



Proteger aplicaciones mediante los complementos compatibles con NetApp

SnapCenter Software 6.0

NetApp
December 19, 2024

This PDF was generated from https://docs.netapp.com/es-es/snapcenter/protect-nsp/netapp_supported_plugins_overview.html on December 19, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

- Proteger aplicaciones mediante los complementos compatibles con NetApp 1
 - Complementos compatibles con NetApp 1
 - Preparar la instalación de complementos compatibles con NetApp 8
 - Prepárese para la protección de datos 33
 - Realizar backup de los recursos de plugins compatibles con NetApp 35
 - Restaurar recursos de plugins compatibles con NetApp 59
 - Backups de recursos de plugins admitidos por Clone NetApp 64

Proteger aplicaciones mediante los complementos compatibles con NetApp

Complementos compatibles con NetApp

Información general sobre los plugins compatibles de NetApp

Es posible usar los complementos compatibles con NetApp, como MongoDB, ORASCPM (aplicaciones Oracle), SAP ASE, SAP MaxDB y el complemento de almacenamiento para aplicaciones que se usen y, a continuación, utilizar SnapCenter para realizar backups, restaurar o clonar tales aplicaciones. Los plugins compatibles con NetApp funcionan como componentes del host del software NetApp SnapCenter y permiten la protección de datos para aplicaciones y la gestión de recursos.

Cuando se instalan plugins compatibles con NetApp, es posible utilizar SnapCenter con la tecnología SnapMirror de NetApp para crear mirrors de conjuntos de backups en otro volumen, y la tecnología NetApp SnapVault para la replicación de backup de disco a disco. Los plugins compatibles con NetApp se pueden utilizar tanto en entornos de Windows como de Linux.



SnapCenterCLI no admite comandos de plugins compatibles con NetApp.

NetApp proporciona el complemento de almacenamiento para realizar operaciones de protección de datos del volumen de datos en el almacenamiento de ONTAP mediante el marco de trabajo de complementos personalizados integrado en SnapCenter.

Puede instalar los plugins compatibles con NetApp desde la página Add Host.

["Añada hosts e instale paquetes de plugins en hosts remotos."](#)



La política de soporte de SnapCenter cubrirá la compatibilidad con el marco de complementos personalizados de SnapCenter, el motor principal y las API asociadas. El soporte técnico no cubrirá el código fuente del complemento ni los scripts asociados incluidos en el marco de complementos personalizados.

Tareas que pueden llevarse a cabo con los plugins compatibles con NetApp

Es posible usar los complementos compatibles con NetApp, como MongoDB, ORASCPM, aplicaciones Oracle, SAP ASE, SAP MaxDB y el complemento de almacenamiento para operaciones de protección de datos.

- Añadir recursos como bases de datos, instancias, documentos o espacios de tablas.
- Crear backups.
- Restaurar desde backups.
- Clonar backups.
- Programar operaciones de backup.
- Supervisar operaciones de backup, de restauración y de clonado.

- Ver informes para operaciones de backup, restauración y clonado.

Es posible usar los plugins compatibles con NetApp para las operaciones de protección de datos.

- Realice copias Snapshot de grupo de coherencia de los volúmenes de almacenamiento en los clústeres de ONTAP.
- Realice copias de seguridad de aplicaciones personalizadas mediante el marco incorporado de secuencias de comandos previas y posteriores

Es posible realizar backups de un volumen de ONTAP, LUN o un qtree.

- Actualice las snapshots creadas del almacenamiento primario a un secundario de ONTAP aprovechando la relación de replicación existente (SnapVault/SnapMirror/replicación unificada) mediante la normativa de SnapCenter

ONTAP principal y secundario puede ser ONTAP FAS, AFF, cabina All SAN (ASA), Select o Cloud ONTAP.

- Recupere volúmenes, LUN o archivos ONTAP completos.

Debe proporcionar la ruta de archivo correspondiente manualmente, ya que las funciones de exploración o indexación no están integradas en el producto.

No se admite la restauración de qtree o directorio, pero solo se puede clonar y exportar el qtree si el alcance de backup se define en el nivel de Qtree.

Las funciones de los plugins compatibles con NetApp

SnapCenter se integra con la aplicación de plugins y con tecnologías de NetApp en el sistema de almacenamiento. Para trabajar con los complementos compatibles con NetApp, como MongoDB, ORASCPM (Aplicaciones Oracle), SAP ASE, SAP MaxDB y el complemento de almacenamiento, se utiliza la interfaz gráfica de usuario de SnapCenter.

- **Interfaz gráfica de usuario unificada**

La interfaz de SnapCenter ofrece estandarización y consistencia entre plugins y entornos. La interfaz de SnapCenter permite completar operaciones de backup, restauración, recuperación y clonado consistentes entre plugins, utilizar informes centralizados, utilizar visualizaciones de consola rápidas, configurar el RBAC y supervisar trabajos en todos los plugins.

- **Administración central automatizada**

Es posible programar operaciones de backup, configurar la retención de backup basado en políticas y realizar operaciones de restauración. También es posible supervisar de manera proactiva el entorno configurando SnapCenter para que envíe alertas por correo electrónico.

- **Tecnología NetApp instantánea no disruptiva**

SnapCenter utiliza la tecnología Snapshot de NetApp con los complementos compatibles con NetApp para realizar backups de recursos. Las snapshots consumen un espacio de almacenamiento mínimo.

Los complementos compatibles con NetApp además ofrecen los siguientes beneficios:

- Compatibilidad con flujos de trabajo de backup, restauración y clonado

- Seguridad compatible con RBAC y delegación de roles centralizada

También es posible configurar las credenciales para que los usuarios de SnapCenter autorizados tengan permisos en el nivel de las aplicaciones.

- Creación de copias de recursos con gestión eficiente del espacio y en un momento específico con fines de prueba o de extracción de datos con la tecnología FlexClone de NetApp

Se requiere una licencia de FlexClone en el sistema de almacenamiento donde desea crear el clon.

- Compatibilidad con la función Snapshot del grupo de consistencia (CG) de ONTAP como parte de la creación de backups.
- Capacidad para ejecutar varios backups de forma simultánea entre varios hosts de recursos

En una sola operación se consolidan Snapshot cuando los recursos en un solo host comparten el mismo volumen.

- Capacidad para crear Snapshot con comandos externos
- Capacidad para crear snapshots consistentes con el sistema de archivos en entornos Windows

Tipos de almacenamiento admitidos por los plugins compatibles con NetApp

SnapCenter admite una amplia variedad de tipos de almacenamiento en máquinas físicas y virtuales. Debe comprobar la compatibilidad de su tipo de almacenamiento antes de instalar los plugins compatibles con NetApp.

Máquina	Tipo de almacenamiento
Montajes físicos y directos de NFS en los hosts de máquinas virtuales (no se admiten VMDK y LUN de RDM).	LUN conectados a FC
Montajes físicos y directos de NFS en los hosts de máquinas virtuales (no se admiten VMDK y LUN de RDM).	LUN conectados a iSCSI
Montajes físicos y directos de NFS en los hosts de máquinas virtuales (no se admiten VMDK y LUN de RDM).	Volúmenes conectados en NFS
VMware ESXi	Almacenes de datos VVOL en NFS y SAN El almacén de datos VVOL solo se puede aprovisionar con ONTAP Tools para VMware vSphere.

Privilegios mínimos de ONTAP requeridos para el plugin compatible con NetApp

Los privilegios mínimos requeridos de ONTAP varían en función de los plugins de SnapCenter que utilice para la protección de datos.

- Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.3.0 y versiones posteriores
 - event generate-autosupport-log
 - se muestra el historial del trabajo
 - detención de trabajo
 - se muestra el atributo de lun
 - lun create
 - eliminación de lun
 - geometría de lun
 - igroup de lun añadido
 - crear lun igroup
 - lun igroup eliminado
 - cambio de nombre de lun igroup
 - lun igroup show
 - asignación de lun de nodos adicionales
 - se crea la asignación de lun
 - se elimina la asignación de lun
 - asignación de lun quitar nodos de generación de informes
 - se muestra el mapa de lun
 - modificación de lun
 - movimiento de lun en volumen
 - lun desconectada
 - lun conectada
 - cambio de tamaño de lun
 - serie de lun
 - muestra de lun
 - interfaz de red
 - regla adicional de la política de snapmirror
 - regla de modificación de la política de snapmirror
 - regla de eliminación de la política de snapmirror
 - la política de snapmirror
 - restauración de snapmirror
 - de snapmirror
 - historial de snapmirror
 - actualización de snapmirror
 - conjunto de actualizaciones de snapmirror
 - destinos de listas de snapmirror
 - versión

- crear el clon de volumen
- show de clon de volumen
- inicio de división de clon de volumen
- detención de división de clon de volumen
- cree el volumen
- destrucción del volumen
- crear el archivo de volumen
- uso show-disk del archivo de volumen
- volumen sin conexión
- volumen en línea
- modificación del volumen
- crear el qtree de volúmenes
- eliminación de qtree de volumen
- modificación del qtree del volumen
- se muestra volume qtree
- restricción de volumen
- visualización de volumen
- crear snapshots de volumen
- eliminación de snapshots de volumen
- modificación de las copias de snapshot de volumen
- cambio de nombre de copias de snapshot de volumen
- restauración de copias snapshot de volumen
- archivo de restauración de snapshots de volumen
- visualización de copias de snapshot de volumen
- desmonte el volumen
- vserver cifs
- vserver cifs share create
- eliminación de vserver cifs share
- se muestra vserver shadowcopy
- visualización de vserver cifs share
- visualización de vserver cifs
- creación de política de exportación de vserver
- eliminación de la política de exportación de vserver
- creación de reglas de política de exportación de vserver
- aparece la regla de política de exportación de vserver
- visualización de la política de exportación de vserver
- se muestra la conexión iscsi del vserver

- se muestra vserver
- Comandos de solo lectura: Privilegios mínimos requeridos para ONTAP 8.3.0 y versiones posteriores
 - interfaz de red

Preparar los sistemas de almacenamiento para la replicación de SnapMirror y de SnapVault para complementos compatibles con NetApp

Es posible utilizar un complemento de SnapCenter con la tecnología SnapMirror de ONTAP para crear copias de reflejo de conjuntos de backups en otro volumen, y con la tecnología ONTAP SnapVault para realizar replications de backup disco a disco para cumplimiento de normativas y otros fines relacionados con la gobernanza. Antes de ejecutar estas tareas, debe configurar una relación de protección de datos entre los volúmenes de origen y de destino, e inicializar la relación.

SnapCenter realiza las actualizaciones a SnapMirror y SnapVault después de que finaliza la operación de Snapshot. Las actualizaciones de SnapMirror y SnapVault se realizan como parte del trabajo de SnapCenter; no cree una programación de ONTAP aparte.



Si llegó a SnapCenter desde un producto NetApp SnapManager y está satisfecho con las relaciones de protección de datos que ha configurado, puede omitir esta sección.

Una relación de protección de datos replica los datos en el almacenamiento primario (el volumen de origen) en el almacenamiento secundario (el volumen de destino). Cuando se inicializa la relación, ONTAP transfiere los bloques de datos a los que se hace referencia en el volumen de origen al volumen de destino.



SnapCenter no admite relaciones en cascada entre volúmenes de SnapMirror y SnapVault (**Primary > Mirror > Vault**). Debe utilizar las relaciones con fanout.

SnapCenter permite la gestión de relaciones de SnapMirror de versión flexible. Si quiere información detallada sobre las relaciones de SnapMirror con versión flexible y sobre cómo configurarlas, consulte "[Documentación de ONTAP](#)".

Defina una estrategia de backup

Definir una estrategia de backup antes de crear las tareas de backup garantiza que se cuente con todos los backups necesarios para restaurar o clonar correctamente los recursos. La estrategia de backup queda determinada principalmente por el SLA, el RTO y el RPO.

Acerca de esta tarea

Un acuerdo de nivel de servicio define el nivel de servicio que se espera y aborda varios problemas vinculados con el servicio, como su disponibilidad y rendimiento. El objetivo de tiempo de recuperación es el plazo de recuperación después de una interrupción del servicio. El RPO define la estrategia respecto de la antigüedad de los archivos que se deben recuperar del almacenamiento de backup para reanudar las operaciones regulares después de un fallo. El acuerdo de nivel de servicio, el objetivo de tiempo de recuperación y el RPO ayudan a establecer una estrategia de protección de datos.

Pasos

1. Determinar cuándo se debe realizar el backup de los recursos.

2. Decidir cuántas tareas de backup se necesitan.
3. Decidir el nombre que se asignará a los backups.
4. Decidir si se harán snapshots de los grupos de consistencia y elegir las opciones apropiadas para eliminar las snapshots de los grupos de consistencia.
5. Decidir si se desean usar la tecnología NetApp SnapMirror para la replicación o la tecnología NetApp SnapVault para la retención a largo plazo.
6. Determinar el período de retención para las copias Snapshot en el sistema de almacenamiento de origen y el destino de SnapMirror.
7. Determinar si se desea ejecutar comandos antes o después de la operación de backup y proporcionar un script previo o posterior.

La estrategia de backup para complementos compatibles con NetApp

Programaciones de backup de recursos de plugins compatibles con NetApp

El factor más importante para determinar una programación de backup es la tasa de cambio del recurso. Mientras más frecuentes sean los backups de los recursos, menos archivos de registro necesitará SnapCenter para la restauración, lo cual puede acelerar las operaciones de restauración.

Puede ser recomendable realizar el backup de un recurso muy utilizado una vez por hora, mientras que, en el caso de un recurso de poco uso, es suficiente hacerlo una vez por día. Otros factores que se deben tener en cuenta son la importancia del recurso para la organización, el SLA y el RPO.

