Documentación de Cloud Manager y Cloud Volumes ONTAP

Cloud Manager 3.8

NetApp
March 25, 2024

Tabla de contenidos

Documentación de Cloud Manager y Cloud Volumes ONTAP

Cloud Manager permite que los expertos EN TECNOLOGÍA y los arquitectos de cloud gestionen de forma centralizada su infraestructura multicloud híbrida mediante las soluciones cloud de NetApp.

BlueXP

NetApp BlueXP amplía y mejora las funcionalidades que se proporcionan a través de Cloud Manager.

"Ve a la documentación de BlueXP"

Descubra las novedades

- "Cambios importantes en Cloud Manager"
- "Novedades en Cloud Manager"
- "Novedades en Cloud Volumes ONTAP"

Manos a la obra

- "Cloud Manager"
- "Configuración de la cuenta"
- "Cloud Volumes ONTAP para AWS"
- "Cloud Volumes ONTAP para Azure"
- "Cloud Volumes ONTAP para Google Cloud"
- "Azure NetApp Files"
- "Cloud Volumes Service para AWS"
- "Cloud Volumes Service para Google Cloud"
- "Cumplimiento de normativas en el cloud"
- "Caché de archivos global"
- "Backup a cloud"
- "Cloud Insights"

Automatización con API

- "Guía para desarrolladores de API"
- "Muestras de automatización"

Conéctese con colegas, obtenga ayuda y obtenga más información

- "Comunidad de NetApp: Servicios de datos en el cloud"

- "Soporte Cloud Volumes ONTAP de NetApp"
- "Dónde encontrar ayuda y más información"

Notas de la versión

Cloud Manager

Novedades de Cloud Manager 3.8

Cloud Manager suele introducir una nueva versión cada mes para traíd nuevas funciones, mejoras y correcciones de errores.

¿Busca una versión anterior?"Novedades en 3.7"
"Novedades en 3.6"
"Novedades en 3.5"

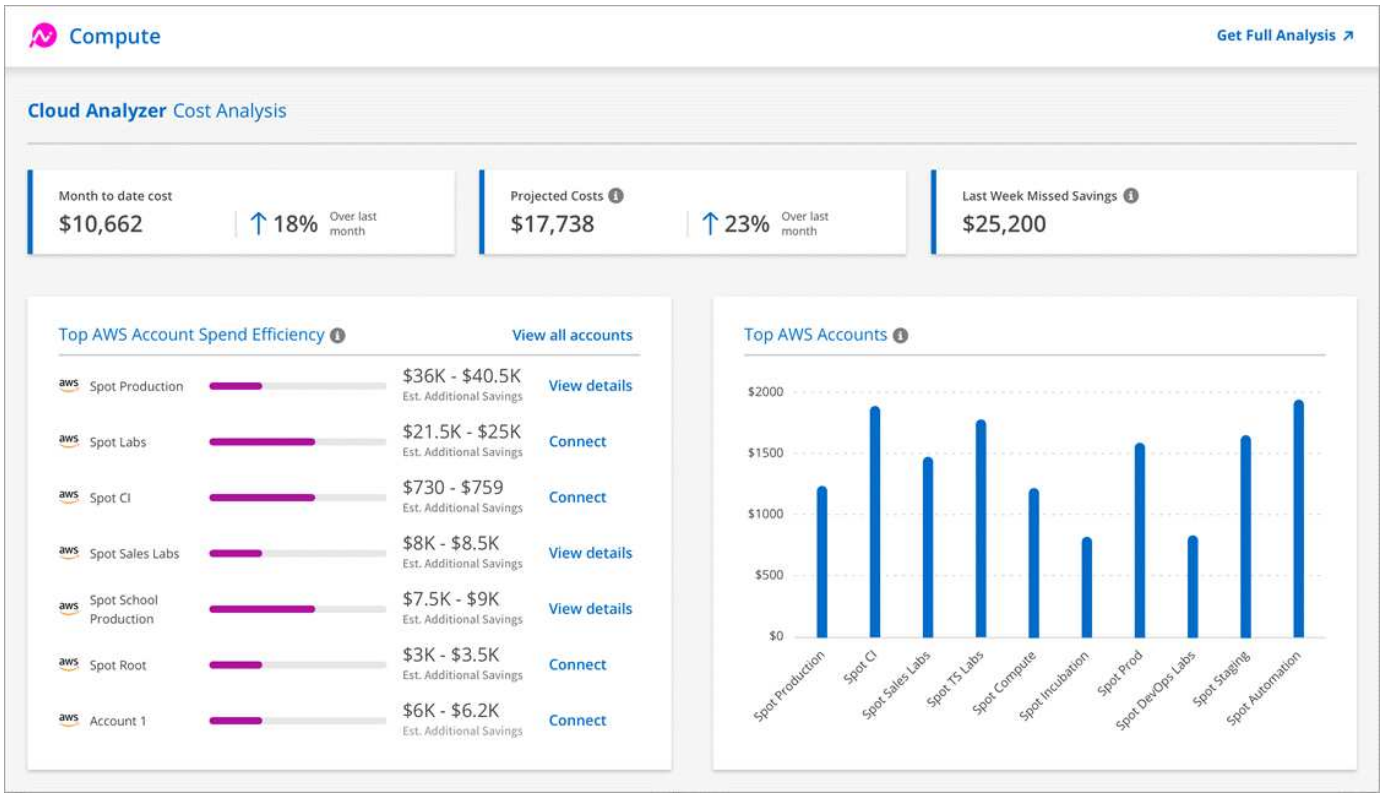
Nuevo proveedor de Terraform (19 de octubre de 2020)

Hemos desarrollado un nuevo proveedor de Terraform que los equipos de DevOps pueden utilizar con Cloud Manager para automatizar e integrar Cloud Volumes ONTAP con la infraestructura como código.

"Consulte el proveedor de cloud-Manager de netapp".

Actualización de Cloud Manager 3.8.9 (18 de octubre de 2020)

Aprovechando "Spot's Cloud Analyzer", Cloud Manager ahora puede proporcionar un análisis de costes de alto nivel de su gasto en informática en la nube e identificar ahorros potenciales. Esta información está disponible en el servicio **Compute** de Cloud Manager. "Leer más".



Actualización de Cloud Manager 3.8.9 (13 de octubre de 2020)

Hemos lanzado dos actualizaciones de Cloud Tiering:

- Las licencias de Cloud Tiering ya están disponibles en Cloud Manager.

  Pague por la organización en niveles de los datos de un clúster ONTAP en las instalaciones al cloud a través de una suscripción de pago por uso, una licencia de organización en niveles de ONTAP llamada *FabricPool*, o una combinación de ambos.

- El servicio de almacenamiento en niveles en el cloud independiente se ha retirado. Ahora debería acceder a Cloud Tiering directamente desde Cloud Manager, donde están disponibles todas las mismas funciones y funcionalidades.

Cloud Manager 3.8.9 (4 de octubre de 2020)

- Mejoras en el cumplimiento normativo del cloud
- Mejoras de Cloud Volumes Service para AWS
- Integración con Cloud Sync
- Mejoras en la gestión de cuentas
- Cambios en las regiones gubernamentales

Mejoras en el cumplimiento normativo del cloud

- Existe una nueva función de **Cloud Compliance Viewer** en Cloud Manager.

  Los usuarios a los que se asigna esta función solo pueden ver la información de cumplimiento y generar informes para los espacios de trabajo a los que tienen permiso de acceso. No pueden gestionar la configuración de Cloud Compliance y no pueden acceder a ninguna otra función y servicios de Cloud Manager. Este puede ser el papel perfecto para su equipo legal para poder controlar los resultados de Cloud Compliance Scan. Consulte "roles de usuario" para obtener más detalles.

- Se ha añadido compatibilidad para escanear esquemas de base de datos MongoDB y PostgreSQL. Consulte "analizando esquemas de base de datos" si quiere más información.
- Los precios de Cloud Compliance cambian a fecha del 7 de octubre.

  Los primeros 1 TB de datos que analiza Cloud Compliance en un espacio de trabajo de Cloud Manager son gratuitos. Esto incluye datos de Cloud Volumes ONTAP Volumes, Azure NetApp Files Volumes, bloques de Amazon S3 y esquemas de base de datos. Se requiere una suscripción para analizar cualquier dato adicional después de alcanzar 1 TB. Consulte "precios" para obtener más detalles.

Mejoras de Cloud Volumes Service para AWS

Al crear un volumen nuevo, puede optar por basar ese volumen en una copia Snapshot existente de otro volumen.

Integración con Cloud Sync

El servicio Cloud Sync de NetApp ya está disponible en Cloud Manager. Cloud Sync ofrece una forma sencilla, segura y automatizada de migrar sus datos desde cualquier destino de origen a cualquier destino de destino, en el cloud o en las instalaciones. "Leer más".

Mejoras en la gestión de cuentas

Hemos añadido más formas de gestionar tu cuenta.

- Ya está disponible una descripción general de los recursos de su cuenta.

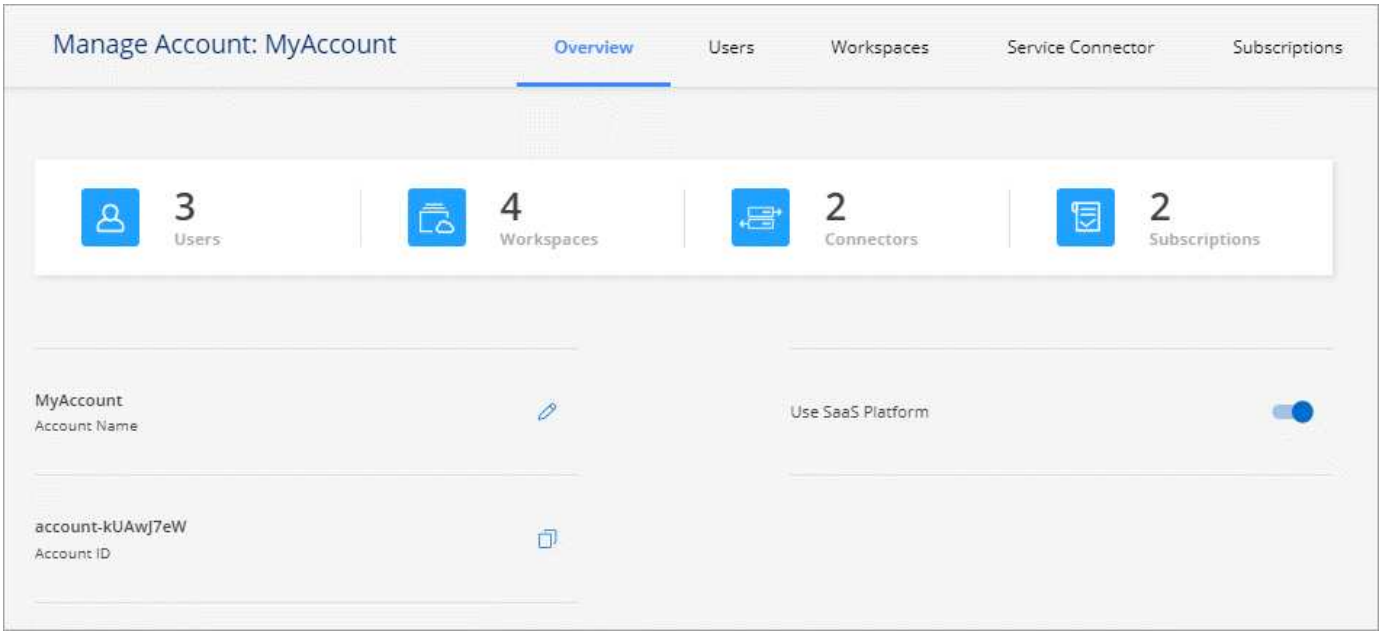
  Puede ver rápidamente el número de usuarios, áreas de trabajo, conectores y suscripciones en su cuenta.

