Obtenga más información sobre el software SnapCenter

SnapCenter software

NetApp
January 09, 2026

Tabla de contenidos

Obtenga más información sobre el software SnapCenter

Información general de SnapCenter

El SnapCenter software es una plataforma simple, centralizada y escalable para la protección de datos consistente con todas las aplicaciones. Protege aplicaciones, bases de datos, sistemas de archivos de host y máquinas virtuales en sistemas ONTAP en la nube híbrida.

SnapCenter utiliza tecnologías NetApp Snapshot, SnapRestore, FlexClone, SnapMirror y SnapVault para proporcionar:

- Backup a disco rápido, con gestión eficiente del espacio y consistente con las aplicaciones
- Restauración rápida y detallada, y recuperación consistente con la aplicación
- Clonado rápido y con un uso eficiente del espacio

SnapCenter incluye SnapCenter Server y complementos livianos. Puede automatizar la implementación de complementos en hosts de aplicaciones remotas, programar operaciones de respaldo, verificación y clonación, y monitorear operaciones de protección de datos.

Puede instalar SnapCenter en sus instalaciones o en una nube pública para proteger los datos.

- En las instalaciones para proteger lo siguiente:
  - Datos en sistemas principales ONTAP FAS, AFF o ASA replicados a sistemas secundarios ONTAP FAS, AFF o ASA
  - Datos en sistemas principales ONTAP Select
  - Datos en sistemas principales y secundarios de ONTAP FAS, AFF o ASA, y protegidos en el almacenamiento de objetos local de StorageGRID
  - Datos en sistemas primarios y secundarios de ONTAP ASA R2
- Local en una nube híbrida para proteger lo siguiente:
  - Datos en sistemas principales ONTAP FAS, AFF o ASA replicados a Cloud Volumes ONTAP
  - Datos que se encuentran en sistemas primarios y secundarios de ONTAP FAS, AFF o ASA y están protegidos en el almacenamiento de objetos y archivos en la nube mediante la integración de respaldo y recuperación de NetApp
- En un cloud público para proteger lo siguiente:
  - Datos sobre sistemas principales de Cloud Volumes ONTAP (antes ONTAP Cloud)
  - Datos en Amazon FSX para ONTAP
  - Datos principales en Azure NetApp Files (Oracle, Microsoft SQL y SAP HANA)

Principales características

SnapCenter ofrece las siguientes funciones clave:

- Protección de datos centralizada y coherente con las aplicaciones de diferentes aplicaciones

La protección de datos es compatible con Microsoft Exchange Server, Microsoft SQL Server, bases de datos de Oracle en Linux o AIX, base de datos SAP HANA, IBM DB2, PostgreSQL, MySQL y sistemas de archivos host de Windows que se ejecutan en sistemas ONTAP. SnapCenter también admite la protección de aplicaciones como MongoDB, Storage, MaxDB, Sybase ASE, ORASCPM.

- Backups basados en normativas

  Las copias de seguridad basadas en políticas aprovechan la tecnología Snapshot de NetApp para crear copias de seguridad basadas en disco, rápidas, eficientes en términos de espacio y consistentes con las aplicaciones. También puede configurar la protección automática de estas copias de seguridad en un almacenamiento secundario actualizando las relaciones de protección existentes.

- Copias de seguridad para múltiples recursos

  Puede realizar copias de seguridad de varios recursos (aplicaciones, bases de datos o sistemas de archivos de host) del mismo tipo a la vez utilizando los grupos de recursos de SnapCenter .

- Restauración y recuperación

  SnapCenter ofrece restauraciones rápidas y granulares de backups y recuperación basada en tiempo y coherente con las aplicaciones. Puede restaurar desde cualquier destino en el cloud híbrido.

- Clonado

  SnapCenter proporciona una clonación rápida, que ahorra espacio y es consistente con las aplicaciones. Puede clonar en cualquier destino en la nube híbrida.

- Interfaz gráfica de usuario para la gestión de un solo usuario

  SnapCenter proporciona una única interfaz para administrar copias de seguridad y clones en cualquier destino de nube híbrida.

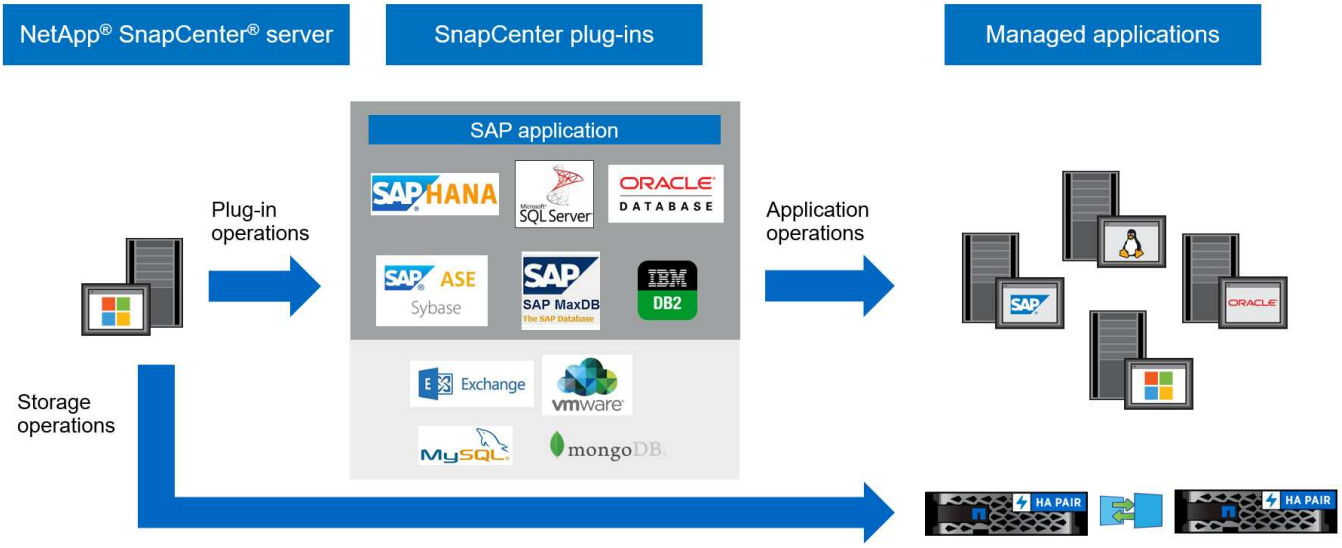
- API DE REST, cmdlets de Windows, comandos de UNIX