El SLA define el nivel de servicio que se espera y aborda varios problemas vinculados con el servicio, como su disponibilidad y rendimiento. El RPO define la estrategia respecto de la antigüedad de los archivos que se deben recuperar del almacenamiento de backup para reanudar las operaciones regulares después de un fallo. El SLA y RPO ayudan a establecer una estrategia de protección de datos.

Las programaciones de backup están compuestas por dos partes:

- Frecuencia de backup

La frecuencia de backup (cada cuánto se deben realizar los backups), también denominada tipo de programación para algunos plugins, es parte de una configuración de políticas. Por ejemplo, se puede configurar una frecuencia de backup horaria, diaria, semanal o mensual. Puede acceder a las directivas en la interfaz gráfica de usuario de SnapCenter haciendo clic en **Configuración > Directivas**.

- Programaciones de backup

Las programaciones de backup (el momento exacto en que se realiza el backup) forman parte de la configuración de un recurso o un grupo de recursos. Por ejemplo, si hay un grupo de recursos con una política configurada para realizar un backup semanal, es posible configurar la programación para que se realice un backup todos los jueves a las 00:10. Para acceder a las programaciones de grupos de recursos en la interfaz gráfica de usuario de SnapCenter, haga clic en **Recursos**, seleccione el complemento adecuado y haga clic en **Ver > Grupo de recursos**.

Cantidad de trabajos de backup necesarios

Algunos factores que determinan la cantidad de trabajos de backup que se necesitan son

el tamaño del recurso, la cantidad de volúmenes que se usan, la tasa de cambio del recurso y el acuerdo de nivel de servicio.

La cantidad de trabajos de backup que se selecciona depende de la cantidad de volúmenes en los que se colocaron los recursos. Por ejemplo, si se colocó un grupo de recursos pequeños en un volumen y un recurso grande en otro volumen, puede ser necesario crear un trabajo de backup para los recursos pequeños y otro trabajo para el recurso grande.

Tipos de estrategias de restauración compatibles con los recursos de plugins compatibles con NetApp añadidos manualmente

Para poder ejecutar correctamente las operaciones de restauración, es necesario definir una estrategia mediante SnapCenter. Existen dos tipos de estrategias de restauración para los recursos de plugins compatibles con NetApp que se añaden manualmente.



No se pueden recuperar manualmente los recursos de plugins compatibles con NetApp que se añadieron manualmente.

Restauración de recursos completa

- Restaura todos los volúmenes, qtrees y LUN de un recurso



Si el recurso contiene volúmenes o qtrees, las snapshots realizadas después de la Snapshot seleccionada para restaurar en los volúmenes o qtrees se eliminan y no pueden recuperarse. Además, si hay algún otro recurso alojado en los mismos volúmenes o qtrees, también se lo elimina.

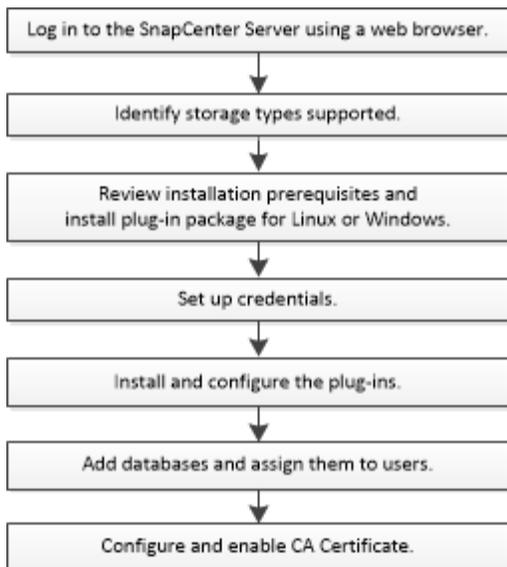
Restauración de nivel de archivos

- Restaura los archivos de volúmenes, qtrees o directorios
- Restaura solo los LUN seleccionados

Preparar la instalación de complementos compatibles con NetApp

Flujo de trabajo de instalación de plugins compatibles con SnapCenter NetApp

Deber instalar y configurar plugins compatibles con SnapCenter NetApp si desea proteger los recursos de plugins compatibles con NetApp.



Requisitos previos para añadir hosts e instalar el paquete de plugins para Windows, Linux o AIX

Antes de añadir un host e instalar los paquetes de plugins, debe satisfacer todos los requisitos. Los plugins compatibles con NetApp son compatibles con entornos Windows, Linux y AIX.



El almacenamiento y las aplicaciones de Oracle son compatibles con AIX.

- Debe haber instalado Java 11 en el host Linux, Windows o AIX.
- Al instalar un plugin en un host de Windows, si especifica una credencial que no está incorporada o si el usuario pertenece a un usuario de grupo de trabajo local, debe deshabilitar UAC en el host.
- Los complementos compatibles con NetApp, como MongoDB, ORASCPM, aplicaciones Oracle, SAP ASE, SAP MaxDB y el complemento de almacenamiento deben estar disponibles en el host del cliente desde el que se ejecuta la operación de añadir host.

Generales

Si utiliza iSCSI, el servicio iSCSI debe estar en ejecución.

Host Windows

- Debe tener un usuario de dominio con privilegios de administrador local y permisos locales para iniciar sesión en el host remoto.
- Si gestiona nodos de clúster en SnapCenter, debe tener un usuario con privilegios de administrador para todos los nodos del clúster.
- Debe seleccionar manualmente el plugin de SnapCenter para Microsoft Windows.

Hosts Linux y AIX



El almacenamiento y las aplicaciones de Oracle son compatibles con AIX.

- Debe haber habilitado la conexión SSH por contraseña para el usuario raíz o no raíz.
- Debe haber instalado Java 11 en el host Linux.

Si utiliza Windows Server 2019 o Windows Server 2016 para el host de SnapCenter Server, debe instalar Java 11. La herramienta de matriz de interoperabilidad (IMT) contiene la información más actualizada sobre requisitos.

["Descargas de Java para todos los sistemas operativos"](#)

["Herramienta de matriz de interoperabilidad de NetApp"](#)

- Tiene que configurar los privilegios sudo para el usuario que no sea raíz con el fin de ofrecer acceso a varias rutas. Añada las siguientes líneas al archivo `/etc/sudoers` mediante la función visudo de Linux.



Asegúrese de utilizar sudo versión 1.8.7 o posterior.

```
Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

`LINUX_USER` es el nombre del usuario que no es raíz que ha creado.

Puede obtener el `checksum_value` del archivo `sc_unix_plugins_checksum.txt`, que se encuentra en:

- `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt` si el servidor SnapCenter está instalado en el host de Windows.
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` si el servidor SnapCenter está instalado en el host Linux.



Se debe utilizar el ejemplo solo como referencia para crear sus propios datos.

Requisitos del host AIX

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



El almacenamiento y las aplicaciones de Oracle son compatibles con AIX.



El plugin de SnapCenter para UNIX que forma parte del paquete de plugins de SnapCenter para AIX, no admite grupos de volúmenes concurrentes.

Elemento	Requisitos
Sistemas operativos	AIX 7,1 o posterior
RAM mínima para el plugin de SnapCenter en el host	4 GB
Espacio de registro e instalación mínimo para el plugin de SnapCenter en el host	2 GB  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.
Paquetes de software obligatorios	Java 11 IBM Java 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.

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

Configure privilegios sudo para usuarios que no son raíz para el host AIX

SnapCenter 4.4 y versiones posteriores permiten que un usuario no raíz instale el paquete de plugins de SnapCenter para AIX e inicie el proceso del plugin. Los procesos del plug-in se ejecutan como un usuario efectivo que no es raíz. Tiene que configurar los privilegios sudo para el usuario que no sea raíz con el fin de ofrecer acceso a varias rutas.

Lo que necesitará

- Sudo versión 1.8.7 o posterior.

- Edite el archivo `/etc/ssh/sshd_config` para configurar los algoritmos de código de autenticación de mensajes: Macs `hmac-sha2-256` y MACs `hmac-sha2-512`.

Reinicie el servicio `sshd` después de actualizar el archivo de configuración.

Ejemplo:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

Acerca de esta tarea

Tiene que configurar los privilegios `sudo` para usuarios que no son raíz con el fin de ofrecer acceso a las rutas siguientes:

- `/Home/AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx`
- `/Custom_location/NetApp/snapcenter/spl/installation/plugins/uninstall`
- `/Custom_location/NetApp/snapcenter/spl/bin/spl`
- Pasos*
 1. Inicie sesión en el host AIX en el que desee instalar el paquete de plugins de SnapCenter para AIX.
 2. Añada las siguientes líneas al archivo `/etc/sudoers` mediante la función `visudo` de Linux.

```

Cmnd_Alias HPPACMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Con
fig_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty

```



Si tiene una configuración de RAC, junto con otros comandos permitidos, debe agregar lo siguiente al archivo `/etc/sudoers`: `'/<crs_home>/bin/olsnodes'`

Puede obtener el valor de `crs_home` del archivo `/etc/oracle/olr.loc`.

`AIX_USER` es el nombre del usuario que no es raíz que ha creado.

Puede obtener el `checksum_value` del archivo `sc_unix_plugins_checksum.txt`, que se encuentra en:

- `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt` si el servidor SnapCenter está instalado en el host de Windows.
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` si el servidor SnapCenter está instalado en el host Linux.



Se debe utilizar el ejemplo solo como referencia para crear sus propios datos.

Requisitos del host para instalar el paquete de plugins de SnapCenter para Windows

Antes de instalar el paquete de plugins de SnapCenter para Windows, debe estar familiarizado con algunos requisitos básicos de espacio y tamaño del sistema host.

Elemento	Requisitos
Sistemas operativos	Microsoft Windows Para obtener la información más reciente sobre las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp" .

Elemento	Requisitos
RAM mínima para el plugin de SnapCenter en el host	1 GB
Espacio de registro e instalación mínimo para el plugin de SnapCenter en el host	<p>5 GB</p> <p> 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.</p>
Paquetes de software obligatorios	<ul style="list-style-type: none"> • .NET Core que comienza con la versión 8.0.5 e incluye todos los parches posteriores de .NET 8 • PowerShell Core 7.4.2 • Java 11 Oracle Java y OpenJDK <p>Para obtener la información más reciente sobre las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp".</p> <p>Para obtener información específica sobre la solución de problemas de .NET, consulte "La actualización o instalación de SnapCenter falla en sistemas heredados que no tienen conexión a Internet."</p>

Requisitos del host para instalar el paquete de plugins de SnapCenter para Linux y AIX

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



El almacenamiento y las aplicaciones de Oracle son compatibles con AIX.

Elemento	Requisitos
Sistemas operativos	<ul style="list-style-type: none"> • Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server (SLES)
RAM mínima para el plugin de SnapCenter en el host	1 GB

Elemento	Requisitos
Espacio de registro e instalación mínimo para el plugin de SnapCenter en el host	2 GB  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.
Paquetes de software obligatorios	Java 11 Oracle Java u OpenJDK 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.

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

Configure credenciales para plugins compatibles con NetApp

SnapCenter utiliza credenciales para autenticar usuarios para las operaciones de SnapCenter. Debe crear credenciales para instalar los plugins de SnapCenter, y credenciales adicionales para realizar operaciones de protección de datos en sistemas de archivos Windows o bases de datos.

Antes de empezar

- Hosts Linux o AIX

Debe configurar credenciales para instalar plugins en hosts Linux o AIX.

Debe configurar las credenciales para el usuario raíz o un usuario que no sea raíz que tenga privilegios sudo para instalar e iniciar el proceso del plugin.

Práctica recomendada: aunque se permite crear credenciales para Linux después de implementar hosts e instalar plugins, la práctica recomendada es crear credenciales después de añadir SVM, antes de implementar hosts e instalar plugins.

- Host Windows

Debe configurar credenciales de Windows antes de instalar plugins.

Debe configurar las credenciales con privilegios de administrador, incluidos los derechos de administrador en el host remoto.

- Aplicaciones de complementos compatibles con NetApp

El plugin utiliza las credenciales seleccionadas o creadas al añadir un recurso. Si un recurso no requiere credenciales durante las operaciones de protección de datos, puede establecer las credenciales como **Ninguno**.

Acerca de esta tarea

Si se configuran las credenciales para grupos de recursos individuales y el nombre de usuario no tiene privilegios de administrador completos, debe asignar al menos los privilegios de grupo de recursos y backup al nombre de usuario.

Pasos

1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
2. En la página Settings, haga clic en **Credential**.
3. Haga clic en **Nuevo**.
4. En la página **Credential**, especifique la información necesaria para configurar las credenciales:

Para este campo...	Realice lo siguiente...
Nombre de credencial	Introduzca un nombre para las credenciales.

Para este campo...	Realice lo siguiente...
Nombre de usuario	<p>Introduzca el nombre de usuario y la contraseña que se utilizarán para la autenticación.</p> <ul style="list-style-type: none"> Administrador de dominio o cualquier miembro del grupo de administradores <p>Especifique el administrador de dominio o cualquier miembro del grupo de administrador en el sistema en el que va a instalar el plugin de SnapCenter. Los formatos válidos para el campo Nombre de usuario son:</p> <ul style="list-style-type: none"> <i>NetBIOS\Username</i> <i>Domain FQDN\Username</i> <ul style="list-style-type: none"> Administrador local (sólo para grupos de trabajo) <p>Para los sistemas que pertenecen a un grupo de trabajo, especifique el administrador local integrado en el sistema en el que va a instalar el plugin de SnapCenter. Puede especificar una cuenta de usuario local que pertenezca al grupo de administradores local si la cuenta de usuario tiene privilegios elevados o si la función de control de acceso de usuario está desactivada en el sistema host. El formato válido para el campo Username es: <i>Username</i></p>
Contraseña	Introduzca la contraseña usada para autenticación.
Tipo de autenticación	Seleccione el tipo de autenticación que desea usar.
Use privilegios sudo	<p>Seleccione la casilla de verificación Use sudo Privileges si va a crear credenciales para usuarios que no son raíz.</p> <div style="display: flex; align-items: center;">  <p>Aplicable únicamente a usuarios Linux y AIX.</p> </div>

5. Haga clic en **Aceptar**.

Después de terminar de configurar las credenciales, puede asignar el mantenimiento de credenciales a un usuario o grupo de usuarios en la página User and Access.

Configurar GMSA en Windows Server 2016 o posterior

Windows Server 2016 o posterior le permite crear una cuenta de servicio administrado de grupo (GMSA) que proporciona gestión automatizada de contraseñas de cuenta de

servicio desde una cuenta de dominio administrado.

Antes de empezar

- Debe tener un controlador de dominio de Windows Server 2016 o posterior.
- Debe tener un host de Windows Server 2016 o posterior, que es miembro del dominio.

Pasos

1. Cree una clave raíz KDS para generar contraseñas únicas para cada objeto de su GMSA.
2. Para cada dominio, ejecute el siguiente comando desde el controlador de dominio de Windows: Add-KDSRootKey -EffectiveImmediately
3. Crear y configurar su GMSA:
 - a. Cree una cuenta de grupo de usuarios con el siguiente formato:

```
domainName\accountName$  
.. Agregar objetos de equipo al grupo.  
.. Utilice el grupo de usuarios que acaba de crear para crear el  
GMSA.
```

Por ejemplo:

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. Ejecución `Get-ADServiceAccount` comando para verificar la cuenta  
de servicio.
```

4. Configure el GMSA en sus hosts:
 - a. Active el módulo de Active Directory para Windows PowerShell en el host en el que desea utilizar la cuenta de GMSA.

