



# **Proteja los sistemas de archivos Unix**

## **SnapCenter software**

NetApp  
January 09, 2026

This PDF was generated from [https://docs.netapp.com/es-es/snapcenter/protect-scu/concept\\_overview\\_snapcenter\\_plug\\_in\\_for\\_UNIX\\_file\\_systems.html](https://docs.netapp.com/es-es/snapcenter/protect-scu/concept_overview_snapcenter_plug_in_for_UNIX_file_systems.html) on January 09, 2026. Always check docs.netapp.com for the latest.

# Tabla de contenidos

Proteja los sistemas de archivos Unix .....	1
Tareas que pueden llevarse a cabo con el plugin de SnapCenter para sistemas de archivos Unix .....	1
Configuraciones admitidas .....	1
Limitaciones .....	2
Funciones .....	2
Instale el plugin de SnapCenter para sistemas de archivos Unix .....	2
Requisitos previos para añadir hosts e instalar el paquete de plugins para Linux .....	2
Añada hosts e instale el paquete de plugins para Linux mediante la interfaz gráfica de usuario .....	4
Configure el servicio de cargador de plugins de SnapCenter .....	7
Configure el certificado de CA con el servicio de cargador de plugins de SnapCenter (SPL) en el host Linux .....	10
Habilite certificados de CA para plugins .....	13
Instale el plugin de SnapCenter para VMware vSphere .....	14
Implemente el certificado de CA .....	14
Configure el archivo CRL .....	14
Prepárese para la protección de sistemas de archivos Unix .....	14
Hacer backup de sistemas de archivos Unix .....	15
Descubra los sistemas de archivos UNIX disponibles para backup .....	15
Crear directivas de backup para sistemas de archivos Unix .....	15
Cree grupos de recursos y adjunte políticas para sistemas de archivos Unix .....	18
Cree grupos de recursos y habilite la protección secundaria para sistemas de archivos Unix en sistemas ASA R2 .....	20
Hacer backup de sistemas de archivos Unix .....	23
Realizar un backup de los grupos de recursos de sistemas de archivos Unix .....	24
Supervisar la copia de seguridad de sistemas de archivos Unix .....	25
Vea los sistemas de archivos Unix protegidos en la página Topology .....	26
Restaurar y recuperar sistemas de archivos Unix .....	28
Restaurar sistemas de archivos Unix .....	28
Supervisar las operaciones de restauración de sistemas de archivos Unix .....	30
Clonar sistemas de archivos Unix .....	31
Clonar backup de sistema de archivos Unix .....	31
Divida un clon .....	32
Supervisar operaciones de clonación de sistemas de archivos Unix .....	33

# Proteja los sistemas de archivos Unix

## Tareas que pueden llevarse a cabo con el plugin de SnapCenter para sistemas de archivos Unix

Cuando el plugin para sistemas de archivos Unix está instalado en el entorno, es posible usar SnapCenter para realizar backup, restaurar y clonar sistemas de archivos Unix. También es posible ejecutar tareas complementarias a estas operaciones.

- Detectar recursos
- Hacer backup de sistemas de archivos Unix
- Programar operaciones de backup
- Restaurar backups de sistema de archivos
- Clonar backups de sistema de archivos
- Supervisar operaciones de backup, de restauración y de clonado

### Configuraciones admitidas

Elemento	Configuración admitida
Entornos	<ul style="list-style-type: none"><li>• Servidor físico</li><li>• Servidor virtual</li></ul> <p>Almacenes de datos VVOL en NFS y SAN. El almacén de datos VVOL solo se puede aprovisionar con ONTAP Tools para VMware vSphere.</p>
Sistemas operativos	<ul style="list-style-type: none"><li>• Red Hat Enterprise Linux</li><li>• Oracle Linux</li><li>• SUSE Linux Enterprise Server (SLES)</li></ul>
Sistemas de ficheros	<ul style="list-style-type: none"><li>• SAN:<ul style="list-style-type: none"><li>◦ Sistemas de archivos basados en LVM y no LVM</li><li>◦ LVM sobre VMDK ext3, ext4 y xfs</li></ul></li><li>• NFS: NFS v3, NFS v4.x</li></ul>
Protocolos	<ul style="list-style-type: none"><li>• FC</li><li>• FCoE</li><li>• iSCSI</li><li>• NFS</li></ul>

Elemento	Configuración admitida
Multivía	sí

## Limitaciones

- No se admite la combinación de RDM y discos virtuales en un grupo de volúmenes.
- No se admite la restauración de nivel de archivos.

Sin embargo, puede realizar manualmente una restauración en el nivel de archivos clonando el backup y luego copiando los archivos manualmente.

- No se admite la combinación de sistemas de archivos distribuidos entre VMDK procedentes de NFS y almacenes de datos VMFS.
- No se admite NVMe.
- No se admite el aprovisionamiento.

## Funciones

- Permite al plugin para bases de datos de Oracle realizar operaciones de protección de datos en bases de datos de Oracle manejar la pila de almacenamiento del host subyacente en sistemas Linux o AIX
- Admite los protocolos de sistema de archivos de red (NFS) y red de área de almacenamiento (SAN) en un sistema de almacenamiento que ejecuta ONTAP.
- En el caso de los sistemas Linux, las bases de datos de Oracle en LUN de VMDK y RDM se admiten cuando se implementa el plugin de SnapCenter para VMware vSphere y se registra el plugin con SnapCenter.
- Admite Mount Guard para AIX en sistemas DE archivos SAN y diseño de LVM.
- Admite el sistema de archivos mejorado Journaled (JFS2) con registro en línea en sistemas DE archivos SAN y diseño LVM sólo para sistemas AIX.

Se admiten los dispositivos nativos DE SAN, sistemas de archivos y diseños de LVM creados en dispositivos SAN.

- Automatiza las operaciones de backup, restauración y clonado para sistemas de archivos UNIX en el entorno de SnapCenter

## Instale el plugin de SnapCenter para sistemas de archivos Unix

### Requisitos previos para añadir hosts e instalar el paquete de plugins para Linux

Antes de añadir un host e instalar el paquete de plugins para Linux, debe satisfacer todos los requisitos.

- Si utiliza iSCSI, el servicio iSCSI debe estar en ejecución.
- Puede usar la autenticación basada en contraseña para el usuario raíz o no raíz, o para la autenticación basada en la clave SSH.

El complemento de SnapCenter para sistemas de archivos Unix puede ser instalado por un usuario que no sea root. Sin embargo, debe configurar los privilegios sudo para el usuario no raíz para instalar e iniciar el proceso del plugin. Después de instalar el plugin, los procesos se ejecutan como un usuario efectivo que no es raíz.

- Cree credenciales con modo de autenticación como Linux para el usuario de instalación.
- Debe haber instalado Java 11 en el host Linux.




Asegúrese de haber instalado únicamente la edición certificada de JAVA 11 en el host Linux.


Para obtener información sobre CÓMO descargar JAVA, consulte: ["Descargas de Java para todos los sistemas operativos"](#)

- Debe tener **bash** como shell por defecto para la instalación del plug-in.

### Requisitos del host Linux

Debe asegurarse de que el host cumpla con los requisitos antes de instalar el paquete de plugins de SnapCenter para Linux.

Elemento	Requisitos
Sistemas operativos	<ul style="list-style-type: none"><li>• Red Hat Enterprise Linux</li><li>• Oracle Linux</li><li>• SUSE Linux Enterprise Server (SLES)</li></ul>
RAM mínima para el plugin de SnapCenter en el host	2 GB
Espacio de registro e instalación mínimo para el plugin de SnapCenter en el host	<div>2 GB</div> <div> Debe asignar el espacio en disco suficiente y supervisar el consumo de almacenamiento en la carpeta de registros. El espacio de registro necesario varía en función de la cantidad de entidades que se han de proteger y la frecuencia de las operaciones de protección de datos. Si no hay espacio en disco suficiente, no se crearán registros de las operaciones ejecutadas recientemente.</div>

Elemento	Requisitos
Paquetes de software obligatorios	<p>Java 11 Oracle Java y OpenJDK</p> <div>  <p>Asegúrese de haber instalado únicamente la edición certificada de JAVA 11 en el host Linux.</p> </div> <p>Si ha actualizado JAVA a la versión más reciente, debe asegurarse de que la opción JAVA_HOME ubicada en /var/opt/snapcenter/spl/etc/spl.properties esté configurada en la versión DE JAVA correcta y en la ruta de acceso correcta.</p>

Para obtener la información más reciente sobre las versiones compatibles, consulte la ["Herramienta de matriz de interoperabilidad de NetApp"](#) .


