Empezar

SnapCenter software

NetApp
November 06, 2025

Tabla de contenidos

Empezar

Obtenga más información sobre el SnapCenter software

Descripción 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:

- Copias de seguridad rápidas, eficientes en cuanto al espacio y consistentes con las aplicaciones basadas en disco
- Restauración rápida y detallada, y recuperación consistente con la aplicación
- Clonación rápida y que ahorra 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 que se encuentran en los sistemas primarios ONTAP FAS, AFF o ASA y se replican en los sistemas secundarios ONTAP FAS, AFF o ASA
  - Datos que se encuentran en los sistemas primarios de ONTAP Select
  - Datos que se encuentran en sistemas primarios y secundarios de ONTAP FAS, AFF o ASA y están protegidos en el almacenamiento de objetos StorageGRID local
  - Datos que se encuentran en los sistemas primarios y secundarios de ONTAP ASA r2
- Local en una nube híbrida para proteger lo siguiente:
  - Datos que se encuentran en los sistemas principales de ONTAP FAS, AFF o ASA y se replican en 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 una nube pública para proteger lo siguiente:
  - Datos que se encuentran en los sistemas principales de Cloud Volumes ONTAP (anteriormente ONTAP Cloud)
  - Datos que están en Amazon FSX para ONTAP
  - Datos que se encuentran en los Azure NetApp Files (Oracle, Microsoft SQL y SAP HANA)

Características principales

SnapCenter ofrece las siguientes características clave:

- Protección de datos centralizada y consistente para cada aplicación

  La protección de datos es compatible con Microsoft Exchange Server, Microsoft SQL Server, bases de datos Oracle en Linux o AIX, bases de datos SAP HANA, IBM Db2, PostgreSQL, MySQL y sistemas de archivos de host de Windows que se ejecutan en sistemas ONTAP . SnapCenter también admite la protección de aplicaciones como MongoDB, Storage, MaxDB, Sybase ASE, ORASCPM.

- Copias de seguridad basadas en políticas

  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 .

- Restaurar y recuperar

  SnapCenter proporciona restauraciones rápidas y granulares de copias de seguridad y una recuperación basada en el tiempo y consistente con las aplicaciones. Puede restaurar desde cualquier destino en la nube híbrida.

- Clonación

  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 REST, cmdlets de Windows, comandos de UNIX

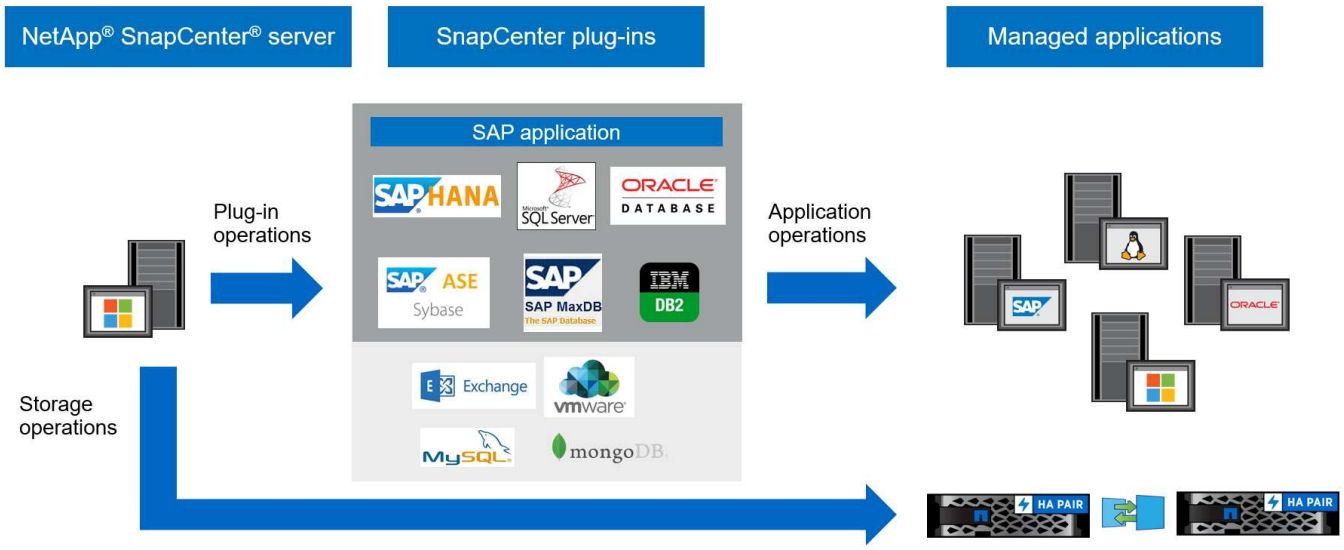
  SnapCenter proporciona API REST para la mayoría de las funciones para la integración con cualquier software de orquestación y el uso de cmdlets de Windows PowerShell y la interfaz de línea de comandos.