  SnapCenter proporciona API REST para la mayoría de las funcionalidades para la integración con cualquier software de orquestación, y el uso de cmdlets de Windows PowerShell y la interfaz de la línea de comandos.

- Consola e informes centralizados para la protección de datos
- Control de acceso basado en roles (RBAC) para seguridad y delegación
- Una base de datos de repositorio incorporada con alta disponibilidad para almacenar todos los metadatos de backup
- Instalación mediante inserción automatizada de plug-ins
- Alta disponibilidad
- Recuperación ante desastres (DR)
- SnapLock "Más información"
- SnapMirror, sincronización activa (lanzado inicialmente como SnapMirror Business Continuity [SM-BC])
- Mirroring sincrónico "Más información"

Arquitectura y componentes de SnapCenter

SnapCenter utiliza un diseño en capas con un servidor de administración central y hosts de complementos. Los hosts del servidor y del complemento pueden estar en ubicaciones diferentes.



SnapCenter incluye el servidor de SnapCenter, el paquete de plugins de SnapCenter para Windows y el paquete de plugins de SnapCenter para Linux. Cada paquete contiene complementos para distintas aplicaciones y componentes de la infraestructura.

Servidor SnapCenter

El servidor SnapCenter es compatible con los sistemas operativos Microsoft Windows y Linux (RHEL 8.x, RHEL 9.x, SLES 15 SP5). El servidor SnapCenter incluye un servidor web, una interfaz de usuario centralizada basada en HTML5, cmdlets de PowerShell, API DE REST y el repositorio de SnapCenter.

SnapCenter almacena información sobre sus operaciones en el repositorio de SnapCenter .

Plugins de SnapCenter

Cada plugin de SnapCenter admite entornos, bases de datos y aplicaciones específicas.

Nombre de complemento	Incluido en el paquete de instalación	Requiere otros plugins	Instalado en el host	Plataforma compatible
Plugin de SnapCenter para Microsoft SQL Server	Paquete de plugins para Windows	Plugin para Windows	Host SQL Server	Windows
Complemento de SnapCenter para Windows	Paquete de plugins para Windows		Host Windows	Windows

Nombre de complemento	Incluido en el paquete de instalación	Requiere otros plugins	Instalado en el host	Plataforma compatible
Plugin de SnapCenter para Microsoft Exchange Server	Paquete de plugins para Windows	Plugin para Windows	Host Exchange Server	Windows
Plugin de SnapCentre para base de datos de Oracle	Paquete de plugins para Linux y el paquete de plugins para AIX	Complemento para UNIX	Host Oracle	Linux o AIX
Plugin de SnapCenter para base de datos SAP HANA	Paquete de plugins para Linux y paquete de plugins para Windows	Plugin para UNIX o plugin para Windows	Host del cliente HDBSQL	Linux o Windows
Complemento de SnapCenter para IBM DB2	Paquete de plugins para Linux y paquete de plugins para Windows	Plugin para UNIX o plugin para Windows	DB2 host	Linux, AIX o Windows
Complemento de SnapCenter para PostgreSQL	Paquete de plugins para Linux y paquete de plugins para Windows	Plugin para UNIX o plugin para Windows	Host PostgreSQL	Linux o Windows
Plug-in de SnaoCenter para MySQL	Paquete de plugins para Linux y paquete de plugins para Windows	Plugin para UNIX o plugin para Windows	Host MySQL	Linux o Windows
Plugin de SnapCenter para MongoDB	Paquete de plugins para Linux y paquete de plugins para Windows	Plugin para UNIX o plugin para Windows	Host MongoDB	Linux o Windows
Complemento de SnapCenter para ORASCPM (Aplicaciones Oracle)	Paquete de plugins para Linux y paquete de plugins para Windows	Plugin para UNIX o plugin para Windows	Host Oracle	Linux o Windows
Complemento de SnapCenter para SAP ASE	Paquete de plugins para Linux y paquete de plugins para Windows	Plugin para UNIX o plugin para Windows	Host SAP	Linux o Windows

Nombre de complemento	Incluido en el paquete de instalación	Requiere otros plugins	Instalado en el host	Plataforma compatible
Complemento de SnapCenter para SAP MaxDB	Paquete de plugins para Linux y paquete de plugins para Windows	Plugin para UNIX o plugin para Windows	Host SAP MaxDB	Linux o Windows
Plugin de SnapCenter para plugin de almacenamiento	Paquete de plugins para Linux y paquete de plugins para Windows	Plugin para UNIX o plugin para Windows	Host de almacenamiento	Linux o Windows

El SnapCenter Plug-in for VMware vSphere admite operaciones de copia de seguridad y restauración consistentes con fallas y con máquinas virtuales para máquinas virtuales (VM), almacenes de datos y discos de máquinas virtuales (VMDK). También admite operaciones de copia de seguridad y restauración consistentes con la aplicación para bases de datos y sistemas de archivos virtualizados.

