Empezar

NetApp Backup and Recovery

NetApp
February 11, 2026

Tabla de contenidos

Empezar . . . 1
- Obtenga más información sobre NetApp Backup and Recovery . . . 1
  - Qué puede hacer con NetApp Backup and Recovery . . . 1
  - Beneficios de utilizar NetApp Backup and Recovery . . . 3
  - Costo . . . 3
  - Licencias . . . 4
  - Cargas de trabajo, sistemas y objetivos de respaldo compatibles . . . 5
  - Cómo funciona NetApp Backup and Recovery . . . 6
  - Términos que podrían ayudarle con NetApp Backup and Recovery . . . 7
- Requisitos previos de NetApp Backup and Recovery . . . 7
  - Requisito previo para ONTAP 9.8 y versiones posteriores . . . 7
  - Requisitos previos para realizar copias de seguridad en el almacenamiento de objetos . . . 7
  - Requisitos para proteger las cargas de trabajo de Microsoft SQL Server . . . 7
  - Requisitos para proteger las cargas de trabajo de VMware . . . 8
  - Requisitos para proteger las cargas de trabajo de KVM . . . 9
  - Requisitos para proteger las cargas de trabajo de Oracle Database . . . 10
  - Requisitos para proteger las aplicaciones de Kubernetes . . . 10
  - Requisitos para proteger las cargas de trabajo de Hyper-V . . . 11
  - En la NetApp Console . . . 12
- Configurar licencias para NetApp Backup and Recovery . . . 12
  - Prueba gratuita de 30 días . . . 13
  - Utilice una suscripción PAYGO de NetApp Backup and Recovery . . . 14
  - Utilice un contrato anual . . . 14
  - Utilice una licencia BYOL de NetApp Backup and Recovery . . . 15
- Configurar certificados de seguridad para StorageGRID y ONTAP en NetApp Backup and Recovery . . . 16
  - Crear un certificado de seguridad para StorageGRID . . . 16
  - Crear un certificado de seguridad para ONTAP . . . 20
  - Cree un certificado para ONTAP y StorageGRID . . . 23
- Configure destinos de respaldo antes de usar NetApp Backup and Recovery . . . 24
  - Preparar el destino de la copia de seguridad . . . 24
  - Configurar permisos S3 . . . 25
- Inicie sesión en NetApp Backup and Recovery . . . 27
- Descubra los destinos de respaldo externos en NetApp Backup and Recovery . . . 28
  - Descubra un destino de respaldo . . . 28
  - Agregar un depósito para un objetivo de respaldo . . . 29
  - Cambiar las credenciales de un destino de respaldo . . . 31
- Cambiar a diferentes cargas de trabajo de NetApp Backup and Recovery . . . 31
  - Cambiar a una carga de trabajo diferente . . . 31
- Configurar los ajustes de NetApp Backup and Recovery . . . 31
  - Agregar credenciales para los recursos del host . . . 32
  - Mantener la configuración de VMware vCenter . . . 33
  - Importar y administrar recursos del host de SnapCenter . . . 34
  - Agregar una plataforma de administración KVM . . . 36

Configurar directorios de registro en instantáneas para hosts de Windows . . . 36
Crear una plantilla de gancho de ejecución . . . 36
Configura el control de acceso basado en roles en NetApp Backup and Recovery . . . 37
Información relacionada . . . 38

Empezar

Obtenga más información sobre NetApp Backup and Recovery

NetApp Backup and Recovery es un servicio de datos que proporciona protección de datos eficiente, segura y rentable para todas sus cargas de trabajo de ONTAP , incluidos volúmenes, bases de datos, máquinas virtuales y cargas de trabajo de Kubernetes.

El soporte para copias de seguridad y recuperación ya está integrado en todos los sistemas ONTAP , por lo que no se necesita hardware adicional, licencias de software ni puertas de enlace de medios. Esto hace que las operaciones de respaldo sean sencillas y rentables. La NetApp Console simplifica la implementación de cualquier estrategia de respaldo, incluido el espectro completo de variantes de respaldo 3-2-1, sin necesidad de múltiples administradores de recursos o personal especializado.

Se proporciona documentación sobre la protección de cargas de trabajo de VMware, KVM, Hyper-V y Kubernetes como una vista previa de la tecnología. Con esta oferta de vista previa, NetApp se reserva el derecho de modificar los detalles, el contenido y el cronograma de la oferta antes de la disponibilidad general.

Qué puede hacer con NetApp Backup and Recovery

Utilice NetApp Backup and Recovery para lograr los siguientes objetivos:

- * Cargas de trabajo de volumen de ONTAP *:
  - Cree instantáneas locales, replique en almacenamiento secundario y realice copias de seguridad de volúmenes ONTAP desde sistemas ONTAP locales o Cloud Volumes ONTAP al almacenamiento de objetos en su cuenta de nube pública o privada.
  - Cree copias de seguridad incrementales a nivel de bloque y permanentes que se almacenan en otro clúster de ONTAP y en el almacenamiento de objetos en la nube.
  - Utilice NetApp Backup and Recovery junto con SnapCenter.
  - Referirse a"Proteger volúmenes ONTAP" .
- **Cargas de trabajo de Microsoft SQL Server**:
  - Realice copias de seguridad de instancias y bases de datos de Microsoft SQL Server desde ONTAP local, Cloud Volumes ONTAP o Amazon FSx for NetApp ONTAP.
  - Restaurar bases de datos de Microsoft SQL Server.
  - Clonar bases de datos de Microsoft SQL Server.
  - Utilice NetApp Backup and Recovery sin SnapCenter.
  - Referirse a"Proteger las cargas de trabajo de Microsoft SQL Server" .
- **Cargas de trabajo de VMware (versión preliminar con nueva interfaz de usuario sin SnapCenter Plug-in for VMware vSphere)**:
  - Proteja sus máquinas virtuales y almacenes de datos VMware con NetApp Backup and Recovery.
  - Realice copias de seguridad de las cargas de trabajo de VMware en Amazon Web Services S3 o StorageGRID (para vista previa).

- Restaure datos de VMware desde la nube al vCenter local.
- Puede restaurar la máquina virtual en la misma ubicación exacta desde donde se realizó la copia de seguridad o en una ubicación alternativa.
- Utilice NetApp Backup and Recovery sin el SnapCenter Plug-in for VMware vSphere.
- Referirse a"Proteger las cargas de trabajo de VMware" .

- **Cargas de trabajo de VMware (con SnapCenter Plug-in for VMware vSphere)**:
  - Realice copias de seguridad de máquinas virtuales y almacenes de datos en Amazon Web Services S3, Microsoft Azure Blob, Google Cloud Platform y StorageGRID y restaure las máquinas virtuales en el SnapCenter Plug-in for VMware vSphere .
  - Restaure datos de máquinas virtuales desde la nube al vCenter local con NetApp Backup and Recovery. Puede restaurar la máquina virtual en la misma ubicación exacta desde donde se realizó la copia de seguridad o en una ubicación alternativa.
  - Utilice NetApp Backup and Recovery junto con el SnapCenter Plug-in for VMware vSphere.
  - Referirse a"Proteger las cargas de trabajo de VMware" .
- **Cargas de trabajo KVM (Vista previa)**:
  - Realizar copias de seguridad y restaurar máquinas virtuales
  - Realizar copias de seguridad de los grupos de almacenamiento de KVM
  - Utilice grupos de protección para administrar tareas de copia de seguridad
  - Referirse a"Proteja las cargas de trabajo de KVM" .
- **Cargas de trabajo de Hyper-V (versión preliminar)**:
  - Realizar copias de seguridad y restaurar máquinas virtuales
  - Utilice grupos de protección para administrar tareas de copia de seguridad
  - Referirse a"Proteger las cargas de trabajo de Hyper-V" .
- **Cargas de trabajo de Oracle Database (Preview)**:
  - Realizar copias de seguridad y restaurar bases de datos y registros
  - Utilice grupos de protección para administrar tareas de copia de seguridad
  - Crear políticas para administrar copias de seguridad de bases de datos y registros
  - Protección de una base de datos con una arquitectura de copia de seguridad 3-2-1
  - Configurar la retención de copias de seguridad
  - Montar y desmontar copias de seguridad de ARCHIVELOG
  - Consulta "Protege las cargas de trabajo de Oracle Database".
- **Cargas de trabajo de Kubernetes (versión preliminar)**:
  - Administre y proteja sus aplicaciones y recursos de Kubernetes, todo en un solo lugar.
  - Utilice políticas de protección para estructurar sus copias de seguridad incrementales.
  - Restaurar aplicaciones y recursos en los mismos clústeres y espacios de nombres o en clústeres diferentes.
  - Utilice NetApp Backup and Recovery sin SnapCenter.
  - Referirse a"Proteger las cargas de trabajo de Kubernetes" .

Beneficios de utilizar NetApp Backup and Recovery

NetApp Backup and Recovery ofrece los siguientes beneficios:

- **Eficiente**: NetApp Backup and Recovery realiza una replicación incremental permanente a nivel de bloque, lo que reduce significativamente la cantidad de datos que se replican y almacenan. Esto ayuda a minimizar el tráfico de la red y los costos de almacenamiento.
- **Seguro**: NetApp Backup and Recovery cifra los datos en tránsito y en reposo, y utiliza protocolos de comunicación seguros para proteger sus datos.
- **Rentable**: NetApp Backup and Recovery utiliza los niveles de almacenamiento de menor costo disponibles en su cuenta de nube, lo que ayuda a reducir costos.
- **Automatizado**: NetApp Backup and Recovery genera automáticamente copias de seguridad según un programa predefinido, lo que ayuda a garantizar que sus datos estén protegidos.
- **Flexible**: NetApp Backup and Recovery le permite restaurar datos en el mismo sistema o en uno diferente, lo que proporciona flexibilidad en la recuperación de datos.

Costo

NetApp no le cobra por utilizar la versión de prueba. Sin embargo, usted es responsable de los costos asociados con los recursos en la nube que utiliza, como los costos de almacenamiento y transferencia de datos.

Hay dos tipos de costos asociados con el uso de la función de respaldo a objeto de NetApp Backup and Recovery con sistemas ONTAP :

- Cargos por recursos
- Cargos por servicio

No se cobra ninguna tarifa por crear instantáneas o volúmenes replicados, aparte del espacio en disco necesario para almacenar las instantáneas y los volúmenes replicados.

Cargos por recursos

Los cargos por recursos se pagan al proveedor de la nube por la capacidad de almacenamiento de objetos y por escribir y leer archivos de respaldo en la nube.

- Para realizar copias de seguridad en almacenamiento de objetos, usted paga a su proveedor de nube los costos de almacenamiento de objetos.

  Debido a que NetApp Backup and Recovery preserva las eficiencias de almacenamiento del volumen de origen, usted paga al proveedor de la nube los costos de almacenamiento de objetos por los datos *después* de las eficiencias de ONTAP (para la menor cantidad de datos después de que se hayan aplicado la deduplicación y la compresión).