- Panel de control y generación de informes de protección de datos centralizados
- 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 respaldo
- Instalación push automatizada de complementos
- Alta disponibilidad
- Recuperación ante desastres (DR)
- SnapLock "Más información"

- Sincronización activa de SnapMirror (inicialmente lanzada como SnapMirror Business Continuity [SM-BC])
- Duplicación sincrónica "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 SnapCenter Server, el paquete de complementos de SnapCenter para Windows y el paquete de complementos de SnapCenter para Linux. Cada paquete contiene complementos para diversas aplicaciones y componentes de 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 REST y el repositorio de SnapCenter .

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

Complementos de SnapCenter

Cada complemento de SnapCenter admite entornos, bases de datos y aplicaciones específicos.

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

Nombre del complemento	Incluido en el paquete de instalación	Requiere otros complementos	Instalado en el host	Plataforma compatible
Complemento de SnapCenter para Microsoft Exchange Server	Paquete de complementos para Windows	Complemento para Windows	Host del servidor Exchange	Ventanas
Complemento de SnapCentre para Oracle Database	Paquete de complementos para Linux y paquete de complementos para AIX	Complemento para UNIX	Host de Oracle	Linux o AIX
Complemento de SnapCenter para la base de datos SAP HANA	Paquete de complementos para Linux y paquete de complementos para Windows	Complemento para UNIX o complemento para Windows	Host del cliente HDBSQL	Linux o Windows
Complemento de SnapCenter para IBM Db2	Paquete de complementos para Linux y paquete de complementos para Windows	Complemento para UNIX o complemento para Windows	Host de Db2	Linux, AIX o Windows
Complemento de SnapCenter para PostgreSQL	Paquete de complementos para Linux y paquete de complementos para Windows	Complemento para UNIX o complemento para Windows	Host de PostgreSQL	Linux o Windows
Complemento SnaoCenter para MySQL	Paquete de complementos para Linux y paquete de complementos para Windows	Complemento para UNIX o complemento para Windows	Host MySQL	Linux o Windows
Complemento de SnapCenter para MongoDB	Paquete de complementos para Linux y paquete de complementos para Windows	Complemento para UNIX o complemento para Windows	Host de MongoDB	Linux o Windows
Complemento de SnapCenter para ORASCPM (aplicaciones Oracle)	Paquete de complementos para Linux y paquete de complementos para Windows	Complemento para UNIX o complemento para Windows	Host de Oracle	Linux o Windows

Nombre del complemento	Incluido en el paquete de instalación	Requiere otros complementos	Instalado en el host	Plataforma compatible
Complemento de SnapCenter para SAP ASE	Paquete de complementos para Linux y paquete de complementos para Windows	Complemento para UNIX o complemento para Windows	Host SAP	Linux o Windows
Complemento de SnapCenter para SAP MaxDB	Paquete de complementos para Linux y paquete de complementos para Windows	Complemento para UNIX o complemento para Windows	Host de SAP MaxDB	Linux o Windows
Complemento de SnapCenter para almacenamiento	Paquete de complementos para Linux y paquete de complementos para Windows	Complemento para UNIX o complemento 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 SnapCenter Plug-in for VMware vSphere" .

Repositorio de SnapCenter

El repositorio de SnapCenter , a veces denominado base de datos NSM, almacena información y metadatos para cada operación de 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:

- Copia de seguridad, clonación, restauración y verificación de metadatos
- Información de informes, trabajos y eventos
- Información del host y del complemento
- Detalles de rol, usuario y permisos
- Información de conexión del sistema de almacenamiento

Funciones de seguridad en SnapCenter

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

SnapCenter incluye las siguientes funciones de seguridad:

- Toda comunicación con SnapCenter utiliza HTTP sobre SSL (HTTPS).
- Todas las credenciales en SnapCenter están protegidas mediante el cifrado Estándar de cifrado avanzado (AES).
- Admite algoritmos de seguridad que cumplen con el Estándar Federal de Procesamiento de Información (FIPS).
- Admite el uso de los certificados CA autorizados proporcionados por el cliente.
- Admite seguridad de la capa de transporte (TLS) 1.3 para la comunicación con ONTAP. También puede utilizar TLS 1.2 para la comunicación entre clientes y servidores.
- Admite un determinado conjunto de suites de cifrado SSL para proporcionar seguridad en las comunicaciones de red. "Más información" .
- SnapCenter se instala dentro del firewall de su empresa para permitir el acceso al servidor SnapCenter y para permitir la comunicación entre el servidor SnapCenter y los complementos.
- El acceso a la API y a las operaciones de SnapCenter utiliza tokens cifrados con cifrado AES, que caducan después de 24 horas.
- SnapCenter se integra con Windows Active Directory para el inicio de sesión y el control de acceso basado en roles (RBAC) que rigen los permisos de acceso.
- IPsec es compatible con SnapCenter en ONTAP para máquinas host de Windows y Linux. "Más información" .
- Los cmdlets de PowerShell de SnapCenter están protegidos por sesión.
- Después de un período predeterminado de 15 minutos de inactividad, SnapCenter le advierte que se cerrará su sesión en 5 minutos.