## Añada hosts e instale el paquete de plugins para Linux mediante la interfaz gráfica de usuario

Puede utilizar la página Add Host para añadir hosts y, a continuación, instalar el paquete de plugins de SnapCenter para Linux. Los plugins se instalan automáticamente en hosts remotos.

- Pasos\*


1. En el panel de navegación de la izquierda, haga clic en **hosts**.
2. Compruebe que la ficha **Managed hosts** está seleccionada en la parte superior.
3. Haga clic en **Agregar**.
4. En la página hosts, realice las siguientes acciones:

Para este campo...	Realice lo siguiente...
Tipo de host	Seleccione <b>Linux</b> como tipo de host.
Nombre de host	<p>Introduzca el nombre de dominio completamente cualificado (FQDN) o la dirección IP del host.</p> <p>SnapCenter depende de una configuración adecuada del DNS. Por lo tanto, lo más recomendable es introducir el FQDN.</p> <p>Si va a añadir un host mediante SnapCenter y el host forma parte de un subdominio, debe proporcionar el FQDN.</p>

Para este campo...	Realice lo siguiente...
Credenciales	<p>Seleccione el nombre de credencial que ha creado o cree nuevas credenciales.</p> <p>Las credenciales deben tener derechos de administrador en el host remoto. Para obtener más detalles, consulte la información acerca de crear credenciales.</p> <p>Puede ver los detalles sobre las credenciales colocando el cursor sobre el nombre de las credenciales que ha especificado.</p> <div>  <p>El modo de autenticación de las credenciales se determina por el tipo de host que especifique en el asistente Add host.</p> </div>

5. En la sección Seleccionar plugins para instalar, seleccione **Sistemas de archivos Unix**.

6. (Opcional) haga clic en **más opciones**.

Para este campo...	Realice lo siguiente...
Puerto	<p>Conserve el número de puerto predeterminado o especifique el número de puerto.</p> <p>El número de puerto predeterminado es 8145. Si el servidor SnapCenter se instaló en un puerto personalizado, ese número de puerto se mostrará como el puerto predeterminado.</p> <div>  <p>Si ha instalado plugins manualmente y ha especificado un puerto personalizado, debe especificar el mismo puerto. De lo contrario, la operación dará error.</p> </div>
Ruta de instalación	<p>La ruta predeterminada es <i>/opt/NetApp/snapcenter</i>.</p> <p>Opcionalmente, puede personalizar la ruta. Si utiliza la ruta personalizada, asegúrese de que el contenido predeterminado de los sudoers se actualiza con la ruta personalizada.</p>
Omitir comprobaciones opcionales de preinstalación	<p>Seleccione esta casilla de comprobación si ya ha instalado los plugins manualmente y no desea validar si el host cumple con los requisitos para la instalación del plugin.</p>

## 7. Haga clic en **Enviar**.

Si no ha seleccionado la casilla de comprobación Skip prechecks, el host se valida para comprobar si cumple con los requisitos para la instalación del plugin.



La secuencia de comandos comprobaciones previas no valida el estado del firewall del puerto del plugin si se especifica en las reglas de rechazo del firewall.

Si no se cumplen los requisitos mínimos, se muestran los mensajes de error o advertencia pertinentes. Si el error está relacionado con el espacio en disco o RAM, es posible actualizar el archivo web.config ubicado en *C:\Program Files\NetApp\SnapCenter WebApp* para modificar los valores predeterminados. Si el error está relacionado con otros parámetros, primero tendrá que solucionar el problema.



En una configuración de alta disponibilidad, si actualiza el archivo web.config, debe actualizar el archivo en ambos nodos.

## 8. Compruebe la huella y, a continuación, haga clic en **Confirmar y enviar**.



SnapCenter no admite el algoritmo ECDSA.



La verificación de huellas digitales es obligatoria aunque se haya añadido anteriormente el mismo host a SnapCenter y se haya confirmado la huella.

## 1. Supervise el progreso de la instalación.

Los archivos de registro específicos de la instalación están en */custom\_location/snapcenter/logs*.

### resultado

Todos los sistemas de archivos montados en el host se detectan automáticamente y se muestran en la página Resources. Si no aparece nada, haga clic en **Actualizar recursos**.

### Supervise el estado de la instalación

Puede supervisar el progreso de la instalación del paquete de plugins de SnapCenter mediante la página Jobs. Tal vez desee comprobar el progreso de la instalación para determinar si está completo o si hay algún problema.

### Acerca de esta tarea

Los siguientes iconos aparecen en la página Jobs e indican el estado de la operación:

- En curso
- Completado correctamente
- Error
- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola

### Pasos

1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **trabajos**.
3. En la página **Jobs**, para filtrar la lista de modo que solo se enumeren las operaciones de instalación de plug-in, haga lo siguiente:
  - a. Haga clic en **filtro**.
  - b. Opcional: Indique las fechas de inicio y finalización.
  - c. En el menú desplegable Tipo, seleccione **instalación Plug-in**.
  - d. En el menú desplegable de estado, seleccione el estado de instalación.
  - e. Haga clic en **aplicar**.
4. Seleccione el trabajo de instalación y haga clic en **Detalles** para ver los detalles del trabajo.
5. En la página **Detalles del trabajo**, haga clic en **Ver registros**.

## Configure el servicio de cargador de plugins de SnapCenter

El servicio de cargador de plugins de SnapCenter carga el paquete del plugin para Linux con el fin de interactuar con el servidor de SnapCenter. El servicio de cargador de plugins de SnapCenter se instala cuando se instala el paquete de plugins de SnapCenter para Linux.


### Acerca de esta tarea


Después de instalar el paquete de plugins de SnapCenter para Linux, el servicio de cargador de plugins de SnapCenter se inicia automáticamente. Si el servicio de cargador de plugins de SnapCenter no se inicia de forma automática, tendrá que:

- Asegúrese de que no se haya eliminado el directorio donde está funcionando el plugin
- Aumente el espacio de la memoria asignado a la máquina virtual Java

El archivo `spl.properties`, que se encuentra en `/custom_location/NetApp/snapcenter/spl/etc/`, contiene los parámetros siguientes. Los valores predeterminados se asignan a estos parámetros.

Nombre del parámetro	Descripción
NIVEL_REGISTRO	Muestra los niveles de los registros que se admiten.  Los posibles valores son TRACE, DEBUG, INFO, WARN, ERROR, Y FATAL.
SPL_PROTOCOL	Muestra el protocolo que admite el cargador del plugin de SnapCenter.  Solo se admite el protocolo HTTPS. Puede agregar el valor si falta el valor predeterminado.

Nombre del parámetro	Descripción
SNAPCENTER_SERVER_PROTOCOL	<p>Muestra el protocolo compatible con SnapCenter Server.</p> <p>Solo se admite el protocolo HTTPS. Puede agregar el valor si falta el valor predeterminado.</p>
SKIP_JAVAHOME_UPDATE	<p>De forma predeterminada, el servicio SPL detecta la ruta de Java y el parámetro update JAVA_HOME.</p> <p>Por lo tanto, el valor predeterminado se establece en FALSE. Puede establecer EN TRUE si desea deshabilitar el comportamiento predeterminado y corregir manualmente la ruta de acceso java.</p>
SPL_KEYSTORE_PASS	<p>Muestra la contraseña del archivo keystore.</p> <p>Puede cambiar este valor solo si cambia la contraseña o crea un nuevo archivo keystore.</p>
SPL_PORT	<p>Muestra el número de puerto en el que se está ejecutando el cargador del plugin de SnapCenter.</p> <p>Puede agregar el valor si falta el valor predeterminado.</p> <div>  <p>No debe cambiar el valor después de instalar los plugins.</p> </div>
SNAPCENTER_SERVER_HOST	Muestra la dirección IP o el nombre de host del servidor SnapCenter.
SPL_KEYSTORE_RUTA	Muestra la ruta absoluta del archivo keystore.
SNAPCENTER_SERVER_PORT	Muestra el número de puerto en el que se está ejecutando el servidor SnapCenter.