Para ello, ejecute el siguiente comando desde PowerShell:

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
-----	----	-----
[] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
-----	-----	-----	-----
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. Reinicie el host.
- b. Instale el GMSA en su host ejecutando el siguiente comando desde el símbolo del sistema de PowerShell: `Install-AdServiceAccount <gMSA>`
- c. Verifique su cuenta de GMSA ejecutando el siguiente comando: `Test-AdServiceAccount <gMSA>`
5. Asigne los privilegios administrativos al GMSA configurado en el host.
6. Agregue el host de Windows especificando la cuenta GMSA configurada en el servidor SnapCenter.

El servidor SnapCenter instalará los plugins seleccionados en el host y el GMSA especificado se utilizará como cuenta de registro de servicio durante la instalación del plugin.

Instale los complementos compatibles con NetApp

Añada hosts e instale paquetes de plugins en hosts remotos

Debe usar la página SnapCenter Add Host para añadir hosts y, a continuación, instalar los paquetes de los plugins. Los plugins se instalan automáticamente en hosts remotos. Puede añadir un host e instalar los paquetes de los plugins para un host individual o para un clúster.

Antes de empezar

- Debe ser un usuario al que se ha asignado una función que tenga permisos de instalación y desinstalación de plugins, como el rol de administrador de SnapCenter.
- Debe asegurarse de que el servicio de cola de mensajes está en ejecución.
- Si está utilizando la cuenta de servicio gestionado en grupo (GMSA), debe configurar GMSA con privilegios administrativos.

["Configurar la cuenta de servicio administrado de grupo en Windows Server 2016 o posterior para aplicaciones personalizadas"](#)

- Para el host de Windows, debe asegurarse de seleccionar el plugin de SnapCenter para Windows.

Acerca de esta tarea

- No es posible añadir un servidor SnapCenter como host de plugins a otro servidor SnapCenter.
- Si instala plugins en un clúster (WSFC), los plugins se instalan en todos los nodos del clúster.

Pasos

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

Para este campo...	Realice lo siguiente...
Tipo de host	<p>Seleccione el tipo de host:</p> <ul style="list-style-type: none"> • Windows • Linux • AIX <p> Los plugins compatibles con NetApp se pueden utilizar en entornos de Windows, Linux y AIX.</p> <p> El almacenamiento y las aplicaciones de Oracle son compatibles con AIX.</p>
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>En los entornos de Windows, la dirección IP es compatible con los hosts de dominio que no son de confianza solo si se resuelve en el FQDN.</p> <p>Puede introducir las direcciones IP o el FQDN de un host independiente.</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 la credencial que ha creado o cree nuevas credenciales.</p> <p>Las credenciales deben tener derechos de administración 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 style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  El modo de autenticación de las credenciales se determina por el tipo de host que especifique en el asistente Add host. </div>

5. En la sección **Seleccione Plug-ins to Install**, seleccione los plugins que desee instalar.

Puede instalar los siguientes plugins de la lista:

- MongoDB
- ORASCPM (se muestra como Aplicaciones Oracle)
- SAP ASE
- MaxDB de SAP
- Reducida

6. (Opcional) Seleccione **Más opciones** para instalar los otros plug-ins.

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 style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  Si ha instalado plugins manualmente y ha especificado un puerto personalizado, debe especificar el mismo puerto. De lo contrario, la operación dará error. </div>

Para este campo...	Realice lo siguiente...
Ruta de instalación	<p>Los plugins compatibles con NetApp pueden instalarse en sistemas Windows o Linux.</p> <ul style="list-style-type: none"> En el caso del paquete de plugins de SnapCenter para Windows, la ruta predeterminada es C:\Program Files\NetApp\SnapCenter. <p>Opcionalmente, puede personalizar la ruta.</p> <ul style="list-style-type: none"> Para el paquete de plugins de SnapCenter para Linux y el paquete de plugins de SnapCenter para AIX, la ruta predeterminada es /opt/NetApp/snapcenter. <p>Opcionalmente, puede personalizar la ruta.</p>
Omitir comprobaciones previas a la instalación	<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>
Utilice Group Managed Service Account (GMSA) para ejecutar los servicios de plug-in	<p>En el caso de host de Windows, seleccione esta casilla de comprobación si desea utilizar una cuenta de servicio gestionado de grupo (GMSA) para ejecutar los servicios de plugin.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> Proporcione el nombre de GMSA con el siguiente formato: Nombre_de_dominio\accountName\$.</p> <p> GMSA se utilizará como cuenta de servicio de inicio de sesión solo en el complemento SnapCenter para el servicio de Windows.</p> </div>

7. Seleccione **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. El espacio en disco, RAM, versión de PowerShell, versión de .NET, ubicación (para plugins de Windows) y versión de Java (para plugins de Linux) se validan frente a los requisitos mínimos. Si no se satisfacen los requisitos mínimos, se muestran los mensajes de error o advertencia correspondientes.

Si el error está relacionado con el espacio en disco o RAM, puede 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 debe solucionar el problema.



En una configuración de alta disponibilidad, si actualiza SnapManager.web.ui.dll.config, debe actualizar el archivo en ambos nodos y reiniciar el grupo de aplicaciones de SnapCenter.

La ruta predeterminada de Windows es `C:\Program Files\NetApp\SnapCenter\WebApp\SnapManager.Web.UI.dll.config`

La ruta predeterminada de Linux es

`/opt/NetApp/snapcenter/SnapManagerWeb/SnapManager.Web.UI.dll.config`

8. Si el tipo de host es Linux, verifique la huella dactilar y, a continuación, seleccione **Confirmar y Enviar**.



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

9. Supervise el progreso de la instalación.

Los archivos de registro específicos de la instalación se encuentran en `/custom_location/snapcenter/registros`.

Instale paquetes de plugins de SnapCenter para Linux, Windows o AIX en varios hosts remotos mediante cmdlets

Puede instalar los paquetes de plugins de SnapCenter para Linux, Windows o AIX en varios hosts a la vez mediante el cmdlet de PowerShell `Install-SmHostPackage`.

Antes de empezar

El usuario que agrega un host debe tener derechos administrativos en el host.



El almacenamiento y las aplicaciones de Oracle son compatibles con AIX.

Pasos

1. Inicie PowerShell.
2. En el host de SnapCenter Server, establezca una sesión mediante el cmdlet `Open-SmConnection` y, a continuación, introduzca sus credenciales.
3. Instale el plugin en varios hosts mediante el cmdlet `Install-SmHostPackage` y los parámetros requeridos.

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"](#).

Puede utilizar la opción `-skipprecheck` cuando haya instalado los plugins manualmente y no quiera validar si el host cumple los requisitos para instalar el plugin.

4. Introduzca sus credenciales para la instalación remota.

Instale los plugins compatibles con NetApp en los hosts Linux mediante la interfaz de línea de comandos

Debe instalar los plugins compatibles de NetApp mediante la interfaz de usuario (UI) de

SnapCenter. Si el entorno no permite la instalación remota del plugin desde la interfaz de usuario de SnapCenter, puede instalar los complementos compatibles con NetApp en el modo de consola o en el modo silencioso mediante la interfaz de línea de comandos (CLI).

Pasos

1. Copie el archivo de instalación del paquete de plugins de SnapCenter para Linux (snapcenter_linux_host_plugin.bin) desde C:\ProgramData\NetApp\SnapCenter\Package Repository en el host en el que desea instalar los plugins compatibles de NetApp.

Puede acceder a esta ruta desde el host en el que está instalado el servidor SnapCenter.

2. Desde el símbolo del sistema, desplácese hasta el directorio en el que copió el archivo de instalación.
3. Instale el plugin: `path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address -DSERVER_HTTPS_PORT=port_number_for_server`
 - -DPORT indica el puerto de comunicación HTTPS de SMCORE.
 - -DSERVER_IP indica la dirección IP del servidor SnapCenter.
 - -DSERVER_HTTPS_PORT indica el puerto HTTPS del servidor SnapCenter.
 - -DUSER_INSTALL_DIR indica el directorio en el que desea instalar el paquete de plugins de SnapCenter para Linux.
 - _DINSTALL_LOG_NAME indica el nombre del archivo de registro.

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. Añada el host al servidor de SnapCenter con el cmdlet Add-Smhost y los parámetros requeridos.

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

5. Inicie sesión en SnapCenter y cargue el plugin compatible con NetApp desde la interfaz de usuario de o mediante cmdlets de PowerShell.

En la sección, puede cargar el plugin compatible con NetApp desde la interfaz de usuario ["Añada hosts e instale paquetes de plugins en hosts remotos"](#).

La ayuda sobre cmdlet de SnapCenter y la información de referencia sobre cmdlet contienen más información acerca de cmdlets de PowerShell.

["Guía de referencia de cmdlets de SnapCenter Software"](#).

Supervise el estado de instalación de los plugins compatibles con NetApp

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**.

Configurar certificado de CA

Genere un archivo CSR de certificado de CA

Es posible generar una solicitud de firma de certificación (CSR) e importar el certificado que puede obtenerse de una entidad de certificación (CA) con la CSR generada. El certificado tendrá una clave privada asociada.

CSR es un bloque de texto codificado que se da a un proveedor de certificados autorizado para obtener el certificado de CA firmado.



La longitud de la clave RSA del certificado de CA debe ser de 3072 bits como mínimo.

Para obtener información sobre cómo generar una CSR, consulte "[Cómo generar el archivo CSR de certificado de CA](#)".



Si posee el certificado de CA para su dominio (*.domain.company.com) o su sistema (machine1.domain.company.com), puede omitir la generación del archivo CSR del certificado de CA. Puede implementar el certificado de CA existente con SnapCenter.

Para las configuraciones de clúster, el nombre de clúster (FQDN de clúster virtual) y los respectivos nombres de host se deben mencionar en el certificado de CA. El certificado se puede actualizar rellorando el campo Nombre alternativo del sujeto (SAN) antes de obtener el certificado. Para un certificado de comodines (*.domain.company.com), el certificado contendrá implícitamente todos los nombres de host del dominio.

Importar certificados de CA

Debe importar los certificados de CA a SnapCenter Server y a los plugins de host de Windows mediante la consola de gestión de Microsoft (MMC).

Pasos

1. Vaya a la consola de administración de Microsoft (MMC) y, a continuación, haga clic en **Archivo > Agregar o quitar Snapin**.
2. En la ventana Agregar o quitar complementos, seleccione **certificados** y, a continuación, haga clic en **Agregar**.
3. En la ventana del complemento certificados, seleccione la opción **cuenta de equipo** y, a continuación, haga clic en **Finalizar**.
4. Haga clic en **raíz de consola > certificados – Equipo local > entidades de certificación raíz de confianza > certificados**.
5. Haga clic con el botón secundario en la carpeta “entidades de certificación raíz de confianza” y, a continuación, seleccione **todas las tareas > Importar** para iniciar el asistente de importación.
6. Complete el asistente de la siguiente manera:

En esta ventana del asistente...	Haga lo siguiente...
Importar clave privada	Seleccione la opción Sí , importe la clave privada y, a continuación, haga clic en Siguiente .
Importar formato de archivo	No realice cambios; haga clic en Siguiente .
Seguridad	Especifique la nueva contraseña que se utilizará para el certificado exportado y, a continuación, haga clic en Siguiente .
Finalización del Asistente para importación de certificados	Revise el resumen y, a continuación, haga clic en Finalizar para iniciar la importación.



El certificado de importación se debe empaquetar con la clave privada (los formatos admitidos son: *.pfx, *.p12 y *.p7b).

7. Repita el paso 5 para la carpeta “personal”.

Obtenga la huella digital del certificado de CA

Una huella digital de certificado es una cadena hexadecimal que identifica un certificado. La huella digital se calcula a partir del contenido del certificado mediante un algoritmo de huella digital.

Pasos

1. Realice lo siguiente en la interfaz gráfica de usuario:
 - a. Haga doble clic en el certificado.
 - b. En el cuadro de diálogo Certificado, haga clic en la ficha **Detalles**.
 - c. Desplácese por la lista de campos y haga clic en **Thumbprint**.
 - d. Copie los caracteres hexadecimales del cuadro.
 - e. Quite los espacios entre los números hexadecimales.