Para proteger bases de datos, sistemas de archivos, máquinas virtuales o almacenes de datos en máquinas virtuales, implemente el SnapCenter Plug-in for VMware vSphere . Para obtener información, consulte "Documentación del plugin de SnapCenter para VMware vSphere" .

Repositorio de SnapCenter

El repositorio de SnapCenter, que a veces se denomina base de datos NSM, almacena información y metadatos para cada operación SnapCenter.

La instalación de SnapCenter Server instala la base de datos del repositorio de MySQL Server de forma predeterminada. Si ya ha instalado MySQL Server y desea realizar una nueva instalación de SnapCenter Server, debe desinstalar MySQL Server.

SnapCenter admite MySQL Server 8.0.37 o posterior como base de datos del repositorio de SnapCenter . Si utiliza una versión anterior de MySQL Server con una versión anterior de SnapCenter, el proceso de actualización de SnapCenter actualiza MySQL Server a la versión 8.0.37 o posterior.

El repositorio de SnapCenter almacena la siguiente información y metadatos:

- Metadatos de backup, clonado, restauración y verificación
- Información sobre informes, trabajos y eventos
- Información sobre el host y los plugins
- Detalles de roles, usuarios y permisos
- Información de conexiones del sistema de almacenamiento

Funciones de seguridad de SnapCenter

SnapCenter emplea funciones de seguridad y autenticación estrictas para permitirle mantener seguros los datos.

SnapCenter incluye las siguientes funciones de seguridad:

- Toda la comunicación con SnapCenter utiliza HTTP sobre SSL (HTTPS).
- Todas las credenciales en SnapCenter están protegidas con el cifrado Advanced Encryption Standard (AES).
- Compatible con algoritmos de seguridad que cumplen con el estándar de procesamiento de información federal (FIPS).
- Admite el uso de certificados de CA autorizados proporcionados por el cliente.
- Admite Seguridad de la capa de transporte (TLS) 1,3 para la comunicación con ONTAP. También puede usar TLS 1,2 para la comunicación entre clientes y servidores.
- Admite un determinado conjunto de conjuntos de conjuntos de cifrado SSL para proporcionar seguridad a través de la comunicación de red. "Leer más".
- SnapCenter se instala dentro del firewall de su compañía para habilitar el acceso al servidor SnapCenter y permitir la comunicación entre SnapCenter Server y los plugins.
- El acceso a la API de SnapCenter y las operaciones utiliza tokens cifrados con el cifrado AES, que caducan luego de 24 horas.
- SnapCenter se integra con Windows Active Directory para el inicio de sesión y RBAC que rige los permisos de acceso.
- IPSec es compatible con SnapCenter en ONTAP para equipos host Windows y Linux. "Leer más".
- Los cmdlets de PowerShell de SnapCenter están protegidos por la sesión.
- Después de un período predeterminado de 15 minutos de inactividad, SnapCenter advierte que la sesión se cerrará en 5 minutos.

  Después de 20 minutos de inactividad, SnapCenter cierra la sesión, que debe volver a iniciarse. Es posible modificar el período de cierre de sesión por inactividad.
- El inicio de sesión se deshabilita temporalmente luego de 5 intentos incorrectos de inicio de sesión.
- Admite la autenticación de certificados de CA entre SnapCenter Server y ONTAP. "Leer más".
- Se añade el verificador de integridad al servidor de SnapCenter y a los plugins y valida todos los binarios enviados durante las operaciones de instalación y actualización nuevas.

Descripción general del certificado CA

El instalador de SnapCenter Server activa la compatibilidad centralizada con certificados SSL durante la instalación. Para mejorar la comunicación segura entre el servidor y el plugin, SnapCenter admite el uso de certificados de CA autorizados proporcionados por el cliente.

Debe implementar certificados de CA después de instalar SnapCenter Server y los respectivos plugins. Para obtener más información, consulte "Genere un archivo CSR de certificado de CA".

También puede implementar el certificado de CA para el plugin de SnapCenter para VMware vSphere. Para obtener más información, consulte "Crear e importar certificados".

Comunicación SSL bidireccional

La comunicación SSL bidireccional protege la comunicación mutua entre el servidor de SnapCenter y los plugins.

Descripción general de la autenticación basada en certificados

La autenticación basada en certificado verifica la autenticidad de los usuarios respectivos que intentan acceder al host del plugin de SnapCenter. El usuario debe exportar el certificado de servidor de SnapCenter sin clave privada e importarlo en el almacén de confianza del host del plugin. La autenticación basada en certificado solo funciona si la función SSL bidireccional está activada.

Autenticación multifactor (MFA)

La MFA usa un proveedor de identidades (IDP) de terceros a través del lenguaje de marcado de aserción de seguridad (SAML) para gestionar las sesiones de los usuarios. Esta funcionalidad mejora la seguridad de la autenticación al tener la opción de utilizar varios factores, como TOTP, biometría, notificaciones de inserción, etc. junto con el nombre de usuario y la contraseña existentes. Además, permite al cliente utilizar sus propios proveedores de identidades de usuario para obtener un inicio de sesión unificado (SSO) en toda su cartera.

La MFA solo se aplica a los inicios de sesión de la interfaz de usuario del servidor de SnapCenter. Los inicios de sesión se autentican a través de los servicios de Federación de Active Directory (AD FS) de IDP. Puede configurar varios factores de autenticación en AD FS. SnapCenter es el proveedor de servicios y debe configurar SnapCenter como parte de confianza en AD FS. Para habilitar la MFA en SnapCenter, necesitará los metadatos de AD FS.