Nombre del parámetro	Descripción
LOGS_MAX_COUNT	<p>Muestra el número de archivos de registro del cargador del plugin de SnapCenter que se conservan en la carpeta <code>/custom_location/snapcenter/spl/logs</code>.</p> <p>El valor predeterminado se establece en 5000. Si la cantidad es superior al valor especificado, se conservan los 5000 últimos archivos modificados. La comprobación del número de archivos se realiza de forma automática cada 24 horas desde el momento en que se inicia el servicio de cargador de plugins de SnapCenter.</p> <div>  <p>Si elimina manualmente el archivo <code>spl.properties</code>, el número de archivos que se desea conservar se establece en 9999.</p> </div>
JAVA_HOME	<p>Muestra la ruta del directorio absoluto DE JAVA_HOME que se utiliza para iniciar el servicio SPL.</p> <p>Esta ruta se determina durante la instalación y como parte del SPL de inicio.</p>
LOG_MAX_SIZE	<p>Muestra el tamaño máximo del archivo de registro de trabajos.</p> <p>Una vez alcanzado el tamaño máximo, el archivo de registro se comprime y los registros se escriben en el nuevo archivo de ese trabajo.</p>
RETAIN_LOGS_OF_LAST_DAYS	<p>Muestra el número de días hasta los que se conservan los registros.</p>
ENABLE_CERTIFICATE_VALIDATION	<p>Muestra TRUE cuando la validación de certificados de CA está habilitada para el host.</p> <p>Puede habilitar o deshabilitar este parámetro editando la versión <code>spl.properties</code> o bien mediante la interfaz gráfica de usuario o el cmdlet de SnapCenter.</p>

Si cualquiera de estos parámetros no se asignan al valor predeterminado, o si desea asignar o cambiar el valor, puede modificar el archivo `spl.properties`. También puede verificar el archivo `spl.properties` y editarlo para solucionar los problemas relacionados con los valores que se asignan a los parámetros. Después de modificar el archivo `spl.properties`, tendrá que reiniciar el servicio de cargador de plugins de SnapCenter.

- Pasos\*

1. Ejecute una de las siguientes acciones, según sea necesario:

- Inicie el servicio de cargador de plugins de SnapCenter:
  - Como usuario root, ejecute: `/custom_location/NetApp/snapcenter/spl/bin/spl start`
  - Como usuario no raíz, ejecute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`
- Detenga el servicio de cargador de plugins de SnapCenter:
  - Como usuario root, ejecute: `/custom_location/NetApp/snapcenter/spl/bin/spl stop`
  - Como usuario no raíz, ejecute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`



Puede utilizar la opción `-force` con el comando `stop` para detener el servicio de cargador de plugins de SnapCenter enérgicamente. Sin embargo, debe ser cauteloso antes de hacerlo, ya que también termina las operaciones existentes.

- Reinicie el servicio de cargador de plugins de SnapCenter:
  - Como usuario root, ejecute: `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
  - Como usuario no raíz, ejecute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`
- Busque el estado del servicio de cargador de plugins de SnapCenter:
  - Como usuario root, ejecute: `/custom_location/NetApp/snapcenter/spl/bin/spl status`
  - Como usuario no root, ejecute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`
- Busque el cambio en el servicio de cargador de plugins de SnapCenter:
  - Como usuario root, ejecute: `/custom_location/NetApp/snapcenter/spl/bin/spl change`
  - Como usuario no raíz, ejecute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

## Configure el certificado de CA con el servicio de cargador de plugins de SnapCenter (SPL) en el host Linux

Debe gestionar la contraseña del almacén de claves de SPL y su certificado, configurar el certificado de CA, configurar los certificados raíz o intermedios para el almacén de confianza de SPL y configurar la pareja de claves firmadas de CA para el almacén de confianza de SPL con el servicio de cargador de plugins de SnapCenter para activar el certificado digital instalado.



SPL utiliza el archivo `'keystore.jks'`, que se encuentra en `'/var/opt/snapcenter/spl/etc'` tanto como su almacén de confianza como su almacén de claves.

## Gestione la contraseña para el almacén de claves SPL y el alias de la pareja de claves firmada de CA en uso

- Pasos\*

1. Puede recuperar la contraseña predeterminada del almacén de claves del SPL desde el archivo de propiedades del SPL.

Es el valor correspondiente a la clave 'PL\_KEYSTORE\_PASS'.

2. Cambie la contraseña del almacén de claves:

```
keytool -storepasswd -keystore keystore.jks
. Cambie la contraseña para todos los alias de las entradas de clave
privada en el almacén de claves por la misma contraseña utilizada
para el almacén de claves:
```

```
keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```

Actualice lo mismo para la clave SPL\_KEYSTORE\_PASS en el archivo spl.properties.1.

3. Reinicie el servicio después de cambiar la contraseña.



La contraseña para el almacén de claves SPL y para toda la contraseña de alias asociada de la clave privada debe ser la misma.

## Configure los certificados intermedios o de raíz para el almacén de confianza SPL

Debe configurar los certificados intermedios o de raíz sin la clave privada en el almacén de confianza de SPL.

- Pasos\*

1. Desplácese hasta la carpeta que contiene el almacén de claves SPL: `/var/opt/snapcenter/spl/etc`.
2. Busque el archivo 'keystore.jks'.
3. Enumere los certificados añadidos al almacén de claves:

```
keytool -list -v -keystore keystore.jks
. Añada un certificado raíz o intermedio:
```

```
keytool -import -trustcacerts -alias
<AliasNameForCertificateToBeImported> -file /<CertificatePath>
-keystore keystore.jks
. Reinicie el servicio después de configurar los certificados raíz o
intermedios en el almacén de confianza de SPL.
```



Debe añadir el certificado de CA raíz y luego los certificados de CA intermedios.

### Configure la pareja de claves firmados de CA para el almacén de confianza SPL

Debe configurar la pareja de claves firmada de CA en el almacén de confianza del SPL.

- Pasos\*

1. Desplácese hasta la carpeta que contiene el almacén de claves /var/opt/snapcenter/spl/etc. de SPL
2. Busque el archivo 'keystore.jks'.
3. Enumere los certificados añadidos al almacén de claves:

```
keytool -list -v -keystore keystore.jks
. Agregue el certificado de CA con clave pública y privada.
```

```
keytool -importkeystore -srckeystore <CertificatePathToImport>
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
. Enumere los certificados añadidos al almacén de claves.
```

```
keytool -list -v -keystore keystore.jks
. Compruebe que el almacén de claves contiene el alias
correspondiente al nuevo certificado de CA, que se añadió al almacén
de claves.
. Cambie la contraseña de clave privada añadida para el certificado
de CA a la contraseña del almacén de claves.
```

La contraseña predeterminada del almacén de claves SPL es el valor de la clave SPL\_KEYSTORE\_PASS en el archivo spl.properties.

```
keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>"
-keystore keystore.jks
. Si el nombre del alias del certificado de CA es largo y contiene
espacio o caracteres especiales ("*", ",", "), cambie el nombre del alias
por un nombre simple:
```