Por ejemplo, si la huella digital es: "a9 09 50 2d 2a e4 e4 14 33 f8 38 86 b0 0d 42 77 a3 2a 7b", después de quitar los espacios, será: "a90d8 2dd82a41433e6f83886b00d4277a32a7b".

2. Realice lo siguiente desde PowerShell:
 - a. Ejecute el siguiente comando para enumerar la huella digital del certificado instalado e identificar el certificado instalado recientemente por el nombre del sujeto.

```
Get-ChildItem -Path Cert:\LocalMachine\My
```

- b. Copie la huella digital.

Configure el certificado de CA con servicios de plugins de host de Windows

Debe configurar el certificado de CA con servicios de plugins del host de Windows para activar el certificado digital instalado.

Realice los siguientes pasos en el servidor de SnapCenter y en todos los hosts del plugin donde ya se hayan implementado certificados de CA.

Pasos

1. Elimine el enlace existente del certificado con el puerto 8145 predeterminado de SMCore. Para ello, ejecute el siguiente comando:

```
> netsh http delete sslcert ipport=0.0.0.0:_{SMCore Port}
```

Por ejemplo:

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. Enlace el certificado recientemente instalado con los servicios de
plugins del host de Windows mediante la ejecución de los siguientes
comandos:
```

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

Por ejemplo:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

Configure el certificado de CA para el servicio de plugins compatibles con NetApp en el host Linux

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

Los plugins personalizados utilizan el archivo 'keystore.jks', que se encuentra en */opt/NetApp/snapcenter/scc/etc* tanto como en su almacén de confianza como en su almacén de claves.

Gestionar contraseña para el almacén de claves del plugin personalizado 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 plugin personalizado desde el archivo de propiedades del agente del plugin personalizado.

Es el valor correspondiente a la clave '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_in_cert" -keystore keystore.jks
```

Actualice lo mismo para el archivo key KEYSTORE_PASS en *agent.properties*.

3. Reinicie el servicio después de cambiar la contraseña.



La contraseña para el almacén de claves de plugin personalizado 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 del plugin personalizado

Debe configurar los certificados intermedios o de raíz sin la clave privada para personalizar el almacén de confianza del plugin.

Pasos

1. Desplácese hasta la carpeta que contiene el almacén de claves del plugin personalizado:
/Opt/NetApp/snapcenter/scc/etc.
2. Busque el archivo 'keystore.jks'.
3. Enumere los certificados añadidos al almacén de claves:

```
keytool -list -v -keystore keystore.jks
```

4. Añada un certificado raíz o intermedio:

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks  
. Reinicie el servicio después de configurar los certificados raíz o  
intermedios en el almacén de confianza del plugin personalizado.
```



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

Configure el par de claves firmadas de CA para el almacén de confianza del plugin personalizado

Debe configurar la pareja de claves firmadas de CA en el almacén de confianza del plugin personalizado.

Pasos

1. Desplácese hasta la carpeta que contiene el almacén de claves del plugin personalizado
/opt/NetApp/snapcenter/scc/etc.
2. Busque el archivo 'keystore.jks'.
3. Enumere los certificados añadidos al almacén de claves:

```
keytool -list -v -keystore keystore.jks
```

4. Agregue el certificado de CA con clave pública y privada.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. Enumere los certificados añadidos al almacén de claves.

```
keytool -list -v -keystore keystore.jks
```

6. Compruebe que el almacén de claves contiene el alias correspondiente al nuevo certificado de CA, que se añadió al almacén de claves.

7. Cambie la contraseña de clave privada añadida para el certificado de CA a la contraseña del almacén de claves.

La contraseña predeterminada del plugin personalizado keystore es el valor de key KEYSTORE_PASS en el archivo agent.properties.

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -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 "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks
```

. Configure el nombre del alias del certificado de CA en el archivo agent.properties.

Actualice este valor con la clave SCC_CERTIFICATE_ALIASES.

8. Reinicie el servicio después de configurar el par de claves firmado de CA en el almacén de confianza del plugin personalizado.

Configurar la lista de revocación de certificados (CRL) para los plugins personalizados de SnapCenter

Acerca de esta tarea

- Los complementos personalizados de SnapCenter buscarán los archivos CRL en un directorio preconfigurado.
- El directorio predeterminado de los archivos CRL de los plugins personalizados de SnapCenter es 'opt/NetApp/snapcenter/scc/etc/crl'.

Pasos

1. Puede modificar y actualizar el directorio predeterminado del archivo agent.properties en función de la CLAVE CRL_PATH.

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

Configure el certificado de CA para el servicio de plugins compatibles con NetApp en el host de Windows

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

Los plugins personalizados utilizan el archivo *keystore.jks*, que se encuentra en *C:\Program*

Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc, tanto como su almacén de confianza como su almacén de claves.

Gestionar contraseña para el almacén de claves del plugin personalizado 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 plugin personalizado desde el archivo de propiedades del agente del plugin personalizado.

Es el valor que corresponde a la clave *KEYSTORE_PASS*.

2. Cambie la contraseña del almacén de claves:

```
keytool -storepasswd -keystore.jks
```



Si el comando "keytool" no se reconoce en el símbolo del sistema de Windows, reemplace el comando keytool por su ruta completa.

```
C:\Archivos de programa\Java\<jdk_version>\bin\keytool.exe" -storepasswd -keystore.jks
```

3. 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_in_cert" -keystore keystore.jks
```

Actualice lo mismo para el archivo key *KEYSTORE_PASS* en *agent.properties*.

4. Reinicie el servicio después de cambiar la contraseña.



La contraseña para el almacén de claves de plugin personalizado 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 del plugin personalizado

Debe configurar los certificados intermedios o de raíz sin la clave privada para personalizar el almacén de confianza del plugin.

Pasos

1. Desplácese hasta la carpeta que contiene el almacén de claves del plugin personalizado *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*

2. Busque el archivo 'keystore.jks'.

3. Enumere los certificados añadidos al almacén de claves:

```
keytool -list -v -keystore.jks
```

4. Añada un certificado raíz o intermedio:

```
Keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore.jks
```

5. Reinicie el servicio después de configurar los certificados raíz o intermedios en el almacén de confianza del plugin personalizado.



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

Configure el par de claves firmadas de CA para el almacén de confianza del plugin personalizado

Debe configurar la pareja de claves firmadas de CA en el almacén de confianza del plugin personalizado.

Pasos

1. Desplácese hasta la carpeta que contiene el almacén de claves del plugin personalizado *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
2. Busque el archivo *keystore.jks*.
3. Enumere los certificados añadidos al almacén de claves:

```
keytool -list -v -keystore.jks
```

4. Agregue el certificado de CA con clave pública y privada.

```
Keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore.jks -deststoretype JKS
```

5. Enumere los certificados añadidos al almacén de claves.

```
keytool -list -v -keystore.jks
```

6. Compruebe que el almacén de claves contiene el alias correspondiente al nuevo certificado de CA, que se añadió al almacén de claves.
7. Cambie la contraseña de clave privada añadida para el certificado de CA a la contraseña del almacén de claves.

La contraseña predeterminada del plugin personalizado keystore es el valor de key KEYSTORE_PASS en el archivo *agent.properties*.

