Conceptos

SnapCenter Software 5.0

NetApp
July 18, 2024

Tabla de contenidos

Conceptos

Información general de SnapCenter

El software SnapCenter es una plataforma sencilla, centralizada y escalable que proporciona protección de datos consistente con las aplicaciones para aplicaciones, bases de datos, sistemas de archivos host y máquinas virtuales que se ejecutan en sistemas ONTAP en cualquier parte del cloud híbrido.

SnapCenter aprovecha las tecnologías Snapshot, SnapRestore, FlexClone, SnapMirror y SnapVault de NetApp para proporcionar lo siguiente:

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

SnapCenter incluye tanto SnapCenter Server como plugins individuales ligeros. Es posible automatizar la implementación de plugins en hosts de aplicaciones remotas, programar operaciones de backup, verificación y clonado, y supervisar todas las operaciones de protección de datos.

SnapCenter puede implementarse de las siguientes maneras:

- En las instalaciones para proteger lo siguiente:
  - Datos en sistemas principales de cabinas ONTAP FAS, AFF o All SAN (ASA) y 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
- En las instalaciones, en un cloud híbrido para proteger lo siguiente:
  - Datos en sistemas principales ONTAP FAS, AFF o ASA replicados a Cloud Volumes ONTAP
  - Datos en sistemas principales y secundarios de ONTAP FAS, AFF o ASA y protegidos para el almacenamiento de objetos y archivos en el cloud (mediante la integración de backup y recuperación de datos de BlueXP).
- 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)

SnapCenter incluye las siguientes funciones clave:

- Protección de datos centralizada y coherente con las 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 y sistemas de archivos de host Windows que se ejecutan en sistemas ONTAP.

  La protección de datos también es compatible con otras aplicaciones y bases de datos estándar o

personalizadas, ya que proporciona un marco de trabajo para crear plugins de SnapCenter definidos por el usuario. Esto permite proteger datos para otras aplicaciones y bases de datos desde el mismo panel único. Al aprovechar este marco, NetApp ha lanzado complementos personalizados de SnapCenter para IBM DB2, MongoDB, MySQL, etc. en el almacén de automatización de NetApp.

"Almacén de automatización del almacenamiento de NetApp"

- Backups basados en normativas

  Los backups basados en políticas aprovechan la tecnología Snapshot de NetApp para crear backups a disco rápidos, con gestión eficiente del espacio y consistentes con las aplicaciones. De manera opcional, puede automatizar la protección de estos backups en el almacenamiento secundario mediante las actualizaciones de las relaciones de protección existentes.

- Realice backups para varios recursos

  Puede realizar el backup de varios recursos (aplicaciones, bases de datos o sistemas de archivos de host) del mismo tipo, al mismo tiempo, mediante 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 un clonado rápido y coherente con las aplicaciones que gestiona el espacio de manera eficiente, lo que permite un desarrollo de software acelerado. Puede clonar en cualquier destino en el cloud híbrido.

- Interfaz gráfica de usuario (GUI) de gestión de usuario única

  La interfaz gráfica de usuario de SnapCenter proporciona una interfaz única y única para gestionar backups y clones de un recurso en cualquier destino en el cloud híbrido.

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

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

  Para obtener más información sobre las API de REST, consulte "Información general de la API de REST".

  Para obtener más información sobre cmdlets de Windows, consulte "Guía de referencia de cmdlets de SnapCenter Software".

  Para obtener más información sobre los comandos de UNIX, consulte "Guía de referencia de comandos del software SnapCenter".

- Consola de protección de datos y generación de informes centralizadas
- Control de acceso basado en roles (RBAC) para seguridad y delegación.
- Base de datos del repositorio con alta disponibilidad

  SnapCenter proporciona una base de datos de repositorio integrada con alta disponibilidad para almacenar todos los metadatos de backups.

- Instalación mediante inserción automatizada de plug-ins

  Puede automatizar una inserción remota de los plugins de SnapCenter desde el host del servidor de SnapCenter a los hosts de aplicaciones.

- Alta disponibilidad

  La alta disponibilidad de SnapCenter se configura usando el equilibrador de carga externo (F5). Se admiten hasta dos nodos en el mismo centro de datos.