```
keytool -changealias -alias "<OriginalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
. Configure el nombre de alias del almacén de claves ubicado en el
archivo spl.properties.
```

Actualice este valor contra la clave SPL\_CERTIFICATE\_ALIAS.

4. Reinicie el servicio después de configurar el par de claves firmado de CA en el almacén de confianza SPL.

## Configurar la lista de revocación de certificados (CRL) para SPL

Debe configurar la CRL para SPL

### Acerca de esta tarea

- SPL buscará los archivos CRL en un directorio preconfigurado.
- El directorio predeterminado para los archivos CRL de SPL es `/var/opt/snapcenter/spl/etc/crl`.
- Pasos\*
  1. Puede modificar y actualizar el directorio predeterminado del archivo `spl.properties` con respecto a la CLAVE `SPL_CRL_PATH`.
  2. Puede colocar más de un archivo CRL en este directorio.

Los certificados entrantes se verificarán en cada CRL.

## Habilite certificados de CA para plugins

Debe configurar los certificados de CA e implementar los certificados de CA en SnapCenter Server y los hosts de plugin correspondientes. Debe habilitar la validación de certificado de CA para los plugins.

### Antes de empezar

- Es posible habilitar o deshabilitar los certificados de CA con el cmdlet `run set-SmCertificateSettings`.
- Puede mostrar el estado del certificado de los plugins con el `Get-SmCertificateSettings`.





La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando `Get-Help nombre_comando`. Alternativamente, también puede consultar la ["Guía de referencia de cmdlets de SnapCenter Software"](#).

### Pasos

1. En el panel de navegación de la izquierda, haga clic en **hosts**.
2. En la página hosts, haga clic en **Managed hosts**.
3. Seleccione uno o varios hosts de plugins.
4. Haga clic en **más opciones**.
5. Seleccione **Activar validación de certificados**.

### Después de terminar

El host de la pestaña Managed hosts muestra un candado y el color del candado indica el estado de la conexión entre SnapCenter Server y el host del plugin.

-  Indica que el certificado de CA no está habilitado ni asignado al host del plugin.
-  Indica que el certificado de CA se ha validado correctamente.
-  Indica que el certificado de CA no se ha podido validar.
-  indica que no se pudo recuperar la información de conexión.



Cuando el estado es amarillo o verde, las operaciones de protección de datos se completan correctamente.

## Instale el plugin de SnapCenter para VMware vSphere

Si su base de datos o sistema de archivos están almacenados en máquinas virtuales (VM) o si desea proteger VM y almacenes de datos, debe implementar el dispositivo virtual del plugin de SnapCenter para VMware vSphere.

Para obtener información sobre la implementación, consulte ["Visión General de la implementación"](#).

### Implemente el certificado de CA

Para configurar el certificado de CA con el plugin de SnapCenter para VMware vSphere, consulte ["Crear o importar certificado SSL"](#).

### Configure el archivo CRL

El plugin de SnapCenter para VMware vSphere busca los archivos CRL en un directorio preconfigurado. El directorio predeterminado de los archivos CRL del plugin SnapCenter para VMware vSphere es `/opt/netapp/config/crl`.

Puede colocar más de un archivo CRL en este directorio. Los certificados entrantes se verificarán en cada CRL.

## Prepárese para la protección de sistemas de archivos Unix

Antes de ejecutar una operación de protección de datos, como un backup, un clon o una restauración, debe configurar el entorno. También debe configurar SnapCenter Server para que use las tecnologías SnapMirror y SnapVault.

Para aprovechar las ventajas de las tecnologías SnapVault y SnapMirror, debe configurar e inicializar una relación de protección de datos entre el volumen de origen y el volumen de destino en el dispositivo de almacenamiento. Puede usar NetApp System Manager o la línea de comandos de la consola de almacenamiento para ejecutar estas tareas.

Antes de utilizar el plugin para sistemas de archivos Unix, el administrador de SnapCenter debe instalar y configurar el servidor SnapCenter y llevar a cabo las tareas de los requisitos previos.

- Instalar y configurar SnapCenter Server. ["Leer más"](#)
- Configure el entorno de SnapCenter añadiendo conexiones con el sistema de almacenamiento. ["Leer más"](#)



SnapCenter no admite varias SVM con el mismo nombre en clústeres diferentes. Cada SVM registrada en SnapCenter con registro de SVM o de clúster debe ser única.

- Añada hosts, instale los plugins y detecte los recursos.
- Si va a utilizar SnapCenter Server para proteger sistemas de archivos Unix que residen en LUN o VMDK de VMware RDM, debe poner en marcha el plugin de SnapCenter para VMware vSphere y registrar el

plugin con SnapCenter.

- Instale Java en el host Linux.
- Configure SnapMirror y SnapVault en ONTAP si quiere realizar una replicación de backup.

## Hacer backup de sistemas de archivos Unix

### Descubra los sistemas de archivos UNIX disponibles para backup

Después de instalar el plugin, se detectan automáticamente todos los sistemas de archivos de ese host y se muestran en la página Resources. Puede añadir estos sistemas de archivos a grupos de recursos para realizar operaciones de protección de datos.

#### Antes de empezar

- Debe haber completado tareas, como instalar SnapCenter Server, añadir hosts y crear conexiones del sistema de almacenamiento.
- Si los sistemas de archivos residen en un disco de máquina virtual (VMDK) o una asignación de dispositivo sin formato (RDM), debe implementar el plugin de SnapCenter para VMware vSphere y registrar el plugin con SnapCenter.

Para obtener más información, consulte ["Ponga en marcha el plugin de SnapCenter para VMware vSphere"](#).

#### Pasos

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página Recursos, seleccione **Ruta** en la lista Ver.
3. Haga clic en **Actualizar recursos**.

Los sistemas de archivos se muestran junto con cierta información, como el tipo, el nombre de host, las políticas y los grupos de recursos asociados, y el estado.

### Crear directivas de backup para sistemas de archivos Unix

Antes de usar SnapCenter para realizar backups de sistemas de archivos Unix, debe crear una política de backup para el recurso o el grupo de recursos que desea incluir en el backup. Una política de backup es un conjunto de reglas que rigen cómo gestionar, programar y retener backups. También puede especificar la configuración de replicación, script y tipo de backup. Crear una política permite ahorrar tiempo cuando se desea volver a utilizar esa política en otro recurso o grupo de recursos.

#### Antes de empezar

- En el marco de los preparativos para la protección de datos, completó tareas como instalar SnapCenter, añadir hosts, detectar sistemas de archivos y crear conexiones con el sistema de almacenamiento.
- Si desea replicar snapshots en un almacenamiento secundario con snapmirror o snapvault, el administrador de SnapCenter debe haberle asignado las SVM de los volúmenes de origen y de destino.

- Revise los requisitos previos y las limitaciones específicos de SnapMirror Active Sync. Para obtener más información, consulte "[Límites de objetos para la sincronización activa de SnapMirror](#)".

#### Acerca de esta tarea

- SnapLock
  - Si se selecciona la opción 'Retain the backup copies for a specific number of days', el período de retención de SnapLock debe ser menor o igual que los días de retención mencionados.

Si se especifica un período de bloqueo de Snapshot, se evita la eliminación de las snapshots hasta que caduque el período de retención. Esto podría llevar a retener un número mayor de instantáneas que el recuento especificado en la política.

Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.



#### Pasos

1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
2. En la página Configuración, haga clic en **Directivas**.
3. Seleccione **Unix File Systems** de la lista desplegable.
4. Haga clic en **Nuevo**.
5. En la página Name, escriba el nombre de la política y sus detalles.
6. En la página Backup and Replication, realice las siguientes acciones:
  - a. Especifique la configuración de backup.
  - b. Especifique la frecuencia de programación seleccionando **a petición, hora, Diario, Semanal o Mensual**.
  - c. En la sección Select secondary replication options, seleccione una de las siguientes opciones de replicación secundaria o ambas:

Para este campo...	Realice lo siguiente...
Actualizar SnapMirror tras crear una copia Snapshot local	<p>Seleccione este campo para crear copias reflejadas de los conjuntos de backup en otro volumen (replicación de SnapMirror).</p> <p>Esta opción debe estar habilitada para la sincronización activa de SnapMirror.</p>
Actualizar SnapVault después de crear una copia Snapshot local	Seleccione esta opción para realizar una replicación de backup disco a disco (backups de SnapVault).
Número de reintentos con error	Escriba el número máximo de intentos de replicación que se permitirán antes de que la operación se detenga.

7. En la página Retention, especifique la configuración de retención para el tipo de backup y el tipo de

programación seleccionados en la página Backup and Replication:

Si desea...	Realice lo siguiente...