Para obtener información sobre cómo habilitar la MFA, consulte "Active la autenticación multifactor".

Control de acceso basado en roles en SnapCenter

El control de acceso basado en roles (RBAC) de SnapCenter y los permisos de ONTAP permiten a los administradores de SnapCenter asignar acceso a recursos a usuarios o grupos. Este acceso administrado centralmente permite a los administradores de aplicaciones trabajar de forma segura dentro de entornos designados.

Debe crear o modificar roles y agregar acceso a recursos a los usuarios. Al configurar SnapCenter por primera vez, agregue usuarios o grupos de Active Directory a los roles y asigne recursos a esos usuarios o grupos.

SnapCenter no crea cuentas de usuarios o grupos. Crear cuentas de usuario o grupo en el Directorio Activo del sistema operativo o de la base de datos.

Tipos de RBAC en SnapCenter

SnapCenter admite los siguientes tipos de control de acceso basado en roles:

- RBAC de SnapCenter
- RBAC en el nivel de aplicaciones
- Control de acceso basado en roles del plugin de SnapCenter para VMware vSphere
- Permisos de ONTAP

RBAC de SnapCenter

SnapCenter tiene roles predefinidos y usted puede asignar usuarios o grupos a estos roles.

- SnapCenter Admin

- App Backup and Clone Admin
- Backup and Clone Viewer
- Infrastructure Admin

Cuando se asigna un rol a un usuario, SnapCenter muestra los trabajos que son relevantes para ese usuario en la página Trabajos, a menos que el usuario tenga el rol SnapCenterAdmin.

También es posible crear nuevos roles y gestionar los permisos y los usuarios. Es posible asignar permisos a usuarios o grupos para que tengan acceso a objetos de SnapCenter, como hosts, conexiones de almacenamiento y grupos de recursos.

Se pueden asignar permisos de RBAC a usuarios y grupos dentro del mismo bosque y a usuarios de distintos bosques. No es posible asignar permisos de RBAC a usuarios que pertenecen a grupos anidados en diferentes bosques.

> Al crear un rol personalizado, asegúrese de que incluya todos los permisos del rol SnapCenterAdmin. Si copia solo algunos permisos, SnapCenter le impedirá realizar todas las operaciones.

Los usuarios deben autenticarse al iniciar sesión a través de la interfaz de usuario o los cmdlets de PowerShell. Si los usuarios tienen varios roles, seleccionan un rol después de iniciar sesión. También se requiere autenticación para ejecutar API.

RBAC en el nivel de aplicaciones

SnapCenter usa credenciales para verificar que los usuarios de SnapCenter autorizados también tengan permisos en el nivel de aplicaciones.

Por ejemplo, para realizar operaciones de protección de datos en un entorno de SQL Server, configure las credenciales de Windows o SQL correctas. Si desea realizar operaciones de protección de datos en un entorno de sistema de archivos de Windows en el almacenamiento ONTAP , el rol de administrador de SnapCenter debe tener privilegios de administrador en el host de Windows.

De manera similar, si desea realizar operaciones de protección de datos en una base de datos Oracle y si la autenticación del sistema operativo (SO) está deshabilitada en el host de la base de datos, debe configurar las credenciales con la base de datos Oracle o las credenciales de Oracle ASM. El servidor SnapCenter autentica las credenciales establecidas utilizando uno de estos métodos según la operación.

Control de acceso basado en roles del plugin de SnapCenter para VMware vSphere

Cuando se utiliza el plugin de SnapCenter VMware para protección de datos coherente con máquinas virtuales, vCenter Server ofrece un nivel adicional de control de acceso basado en roles. El plugin de VMware de SnapCenter es compatible con el control de acceso basado en roles de vCenter Server y de ONTAP. "Más información"

NOTA: NetApp recomienda crear una función de ONTAP para las operaciones del SnapCenter Plug-in for VMware vSphere y asignarle todos los privilegios necesarios.

Permisos de ONTAP

Debe crear una cuenta vsadmin con los permisos necesarios para acceder al sistema de almacenamiento."Más información"

Permisos asignados a los roles predefinidos de SnapCenter

Cuando agrega un usuario a un rol, asigne el permiso StorageConnection para habilitar la comunicación de la máquina virtual de almacenamiento (SVM) o asigne una SVM al usuario para otorgarle permiso para usar la SVM. El permiso de Conexión de almacenamiento permite a los usuarios crear conexiones SVM.

Por ejemplo, un administrador de SnapCenter puede crear conexiones SVM y asignarlas a usuarios administradores de App Backup y Clone, quienes no pueden crear ni editar conexiones SVM. Sin una conexión SVM, los usuarios no pueden realizar operaciones de copia de seguridad, clonación o restauración.

SnapCenter Admin

El rol SnapCenter Admin tiene todos los permisos habilitados. No es posible modificar los permisos de este rol. Se pueden agregar usuarios y grupos al rol o quitarlos.

App Backup and Clone Admin

El rol App Backup and Clone Admin tiene los permisos necesarios para ejecutar acciones administrativas para tareas vinculadas con el backup y la clonado de aplicaciones. Este rol no tiene permisos para gestión de hosts, aprovisionamiento, gestión de conexiones de almacenamiento o instalación remota.