  Después de 20 minutos de inactividad, SnapCenter cerrará su sesión y deberá iniciar sesión nuevamente. Puede modificar el período de cierre de sesión.

- El inicio de sesión se deshabilita temporalmente después de 5 intentos de inicio de sesión incorrectos.
- Admite la autenticación de certificados CA entre SnapCenter Server y ONTAP. "Más información" .
- Integrity Verifier se agrega al servidor SnapCenter y a los complementos y valida todos los binarios enviados durante las operaciones de instalación y actualización nuevas.

Descripción general del certificado CA

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

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

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

Comunicación SSL bidireccional

La comunicación SSL bidireccional asegura la comunicación mutua entre SnapCenter Server y los complementos.

Descripción general de la autenticación basada en certificados

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

Autenticación multifactor (MFA)

MFA utiliza un proveedor de identidad (IdP) de terceros a través del lenguaje de marcado de aserción de seguridad (SAML) para administrar las sesiones de usuario. Esta funcionalidad mejora la seguridad de la autenticación al tener la opción de utilizar múltiples factores como TOTP, biometría, notificaciones push, etc. junto con el nombre de usuario y la contraseña existentes. Además, permite al cliente utilizar sus propios proveedores de identidad de usuario para obtener un inicio de sesión de usuario unificado (SSO) en toda su cartera.

MFA solo se aplica para iniciar sesión en la interfaz de usuario de SnapCenter Server. Los inicios de sesión se autentican a través del IdP Servicios de federación de Active Directory (AD FS). Puede configurar varios factores de autenticación en AD FS. SnapCenter es el proveedor de servicios y debe SnapCenter como parte confiable en AD FS. Para habilitar MFA en SnapCenter, necesitará los metadatos de AD FS.

Para obtener información sobre cómo habilitar MFA, consulte"Habilitar 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 delegar el control de los recursos de SnapCenter a diferentes usuarios o grupos de usuarios. Este acceso administrado centralmente permite a los administradores de aplicaciones trabajar de forma segura dentro de entornos delegados.

Puede crear y modificar roles y agregar acceso a recursos a los usuarios en cualquier momento. Sin embargo, cuando configure SnapCenter por primera vez, deberá al menos agregar usuarios o grupos de Active Directory a los roles y luego agregar acceso a recursos a esos usuarios o grupos.

> No puede utilizar SnapCenter para crear cuentas de usuario o grupo. Debe crear cuentas de usuario o grupo en Active Directory del sistema operativo o la base de datos.

Tipos de RBAC en SnapCenter

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

- RBAC de SnapCenter
- RBAC a nivel de aplicación
- Complemento de SnapCenter para VMware vSphere RBAC
- Permisos de ONTAP

RBAC de SnapCenter

SnapCenter tiene roles predefinidos y usted puede asignar usuarios o grupos de usuarios a estos roles. Los roles predefinidos son:

- Rol de administrador de SnapCenter
- Rol de administrador de copias de seguridad y clonación de aplicaciones
- Función de visor de copias de seguridad y clones
- Rol de administrador de infraestructura

Cuando asigna un rol a un usuario, solo los trabajos que son relevantes para ese usuario son visibles en la página Trabajos, a menos que le asigne el rol SnapCenterAdmin.

También puede crear nuevos roles y administrar permisos y usuarios. Puede asignar permisos a usuarios o grupos para acceder a objetos de SnapCenter , como hosts, conexiones de almacenamiento y grupos de recursos.

Puede asignar permisos RBAC a usuarios y grupos dentro del mismo bosque y a usuarios que pertenecen a diferentes bosques. No se pueden asignar permisos RBAC a usuarios que pertenecen a grupos anidados en distintos bosques.

> Si crea un rol personalizado, debe contener todos los permisos del rol SnapCenterAdmin. Si solo copia algunos de los permisos, por ejemplo, agregar host o quitar host, no podrá realizar esas operaciones.

Los usuarios deben proporcionar autenticación durante el inicio de sesión, a través de la interfaz gráfica de usuario (GUI) o utilizando cmdlets de PowerShell. Si los usuarios son miembros de más de un rol, después de ingresar las credenciales de inicio de sesión, se les solicita que especifiquen el rol que desean usar. Los usuarios también deben proporcionar autenticación para ejecutar las API.

RBAC a nivel de aplicación

SnapCenter utiliza credenciales para verificar que los usuarios autorizados de SnapCenter también tengan permisos a nivel de aplicación.

Por ejemplo, si desea realizar operaciones de protección de datos en un entorno de SQL Server, debe configurar las credenciales con las credenciales de Windows o SQL adecuadas. El servidor SnapCenter autentica las credenciales establecidas utilizando cualquiera de los métodos. 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.