- Para restaurar datos mediante Búsqueda y restauración, su proveedor de nube proporciona ciertos recursos y existe un costo por TiB asociado con la cantidad de datos escaneados por sus solicitudes de búsqueda. (Estos recursos no son necesarios para Explorar y restaurar).
  - En AWS, "Amazona Atenea" y "Pegamento de AWS" Los recursos se implementan en un nuevo bucket S3.
  - En Azure, un "Área de trabajo de Azure Synapse" y "Almacenamiento de Azure Data Lake" Se aprovisionan en su cuenta de almacenamiento para almacenar y analizar sus datos.

    - En Google, se implementa un nuevo depósito y el "Servicios de Google Cloud BigQuery" se aprovisionan a nivel de cuenta/proyecto.
- Si planea restaurar datos de volumen desde un archivo de respaldo que se ha movido al almacenamiento de objetos de archivo, entonces hay una tarifa de recuperación adicional por GiB y una tarifa por solicitud del proveedor de la nube.
- Si planea escanear un archivo de respaldo en busca de ransomware durante el proceso de restauración de datos de volumen (si habilitó DataLock y Ransomware Resilience para sus copias de seguridad en la nube), también incurrirá en costos de salida adicionales de su proveedor de la nube.

Cargos por servicio

Para las cargas de trabajo de volumen de ONTAP , solo se le cobrará por los volúmenes protegidos por el almacenamiento de objetos. Los cargos se basan en la capacidad lógica utilizada de los volúmenes ONTAP de origen antes de que se apliquen las eficiencias, también conocidas como Terabytes Front-End (FETB).

Para cargas de trabajo de Kubernetes, se te cobrará según el tamaño combinado de todos los volúmenes persistentes.

Para todas las demás cargas de trabajo, se le cobrará por los recursos protegidos en al menos un destino de almacenamiento de objetos o secundario. Los cargos se calculan utilizando el tamaño lógico de la carga de trabajo de origen. Para las bases de datos, esto significa el tamaño de la base de datos; para las máquinas virtuales, el tamaño de la máquina virtual.

Hay tres formas de pagar por Backup and Recovery:

- La primera opción es suscribirse a través de su proveedor de nube, lo que le permite pagar por mes.
- La segunda opción es comprar un contrato anual.
- La tercera opción es comprar licencias directamente de NetApp. Consulte la Licencias Sección para más detalles.

Licencias

NetApp Backup and Recovery ofrece una prueba gratuita que le permite usarlo sin una clave de licencia durante un tiempo limitado.

Una licencia de Backup solo es necesaria para las operaciones de copia de seguridad y restauración que impliquen almacenamiento de objetos. La creación de instantáneas y volúmenes replicados no requiere licencia.

Puedes elegir entre tres opciones de licencia:

- **Traiga su propia licencia (BYOL)**: Compre una licencia basada en plazos (1, 2 o 3 años) y en capacidad (en incrementos de 1 TiB) de NetApp. Introduzca el número de serie proporcionado en la NetApp Console para activarlo. La licencia cubre todos los sistemas fuente de su organización. La renovación es obligatoria cuando se alcanza el plazo o el límite de capacidad.
- **Pago por uso (PAYGO)**: Suscríbase a través del mercado de su proveedor de nube y pague por GiB de datos respaldados, con facturación mensual. No se requiere pago por adelantado. Al registrarte por primera vez, tienes disponible una prueba gratuita de 30 días. Para obtener más información, consulte "Utilice una suscripción de pago por uso de NetApp Backup and Recovery." .
- **Contrato anual**: Disponible a través de los marketplaces de AWS y Azure por 1, 2 o 3 años. Hay dos contratos anuales disponibles:

- **Copia de seguridad en la nube**: Realiza copias de seguridad de los Cloud Volumes ONTAP y de los datos de ONTAP locales.
- **CVO Professional**: Incluye Cloud Volumes ONTAP y NetApp Backup and Recovery, con copias de seguridad ilimitadas para volúmenes de Cloud Volumes ONTAP (la capacidad de copia de seguridad no se contabiliza en la licencia).
  - Con el plan CVO Professional, existen dos tipos de cargos:
    - **Cargos por recursos**: Basados en el uso del almacenamiento. Para obtener más información, consulte "Licencias para Cloud Volumes ONTAP" .
    - **Cargos por servicio**: Tarifas por NetApp Backup and Recovery. Sin embargo, si el volumen de origen se encuentra en un sistema de almacenamiento que utiliza el plan CVO Professional, NetApp Backup and Recovery se proporciona de forma gratuita.

Cuando utilice Google Cloud Platform, solicite una oferta privada a NetApp y seleccione su plan durante la activación en Google Cloud Marketplace.

"Aprenda a configurar licencias".

Cargas de trabajo, sistemas y objetivos de respaldo compatibles

Cargas de trabajo admitidas

NetApp Backup and Recovery protege los siguientes tipos de cargas de trabajo:

- Volúmenes de ONTAP
- Instancias y bases de datos de Microsoft SQL Server almacenadas en un disco físico y VMware Virtual Machine Disk (VMDK) a través de VMFS o NFS
- Máquinas virtuales y almacenes de datos de VMware
- Cargas de trabajo KVM (Vista previa)
- Cargas de trabajo de Hyper-V (versión preliminar)
- Cargas de trabajo de Oracle Database (versión preliminar)
- Cargas de trabajo de Kubernetes (versión preliminar)

Sistemas compatibles

- SAN ONTAP local (protocolo iSCSI) y NAS (mediante protocolos NFS y CIFS) con ONTAP versión 9.8 o superior
- Cloud Volumes ONTAP 9.8 o superior para AWS (usando SAN y NAS)
- Cloud Volumes ONTAP 9.8 o superior para Google Cloud Platform (utilizando protocolos NFS y CIFS)
- Cloud Volumes ONTAP 9.8 o superior para Microsoft Azure (usando SAN y NAS)
- Amazon FSx for NetApp ONTAP (solo cargas de trabajo de Microsoft SQL Server)

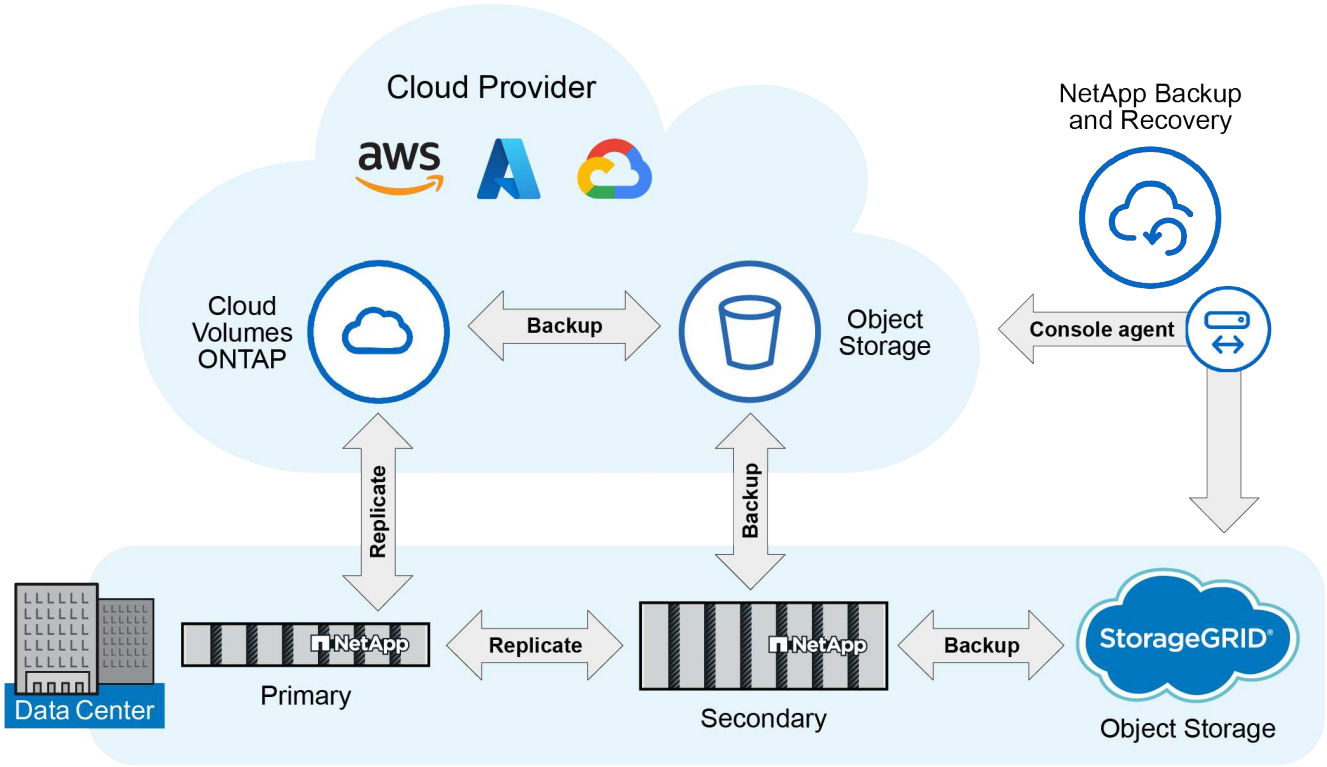
Destinos de copia de seguridad compatibles

- Servicios web de Amazon (AWS) S3
- Almacenamiento en la nube de Google
- Microsoft Azure Blob (no disponible para cargas de trabajo de VMware en versión preliminar)
- StorageGRID
- ONTAP S3 (no disponible para cargas de trabajo de VMware en versión preliminar)

Cómo funciona NetApp Backup and Recovery

Cuando habilita NetApp Backup and Recovery, el servicio realiza una copia de seguridad completa de sus datos. Después de la copia de seguridad inicial, todas las copias de seguridad adicionales son incrementales. Esto mantiene el tráfico de red al mínimo.

La siguiente imagen muestra la relación entre los componentes.



También se admite el paso del almacenamiento primario al almacenamiento de objetos, no solo del almacenamiento secundario al almacenamiento de objetos.

Dónde residen las copias de seguridad en las ubicaciones del almacén de objetos

Las copias de seguridad se almacenan en un almacén de objetos que la NetApp Console crea en su cuenta en la nube. Hay un almacén de objetos por clúster o sistema, y la consola nombra el almacén de objetos de la siguiente manera: `netapp-backup-clusteruuid` . Asegúrese de no eliminar este almacén de objetos.

- En AWS, la NetApp Console permite "Función de acceso público bloqueado de Amazon S3" en el cubo S3.
- En Azure, la NetApp Console utiliza un grupo de recursos nuevo o existente con una cuenta de almacenamiento para el contenedor de blobs. "bloquea el acceso público a sus datos de blobs" por defecto.
- En StorageGRID, la consola utiliza una cuenta de almacenamiento existente para el depósito de almacenamiento de objetos.
- En ONTAP S3, la consola utiliza una cuenta de usuario existente para el bucket S3.