Permisos	Activado	Cree	Lea	Actualizar	Eliminar
Grupo de recursos	No aplicable	Sí	Sí	Sí	Sí
Política	No aplicable	Sí	Sí	Sí	Sí
Backup	No aplicable	Sí	Sí	Sí	Sí
Host	No aplicable	Sí	Sí	Sí	Sí
Conexión de almacenamiento	No aplicable	No	Sí	No	No
Clonar	No aplicable	Sí	Sí	Sí	Sí
Provisionamiento	No aplicable	No	Sí	No	No
Consola	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Leídos	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Restaurar	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Recurso	Sí	Sí	Sí	Sí	Sí

Permisos	Activado	Cree	Lea	Actualizar	Eliminar
Instalar/desinstalar plugins	No	No aplicable		No aplicable	No aplicable
Migración	No	No aplicable	No aplicable	No aplicable	No aplicable
Montaje	Sí	Sí	No aplicable	No aplicable	No aplicable
Desmontar	Sí	Sí	No aplicable	No aplicable	No aplicable
Restaurar volumen completo	No	No	No aplicable	No aplicable	No aplicable
Protección secundaria	No	No	No aplicable	No aplicable	No aplicable
Monitor de trabajos	Sí	No aplicable	No aplicable	No aplicable	No aplicable

Backup and Clone Viewer

La función Visor de copias de seguridad y clones tiene una vista de solo lectura de todos los permisos. Esta función también tiene permisos habilitados para descubrimiento, informes y acceso al Panel de Control.

Permisos	Activado	Cree	Lea	Actualizar	Eliminar
Grupo de recursos	No aplicable	No	Sí	No	No
Política	No aplicable	No	Sí	No	No
Backup	No aplicable	No	Sí	No	No
Host	No aplicable	No	Sí	No	No
Conexión de almacenamiento	No aplicable	No	Sí	No	No
Clonar	No aplicable	No	Sí	No	No
Provisionamiento	No aplicable	No	Sí	No	No
Consola	Sí	No aplicable	No aplicable	No aplicable	No aplicable

Permisos	Activado	Cree	Lea	Actualizar	Eliminar
Leídos	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Restaurar	No	No	No aplicable	No aplicable	No aplicable
Recurso	No	No	Sí	Sí	No
Instalar/desinstalar plugins	No	No aplicable	No aplicable	No aplicable	No aplicable
Migración	No	No aplicable	No aplicable	No aplicable	No aplicable
Montaje	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Desmontar	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Restaurar volumen completo	No	No aplicable	No aplicable	No aplicable	No aplicable
Protección secundaria	No	No aplicable	No aplicable	No aplicable	No aplicable
Monitor de trabajos	Sí	No aplicable	No aplicable	No aplicable	No aplicable

Infrastructure Admin

El rol Infrastructure Admin tiene permisos habilitados para gestión de hosts, administración del almacenamiento, aprovisionamiento, grupos de recursos, informes de instalación remota, Y acceso a la consola.

Permisos	Activado	Cree	Lea	Actualizar	Eliminar
Grupo de recursos	No aplicable	Sí	Sí	Sí	Sí
Política	No aplicable	No	Sí	Sí	Sí
Backup	No aplicable	Sí	Sí	Sí	Sí
Host	No aplicable	Sí	Sí	Sí	Sí
Conexión de almacenamiento	No aplicable	Sí	Sí	Sí	Sí

Permisos	Activado	Cree	Lea	Actualizar	Eliminar
Clonar	No aplicable	No	Sí	No	No
Provisionamiento	No aplicable	Sí	Sí	Sí	Sí
Consola	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Leídos	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Restaurar	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Recurso	Sí	Sí	Sí	Sí	Sí
Instalar/desinstalar plugins	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Migración	No	No aplicable	No aplicable	No aplicable	No aplicable
Montaje	No	No aplicable	No aplicable	No aplicable	No aplicable
Desmontar	No	No aplicable	No aplicable	No aplicable	No aplicable
Restaurar volumen completo	No	No	No aplicable	No aplicable	No aplicable
Protección secundaria	No	No	No aplicable	No aplicable	No aplicable
Monitor de trabajos	Sí	No aplicable	No aplicable	No aplicable	No aplicable

Recuperación ante desastres en SnapCenter

La función de recuperación ante desastres (DR) de SnapCenter le permite recuperarse de desastres como la corrupción de recursos o fallos del servidor. Esto ayuda a restaurar el repositorio de SnapCenter, las programaciones del servidor, los componentes de configuración y el plugin de SnapCenter para SQL Server y su almacenamiento.

En esta sección se explican los dos tipos de DR que hay en SnapCenter:

Recuperación ante desastres de servidores SnapCenter

- Se realiza una copia de seguridad de los datos del servidor de SnapCenter y se pueden recuperar sin que se añada ningún plugin al servidor de SnapCenter ni se gestione.

- El servidor SnapCenter secundario debe instalarse en el mismo directorio de instalación y en el mismo puerto que el servidor SnapCenter primario.
- En el caso de la autenticación multifactor (MFA), durante la recuperación ante desastres del servidor de SnapCenter, cierre todas las pestañas del explorador y vuelva a abrir un explorador para iniciar sesión de nuevo. Esto borrará las cookies de sesión existentes o activas y actualizará los datos de configuración correctos.
- La funcionalidad de recuperación ante desastres de SnapCenter utiliza la API de REST para realizar backups del servidor de SnapCenter. Consulte "Flujos de trabajo de API de REST para la recuperación ante desastres de SnapCenter Server".
- El archivo de configuración relacionado con la configuración de auditoría no se realiza un backup en el backup de recuperación ante desastres ni en el servidor de recuperación ante desastres después de la operación de restauración. Debe repetir manualmente la configuración del registro de auditoría.

Complemento SnapCenter y recuperación ante desastres de almacenamiento

La recuperación ante desastres solo está disponible para el plugin de SnapCenter para SQL Server. Si el plugin está inactivo, cambie a otro host de SQL y recupere los datos siguiendo unos pasos. Consulte "Recuperación ante desastres del plugin de SnapCenter para SQL Server".

