a los datos, como evitar ataques de denegación de servicio en la unidad.

Acerca de esta tarea

Es posible que la configuración de seguridad requiera el uso de claves diferentes para la autenticación de datos y la autenticación FIPS 140-2-2. Si no es así, puede usar la misma clave de autenticación para el cumplimiento de FIPS que se usa para acceder a los datos.

Este procedimiento no causa interrupciones.

Antes de empezar

El firmware de la unidad debe ser compatible con el cumplimiento de normativas FIPS 140-2-2. El ["Herramienta de matriz de interoperabilidad de NetApp"](#) contiene información sobre las versiones de firmware de la unidad compatibles.

Pasos

1. Primero debe asegurarse de que ha asignado una clave de autenticación de datos. Esto se puede hacer con un [gestor de claves externas](#) o un [gestión de claves incorporada](#). Compruebe que la clave se ha asignado con el comando `storage encryption disk show`.
2. Asigne una clave de autenticación FIPS 140-2 a SED:

```
storage encryption disk modify -disk disk_id -fips-key-id  
fips_authentication_key_id
```

Puede usar el `security key-manager query` comando para ver ID de claves.

```
cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id  
<id_value>
```

```
Info: Starting modify on 14 disks.  
View the status of the operation by using the  
storage encryption disk show-status command.
```

3. Compruebe que se ha asignado la clave de autenticación:

```
storage encryption disk show -fips
```

Obtenga más información sobre `storage encryption disk show` en el ["Referencia de comandos del ONTAP"](#).

```
cluster1::> storage encryption disk show -fips
Disk      Mode FIPS-Compliance Key ID
-----
2.10.0    full <id_value>
2.10.1    full <id_value>
[...]
```

Información relacionada

- ["modificar disco de cifrado de almacenamiento"](#)
- ["Mostrar disco de cifrado de almacenamiento"](#)
- ["estado del disco de cifrado de almacenamiento"](#)

Habilite el modo conforme a FIPS para todo el clúster para las conexiones del servidor KMIP en ONTAP

Puede usar `security config modify` el comando con `-is-fips-enabled` la opción de habilitar un modo conforme a FIPS para todo el clúster con los datos sobre transferencia. Al hacerlo, obliga al clúster a usar OpenSSL en modo FIPS al conectarse a servidores KMIP.

Acerca de esta tarea

Cuando habilita el modo compatible con FIPS en todo el clúster, el clúster utilizará únicamente paquetes de cifrado validados TLS1.2 y FIPS. El modo compatible con FIPS para todo el clúster está deshabilitado de forma predeterminada.

Debe reiniciar los nodos del clúster de forma manual después de modificar la configuración de seguridad de todo el clúster.

Antes de empezar

- La controladora de almacenamiento debe configurarse en modo conforme a FIPS.
- Todos los servidores KMIP deben ser compatibles con TLSv1.2. El sistema requiere TLSv1.2 para completar la conexión con el servidor KMIP cuando se habilita el modo compatible con FIPS en todo el clúster.

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Compruebe que TLSv1.2 es compatible:

```
security config show -supported-protocols
```

Obtenga más información sobre `security config show` en el ["Referencia de comandos del ONTAP"](#).

```
cluster1::> security config show
```

	Cluster		Cluster
Security			
Interface	FIPS Mode	Supported Protocols	Supported Ciphers Config
Ready			
-----	-----	-----	-----

SSL	false	TLSv1.2, TLSv1.1, TLSv1	ALL:!LOW: !aNULL:!EXP: !eNULL
			yes

3. Habilite el modo compatible con FIPS para todo el clúster:

```
security config modify -is-fips-enabled true -interface SSL
```

Obtenga más información sobre `security config modify` en el ["Referencia de comandos del ONTAP"](#).

4. Reiniciar nodos del clúster de forma manual.

5. Compruebe que el modo compatible con FIPS en todo el clúster esté habilitado:

```
security config show
```

```
cluster1::> security config show
```

	Cluster		Cluster
Security			
Interface	FIPS Mode	Supported Protocols	Supported Ciphers Config
Ready			
-----	-----	-----	-----

SSL	true	TLSv1.2, TLSv1.1	ALL:!LOW: !aNULL:!EXP: !eNULL:!RC4
			yes

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.