Las copias de seguridad están asociadas con su organización de la NetApp Console

Las copias de seguridad están asociadas con la organización de la NetApp Console en la que reside el agente de la consola. "Obtenga más información sobre la identidad y el acceso a la NetApp Console" .

Si tiene varios agentes de consola en la misma organización de NetApp Console , cada agente de consola muestra la misma lista de copias de seguridad.

Términos que podrían ayudarle con NetApp Backup and Recovery

Podría resultarle beneficioso comprender algunos términos relacionados con la protección.

- **Protección**: La protección en NetApp Backup and Recovery significa garantizar que se realicen instantáneas y copias de seguridad inmutables de forma periódica en un dominio de seguridad diferente mediante políticas de protección.
- **Carga de trabajo**: una carga de trabajo en NetApp Backup and Recovery puede incluir volúmenes ONTAP , instancias y bases de datos de Microsoft SQL Server; máquinas virtuales y almacenes de datos de VMware; o aplicaciones y clústeres de Kubernetes.

Requisitos previos de NetApp Backup and Recovery

Comience a utilizar NetApp Backup and Recovery verificando la preparación de su entorno operativo, el agente de la NetApp Console y la cuenta de la NetApp Console . Para utilizar NetApp Backup and Recovery, necesitará estos requisitos previos.

Requisito previo para ONTAP 9.8 y versiones posteriores

Se debe habilitar una licencia de ONTAP One en la instancia de ONTAP local.

Requisitos previos para realizar copias de seguridad en el almacenamiento de objetos

Para utilizar el almacenamiento de objetos como destino de respaldo, necesita una cuenta con AWS S3, Microsoft Azure Blob, StorageGRID u ONTAP y los permisos de acceso adecuados configurados.

- "Proteja sus datos de volumen de ONTAP"

Requisitos para proteger las cargas de trabajo de Microsoft SQL Server

Para utilizar NetApp Backup and Recovery para cargas de trabajo de Microsoft SQL Server, necesita los siguientes requisitos previos de tamaño, espacio y sistema host.

Artículo	Requisitos
Sistemas operativos	Microsoft Windows Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp" .
Versiones de Microsoft SQL Server	Las versiones 2012 y posteriores son compatibles con VMware Virtual Machine File System (VMFS) y VMware Virtual Machine Disk (VMDK) NFS.

Artículo	Requisitos
Versión del servidor SnapCenter	Se requiere la versión 5.0 o superior de SnapCenter Server si va a importar sus datos existentes de SnapCenter a NetApp Backup and Recovery. Si ya tiene SnapCenter, primero verifique que cumple con los requisitos previos antes de importar desde SnapCenter. Ver"Requisitos previos para importar recursos desde SnapCenter" .
RAM mínima para el complemento en el host de SQL Server	1 GB
Espacio mínimo de instalación y registro para el complemento en el host de SQL Server	5 GB Asigne suficiente espacio en disco y supervise el consumo de almacenamiento de la carpeta de registros. El espacio de registro necesario varía según la cantidad de copias de seguridad realizadas y la frecuencia de las operaciones de protección de datos. Si no hay suficiente espacio, no se crearán los registros para las operaciones.
Paquetes de software necesarios	• Paquete de alojamiento de ASP.NET Core Runtime 8.0.12 (y todos los parches 8.0.x posteriores) • PowerShell 7.4.2 Para obtener la información más reciente sobre las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad de NetApp" .

Requisitos para proteger las cargas de trabajo de VMware

Necesita requisitos específicos para descubrir y proteger sus cargas de trabajo de VMware.

Soporte de software

- Se admiten los almacenes de datos NFS y VMFS.
- Versiones de NFS compatibles: NFS 3 y NFS 4.1
- Versiones de VMware ESXi Server compatibles: 7.0U1 y superiores
- Versiones de VMware vCenter vSphere compatibles: 7.0U1 y superiores
- Direcciones IP: IPv4 e IPv6
- VMware TLS: 1.2, 1.3
- Almacenamiento conectado compatible: ONTAP 9.13 o posterior

Requisitos de conexión y puerto para proteger las cargas de trabajo de VMware

Tipo de puerto	Puerto preconfigurado
Puerto del servidor VMware ESXi	443 (HTTPS), bidireccional. La función de restauración de archivos invitados utiliza este puerto.
Clúster de almacenamiento o puerto de máquina virtual de almacenamiento	443 (HTTPS), bidireccional. 80 (HTTP), bidireccional. Este puerto se utiliza para la comunicación entre el dispositivo virtual y la máquina virtual de almacenamiento o el clúster que contiene la máquina virtual de almacenamiento.

Requisitos de control de acceso basado en roles (RBAC) para proteger las cargas de trabajo de VMware

La cuenta de administrador de vCenter debe tener los privilegios de vCenter necesarios.

Para obtener una lista de los privilegios de vCenter necesarios, consulte "SnapCenter Plug-in for VMware vSphere Se necesitan privilegios de vCenter" .

Requisitos para proteger las cargas de trabajo de KVM

Necesita requisitos específicos para descubrir y proteger máquinas virtuales KVM.

- Una distribución de Linux moderna que ejecuta la versión del kernel 5.14.0-503.22.1.el9_5.x86_64 (a largo plazo) o posterior
- Sus hosts KVM y máquinas virtuales deben estar administrados por una plataforma de administración. NetApp Backup and Recovery admite las siguientes plataformas de administración:
  - Apache CloudStack 4.22.0.0
- Asegúrese de que el tráfico de red entrante al puerto 22 esté permitido desde el agente de la consola al host KVM
- Agente invitado QEMU versión 9.0.0 o posterior
- libvirt versión 10.5.0 o posterior

Para garantizar que las restauraciones de la carga de trabajo de KVM se completen correctamente, asegúrese de que la configuración **Habilitar instantánea consistente con VM** esté activa en la política de protección que utiliza para las copias de seguridad de KVM.

Para habilitar la protección de las máquinas virtuales KVM administradas por usuarios sin privilegios de administrador, siga los siguientes pasos:

1. Monta el volumen como tipo NFS3 para evitar el uso de `nobody` usuario y grupo.
2. Utilice el siguiente comando para agregar un usuario sin privilegios de administrador al `qemu` grupo preservando sus grupos existentes:

```
usermod -aG qemu <non-root-user>
```

3. Utilice el siguiente comando para otorgar la propiedad de la ruta de montaje al `qemu` Usuario y grupo, y cambiar permisos para la ruta de montaje:

```
chown -R qemu:qemu <kvm_vm_mount_path> & chmod 771
<kvm_vm_mount_path>
```

4. Elimine el directorio NetApp_SnapCenter_Backups existente, si lo hubiera.

Requisitos para proteger las cargas de trabajo de Oracle Database

Asegúrese de que su entorno cumpla con los requisitos específicos para descubrir y proteger los recursos de Oracle.

- Base de datos Oracle:
  - Oracle 19C y 21C son compatibles en una implementación independiente.
  - La base de datos Oracle debe implementarse en el almacenamiento NetApp ONTAP primario o secundario.
  - Compatibilidad con SO host: Red Hat Enterprise Linux 8 y 9
- Soporte de almacenamiento de objetos:
  - Almacenamiento de objetos de Azure
  - Amazon AWS
  - StorageGRID en NetApp
  - ONTAP S3

Requisitos para proteger las aplicaciones de Kubernetes

Necesita requisitos específicos para descubrir recursos de Kubernetes y proteger sus aplicaciones de Kubernetes.

Para conocer los requisitos de la NetApp Console , consulteEn la NetApp Console .

- Un sistema ONTAP primario (ONTAP 9.16.1 o posterior)
- Un clúster de Kubernetes: las distribuciones y versiones de Kubernetes compatibles incluyen:
  - Anthos On-Prem (VMware) y Anthos en hardware 1.16
  - Kubernetes 1.27 - 1.33

    - OpenShift 4.10 - 4.18
    - Rancher Kubernetes Engine 2 (RKE2) v1.26.7+rke2r1, v1.28.5+rke2r1
    - Suse Rancher
- NetApp Trident 24.10 o posterior
- NetApp Trident Protect 25.07 o posterior (instalado durante el descubrimiento de cargas de trabajo de Kubernetes)
- NetApp Trident Protect Connector 25.07 o posterior (instalado durante el descubrimiento de cargas de trabajo de Kubernetes)
    - Asegúrate de que el puerto TCP 443 no esté filtrado en la dirección de salida entre el clúster de Kubernetes, el Trident Protect Connector y el Trident Protect proxy.

Requisitos para proteger las cargas de trabajo de Hyper-V

Asegúrese de que su instancia de Hyper-V cumpla con los requisitos específicos para descubrir y proteger máquinas virtuales.

- Requisitos de software para el host de Windows Server Hyper-V:
    - Ediciones de Microsoft Hyper-V 2019, 2022 y 2025
    - Paquete de alojamiento de ASP.NET Core Runtime 8.0.12 (y todos los parches 8.0.x posteriores)
    - PowerShell 7.4.2 o posterior
    - Si usuarios que no forman parte de un dominio de administrador van a proteger máquinas virtuales Hyper-V, asegúrese de que el usuario tenga los siguientes permisos:
        - Asegúrese de que el usuario sea miembro del grupo de administradores locales.
        - Asegúrese de que el usuario forme parte de la política de seguridad local "Iniciar sesión como servicio".
    - Asegúrese de que el tráfico HTTPS bidireccional esté permitido para los siguientes puertos en la configuración del Firewall de Windows:
        - 8144 (complemento de NetApp para Hyper-V)
        - 8145 (complemento de NetApp para Windows)
- Requisitos de hardware para el host Hyper-V:
    - Se admiten hosts independientes y agrupados en FCI
    - 1 GB de RAM como mínimo para el complemento Hyper-V de NetApp en el host Hyper-V
    - 5 GB de espacio mínimo de instalación y registro para el complemento en el host Hyper-V

Asegúrese de asignar suficiente espacio en disco en el host Hyper-V para la carpeta de registros y monitoree periódicamente su uso. El espacio requerido depende de la frecuencia con la que se realizan copias de seguridad y operaciones de protección de datos. Si no hay suficiente espacio, no se generarán registros.

- Requisitos de configuración de NetApp ONTAP :
    - Un sistema ONTAP primario (ONTAP 9.14.1 o posterior)
    - Para las implementaciones de Hyper-V que utilizan recursos compartidos CIFS para almacenar datos de máquinas virtuales, asegúrese de que la propiedad de recursos compartidos de disponibilidad continua esté habilitada en el sistema ONTAP . Consulte la "Documentación de ONTAP" para obtener

instrucciones.

En la NetApp Console

Asegúrese de que NetApp Console cumpla con los siguientes requisitos.