SnapCenter usa ONTAP SnapMirror para replicar datos, que se pueden usar para la recuperación ante desastres manteniendo los datos sincronizados en un sitio secundario. Para iniciar la recuperación tras fallos, rompa la replicación de SnapMirror. Durante la conmutación de respaldo, invierta la sincronización para replicar los datos del sitio de recuperación de desastres de nuevo a la ubicación principal.

Licencias requeridas por SnapCenter

SnapCenter requiere varias licencias para permitir la protección de datos de aplicaciones, bases de datos, sistemas de archivos y máquinas virtuales. El tipo de licencia de SnapCenter que instale dependerá del entorno de almacenamiento y de las funciones que desee utilizar.

Licencia	Donde se la requiere
Basado en controladora estándar de SnapCenter	Requerido para FAS, AFF, ASA La licencia estándar de SnapCenter es una licencia basada en controladora y se incluye como parte de NetApp ONTAP One. Si tiene la licencia de conjunto de SnapManager, también obtendrá el derecho de licencia estándar de SnapCenter. Si desea instalar SnapCenter a modo de prueba con almacenamiento FAS, AFF o ASA, puede obtener una licencia de evaluación de NetApp ONTAP One poniéndose en contacto con el representante de ventas. Para obtener información sobre las licencias incluidas con NetApp ONTAP One, consulte "Licencias incluidas con NetApp ONTAP One" . SnapCenter también se ofrece como parte del paquete de protección de datos. Si ha adquirido el A400 o una versión posterior, debe comprar el paquete de protección de datos.
SnapMirror o SnapVault	ONTAP Se requieren licencias de SnapMirror o SnapVault si la replicación se habilita en SnapCenter.
SnapRestore	Necesario para restaurar y verificar backups. En sistemas de almacenamiento principales • Requerida en sistemas de destino de SnapVault para realizar la verificación remota y restaurar desde un backup • Requerida en sistemas de destino de SnapMirror para realizar la verificación remota
FlexClone	Necesario para clonar bases de datos y operaciones de verificación. En sistemas de almacenamiento principales y secundarios • Requerida en sistemas de destino de SnapVault para crear clones a partir de un backup de almacén secundario • Requerida en sistemas de destino de SnapMirror para crear clones a partir de un backup de SnapMirror secundario

Licencia	Donde se la requiere
Licencias de protocolos	• Licencia de iSCSI o FC para LUN • Licencia de CIFS para recursos compartidos de SMB • Licencia de NFS para VMDK de tipo NFS • Licencia de iSCSI o FC para VMDK de tipo VMFS Requerida en sistemas de destino de SnapMirror para suministrar datos si un volumen de origen no se encuentra disponible
Licencias estándar de SnapCenter (opcional)	Destinos secundarios Se recomienda, pero no es obligatorio, añadir licencias estándar de SnapCenter a destinos secundarios. Si las licencias estándar de SnapCenter están deshabilitadas en destinos secundarios, no puede usar SnapCenter para realizar un backup de los recursos en el destino secundario después de realizar una operación de conmutación al nodo de respaldo. Sin embargo, se requiere una licencia de FlexClone en destinos secundarios para realizar operaciones de clonado y verificación.

Licencia	Donde se la requiere
Licencias de Single Mailbox Recovery (SMBR)	Si utiliza el plugin de SnapCenter para Exchange para gestionar bases de datos de Microsoft Exchange Server y Single Mailbox Recovery (SMBR), necesita una licencia adicional para SMBR, la cual debe adquirirse por separado en función del buzón de usuario. NetApp® Single Mailbox Recovery ha llegado al final de la disponibilidad (EOA) el 12 de mayo de 2023. Para obtener más información, consulte "CPC-00507". NetApp continuará prestando soporte a los clientes que hayan adquirido capacidad, mantenimiento y soporte de sus buzones mediante números de referencia de marketing introducidos el 24 de junio de 2020, durante el periodo de concesión de soporte. Single Mailbox Recovery de NetApp es un producto de partner que proporciona Ontrack. Ontrack PowerControls ofrece capacidades similares a las de Single Mailbox Recovery de NetApp. Los clientes pueden adquirir nuevas licencias de software Ontrack PowerControls y renovaciones de mantenimiento y soporte de Ontrack PowerControls desde Ontrack (hasta licensingteam@ontrack.com) para la recuperación granular de buzones después de la fecha EOA del 12 de mayo de 2023.

Las licencias avanzada y SnapCenter de servicios de archivos NAS de SnapCenter quedaron obsoletas y ya no están disponibles. La licencia estándar y la licencia basada en la capacidad ya no son necesarias para Amazon FSx para NetApp ONTAP, ONTAP Select, Cloud Volumes ONTAP y Azure NetApp Files.

Debe instalar una o más licencias de SnapCenter. Para obtener información sobre cómo agregar licencias, consulte "Añada licencias estándar basadas en controladora de SnapCenter".

SnapMirror sincronización activa en SnapCenter

La sincronización activa de SnapMirror permite que los servicios empresariales continúen funcionando incluso si se produce un fallo completo del sitio, lo que permite a las aplicaciones conmutar por error de forma transparente mediante una copia secundaria. No se requiere intervención manual ni secuencias de comandos adicionales para activar una recuperación tras fallos con SnapMirror sincronización activa.

Para obtener más información sobre la sincronización activa de SnapMirror, consulte "Información general sobre sincronización activa de SnapMirror".

Para la sincronización activa de SnapMirror, asegúrese de haber cumplido los distintos requisitos de configuración de hardware, software y sistema. Para obtener más información, consulte "Requisitos previos"

Los plugins compatibles con esta función son el plugin de SnapCenter para SQL Server, el plugin de SnapCenter para Windows, el plugin de SnapCenter para base de datos de Oracle, el plugin de SnapCenter para base de datos SAP HANA, el plugin de SnapCenter para Microsoft Exchange Server y el plugin de SnapCenter para Unix.