- Recuperación ante desastres (DR)

  Puede recuperar el servidor SnapCenter en caso de desastres como daños en los recursos o bloqueo del servidor.

- SnapLock

  SnapLock es una solución de cumplimiento de alto rendimiento para organizaciones que utilizan almacenamiento WORM para conservar los ficheros en un formato sin modificar para cumplir las normativas y el gobierno.

  Para obtener más información sobre SnapLock, consulte "Qué es SnapLock"

- Continuidad del negocio de SnapMirror (SM-BC)

  SnapMirror Business Continuity (SM-BC) permite que los servicios empresariales sigan funcionando incluso si se produce un fallo completo en el 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 SM-BC.

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

  Para obtener más información sobre SM-BC, consulte "Continuidad del negocio de SnapMirror (SM-BC)"

  Para SM-BC, asegúrese de haber cumplido los diversos requisitos de configuración de hardware, software y sistema. Para obtener más información, consulte "Requisitos previos"

- Mirroring sincrónico

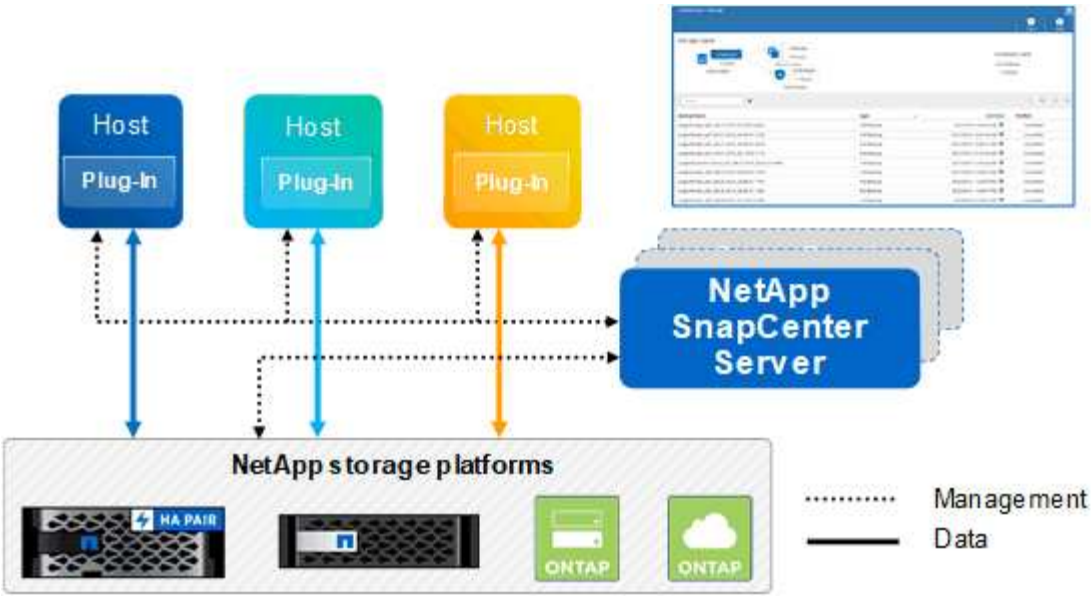
  La función Synchronous Mirroring proporciona la replicación de datos en línea en tiempo real entre las cabinas de almacenamiento a una distancia remota.

  Para obtener más información sobre el espejo de sincronización, consulte "Información general de mirroring síncrono"

Arquitectura SnapCenter

La plataforma de SnapCenter se basa en una arquitectura de varios niveles que incluye un servidor de gestión centralizado (servidor SnapCenter) y un host de complementos de SnapCenter.

SnapCenter admite centros de datos multisitio. El servidor de SnapCenter y el host del plugin pueden estar en diferentes ubicaciones geográficas.



Componentes de SnapCenter

SnapCenter consiste en los plugins de SnapCenter Server y SnapCenter. Debe instalar solo los plugins adecuados para los datos que desea proteger.