- Un usuario de la consola debe tener el rol y los privilegios necesarios para realizar operaciones en cargas de trabajo de Microsoft SQL Server y Kubernetes. Para descubrir los recursos, debe tener el rol de Superadministrador de NetApp Backup and Recovery . Ver"Acceso a funciones basado en roles de NetApp Backup and Recovery" para obtener detalles sobre los roles y permisos necesarios para realizar operaciones en NetApp Backup and Recovery.
- Una organización de consola con al menos un agente de consola activo que se conecta a clústeres de ONTAP locales o Cloud Volumes ONTAP.
- Al menos un sistema de consola con un clúster ONTAP local de NetApp o Cloud Volumes ONTAP .
- Un agente de consola

  Referirse a "Aprenda a configurar un agente de consola" y "Requisitos estándar de la NetApp Console" .

  - La versión preliminar requiere el sistema operativo Ubuntu 22.04 LTS para el agente de consola.

Configurar la NetApp Console

El siguiente paso es configurar la consola y NetApp Backup and Recovery.

Revisar "Requisitos estándar de la NetApp Console" .

Crear un agente de consola

Deberías comunicarte con tu equipo de productos de NetApp para probar Backup and Recovery. Luego, cuando utilice el agente de consola, incluirá las capacidades adecuadas para el servicio.

Para crear un agente de consola en la NetApp Console antes de usar el servicio, consulte la documentación de la consola que describe "Cómo crear un agente de consola" .

Dónde instalar el agente de consola

Para completar una operación de restauración, el agente de consola se puede instalar en las siguientes ubicaciones:

- Para Amazon S3, el agente de consola se puede implementar en sus instalaciones.
- Para Azure Blob, el agente de consola se puede implementar en sus instalaciones.
- Para StorageGRID, el agente de consola debe implementarse en sus instalaciones, con o sin acceso a Internet.
- Para ONTAP S3, el agente de consola se puede implementar en sus instalaciones (con o sin acceso a Internet) o en un entorno de proveedor de nube.

Las referencias a "sistemas ONTAP locales" incluyen los sistemas FAS y AFF .

Configurar licencias para NetApp Backup and Recovery

Puede obtener una licencia de NetApp Backup and Recovery comprando una

suscripción de pago por uso (PAYGO) o una suscripción anual en el mercado de * NetApp Intelligent Services* a su proveedor de nube, o comprando una licencia BYOL (traiga su propia licencia) a NetApp. Se requiere una licencia válida para activar NetApp Backup and Recovery en un sistema, para crear copias de seguridad de sus datos de producción y para restaurar datos de copia de seguridad en un sistema de producción.

Algunas notas antes de seguir leyendo:

- Si ya se ha suscrito a la suscripción de pago por uso (PAYGO) en el mercado de su proveedor de nube para un sistema Cloud Volumes ONTAP , entonces también estará suscrito automáticamente a NetApp Backup and Recovery . No necesitarás suscribirte nuevamente.
- La licencia BYOL (traiga su propia licencia) de NetApp Backup and Recovery es una licencia flotante que puede usar en todos los sistemas asociados con su organización o cuenta de NetApp Console . Por lo tanto, si tiene suficiente capacidad de respaldo disponible en una licencia BYOL existente, no necesitará comprar otra licencia BYOL.
- Si utiliza una licencia BYOL, se recomienda que también se suscriba a una suscripción PAYGO. Si realiza una copia de seguridad de más datos de los permitidos por su licencia BYOL, o si vence el plazo de su licencia, la copia de seguridad continúa a través de su suscripción de pago por uso: no hay interrupción del servicio.
- Al realizar una copia de seguridad de los datos locales de ONTAP en StorageGRID, necesita una licencia BYOL, pero no hay ningún costo por el espacio de almacenamiento del proveedor de la nube.

"Obtenga más información sobre los costos relacionados con el uso de NetApp Backup and Recovery."

Prueba gratuita de 30 días

Tiene disponible una prueba gratuita de 30 días de NetApp Backup and Recovery si se suscribe a una suscripción de pago por uso en el mercado de su proveedor de nube para * NetApp Intelligent Services*. La prueba gratuita comienza en el momento en que usted se suscribe al listado del mercado. Tenga en cuenta que si paga la suscripción al mercado al implementar un sistema Cloud Volumes ONTAP y luego comienza su prueba gratuita de NetApp Backup and Recovery 10 días después, le quedarán 20 días para usar la prueba gratuita.

Cuando finalice la prueba gratuita, pasarás automáticamente a la suscripción PAYGO sin interrupciones. Si decide no continuar utilizando NetApp Backup and Recovery, simplemente"cancelar el registro de NetApp Backup and Recovery del sistema" antes de que finalice la prueba y no se le cobrará.

Finalizar la prueba gratuita

Si desea continuar usando NetApp Backup and Recovery después de que finalice la prueba gratuita, deberá configurar una suscripción paga. Puede hacerlo desde la interfaz de la NetApp Console navegando a la sección de facturación y seleccionando un plan de suscripción que se ajuste a sus necesidades. Si no desea continuar usando NetApp Backup and Recovery, puede finalizar la prueba gratuita.

Cuando finaliza la prueba gratuita sin suscribirse a un plan pago, sus datos se eliminan automáticamente 60 días después de que finalice la prueba gratuita. Opcionalmente, puede hacer que el sistema elimine sus datos inmediatamente.

Pasos

1. Desde la página de inicio de NetApp Backup and Recovery , seleccione **Ver prueba gratuita**.
2. Seleccione **Finalizar prueba gratuita**.

3. Seleccione **Eliminar datos inmediatamente después de finalizar mi prueba gratuita** para eliminar sus datos inmediatamente.
4. Escriba **finalizar prueba** en el cuadro.
5. Seleccione **Fin** para confirmar.

Utilice una suscripción PAYGO de NetApp Backup and Recovery

En el plan de pago por uso, pagará a su proveedor de nube los costos de almacenamiento de objetos y los costos de licencia de respaldo de NetApp por hora en una sola suscripción. Debes suscribirte a * NetApp Intelligent Services* en el Marketplace incluso si tienes una prueba gratuita o si traes tu propia licencia (BYOL):

- Suscribirse garantiza que no habrá interrupciones del servicio una vez finalizada su prueba gratuita. Cuando finalice la prueba, se le cobrará por hora según la cantidad de datos que respalde.
- Si realiza una copia de seguridad de más datos de los permitidos por su licencia BYOL, las operaciones de copia de seguridad y restauración de datos continuarán a través de su suscripción de pago por uso. Por ejemplo, si tiene una licencia BYOL de 10 TiB, toda la capacidad que exceda los 10 TiB se cobra a través de la suscripción PAYGO.

No se le cobrará nada de su suscripción de pago por uso durante su prueba gratuita o si no ha excedido su licencia BYOL.

Hay algunos planes PAYGO para NetApp Backup and Recovery:

- Un paquete de "Copia de seguridad en la nube" que le permite realizar copias de seguridad de los datos de Cloud Volumes ONTAP y de los datos de ONTAP locales.
- Un paquete "CVO Professional" que le permite combinar Cloud Volumes ONTAP y NetApp Backup and Recovery. Esto incluye copias de seguridad ilimitadas para el sistema Cloud Volumes ONTAP usando la licencia (la capacidad de copia de seguridad no se descuenta de la capacidad con licencia). Esta opción no le permite realizar copias de seguridad de los datos de ONTAP locales.

  Tenga en cuenta que esta opción también requiere una suscripción PAYGO de respaldo y recuperación, pero no se incurrirá en cargos por los sistemas Cloud Volumes ONTAP elegibles.

"Obtenga más información sobre estos paquetes de licencias basados en capacidad".

Utilice estos enlaces para suscribirse a NetApp Backup and Recovery desde el mercado de su proveedor de nube:

- AWS: "Vaya a la oferta de Marketplace para NetApp Intelligent Services para obtener detalles de precios" .
- Azur: "Vaya a la oferta de Marketplace para NetApp Intelligent Services para obtener detalles de precios" .
- Google Cloud: "Vaya a la oferta de Marketplace para NetApp Intelligent Services para obtener detalles de precios" .

Utilice un contrato anual

Pague NetApp Backup and Recovery anualmente comprando un contrato anual. Están disponibles en plazos de 1, 2 o 3 años.

Si tiene un contrato anual de un mercado, todo el consumo de NetApp Backup and Recovery se cargará a ese contrato. No es posible combinar un contrato de mercado anual con un BYOL.

Cuando utiliza AWS, hay dos contratos anuales disponibles desde "Página de AWS Marketplace" Para Cloud Volumes ONTAP y sistemas ONTAP locales:

- Un plan de "Copia de seguridad en la nube" que le permite realizar copias de seguridad de los datos de Cloud Volumes ONTAP y de los datos de ONTAP locales.

  Si desea utilizar esta opción, configure su suscripción desde la página de Marketplace y luego "asociar la suscripción con sus credenciales de AWS" . Tenga en cuenta que también deberá pagar por sus sistemas Cloud Volumes ONTAP mediante esta suscripción de contrato anual, ya que solo puede asignar una suscripción activa a sus credenciales de AWS en la consola.

- Un plan "CVO Professional" que le permite combinar Cloud Volumes ONTAP y NetApp Backup and Recovery. Esto incluye copias de seguridad ilimitadas para el sistema Cloud Volumes ONTAP usando la licencia (la capacidad de copia de seguridad no se descuenta de la capacidad con licencia). Esta opción no le permite realizar copias de seguridad de los datos de ONTAP locales.

  Ver el "Tema de licencias de Cloud Volumes ONTAP" para obtener más información sobre esta opción de licencia.

  Si desea utilizar esta opción, puede configurar el contrato anual cuando cree un sistema Cloud Volumes ONTAP y la consola le solicite que se suscriba a AWS Marketplace.

Cuando utiliza Azure, hay dos contratos anuales disponibles desde "Página de Azure Marketplace" Para Cloud Volumes ONTAP y sistemas ONTAP locales:

- Un plan de "Copia de seguridad en la nube" que le permite realizar copias de seguridad de los datos de Cloud Volumes ONTAP y de los datos de ONTAP locales.

  Si desea utilizar esta opción, configure su suscripción desde la página de Marketplace y luego "asociar la suscripción con sus credenciales de Azure" . Tenga en cuenta que también deberá pagar por sus sistemas Cloud Volumes ONTAP mediante esta suscripción de contrato anual, ya que solo puede asignar una suscripción activa a sus credenciales de Azure en la consola.

- Un plan "CVO Professional" que le permite combinar Cloud Volumes ONTAP y NetApp Backup and Recovery. Esto incluye copias de seguridad ilimitadas para el sistema Cloud Volumes ONTAP usando la licencia (la capacidad de copia de seguridad no se descuenta de la capacidad con licencia). Esta opción no le permite realizar copias de seguridad de los datos de ONTAP locales.

  Ver el "Tema de licencias de Cloud Volumes ONTAP" para obtener más información sobre esta opción de licencia.