- Puede cambiar el nombre de su cuenta.
- Puede copiar su ID de cuenta, ID de área de trabajo o ID de conector.

  Copiar estos ID ayudará con las funciones de automatización que estamos planificando.

- Puede desactivar el uso de la plataforma SaaS.

  No recomendamos desactivar la plataforma SaaS a menos que necesite para cumplir con las políticas de seguridad de su empresa. Al deshabilitar la plataforma SaaS, esto limita su capacidad para usar los servicios de cloud integrados de NetApp. "Leer más".



Cambios en las regiones gubernamentales

Si implementa un conector en una región de AWS GovCloud, una región de Azure Gov o una región de Azure DoD, el acceso a Cloud Manager solo está disponible a través de la dirección IP de host de un conector. El acceso a la plataforma SaaS está desactivado para toda la cuenta.

Esto significa que solo los usuarios con privilegios que pueden acceder al VPC/vnet interno del usuario final pueden usar la IU o la API de Cloud Manager.

"Obtenga más información sobre esta limitación".

Actualización de Cloud Manager 3.8.8 (22 de septiembre de 2020)

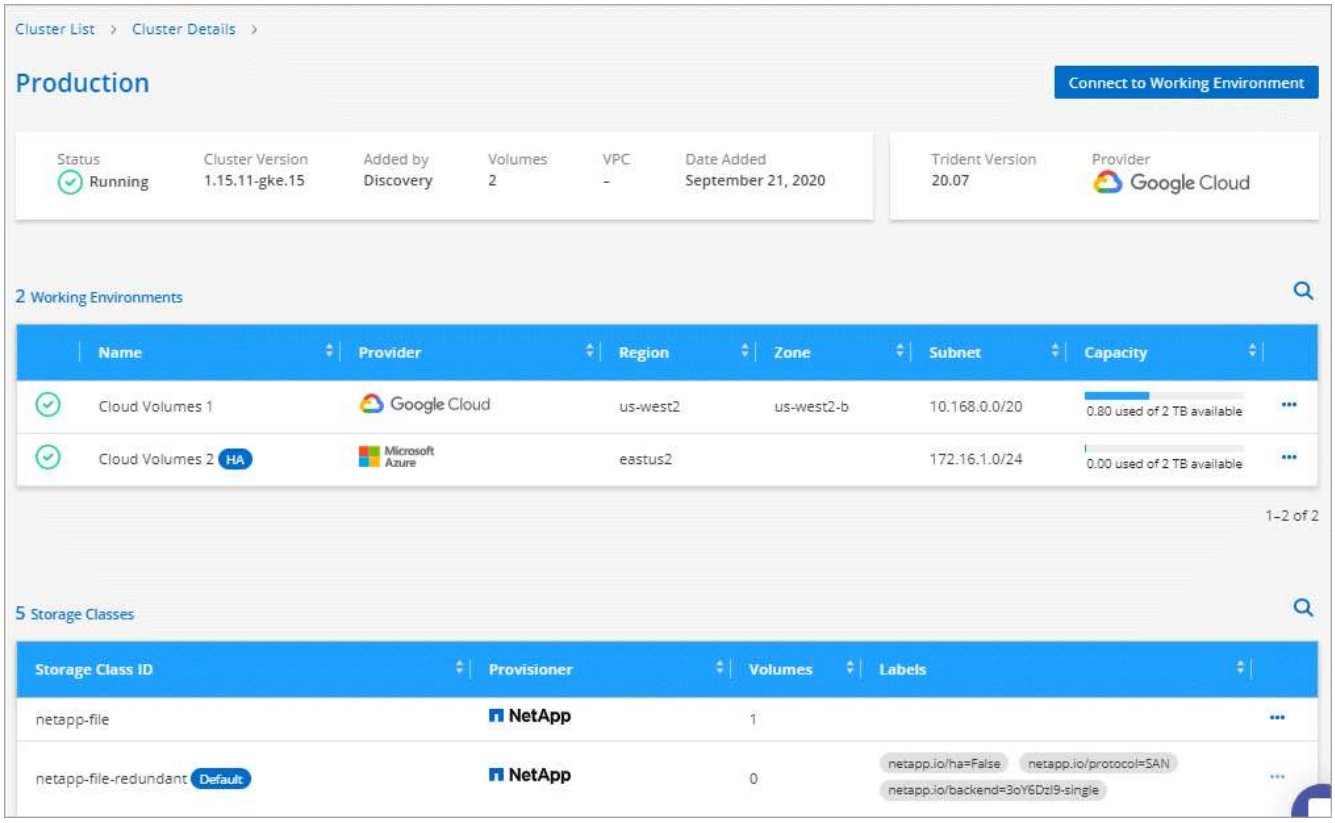
Hemos mejorado el servicio Kubernetes para facilitar el uso y el uso de funcionalidades adicionales:

- Hemos facilitado el descubrimiento de los clústeres de Kubernetes que se ejecutan en el servicio

Kubernetes gestionado de su proveedor de cloud.

Simplemente haga clic en **Discover Clusters** y Cloud Manager descubrirá sus clústeres administrados con los permisos de proveedor de cloud que ya ha proporcionado.

- Ahora puede ver más información sobre un clúster de Kubernetes detectado, incluido su estado, la cantidad de volúmenes, las clases de almacenamiento, etc.



- Hemos añadido la comprobación de los recursos y errores para garantizar que la comunicación está disponible entre el clúster y Cloud Volumes ONTAP. Si no es así, le informaremos.

"Aprenda cómo empezar".

Tenga en cuenta que la cuenta de servicio de un conector requiere los siguientes permisos para detectar y gestionar clústeres de Kubernetes que se ejecutan en Google Kubernetes Engine (GKE):

```
- container.*
```

Actualización de Cloud Manager 3.8.8 (10 de septiembre de 2020)

Las siguientes mejoras están disponibles al implementar la caché de archivos global mediante Cloud Manager:

- Un par de alta disponibilidad de Cloud Volumes ONTAP en AWS ahora es compatible como plataforma de almacenamiento de back-end para su almacenamiento central.
- Se pueden implementar varias instancias principales de caché global de archivos en un diseño de carga distribuida.

"Obtenga más información acerca de la caché global de archivos".

Cloud Manager 3.8.8 (9 de septiembre de 2020)

- Compatibilidad con Cloud Volumes Service para Google Cloud
- Backup en cloud ahora admite clústeres de ONTAP en las instalaciones
- Mejoras de backup en el cloud
- Mejoras en el cumplimiento normativo del cloud
- Navegación actualizada
- Mejoras administrativas

Compatibilidad con Cloud Volumes Service para Google Cloud

- Añada un entorno de trabajo para gestionar volúmenes existentes de Cloud Volumes Service para GCP y crear nuevos volúmenes. "Vea cómo".
- Cree y gestione volúmenes NFSv3 y NFSv4.1 para clientes de Linux y UNIX y volúmenes de SMB 3.x para clientes de Windows.
- Crear, eliminar y restaurar copias de Snapshot de volumen.

Backup en cloud ahora admite clústeres de ONTAP en las instalaciones

Empiece a realizar backups de datos desde sus sistemas ONTAP en las instalaciones al cloud. Habilite Backup en el cloud en sus entornos de trabajo en las instalaciones para realizar backups de volúmenes en el almacenamiento de Azure Blob. "Leer más".

Mejoras de backup en el cloud

Hemos revisado la interfaz de usuario para una mayor facilidad de uso:

- Página de lista de volúmenes para ver fácilmente los volúmenes de los que se va a realizar un backup junto con los backups disponibles
- Página de ajustes de copia de seguridad para ver la configuración de copia de seguridad de cada entorno de trabajo

Mejoras en el cumplimiento normativo del cloud

- Capacidad de analizar datos de bases de datos

  Analice sus bases de datos para identificar los datos personales y confidenciales que se encuentran en cada esquema. Entre las bases de datos compatibles se incluyen Oracle, SAP HANA y SQL Server (MSSQL). "Obtenga más información sobre el análisis de bases de datos".