- Servidor SnapCenter
- Paquete de plugins de SnapCenter para Windows, que incluye los siguientes plugins:
  - Plugin de SnapCenter para Microsoft SQL Server
  - Plugin de SnapCenter para Microsoft Windows
  - Plugin de SnapCenter para Microsoft Exchange Server
  - Plugin de SnapCenter para base de datos SAP HANA
- Paquete de plugins de SnapCenter para Linux, que incluye los siguientes plugins:
  - Plugin de SnapCenter para base de datos de Oracle
  - Plugin de SnapCenter para base de datos SAP HANA
  - Complemento de SnapCenter para sistemas de archivos UNIX
- Paquete de plugins de SnapCenter para AIX, incluido los siguientes plugins:
  - Plugin de SnapCenter para base de datos de Oracle
  - Complemento de SnapCenter para sistemas de archivos UNIX
- Plugins personalizados de SnapCenter

  Los plugins personalizados poseen soporte de la comunidad y pueden descargarse en el "Almacén de automatización del almacenamiento de NetApp".

El plugin de SnapCenter para VMware vSphere, anteriormente conocido como Data Broker de NetApp, es un dispositivo virtual independiente que admite operaciones de protección de datos de SnapCenter en sistemas de archivos y bases de datos virtualizadas.

Servidor SnapCenter

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 ofrece alta disponibilidad y escalado horizontal entre varias instancias de SnapCenter Server dentro de una sola interfaz de usuario. Puede lograr una alta disponibilidad mediante un equilibrador de carga externo (F5). Para entornos más grandes con miles de hosts, añadir varias instancias de SnapCenter Server puede ayudar a equilibrar la carga.

- Si utiliza el paquete de plugins de SnapCenter para Windows, el agente del host se ejecuta en SnapCenter Server y el host de plugins de Windows. El agente del host ejecuta las programaciones de forma nativa en el host Windows remoto; o bien, para instancias de Microsoft SQL Server, la programación se ejecuta en la instancia de SQL local.

  SnapCenter Server se comunica con los plugins de Windows a través del agente del host.

- Si utiliza el paquete de plugins de SnapCenter para Linux o el paquete de plugins de SnapCenter para AIX, las programaciones se ejecutan en SnapCenter Server como programaciones de tareas de Windows.
  - Para el plugin de SnapCenter para bases de datos de Oracle, el agente del host que se ejecuta en el host del servidor SnapCenter se comunica con el cargador de plugins (SPL) de SnapCenter que se ejecuta en el host Linux o AIX para realizar distintas operaciones de protección de datos.
  - Para el plugin de SnapCenter para bases de datos de SAP HANA y los plugins personalizados de SnapCenter, el servidor de SnapCenter se comunica con estos plugins a través del agente SCCore que se ejecuta en el host.

SnapCenter Server y los plugins se comunican con el agente del host mediante HTTPS. La información sobre las operaciones de SnapCenter se almacena en el repositorio de SnapCenter.

SnapCenter admite espacios de nombres separados para hosts Windows. Si tiene problemas al utilizar un espacio de nombres separado, consulte "SnapCenter no puede detectar recursos al utilizar espacios de nombres separados".

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 para SQL Server	Paquete de plugins para Windows	Plugin para Windows	Host SQL Server	Windows
Plugin para Windows	Paquete de plugins para Windows		Host Windows	Windows
Plugin para Exchange	Paquete de plugins para Windows	Plugin para Windows	Host Exchange Server	Windows

Nombre de complemento	Incluido en el paquete de instalación	Requiere otros plugins	Instalado en el host	Plataforma compatible
Plugin para base de datos de Oracle	Paquete de plugins para Linux y paquete de plugins para AIX	Complemento para UNIX	Host Oracle	Linux o AIX
Plugin 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
Plugins personalizados	"Almacén de automatización del almacenamiento de NetApp"	Para backups del sistema de archivos, plugin para Windows	Host de aplicación personalizada	Linux o Windows

El plugin de SnapCenter para VMware vSphere admite operaciones de backup y restauración consistentes con los fallos y consistentes con las máquinas virtuales (VM), almacenes de datos y discos de máquina virtual (VMDK), y admite los plugins específicos para aplicaciones de SnapCenter para proteger operaciones de backup y restauración consistentes con las aplicaciones para bases de datos y sistemas de archivos virtualizados.