  Si desea utilizar esta opción, puede configurar el contrato anual cuando cree un sistema Cloud Volumes ONTAP y la consola le solicite que se suscriba a Azure Marketplace.

Cuando utilice GCP, comuníquese con su representante de ventas de NetApp para comprar un contrato anual. El contrato está disponible como oferta privada en Google Cloud Marketplace.

Después de que NetApp comparta la oferta privada contigo, podrás seleccionar el plan anual al suscribirte desde Google Cloud Marketplace durante la activación de NetApp Backup and Recovery .

Utilice una licencia BYOL de NetApp Backup and Recovery

Las licencias Bring-your-own de NetApp ofrecen plazos de 1, 2 o 3 años. Usted paga solo por los datos que protege, calculados según la capacidad lógica utilizada (antes de cualquier eficiencia) de los volúmenes

ONTAP de origen que se están respaldando. Esta capacidad también se conoce como Front-End Terabytes (FETB).

La licencia BYOL NetApp Backup and Recovery es una licencia flotante donde la capacidad total se comparte entre todos los sistemas asociados con su organización o cuenta de NetApp Console . Para los sistemas ONTAP , puede obtener una estimación aproximada de la capacidad que necesitará ejecutando el comando CLI `volume show -fields logical-used-by-afs` para los volúmenes que planea respaldar.

Si no tiene una licencia BYOL de NetApp Backup and Recovery , haga clic en el ícono de chat en la parte inferior derecha de la consola para comprar una.

De manera opcional, si tiene una licencia basada en nodo no asignado para Cloud Volumes ONTAP que no utilizará, puede convertirla en una licencia de NetApp Backup and Recovery con la misma equivalencia en dólares y la misma fecha de vencimiento. "Haga clic aquí para más detalles" .

Utilice la NetApp Console para administrar las licencias BYOL. Puede agregar nuevas licencias, actualizar licencias existentes y ver el estado de las licencias desde la Consola.

"Obtenga información sobre cómo agregar licencias".

Configurar certificados de seguridad para StorageGRID y ONTAP en NetApp Backup and Recovery

Cree un certificado de seguridad para habilitar la comunicación entre NetApp Backup and Recovery y StorageGRID u ONTAP.

Crear un certificado de seguridad para StorageGRID

Si la comunicación entre los contenedores de NetApp Backup and Recovery y StorageGRID debe verificar el certificado de StorageGRID , complete los siguientes pasos.

El certificado generado debe tener CN y nombre alternativo del sujeto como el nombre proporcionado en NetApp Backup and Recovery cuando activó la copia de seguridad.

Pasos

1. Siga los pasos de la documentación de StorageGRID para crear el certificado de StorageGRID .

   "Información de StorageGRID sobre la configuración de certificados"

2. Actualice StorageGRID con el certificado si aún no lo ha hecho.
3. Inicie sesión en el agente de la consola como usuario raíz. Correr:

   ```
   sudo su
   ```

4. Obtenga el volumen Docker de NetApp Backup and Recovery (Cloud Backup Service). Correr:

   ```
   docker volume ls | grep cbs
   ```

   Ejemplo de salida:

```
local service-manager-2_cloudmanager_cbs_volume"
```

El nombre del volumen difiere entre los modos de implementación Estándar, Privado y Restringido. Este ejemplo utiliza el modo estándar. Referirse a "Modos de implementación de la NetApp Console" .

5. Encuentre el punto de montaje del volumen de NetApp Backup and Recovery . Correr:

```
docker volume inspect service-manager-2_cloudmanager_cbs_volume | grep
Mountpoint
```

Ejemplo de salida:

```
"Mountpoint": "/var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data"
```

El punto de montaje difiere entre los modos de implementación Estándar, Privado y Restringido. Este ejemplo muestra una implementación de nube estándar. Referirse a "Modos de implementación de la NetApp Console" .

6. Cambie al directorio MountPoint. Correr:

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

7. Si el certificado de StorageGRID está firmado por la CA raíz y una CA intermedia, entonces agregue el `pem` archivos de ambos en un solo archivo llamado `sgws.crt` en la ubicación actual. No agregue el certificado de hoja a este archivo.

Pasos para el contenedor cloudmanager_cbs

Necesitará habilitar la verificación del certificado del servidor StorageGRID en NetApp Backup and Recovery (Cloud Backup Service).

1. Cambie los directorios al volumen Docker obtenido en los pasos anteriores.

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

2. Cambie los directorios al directorio de configuración.

```
cd cbs_config
```

3. Cree y guarde un archivo de configuración como se muestra a continuación con uno de los siguientes nombres según su entorno de implementación:

   - `production-customer.json`Se utiliza para implementaciones en modo estándar y modo restringido.
   - `darksite-customer.json`Se utiliza para implementaciones en modo privado.

   Referirse a "Modos de implementación de la NetApp Console" .

   Archivo de configuración

```
{
  "protocols": {
    "sgws": {
      "certificates": {
        "reject-unauthorized": true,
        "ca-bundle": "/config/sgws.crt"
      }
    }
  }
}
```

4. Salir del contenedor. Correr:

```
exit
```

5. Reanudar `cloudmanager_cbs` . Correr:

```
docker restart cloudmanager_cbs
```

Pasos para el contenedor cloudmanager_cbs_catalog

A continuación, deberá habilitar la verificación del certificado del servidor StorageGRID para el servicio de catalogación.

1. Cambiar directorios al volumen Docker:

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

2. Configurar el catálogo. Correr:

```
cd cbs_catalog_config
```

3. Cree un archivo de configuración como se muestra a continuación con uno de los siguientes nombres según su entorno de implementación:

   - `production-customer.json`Se utiliza para implementaciones en modo estándar y modo restringido.
   - `darksite-customer.json`Se utiliza para implementaciones en modo privado.

   Referirse a "Modos de implementación de la NetApp Console" .

   Archivo de configuración del catálogo

```
{
  "protocols": {
    "sgws": {
      "certificates": {
        "reject-unauthorized": true,
        "ca-bundle": "/config/sgws.crt"
      }
    }
  }
}
```

4. Reiniciar el catálogo. Correr:

```
docker restart cloudmanager_cbs_catalog
```

Actualice el certificado del agente de la consola con el certificado StorageGRID según el sistema operativo del agente

Ubuntu

1. Copiar el certificado SGWS a `/usr/local/share/ca-certificates` . He aquí un ejemplo:

```
cp /config/sgws.crt /usr/local/share/ca-certificates/
```

   dónde `sgws.crt` es el certificado CA raíz.

2. Actualice los certificados del host con el certificado StorageGRID . Correr

```
sudo update-ca-certificates
```

Red Hat Enterprise Linux

1. Copiar el certificado SGWS a `/etc/pki/ca-trust/source/anchors/` .

```
cp /config/sgws.crt /etc/pki/ca-trust/source/anchors/
```

dónde `sgws.crt` es el certificado CA raíz.

2. Actualice los certificados del host con el certificado StorageGRID .

```
update-ca-trust extract
```

3. Actualizar el `ca-bundle.crt`

```
cd /etc/pki/tls/certs/
openssl x509 -in ca-bundle.crt -text -noout
```

4. Para comprobar si los certificados están presentes, ejecute el siguiente comando:

```
openssl crl2pkcs7 -nocrl -certfile /etc/pki/tls/certs/ca-bundle.crt |
openssl pkcs7 -print_certs | grep subject | head
```

Crear un certificado de seguridad para ONTAP

Si la comunicación entre los contenedores de NetApp Backup and Recovery y ONTAP debe validar el certificado de ONTAP , complete los siguientes pasos.

NetApp Backup and Recovery utiliza la IP de administración de clúster para conectarse a ONTAP. Introduzca la dirección IP del clúster en los nombres alternativos del sujeto del certificado. Especifique este paso cuando genere la CSR mediante la interfaz de usuario del Administrador del sistema.

Utilice la documentación del Administrador del sistema para crear un nuevo certificado CA para ONTAP.

- "Administrar certificados con el Administrador del sistema"
- "Cómo administrar certificados SSL de ONTAP con System Manager"

Pasos

1. Inicie sesión en el agente de la consola como root. Correr:

```
sudo su
```

2. Obtenga el volumen Docker de NetApp Backup and Recovery . Correr:

```
docker volume ls | grep cbs
```

Ejemplo de salida:

```
local service-manager-2_cloudmanager_cbs_volume
```

El nombre del volumen difiere entre los modos de implementación Estándar, Privado y Restringido. Este ejemplo muestra una implementación de nube estándar. Referirse a "Modos de implementación de la NetApp Console" .

3. Obtenga el soporte para el volumen. Correr:

```
docker volume inspect service-manager-2_cloudmanager_cbs_volume | grep Mountpoint
```

Ejemplo de salida:

```
"Mountpoint": "/var/lib/docker/volumes/service-manager-2_cloudmanager_cbs_volume/_data
```

El punto de montaje difiere entre los modos de implementación Estándar, Privado y Restringido. Este ejemplo muestra una implementación de nube estándar. Referirse a "Modos de implementación de la NetApp Console" .

4. Cambiar al directorio del punto de montaje. Correr:

```
cd /var/lib/docker/volumes/service-manager-2_cloudmanager_cbs_volume/_data
```

5. Complete uno de los siguientes pasos:
   - Si el certificado ONTAP está firmado por la CA raíz y una CA intermedia, entonces agregue el `pem` archivos de ambos en un solo archivo llamado `ontap.crt` en la ubicación actual.
   - Si el certificado ONTAP está firmado por una sola CA, cambie el nombre del certificado. `pem` archivar como `ontap.crt` y copiarlo en la ubicación actual. No agregue el certificado de hoja a este archivo.

Pasos para el contenedor cloudmanager_cbs

A continuación, habilite la verificación del certificado del servidor ONTAP en NetApp Backup and Recovery (Cloud Backup Service).

1. Cambie los directorios al volumen Docker obtenido en los pasos anteriores.

```
cd /var/lib/docker/volumes/service-manager-2_cloudmanager_cbs_volume/_data
```

2. Cambie al directorio de configuración. Correr:

```
cd cbs_config
```

3. Cree un archivo de configuración como se muestra a continuación con uno de los siguientes nombres según su entorno de implementación:

   - `production-customer.json`Se utiliza para implementaciones en modo estándar y modo restringido.
   - `darksite-customer.json`Se utiliza para implementaciones en modo privado.

   Referirse a "Modos de implementación de la NetApp Console" .

   Archivo de configuración

```
{
  "ontap": {
    "certificates": {
      "reject-unauthorized": true,
      "ca-bundle": "/config/ontap.crt"
    }
  }
}
```

4. Salir del contenedor. Correr:

```
exit
```

5. Reinicie NetApp Backup and Recovery. Correr:

```
docker restart cloudmanager_cbs
```

Pasos para el contenedor cloudmanager_cbs_catalog

Habilite la verificación del certificado del servidor ONTAP para el servicio de catalogación.