- Capacidad de analizar volúmenes de protección de datos (DP)

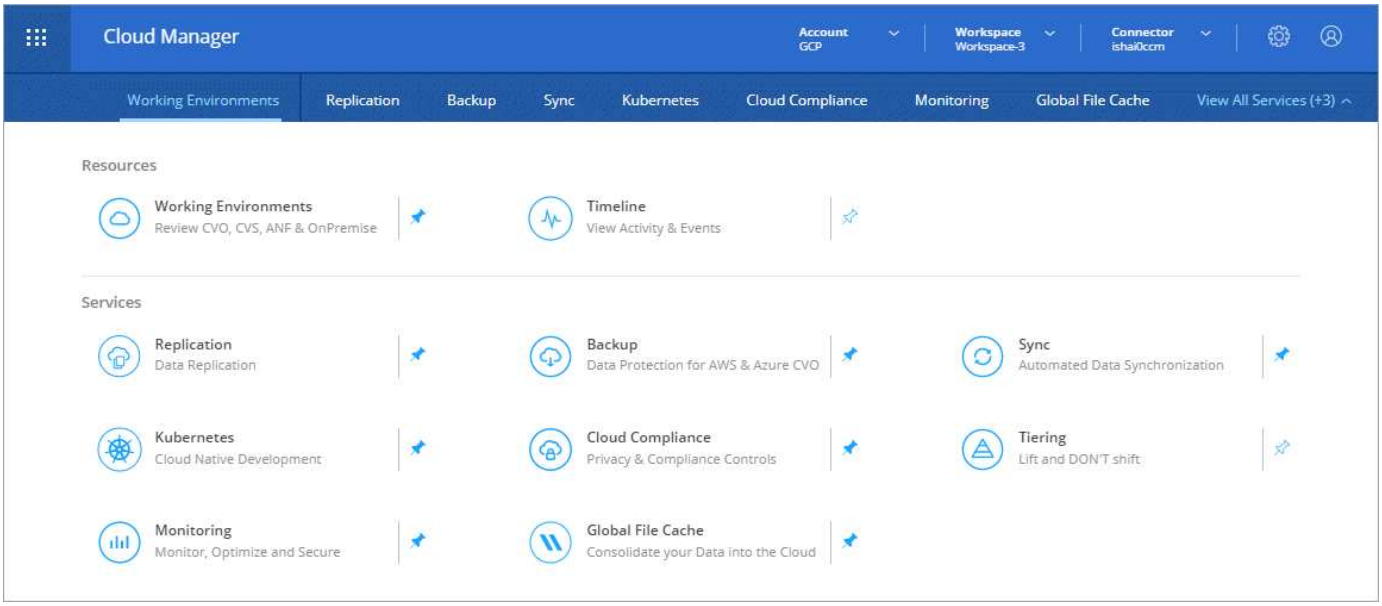
  Los volúmenes de DP son volúmenes de destino de las operaciones de SnapMirror, normalmente de los clústeres de ONTAP en las instalaciones. Ahora puede identificar fácilmente los datos personales y confidenciales que se encuentran en esos archivos en las instalaciones. "Descubra cómo".

Navegación actualizada

Hemos actualizado la cabecera en Cloud Manager para que pueda navegar más fácilmente entre los servicios

cloud de NetApp.

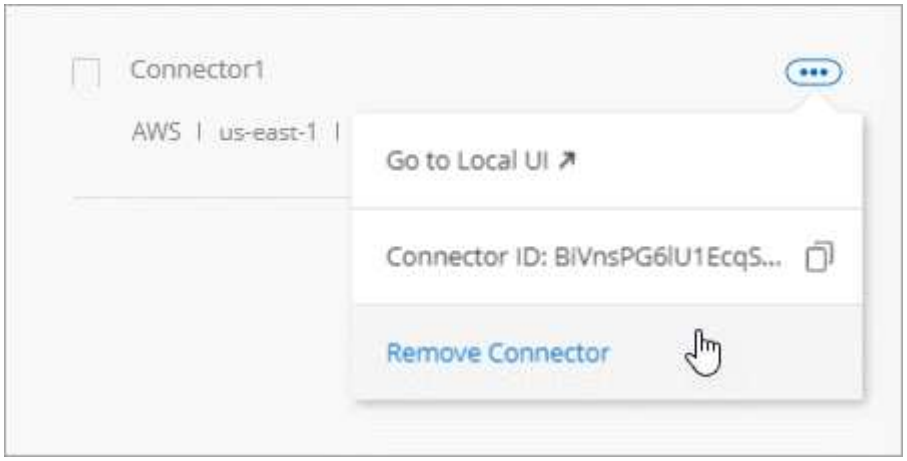
Haga clic en **Ver todos los servicios** y puede anclar y desanclar los servicios que desea ver en la navegación.



Como puede ver, también hemos actualizado las listas desplegables cuenta, espacio de trabajo y conector, por lo que es más fácil ver sus selecciones actuales.

Mejoras administrativas

- Ahora puede quitar conectores inactivos de Cloud Manager. "Vea cómo".



- Ahora puede sustituir la suscripción a Marketplace que está asociada con sus credenciales de proveedor de cloud. Si alguna vez necesita cambiar la forma en que se le cobra, este cambio puede ayudarle a asegurarse de que se le cobra a través de la suscripción a Marketplace correcta.

  Vea cómo "En AWS", "En Azure", y. "En GCP".

Actualización de los permisos de Azure necesarios (6 de agosto de 2020)

Para evitar que se produzcan errores en la implementación de Azure, asegúrese de que su política de Cloud Manager en Azure incluya el siguiente permiso:

```
"Microsoft.Resources/deployments/operationStatuses/read"
```

Ahora Azure requiere este permiso para algunas implementaciones de máquinas virtuales (depende del hardware físico subyacente que se utilice durante la implementación).

"Consulte la última política de Cloud Manager para Azure".

Cloud Manager 3.8.7 (3 de agosto de 2020)

- Nueva experiencia de software como servicio
- Mejoras de Cloud Volumes ONTAP
- Mejoras de Azure NetApp Files
- Mejoras de Cloud Volumes Service para AWS
- Mejoras en el cumplimiento normativo del cloud
- Mejoras de backup en el cloud
- Compatibilidad con caché de archivos global

Nueva experiencia de software como servicio

Hemos presentado al completo una experiencia de software como servicio para Cloud Manager. Esta nueva experiencia le facilita el uso de Cloud Manager y nos permite proporcionar funciones adicionales para gestionar su infraestructura de cloud híbrido.

Cloud Manager incluye una "Interfaz basada en SaaS" Que se integra con Cloud Central de NetApp y con conectores que permiten a Cloud Manager gestionar recursos y procesos dentro de su entorno de cloud público. (En realidad, el conector es el mismo que el software de Cloud Manager existente que ha instalado).

> En la mayoría de los casos, es necesario un conector, pero no es necesario utilizar Azure NetApp Files, Cloud Volumes Service ni Cloud Sync de Cloud Manager.

Como se ha mencionado anteriormente en estas notas de la versión, deberá actualizar el tipo de máquina de sus conectores para acceder a las nuevas capacidades que ofrecemos. Cloud Manager le pedirá instrucciones para cambiar el tipo de máquina. "Leer más".

Mejoras de Cloud Volumes ONTAP

Cloud Volumes ONTAP ofrece dos mejoras.

- **Múltiples licencias BYOL para asignar capacidad adicional**

  Ahora puede comprar varias licencias para un sistema BYOL de Cloud Volumes ONTAP con el fin de asignar más de 368 TB de capacidad. Por ejemplo, puede adquirir dos licencias para asignar hasta 736 TB de capacidad a Cloud Volumes ONTAP. O bien podría comprar cuatro licencias para obtener hasta 1.4 PB.

  El número de licencias que se pueden comprar para un único sistema de nodo o par de alta disponibilidad es ilimitado.

  Tenga en cuenta que los límites de disco pueden impedir que llegue al límite de capacidad utilizando solo discos. Puede superar el límite de discos mediante "organización en niveles de los datos inactivos en el

almacenamiento de objetos". Para obtener más información acerca de los límites de disco, consulte "Límites de almacenamiento en las notas de la versión de Cloud Volumes ONTAP".

"Aprenda a añadir una nueva licencia del sistema".

- **Cifrar discos administrados de Azure utilizando claves externas**

  Ahora puede cifrar discos gestionados de Azure en sistemas Cloud Volumes ONTAP de un solo nodo utilizando claves externas de otra cuenta. Esta función es compatible con el uso de API.

  Solo tiene que agregar lo siguiente a la solicitud API cuando crea el sistema de un solo nodo:

```
"azureEncryptionParameters": {
      "key": <azure id of encryptionset>
  }
```

  Esta función requiere nuevos permisos, como se muestra en la última "Política de Cloud Manager para Azure".

```
"Microsoft.Compute/diskEncryptionSets/read"
```

Mejoras de Azure NetApp Files

Esta versión incluye varias mejoras de soporte para Azure NetApp Files.

- **Configuración de Azure NetApp Files**

  Ahora puede configurar y gestionar Azure NetApp Files directamente desde Cloud Manager. "Vea cómo".

- **Nueva compatibilidad con el protocolo**

  Ahora es posible crear volúmenes NFSv4.1 y volúmenes SMB.

- **Gestión de instantáneas de volumen y pool de capacidad**

  Cloud Manager permite crear, eliminar y restaurar snapshots de volúmenes. También puede crear nuevos pools de capacidad y especificar sus niveles de servicio.

- **Capacidad para editar volúmenes**

  Puede editar un volumen cambiando su tamaño y gestionando las etiquetas.

Mejoras de Cloud Volumes Service para AWS

Cloud Manager admite muchas mejoras en Cloud Volumes Service para AWS.

- **Nueva compatibilidad con el protocolo**

  Ahora puede crear volúmenes NFSv4.1, volúmenes SMB y volúmenes de protocolo doble. Antes, solo podía crear y detectar volúmenes NFSv3 en Cloud Manager.

- **Compatibilidad con Snapshot**

  Es posible crear políticas de Snapshot para automatizar la creación de copias de Snapshot de volumen, crear una copia de Snapshot bajo demanda, restaurar un volumen a partir de una copia Snapshot, crear un nuevo volumen según una copia de Snapshot existente, etc. Consulte "Permite gestionar copias de Snapshot de Cloud Volumes" si quiere más información.

- **Cree el volumen inicial en una región desde Cloud Manager**

  Antes de esta versión, se debía crear el primer volumen de cada región en la interfaz de Cloud Volumes Service para AWS. Ahora puede suscribirse a. "Una de las ofertas de Cloud Volumes Service de NetApp en AWS Marketplace" Y, a continuación, cree el primer volumen desde Cloud Manager.

Mejoras en el cumplimiento normativo del cloud

Las siguientes mejoras ya están disponibles para Cloud Compliance.

- **Proceso de implementación revisado para su instancia de Cloud Compliance**

  La instancia de Cloud Compliance se configura e implementa usando un nuevo asistente de Cloud Manager. Una vez completada la implementación, se habilita el servicio para cada entorno de trabajo que desee analizar.

- **Capacidad para seleccionar los volúmenes que se van a escanear dentro de un entorno de trabajo**

  Ahora puede habilitar y deshabilitar el análisis de volúmenes individuales en un entorno de trabajo Cloud Volumes ONTAP o Azure NetApp Files. Si no necesita analizar ciertos volúmenes para asegurar el cumplimiento de normativas, apáguelos.

  "Obtenga más información sobre cómo deshabilitar el análisis de volúmenes."

- * Pestañas de navegación para saltar rápidamente a su área de interés*

  Las nuevas fichas de Panel, Investigación y Configuración permiten acceder a estas secciones con mayor facilidad.