Después de instalar SnapCenter Server y los complementos, debe habilitar la API REST para que SnapCenter detecte las relaciones de sincronización activas de SnapMirror .

- En el host del servidor SnapCenter , edite el archivo *C:\Program Files\ NetApp\SMCore\SMCoreServiceHost.dll.config* para modificar el valor del parámetro *IsRestEnabledForStorageConnection* a *true* y luego reinicie el servicio SnapCenter SMCore.
- En los hosts de complementos de Windows:
  - Edite el archivo *C:\Program Files\ NetApp\ SnapCenter\SMCore\SMCoreServiceHost.dll.config* para modificar el valor del parámetro *IsRestEnabledForStorageConnection* a *true*.
  - Edite el archivo *C:\Program Files\ NetApp\ SnapCenter\SMCore\SnapDriveService.dll.config* para modificar el valor del parámetro *IsRestEnabledForStorageConnection* a *true*.
  - Reinicie el servicio SnapCenter SMCore.

Para admitir la proximidad del iniciador de host en SnapCenter, su valor, ya sea el origen o el destino deben establecerse en ONTAP.

Los casos de uso no compatibles con SnapCenter:

- Si convierte las cargas de trabajo asimétricas existentes de SnapMirror sincronización activa en simétricas cambiando la política de las relaciones de sincronización activa de SnapMirror de *automatedfailover* a *automatedfailoverduplex* en ONTAP, no se admite lo mismo en SnapCenter.
- Si existen backups de un grupo de recursos (ya protegido en SnapCenter) y se cambia la política de almacenamiento en las relaciones de sincronización activa de SnapMirror desde *automatedfailover* a *automatedfailoverduplex* en ONTAP, no se admite lo mismo en SnapCenter.

Conceptos clave de la protección de datos

Antes de usar SnapCenter, entienda conceptos clave para el backup, el clonado y la restauración.

Recursos

Los recursos incluyen bases de datos, sistemas de archivos Windows o recursos compartidos de archivos incluidos en un backup o clonados con SnapCenter. En función del entorno, los recursos también pueden ser instancias de bases de datos, grupos de disponibilidad de SQL Server, bases de datos de Oracle, base de datos RAC o grupos de aplicaciones personalizados.

Grupo de recursos

Un grupo de recursos es una agrupacion de recursos en un host o un clúster, potencialmente de varios hosts y clústeres. Las operaciones realizadas en un grupo de recursos se aplican a todos sus recursos en función de la programación especificada. Puede ejecutar backups bajo demanda o programados para recursos o grupos individuales.

Si un host de un grupo de recursos compartidos entra en modo de mantenimiento, todas las operaciones programadas de ese grupo se suspenden en todos los hosts.

Use plugins relevantes para realizar el backup de recursos específicos: Plugins de bases de datos para bases de datos, plugins del sistema de archivos para sistemas de archivos y plugin de SnapCenter para VMware vSphere para máquinas virtuales y almacenes de datos.

Normativas

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.

Se pueden seleccionar una o varias políticas al crear un grupo de recursos o al ejecutar un backup bajo demanda.

Un grupo de recursos define qué es necesario proteger y cuándo debe protegerse en términos de día y hora. Una política describe cómo se llevará a cabo la protección. Por ejemplo, si se necesita realizar un backup de todas las bases de datos o los sistemas de archivos de un host, puede crearse un grupo de recursos que incluya todas las bases de datos o los sistemas de archivos del host. Luego, se podrían vincular dos políticas al grupo de recursos: Una diaria y una horaria.

Al crear el grupo de recursos y añadir las políticas, es posible configurarlo para que se realice un backup completo todos los días, y agregar programaciones para backups de registros por hora.

Se pueden usar scripts previos y posteriores en operaciones de protección de datos. Estos scripts permiten la automatización antes o después del trabajo de protección de datos. Por ejemplo, un script podría notificar automáticamente cuando hay errores o advertencias en un trabajo de protección de datos. Comprender los requisitos para la creación de estos scripts es esencial antes de configurar scripts previos y posteriores.

Grupo de consistencia (GC)

Un grupo de consistencia es una colección de volúmenes administrados como una sola unidad. Los CG están sincronizados para garantizar la coherencia de los datos en todas las unidades de almacenamiento y volúmenes. En ONTAP, proporcionan una gestión sencilla y una garantía de protección para una carga de trabajo de aplicaciones que abarca múltiples volúmenes. Obtenga más información sobre "grupos de consistencia" .

Uso de scripts previos y posteriores

Los scripts previos y posteriores pueden automatizar las tareas de protección de datos antes o después del trabajo. Por ejemplo, puede agregar un script para notificarle los fallos o advertencias del trabajo. Antes de configurarlos, asegúrese de comprender los requisitos de estos scripts.

Tipos de scripts compatibles

Los siguientes tipos de scripts son compatibles con Windows:

- Archivos de lotes
- Scripts de PowerShell
- Scripts Perl

Los siguientes tipos de scripts se admiten para UNIX:

- Scripts Perl
- Scripts Python
- Scripts de shell

> Junto con el shell bash predeterminado, también se admiten otros shell como sh-shell, k-shell y c-shell.

Ruta del script

Todos los scripts previos y posteriores que se ejecutan como parte de las operaciones de SnapCenter tanto en sistemas de almacenamiento no virtualizados como en los virtualizados, se ejecutan en el host del plugin.

- Los scripts de Windows deben encontrarse en el host del plugin.