Mantenga un cierto número de Snapshots	<p>Seleccione <b>Copias para guardar</b> y, a continuación, especifique el número de instantáneas que desea conservar.</p> <p>Si la cantidad de snapshots supera el número especificado, las snapshots se eliminan empezando por las más antiguas.</p> <div> <div></div> <div>El valor de retención máximo es 1018. Se producirá un error en los backups si la retención se establece en un valor superior a la versión de ONTAP subyacente.</div> </div> <div> <div></div> <div>Debe establecer el número de retención en 2 o un valor más alto si tiene pensado habilitar la replicación de SnapVault. Si establece el número de retención en 1, la operación puede generar un error, ya que la primera Snapshot es la de referencia para la relación de SnapVault hasta que se replica una nueva Snapshot en el destino.</div> </div>
Mantenga los Snapshots durante una cierta cantidad de días	<p>Seleccione <b>Retener copias para</b> y, a continuación, especifique el número de días durante los cuales desea conservar las instantáneas antes de eliminarlas.</p>
Período de bloqueo de copia de instantánea	<p>Seleccione <b>Período de bloqueo de copia de instantánea</b> y especifique la duración en días, meses o años.</p> <p>El período de retención de SnapLock debe ser inferior a 100 años.</p>

8. Seleccione la etiqueta de política.



Puede asignar etiquetas SnapMirror a instantáneas principales para replicación remota, lo que permite que las instantáneas principales descarguen la operación de replicación de instantáneas de SnapCenter a los sistemas secundarios de ONTAP . Esto se puede hacer sin habilitar la opción SnapMirror o SnapVault en la página de políticas.

9. En la página Script, introduzca la ruta y los argumentos del script previo o script posterior que desea ejecutar antes o después de la operación de backup, según corresponda.



Debe comprobar si los comandos existen en la lista de comandos disponible en el host del plugin desde la ruta `_ /opt/NetApp/SnapCenter/scc/etc/allowed_commands.config_`.

También puede especificar el valor de tiempo de espera del script. El valor predeterminado es 60 segundos.

10. Revise el resumen y, a continuación, haga clic en **Finalizar**.

## Cree grupos de recursos y adjunte políticas para sistemas de archivos Unix

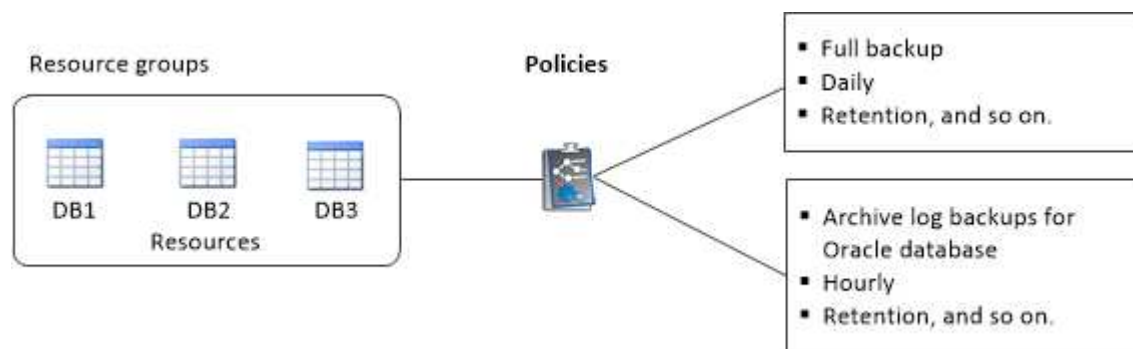
Un grupo de recursos es un contenedor donde se añaden recursos que se quieren proteger e incluir en un backup. El grupo de recursos permite realizar un backup con todos los datos que están asociados con los sistemas de archivos.

### Acerca de esta tarea

- Una base de datos con archivos en grupos de discos de ASM debe tener el estado «MOUNT» o «OPEN» para verificar sus backups mediante la utilidad Oracle DBVERIFY.

Añada una o más políticas al grupo de recursos para definir el tipo de trabajo de protección de datos que desea realizar.

En la siguiente imagen, se muestra la relación entre los recursos, los grupos de recursos y las políticas para las bases de datos:



- Para las políticas con SnapLock habilitado, para ONTAP 9.12.1 y versiones anteriores, si se especifica un período de bloqueo de Snapshot, los clones creados a partir de las instantáneas a prueba de manipulaciones como parte de la restauración heredarán el tiempo de caducidad de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.
- No se admiten la adición de nuevos sistemas de archivos sin sincronización activa de SnapMirror a un grupo de recursos existente que contiene recursos con sincronización activa de SnapMirror.
- No se admite la adición de nuevos sistemas de archivos a un grupo de recursos existente en el modo de conmutación por error de la sincronización activa de SnapMirror. Puede añadir recursos al grupo de recursos solo en estado normal o de conmutación por error.

### Pasos

1. En el panel de navegación de la izquierda, seleccione **Recursos** y el plug-in apropiado de la lista.
2. En la página Resources, haga clic en **New Resource Group**.
3. En la página Name, realice los siguientes pasos:

a. Escriba un nombre para el grupo de recursos en el campo Name.



El nombre del grupo de recursos no debe superar los 250 caracteres.

b. Escriba una o más etiquetas en el campo Etiqueta para que le ayude a buscar el grupo de recursos más adelante.

Por ejemplo, si añadió HR como etiqueta a varios grupos de recursos, más adelante encontrará todos los grupos de recursos asociados usando esa etiqueta.

c. Marque la casilla de comprobación e introduzca un formato de nombre personalizado que desee usar para el nombre de Snapshot.

Por ejemplo, customtext\_resource group\_policy\_hostname o resource group\_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la Snapshot.

4. En la página Recursos, seleccione un nombre de host de sistemas de archivos Unix de la lista desplegable **Host**.



Los recursos aparecen en la sección Available Resources solo si se detectan correctamente. Si agregó recursos recientemente, aparecerán en la lista de recursos disponibles únicamente después de actualizar la lista de recursos.

5. Seleccione los recursos de la sección Available Resources y muévalos a la sección Selected Resources.

6. En la página Application Settings, realice lo siguiente:

- Seleccione la flecha Scripts y escriba los comandos previos y posteriores para el modo de inactividad, Snapshot y la reanudación de la copia. También puede escribir los comandos previos para que se ejecuten antes de salir en caso de un fallo.
- Seleccione una de las opciones de consistencia de backup:
  - Seleccione **Sistema de archivos consistente** si desea asegurarse de que los datos almacenados en caché de los sistemas de archivos se vacían antes de crear la copia de seguridad y no se permiten operaciones de entrada o salida en el sistema de archivos durante la creación de la copia de seguridad.



Para la consistencia del sistema de archivos, se tomarán snapshots de grupo de consistencia para las LUN involucradas en el grupo de volúmenes.

- Seleccione **Consistente al bloqueo** si desea asegurarse de que los datos almacenados en caché de los sistemas de archivos se vacían antes de crear la copia de seguridad.



Si añadió diferentes sistemas de archivos en el grupo de recursos, todos los volúmenes de diferentes sistemas de archivos del grupo de recursos se colocarán en un grupo de consistencia.


7. En la página Policies, realice los siguientes pasos:

a. Seleccione una o varias políticas de la lista desplegable.



También puede crear una política haciendo clic en  .

En la sección *Configure schedules for selected policies*, se muestran las políticas seleccionadas.

- b. Haga clic en  En la columna *Configure Schedules* correspondiente a la política para la cual se desea configurar una programación.
- c. En la ventana *Add schedules for policy `policy_name`*, configure la programación y haga clic en **OK**.

Donde, *policy\_name* es el nombre de la directiva seleccionada.

Las programaciones configuradas figuran en la columna *Applied Schedules*.

No se admiten programas de backup de terceros cuando se solapan con los programas de backup de SnapCenter.

8. En la página *Notification*, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.

También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. Si desea adjuntar el informe de la operación realizada en el grupo de recursos, seleccione **Adjuntar informe de trabajo**.



Para las notificaciones de correo electrónico, se deben haber especificado los detalles del servidor SMTP desde la interfaz gráfica de usuario o desde el comando de PowerShell `Set-SmSmtServer`.

9. Revise el resumen y, a continuación, haga clic en **Finalizar**.

## Cree grupos de recursos y habilite la protección secundaria para sistemas de archivos Unix en sistemas ASA R2

Debe crear el grupo de recursos para añadir los recursos que están en los sistemas ASA R2. También puede aprovisionar la protección secundaria al crear el grupo de recursos.

### Antes de empezar

- Debe asegurarse de no añadir recursos de ONTAP 9.x y recursos de ASA R2 al mismo grupo de recursos.
- Debe asegurarse de que no dispone de una base de datos con recursos de ONTAP 9.x y recursos de ASA R2.

### Acerca de esta tarea

- La protección secundaria solo está disponible si el usuario que ha iniciado sesión está asignado al rol que tiene habilitada la capacidad **SecondaryProtection**.
- Si habilitó la protección secundaria, el grupo de recursos se pone en modo de mantenimiento mientras crea los grupos de coherencia primario y secundario. Una vez creados los grupos de coherencia primario y secundario, el grupo de recursos se queda sin modo de mantenimiento.
- SnapCenter no admite la protección secundaria para un recurso clonado.

### Pasos

1. En el panel de navegación de la izquierda, seleccione **Recursos** y el plug-in apropiado de la lista.
2. En la página *Resources*, haga clic en **New Resource Group**.
3. En la página *Name*, realice los siguientes pasos:

a. Escriba un nombre para el grupo de recursos en el campo Name.



El nombre del grupo de recursos no debe superar los 250 caracteres.

b. Escriba una o más etiquetas en el campo Etiqueta para que le ayude a buscar el grupo de recursos más adelante.

Por ejemplo, si añadió HR como etiqueta a varios grupos de recursos, más adelante encontrará todos los grupos de recursos asociados usando esa etiqueta.

c. Marque esta casilla de comprobación e introduzca un formato de nombre personalizado que desee usar para el nombre de Snapshot.

Por ejemplo, customtext\_resource group\_policy\_hostname o resource group\_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la Snapshot.