- **Informe HIPAA**

  Ya está disponible un nuevo Informe de la Ley de Portabilidad y responsabilidad de Seguros médicos (HIPAA). Este informe está diseñado para ayudar en el requisito de su organización de cumplir con las leyes de privacidad de datos HIPAA.

  "Obtenga más información sobre el informe HIPAA."

- **Nuevo tipo de datos personales sensibles**

  Cloud Compliance puede encontrar ahora códigos médicos ICD-9-cm en archivos.

- **Nuevo tipo de datos personales**

  Cloud Compliance ahora puede encontrar dos nuevos identificadores nacionales en los archivos: Croata ID (OIB) e ID Griego.

Mejoras de backup en el cloud

Las siguientes mejoras ahora están disponibles para Backup en el cloud.

- **Traer su propia licencia (BYOL) está ahora disponible**

  Backup en Cloud solo está disponible con licencia de pago por uso (PAYGO). Una licencia BYOL le permite comprar una licencia de NetApp para usar Backup en cloud durante un determinado periodo de tiempo y un espacio de backup máximo. Cuando se alcance cualquiera de los límites, deberá renovar la licencia.

  "Más información acerca de la nueva licencia BYOL de backup en cloud."

- **Compatibilidad con volúmenes de protección de datos (DP)**

  Los volúmenes de protección de datos pueden realizarse backups y restaurarse ahora.

Compatibilidad con caché de archivos global

NetApp Global File Cache le permite consolidar silos de servidores de archivos distribuidos en un espacio de almacenamiento global cohesivo en el cloud público. Esto crea un sistema de archivos con acceso global en la nube que todas las ubicaciones distribuidas pueden usar como si fueran locales.

A partir de esta versión, la instancia de gestión de caché de archivos global y la instancia de Core se pueden implementar y gestionar a través de Cloud Manager. Esto permite ahorrar muchas horas durante el proceso de implementación inicial y ofrece un solo panel a través de Cloud Manager para este y otros sistemas implementados. Las instancias de Global File Cache Edge aún se implementan localmente en sus oficinas remotas.

Consulte "Información general sobre Global File Cache" si quiere más información.

La configuración inicial que se puede implementar mediante Cloud Manager debe cumplir con los siguientes requisitos. Otras configuraciones como Cloud Volumes Service, Azure NetApp Files y Cloud Volumes Service para AWS y GCP se siguen poniendo en marcha siguiendo los procedimientos anteriores. "Leer más".

- La plataforma de almacenamiento de back-end que utiliza como almacenamiento central debe ser un entorno de trabajo en el que haya puesto en marcha un par de alta disponibilidad de Cloud Volumes ONTAP en Azure.

  Actualmente, otras plataformas de almacenamiento y otros proveedores de cloud no son compatibles con Cloud Manager, pero se pueden poner en marcha utilizando procedimientos de puesta en marcha anteriores.

- GFC Core solo se puede poner en marcha como instancia independiente.

  Si necesita utilizar un diseño distribuido de carga que incluya varias instancias principales, debe utilizar los procedimientos heredados.

Esta función requiere nuevos permisos, como se muestra en la última "Política de Cloud Manager para Azure".

```
"Microsoft.Resources/deployments/operationStatuses/read",
"Microsoft.Insights/Metrics/Read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/extensions/delete",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
```

La mejora de la experiencia requiere un tipo de máquina más fuerte (15 de julio de 2020)

A medida que mejoremos la experiencia de Cloud Manager, necesitará actualizar el tipo de máquina para acceder a las nuevas funcionalidades que ofreceremos. Las mejoras incluirán un "Experiencia de software como servicio para Cloud Manager" e integraciones de servicios cloud nuevas y mejoradas.

Cloud Manager le pedirá instrucciones para cambiar el tipo de máquina.

A continuación se ofrecen algunos detalles:

1. Con el fin de garantizar que hay disponibles recursos adecuados para disponer de las nuevas funciones en Cloud Manager, hemos cambiado el tipo predeterminado de instancia, máquina virtual y máquina virtual:
   - AWS: t3.xlarge
   - Azure: DS3 v2
   - GCP: n1-estándar-4

   Los tamaños predeterminados son el mínimo admitido "Según los requisitos de CPU y RAM".
2. Como parte de esta transición, Cloud Manager requiere acceso al siguiente extremo para poder obtener imágenes de software de componentes de contenedores en una infraestructura Docker:

   https://cloudmanagerinfraprod.azurecr.io

   Asegúrese de que el firewall permite el acceso a este extremo desde Cloud Manager.

Cloud Manager 3.8.6 (6 de julio de 2020)

- Compatibilidad con volúmenes iSCSI
- Soporte para la política de toda la organización en niveles

Compatibilidad con volúmenes iSCSI

Cloud Manager ahora le permite crear volúmenes iSCSI para clústeres de Cloud Volumes ONTAP y ONTAP en las instalaciones directamente desde la interfaz de usuario.

Cuando se crea un volumen iSCSI, Cloud Manager crea automáticamente un LUN. Lo hemos hecho sencillo creando sólo una LUN por volumen, por lo que no hay que realizar ninguna gestión. Después de crear el volumen, "Utilice el IQN para conectarse con la LUN del hosts".

Puede crear LUN adicionales desde System Manager o desde la CLI.

Soporte para la política de toda la organización en niveles

Ahora es posible elegir la política de organización en niveles al crear o modificar un volumen para Cloud Volumes ONTAP. Cuando usa la política de todos los niveles, los datos se marcan inmediatamente como inactivos y organizados en niveles en Lo antes posible. de almacenamiento de objetos. "Más información acerca de la organización en niveles de los datos".

Transición de Cloud Manager a SaaS (22 de junio de 2020)

Presentamos una experiencia de software como servicio para Cloud Manager. Esta nueva experiencia le facilita el uso de Cloud Manager y nos permite proporcionar funciones adicionales para gestionar su infraestructura de cloud híbrido. "Leer más".

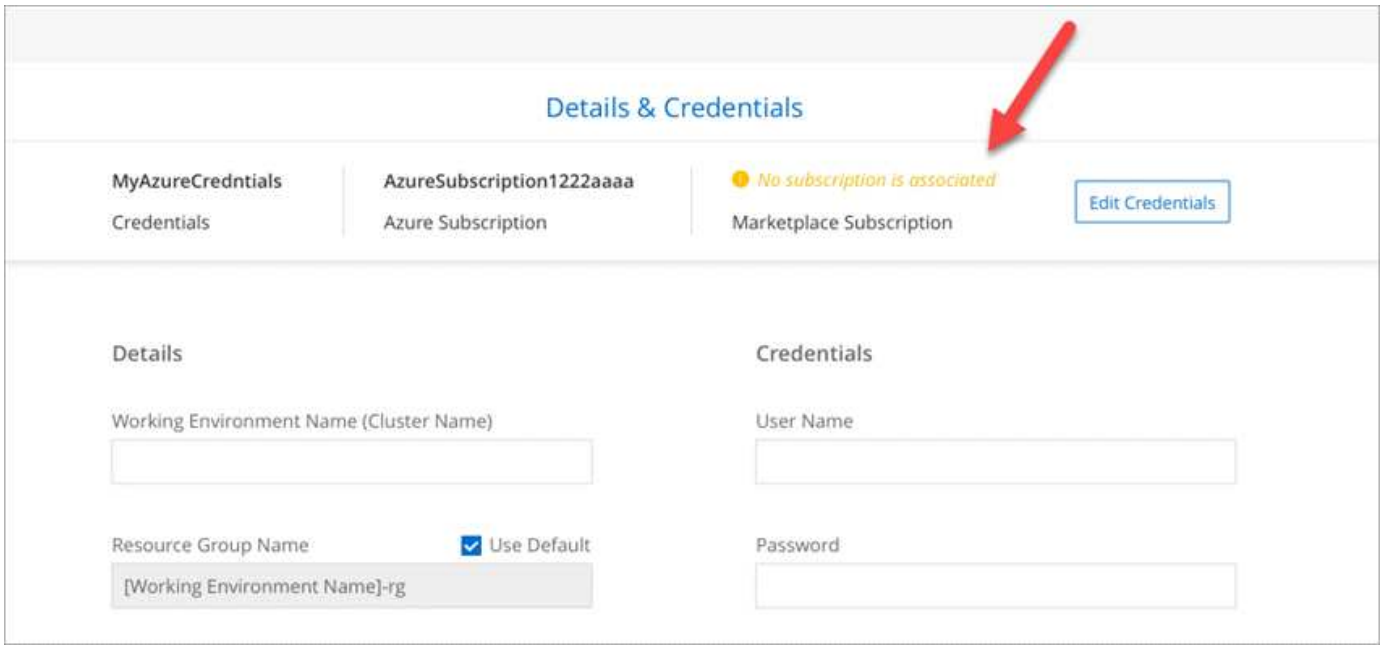
Cloud Manager 3.8.5 (31 de mayo de 2020)

- Es necesaria una nueva suscripción en Azure Marketplace
- Mejoras de backup en el cloud
- Mejoras en el cumplimiento normativo del cloud

Es necesaria una nueva suscripción en Azure Marketplace

Azure Marketplace cuenta con una nueva suscripción. Esta suscripción única es necesaria para desplegar Cloud Volumes ONTAP 9.7 PAYGO (excepto su sistema de prueba de 30 días gratis). Esta suscripción también nos permite ofrecer funciones complementarias para Cloud Volumes ONTAP PAYGO y BYOL. A partir de esta suscripción se le cobrará cada sistema Cloud Volumes ONTAP PAYGO que cree y cada función complementaria que habilite.

Cloud Manager le pedirá que se suscriba a esta oferta cuando ponga en marcha un nuevo sistema Cloud Volumes ONTAP (9.7 P1 o posterior).



Mejoras de backup en el cloud

Las siguientes mejoras ahora están disponibles para Backup en el cloud.

- En Azure, ahora puede crear un nuevo grupo de recursos o seleccionar un grupo de recursos existente en lugar de que Cloud Manager lo cree uno para usted. No se puede cambiar el grupo de recursos después de habilitar Backup en el cloud.
- En AWS, ahora puede realizar backups de instancias de Cloud Volumes ONTAP que residen en una cuenta de AWS diferente a la de AWS de Cloud Manager.
- Ahora hay disponibles más opciones al seleccionar la programación de backup para los volúmenes. Además de las opciones de backup diaria, semanal y mensual, ahora puede seleccionar una de las políticas definidas por el sistema que proporcionan normativas de combinación, como 30 backups diarios, 13 semanales y 12 mensuales.
- Después de eliminar todos los backups de un volumen, ahora es posible volver a crear backups para ese volumen. Esta era una limitación conocida en la versión anterior.