Para los usuarios de SnapCenter 4.1.1, la documentación del plugin de SnapCenter para VMware vSphere 4.1.1 tiene información sobre la protección de las bases de datos y los sistemas de archivos virtualizados. Para los usuarios de SnapCenter 4.2.x, la documentación de NetApp Data Broker 1.0 y 1.0.1 ofrece información sobre la protección de bases de datos y sistemas de archivos virtualizados mediante el plugin de SnapCenter para VMware vSphere que proporciona el dispositivo virtual de agente de datos de NetApp basado en Linux (formato de dispositivo virtual abierto). Para usuarios que utilicen SnapCenter 4,3 o posterior, el "Documentación del plugin de SnapCenter para VMware vSphere" tiene información sobre la protección de bases de datos y sistemas de archivos virtualizados que utilizan el dispositivo virtual del plugin de SnapCenter basado en Linux para VMware vSphere (formato de dispositivo abierto).

Funciones del plugin de SnapCenter para Microsoft SQL Server

- Automatiza las operaciones de backup, restauración y clonado para aplicaciones en bases de datos de Microsoft SQL Server en el entorno SnapCenter.
- Admite bases de datos de Microsoft SQL Server en VMDK y LUN de asignación de dispositivo sin formato (RDM) cuando se implementa el plugin de SnapCenter para VMware vSphere y se registra el plugin con SnapCenter
- Admite el aprovisionamiento de solo recursos compartidos SMB. No se ofrece compatibilidad para realizar backups de bases de datos de SQL Server en recursos compartidos de SMB.
- Admite importar backups desde SnapManager para Microsoft SQL Server a SnapCenter.

Funciones del plugin de SnapCenter para Microsoft Windows

- Posibilita la protección de datos para aplicaciones de otros plugins que se ejecutan en hosts Windows en el entorno de SnapCenter

- Automatiza las operaciones de backup, restauración y clonado para aplicaciones en sistemas de archivos de Microsoft en su entorno SnapCenter
- Admite el aprovisionamiento de almacenamiento, la coherencia de Snapshot y la reclamación de espacio para hosts Windows

> El plugin para Windows aprovisiona recursos compartidos SMB y sistemas de archivos Windows en LUN de RDM físicos, pero no admite operaciones de backup para sistemas de archivos Windows en recursos compartidos SMB.

Funciones del plugin de SnapCenter para Microsoft Exchange Server

- Automatiza las operaciones de backup y restauración para aplicaciones en el entorno de SnapCenter para bases de datos y grupos de disponibilidad de bases de datos (DAG) de Microsoft Exchange Server
- Admite servidores Exchange virtualizados en LUN de RDM cuando se implementa el plugin de SnapCenter para VMware vSphere y se registra el plugin con SnapCenter

Funciones del plugin de SnapCenter para bases de datos de Oracle

- Automatiza los backups, las restauraciones, la recuperación, la verificación, el montaje Operaciones de desmontaje y clonado de bases de datos de Oracle en el entorno de SnapCenter
- Sin embargo, no se proporciona integración con BR*Tools de SAP admite bases de datos Oracle para SAP

Características del plugin de SnapCenter para UNIX

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

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

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

Funciones del plugin de SnapCenter para base de datos SAP HANA

- Automatiza el backup, la restauración y la clonado de bases de datos de SAP HANA en su entorno SnapCenter

Funciones de los plugins personalizados de SnapCenter

- Admite plugins personalizados para gestionar aplicaciones o bases de datos que otros plugins de

SnapCenter no admiten. No se incluyen los plugins personalizados como parte de la instalación de SnapCenter.

- Admite la creación de copias reflejadas de conjuntos de backup en otro volumen y la ejecución de la replicación de backup de disco a disco.
- Es compatible con entornos Windows y Linux. En los entornos de Windows, las aplicaciones personalizadas a través de plugins personalizados pueden utilizar, opcionalmente, el plugin de SnapCenter para Microsoft Windows con el fin de realizar backups consistentes del sistema de archivos.

Los ejemplos de plugins personalizados de MySQL, DB2 y MongoDB para software de SnapCenter se pueden descargar de la "Almacén de automatización del almacenamiento de NetApp".