d. Especifique los destinos de los archivos de registro de archivos que no desea incluir en el backup.



Debe utilizar exactamente el mismo destino que se estableció en la aplicación, incluido el prefijo, si es necesario.

4. En la página Recursos, seleccione el nombre del host de la base de datos en la lista desplegable **Host**.



Los recursos aparecen en la sección Available Resources solo si se detectan correctamente. Si agregó recursos recientemente, aparecerán en la lista de recursos disponibles únicamente después de actualizar la lista de recursos.

5. Seleccione los recursos de ASA R2 de la sección Available Resources y muévelos a la sección Selected Resources.

6. En la página Application Settings, seleccione la opción de backup.


7. En la página Políticas, realice los siguientes pasos:

a. Seleccione una o varias políticas de la lista desplegable.



También puede crear una política haciendo clic en .

En la sección Configure schedules for selected policies, se muestran las políticas seleccionadas.

b. Haga clic en  En la columna Configure Schedules correspondiente a la política para la cual se desea configurar una programación.

c. En la ventana Add schedules for policy *policy\_name*, configure la programación y haga clic en **OK**.

Donde, *policy\_name* es el nombre de la directiva seleccionada.

Las programaciones configuradas figuran en la columna Applied Schedules.

No se admiten programas de backup de terceros cuando se solapan con los programas de backup de SnapCenter.

8. Si la protección secundaria está habilitada para la política seleccionada, se muestra la página Secondary

Protection y debe realizar los siguientes pasos:

- a. Seleccione el tipo de política de replicación.



No se admite la política de replicación síncrona.

- b. Especifique el sufijo del grupo de consistencia que desea utilizar.
- c. En los menús desplegables Cluster de destino y SVM de destino, seleccione el clúster con relaciones entre iguales y la SVM que desee utilizar.




SnapCenter no admite la relación entre iguales de los clústeres ni de SVM. Debe usar System Manager o CLI de ONTAP para realizar relaciones entre iguales de clústeres y SVM.



Si los recursos ya están protegidos fuera de SnapCenter, esos recursos aparecerán en la sección Secondary Protected Resources.

1. En la página Verification, realice los siguientes pasos:

- a. Haga clic en **Load locators** para cargar los volúmenes de SnapMirror o SnapVault y realizar la verificación en el almacenamiento secundario.
- b. Haga clic en  En la columna Configure Schedules para configurar la programación de verificación de todos los tipos de programación de la política.
- c. En el cuadro de diálogo Add Verification Schedules policy\_name, realice las siguientes acciones:

Si desea...	Realice lo siguiente...
Ejecutar la verificación después del backup	Seleccione <b>Ejecutar verificación después de la copia de seguridad</b> .
Programar una verificación	Seleccione <b>Ejecutar verificación programada</b> y, a continuación, seleccione el tipo de programa en la lista desplegable.

- d. Seleccione **verificar en la ubicación secundaria** para verificar las copias de seguridad en el sistema de almacenamiento secundario.
- e. Haga clic en **Aceptar**.

Las programaciones de verificación configuradas aparecerán en la columna Applied Schedules.

2. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.

También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. Si desea adjuntar el informe de la operación realizada en el grupo de recursos, seleccione **Adjuntar informe de trabajo**.




Para las notificaciones de correo electrónico, se deben haber especificado los detalles del servidor SMTP desde la interfaz gráfica de usuario o desde el comando de PowerShell `Set-SmSntpServer`.

3. Revise el resumen y, a continuación, haga clic en **Finalizar**.

## Hacer backup de sistemas de archivos Unix

Si un recurso no es parte de ningún grupo de recursos, es posible realizar backups del recurso desde la página Resources.

### Pasos

1. En el panel de navegación de la izquierda, seleccione **Recursos** y el plug-in apropiado de la lista.
2. En la página Recursos, seleccione **Ruta** en la lista Ver.
3. Haga clic en , a continuación, seleccione el nombre de host y los sistemas de archivos Unix para filtrar los recursos.
4. Seleccione el sistema de archivos del que desea realizar un backup.
5. En la página Resources, puede realizar los siguientes pasos:
  - a. Marque la casilla de comprobación e introduzca un formato de nombre personalizado que desee usar para el nombre de Snapshot.


Por ejemplo: `customtext_policy_hostname 0. resource_hostname`. De forma predeterminada, se añade una fecha/hora al nombre de Snapshot.

6. En la página Application Settings, realice lo siguiente:
  - Seleccione la flecha Scripts y escriba los comandos previos y posteriores para el modo de inactividad, Snapshot y la reanudación de la copia. También puede escribir los comandos previos para que se ejecuten antes de salir en caso de un fallo.
  - Seleccione una de las opciones de consistencia de backup:
    - Seleccione **Sistema de archivos consistente** si desea asegurarse de que los datos almacenados en caché de los sistemas de archivos se vacían antes de crear la copia de seguridad y no se realizan operaciones en el sistema de archivos durante la creación de la copia de seguridad.
    - Seleccione **Consistente al bloqueo** si desea asegurarse de que los datos almacenados en caché de los sistemas de archivos se vacían antes de crear la copia de seguridad.
7. En la página Policies, realice los siguientes pasos:
  - a. Seleccione una o varias políticas de la lista desplegable.



Puede crear una política haciendo clic en  .

En la sección Configure schedules for selected policies, se muestran las políticas seleccionadas.

- b. Haga clic en  En la columna Configure Schedules para configurar una programación para la política que desea.
- c. En la ventana Add schedules for policy *policy\_name*, configure la programación y, a continuación, seleccione OK.

*policy\_name* es el nombre de la directiva seleccionada.

Las programaciones configuradas figuran en la columna Applied Schedules.

8. En la página Notificación, seleccione los escenarios en los que desea enviar los correos electrónicos desde la lista desplegable **Preferencias de correo electrónico**.

Debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. Si desea asociar el informe de la operación de backup ejecutada en el recurso, seleccione **Attach Job Report**.



Para las notificaciones de correo electrónico, se deben haber especificado los detalles del servidor SMTP desde la interfaz gráfica de usuario o el comando de PowerShell `Set-SmSmtServer`.

9. Revise el resumen y, a continuación, haga clic en **Finalizar**.

Se muestra la página de topología.

10. Haga clic en **copia de seguridad ahora**.

11. En la página Backup, realice los siguientes pasos:

- a. Si aplicó varias políticas al recurso, en la lista desplegable Policy seleccione la política que desea usar para el backup.

Si la política seleccionada para el backup bajo demanda está asociada a una programación de backup, los backups bajo demanda se retendrán en función de la configuración de retención especificada para el tipo de programación.


- b. Haga clic en **copia de seguridad**.


12. Supervise el progreso de la operación haciendo clic en **Monitor > Jobs**.

## Realizar un backup de los grupos de recursos de sistemas de archivos Unix

Puede realizar una copia de seguridad de los sistemas de archivos Unix definidos en el grupo de recursos. Puede realizar un backup del grupo de recursos bajo demanda en la página Resources. Si el grupo de recursos tiene una política anexada y una programación configurada, los backups se crean según esa programación.

### Pasos

1. En el panel de navegación de la izquierda, seleccione **Recursos** y el plug-in apropiado de la lista.
2. En la página Resources, seleccione **Resource Group** en la lista **View**.
3. Escriba el nombre del grupo de recursos en el cuadro de búsqueda o haga clic en  y seleccione la etiqueta.

Haga clic en  para cerrar el panel de filtros.

4. En la página Resource Group, seleccione el grupo de recursos que desea incluir en un backup.
5. En la página Backup, realice los siguientes pasos:
  - a. Si tiene varias políticas asociadas con el grupo de recursos, seleccione la política de copia de seguridad que desea usar en la lista desplegable **Política**.

Si la política seleccionada para el backup bajo demanda está asociada a una programación de backup, los backups bajo demanda se retendrán en función de la configuración de retención especificada para el tipo de programación.

b. Seleccione **copia de seguridad**.

6. Controla el progreso seleccionando **Monitor > Trabajos**.

## Supervisar la copia de seguridad de sistemas de archivos Unix







Descubra cómo supervisar el progreso de las operaciones de backup y las operaciones de protección de datos.

### Supervisar las operaciones de copia de seguridad de sistemas de archivos Unix


Es posible supervisar el progreso de diferentes operaciones de backup mediante la página Jobs de SnapCenter. Se recomienda comprobar el progreso para determinar cuándo se completó la tarea o si existe un problema.

#### Acerca de esta tarea


Los siguientes iconos aparecen en la página Jobs e indican el estado correspondiente de las operaciones:

-  En curso