SnapCenter Plug-in for VMware vSphere RBAC

Si utiliza el complemento VMware de SnapCenter para la protección de datos consistente con la máquina virtual, vCenter Server proporciona un nivel adicional de RBAC. El complemento VMware de SnapCenter admite tanto vCenter Server RBAC como ONTAP RBAC. "Más información"

Mejor práctica: 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, debe asignar el permiso StorageConnection para habilitar la comunicación de la máquina virtual de almacenamiento (SVM) o asignar una SVM al usuario para habilitar el permiso para usar la SVM. El permiso de Conexión de almacenamiento permite a los usuarios crear conexiones SVM.

Por ejemplo, un usuario con el rol de administrador de SnapCenter puede crear conexiones SVM y asignarlas a un usuario con el rol de administrador de copias de seguridad y clones de aplicaciones, que de manera predeterminada no tiene permiso para crear o editar conexiones SVM. Sin una conexión SVM, los usuarios no pueden completar ninguna operación de copia de seguridad, clonación o restauración.

Rol de administrador de SnapCenter

El rol de administrador de SnapCenter tiene todos los permisos habilitados. No puedes modificar los permisos para este rol. Puede agregar usuarios y grupos al rol o eliminarlos.

Rol de administrador de copias de seguridad y clonación de aplicaciones

El rol de administrador de copias de seguridad y clones de aplicaciones tiene los permisos necesarios para realizar acciones administrativas para copias de seguridad de aplicaciones y tareas relacionadas con clones. Esta función no tiene permisos para administración de host, aprovisionamiento, administración de conexión de almacenamiento o instalación remota.

Permisos	Habilitado	Crear	Leer	Actualizar	Borrar
Grupo de recursos	No aplicable	Sí	Sí	Sí	Sí
Política	No aplicable	Sí	Sí	Sí	Sí
Respaldo	No aplicable	Sí	Sí	Sí	Sí
Host	No aplicable	Sí	Sí	Sí	Sí
Conexión de almacenamiento	No aplicable	No	Sí	No	No
Clon	No aplicable	Sí	Sí	Sí	Sí
Disposición	No aplicable	No	Sí	No	No
Consola	Sí	No aplicable	No aplicable	No aplicable	No aplicable

Permisos	Habilitado	Crear	Leer	Actualizar	Borrar
Informes	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 complementos	No	No aplicable		No aplicable	No aplicable
Migración	No	No aplicable	No aplicable	No aplicable	No aplicable
Montar	Sí	Sí	No aplicable	No aplicable	No aplicable
Desmontar	Sí	Sí	No aplicable	No aplicable	No aplicable
Restauración de volumen completo	No	No	No aplicable	No aplicable	No aplicable
Protección secundaria	No	No	No aplicable	No aplicable	No aplicable
Monitor de trabajo	Sí	No aplicable	No aplicable	No aplicable	No aplicable

Función de visor de copias de seguridad y clones

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	Habilitado	Crear	Leer	Actualizar	Borrar
Grupo de recursos	No aplicable	No	Sí	No	No
Política	No aplicable	No	Sí	No	No
Respaldo	No aplicable	No	Sí	No	No
Host	No aplicable	No	Sí	No	No
Conexión de almacenamiento	No aplicable	No	Sí	No	No

Permisos	Habilitado	Crear	Leer	Actualizar	Borrar
Clon	No aplicable	No	Sí	No	No
Disposición	No aplicable	No	Sí	No	No
Consola	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Informes	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 complementos	No	No aplicable	No aplicable	No aplicable	No aplicable
Migración	No	No aplicable	No aplicable	No aplicable	No aplicable
Montar	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Desmontar	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Restauración de volumen completo	No	No aplicable	No aplicable	No aplicable	No aplicable
Protección secundaria	No	No aplicable	No aplicable	No aplicable	No aplicable
Monitor de trabajo	Sí	No aplicable	No aplicable	No aplicable	No aplicable

Rol de administrador de infraestructura

El rol de administrador de infraestructura tiene permisos habilitados para la administración de host, administración de almacenamiento, aprovisionamiento, grupos de recursos, informes de instalación remota y acceso al Panel de control.