Los plugins personalizados de MySQL, DB2 y MongoDB reciben soporte exclusivamente a través de las comunidades de NetApp.

NetApp admite la funcionalidad de crear y utilizar plugins personalizados; sin embargo, los plugins personalizados que usted crea no son compatibles con NetApp.

Para obtener más información, consulte "Desarrolle un complemento para la aplicación"

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 base de datos del repositorio de MySQL Server se instala de manera predeterminada cuando se instala el servidor SnapCenter. Si MySQL Server ya está instalado y está realizando una instalación nueva de SnapCenter Server, deberá desinstalar MySQL Server.

SnapCenter admite MySQL Server 5.7.25 o posterior como base de datos del repositorio de SnapCenter. Si utilizaba una versión anterior de MySQL Server con una versión anterior de SnapCenter, durante la actualización de SnapCenter, se actualizó el servidor MySQL a la versión 5.7.25 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

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).

- SnapCenter utiliza algoritmos de seguridad que cumplen con el estándar de procesamiento de información federal (FIPS).
- SnapCenter admite el uso de certificados de CA autorizados que proporciona el cliente.
- SnapCenter 4.1.1 o versiones posteriores son compatibles con la seguridad de la capa de transporte (TLS) 1,2 para la comunicación con ONTAP. También puede usar TLS 1,2 para la comunicación entre clientes y servidores.

  Desde 5,0, SnapCenter admite (TLS) 1,3 para la comunicación con ONTAP.

- SnapCenter admite un conjunto determinado de conjuntos de claves de cifrado SSL para proporcionar seguridad a través de la comunicación de red.

  Para obtener más información, consulte "Cómo configurar el conjunto de claves de cifrado SSL".

- 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 o más intentos incorrectos de inicio de sesión.
- Es compatible con 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 activar MFA, consulte "Active la autenticación multifactor".

Control de acceso basado en roles (RBAC) de SnapCenter

Tipos de RBAC

El control de acceso basado en roles (RBAC) de SnapCenter y los permisos de ONTAP permiten que los administradores de SnapCenter delegen el control de los recursos de SnapCenter a diferentes usuarios o grupos de usuarios. Este acceso con gestión central otorga a los administradores de aplicaciones la posibilidad de trabajar con seguridad dentro de entornos delegados.

Es posible crear y modificar roles, y añadir acceso a recursos para usuarios en cualquier momento, pero cuando configura SnapCenter por primera vez, debe añadir al menos usuarios o grupos de Active Directory a roles, y luego añadir acceso a recursos para esos usuarios o grupos.

No se puede usar SnapCenter para cuentas de usuarios o grupos. Creó cuentas de usuario o de grupo en Active Directory mediante el sistema operativo o la base de datos.

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

- RBAC de SnapCenter
- RBAC para plugin de SnapCenter (para algunos plugins)
- RBAC en el nivel de aplicaciones
- Permisos de ONTAP

RBAC de SnapCenter

Roles y permisos

SnapCenter incluye roles predefinidos con permisos ya asignados. Es posible asignar usuarios o grupos de usuarios a estos roles. También es posible crear nuevos roles y gestionar los permisos y los usuarios.

Asignación de permisos a usuarios o grupos

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. No es posible cambiar los permisos del rol SnapCenterAdmin.

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.

> Si se crea un rol personalizado, este debe contener todos los permisos del rol SnapCenter Admin. Si solo se copian algunos de los permisos, como Host add o Host remove, no se pueden ejecutar tales operaciones.

Autenticación

Los usuarios deben proporcionar autenticación durante el inicio de sesión, ya sea desde la interfaz gráfica de usuario o mediante cmdlets de PowerShell. Si un usuario es parte de más de un rol, después de introducir las credenciales de inicio de sesión, se le solicita que especifique el rol que desea usar. Los usuarios también deben proporcionar autenticación para ejecutar las 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 ejecutar operaciones de Snapshot y protección de datos en un entorno de SQL Server, se deben configurar las credenciales con las credenciales de Windows o SQL correspondientes. El servidor de SnapCenter autentica el conjunto de credenciales con cualquiera de estos métodos. Para ejecutar operaciones de Snapshot y protección de datos en un entorno de sistema de archivos de Windows sobre almacenamiento ONTAP, el rol SnapCenter Admin debe tener privilegios de administrador en el host de Windows.