```
Keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore.jks
```

8. Configure el nombre del alias del certificado de CA en el archivo *agent.properties*.

Actualice este valor con la clave SCC_CERTIFICATE_ALIAS.

9. Reinicie el servicio después de configurar el par de claves firmado de CA en el almacén de confianza del plugin personalizado.

Configurar la lista de revocación de certificados (CRL) para los plugins personalizados de SnapCenter

Acerca de esta tarea

- Para descargar el último archivo CRL del certificado de CA relacionado, consulte ["Cómo actualizar el archivo de lista de revocación de certificados en el certificado de CA de SnapCenter"](#).
- Los complementos personalizados de SnapCenter buscarán los archivos CRL en un directorio preconfigurado.
- El directorio predeterminado de los archivos CRL de los plugins personalizados de SnapCenter es *'C:\Archivos de programa\NetApp\SnapCenter\Snapcenter Plug-in Creator\ etc\crl'*.

Pasos

1. Puede modificar y actualizar el directorio predeterminado del archivo *agent.properties* en función de la

CLAVE 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.

Prepárese para la protección de datos

Requisitos previos para usar los plugins compatibles de NetApp

Antes de usar plugins compatibles con SnapCenter NetApp, el administrador de SnapCenter debe instalar y configurar SnapCenter Server, así como ejecutar las tareas especificadas en los requisitos previos.

- Instalar y configurar SnapCenter Server.
- Inicie sesión en el servidor SnapCenter.
- Configure el entorno de SnapCenter añadiendo conexiones con el sistema de almacenamiento y creando credenciales, si es necesario.
- Añada hosts, e instale y cargue los plugins.
- Si corresponde, instale Java 11 en el host del plugin.
- Si tiene varias rutas de datos (LIF) o una configuración de dNFS, puede realizar lo siguiente mediante la CLI de SnapCenter en el host de la base de datos:
 - De forma predeterminada, todas las direcciones IP del host de la base de datos se añaden a la directiva de exportación de almacenamiento de NFS en la máquina virtual de almacenamiento (SVM) para los volúmenes clonados. Si desea contar con una dirección IP específica o restringir a una subred de direcciones IP, ejecute la CLI de `Set-PreferredHostIPsInStorageExportPolicy`.
 - Si tiene varias LIF en las SVM, SnapCenter elige la ruta de LIF correspondiente para montar el volumen clonado de NFS. No obstante, si desea especificar una determinada ruta de LIF, debe ejecutar la CLI de `Set-SvmPreferredDataPath`. La información relativa a los parámetros que se pueden utilizar con el comando y sus descripciones se puede obtener ejecutando `Get-Help nombre_comando`. Alternativamente, también puede consultar la ["Guía de referencia de comandos del software SnapCenter"](#).
- Configure SnapMirror y SnapVault si quiere realizar una replicación de backup.
- Asegúrese de que el puerto 9090 no esté en uso en otra aplicación del host.

El uso del puerto 9090 debe reservarse a los plugins compatibles con NetApp, junto con los otros puertos requeridos por SnapCenter.

Cómo se usan los recursos, los grupos de recursos y las políticas para proteger los recursos de plugins compatibles con NetApp

Antes de usar SnapCenter, es necesario comprender ciertos conceptos básicos vinculados con las operaciones de backup, clonado y restauración que se ejecutan. El usuario interactúa con recursos, grupos de recursos y políticas para diferentes operaciones.

- Los recursos generalmente son bases de datos, sistemas de archivos de Windows o máquinas virtuales que se incluyen en un backup o se clonan con SnapCenter.
- Un grupo de recursos de SnapCenter es una agrupación de recursos en un host o un clúster.

Al realizar una operación con un grupo de recursos, esta se ejecuta en los recursos definidos en el grupo de acuerdo con la programación que se especificó para dicho grupo de recursos.

Es posible realizar un backup bajo demanda de un solo recurso o de un grupo de recursos. También puede realizar backups programados para recursos individuales y para grupos de recursos.

- Las políticas especifican la frecuencia de backup, la retención de copias, la replicación, los scripts y otras características de las operaciones de protección de datos.

Cuando se crea un grupo de recursos, se seleccionan una o varias políticas para él. Asimismo, puede seleccionar una política al realizar un backup bajo demanda para un recurso individual.

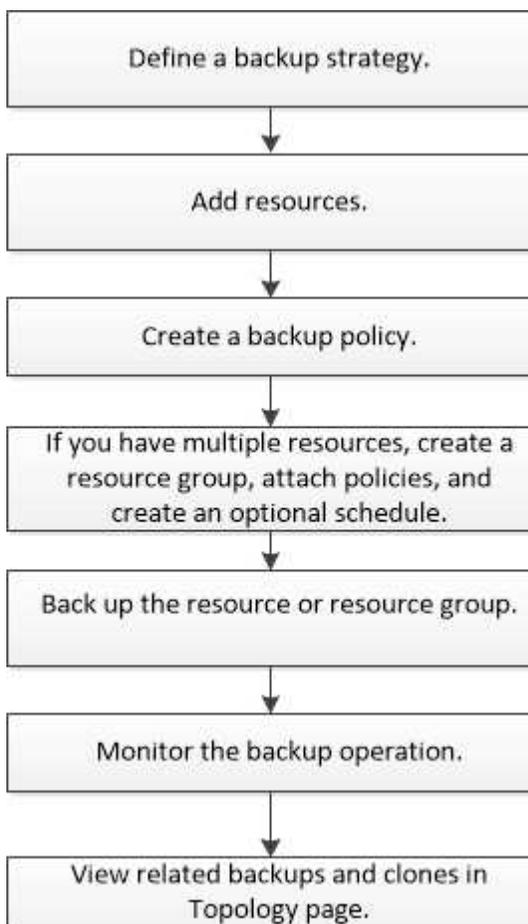
Piense en un grupo de recursos como definir *qué* desea proteger y cuándo desea protegerlo en términos de día y hora. Piense en una directiva como definir *how* desea protegerla. Cuando se realiza un backup de todas las bases de datos o todos los sistemas de archivos de un host, por ejemplo, puede crearse un grupo de recursos que incluya todas las bases de datos o todos los sistemas de archivos del host. Luego, se pueden vincular dos políticas al grupo de recursos: Una diaria y una horaria. Cuando crea el grupo de recursos y añade las políticas, puede configurar el grupo de recursos para que ejecute un backup diario basado en archivos y otra programación que ejecute un backup por hora basado en Snapshot.

Realizar backup de los recursos de plugins compatibles con NetApp

Realizar backup de los recursos de plugins compatibles con NetApp

El flujo de trabajo de backup incluye planificar, identificar los recursos para el backup, gestionar las políticas de backup, crear grupos de recursos y añadir políticas, crear backups y supervisar las operaciones.

Los siguientes flujos de trabajo muestran la secuencia que debe seguirse para realizar la operación de backup:



También puede usar los cmdlets de PowerShell manualmente o en scripts para realizar operaciones de backup, restauración y clonado. Para obtener información detallada sobre los cmdlets de PowerShell, use la ayuda de cmdlets de SnapCenter o consulte la ["Guía de referencia de cmdlets de SnapCenter Software"](#)

Añada recursos a los plugins compatibles con NetApp

Debe añadir los recursos que desee incluir en un backup o clonar. En función de su entorno, los recursos pueden ser instancias de una base de datos o recopilaciones que desee clonar o incluir en un backup.

Antes de empezar

- Debe haber completado ciertas tareas, como instalar el servidor SnapCenter, añadir hosts, crear conexiones con el sistema de almacenamiento y añadir credenciales.
- Debe haber cargado los plugins en SnapCenter Server.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Recursos, selecciona **Agregar recurso**.
3. En la página Provide Resource Details, realice las siguientes acciones:

Para este campo...	Realice lo siguiente...
Nombre	Escriba el nombre del recurso.
Nombre de host	Seleccione el host.
Tipo	Seleccione el tipo. El usuario define el tipo según el archivo de descripción del plugin. Por ejemplo, base de datos e instancia. Si el tipo seleccionado tiene un elemento principal, escriba los detalles de dicho elemento. Por ejemplo, si el tipo es una base de datos y el elemento principal es una instancia, escriba los detalles de la instancia.
Nombre de credencial	Seleccione Credencial o cree una credencial nueva.
Monte las rutas	Escriba las rutas de montaje en el punto donde se monta el recurso. Solo corresponde a un host Windows.

4. En la página Provide Storage Footprint, seleccione un sistema de almacenamiento y elija uno o más volúmenes, LUN y qtrees y, a continuación, seleccione **Save**.

Opcional: Seleccione la  Icono para añadir más volúmenes, LUN y qtrees desde otros sistemas de almacenamiento.



Los plugins compatibles con NetApp no admiten la detección automática de los recursos. Los detalles de almacenamiento de entornos físicos y virtuales también no se detectan automáticamente. Debe proporcionar la información de almacenamiento de los entornos físico y virtual durante la creación de los recursos.

Add Storage Resource

1 Name

2 **Storage Footprint**

3 Resource Settings

4 Summary

Provide Storage Footprint Details

Storage Type ONTAP Azure NetApp Files

Add Storage Footprint

Storage System

Select one or more volumes and if required their associated Qtrees and LUNs

Volume name LUNs or Qtrees

Save

5. En la página Resource Settings, proporcione pares personalizados de clave-valor para el recurso.



Asegúrese de que el nombre de las claves personalizadas está en mayúsculas.

Resource settings

Custom key-value pairs for MySQL plug-in

Name	Value
HOST	localhost
PORT	3306
MASTER_SLAVE	NO

Para conocer los parámetros de conexión correspondientes, consulte "[Parámetros para configurar el recurso](#)"

6. Revisa el resumen y luego selecciona **Finalizar**.

Resultado

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



Es necesario actualizar los recursos si se cambia el nombre de las bases de datos fuera de SnapCenter.

Después de terminar

Si desea proporcionar acceso a los activos a otros usuarios, el administrador de SnapCenter debe realizar la asignación. De este modo, los usuarios pueden realizar las acciones para las cuales tienen permisos sobre los activos que les asignaron.

Después de añadir los recursos, puede modificar sus detalles. Si un recurso de plugins compatibles con NetApp tiene backups asociados, los siguientes campos no se pueden modificar: Nombre del recurso, tipo de recurso y nombre de host.

Parámetros para configurar el recurso

Si va a añadir los plugins manualmente, puede utilizar los siguientes parámetros para configurar el recurso en la página Resource Settings.

Plugin para MongoDB

Configuración del recurso:

- MONGODB_APP_SERVER=(para el tipo de recurso como cluster compartido) o MONGODB_REPLICASET_SERVER=(para el tipo de recurso como replicaset)
- OPLOG_PATH=(Parámetro opcional en caso de que se proporcione desde MongoDB.propertiesfile)
- MONGODB_AUTHENTICATION_TYPE= (PLAIN para la autenticación LDAP y Ninguno para otros)

Debe proporcionar los siguientes parámetros n archivo MongoDB.properties:

- DISABLE_START_STOP_SERVICES=
 - N si el plugin realiza los servicios start/stop.
 - Si el usuario realiza los servicios START/**STOP.
 - El parámetro opcional como valor predeterminado se establece en N.
- OPLOG_PATH_= (Parámetro opcional en caso de que ya se haya proporcionado como par clave-valor personalizado en SnapCenter).

Plugin para MaxDB

Configuración del recurso:

- XUSER_ENABLE (Y|N) activa o desactiva el uso de un xuser para MaxDB para que no se necesite una contraseña para el usuario de la base de datos.
- HANDLE_LOGWRITER (Y|N) ejecuta operaciones de suspensión del escritor de registro (N) o reanudación del escritor de registro (Y).
- DBMCLICMD (path_to_dbmcli_cmd) especifica la ruta al comando dbmcli de MaxDB. Si no se define, se utiliza dbmcli en la ruta de búsqueda.



En el caso de entornos Windows, la ruta debe estar entre comillas dobles ('...').

- SQLCLICMD (path_to_sqlcli_cmd) especifica la ruta al comando sqlcli de MaxDB. Si la ruta de acceso no está definida, sqlcli se utiliza en la ruta de búsqueda.
- MAXDB_UPDATE_HIST_LOG (Y|N) indica al programa de copia de seguridad de MaxDB si debe actualizar el registro del historial de MaxDB.
- MAXDB_CHECK_SNAPSHOT_DIR : example, SID1:directory[,directory...]; [SID2:directoary[,directory...]
Comprueba que una operación de copia de Snapshot de Snap Creator se realice correctamente y garantiza que se cree la snapshot.

Esto se aplica únicamente a NFS. El directorio debe apuntar a la ubicación que contiene el directorio .snapshot. Se pueden incluir varios directorios en una lista separada por comas.

En MaxDB 7.8 y versiones posteriores, la solicitud de backup de base de datos se Marca con errores en el historial de backup.

- **MAXDB_BACKUP_TEMPLATES:** Especifica una plantilla de copia de seguridad para cada base de datos.

La plantilla debe existir y ser un tipo externo de plantilla de copia de seguridad. Para habilitar la integración de instantáneas para MaxDB 7,8 y posterior, debe tener la funcionalidad de servidor en segundo plano de MaxDB y la plantilla de copia de seguridad de MaxDB ya configurada del tipo EXTERNO.

- **MAXDB_BG_SERVER_PREFIX:** Especifica el prefijo para el nombre del servidor en segundo plano.

Si se establece el parámetro **MAXDB_BACKUP_TEMPLATES**, también debe establecer el parámetro **MAXDB_BG_SERVER_PREFIX**. Si no establece el prefijo, se utiliza el valor predeterminado **na_bg_**.

Plugin para SAP ASE

Configuración del recurso:

- **SYBASE_SERVER (DATA_SERVER_NAME)** especifica el nombre del servidor de datos Sybase (opción-S en el comando isql). Por ejemplo, **p_test**.
- **SYBASE_DATABASES_EXCLUDE (db_name)** permite excluir las bases de datos si se utiliza la construcción "ALL".

Puede especificar varias bases de datos con una lista separada por punto y coma. Por ejemplo: **pubs2;test_db1**.

- **SYBASE_USER:** **User_name** especifica el usuario del sistema operativo que puede ejecutar el comando isql.

Necesario para UNIX. Este parámetro es obligatorio si el usuario que ejecuta los comandos start y stop de Snap Creator Agent (normalmente el usuario raíz) y el usuario que ejecuta el comando isql son diferentes.

- **SYBASE_TRAN_DUMP db_name:DIRECTORY_PATH** permite realizar un volcado de transacciones de Sybase después de crear una instantánea. Por ejemplo, **pubs2:/sybasedumps/ pubs2**

Debe especificar cada base de datos que necesita un volcado de transacciones.

- **SYBASE_TRAN_DUMP_COMPRESS (Y|N)** activa o desactiva la compresión de volcado de transacciones de Sybase nativa.
- **SYBASE_iSQL_CMD** (por ejemplo, **/opt/sybase/ocs-15_0/bin/isql**) define la ruta de acceso al comando isql.
- **SYBASE_EXCLUDE_TEMPDB (Y|N)** permite excluir automáticamente las bases de datos temporales creadas por el usuario.

Complemento para aplicaciones Oracle (ORASCPM)

Configuración del recurso:

- **SQLPLUS_cmd** especifica la ruta a sqlplus.
- **ORACLE_DATABASES** muestra las bases de datos de Oracle de las que se debe realizar un backup y el usuario correspondiente (database:user).
- **CNTL_FILE_BACKUP_DIR** especifica el directorio para la copia de seguridad del archivo de control.

- ORA_TEMP especifica el directorio de los archivos temporales.
- ORACLE_HOME especifica el directorio en el que está instalado el software de Oracle.
- ARCHIVE_LOG_ONLY especifica si se realizará o no el backup de los registros de archivos.
- ORACLE_BACKUP_MODE especifica si se realizará una copia de seguridad en línea o fuera de línea.

Crear políticas para los recursos de plugins compatibles con NetApp

Antes de usar SnapCenter para realizar un backup de recursos específicos de un plugin compatible con NetApp, debe crear una política de backup para el recurso o el grupo de recursos que incluirá en el backup.

Antes de empezar

- Debe tener definida una estrategia de backup.

Para obtener detalles, consulte la información sobre cómo definir una estrategia de protección de datos para los plugins compatibles con NetApp.

- Debe tener preparada la protección de datos.

La preparación de la protección de datos incluye instalar SnapCenter, añadir hosts, crear conexiones con el sistema de almacenamiento y añadir recursos.

- Debe asignar las máquinas virtuales de almacenamiento (SVM) para operaciones de mirroring o almacén.

El administrador de SnapCenter debe haberle asignado las instancias de SVM de los volúmenes de origen y de destino en caso de que replique snapshots en un reflejo o almacén.

- Debe añadir manualmente los recursos que desee proteger.

Acerca de esta tarea

- Una política de backup es un conjunto de reglas que rigen cómo gestionar, programar y retener backups. De forma adicional, puede definir la configuración de replicación, script y aplicaciones.
- Puede especificar opciones en la política para ahorrar tiempo cuando desee reutilizarla con otro grupo de recursos.
- 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.



La configuración principal de SnapLock se gestiona en la política de backup de SnapCenter y la configuración secundaria de SnapLock se gestiona mediante ONTAP.

Pasos

1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
2. En la página Configuración, haga clic en **Directivas**.
3. Haga clic en **Nuevo**.
4. En la página Name, escriba el nombre de la política y una descripción.
5. En la página Settings, realice los siguientes pasos:
 - Especifique el tipo de programa seleccionando **a petición, hora, Diario, Semanal** o **Mensual**.



Puede especificar la programación (fecha de inicio, fecha de finalización y frecuencia) para la operación de backup mientras crea un grupo de recursos. De este modo, puede crear grupos de recursos que compartan la misma política y la misma frecuencia de backup, pero también asignar diferentes programaciones de backup a cada política.

Schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

On demand

Hourly

Daily

Weekly

Monthly



Si ha programado para las 2:00 a.m., la programación no se activará durante el horario de verano.

- En la sección Custom backup settings, proporcione los ajustes específicos de backup que deban pasarse al plugin en formato de clave-valor. Puede pasar varios pares de clave-valor al plugin.
6. En la página **Retention**, especifique la configuración de retención para el tipo de copia de seguridad y el tipo de programación seleccionado en la página **Backup Type**:

Si desea...	Realice lo siguiente...
Mantenga un cierto número de Snapshots	<p>Seleccione Total Snapshot copies to keep 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 style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p> 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.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p> El valor de retención máximo es 1018 para recursos en ONTAP 9.4 o posterior, y 254 para recursos en ONTAP 9.3 o anterior. Se producirá un error en los backups si la retención se establece en un valor superior a la versión de ONTAP subyacente.</p> </div>
Mantenga los Snapshots durante una cierta cantidad de días	Seleccione Mantener copias snapshot para y, a continuación, especifique el número de días durante los cuales desea conservar las instantáneas antes de eliminarlas.
Período de bloqueo de copia de snapshot	<p>Seleccione Período de bloqueo de instantáneas y seleccione Días, Meses o Años.</p> <p>El período de retención de SnapLock debe ser inferior a 100 años.</p>

7. En la página **Replicación**, especifique la configuración de replicación:

Para este campo...	Realice lo siguiente...
<p>Actualizar SnapMirror después de crear una copia Snapshot local</p>	<p>Seleccione este campo para crear copias reflejadas de los conjuntos de backup en otro volumen (replicación de SnapMirror).</p> <p>Si la relación en ONTAP es del tipo Reflejo y almacén y solo se selecciona esta opción, Snapshot creado en el origen no se transferirá al destino, pero figurará en el destino. Si esta copia Snapshot se selecciona del destino con el fin de realizar una operación de recuperación, aparece un mensaje de error indicando que la ubicación secundaria no está disponible para el backup reflejado/en almacenamiento.</p> <p>Durante la replicación secundaria, el tiempo de caducidad del SnapLock carga el tiempo de caducidad del SnapLock principal.</p> <p>Al hacer clic en el botón Refrescar de la página Topología, se actualiza el tiempo de caducidad de SnapLock secundario y primario que se recuperan de ONTAP.</p> <p>Consulte "Ver los clones y backups relacionados con los recursos de plugins admitidos en NetApp en la página Topology".</p>
<p>Actualizar SnapVault después de crear una copia Snapshot local</p>	<p>Seleccione esta opción para realizar una replicación de backup disco a disco (backups de SnapVault).</p> <p>Durante la replicación secundaria, el tiempo de caducidad del SnapLock carga el tiempo de caducidad del SnapLock principal. Al hacer clic en el botón Refrescar de la página Topología, se actualiza el tiempo de caducidad de SnapLock secundario y primario que se recuperan de ONTAP.</p> <p>Cuando SnapLock se configura solo en el secundario desde ONTAP conocido como Almacén de SnapLock, al hacer clic en el botón Refrescar de la página Topología se actualiza el período de bloqueo en el secundario que se recupera de ONTAP.</p> <p>Para obtener más información sobre el almacén de SnapLock, consulte Confirmar instantáneas en WORM en un almacén destino</p> <p>"Ver los clones y backups relacionados con los recursos de plugins admitidos en NetApp en la página Topology".</p>

Para este campo...	Realice lo siguiente...
Etiqueta de política secundaria	<p>Seleccione una etiqueta de Snapshot.</p> <p>Según la etiqueta de Snapshot que seleccione, ONTAP aplicará la política de retención de Snapshot secundaria que corresponda a esa etiqueta.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> Si ha seleccionado Actualizar SnapMirror después de crear una copia Snapshot local, puede especificar opcionalmente la etiqueta de la directiva secundaria. Sin embargo, si ha seleccionado Actualizar SnapVault después de crear una copia Snapshot local, debe especificar la etiqueta de la directiva secundaria.</p> </div>
Número de reintentos de error	<p>Escriba el número máximo de intentos de replicación que se permitirán antes de que la operación se detenga.</p>



Debe configurar la política de retención de SnapMirror en ONTAP para el almacenamiento secundario a fin de evitar que se alcance el límite máximo de Snapshots en el almacenamiento secundario.

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

Crear grupos de recursos y añadir políticas

Un grupo de recursos es el contenedor al que debe añadir los recursos que desea proteger e incluir en un backup. Permite realizar un backup en simultáneo con todos los datos que están asociados con una aplicación determinada. También debe añadir una o más políticas al grupo de recursos para definir el tipo de trabajo de protección de datos que desea realizar.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Resources, seleccione New Resource Group.
3. En la página Name, realice los siguientes pasos:

Para este campo...	Realice lo siguiente...
Nombre	<p>Escriba un nombre para el grupo de recursos.</p> <p>Nota: El nombre del grupo de recursos no debe superar los 250 caracteres.</p>
Etiquetas	<p>Escriba una o más etiquetas que más adelante le permitirán buscar el grupo de recursos.</p> <p>Por ejemplo, si añadió HR como etiqueta a varios grupos de recursos, más adelante encontrará todos los grupos de recursos asociados usando esa etiqueta.</p>
Utilice un formato de nombre personalizado para la copia de Snapshot	<p>Marque esta casilla de comprobación e introduzca un formato de nombre personalizado que desee usar para el nombre de Snapshot.</p> <p>Por ejemplo, <i>customtext_resource_group_policy_hostname</i> o <i>resource_group_hostname</i>. De forma predeterminada, se añade una fecha/hora al nombre de la Snapshot.</p>

4. Opcional: En la página Recursos, seleccione un nombre de host de la lista desplegable **Host** y el tipo de recurso de la lista desplegable **Tipo de recurso**.

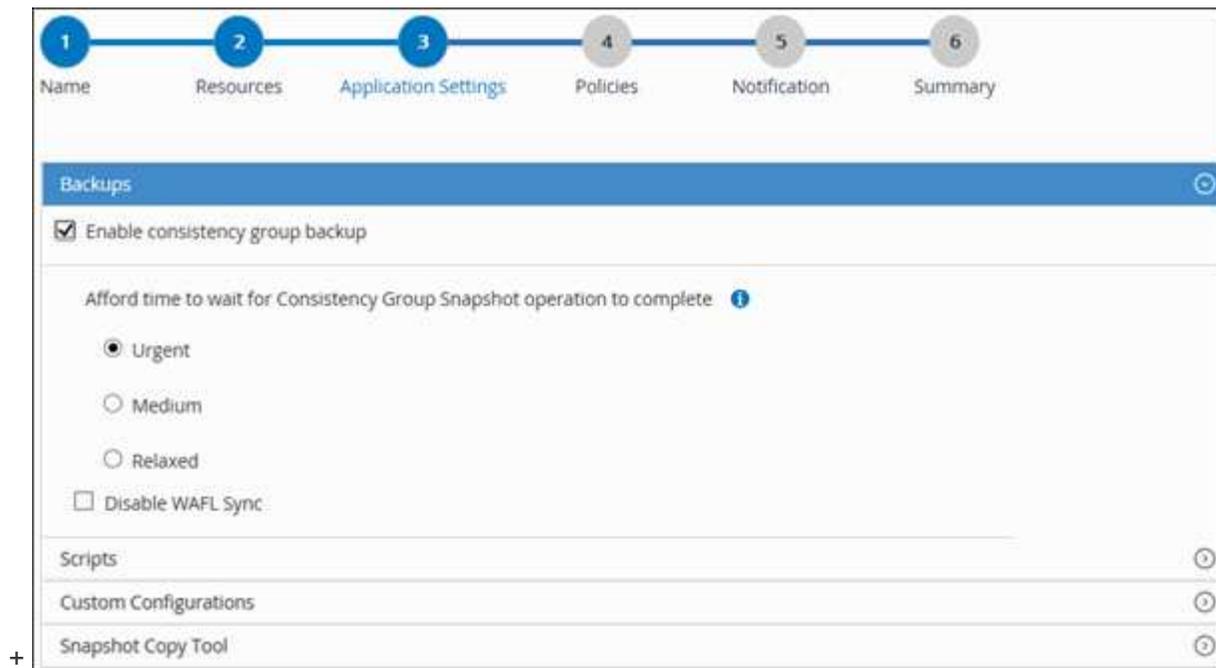
Esto permite filtrar información en la pantalla.

5. Seleccione los recursos de la sección **Recursos disponibles** y, a continuación, seleccione la flecha derecha para moverlos a la sección **Recursos seleccionados**.
6. Opcional: En la página **Configuración de la aplicación**, haga lo siguiente:

- a. Seleccione la flecha Backups para establecer las opciones de backup adicionales.

Habilite el backup del grupo de consistencia y realice las siguientes tareas:

Para este campo...	Realice lo siguiente...
Permitir que se complete la operación de snapshot del grupo de consistencia	<p>Seleccione Urgent, Medium o Relaxed para especificar el tiempo de espera hasta completar la operación de Snapshot.</p> <p>Urgent = 5 segundos, Medium = 7 segundos y Relaxed = 20 segundos.</p>
Deshabilite la sincronización WAFL	<p>Seleccione este campo para evitar forzar un punto de coherencia de WAFL.</p>



- 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 la flecha Custom Configurations y utilice este recurso para escribir los pares personalizados clave-valor requeridos en todas las operaciones de protección de datos.

Parámetro	Ajuste	Descripción
ARCHIVE_LOG_ENABLE	(S/N)	Permite la gestión del registro de archivos para eliminar los registros de archivos.
RETENCIÓN_LOG_ARCHIVO	número_de_días	Especifica la cantidad de días que se conservan los registros de archivo. Este valor debe ser igual o mayor que las RETENTIONS NTAP_SNAPSHOT_.
ARCHIVE_LOG_DIR	change_info_directory/logs	Especifica la ruta de acceso al directorio que contiene los registros de archivo.

Parámetro	Ajuste	Descripción
ARCHIVO_LOG_EXT	extensión_archivo	Especifica la longitud de la extensión del archivo de registro de archivos. Por ejemplo, si el registro de archivos es log_backup_0_0_0_0.161518551942 9 y si el valor file_extension es 5, la extensión del registro conservará 5 dígitos, que son 16151.
ARCO ARCHIVE_LOG_RECURSIVE_SE	(S/N)	Permite la gestión de registros de ficheros en subdirectorios. Debe utilizar este parámetro si los registros de archivo se encuentran en subdirectorios.

- c. Seleccione la flecha * Herramienta de copia de instantáneas * para seleccionar la herramienta para crear instantáneas:

Si desea que...	Realice lo siguiente...
SnapCenter utilice el plugin para Windows y coloque el sistema de archivos en estado coherente antes de crear una Snapshot. En el caso de recursos de Linux, esta opción no es aplicable.	Seleccione SnapCenter with File System Consistency . Esta opción no es aplicable para el plugin de SnapCenter para la base de datos SAP HANA.
SnapCenter creará una snapshot a nivel del almacenamiento	Seleccione SnapCenter sin coherencia del sistema de archivos .
Se escriba el comando que se ejecutará en el host a fin de crear snapshots.	Seleccione Otro y, a continuación, introduzca el comando que se ejecutará en el host para crear una instantánea.

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

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



También puede crear una política seleccionando .

Las directivas se enumeran en la sección **Configurar horarios para directivas seleccionadas**.

- b. En la columna **Configure Schedules**, seleccione para la directiva que desea configurar.
- c. En el cuadro de diálogo Add schedules for policy *policy_name*, configure la programación y seleccione

OK.

Donde `policy_name` es el nombre de la política 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 lista desplegable **Preferencias de correo** de la página **Notificación**, selecciona los escenarios en los que deseas enviar los correos electrónicos.

También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. El servidor SMTP debe configurarse en **Ajustes > Ajustes globales**.

9. Revisa el resumen y luego selecciona **Finalizar**.

Crear una conexión del sistema de almacenamiento y una credencial mediante cmdlets de PowerShell

Debe crear una conexión de máquina virtual de almacenamiento (SVM) y una credencial antes de usar los cmdlets de PowerShell para realizar operaciones de protección de datos.

Antes de empezar

- Debe haber preparado el entorno de PowerShell para ejecutar los cmdlets de PowerShell.
- Debe tener los permisos necesarios en el rol de administrador de infraestructura para crear conexiones de almacenamiento.
- Debe asegurarse de que no se encuentren en curso las instalaciones de plugins.

No debe haber instalaciones de complementos de host en curso al añadir una conexión a sistemas de almacenamiento, ya que puede que la caché del host no se actualice y que el estado de las bases de datos pueda aparecer en la interfaz gráfica de usuario de SnapCenter como «'no disponible para el backup' o «'no en el almacenamiento de NetApp'».

- Los nombres de los sistemas de almacenamiento deben ser únicos.

SnapCenter no admite varios sistemas de almacenamiento con el mismo nombre en clústeres diferentes. Cada uno de los sistemas de almacenamiento que admite SnapCenter debe tener un nombre único y una dirección IP de LIF de gestión única.

Pasos

1. Inicie una sesión de conexión de PowerShell Core mediante el cmdlet `Open-SmConnection`.

En este ejemplo, se abre una sesión de PowerShell:

```
PS C:\> Open-SmConnection
```

2. Cree una nueva conexión con el sistema de almacenamiento mediante el cmdlet `Add-SmStorageConnection`.

En este ejemplo, se crea una nueva conexión con el sistema de almacenamiento:

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https  
-Timeout 60
```

3. Cree una credencial nueva mediante el cmdlet Add-SmCredential.

En este ejemplo, se crea una nueva credencial llamada FinanceAdmin con las credenciales de Windows:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

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"](#).

Realizar backup de los recursos de plugins compatibles con NetApp individuales

Si un recurso individual de plugins compatibles con NetApp no forma parte de ningún grupo de recursos, puede incluirlo en el backup mediante la página Resources. Puede realizar el backup del recurso bajo demanda, o bien, si el recurso tiene una política anexada y una programación configurada, el backup se realiza automáticamente según esa programación.

Antes de empezar

- Debe tener creada una política de backup.
- Si desea realizar un backup de un recurso que tenga una relación de SnapMirror con un almacenamiento secundario, la función ONTAP asignada al usuario de almacenamiento debería incluir el privilegio «snapmirror all». Sin embargo, si usted está utilizando el rol "vsadmin", entonces no se requiere el privilegio "napmirror all".

UI de 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 Resources, filtre los recursos de la lista desplegable **View** en función del tipo de recurso.

Haga clic en , a continuación, seleccione el nombre de host y el tipo de recurso para filtrar los recursos. A continuación, puede hacer clic en  para cerrar el panel de filtros.

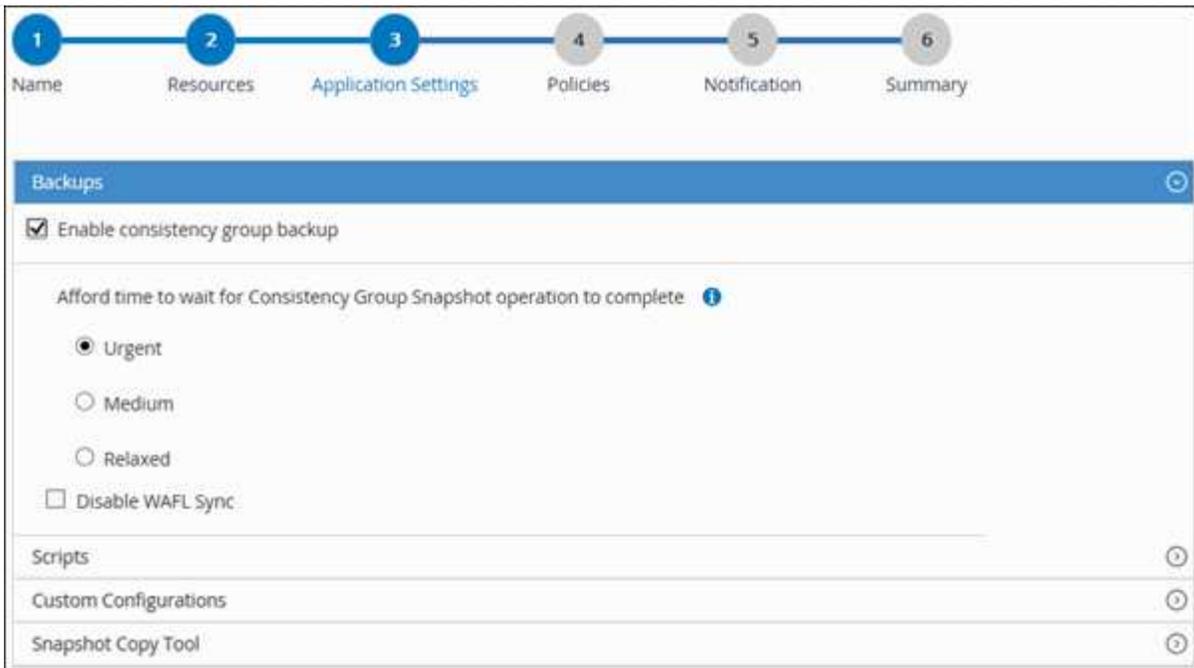
3. Haga clic en el recurso que desea incluir en el backup.
4. En la página Recurso, si desea utilizar un nombre personalizado, active la casilla de verificación **Use custom name format for Snapshot copy** y, a continuación, introduzca un formato de nombre personalizado para el nombre de la instantánea.