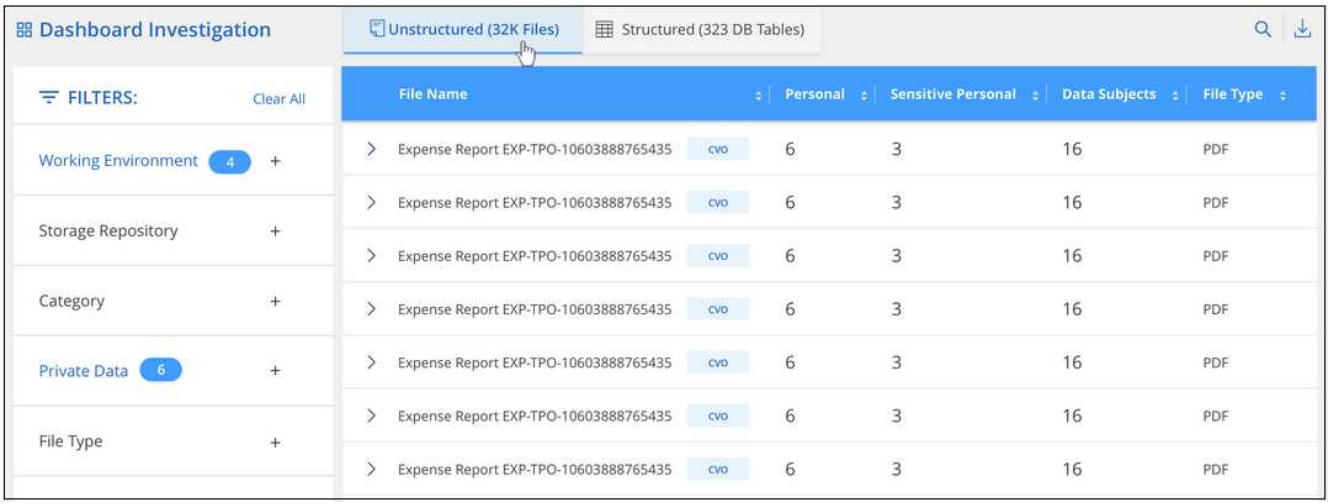
Mejoras en el cumplimiento normativo del cloud

Las siguientes mejoras están disponibles para Cloud Compliance.

- Ahora puede analizar bloques de S3 que están en cuentas de AWS diferentes a la instancia de Cloud Compliance. Solo tiene que crear una función en esa nueva cuenta para que la instancia de Cloud Compliance existente pueda conectarse a esos bloques. "Leer más".

  Si ha configurado Cloud Compliance antes de la versión 3.8.5, deberá modificar el existente "Rol IAM para la instancia de Cloud Compliance" para utilizar esta funcionalidad.

- Ahora puede filtrar el contenido de la página Investigación para que muestre sólo los resultados que desea ver. Los filtros incluyen entorno de trabajo, categoría, datos privados, tipo de archivo, fecha de última modificación, Y si los permisos del objeto S3 están abiertos al acceso público.



- Ahora puede activar y desactivar Cloud Compliance en un entorno de trabajo directamente desde la pestaña Cloud Compliance.

Actualización de Cloud Manager 3.8.4 (10 de mayo de 2020)

Lanzamos una mejora a Cloud Manager 3.8.4.

Integración con Cloud Insights

Al aprovechar el servicio Cloud Insights de NetApp, Cloud Manager le proporciona información sobre el estado y el rendimiento de sus instancias de Cloud Volumes ONTAP y le ayuda a solucionar problemas y optimizar el rendimiento de su entorno de almacenamiento en cloud. "Leer más".

Cloud Manager 3.8.4 (3 de mayo de 2020)

Cloud Manager 3.8.4 incluye la siguiente mejora.

Mejoras de backup en el cloud

Las siguientes mejoras ahora están disponibles para Backup en el cloud (anteriormente denominado *Backup to S3* para AWS):

- **Copia de seguridad en almacenamiento de Azure Blob**

  Backup en cloud ya está disponible para Cloud Volumes ONTAP en Azure. Backup en cloud proporciona funcionalidades de backup y restauración para la protección y archivado a largo plazo de sus datos en el cloud. "Leer más".

- **Eliminación de copias de seguridad**

  Ahora puede eliminar todos los backups de un volumen específico directamente desde la interfaz de Cloud Manager. "Leer más".

Cloud Manager 3.8.3 (5 de abril de 2020)

- Integración con la organización en niveles del cloud
- Migración de datos a Azure NetApp Files
- Mejoras en el cumplimiento normativo del cloud
- Backup a S3
- Volúmenes iSCSI mediante API

Integración con la organización en niveles del cloud

El servicio Cloud Tiering de NetApp ya está disponible desde Cloud Manager. Cloud Tiering le permite organizar los datos en niveles desde un clúster ONTAP en las instalaciones hasta el almacenamiento de objetos en el cloud de menor coste. De este modo se libera espacio de almacenamiento de alto rendimiento en el clúster para que se creen más cargas de trabajo.

"Leer más".

Migración de datos a Azure NetApp Files

Ahora puede migrar datos de NFS o SMB a Azure NetApp Files directamente desde Cloud Manager. El servicio Cloud Sync de NetApp alimenta la sincronización de datos.

"Descubra cómo migrar datos a Azure NetApp Files".

Mejoras en el cumplimiento normativo del cloud

Las siguientes mejoras ya están disponibles para Cloud Compliance.

- **Prueba gratuita de 30 días para Amazon S3**

  Ya está disponible una prueba gratuita de 30 días para analizar datos de Amazon S3 con Cloud Compliance. Si anteriormente habilitó Cloud Compliance en Amazon S3, su prueba gratuita de 30 días estará activa a partir de hoy (5 de abril de 2020).

  Es necesario suscribirse al AWS Marketplace para seguir analizando Amazon S3 una vez finalizada la prueba gratuita. "Aprenda a suscribirse".

  "Descubra los precios para explorar Amazon S3".

- **Nuevo tipo de datos personales**

  Cloud Compliance puede encontrar ahora un nuevo identificador nacional en los archivos: ID Brasileño (CPF).

  "Obtenga más información sobre los tipos de datos personales".

- **Soporte para categorías de metadatos adicionales**

  Cloud Compliance ahora puede clasificar sus datos en nueve categorías adicionales de metadatos. "Vea la lista completa de las categorías de metadatos compatibles".

Backup a S3

Ahora, las siguientes mejoras están disponibles para el servicio Backup to S3.

- **Política de ciclo de vida de S3 para copias de seguridad**

  Las copias de seguridad empiezan en la clase de almacenamiento *Standard* y realizan la transición a la clase de almacenamiento *Standard-Infrecuente Access* después de 30 días.

- **Eliminación de copias de seguridad**

  Ahora es posible eliminar backups con una API de Cloud Manager. "Leer más".

- **Bloquear el acceso público**

  Cloud Manager ahora habilita el "Función de acceso público en bloque de Amazon S3" En el bloque de S3, donde se almacenan los backups.

Volúmenes iSCSI mediante API

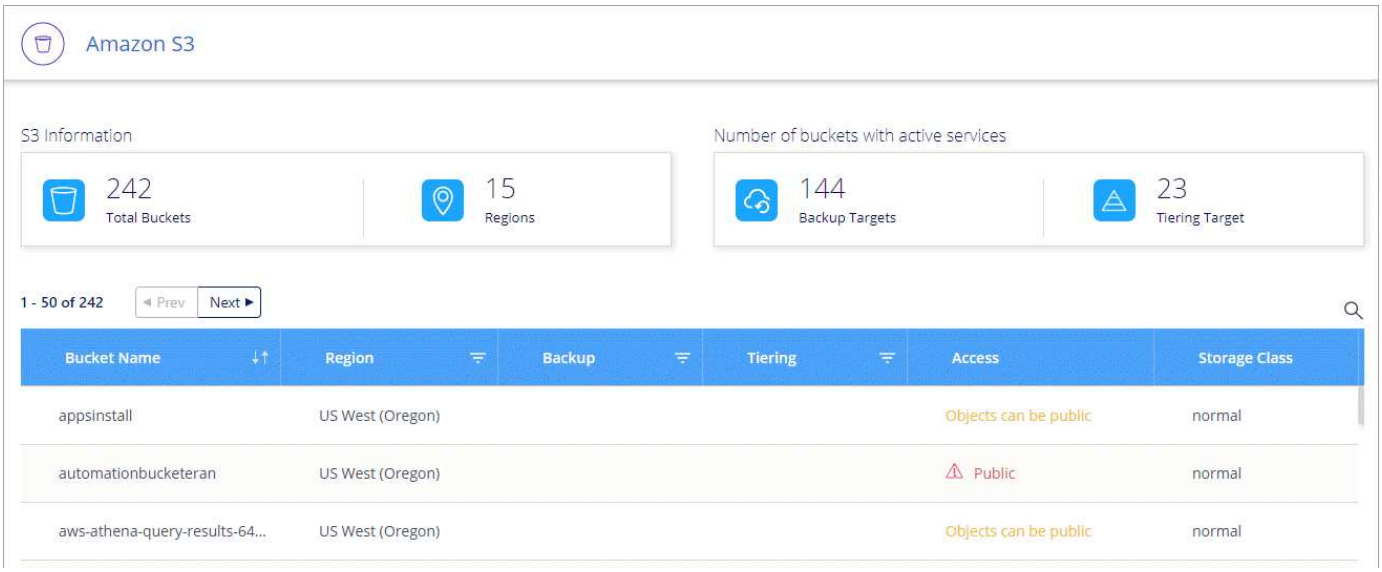
Las API de Cloud Manager ahora le permiten crear volúmenes iSCSI. "Vea un ejemplo aquí".

Cloud Manager 3.8.2 (1 de marzo de 2020)

- Entornos de trabajo de Amazon S3
- Mejoras en el cumplimiento normativo del cloud
- Versión de NFS para volúmenes
- Soporte para las regiones de Azure US Gov

Entornos de trabajo de Amazon S3

Cloud Manager ahora detecta automáticamente información sobre los bloques de Amazon S3 que residen en la cuenta de AWS en el lugar donde está instalada. Esto le permite ver fácilmente detalles sobre sus bloques de S3, incluida la región, el nivel de acceso, la clase de almacenamiento y si el bloque se utiliza con Cloud Volumes ONTAP para backups o la organización en niveles de los datos. Además, puede analizar los bloques de S3 con Cloud Compliance, como se describe a continuación.



Mejoras en el cumplimiento normativo del cloud

Las siguientes mejoras ya están disponibles para Cloud Compliance.