-  Completado correctamente
-  Error
-  Completado con advertencias o no pudo iniciarse debido a advertencias
-  En cola
-  Cancelada

#### Pasos

1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
2. En la página Monitor, haga clic en **Jobs**.
3. En la página Jobs, realice los siguientes pasos:
  - a. Haga clic en  para filtrar la lista de modo que solo se muestren las operaciones de backup.
  - b. Especifique las fechas de inicio y finalización.
  - c. En la lista desplegable **Tipo**, seleccione **copia de seguridad**.
  - d. En la lista desplegable **Estado**, seleccione el estado de copia de seguridad.
  - e. Haga clic en **aplicar** para ver las operaciones completadas correctamente.
4. Seleccione un trabajo de copia de seguridad y, a continuación, haga clic en **Detalles** para ver los detalles del trabajo.



Aunque se muestra el estado del trabajo de copia de seguridad  , al hacer clic en los detalles del trabajo, es posible que algunas de las tareas secundarias de la operación de copia de seguridad estén aún en curso o marcadas con señales de advertencia.

5. En la página Detalles del trabajo, haga clic en **Ver registros**.


El botón **Ver registros** muestra los registros detallados para la operación seleccionada.

## Supervise las operaciones de protección de datos en el panel Activity

El panel Activity muestra las cinco operaciones más recientes que se ejecutaron. También muestra el momento en que se inició la operación y su estado.

El panel Activity muestra información sobre las operaciones de backup, restauración, clonado y backup programado.

### Pasos

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. Haga clic en  en el panel Activity para ver las cinco operaciones más recientes.

Al hacer clic en una de las operaciones, los detalles de la operación se enumeran en la página **Detalles del trabajo**.




## Vea los sistemas de archivos Unix protegidos en la página Topology

Al prepararse para realizar un backup, restaurar o clonar un recurso, puede ser útil ver una representación gráfica de todos los backups, sistemas de archivos restaurados y clones en el almacenamiento principal y secundario.

### Acerca de esta tarea

En la página Topology, puede ver todos los backups, los sistemas de archivos restaurados y los clones que están disponibles para el recurso o el grupo de recursos seleccionado. Pueden verse los detalles de estos backups, sistemas de archivos restaurados y clones, y luego seleccionarlos para realizar operaciones de protección de datos.

Puede consultar los siguientes iconos de la vista gestionar copias para determinar si los backups o clones están disponibles en el almacenamiento principal y secundario (copias reflejadas o en almacén).




-  muestra la cantidad de backups y clones que están disponibles en el almacenamiento principal.
-  Muestra la cantidad de backups y clones que están copiados en el almacenamiento secundario mediante SnapMirror.
-  Muestra la cantidad de backups y clones que se replican en el almacenamiento secundario mediante la tecnología SnapVault.

La cantidad de backups que se muestra incluye los backups eliminados del almacenamiento secundario. Por ejemplo, si creó 6 backups con una política para retener solamente 4 backups, se muestran 6 backups.



Los clones de un backup de un reflejo con versión flexible en un volumen de tipo reflejo-almacén se muestran en la vista de topología, pero el número de backups de reflejo no incluye el backup con versión flexible.

Si tiene una relación secundaria como SnapMirror Active Sync (inicialmente lanzado como SnapMirror Business Continuity [SM-BC]), verá los siguientes iconos adicionales:

-  El sitio de réplica está activo.
-  El sitio de réplica está inactivo.
-  No se restableció la relación de reflejo o almacén secundario.
- Pasos\*
  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
  2. En la página Resources, seleccione el recurso o el grupo de recursos de la lista desplegable **View**.
  3. Seleccione el recurso desde la vista de detalles del recurso o desde la vista de detalles del grupo de recursos.

Si el recurso está protegido, se muestra la página Topology del recurso seleccionado.

4. Consulte Summary Card para ver un resumen de la cantidad de backups y clones disponibles en el almacenamiento principal y secundario.

La sección Summary Card muestra la cantidad total de backups y clones.

Al hacer clic en el botón **Actualizar** se inicia una consulta del almacenamiento para mostrar un recuento preciso.

Si se realiza una copia de seguridad habilitada para SnapLock, al hacer clic en el botón **Actualizar** se actualiza el tiempo de caducidad de SnapLock principal y secundario recuperado de ONTAP. Una programación semanal también actualiza el tiempo de caducidad de SnapLock principal y secundario recuperado de ONTAP.

Cuando el sistema de archivos se distribuya entre varios volúmenes, el tiempo de caducidad de SnapLock del backup será el tiempo de caducidad de SnapLock más largo que se establezca para una snapshot en un volumen. El tiempo de caducidad de SnapLock más largo se recupera de ONTAP.

Para la sincronización activa de SnapMirror, al hacer clic en el botón **Actualizar** se actualiza el inventario de copia de seguridad de SnapCenter consultando ONTAP tanto para los sitios primarios como para los de réplica. Una programación semanal también realiza esta actividad en todas las bases de datos que contienen una relación de sincronización activa de SnapMirror.

- Para la sincronización activa de SnapMirror y solo para ONTAP 9.14.1, las relaciones de reflejo asíncrono o reflejo asíncrono de almacén con el nuevo destino primario deben configurarse manualmente después de una conmutación al nodo de respaldo. A partir de ONTAP 9.15.1 en adelante, el reflejo asíncrono o el reflejo asíncrono se configura automáticamente en el nuevo destino primario.
- Después de la conmutación por error, es necesario crear un backup para que SnapCenter detecte la conmutación al nodo de respaldo. Puede hacer clic en **Actualizar** solo después de que se haya

creado una copia de seguridad.

5. En la vista Administrar copias, haga clic en **copias de seguridad** o **clones** en el almacenamiento principal o secundario para ver los detalles de una copia de seguridad o un clon.

Estos detalles se muestran en forma de tabla.

6. Seleccione el backup de la tabla y, a continuación, haga clic en los iconos de protección de datos para llevar a cabo operaciones de restauración, clonado y eliminación.



Los backups que figuran en el almacenamiento secundario no pueden eliminarse ni cambiar de nombre.

7. Si desea eliminar un clon, selecciónelo de la tabla y, a continuación, haga clic en .

## Ejemplo que muestra backups y clones en el almacenamiento principal

Manage Copies



Summary Card	
2 Backups	
1 Clone	
0 Snapshots Locked	

# Restaurar y recuperar sistemas de archivos Unix

## Restaurar sistemas de archivos Unix

En caso de pérdida de datos, puede utilizar SnapCenter para restaurar sistemas de archivos Unix.

### Acerca de esta tarea

- Debe ejecutar los siguientes comandos para establecer la conexión con SnapCenter Server, enumerar los backups y recuperar su información, y restaurar el backup.

La información sobre los parámetros que se pueden utilizar con el comando y sus descripciones se pueden obtener ejecutando `Get-Help command_name`. Alternativamente, también puede consultar la ["Guía de referencia de comandos del software SnapCenter"](#).

- Para la operación de restauración de sincronización activa de SnapMirror, debe seleccionar el backup de la ubicación principal.

## Pasos

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página Recursos, seleccione **Ruta o Grupo de recursos** en la lista **Ver**.
3. Seleccione el sistema de archivos en la vista de detalles o en la vista de detalles del grupo de recursos.

Se muestra la página de topología.

4. En la vista Manage Copies, seleccione **copias de seguridad** en los sistemas de almacenamiento principal o secundario (reflejado o replicado).
5. Seleccione el backup en la tabla y haga clic en .

6. En la página Restore Scope:

- Para los sistemas de archivos NFS, por defecto se selecciona la opción **Connect and Copy** restore. También puede seleccionar **Reversión de volumen** o **Restauración rápida**.
- Para sistemas de archivos que no son NFS, el alcance de la restauración se selecciona según el diseño.

Es posible que los nuevos archivos creados después de la copia de seguridad no estén disponibles después de la restauración, según el tipo y el diseño del sistema de archivos.

7. En la página PreOps, escriba los comandos previos a la restauración que se ejecutarán antes de realizar un trabajo de restauración.
8. En la página PostOps, escriba los comandos posteriores a la restauración que se ejecutarán después de realizar un trabajo de restauración.



Debe comprobar si los comandos existen en la lista de comandos disponible en el host del plugin en la ubicación `/opt/NetApp/SnapCenter/scc/etc/allowed_commands.config` path.

9. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar las notificaciones por correo electrónico.

También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. Si desea adjuntar el informe de la operación de restauración realizada, debe seleccionar **Adjuntar informe de trabajo**.



Para la notificación por correo electrónico, debe haber especificado los detalles del servidor SMTP a través de la interfaz gráfica de usuario o el comando `Set-SmSmtServer` de PowerShell.