> La ruta scripts previos o posteriores no debe incluir unidades o recursos compartidos. La ruta debe ser relativa a LA RUTA DE ACCESO_SCRIPTS.

- Los scripts de UNIX deben encontrarse en el host del plugin.

> La ruta de acceso del script se valida en el momento de la ejecución.

Dónde especificar scripts

Los scripts se especifican en las políticas de backup. Cuando se inicia una tarea de backup, la política asocia automáticamente el script con los recursos que se incluirán en el backup. Al crear una política de backup, se pueden especificar los argumentos de script previo y script posterior.

> No puede especificar varios scripts.

Tiempo de espera de scripts

De forma predeterminada, el tiempo de espera se establece en 60 segundos. Puede modificar el valor del tiempo de espera.

Salida de script

El directorio predeterminado para los archivos de salida scripts previos y posteriores de Windows es Windows\System32.

No hay una ubicación predeterminada para los scripts previos y posteriores de UNIX. Puede redirigir el archivo de salida a cualquier ubicación preferida.

Aplicaciones y sistemas de almacenamiento compatibles con SnapCenter

Debe conocer los sistemas de almacenamiento, aplicaciones y bases de datos que admite SnapCenter.

Sistemas de almacenamiento compatibles

- NetApp ONTAP 9.12.1 y versiones posteriores
- Azure NetApp Files
- Amazon FSX para ONTAP de NetApp

  Amazon FSx for NetApp ONTAP admite memoria no volátil express (NVMe) a través del Protocolo de control de transporte (TCP).

  Para obtener más información sobre Amazon FSX para ONTAP de NetApp, consulte "Documentación de Amazon FSX para ONTAP de NetApp".

- Sistemas NetApp ASA r2 que ejecutan NetApp ONTAP 9.16.1 y versiones posteriores

  Debe utilizar ONTAP 9.17.1 si está utilizando SnapCenter Server 6.2 y los complementos de SnapCenter 6.2.

Aplicaciones y bases de datos compatibles

SnapCenter admite la protección de diferentes aplicaciones y bases de datos.

SnapCenter admite la protección de las cargas de trabajo de Oracle y Microsoft SQL en entornos de centro de datos definido por software (SDDC) de VMware Cloud on Amazon Web Services (AWS). "Más información".

Métodos de autenticación para las credenciales de SnapCenter

Las credenciales utilizan métodos de autenticación diferentes según la aplicación o el entorno. Las credenciales autentican a los usuarios para que puedan realizar operaciones de SnapCenter. Debe crear un conjunto de credenciales para instalar plugins y otro para operaciones de protección de datos.

Autenticación de Windows

El método de autenticación de Windows autentica de acuerdo con Active Directory. Para la autenticación de Windows, se configura Active Directory fuera de SnapCenter. SnapCenter autentica sin configuración adicional. Es necesario contar con credenciales de Windows para añadir hosts, instalar paquetes de plugins y programar trabajos.

Autenticación de dominio que no es de confianza

SnapCenter permite que los usuarios y grupos que pertenecen a dominios que no son de confianza creen credenciales de Windows. Para que la autenticación se complete correctamente, debe registrar los dominios que no son de confianza en SnapCenter.

Autenticación de grupo de trabajo local

SnapCenter permite la creación de credenciales de Windows con grupos y usuarios de grupo de trabajo local. La autenticación de Windows para los grupos y usuarios de grupos de trabajo locales no se produce durante la creación de las credenciales de Windows, pero se aplaza hasta que se realizan el registro del host y otras

operaciones del host.

Autenticación de SQL Server

El método de autenticación de SQL se verifica de acuerdo con una instancia de SQL Server. Esto significa que debe detectarse una instancia de SQL Server en SnapCenter. Por lo tanto, antes de añadir una credencial de SQL, debe añadir un host, instalar paquetes de plugins y actualizar los recursos. Necesita la autenticación de SQL Server para realizar operaciones, como programar en SQL Server o detectar recursos.

Autenticación de Linux

El método de autenticación de Linux autentica con un host Linux. Necesita la autenticación de Linux durante el paso inicial de añadir el host Linux e instalar el paquete de plugins de SnapCenter para Linux de forma remota desde la interfaz gráfica de usuario de SnapCenter.

Autenticación AIX

El método de autenticación AIX autentica con un host AIX. Necesita la autenticación de AIX durante el paso inicial de añadir el host AIX e instalar el paquete de plugins de SnapCenter para AIX de forma remota desde la interfaz gráfica de usuario de SnapCenter.

Autenticación de base de datos de Oracle

El método de autenticación de base de datos de Oracle autentica con una base de datos de Oracle. Necesita una autenticación de base de datos de Oracle para realizar operaciones en la base de datos de Oracle si la autenticación de sistema operativo (SO) está deshabilitada en el host de bases de datos. Por lo tanto, antes de añadir una credencial de base de datos de Oracle, debe crear un usuario de Oracle en la base de datos de Oracle con Privileges de sysdba.

Autenticación de Oracle ASM

El método de autenticación de Oracle ASM autentica con una instancia de Oracle Automatic Storage Management (ASM). Si necesita acceder a una instancia de Oracle ASM y la autenticación del sistema operativo está deshabilitada en el host de base de datos, es necesaria la autenticación de Oracle ASM. Antes de agregar una credencial de Oracle ASM, cree un usuario oracle con SYSTEM Privileges en la instancia de ASM.

Autenticación de catálogo de RMAN

El método de autenticación de catálogo de RMAN autentica con la base de datos de catálogos de Oracle Recovery Manager (RMAN). Si configuró un mecanismo de catálogo externo y registró la base de datos en la base de datos de catálogos, debe añadir una autenticación de catálogo de RMAN.