- **Soporte para Amazon S3**

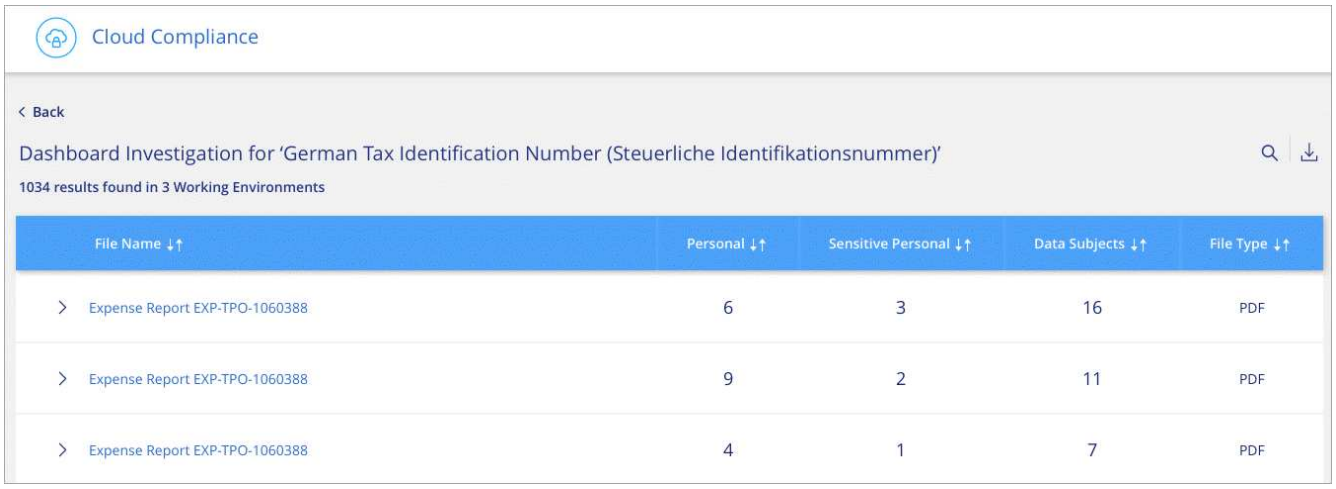
  Cloud Compliance ahora puede analizar sus buckets de Amazon S3 para identificar los datos personales y confidenciales que se encuentran en el almacenamiento de objetos S3. Cloud Compliance puede analizar cualquier bloque de la cuenta, independientemente de si se ha creado para una solución de NetApp.

  "Aprenda cómo empezar".

- **Página de investigación**

  Ahora hay disponible una nueva página de investigación para cada tipo de archivo personal, archivo personal confidencial, categoría y tipo de archivo. La página muestra los detalles de los archivos afectados y le permite ordenar por los archivos que incluyen los datos más personales, datos personales confidenciales y nombres de los temas de datos. Esta página sustituye al informe CSV que estaba disponible anteriormente.

  He aquí un ejemplo:



"Obtenga más información sobre la página Investigación".

- **PCI DSS Report**

  Ya está disponible un nuevo informe PCI DSS (estándar de seguridad de datos del sector de tarjetas de pago). Este informe puede ayudarle a identificar la distribución de la información de la tarjeta de crédito a través de sus archivos. Puede ver cuántos archivos contienen información de tarjetas de crédito, tanto si los entornos en funcionamiento están protegidos mediante cifrado o protección contra ransomware, detalles de retención, etc.

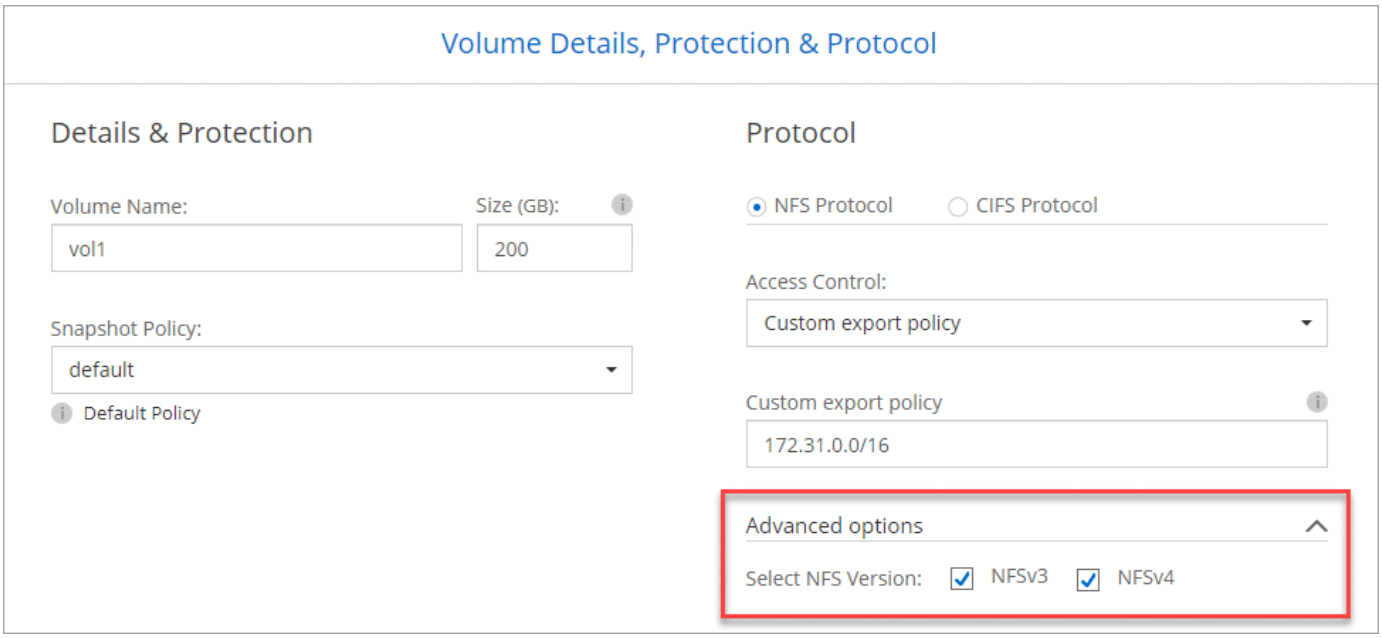
  "Obtenga más información sobre el informe PCI DSS".

- **Nuevo tipo de datos personales sensibles**

  Cloud Compliance puede encontrar ahora códigos médicos ICD-10-cm, que se utilizan en el sector médico y sanitario.

Versión de NFS para volúmenes

Ahora puede seleccionar la versión de NFS para habilitar en un volumen al crear o editar un volumen para Cloud Volumes ONTAP.



Soporte para las regiones de Azure US Gov

Los pares de alta disponibilidad de Cloud Volumes ONTAP ahora son compatibles con las regiones de Azure US Gov.

"Consulte la lista de regiones de Azure admitidas".

Actualización de Cloud Manager 3.8.1 (16 de febrero de 2020)

Lanzamos algunas mejoras a Cloud Manager 3.8.1.

Backup a S3

- Las copias de backup se almacenan ahora en un bloque de S3 que Cloud Manager crea en su cuenta de AWS, con un bloque por entorno de trabajo Cloud Volumes ONTAP.
- El backup en S3 ahora se admite en todas las regiones de AWS "Donde se admite Cloud Volumes ONTAP".
- Se puede configurar la programación de backup como diaria, semanal o mensual.
- Cloud Manager ya no tiene que configurar *private links* al servicio Backup to S3.

Se requieren permisos adicionales de S3 para estas mejoras. El rol IAM que proporciona permisos a Cloud Manager debe incluir los permisos más recientes "Política de Cloud Manager".

"Más información acerca de Backup en S3".

Actualizaciones de AWS

Hemos introducido compatibilidad con nuevas instancias EC2 y un cambio en el número de discos de datos compatibles con Cloud Volumes ONTAP 9.6 y 9.7. Compruebe los cambios en las notas de la versión de Cloud Volumes ONTAP.

- "Notas de la versión de Cloud Volumes ONTAP 9.7"
- "Notas de la versión de Cloud Volumes ONTAP 9.6"

Cloud Manager 3.8.1 (2 de febrero de 2020)

- Mejoras en el cumplimiento normativo del cloud
- Mejoras en cuentas y suscripciones
- Mejoras en la línea de tiempo

Mejoras en el cumplimiento normativo del cloud

Las siguientes mejoras ya están disponibles para Cloud Compliance.

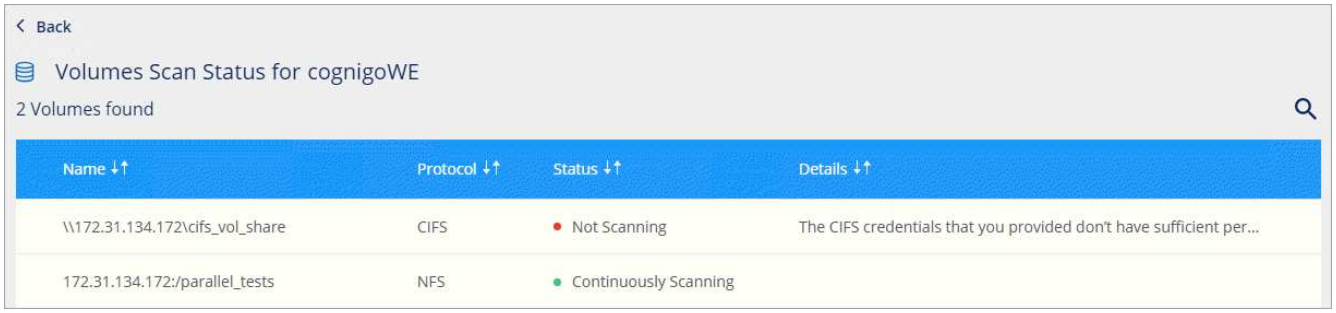
- **Soporte para Azure NetApp Files**

  Nos complace anunciar que Cloud Compliance puede analizar Azure NetApp Files para identificar los datos personales y confidenciales que se encuentran en los volúmenes.

  "Aprenda cómo empezar".