Por ejemplo, *customtext_policy_hostname* o *resource_hostname*. De forma predeterminada, se añade una fecha/hora al nombre de la Snapshot.

5. En la página Application Settings, realice lo siguiente:
 - a. Haga clic en la flecha **copias de seguridad** para establecer las opciones de copia de seguridad adicionales:

Habilite el backup del grupo de consistencia y, si es necesario, realice las siguientes tareas:

Para este campo...	Realice lo siguiente...
Permitir que se complete la operación de snapshot del grupo de consistencia	Seleccione Urgent, Medium o Relaxed para especificar el tiempo de espera hasta completar la operación de Snapshot. Urgent = 5 segundos, Medium = 7 segundos y Relaxed = 20 segundos.
Deshabilite la sincronización WAFL	Seleccione este campo para evitar forzar un punto de coherencia de WAFL.



- a. Haga clic en la flecha **Scripts** para ejecutar los comandos PRE y POST para las operaciones de inactividad, instantánea y desactivación. También puede ejecutar los comandos previos antes de salir de la operación de backup.

Los scripts previos y posteriores se ejecutan en el servidor de SnapCenter.

- b. Haga clic en la flecha **configuraciones personalizadas** y, a continuación, introduzca los pares de valores personalizados necesarios para todos los trabajos que utilicen este recurso.
- c. Haga clic en la flecha * Herramienta de copia de instantáneas * para seleccionar la herramienta para crear instantáneas:

Si desea que...	Realice lo siguiente...
SnapCenter tomará una snapshot en el nivel del almacenamiento	Seleccione SnapCenter sin coherencia del sistema de archivos .
SnapCenter utilice el plugin para Windows y coloque el sistema de archivos en estado coherente para luego crear una copia Snapshot	Seleccione SnapCenter with File System Consistency .
Para escribir el comando para crear una snapshot	Seleccione Otro y luego ingrese el comando para crear una instantánea.

6. 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 el cuadro de diálogo Agregar programas para la directiva *policy_name* , configure la programación y, a continuación, haga clic en **Aceptar**.

Donde, *policy_name* es el nombre de la directiva seleccionada.

Las programaciones configuradas figuran en la columna Applied Schedules.

7. 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. SMTP también debe configurarse en **Ajustes > Ajustes globales**.

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

Se muestra la página de topología de los recursos.

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

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

a. Si ha aplicado varias políticas al recurso, en la lista desplegable **Política**, seleccione la directiva que desea utilizar para la copia de seguridad.

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**.

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

Cmdlets de PowerShell

Pasos

1. Inicie una sesión de conexión con el servidor de SnapCenter para el usuario especificado mediante el cmdlet de Open-SmConnection.

```
Open-smconnection -SMSbaseurl  
https:\\snapctr.demo.netapp.com:8146\
```

Se muestra una solicitud de nombre de usuario y contraseña.

2. Añada los recursos mediante el cmdlet Add-SmResources.

En este ejemplo, se añaden recursos:

```
Add-SmResource -HostName 'scc55.sscore.test.com' -PluginCode
'DummyPlugin' -ResourceName QDBVOL1 -ResourceType Database
-StorageFootPrint (
@{"VolumeName"="qtree_voll_scc55_sscore_test_com";"QTREE_NAME"="qtree
Voll";"StorageSystem"="vserver_scauto_primary"}) -Instance QTREE1
```

3. Cree una política de backup mediante el cmdlet Add-SmPolicy.

En este ejemplo, se crea una nueva política de backup:

```
Add-SMPolicy -PolicyName 'test2' -PolicyType 'Backup'
-PluginPolicyType DummyPlugin -description 'testPolicy'
```

4. Añada un nuevo grupo de recursos a SnapCenter mediante el cmdlet Add-SmResourceGroup.

En este ejemplo, se crea un nuevo grupo de recursos con la política y los recursos especificados:

```
Add-SmResourceGroup -ResourceGroupName
'Verify_Backup_on_Multiple_Qtree_different_vserver_windows'
-Resources
@(@{"Host"="scc55.sscore.test.com";"Uid"="QTREE2";"PluginName"="Dumm
yPlugin"},@{"Host"="scc55.sscore.test.com";"Uid"="QTREE";"PluginName
"="DummyPlugin"}) -Policies test2 -plugincode 'DummyPlugin'
-usesnapcenterwithoutfilesystemconsistency
```

5. Para iniciar una tarea de backup se usa el cmdlet New-SmBackup.

```
New-SMBackup -DatasetName
Verify_Backup_on_Multiple_Qtree_different_vserver_windows -Policy
test2
```

6. Consulte el estado del trabajo de backup mediante el cmdlet Get-SmBackupReport.

Este ejemplo muestra un informe con un resumen de todos los trabajos realizados en la fecha especificada:

```

Get-SmBackupReport -JobId 149

BackedUpObjects      : {QTREE2, QTREE}
FailedObjects        : {}
IsScheduled           : False
HasMetadata           : False
SmBackupId           : 1
SmJobId              : 149
StartDateTime         : 1/15/2024 1:35:17 AM
EndDateTime          : 1/15/2024 1:36:19 AM
Duration              : 00:01:02.4265750
CreatedDateTime       : 1/15/2024 1:35:51 AM
Status                : Completed
ProtectionGroupName  :
Verify_Backup_on_Multiple_Qtree_different_vserver_windows
SmProtectionGroupId  : 1
PolicyName            : test2
SmPolicyId            : 4
BackupName            :
Verify_Backup_on_Multiple_Qtree_different_vserver_windows_scc55_01-
15-2024_01.35.17.4467
VerificationStatus    : NotApplicable
VerificationStatuses :
SmJobError            :
BackupType            : SCC_BACKUP
CatalogingStatus      : NotApplicable
CatalogingStatuses   :
ReportDataCreatedDateTime :
PluginCode            : SCC
PluginName            : DummyPlugin
PluginDisplayName     : DummyPlugin
JobTypeId             :
JobHost               : scc55.sscore.test.com

```

Realizar backup de grupos de recursos de plugins admitidos por NetApp

Puede realizar un backup del grupo de recursos bajo demanda en la página Resources. Si un grupo de recursos tiene una política anexada y una programación configurada, los backups se realizan automáticamente según esa programación.

Antes de empezar

- Debe tener creado un grupo de recursos con una política anexada.
- Si desea realizar un backup de un recurso que tenga una relación de SnapMirror con un almacenamiento secundario, la función ONTAP asignada al usuario de almacenamiento debería incluir el privilegio «incluir

toda la copia reflejada». Sin embargo, si usted está utilizando el rol "vsadmin", entonces no se requiere el privilegio "nnapmirror all".

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 **Resource Group** en la lista **View**.

Se puede buscar el grupo de recursos ingresando su nombre en el cuadro de búsqueda o haciendo clic en  y seleccionando la etiqueta. A continuación, puede hacer clic en  para cerrar el panel de filtros.

3. En la página Resource Groups, seleccione el grupo de recursos que desea incluir en un backup y, a continuación, haga clic en **Back up Now**.

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

- a. Si asoció varias políticas al grupo de recursos, en la lista desplegable **Policy**, seleccione la política que desea usar para la copia de seguridad.

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**.

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

- En las configuraciones de MetroCluster, es posible que SnapCenter no pueda detectar una relación de protección tras una conmutación por error.

["No es posible detectar la relación de SnapMirror o SnapVault tras un fallo en MetroCluster"](#)

- Si va a realizar el backup de datos de aplicación en VMDK y el tamaño de pila de Java para el plugin de SnapCenter para VMware vSphere no es suficientemente grande, se puede producir un error en el backup. Para aumentar el tamaño de pila de Java, busque el archivo de script `/opt/netapp/init_scripts/scvservice`. En ese script, la `do_start method Command` inicia el servicio de plugin de VMware de SnapCenter. Actualice este comando a lo siguiente: `Java -jar -Xmx8192M -Xms4096M`.

Supervise operaciones de backup de recursos de plugins compatibles con NetApp

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.

Cancelar las operaciones de backup de los plugins compatibles con NetApp

Es posible cancelar las operaciones de backup que se encuentran en cola.

Lo que necesitará

- Debe iniciar sesión como administrador de SnapCenter o propietario del trabajo para cancelar las operaciones.
- Puede cancelar una operación de copia de seguridad desde la página **Monitor** o el panel **Activity**.
- No es posible cancelar una operación de backup en ejecución.
- Es posible utilizar la interfaz gráfica de usuario de SnapCenter, los cmdlets de PowerShell o los comandos de la CLI para cancelar las operaciones de backup.
- El botón **Cancelar trabajo** está desactivado para operaciones que no se pueden cancelar.
- Si seleccionó **todos los miembros de esta función pueden ver y operar en otros objetos de miembros** en la página usuarios/grupos mientras crea una función, puede cancelar las operaciones de copia de seguridad en cola de otros miembros mientras utiliza esa función.
- Pasos*
 1. Ejecute una de las siguientes acciones:

Del...	Acción
Página Monitor	<ol style="list-style-type: none"> En el panel de navegación izquierdo, haga clic en Monitor > Jobs. Seleccione la operación y, a continuación, haga clic en Cancelar trabajo.
Panel de actividades	<ol style="list-style-type: none"> Tras iniciar la operación de backup, haga clic en  En el panel Activity para ver las cinco operaciones más recientes. Seleccione la operación. En la página Detalles del trabajo, haga clic en Cancelar trabajo.

Se cancela la operación y el recurso se revierte al estado anterior.

Ver los clones y backups relacionados con los recursos de plugins admitidos en NetApp en la página Topology

Al prepararse para clonar un recurso o incluirlo en un backup, puede resultar útil ver una representación gráfica de todos los backups y clones del almacenamiento principal y secundario. En la página Topology, es posible ver todos los backups y clones que están disponibles para el recurso o el grupo de recursos seleccionado. Pueden verse los detalles de estos backups y clones, y luego seleccionarlos para realizar operaciones de protección de datos.

Acerca de esta tarea

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

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 con el resumen 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 de actualización, se inicia una consulta del almacenamiento para ver un número 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 recurso de la aplicación se distribuya entre varios volúmenes, el tiempo de caducidad de SnapLock para el 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.

Después de la copia de seguridad a petición, haciendo clic en el botón **Actualizar** actualiza los detalles de la copia de seguridad o clonación.

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 en la tabla y haga clic en los iconos de protección de datos para realizar operaciones de restauración, clonado, cambio de nombre y eliminación.



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



Los backups que figuran en el sistema de almacenamiento principal no pueden cambiar de nombre.

7. Si desea eliminar un clon, selecciónelo en la tabla y haga clic en  para eliminar el clon.

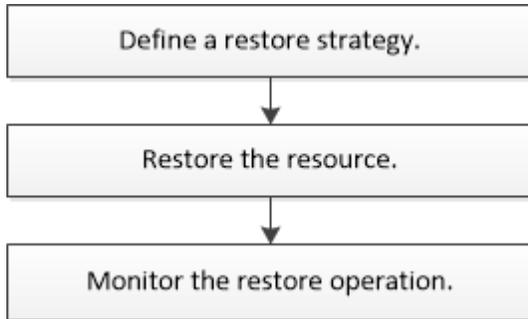
Restaurar recursos de plugins compatibles con NetApp

Restaurar recursos de plugins admitidos por NetApp

El flujo de trabajo de restauración y recuperación incluye planificar, realizar las operaciones de restauración y supervisarlas.

Acerca de esta tarea

El siguiente flujo de trabajo muestra la secuencia que debe seguirse para realizar la operación de restauración:



También puede usar los cmdlets de PowerShell manualmente o en scripts para realizar operaciones de backup, restauración y clonado. Para obtener información sobre los cmdlets de PowerShell, use la ayuda de cmdlets de SnapCenter o consulte "[Guía de referencia de cmdlets de SnapCenter Software](#)".

Restaurar un backup de recursos

Es posible usar SnapCenter para restaurar recursos. Las capacidades de las operaciones de restauración dependen del plugin que se use.

Antes de empezar

- Debe tener un backup de los recursos o del grupo de recursos.
- El administrador de SnapCenter asignó SVM para los volúmenes de origen y los volúmenes de destino si va a replicar Snapshots a un reflejo o un almacén.
- Cancele la operación de backup que se encuentra en curso y que corresponde al recurso o grupo de recursos que desea restaurar.

Acerca de esta tarea

- La operación de restauración predeterminada solo restaura objetos del almacenamiento. Las operaciones de restauración en el nivel de la aplicación solo pueden realizarse si el plugin NetApp compatible incluye dicha capacidad.
- 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.