Permisos	Habilitado	Crear	Leer	Actualizar	Borrar
Grupo de recursos	No aplicable	Sí	Sí	Sí	Sí
Política	No aplicable	No	Sí	Sí	Sí

Permisos	Habilitado	Crear	Leer	Actualizar	Borrar
Respaldo	No aplicable	Sí	Sí	Sí	Sí
Host	No aplicable	Sí	Sí	Sí	Sí
Conexión de almacenamiento	No aplicable	Sí	Sí	Sí	Sí
Clon	No aplicable	No	Sí	No	No
Disposición	No aplicable	Sí	Sí	Sí	Sí
Consola	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Informes	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 complementos	Sí	No aplicable	No aplicable	No aplicable	No aplicable
Migración	No	No aplicable	No aplicable	No aplicable	No aplicable
Montar	No	No aplicable	No aplicable	No aplicable	No aplicable
Desmontar	No	No aplicable	No aplicable	No aplicable	No aplicable
Restauración de volumen completo	No	No	No aplicable	No aplicable	No aplicable
Protección secundaria	No	No	No aplicable	No aplicable	No aplicable
Monitor de trabajo	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 corrupción de recursos o fallas del servidor. Ayuda a restaurar el repositorio de SnapCenter , las programaciones del servidor, los componentes de

configuración y el complemento de SnapCenter para SQL Server y su almacenamiento.

Esta sección explica los dos tipos de DR en SnapCenter:

Recuperación ante desastres del servidor SnapCenter

- Los datos de SnapCenter Server se respaldan y se pueden recuperar sin necesidad de agregar ni administrar ningún complemento a SnapCenter Server.
- El servidor SnapCenter secundario debe instalarse en el mismo directorio de instalación y en el mismo puerto que el servidor SnapCenter principal.
- Para la autenticación multifactor (MFA), durante la recuperación ante desastres de SnapCenter Server, cierre todas las pestañas del navegador y vuelva a abrir un navegador para iniciar sesión nuevamente. 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 API REST para realizar copias de seguridad del servidor SnapCenter . Ver "Flujos de trabajo de API REST para la recuperación ante desastres de SnapCenter Server" .
- El archivo de configuración relacionado con la configuración de auditoría no se respalda en la copia de seguridad de DR ni en el servidor de DR después de la operación de restauración. Debe repetir manualmente la configuración del registro de auditoría.

Complemento de SnapCenter y recuperación ante desastres de almacenamiento

DR solo está disponible para el complemento SnapCenter para SQL Server. Si el complemento no funciona, cambie a otro host SQL y recupere los datos siguiendo unos pocos pasos. Ver "Recuperación ante desastres del complemento SnapCenter para SQL Server" .

SnapCenter utiliza ONTAP SnapMirror para replicar datos, que pueden usarse para recuperación ante desastres manteniendo los datos sincronizados en un sitio secundario. Para iniciar la conmutación por error, interrumpa la replicación de SnapMirror . Durante la recuperación, invierta la sincronización para replicar los datos desde el sitio de recuperación ante desastres a la ubicación principal.

Licencias requeridas por SnapCenter

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

Licencia	Cuando sea necesario
SnapCenter Standard basado en controlador	Requerido para FAS, AFF, ASA La licencia estándar de SnapCenter es una licencia basada en controlador y se incluye como parte de NetApp ONTAP One. Si tiene la licencia de SnapManager Suite, también obtendrá el derecho de licencia de SnapCenter Standard. Si desea instalar SnapCenter a modo de prueba con almacenamiento FAS, AFF o ASA , puede obtener una licencia de evaluación de NetApp ONTAP One comunicándose 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 modelo A400 o posterior, deberá adquirir el paquete de protección de datos.
SnapMirror o SnapVault	ONTAP Se requiere una licencia de SnapMirror o SnapVault si la replicación está habilitada en SnapCenter.
SnapRestore	Necesario para restaurar y verificar copias de seguridad. Sobre los sistemas de almacenamiento primario • Requerido en los sistemas de destino SnapVault para realizar la verificación remota y restaurar desde una copia de seguridad. • Requerido en los sistemas de destino SnapMirror para realizar la verificación remota.

Licencia	Cuando sea necesario
FlexClone	Necesario para clonar bases de datos y realizar operaciones de verificación. Sobre sistemas de almacenamiento primario y secundario • Requerido en los sistemas de destino SnapVault para crear clones a partir de una copia de seguridad de la bóveda secundaria. • Requerido en los sistemas de destino SnapMirror para crear clones a partir de una copia de seguridad secundaria de SnapMirror .
Licencias de protocolo	• Licencia iSCSI o FC para LUN • Licencia CIFS para acciones SMB • Licencia NFS para VMDK de tipo NFS • Licencia iSCSI o FC para VMDK de tipo VMFS Obligatorio en los sistemas de destino SnapMirror para servir datos si un volumen de origen no está disponible.
Licencias estándar de SnapCenter (opcionales)	Destinos secundarios Se recomienda, aunque no es obligatorio, que agregue licencias estándar de SnapCenter a destinos secundarios. Si las licencias estándar de SnapCenter no están habilitadas en destinos secundarios, no podrá usar SnapCenter para realizar copias de seguridad de recursos en el destino secundario después de realizar una operación de conmutación por error. Sin embargo, se requiere una licencia FlexClone en destinos secundarios para realizar operaciones de clonación y verificación.