Del mismo modo, si se desean ejecutar operaciones de protección de datos en una base de datos de Oracle y la autenticación del sistema operativo está deshabilitada en el host de base de datos, se deben configurar las credenciales con la base de datos de Oracle o las credenciales de ASM de Oracle. El servidor de SnapCenter autentica el conjunto de credenciales mediante 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 SnapCenter de VMware es compatible con el control de acceso basado en roles de vCenter Server y de Data ONTAP.

Para obtener más información, consulte "Control de acceso basado en roles del plugin de SnapCenter para VMware vSphere"

Permisos de ONTAP

Es necesario crear una cuenta de vsadmin con los permisos requeridos para acceder al sistema de almacenamiento.

Para obtener información sobre cómo crear la cuenta y asignar permisos, consulte "Cree un rol de clúster de ONTAP con privilegios mínimos"

Permisos y roles de RBAC

El control de acceso basado en roles de SnapCenter permite crear roles y asignar permisos a esos roles para luego asignar usuarios o grupos de usuarios a ellos. Esto permite que los administradores de SnapCenter creen un entorno gestionado de manera centralizada, mientras que los administradores de aplicaciones pueden gestionar trabajos de protección de datos. SnapCenter se envía con algunos roles y permisos predefinidos.

Roles de SnapCenter

SnapCenter se envía con los siguientes roles predefinidos. Es posible asignar usuarios y grupos a estos roles, o bien crear roles nuevos.

Cuando se asigna un rol a un usuario, solo los trabajos relevantes para ese usuario son visibles en la página Jobs, a menos que se haya asignado el rol SnapCenter Admin.

- App Backup y Clone Admin
- Backup y Clone Viewer
- Administrador de infraestructuras
- Administrador de SnapCenter

Roles del plugin de SnapCenter para VMware vSphere

Para gestionar la protección de datos coherente con las máquinas virtuales de máquinas virtuales, VMDK y almacenes de datos, el plugin de SnapCenter para VMware vSphere crea los siguientes roles en vCenter:

- Administrador de SCV
- Vista de VCS
- Backup de SCV
- Restauración de SCV
- Restauración de archivos invitados de SCV

Para obtener más información, consulte "Tipos de RBAC para usuarios del plugin de SnapCenter para VMware vSphere"

Mejor práctica: NetApp recomienda crear un rol de ONTAP para las operaciones del plugin de SnapCenter para VMware vSphere y asignarle todos los privilegios necesarios.

Permisos de SnapCenter

SnapCenter otorga los siguientes permisos:

- Grupo de recursos
- Política
- Backup
- Host
- Conexión de almacenamiento
- Clonar
- Aprovisionamiento (solo para bases de datos Microsoft SQL)
- Consola
- Leídos
- Restaurar
  - Restauración de volúmenes completa (solo para plugins personalizados)
- Recurso

  El administrador debe otorgar privilegios de plugins para que los no administradores realicen operaciones de detección de recursos.
- Instalar o desinstalar plugins

  Cuando habilita los permisos de instalación de plugins, también debe modificar el permiso del host para permitir lecturas y actualizaciones.
- Migración
- Montaje (solo para bases de datos de Oracle)
- Desmontaje (solo para bases de datos de Oracle)
- Monitor de trabajos

  El permiso Monitor de trabajo permite a los miembros de diferentes roles ver las operaciones en todos los objetos a los que están asignados.

Roles y permisos predefinidos de SnapCenter

SnapCenter incluye de forma predeterminada varios roles predefinidos, cada uno con un conjunto de permisos ya habilitados. Al configurar y administrar el control de acceso basado en roles, se pueden usar estos roles predefinidos o crear roles nuevos.

SnapCenter incluye los siguientes roles predefinidos:

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

Cuando se agrega un usuario a un rol, se le debe asignar el permiso StorageConnection para permitir la comunicación con Storage Virtual Machine (SVM) o asignarle una SVM al usuario para habilitar su uso. El permiso Storage Connection permite que los usuarios creen conexiones de SVM.