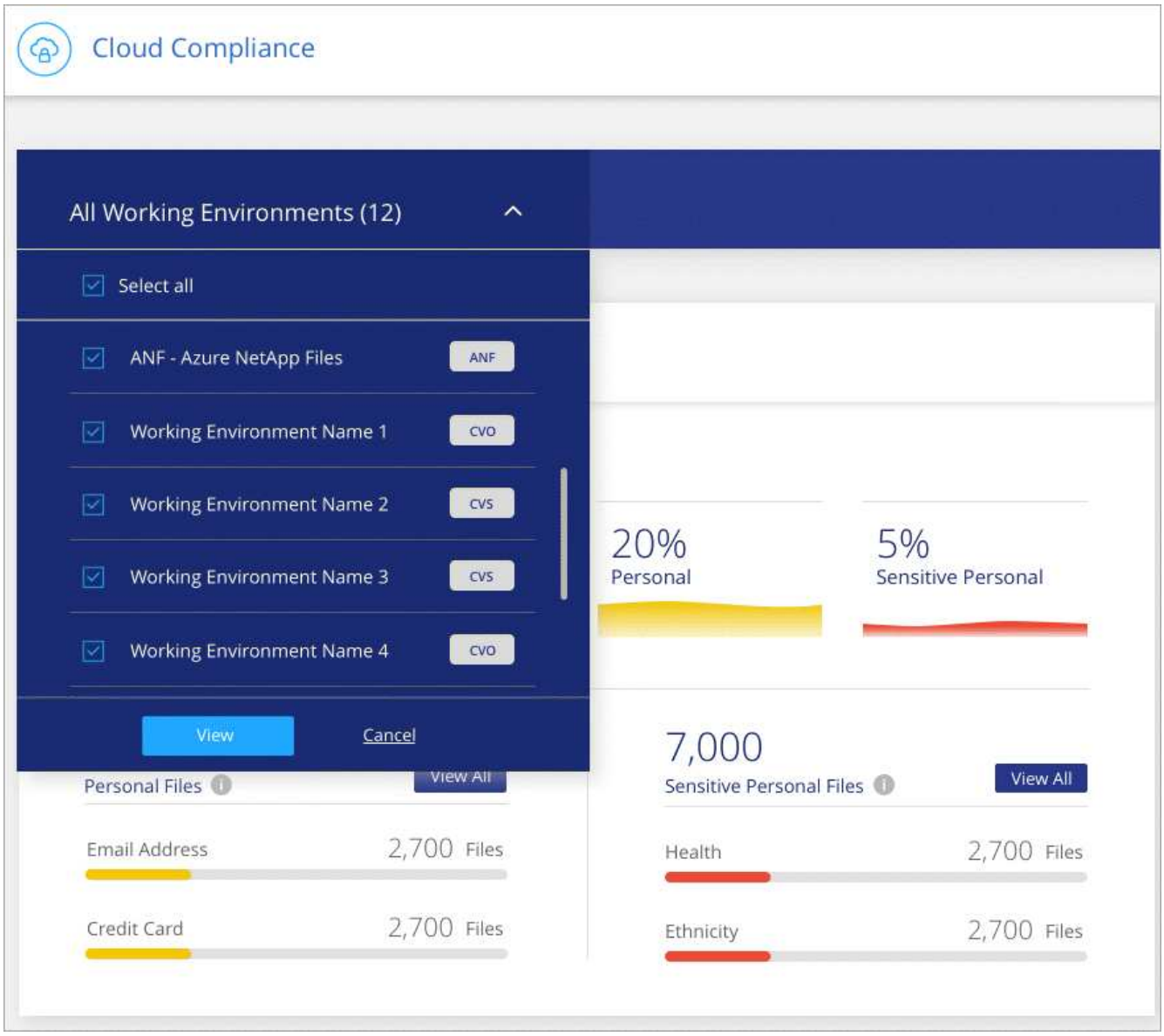
- **Estado de escaneado**

  Cloud Compliance ahora muestra el estado de los análisis de cada volumen CIFS y NFS, incluidos los mensajes de error que puede utilizar para corregir cualquier problema.



- **Filtrar tablero de mandos por medio del entorno de trabajo**

  Ahora puede filtrar el contenido de la consola de Cloud Compliance para ver los datos de cumplimiento de normativas de entornos de trabajo específicos.



- **Nuevo tipo de datos personales**

  Cloud Compliance ahora puede identificar una licencia de conducir de California al escanear datos.

- **Soporte para categorías adicionales**

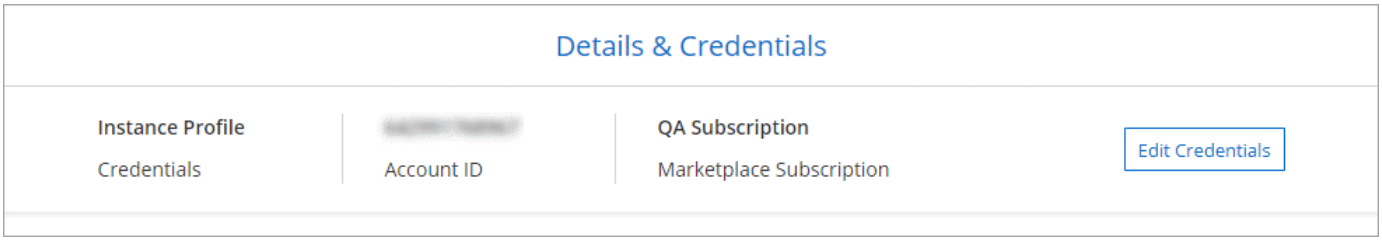
  Se admiten tres categorías adicionales: Datos de aplicación, registros y archivos de base de datos e índice.

  "Más información sobre categorías".

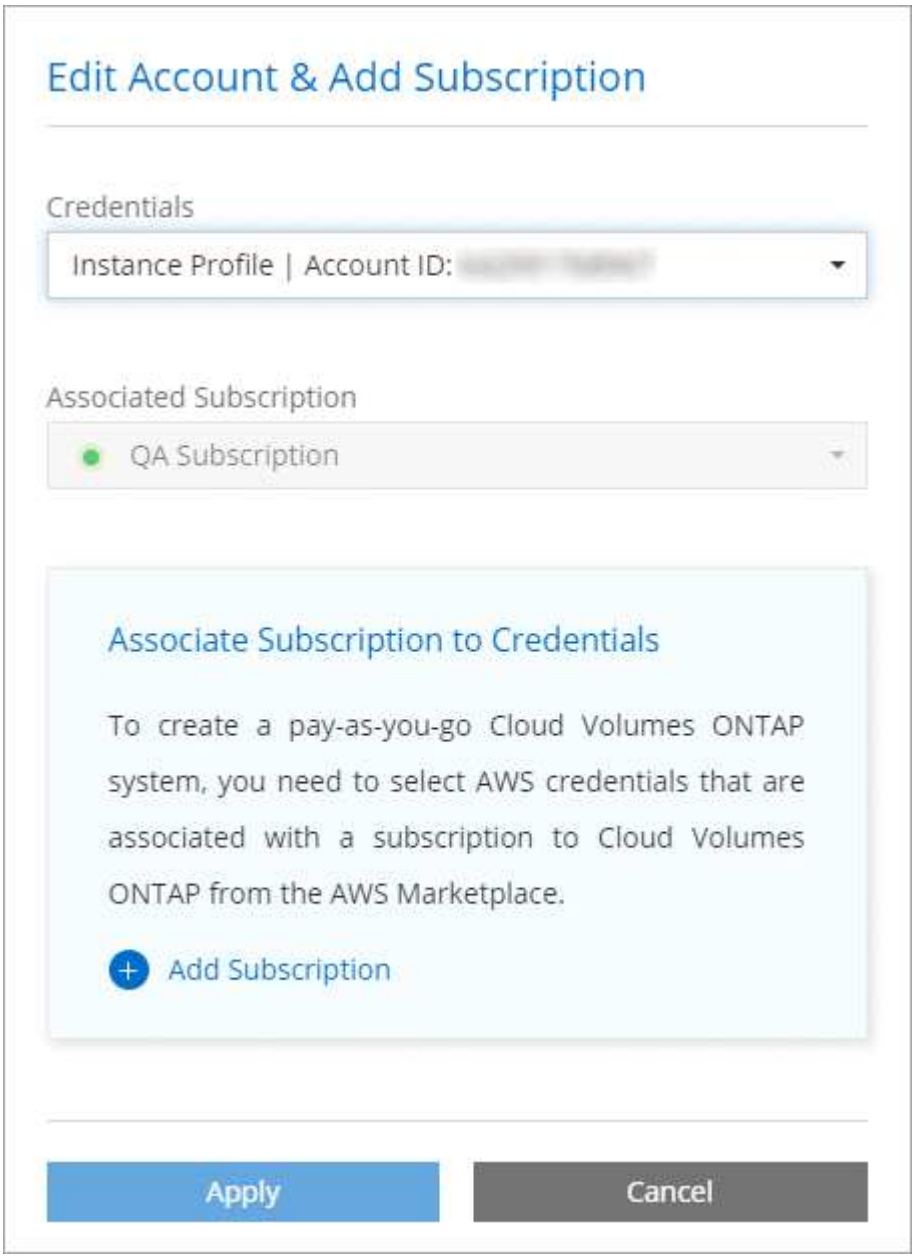
Mejoras en cuentas y suscripciones

Se ha facilitado la selección de una cuenta de AWS o de un proyecto de GCP y de una suscripción de mercado asociada para un sistema Cloud Volumes ONTAP de pago por uso. Estas mejoras ayudan a garantizar que paga con la cuenta o el proyecto adecuados.

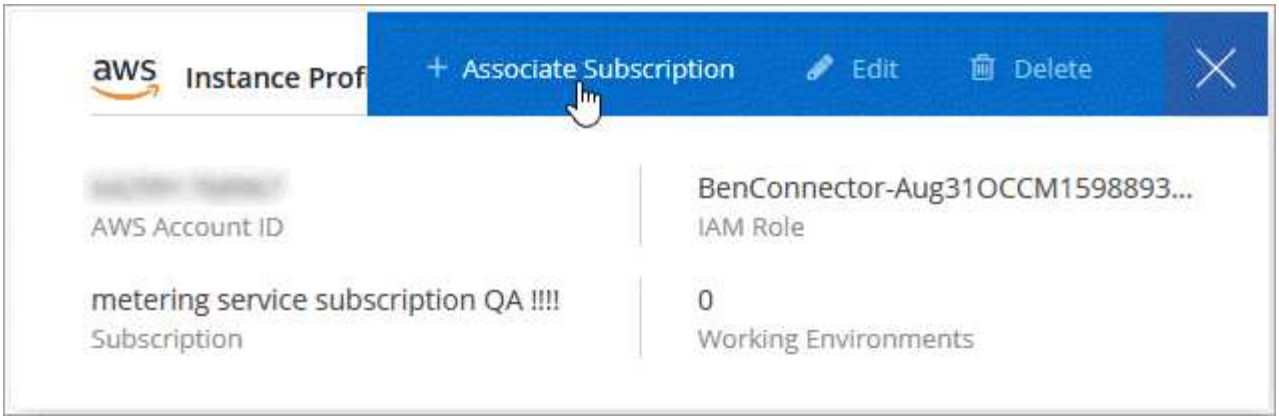
Por ejemplo, cuando cree un sistema en AWS, haga clic en **Editar credenciales** si no desea utilizar la cuenta y la suscripción predeterminadas:



Desde allí, puede elegir las credenciales de cuenta que desee utilizar y la suscripción al mercado AWS asociado. Incluso puede añadir una suscripción al mercado si lo necesita.