Licencia	Cuando sea necesario
Licencias de recuperación de buzón único (SMBR)	Si utiliza el complemento SnapCenter para Exchange para administrar las bases de datos de Microsoft Exchange Server y Single Mailbox Recovery (SMBR), necesitará una licencia adicional para SMBR que debe comprarse por separado según el buzón del usuario. NetApp® Single Mailbox Recovery llegó al final de su disponibilidad (EOA) el 12 de mayo de 2023. Para obtener más información, consulte"CPC-00507" . NetApp seguirá brindando soporte a los clientes que hayan adquirido capacidad de buzón, mantenimiento y soporte a través de los números de pieza de marketing introducidos el 24 de junio de 2020, mientras dure el derecho de soporte. NetApp Single Mailbox Recovery es un producto asociado proporcionado por Ontrack. Ontrack PowerControls ofrece capacidades similares a las de NetApp Single Mailbox Recovery. Los clientes pueden adquirir nuevas licencias de software Ontrack PowerControls y renovaciones de mantenimiento y soporte de Ontrack PowerControls de Ontrack (a través de licensingteam@ontrack.com) para la recuperación granular del buzón después de la fecha de fin de operación del 12 de mayo de 2023.

Las licencias de SnapCenter Advanced y SnapCenter NAS File Services están obsoletas y ya no están disponibles. La licencia estándar y la licencia basada en capacidad ya no son necesarias para Amazon FSx for 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"Agregar licencias basadas en controlador de SnapCenter Standard" .

Sincronización activa de SnapMirror en SnapCenter

La sincronización activa de SnapMirror permite que los servicios empresariales sigan funcionando incluso en caso de una falla total del sitio, permitiendo que las aplicaciones conmuten por error de forma transparente mediante una copia secundaria. No se requiere intervención manual ni secuencias de comandos adicionales para activar una conmutación por error con la sincronización activa de SnapMirror .

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

Para la sincronización activa de SnapMirror , asegúrese de cumplir con los distintos requisitos de configuración de hardware, software y sistema. Para obtener información, consulte "Prerrequisitos"

Los complementos compatibles con esta función son el complemento de SnapCenter para SQL Server, el

complemento de SnapCenter para Windows, el complemento de SnapCenter para la base de datos Oracle, el complemento de SnapCenter para la base de datos SAP HANA, el complemento de SnapCenter para Microsoft Exchange Server y el complemento de SnapCenter para Unix.

> Para admitir la proximidad del iniciador del host en SnapCenter, su valor, ya sea de origen o de destino, debe configurarse en ONTAP.

Los casos de uso no compatibles con SnapCenter:

- Si convierte las cargas de trabajo de sincronización activa asimétrica de SnapMirror existentes en simétricas al cambiar la política en las relaciones de sincronización activa de SnapMirror de *automatedfailover* a *automatedfailoverduplex* en ONTAP, lo mismo no será compatible en SnapCenter.
- Si hay copias de seguridad de un grupo de recursos (ya protegido en SnapCenter) y luego se cambia la política de almacenamiento en las relaciones de sincronización activa de SnapMirror de *automatedfailover* a *automatedfailoverduplex* en ONTAP, lo mismo no se admite en SnapCenter.

Conceptos clave de la protección de datos

Antes de utilizar SnapCenter, comprenda los conceptos clave de copia de seguridad, clonación y restauración.

Recursos

Los recursos incluyen bases de datos, sistemas de archivos de Windows o recursos compartidos de archivos respaldados o clonados con SnapCenter. Según su entorno, los recursos también podrían ser instancias de base de datos, grupos de disponibilidad de SQL Server, bases de datos Oracle, bases de datos RAC o grupos de aplicaciones personalizados.

Grupo de recursos

Un grupo de recursos es una colección de recursos en un host o clúster, potencialmente de múltiples hosts y clústeres. Las operaciones realizadas en un grupo de recursos se aplican a todos sus recursos según la programación especificada. Puede realizar copias de seguridad programadas o a pedido para recursos individuales o grupos.

> Si un host de un grupo de recursos compartidos ingresa al modo de mantenimiento, todas las operaciones programadas para ese grupo se suspenderán en todos los hosts.

Utilice complementos relevantes para realizar copias de seguridad de recursos específicos: complementos de base de datos para bases de datos, complementos de sistema de archivos para sistemas de archivos y SnapCenter Plug-in for VMware vSphere para máquinas virtuales y almacenes de datos.

Políticas

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

Se pueden seleccionar una o más políticas al crear un grupo de recursos o al realizar una copia de seguridad a pedido.

Un grupo de recursos define qué necesita protegerse y cuándo debe protegerse en términos de día y hora. Una política describe cómo se llevará a cabo la protección. Por ejemplo, si es necesario realizar una copia de seguridad de todas las bases de datos o sistemas de archivos de un host, se podría crear un grupo de

recursos que incluya todas las bases de datos o sistemas de archivos del host. Luego se podrían asociar dos políticas al grupo de recursos: una política diaria y una política por hora.