Por ejemplo, un usuario con el rol SnapCenter Admin puede crear conexiones de SVM y asignarlas a un usuario con el rol App Backup and Clone Admin, cuyos permisos predeterminados no incluyen la creación o edición de SVM. Si no hay una conexión de SVM, los usuarios no pueden ejecutar ninguna operación de backup, clonado 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
Instalar/desinstalar plugins	No	No aplicable		No aplicable	No aplicable

Permisos	Activado	Cree	Lea	Actualizar	Eliminar
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
Monitor de trabajos	Sí	No aplicable	No aplicable	No aplicable	No aplicable

Backup and Clone Viewer

El rol Backup and Clone Viewer tiene una vista de solo lectura de todos los permisos. Este rol también tiene permisos habilitados para detección, generación de informes y acceso a la consola.

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
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

Permisos	Activado	Cree	Lea	Actualizar	Eliminar
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
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
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

Permisos	Activado	Cree	Lea	Actualizar	Eliminar
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
Monitor de trabajos	Sí	No aplicable	No aplicable	No aplicable	No aplicable

Recuperación ante desastres de SnapCenter

Es posible recuperar el servidor de SnapCenter en caso de desastres como daños en los recursos o fallos del servidor mediante la función de recuperación ante desastres (DR) de SnapCenter. Es posible recuperar el repositorio de SnapCenter, las programaciones de servidores y los componentes de configuración del servidor. También puede recuperar el plugin de SnapCenter para SQL Server y el plugin de SnapCenter para el almacenamiento de SQL Server.

En esta sección se describen los dos tipos de recuperación ante desastres (DR) de 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.
- Para la autenticación multifactor (MFA), durante la recuperación ante desastres del servidor de SnapCenter, cierre todas las pestañas del explorador y vuelva a abrir un navegador 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 usa API DE REST para hacer backups de SnapCenter Server. Consulte "Flujos de trabajo de API de REST para la recuperación ante desastres de SnapCenter Server".
- No se realiza una copia de seguridad del archivo de configuración relacionado con la configuración de auditoría en un backup de la 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

DR solo es compatible con el plugin de SnapCenter para SQL Server. Cuando el plugin de SnapCenter para SQL Server está inactivo, cambie a un host SQL diferente y recupere los datos mediante unos pasos. Consulte "Recuperación ante desastres del plugin de SnapCenter para SQL Server".

SnapCenter utiliza la tecnología SnapMirror de ONTAP para replicar datos. Se puede utilizar para replicar datos en un sitio secundario a fin de realizar tareas de recuperación ante desastres y mantenerlos sincronizados. Es posible iniciar una conmutación por error rompiendo la relación de replicación en SnapMirror. Durante la conmutación por recuperación, es posible revertir la sincronización y volver a replicar los datos del sitio de recuperación ante desastres en la ubicación principal.

Recursos, grupos de recursos y políticas

Antes de usar SnapCenter, es necesariol 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** suelen ser las bases de datos, los sistemas de archivos Windows o los recursos compartidos de archivos de los que se realiza una copia de seguridad o se clonan con SnapCenter.

  No obstante, según cuál sea el entorno, los recursos también pueden ser instancias de bases de datos, grupos de disponibilidad de Microsoft SQL Server, bases de datos de Oracle, base de datos de Oracle RAC, sistemas de archivos Windows o un grupo de aplicaciones personalizadas.

- Un **grupo de recursos** es una colección de recursos en un host o clúster. El grupo de recursos también puede contener recursos de varios hosts y varios clústeres.

  Cuando se ejecuta una operación con un grupo de recursos, esta se aplica a todos los recursos definidos en el grupo de acuerdo con la programación especificada para el grupo de recursos.

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

  > Si se coloca un host de un grupo de recursos compartidos en modo de mantenimiento y existen programaciones asociadas con el mismo grupo, se suspenden todas las operaciones programadas en todos los demás hosts del grupo de recursos compartidos.

  Es conveniente usar un plugin de base de datos para el backup de bases de datos, un plugin de sistema de archivos para el backup de sistemas de archivos y el plugin de SnapCenter para VMware vSphere para el backup de máquinas virtuales y almacenes de datos.

- **Las directivas** especifican la frecuencia de copia de seguridad, la retención de copias, la replicación, las secuencias de comandos y otras características de las operaciones de protección de datos.