1. Cambiar directorios al volumen Docker. Correr:

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

2. Correr:

```
cd cbs_catalog_config
```

3. Cree un archivo de configuración como se muestra a continuación con uno de los siguientes nombres según su entorno de implementación:

   - `production-customer.json`Se utiliza para implementaciones en modo estándar y modo restringido.
   - `darksite-customer.json`Se utiliza para implementaciones en modo privado.

   Referirse a "Modos de implementación de la NetApp Console" .

   Archivo de configuración

```
{
  "ontap": {
    "certificates": {
      "reject-unauthorized": true,
      "ca-bundle": "/config/ontap.crt"
    }
  }
}
```

4. Reinicie NetApp Backup and Recovery. Correr:

```
docker restart cloudmanager_cbs_catalog
```

Cree un certificado para ONTAP y StorageGRID

Si necesita habilitar el certificado tanto para ONTAP como para StorageGRID, el archivo de configuración se verá así:

Archivo de configuración para ONTAP y StorageGRID

```
{
  "protocols": {
    "sgws": {
      "certificates": {
        "reject-unauthorized": true,
        "ca-bundle": "/config/sgws.crt"
      }
    }
  },
  "ontap": {
    "certificates": {
      "reject-unauthorized": true,
      "ca-bundle": "/config/ontap.crt"
    }
  }
}
```

Configure destinos de respaldo antes de usar NetApp Backup and Recovery

Antes de utilizar NetApp Backup and Recovery, realice algunos pasos para configurar los destinos de respaldo.

Antes de comenzar, revise"prerrequisitos" para garantizar que su entorno esté preparado.

Preparar el destino de la copia de seguridad

Prepare uno o más de los siguientes destinos de respaldo:

- StorageGRID NetApp .

  Referirse a "Descubra StorageGRID" .

  Referirse a "Documentación de StorageGRID" para obtener detalles sobre StorageGRID.

- Servicios web de Amazon. Referirse a "Documentación de Amazon S3" .

  Haga lo siguiente para preparar AWS como destino de respaldo:

  - Configurar una cuenta en AWS.
  - Configure los permisos S3 en AWS, que se enumeran en la siguiente sección.
  - Para obtener detalles sobre cómo administrar su almacenamiento de AWS en la consola, consulte "Administra tus buckets de Amazon S3" .

- Microsoft Azure.
  - Referirse a "Documentación de Azure NetApp Files" .
  - Configurar una cuenta en Azure.

- Configurar "Permisos de Azure" en Azure.
- Para obtener detalles sobre cómo administrar su almacenamiento de Azure en la consola, consulte "Administrar sus cuentas de almacenamiento de Azure" .

Después de configurar las opciones en el destino de la copia de seguridad, más tarde lo configurará como destino de copia de seguridad en NetApp Backup and Recovery. Para obtener detalles sobre cómo configurar el destino de la copia de seguridad en NetApp Backup and Recovery, consulte"Descubrir objetivos de respaldo" .

Configurar permisos S3

Necesitará configurar dos conjuntos de permisos de AWS S3:

- Permisos para que el agente de la consola cree y administre el depósito S3.
- Permisos para el clúster ONTAP local para que pueda leer y escribir datos en el depósito S3.

Pasos

1. Asegúrese de que el agente de la consola tenga los permisos necesarios. Para más detalles, consulte "Permisos de políticas de la NetApp Console" .

   Al crear copias de seguridad en las regiones de AWS China, debe cambiar el nombre del recurso de AWS "arn" en todas las secciones *Resource* en las políticas de IAM de "aws" a "aws-cn"; por ejemplo `arn:aws-cn:s3:::netapp-backup-*` .

2. Cuando active el servicio, el asistente de copia de seguridad le solicitará que ingrese una clave de acceso y una clave secreta. Estas credenciales se pasan al clúster de ONTAP para que ONTAP pueda realizar copias de seguridad y restaurar datos en el depósito S3. Para ello, necesitarás crear un usuario IAM con los siguientes permisos.