UI de 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 Resources, filtre los recursos de la lista desplegable **View** en función del tipo de recurso.

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



Aunque se puede realizar un backup del grupo de recursos, al restaurar, debe seleccionar los recursos individuales que restaurará.

Si el recurso no está protegido, se muestra *not protected* en la columna **Overall Status**.

El estado *not protected* en la columna **Overall Status** puede significar que el recurso no está protegido o que un usuario diferente hizo una copia de seguridad del recurso.

3. Seleccione el recurso, o bien seleccione un grupo de recursos y, a continuación, elija un recurso de ese grupo.

Se muestra la página con el resumen.

4. En la vista **Manage Copies**, seleccione **copias de seguridad** ya sea en los sistemas de almacenamiento primario o secundario (reflejado o en almacén).
5. En la tabla de backups primarios, seleccione el backup desde el cual quiere restaurar y, a continuación, haga clic en .



Backup Name	End Date
rg1_scscr0191683001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM

6. En la página Restore Scope, seleccione **Complete Resource** o **File Level**.
 - a. Si seleccionó **Complete Resource**, se restaura la copia de seguridad del recurso.

Si el recurso contiene volúmenes o qtrees como Storage Footprint, entonces los snapshots más recientes, como los volúmenes o qtrees, se eliminan y no pueden recuperarse. Además, si hay algún otro recurso alojado en los mismos volúmenes o qtrees, también se lo elimina.

- b. Si ha seleccionado **nivel de archivo**, puede seleccionar **todo** o seleccionar volúmenes o qtrees y, a continuación, introducir la ruta relacionada con los volúmenes o qtrees que se seleccionan separados por comas.
 - Puede seleccionar varios volúmenes y qtrees.
 - Si el tipo de recurso es LUN, se restaura el LUN completo. Puede seleccionar varios LUN. +
NOTA: Si selecciona **todo**, se restauran todos los archivos de los volúmenes, qtrees o LUN.

7. En la página **Pre OPS**, escriba los comandos previos a la restauración y los comandos de

desmontaje que se ejecutarán antes de realizar un trabajo de restauración.

8. En la página **Post OPS**, escriba los comandos Mount y post restore que se ejecutarán después de realizar un trabajo de restauración.
9. En la página **notificación**, en la lista desplegable **preferencia de correo electrónico**, 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. SMTP también debe configurarse en la página **Ajustes > Ajustes globales**.

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

Cmdlets de PowerShell

Pasos

1. Inicie una sesión de conexión con el servidor de SnapCenter para el usuario especificado mediante el cmdlet de Open-SmConnection.

```
PS C:\> Open-Smconnection
```

2. Para recuperar la información sobre los backups que desea restaurar, puede usar los cmdlets Get-SmBackup y Get-SmBackupReport.

Este ejemplo muestra información sobre todos los backups disponibles:

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015	11:02:32
AM	Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015	11:23:17
AM			

En este ejemplo, se muestra información detallada sobre el backup del 29 de enero de 2015 al 3 de febrero de 2015:

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId      : 113
SmJobId         : 2032
StartDateTime   : 2/2/2015 6:57:03 AM
EndDateTime     : 2/2/2015 6:57:11 AM
Duration        : 00:00:07.3060000
CreatedDateTime : 2/2/2015 6:57:23 AM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName      : Vault
SmPolicyId      : 18
BackupName      : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId      : 114
SmJobId         : 2183
StartDateTime   : 2/2/2015 1:02:41 PM
EndDateTime     : 2/2/2015 1:02:38 PM
Duration        : -00:00:03.2300000
CreatedDateTime : 2/2/2015 1:02:53 PM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName      : Vault
SmPolicyId      : 18
BackupName      : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Puede restaurar los datos del backup mediante el cmdlet `Restore-SmBackup`.

```

Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority            : None
Tasks               : {}
ParentJobID         : 0
EventId            : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName         :

```

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"](#).

Supervise operaciones de restauración de recursos de plugins compatibles con NetApp

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.

Backups de recursos de plugins admitidos por Clone NetApp

Backups de recursos de plugins admitidos por Clone NetApp

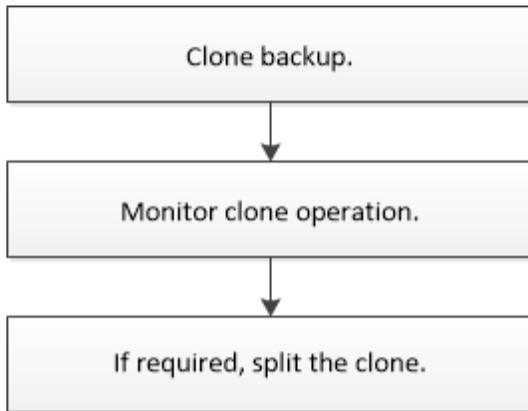
El flujo de trabajo de clonado incluye realizar la operación de clonado y supervisarla.

Acerca de esta tarea

Es posible clonar backups de recursos por los siguientes motivos:

- Para probar la funcionalidad que debe implementarse mediante la estructura de recursos actuales y el contenido durante los ciclos de desarrollo de aplicaciones
- Para herramientas de manipulación y extracción de datos cuando se rellenan almacenes de datos
- Para recuperar datos que se eliminaron o se modificaron por error

Los siguientes flujos de trabajo muestran la secuencia que debe seguirse para realizar la operación de clonado:



También puede usar los cmdlets de PowerShell manualmente o en scripts para realizar operaciones de backup, restauración y clonado. Para obtener información detallada sobre los cmdlets de PowerShell, use la ayuda de cmdlets de SnapCenter o consulte ["Guía de referencia de cmdlets de SnapCenter Software"](#).

Clonar desde un backup

Es posible usar SnapCenter para clonar un backup. Es posible clonar desde un backup primario o secundario. Las capacidades de las operaciones de clonado dependen del plugin que se use.

Antes de empezar

- Debe tener un backup de los recursos o del grupo de recursos.
- La operación de clonado predeterminada solo clona objetos del almacenamiento. Las operaciones de clonado en el nivel de la aplicación solo pueden realizarse si el plugin NetApp compatible incluye dicha capacidad.
- Debe asegurarse de que los agregados donde se alojan los volúmenes deben estar en la lista de agregados asignados de la máquina virtual de almacenamiento (SVM).

Acerca de esta tarea

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.

UI de 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**, filtre los recursos de la lista desplegable **Ver** en función del tipo de recurso.

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

3. Seleccione el recurso o el grupo de recursos.

Debe seleccionar un recurso para seleccionar un grupo de recursos.

Se muestra la página con el resumen o grupo de recursos.

4. En la vista Manage Copies, seleccione **copias de seguridad** ya sea en los sistemas de almacenamiento primario o secundario (reflejado o en almacén).

5. Seleccione el backup de datos de la tabla y haga clic en .

6. En la página Locations, realice lo siguiente:

Para este campo...	Realice lo siguiente...
Clone el servidor	<p>De forma predeterminada, se llena el host de origen.</p> <p>Si desea especificar otro host, seleccione el host donde debe montarse el clon y donde esté instalado el plugin.</p>
Sufijo de clon	<p>Es obligatorio cuando el destino y el origen del clon son iguales.</p> <p>Escriba un sufijo que se anexará al nombre del recurso recién clonado. El sufijo garantiza que el recurso clonado sea único en el host.</p> <p>Por ejemplo, rs1_clone. Si clona en el mismo host que el recurso original, debe proporcionar un sufijo para diferenciar el recurso clonado del original; de lo contrario, se producirá un error en la operación.</p>

Si el recurso seleccionado es un LUN y se está clonando a partir de un backup secundario, se muestran los volúmenes de destino. Un único origen puede tener varios volúmenes de destino.

7. En la página **Configuración**, realice lo siguiente:

Para este campo...	Realice lo siguiente...
Nombre del iniciador	Escriba el nombre del iniciador del host, que es IQDN o WWPN.
Protocolo de iGroup	Seleccione el protocolo de iGroup.



La página Settings se muestra solo si el tipo de almacenamiento es un LUN.

- En la página Scripts, escriba los comandos previos o posteriores a la clonado que deben ejecutarse, respectivamente, antes o después de la operación de clonado. Escriba el comando de montaje para montar un sistema de archivos en un host.

Por ejemplo:

- Comando previo a la clonado: Elimine las bases de datos existentes con el mismo nombre
- Comando posterior a la clonado: Verifique o inicie una base de datos.

Comando de montaje para un volumen o qtree en una máquina Linux: Lcódigo
 <VSERVER_NAME>:%<VOLUME_NAME_Clone /mnt>

- En la página **notificación**, en la lista desplegable **preferencia de correo electrónico**, 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.

- Revise el resumen y haga clic en **Finalizar**.
- Supervise el progreso de la operación haciendo clic en **Monitor > Jobs**.

Cmdlets de PowerShell

Pasos

- Inicie una sesión de conexión con el servidor de SnapCenter para el usuario especificado mediante el cmdlet de Open-SmConnection.

```
Open-SmConnection -SMSbaseurl
https:\\snapctr.demo.netapp.com:8146/
```

- Enumere los backups que pueden clonarse mediante el cmdlet Get-SmBackup o Get-SmResourceGroup.

Este ejemplo muestra información sobre todos los backups disponibles:

```
C:\PS>PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM	

En este ejemplo, se muestra información sobre un grupo de recursos especificado:

```
PS C:\> Get-SmResourceGroup
```

```
Description :  
CreationTime : 10/10/2016 4:45:53 PM  
ModificationTime : 10/10/2016 4:45:53 PM  
EnableEmail : False  
EmailSMTPServer :  
EmailFrom :  
EmailTo :  
EmailSubject :  
EnableSysLog : False  
ProtectionGroupType : Backup  
EnableAsupOnFailure : False  
Policies : {}  
HostResourceMapping : {}  
Configuration :  
SMCoreContracts.SmCloneConfiguration  
LastBackupStatus : Completed  
VerificationServer :  
EmailBody :  
EmailNotificationPreference : Never  
VerificationServerInfo :  
SchedulerSQLInstance :  
CustomText :  
CustomSnapshotFormat :  
SearchResources : False  
ByPassCredential : False  
IsCustomSnapshot :  
MaintenanceStatus : Production  
PluginProtectionGroupTypes : {SMSQL}  
Tag :  
IsInternal : False
```

```

EnableEmailAttachment      : False
VerificationSettings       : {}
Name                       : NFS_DB
Type                       : Group
Id                         : 2
Host                       :
UserName                   :
Passphrase                 :
Deleted                    : False
Auth                       : SMCoreContracts.SmAuth
IsClone                    : False
CloneLevel                 : 0
Hosts                      :
StorageName                :
ResourceGroupNames        :
PolicyNames                :

Description                 :
CreationTime                : 10/10/2016 4:51:36 PM
ModificationTime           : 10/10/2016 5:27:57 PM
EnableEmail                : False
EmailSMTPServer            :
EmailFrom                  :
EmailTo                    :
EmailSubject               :
EnableSysLog                : False
ProtectionGroupType        : Backup
EnableAsupOnFailure        : False
Policies                   : {}
HostResourceMapping        : {}
Configuration              :
SMCoreContracts.SmCloneConfiguration
LastBackupStatus           : Failed
VerificationServer         :
EmailBody                  :
EmailNotificationPreference : Never
VerificationServerInfo     :
SchedulerSQLInstance       :
CustomText                  :
CustomSnapshotFormat       :
SearchResources            : False
ByPassRunAs                : False
IsCustomSnapshot           :
MaintenanceStatus          : Production
PluginProtectionGroupTypes : {SMSQL}
Tag                        :

```

```

IsInternal           : False
EnableEmailAttachment : False
VerificationSettings : {}
Name                 : Test
Type                 : Group
Id                   : 3
Host                 :
UserName             :
Passphrase           :
Deleted              : False
Auth                 : SMCoreContracts.SmAuth
IsClone              : False
CloneLevel           : 0
Hosts                 :
StorageName          :
ResourceGroupNames   :
PolicyNames          :

```

3. Inicie una operación de clonado de un grupo de recursos de clonado o un backup existente con el cmdlet `New-SmClone`.

En este ejemplo, se crea un clon a partir de un determinado backup con todos los registros:

```

New-SmClone -BackupName
Verify_delete_clone_on_qtree_windows_scc54_10-04-2016_19.05.48.0886
-Resources @{"Host"="scc54.sccore.test.com";"Uid"="QTREE1"} -
CloneToInstance scc54.sccore.test.com -Suffix '_QtreeCloneWin9'
-AutoAssignMountPoint -AppPluginCode 'DummyPlugin' -initiatorname
'iqn.1991-
05.com.microsoft:scc54.sccore.test.com' -igroupprotocol 'mixed'

```

4. Puede consultar el estado del trabajo de clonado mediante el cmdlet `Get-SmCloneReport`.

En este ejemplo, se muestra un informe de clonado con el correspondiente ID de trabajo:

```

PS C:\> Get-SmCloneReport -JobId 186

SmCloneId           : 1
SmJobId             : 186
StartDateTime       : 8/3/2015 2:43:02 PM
EndDateTime         : 8/3/2015 2:44:08 PM
Duration            : 00:01:06.6760000
Status              : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName          : OnDemand_Clone
SmPolicyId          : 4
BackupPolicyName    : OnDemand_Full_Log
SmBackupPolicyId    : 1
CloneHostName       : SCSPR0054212005.mycompany.com
CloneHostId         : 4
CloneName           : Draper__clone__08-03-2015_14.43.53
SourceResources     : {Don, Betty, Bobby, Sally}
ClonedResources     : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
SmJobError          :

```

Supervisar operaciones de clonado de recursos de plugins admitidas por NetApp

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 © 2024 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.