Al crear el grupo de recursos y adjuntar las políticas, es posible configurarlo para realizar una copia de seguridad completa diariamente y otra programación para copias de seguridad de registros cada hora.

Se pueden utilizar prescripciones y posdatas personalizadas 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 sobre fallas o advertencias en tareas de protección de datos. Comprender los requisitos para crear estos guiones es fundamental antes de configurar prescriptos y posscriptos.

Uso de prescriptos y posscriptos

Las prescripciones y posdatas personalizadas pueden automatizar sus tareas de protección de datos antes o después del trabajo. Por ejemplo, puede agregar un script para notificarle sobre fallas o advertencias en el trabajo. Antes de configurarlos, asegúrese de comprender los requisitos para estos scripts.

Tipos de scripts admitidos

Los siguientes tipos de scripts son compatibles con Windows:

- Archivos por lotes
- Scripts de PowerShell
- Scripts de Perl

Los siguientes tipos de scripts son compatibles con UNIX:

- Scripts de Perl
- Scripts de Python
- Scripts de shell

> Además del shell bash predeterminado, también se admiten otros shells como sh-shell, k-shell y c-shell.

Ruta de script

Todos los prescripts y posscripts que se ejecutan como parte de las operaciones de SnapCenter en sistemas de almacenamiento virtualizados y no virtualizados se ejecutan en el host del complemento.

- Los scripts de Windows deben estar ubicados en el host del complemento.

> La ruta de prescripts o posscripts no debe incluir unidades ni recursos compartidos. La ruta debe ser relativa a SCRIPTS_PATH.

- Los scripts de UNIX deben estar ubicados en el host del complemento.

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

Dónde especificar scripts

Los scripts se especifican en las políticas de copia de seguridad. Cuando se inicia un trabajo de respaldo, la

política asocia automáticamente el script con los recursos que se están respaldando. Al crear una política de respaldo, puede especificar los argumentos prescript y postscript.

No se pueden especificar varios scripts.

Tiempos de espera de script

El tiempo de espera está establecido en 60 segundos, de manera predeterminada. Puede modificar el valor del tiempo de espera.

Salida del script

El directorio predeterminado para los archivos de salida de prescripts y postscripts de Windows es Windows\System32.

No existe una ubicación predeterminada para los prescripts y posscripts de UNIX. Puede redirigir el archivo de salida a cualquier ubicación preferida.

Sistemas de almacenamiento y aplicaciones compatibles con SnapCenter

Debe conocer los sistemas de almacenamiento, las aplicaciones y las bases de datos compatibles con SnapCenter.

Sistemas de almacenamiento compatibles

- NetApp ONTAP 9.12.1 y posteriores
- Azure NetApp Files
- Amazon FSx for NetApp ONTAP

  Admite memoria no volátil expresa (NVMe) a través del Protocolo de control de transporte (TCP).

  Para obtener información sobre Amazon FSx for NetApp ONTAP, consulte "Documentación de Amazon FSx for NetApp ONTAP" .

- Sistemas NetApp ASA r2 que ejecutan NetApp ONTAP 9.16.1.

Aplicaciones y bases de datos compatibles

SnapCenter admite la protección de diferentes aplicaciones y bases de datos. Para obtener información detallada sobre las aplicaciones y bases de datos compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp" .

SnapCenter admite la protección de 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 diferentes métodos de autenticación 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 complementos y otro para las operaciones de protección de datos.

Autenticación de Windows

El método de autenticación de Windows se autentica contra Active Directory. Para la autenticación de Windows, Active Directory se configura fuera de SnapCenter. SnapCenter se autentica sin configuración adicional. Necesita una credencial de Windows para agregar hosts, instalar paquetes de complementos y programar trabajos.

Autenticación de dominio no confiable

SnapCenter permite que los usuarios y grupos que pertenecen a dominios no confiables creen credenciales de Windows. Para que la autenticación sea exitosa, debes registrar los dominios no confiables con SnapCenter.

Autenticación de grupo de trabajo local

SnapCenter permite la creación de credenciales de Windows con usuarios y grupos de trabajo locales. La autenticación de Windows para usuarios y grupos de grupos de trabajo locales no ocurre durante la creación de credenciales de Windows, sino que se pospone hasta que se realizan el registro del host y otras operaciones del host.

Autenticación de SQL Server

El método de autenticación SQL se autentica contra una instancia de SQL Server. Esto significa que se debe descubrir una instancia de SQL Server en SnapCenter. Por lo tanto, antes de agregar una credencial SQL, debe agregar un host, instalar paquetes de complementos y actualizar los recursos. Necesita la autenticación de SQL Server para realizar operaciones como programar en SQL Server o descubrir recursos.

Autenticación de Linux

El método de autenticación de Linux se autentica contra un host Linux. Necesita autenticación de Linux durante el paso inicial de agregar el host Linux e instalar el paquete de complementos de SnapCenter para Linux de forma remota desde la GUI de SnapCenter .