   Consulte la "Documentación de AWS: Creación de un rol para delegar permisos a un usuario de IAM" .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource": "arn:aws:s3:::netapp-backup-*",
      "Effect": "Allow",
      "Sid": "backupPolicy"
    },
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListAllMyBuckets",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:RestoreObject",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetObjectRetention",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutObjectRetention"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*/*",
      "Effect": "Allow"
    }
  ]
}
```

Inicie sesión en NetApp Backup and Recovery

Utilice la NetApp Console para iniciar sesión en NetApp Backup and Recovery.

NetApp Backup and Recovery utiliza la gestión de identidad y acceso para controlar lo que puede hacer cada usuario.

Para obtener detalles sobre las acciones que puede realizar cada rol, consulte"Roles de usuario de NetApp Backup and Recovery" .

Para iniciar sesión en la NetApp Console, puede utilizar sus credenciales del sitio de soporte de NetApp o puede registrarse para iniciar sesión en la NetApp Console usando su correo electrónico y una contraseña. "Obtenga más información sobre cómo iniciar sesión" .

Rol de NetApp Console requerido Rol de superadministrador de Backup and Recovery o rol de administrador de restauración de Backup and Recovery. "Obtenga información sobre los roles de acceso a la NetApp Console para todos los servicios" .

Para agregar un agente de consola, debe tener el rol de superadministrador de Copia de seguridad y recuperación.

Pasos

1. Abra un navegador web y vaya a "NetApp Console" .

   Aparece la página de inicio de sesión de la NetApp Console .

2. Inicie sesión en la consola.
3. Desde la navegación izquierda de la Consola, seleccione **Protección** > **Copia de seguridad y recuperación**.
   - Si es la primera vez que inicia sesión en Backup and Recovery y aún no ha agregado un sistema a la página **Sistemas**, Backup and Recovery muestra la página de inicio "Bienvenido a la nueva NetApp Backup and Recovery" con una opción para agregar un sistema. Para obtener detalles sobre cómo agregar un sistema a la página **Sistemas**, consulte "Introducción al modo estándar de la NetApp Console".
   - Si inicia sesión en Backup and Recovery por primera vez y tiene un sistema en la consola pero no ha descubierto ningún recurso, aparecerá la página *Bienvenido a la nueva NetApp Backup and Recovery* con una opción para **Descubrir recursos**.
4. Si aún no lo ha hecho, seleccione la opción **Descubrir y administrar**.
   - Para cargas de trabajo de Microsoft SQL Server, consulte"Descubra las cargas de trabajo de Microsoft SQL Server" .
   - Para cargas de trabajo de VMware, consulte"Descubra las cargas de trabajo de VMware" .
   - Para cargas de trabajo KVM, consulte"Descubra las cargas de trabajo KVM" .
   - Para cargas de trabajo de Oracle Database, consulta "Descubre las cargas de trabajo de Oracle Database".
   - Para cargas de trabajo de Hyper-V, consulte"Descubra las cargas de trabajo de Hyper-V" .
   - Para cargas de trabajo de Kubernetes, consulte"Descubra las cargas de trabajo de Kubernetes" .

Descubra los destinos de respaldo externos en NetApp Backup and Recovery

Complete unos pocos pasos para descubrir o agregar manualmente destinos de respaldo externos en NetApp Backup and Recovery.

Descubra un destino de respaldo

Configure sus destinos de respaldo (Amazon Web Services (AWS) S3, Microsoft Azure Blob Storage, Google Cloud Storage o StorageGRID) antes de usar NetApp Backup and Recovery.

Puede descubrir estos objetivos automáticamente o agregarlos manualmente.

Proporcione credenciales para acceder a la cuenta de almacenamiento. NetApp Backup and Recovery utiliza estas credenciales para descubrir las cargas de trabajo que desea respaldar.

Antes de empezar

Debe descubrir al menos una carga de trabajo antes de poder agregar un destino de respaldo externo.

Pasos

1. En el menú de NetApp Backup and Recovery , seleccione **Inventario**.
2. Seleccione la pestaña **Destinos de copia de seguridad externos**.
3. Seleccione **Descubrir destino de copia de seguridad**.
4. Seleccione uno de los tipos de destino de copia de seguridad: **Amazon Web Services (AWS) S3**, **Microsoft Azure Blob Storage**, * StorageGRID* o * ONTAP S3*.
5. En la sección **Elegir ubicación de credenciales**, elija la ubicación donde residen las credenciales y luego elija cómo asociarlas.
6. Seleccione **Siguiente**.
7. Ingrese la información de las credenciales. Esta información varía según el tipo de destino de copia de seguridad seleccionado y la ubicación de las credenciales elegida.
   - Para AWS:
     - **Nombre de la credencial**: ingrese el nombre de la credencial de AWS.
     - **Tecla de acceso**: Ingrese el secreto de AWS.
     - **Clave secreta**: Ingrese la clave secreta de AWS.
   - Para Azure:
     - **Nombre de la credencial**: ingrese el nombre de la credencial de Azure Blob Storage.
     - **Secreto del cliente**: ingrese el secreto del cliente de Azure Blob Storage.
     - **ID de aplicación (cliente)**: seleccione el ID de la aplicación de Azure Blob Storage.
     - **ID de inquilino del directorio**: ingrese el ID de inquilino de Azure Blob Storage.
   - Para StorageGRID:
     - **Nombre de la credencial**: Ingrese el nombre de la credencial de StorageGRID .
     - **FQDN del nodo de puerta de enlace**: ingrese un nombre FQDN para StorageGRID.
     - **Puerto**: Ingrese el número de puerto para StorageGRID.

- **Tecla de acceso**: Ingrese la clave de acceso de StorageGRID S3.
- **Clave secreta**: Ingrese la clave secreta de StorageGRID S3.

◦ Para ONTAP S3:

- **Nombre de la credencial**: ingrese el nombre de la credencial de ONTAP S3.
- **FQDN del nodo de puerta de enlace**: ingrese un nombre FQDN para ONTAP S3.
- **Puerto**: Ingrese el número de puerto para ONTAP S3.
- **Tecla de acceso**: Ingrese la clave de acceso de ONTAP S3.
- **Clave secreta**: Ingrese la clave secreta de ONTAP S3.

8. Seleccione **Descubrir**.

Agregar un depósito para un objetivo de respaldo

En lugar de que NetApp Backup and Recovery descubra los depósitos automáticamente, puede agregar manualmente un depósito a un destino de respaldo externo.

Pasos

1. En el menú de NetApp Backup and Recovery , seleccione **Inventario**.
2. Seleccione **Destinos de copia de seguridad externos**.
3. Seleccione el objetivo y a la derecha, seleccione **Acciones*** icono y seleccione *Agregar depósito**.
4. Ingrese la información del depósito. La información varía según el tipo de destino de copia de seguridad que haya seleccionado.

◦ Para AWS:

- **Nombre del depósito**: Ingrese el nombre del depósito S3. El prefijo "netapp-backup" es un prefijo obligatorio y se agrega automáticamente al nombre que proporcione.
- **Cuenta de AWS**: Ingrese el nombre de la cuenta de AWS.
- **Región del depósito**: Ingrese la región de AWS para el depósito.
- **Habilitar bloqueo de objetos S3**: seleccione esta opción para habilitar el bloqueo de objetos S3 para el depósito. S3 Object Lock evita que los objetos se eliminen o sobrescriban durante un período de retención específico, lo que proporciona una capa adicional de protección de datos. Puedes habilitar esto solo cuando estás creando un depósito y no podrás desactivarlo más tarde.
  - **Modo de gobernanza**: seleccione esta opción para habilitar el modo de gobernanza para el depósito S3 Object Lock. El modo de gobernanza le permite proteger los objetos para que no sean eliminados ni sobrescritos por la mayoría de los usuarios, pero permite que ciertos usuarios alteren la configuración de retención.
  - **Modo de cumplimiento**: seleccione esta opción para habilitar el modo de cumplimiento para el depósito de bloqueo de objetos S3. El modo de cumplimiento impide que cualquier usuario, incluido el usuario root, altere la configuración de retención o elimine objetos hasta que expire el período de retención.
- **Control de versiones**: seleccione esta opción para habilitar el control de versiones para el bucket S3. El control de versiones le permite mantener múltiples versiones de objetos en el depósito, lo que puede resultar útil para fines de copia de seguridad y recuperación.
- **Etiquetas**: seleccione etiquetas para el depósito S3. Las etiquetas son pares clave-valor que se pueden utilizar para organizar y administrar sus recursos S3.
- **Cifrado**: seleccione el tipo de cifrado para el depósito S3. Las opciones son claves administradas

por AWS S3 o claves de AWS Key Management Service. Si selecciona claves de AWS Key Management Service, deberá proporcionar el ID de la clave.

- Para Azure:
  - **Suscripción**: seleccione el nombre del contenedor de Azure Blob Storage.
  - **Grupo de recursos**: seleccione el nombre del grupo de recursos de Azure.
  - **Detalles de la instancia**:
    - **Nombre de la cuenta de almacenamiento**: ingrese el nombre del contenedor de Azure Blob Storage.
    - **Región de Azure**: ingrese la región de Azure para el contenedor.
    - **Tipo de rendimiento**: seleccione el tipo de rendimiento estándar o premium para el contenedor de Azure Blob Storage indicando el nivel de rendimiento requerido.
    - **Cifrado**: seleccione el tipo de cifrado para el contenedor de Azure Blob Storage. Las opciones son claves administradas por Microsoft o claves administradas por el cliente. Si selecciona claves administradas por el cliente, debe proporcionar el nombre del almacén de claves y el nombre de la clave.
- Para StorageGRID:
  - **Nombre del destino de la copia de seguridad**: seleccione el nombre del depósito StorageGRID .
  - **Nombre del depósito**: Ingrese el nombre del depósito StorageGRID .
  - **Región**: Ingrese la región StorageGRID para el depósito.
  - **Habilitar control de versiones**: seleccione esta opción para habilitar el control de versiones para el depósito StorageGRID . El control de versiones le permite mantener múltiples versiones de objetos en el depósito, lo que puede resultar útil para fines de copia de seguridad y recuperación.
  - **Bloqueo de objetos**: seleccione esta opción para habilitar el bloqueo de objetos para el depósito StorageGRID . El bloqueo de objetos evita que se eliminen o sobrescriban objetos durante un período de retención específico, lo que proporciona una capa adicional de protección de datos. Puedes habilitar esto solo cuando estás creando un depósito y no podrás desactivarlo más tarde.
  - **Capacidad**: Ingrese la capacidad para el depósito StorageGRID . Esta es la cantidad máxima de datos que se pueden almacenar en el depósito.
- Para ONTAP S3:
  - **Nombre del destino de la copia de seguridad**: seleccione el nombre del depósito ONTAP S3.
  - **Nombre del destino del depósito**: Ingrese el nombre del depósito ONTAP S3.
  - **Capacidad**: Ingrese la capacidad para el depósito ONTAP S3. Esta es la cantidad máxima de datos que se pueden almacenar en el depósito.
  - **Habilitar control de versiones**: seleccione esta opción para habilitar el control de versiones para el bucket ONTAP S3. El control de versiones le permite mantener múltiples versiones de objetos en el depósito, lo que puede resultar útil para fines de copia de seguridad y recuperación.
  - **Bloqueo de objetos**: seleccione esta opción para habilitar el bloqueo de objetos para el depósito ONTAP S3. El bloqueo de objetos evita que se eliminen o sobrescriban objetos durante un período de retención específico, lo que proporciona una capa adicional de protección de datos. Puedes habilitar esto solo cuando estás creando un depósito y no podrás desactivarlo más tarde.

5. Seleccione **Agregar**.

Cambiar las credenciales de un destino de respaldo

Introduzca las credenciales necesarias para acceder al destino de la copia de seguridad.

Pasos

1. En el menú de NetApp Backup and Recovery , seleccione **Inventario**.
2. Seleccione **Destinos de copia de seguridad externos**.
3. Seleccione el objetivo y a la derecha, seleccione **Acciones*** **icono y seleccione *Cambiar credenciales**.
4. Introduzca las nuevas credenciales para el destino de la copia de seguridad. La información varía según el tipo de destino de copia de seguridad que haya seleccionado.
5. Seleccione **Listo**.

Cambiar a diferentes cargas de trabajo de NetApp Backup and Recovery

Puede cambiar entre las diferentes cargas de trabajo de NetApp Backup and Recovery .

Cambiar a una carga de trabajo diferente

Puede cambiar a una carga de trabajo diferente en la interfaz de usuario de NetApp Backup and Recovery .

Pasos

1. Desde la navegación izquierda de la Consola, seleccione **Protección** > **Copia de seguridad y recuperación**.
2. Desde la esquina superior derecha de la página, seleccione la lista desplegable **Cambiar carga de trabajo**.
3. Seleccione la carga de trabajo a la que desea cambiar.

   La página se actualiza y muestra la carga de trabajo seleccionada.

Configurar los ajustes de NetApp Backup and Recovery

Después de configurar la NetApp Console, configure los ajustes de copia de seguridad y recuperación. Agregue credenciales para los recursos del host, importe recursos de SnapCenter , configure directorios de registro y establezca la configuración de VMware vCenter. Complete estos pasos antes de realizar una copia de seguridad o recuperar datos.

- Agregar credenciales para los recursos del host para cualquier host de Windows, Microsoft SQL Server, Oracle Database o Linux con el que NetApp Backup and Recovery necesite autenticarse. Esto incluye las credenciales del sistema operativo invitado Windows utilizadas al restaurar archivos o carpetas invitados.
- Mantener la configuración de VMware vCenter.
- Importar y administrar recursos del host de SnapCenter. (Solo cargas de trabajo de Microsoft SQL Server)
- Agregar una plataforma de administración KVM. (Solo cargas de trabajo KVM)

- Configurar directorios de registro en instantáneas para hosts de Windows.
- Crear una plantilla de gancho de ejecución para ejecutar scripts antes y después de los trabajos de backup. (Solo cargas de trabajo de Kubernetes)

Rol de NetApp Console requerido Superadministrador de Backup and Recovery, Administrador de backup de Backup and Recovery, Administrador de restauración de Backup and Recovery. Conozca más sobre"Roles y privilegios de copia de seguridad y recuperación" . "Obtenga información sobre los roles de acceso a la NetApp Console para todos los servicios" .

Agregar credenciales para los recursos del host