10. Revise el resumen y, a continuación, haga clic en **Finalizar**.



Si la operación de restauración falla, no se admite la reversión.



En caso de restauración de un sistema de archivos que reside en el grupo de volúmenes, el contenido antiguo del sistema de archivos no se eliminará. Solo el contenido del sistema de archivos clonado se copiará al sistema de archivos de origen. Esto es aplicable cuando hay varios sistemas de archivos en el grupo de volúmenes y restauraciones predeterminadas del sistema de archivos NFS.

11. Supervise el progreso de la operación haciendo clic en **Monitor > Jobs**.







## Supervisar las operaciones de restauración de sistemas de archivos Unix

Es posible supervisar el progreso de diferentes operaciones de restauración de SnapCenter mediante la página Jobs. El progreso de una operación puede revisarse para determinar cuándo está completa o si hay un problema.


### Acerca de esta tarea

los estados posteriores a la restauración describen las condiciones del recurso una vez ejecutada la operación de restauración, así como otras acciones de restauración que pueden realizarse.

Los siguientes iconos aparecen en la página Jobs e indican el estado de la operación:

-  En curso
-  Completado correctamente
-  Error
-  Completado con advertencias o no pudo iniciarse debido a advertencias
-  En cola
-  Cancelada

### Pasos

1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **trabajos**.
3. En la página **trabajos**, realice los siguientes pasos:
  - a. Haga clic  en para filtrar la lista de modo que solo figuren las operaciones de restauración.
  - b. Especifique las fechas de inicio y finalización.
  - c. En la lista desplegable **Tipo**, seleccione **Restaurar**.
  - d. En la lista desplegable **Estado**, seleccione el estado de restauración.
  - e. Haga clic en **aplicar** para ver las operaciones que se han completado correctamente.
4. Seleccione el trabajo de restauración y, a continuación, haga clic en **Detalles** para ver los detalles del trabajo.
5. En la página **Detalles del trabajo**, haga clic en **Ver registros**.

El botón **Ver registros** muestra los registros detallados para la operación seleccionada.

## Clonar sistemas de archivos Unix

### Clonar backup de sistema de archivos Unix

Puede utilizar SnapCenter para clonar el sistema de archivos Unix mediante la copia de seguridad del sistema de archivos.

#### Antes de empezar

- Para omitir la actualización del archivo fstab, debe configurarse el valor de `SKIP_FSTAB_UPDATE` como **true** en el archivo `agent.properties` ubicado en `/opt/NetApp/snapcenter/scc/etc`.
- Puede contar con un nombre de volumen de clon estático y una ruta de unión si se configura el valor de `USE_CUSTOM_CLONE_VOLUME_NAME_FORMAT` a **true** en el archivo `agent.properties` ubicado en `/opt/NetApp/snapcenter/scc/etc`. Después de actualizar el archivo, debe reiniciar el servicio creador del complemento SnapCenter ejecutando el comando: `/opt/NetApp/snapcenter/scc/bin/scc restart`.


Ejemplo: Sin esta propiedad, el nombre del volumen clonado y la ruta de unión serán como `<Source_volume_name>_Clone_<Timestamp>`, pero ahora serán `<Source_volume_name>_Clone_<Clone_Name>`

Esto mantiene el nombre constante para que pueda mantener el archivo fstab actualizado manualmente si no prefiere actualizar el fstab por SnapCenter.

#### Pasos

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página Recursos, seleccione **Ruta** o **Grupo de recursos** en la lista **Ver**.
3. Seleccione el sistema de archivos en la vista de detalles o en la vista de detalles del grupo de recursos.

Se muestra la página de topología.

4. En la vista Manage Copies, seleccione los backups desde local copies (primary), Mirror copies (secondary) o Vault copies (secondary).
5. Seleccione el backup en la tabla y haga clic en .
6. En la página Location, lleve a cabo las siguientes acciones:

Para este campo...	Realice lo siguiente...
Clone el servidor	De forma predeterminada, se llena el host de origen.
Clone el punto de montaje	Especifique la ruta de acceso en la que se montará el sistema de archivos.

7. En la página Scripts, realice los siguientes pasos:

- a. Introduzca los comandos para el clon previo o posterior que se deben ejecutar antes o después de la operación de clonado, respectivamente.



Debe comprobar si los comandos existen en la lista de comandos disponible en el host del plugin en la ruta `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`.

8. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.

También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. Si desea adjuntar el informe de la operación de clonado realizada, seleccione **Adjuntar informe de trabajo**.



Para las notificaciones de correo electrónico, se deben haber especificado los detalles del servidor SMTP desde la interfaz gráfica de usuario o desde el comando de PowerShell `Set-SmSmtServer`.

9. Revise el resumen y, a continuación, haga clic en **Finalizar**.
10. Supervise el progreso de la operación haciendo clic en **Monitor > Jobs**.

## Divida un clon

Es posible usar SnapCenter para dividir un recurso clonado de un recurso primario. El clon que se divide se independiza del recurso primario.

### Acerca de esta tarea

- No se puede ejecutar la operación de división de clones en un clon intermedio.

Por ejemplo, después de crear el clon 1 a partir de un backup de la base de datos, puede realizar un backup del clon 1 y luego clonar este backup (que sería el clon 2). Una vez creado el clon 2, el clon 1 se convierte en un clon intermedio y la operación de división de clones puede hacerse con el clon 1. No obstante, esta operación también puede ejecutarse con el clon 2.

Después de dividir el clon 2, puede ejecutar la operación de división de clones con el clon 1, ya que este deja de ser el clon intermedio.

- Cuando divide un clon, se eliminan las copias de backup y los trabajos de clonado del clon.
- Para obtener más información sobre las operaciones de división de volúmenes de FlexClone, consulte, ["Divida un volumen FlexClone de su volumen principal"](#).
- Asegúrese de que el volumen o el agregado del sistema de almacenamiento estén en línea.

### Pasos


1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página **Recursos**, seleccione la opción adecuada en la lista Ver:

Opción	Descripción
Para aplicaciones de base de datos	Seleccione <b>base de datos</b> en la lista View.

Opción	Descripción
Para sistemas de archivos	Seleccione <b>Ruta</b> en la lista Ver.

3. Seleccione el recurso adecuado de la lista.

Se muestra la página con el resumen.

- En la vista **Administrar copias**, seleccione el recurso clonado (por ejemplo, la base de datos o LUN) y, a continuación, haga clic en .
- Revise el tamaño estimado del clon que se va a dividir y el espacio necesario disponible en el agregado y, a continuación, haga clic en **Inicio**.
- Supervise el progreso de la operación haciendo clic en **Monitor > Jobs**.

La operación de división de clones se detiene si se reinicia el servicio de SMCore. Debe ejecutar el cmdlet Stop-SmJob para detener la operación de división de clones y luego volver a intentar la operación de división de clones.

Si necesita más o menos tiempo de sondeo para comprobar si el clon está dividido o no, puede cambiar el valor del parámetro *CloneSplitStatusCheckPollTime* en el archivo *SMCoreServiceHost.exe.config* para establecer un intervalo para que SMCore sondee el estado de la operación de división de clones. El valor se registra en milisegundos; el predeterminado son 5 minutos.

Por ejemplo:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

Se produce un error en la operación de inicio de división de clones si hay un backup, una restauración u otra división de clones en curso. Solo debe reiniciar la operación de división de clones una vez que hayan finalizado las operaciones en ejecución.

## Información relacionada





["Se produce un error en la verificación o el clon de SnapCenter porque no existe agregado"](#)




## Supervisar operaciones de clonación de sistemas de archivos Unix

Es posible supervisar el progreso de las operaciones de clonado de SnapCenter mediante la página Jobs. El progreso de una operación puede revisarse para determinar cuándo está completa o si hay un problema.

### Acerca de esta tarea

Los siguientes iconos aparecen en la página Jobs e indican el estado de la operación:

-  En curso
-  Completado correctamente
-  Error
-  Completado con advertencias o no pudo iniciarse debido a advertencias

-  En cola
-  Cancelada
- Pasos\*
  1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
  2. En la página **Monitor**, haga clic en **trabajos**.
  3. En la página **trabajos**, realice los siguientes pasos:
    - a. Haga clic  en para filtrar la lista de modo que solo figuren las operaciones de clonado.
    - b. Especifique las fechas de inicio y finalización.
    - c. En la lista desplegable **Tipo**, seleccione **Clonar**.
    - d. En la lista desplegable **Estado**, seleccione el estado del clon.
    - e. Haga clic en **aplicar** para ver las operaciones que se han completado correctamente.
  4. Seleccione el trabajo de clonado y, a continuación, haga clic en **Detalles** para ver los detalles del trabajo.
  5. En la página Detalles del trabajo, haga clic en **Ver registros**.

## 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.