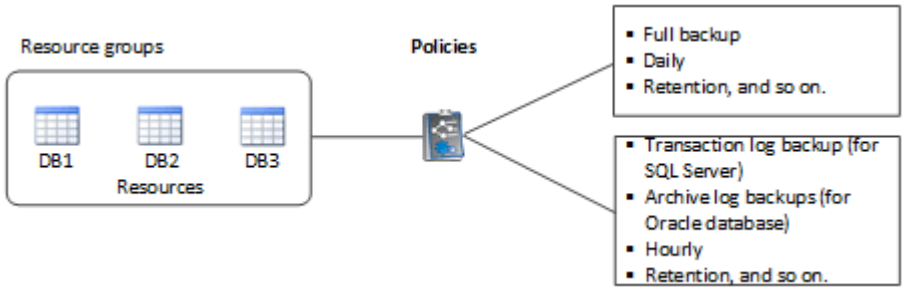
  Cuando se crea un grupo de recursos, se seleccionan una o varias políticas para él. También es posible seleccionar una política al ejecutar un backup bajo demanda.

Piense en un grupo de recursos como definir *qué* desea proteger y cuándo desea protegerlo en términos de

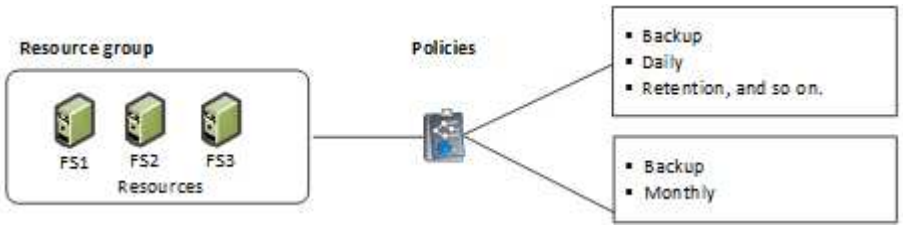
día y hora. Piense en una directiva como definir *how* desea protegerla. Cuando se realiza un backup de todas las bases de datos o todos los sistemas de archivos de un host, por ejemplo, puede crearse un grupo de recursos que incluya todas las bases de datos o todos los sistemas de archivos del host. Luego, se pueden vincular dos políticas al grupo de recursos: Una diaria y una horaria.

Cuando se crea el grupo de recursos y se vinculan las políticas, es posible configurar el grupo de recursos para que se ejecute un backup completo todos los días, y agregar una programación que ejecute un backup del registro por hora.

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



En la siguiente imagen, se muestra la relación entre los recursos, los grupos de recursos y las políticas para los sistemas de archivos Windows:



Scripts previos y posteriores

Es posible usar scripts previos y posteriores como parte de las operaciones de protección de datos. Estos scripts permiten la automatización antes o después del trabajo de protección de datos. Por ejemplo, se puede incluir un script para notificar automáticamente si hay fallos o advertencias en un trabajo de protección de datos. Para configurar scripts previos y posteriores, es necesario comprender algunos de los requisitos para crearlos.

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, en sistemas de almacenamiento virtualizados y no 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.

Automatización de SnapCenter mediante API de REST

Es posible utilizar API DE REST para realizar varias operaciones de gestión de SnapCenter. Las API DE REST se exponen a través de la página web de Swagger. Es posible acceder a la página web de Swagger para ver la documentación de la API DE REST, y también para emitir manualmente una llamada API. Es posible usar la API DE REST para ayudar a gestionar SnapCenter Server o el host de SnapCenter vSphere.

Las API DE REST para…	Se encuentran en…
Servidor SnapCenter	\Https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/Swagger/
Plugin de SnapCenter para VMware vSphere	\Https://<OVA_IP_address_or_host_name>:<scv_plugin_port>/api/swagger-ui.html#

Para obtener información sobre las API DE REST DE SnapCenter, consulte "Información general de las API de REST"

Para obtener información sobre las API DE REST del plugin de SnapCenter para VMware vSphere, consulte "API de REST del plugin de SnapCenter para VMware vSphere"

Información de copyright

Información de la marca comercial