Agregar credenciales para los recursos del host. NetApp Backup and Recovery utiliza estas credenciales para descubrir cargas de trabajo y aplicar políticas de respaldo.

Si no tiene credenciales, créelas con permisos para acceder y administrar las cargas de trabajo del host.

Debe configurar los siguientes tipos de credenciales:

- Credenciales de Microsoft SQL Server
- Credenciales del host de Windows de SnapCenter
- Credenciales del sistema operativo invitado de Windows utilizadas al restaurar archivos o carpetas de invitados
- Credenciales de la base de datos Oracle
- Credenciales del host de Linux

Pasos

1. Desde el menú NetApp Backup and Recovery , seleccione **Configuración**.
2. Seleccione la flecha hacia abajo para **Credenciales**.
3. Seleccione **Agregar nuevas credenciales**.
4. Ingrese información para las credenciales. Aparecen diferentes campos según el modo de autenticación que seleccione. Pase el cursor sobre el ícono de Información **i** para obtener más información sobre los campos.
    - **Nombre de las credenciales**: Ingrese un nombre para las credenciales.
    - **Modo de autenticación**: seleccione **Windows**, **Microsoft SQL**, **Oracle Database** o **Linux**.

Para las cargas de trabajo de Microsoft SQL Server, debe ingresar credenciales tanto para Windows como para Microsoft SQL Server, por lo que deberá agregar dos conjuntos de credenciales.

Ventanas

i. Si seleccionó **Windows**:

- **Agentes**: seleccione un agente de consola de la lista.
- **Dominio y nombre de usuario**: Ingrese el FQDN de NetBIOS o dominio y el nombre de usuario para las credenciales.
- **Contraseña**: Ingrese la contraseña para las credenciales.

Microsoft SQL Server

i. Si seleccionó **Microsoft SQL Server**:

- **Dominio y nombre de usuario**: Ingrese el FQDN de NetBIOS o dominio y el nombre de usuario para las credenciales.
- **Contraseña**: Ingrese la contraseña para las credenciales.
- **Hosts**: seleccione una dirección de host de SQL Server detectada.
- **Instancia de SQL Server**: seleccione una instancia de SQL Server detectada.

Base de datos Oracle

i. Si seleccionó **Oracle Database**:

- **Agentes**: seleccione un agente de consola de la lista.
- **Nombre de usuario**: Ingrese el nombre de usuario para las credenciales.
- **Contraseña**: Ingrese la contraseña para las credenciales.

Linux

i. Si seleccionó **Linux**:

- **Agentes**: seleccione un agente de consola de la lista.
- **Nombre de usuario**: Ingrese el nombre de usuario para las credenciales.
- **Contraseña**: Ingrese la contraseña para las credenciales.

5. Seleccione **Agregar**.

Editar credenciales para recursos del host

Posteriormente podrás editar la contraseña de cualquier credencial que hayas creado.

Pasos

1. Desde el menú NetApp Backup and Recovery , seleccione **Configuración**.
2. Seleccione la flecha hacia abajo para expandir la sección **Credenciales**.
3. Seleccione el icono Acciones ••• > **Editar credenciales**.
   - **Contraseña**: Ingrese la contraseña para las credenciales.
4. Seleccione **Guardar**.

Mantener la configuración de VMware vCenter

Proporcione las credenciales de VMware vCenter para descubrir cargas de trabajo para realizar copias de

seguridad. Si no tiene credenciales, créelas con permisos para acceder y administrar las cargas de trabajo de VMware vCenter Server.

Pasos

1. Desde el menú NetApp Backup and Recovery , seleccione **Configuración**.
2. Seleccione la flecha hacia abajo para expandir la sección **VMware vCenter**.
3. Seleccione **Agregar vCenter**.
4. Ingrese la información de VMware vCenter Server.
   - **vCenter FQDN o dirección IP**: ingrese un nombre FQDN o la dirección IP para VMware vCenter Server.
   - **Nombre de usuario** y **Contraseña**: ingrese el nombre de usuario y la contraseña para VMware vCenter Server.
   - **Puerto**: Ingrese el número de puerto para VMware vCenter Server.
   - **Protocolo**: Seleccione **HTTP** o **HTTPS**.
5. Seleccione **Agregar**.

Importar y administrar recursos del host de SnapCenter

Si anteriormente utilizó SnapCenter para realizar copias de seguridad de sus recursos, puede importar y administrar esos recursos en NetApp Backup and Recovery. Esta opción le permite importar información del servidor SnapCenter para registrar varios servidores SnapCenter y descubrir cargas de trabajo de bases de datos.

Este es un proceso de dos partes:

- Importar recursos de host y aplicaciones de SnapCenter Server
- Administrar recursos de host de SnapCenter seleccionados

Importar recursos de host y aplicaciones de SnapCenter Server

Este primer paso importa recursos del host desde SnapCenter y muestra esos recursos en la página Inventario de NetApp Backup and Recovery . En ese momento, los recursos aún no están administrados por NetApp Backup and Recovery.

Después de importar los recursos del host de SnapCenter , NetApp Backup and Recovery no se hace cargo de la administración de la protección. Para ello, debe seleccionar explícitamente administrar estos recursos en NetApp Backup and Recovery.

Pasos

1. Desde el menú NetApp Backup and Recovery , seleccione **Configuración**.
2. Seleccione la flecha hacia abajo para expandir la sección **Importar desde SnapCenter**.
3. Seleccione **Importar desde SnapCenter** para importar los recursos de SnapCenter .
4. Ingrese * credenciales de la aplicación SnapCenter *:
   a. * FQDN o dirección IP de SnapCenter *: ingrese el FQDN o la dirección IP de la aplicación SnapCenter .
   b. **Puerto**: Ingrese el número de puerto para el servidor SnapCenter .

c. **Nombre de usuario** y **Contraseña**: Ingrese el nombre de usuario y la contraseña para el servidor SnapCenter .

d. **Agente de consola**: seleccione el agente de consola para SnapCenter.

5. Ingrese * credenciales del host del servidor SnapCenter *:

a. **Credenciales existentes**: si selecciona esta opción, puede utilizar las credenciales existentes que ya haya agregado. Introduzca el nombre de las credenciales.

b. **Agregar nuevas credenciales**: si no tiene credenciales de host de SnapCenter existentes, puede agregar nuevas credenciales. Ingrese el nombre de las credenciales, el modo de autenticación, el nombre de usuario y la contraseña.

6. Seleccione **Importar** para validar sus entradas y registrar el servidor SnapCenter .

Si el servidor SnapCenter ya está registrado, puede actualizar los detalles de registro existentes.

Resultado

La página Inventario muestra los recursos de SnapCenter importados.

Administrar los recursos del host de SnapCenter

Después de importar los recursos de SnapCenter , administre esos recursos de host en NetApp Backup and Recovery. Después de seleccionar administrar esos recursos importados, NetApp Backup and Recovery puede realizar copias de seguridad y recuperar los recursos que está importando desde SnapCenter. Ya no es necesario administrar esos recursos en SnapCenter Server.

Pasos

1. Después de importar los recursos de SnapCenter , en la página Inventario que aparece, seleccione los recursos de SnapCenter que importó y que desea que NetApp Backup and Recovery administre de ahora en adelante.
2. Seleccione el icono Acciones ••• > **Administrar** para administrar los recursos.
3. Seleccione **Administrar en la NetApp Console**.

   La página Inventario muestra **Administrado** debajo del nombre del host para indicar que los recursos del host seleccionados ahora están administrados por NetApp Backup and Recovery.

Editar recursos de SnapCenter importados

Posteriormente puede volver a importar recursos de SnapCenter o editar los recursos de SnapCenter importados para actualizar los detalles de registro.

Puede cambiar solo los detalles del puerto y la contraseña para el servidor SnapCenter .

Pasos

1. Desde el menú NetApp Backup and Recovery , seleccione **Configuración**.
2. Seleccione la flecha hacia abajo para **Importar desde SnapCenter**.

   La página Importar desde SnapCenter muestra todas las importaciones anteriores.

3. Seleccione el icono Acciones ••• > **Editar** para actualizar los recursos.

4. Actualice la contraseña de SnapCenter y los detalles del puerto, según sea necesario.
5. Seleccione **Importar**.

Agregar una plataforma de administración KVM

Si utiliza la plataforma de administración Apache CloudStack para administrar recursos KVM, debe integrarla con NetApp Backup and Recovery para que Backup and Recovery pueda descubrir y proteger los hosts y las máquinas virtuales KVM administrados.

Pasos

1. Desde el menú NetApp Backup and Recovery , seleccione **Configuración**.
2. Seleccione la flecha hacia abajo para expandir la sección **Plataforma de administración**.
3. Seleccione **Agregar credencial de plataforma de administración**.
4. Introduzca la siguiente información:
   - **Dirección IP o FQDN de la plataforma de administración**: ingrese la dirección IP o el nombre de dominio completo de la plataforma de administración.
   - **Clave API**: Ingrese la clave API que se utilizará para autenticar las solicitudes API.
   - **Clave secreta**: Ingrese la clave secreta que se utilizará para autenticar las solicitudes de API.
   - **Puerto**: Ingrese el puerto que se utilizará para la comunicación entre Backup and Recovery y la plataforma de administración.
   - **Agentes**: seleccione un agente de consola para utilizar para facilitar la comunicación entre Backup and Recovery y la plataforma de administración.
5. Cuando haya terminado, seleccione **Agregar**.

Configurar directorios de registro en instantáneas para hosts de Windows

Antes de crear políticas para los hosts de Windows, debe configurar los directorios de registro en las instantáneas para los hosts de Windows. Los directorios de registro se utilizan para almacenar los registros que se generan durante el proceso de copia de seguridad.

Pasos

1. En el menú de NetApp Backup and Recovery , seleccione **Inventario**.
2. Desde la página Inventario, seleccione una carga de trabajo y luego seleccione el ícono Acciones ••• > **Ver detalles** para mostrar los detalles de la carga de trabajo.
3. Desde la página de detalles de inventario que muestra Microsoft SQL Server, seleccione la pestaña Hosts.
4. Desde la página de detalles de inventario, seleccione un host y seleccione el ícono Acciones ••• > **Configurar directorio de registro**.
5. Busque o ingrese la ruta del directorio de registro.
6. Seleccione **Guardar**.

Crear una plantilla de gancho de ejecución

Puede crear una plantilla de gancho de ejecución personalizada que pueda utilizar para realizar acciones antes o después de una operación de protección de datos en una aplicación.

Las plantillas que crees aquí solo se pueden usar cuando proteges cargas de trabajo de Kubernetes.

Pasos

1. En la consola, vaya a **Protección** > **Copia de seguridad y recuperación**.
2. Seleccione la pestaña **Configuración**.
3. Expande la sección **Plantilla de gancho de ejecución**.
4. Seleccione **Crear plantilla de gancho de ejecución**.
5. Introduzca un nombre para el gancho de ejecución.
6. Opcionalmente, elija un tipo de enlace. Por ejemplo, un enlace posterior a la restauración se ejecuta una vez finalizada la operación.
7. En el cuadro de texto **Script**, ingrese el script de shell ejecutable que desea ejecutar como parte de la plantilla de gancho de ejecución. Opcionalmente, puede seleccionar **Cargar script** para cargar un archivo de script en su lugar.
8. Seleccione **Crear**.

   Después de crear la plantilla, ésta aparece en la lista de plantillas en la sección **Plantilla de gancho de ejecución**.

Configura el control de acceso basado en roles en NetApp Backup and Recovery

Para aumentar la seguridad y controlar el acceso a los recursos, configura el control de acceso basado en roles para NetApp Backup and Recovery. La NetApp Console admite control de acceso basado en roles (RBAC) para algunas cargas de trabajo de Backup and Recovery. Puedes asignar roles administrativos o de espectador específicos para estas cargas de trabajo. Otras cargas de trabajo que aún no admiten control de acceso basado en roles siguen siendo accesibles para todos los usuarios con roles de Backup and Recovery hasta que se admita la asociación a nivel de proyecto.

Sigue estos pasos para controlar el acceso a los recursos de tu organización. Haz cambios en la página **Administración > Identidad y acceso** en el menú de la NetApp Console.

Estos pasos suponen que tienes asignado el rol de Organization Admin en la Console.

Pasos

1. Crea la estructura del proyecto de identidad y acceso.

   Como administrador de la organización, configura la carpeta de identidad y acceso y la estructura del proyecto donde residirán las cargas de trabajo.

2. Asigna roles de usuario.
   a. Opción principal:

      Agrega usuarios a cada proyecto designado para cargas de trabajo y asígnales el rol adecuado. Por ejemplo:

- **Organization admin** y **Backup and Recovery super admin**: un usuario con estos roles puede ver todos los recursos en todas las organizaciones y descubrir las cargas de trabajo de Backup and Recovery y asignarlas a proyectos (por ejemplo, US East o US West).
- **Administrador de carpeta o proyecto** y **Backup and Recovery super admin**: Un usuario con estos roles puede ver solo los recursos de la carpeta o proyecto para los que tiene permisos, pero puede descubrir cargas de trabajo de Backup and Recovery y asignarlas a ese proyecto.

b. Opción alternativa:

   En lugar de conceder a un usuario acceso completo de administrador de Backup and Recovery, puedes asignarte a ti mismo el rol de superadministrador de Backup and Recovery y descubrir las cargas de trabajo directamente.

3. Descubre las cargas de trabajo en Backup and Recovery.

   Los administradores de la organización o los administradores de carpetas o proyectos descubren las cargas de trabajo disponibles y seleccionan el proyecto adecuado (como US East o US West). Cada carga de trabajo se asocia automáticamente con el proyecto seleccionado.

4. Agrega usuarios a los proyectos.

   Los administradores de la organización o los administradores de carpetas/proyectos añaden usuarios de Console a proyectos con cargas de trabajo. Asigna a los usuarios el rol de Organization viewer y un rol de Backup and Recovery según sus necesidades de acceso. Los usuarios con el rol correcto de Backup and Recovery obtendrán acceso automáticamente a las nuevas cargas de trabajo en estos proyectos.

Información relacionada

- "Conoce la gestión de identidades y accesos de NetApp Console".
- "Funciones de NetApp Backup and Recovery en la NetApp Console".