Autenticación AIX

El método de autenticación AIX se autentica contra un host AIX. Necesita autenticación AIX durante el paso inicial de agregar el host AIX e instalar el paquete de complementos de SnapCenter para AIX de forma remota desde la GUI de SnapCenter .

Autenticación de base de datos de Oracle

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

Autenticación de Oracle ASM

El método de autenticación de Oracle ASM se autentica contra una instancia de Oracle Automatic Storage Management (ASM). Se requiere autenticación de Oracle ASM si necesita acceder a una instancia de Oracle ASM y la autenticación del sistema operativo está deshabilitada en el host de la base de datos. Antes de agregar una credencial de Oracle ASM, cree un usuario de Oracle con privilegios de sistema en la instancia de ASM.

Autenticación del catálogo RMAN

El método de autenticación del catálogo RMAN se autentica contra la base de datos del catálogo de Oracle Recovery Manager (RMAN). Si ha configurado un mecanismo de catálogo externo y ha registrado su base de datos en la base de datos del catálogo, debe agregar la autenticación del catálogo RMAN.

Operaciones de SnapCenter compatibles con sistemas ASA r2

Los sistemas de almacenamiento ASA r2 son compatibles a partir de SnapCenter 6.1. "Obtenga más información sobre los sistemas ASA r2"

SnapCenter aprovecha las API REST para realizar todas las operaciones en sistemas ASA r2, que no admiten ZAPI.

Operaciones compatibles con SnapCenter para sistemas ASA r2

- Creación de copias de seguridad primarias de aplicaciones a través de VMDK
- Transferencia de instantáneas del grupo de consistencia al sistema de almacenamiento secundario
- Restaurar las copias de seguridad de los sistemas de almacenamiento primario y secundario al host original o al host alternativo
  - Restauración en el lugar desde sistemas de almacenamiento primarios y secundarios mediante VMware vMotion
  - Conectar y copiar la restauración desde los sistemas de almacenamiento primario y secundario
- Clonación de las copias de seguridad en el host original o en el host alternativo

SnapCenter puede descubrir o crear grupos de consistencia ONTAP . También puede aprovisionar e inicializar relaciones de SnapMirror con el clúster de destino para protección secundaria.

Para obtener información sobre cómo habilitar la protección secundaria en los sistemas ASA r2 para su aplicación, consulte:

- "Habilitar la protección secundaria para los recursos de Microsoft SQL Server"
- "Habilitar la protección secundaria para los recursos de SAP HANA"
- "Habilitar la protección secundaria para los recursos de Oracle"
- "Habilitar la protección secundaria para los sistemas de archivos de Windows"
- "Habilitar la protección secundaria para los recursos de IBM Db2"
- "Habilitar la protección secundaria para los recursos de PostgreSQL"
- "Habilitar la protección secundaria para los recursos de MySQL"
- "Habilitar la protección secundaria para los sistemas de archivos Unix"

Operaciones no compatibles con SnapCenter para sistemas ASA r2

- Mapeo de dispositivos sin procesar (RDM)
- Volúmenes de aplicaciones para Oracle
- SAP HANA NDV

- Bóveda de bloqueo
- Instantáneas a prueba de manipulaciones
- Volúmenes de FlexGroup
- Grupo de consistencia jerárquica
- Migración de sistemas de almacenamiento ASA, AFF o FAS a sistemas de almacenamiento ASA r2
- Protección de bases de datos que tienen una combinación de recursos ASA, AFF o FAS y recursos ASA r2
- Cambio de nombre de instantáneas
- Aprovisionamiento secundario del directorio de registro del host del complemento SQL

Inicio rápido del SnapCenter software

La guía de inicio rápido describe los pasos básicos para instalar y configurar el SnapCenter software.

Prepárese para instalar SnapCenter Server

Debe asegurarse de que se cumplan todos los requisitos para instalar SnapCenter Server.

- "Requisitos"
- "Regístrese para acceder al SnapCenter software"
- "Habilitar la autenticación multifactor"

Instalar SnapCenter Server

El servidor SnapCenter se puede instalar en hosts Windows o Linux. Descargue el paquete de instalación de SnapCenter Server desde "Sitio de soporte de NetApp" y ejecutar el instalador.

- "Instalar el servidor SnapCenter en Windows"
- "Instalar SnapCenter Server en Linux"

Configurar el servidor SnapCenter

Después de instalar SnapCenter Server, debe configurarlo según su entorno.

Instale el complemento para su aplicación

Asegúrese de que se cumplan todos los requisitos para instalar el complemento específico de la aplicación en uso y luego proceda con la instalación del complemento correspondiente.

Proteja su aplicación

Después de instalar exitosamente SnapCenter Server y los complementos necesarios, puede iniciar la creación de copias de seguridad de la aplicación. Estas copias de seguridad se pueden utilizar posteriormente

para fines de restauración y clonación cuando sea necesario.