Además, si administra varias suscripciones de AWS, puede asignar cada una de ellas a credenciales de AWS diferentes desde la página Credentials de la configuración:

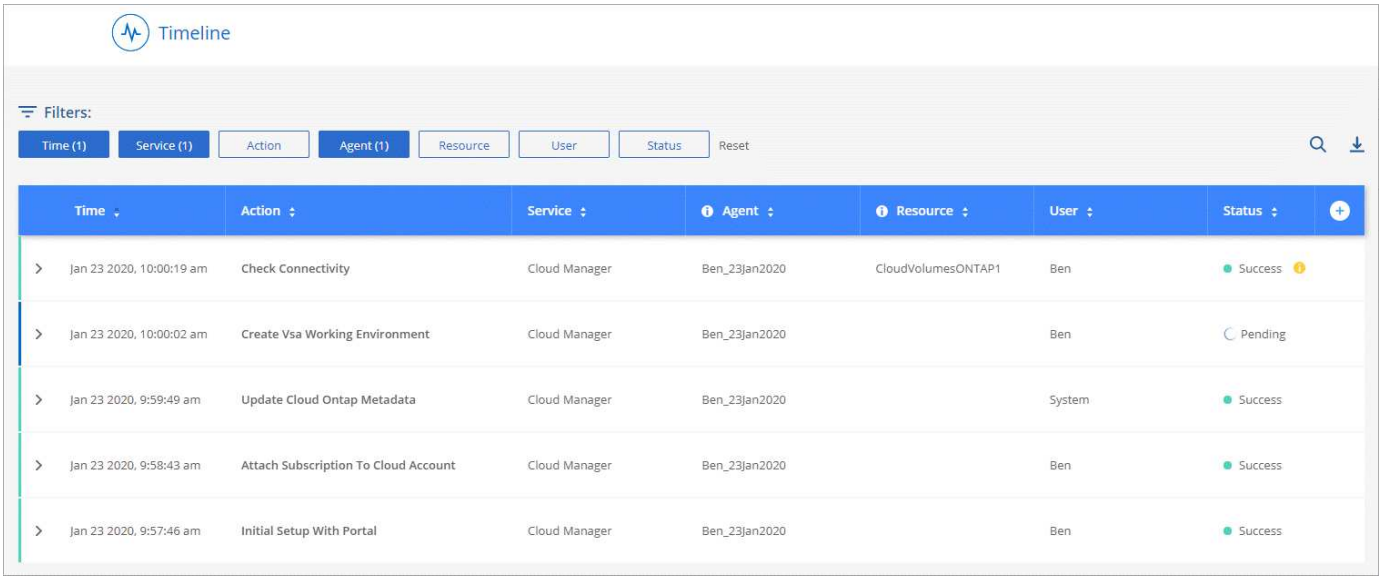


"Descubra cómo gestionar las credenciales de AWS en Cloud Manager".

Mejoras en la línea de tiempo

Se ha mejorado la escala de tiempo para proporcionarle más información acerca de los servicios cloud de NetApp que utiliza.

- La línea de tiempo ahora muestra acciones para todos los sistemas de Cloud Manager dentro de la misma cuenta de Cloud Central
- Ahora puede encontrar información más fácilmente filtrando, buscando y agregando y quitando columnas
- Ahora puede descargar los datos de la línea de tiempo en formato CSV
- En el futuro, la línea de tiempo mostrará acciones para cada servicio cloud de NetApp que utilice (pero puede filtrar la información a un único servicio).



Cloud Manager 3.8 (8 de enero de 2020)

- Mejoras de ALTA DISPONIBILIDAD en Azure
- Mejoras en la organización en niveles de datos en GCP

Mejoras de ALTA DISPONIBILIDAD en Azure

Las siguientes mejoras ahora están disponibles para las parejas de alta disponibilidad de Cloud Volumes

ONTAP en Azure.

- **Anular bloqueos CIFS para Cloud Volumes ONTAP ha en Azure**

  Ahora es posible habilitar una configuración en Cloud Manager para evitar problemas con la conmutación al nodo de respaldo del almacenamiento de Cloud Volumes ONTAP durante eventos de mantenimiento de Azure. Cuando se habilita este ajuste, Cloud Volumes ONTAP veta CIFS locks y restablece las sesiones CIFS activas. "Leer más".

- **Conexión HTTPS de Cloud Volumes ONTAP a cuentas de almacenamiento**

  Ahora puede habilitar una conexión HTTPS desde una pareja de ha Cloud Volumes ONTAP 9.7 a cuentas de almacenamiento de Azure al crear un entorno de trabajo. Tenga en cuenta que al habilitar esta opción, el rendimiento de escritura puede afectar. No se puede cambiar la configuración después de crear el entorno de trabajo.

- **Compatibilidad con las cuentas de almacenamiento de Azure v2 de uso general**

  Las cuentas de almacenamiento que crea Cloud Manager para los pares de alta disponibilidad Cloud Volumes ONTAP 9.7 ahora son cuentas de almacenamiento generales de v2.

Mejoras en la organización en niveles de datos en GCP

Las siguientes mejoras están disponibles para la organización en niveles de datos de Cloud Volumes ONTAP en GCP.

- **Clases de almacenamiento de Google Cloud para la organización en niveles de datos**

  Ahora puede elegir una clase de almacenamiento para datos por niveles en Cloud Volumes ONTAP para Google Cloud Storage:

  - Almacenamiento estándar (predeterminado)
  - Almacenamiento Nearline
  - Almacenamiento de Coldline

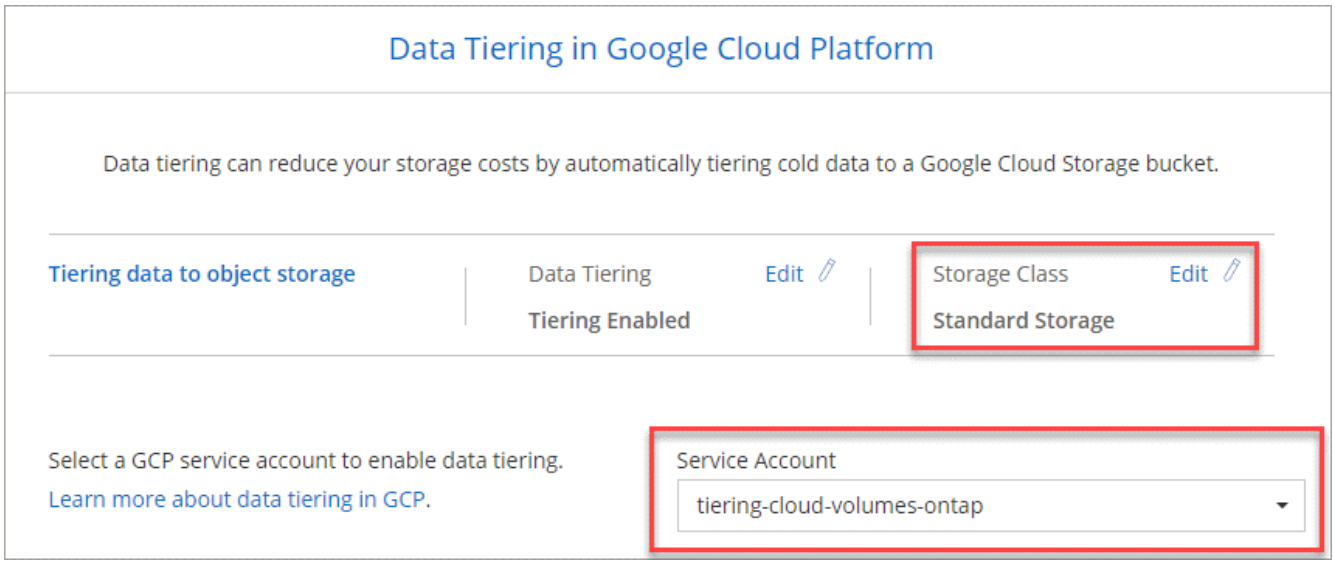
    "Obtenga más información sobre las clases de almacenamiento de Google Cloud".

  "Aprenda a cambiar la clase de almacenamiento de Cloud Volumes ONTAP".

- **Distribución de datos por niveles mediante una cuenta de servicio**

  A partir del lanzamiento de la versión 9.7, Cloud Manager ahora establece una cuenta de servicio en la instancia de Cloud Volumes ONTAP. Esta cuenta de servicio proporciona permisos para organizar los datos en niveles en un bloque de Google Cloud Storage. Este cambio ofrece más seguridad y requiere menos instalación. Para obtener instrucciones paso a paso al implementar un sistema nuevo, "consulte el paso 4 en esta página".

  En la siguiente imagen se muestra el asistente de entorno de trabajo, donde puede seleccionar una clase de almacenamiento y una cuenta de servicio:



Cloud Manager requiere los siguientes permisos de GCP para estas mejoras, como se muestra en la última "Política de Cloud Manager para GCP".

```
- storage.buckets.update
- compute.instances.setServiceAccount
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
```

Cloud Manager realiza la transición a SaaS

Hemos presentado una experiencia de software como servicio para Cloud Manager. Esta nueva experiencia le facilita el uso de Cloud Manager y nos permite proporcionar funciones adicionales para gestionar su infraestructura de cloud híbrido.

La experiencia anterior con Cloud Manager

El software Cloud Manager se compone previamente de una interfaz de usuario y una capa de gestión que envía solicitudes a proveedores de cloud. Para empezar, debería poner en marcha Cloud Manager en su red de cloud o en la red local y, después, acceder a la interfaz de usuario que se ejecuta en esa instancia.

Esa experiencia ha cambiado.

La nueva experiencia de SaaS

Ahora puede accederse a la interfaz de Cloud Manager mediante una interfaz de usuario basada en SaaS en la que inicia sesión desde Cloud Central de NetApp. Ya no es necesario acceder a una interfaz de usuario desde el software que se ejecuta en la red.

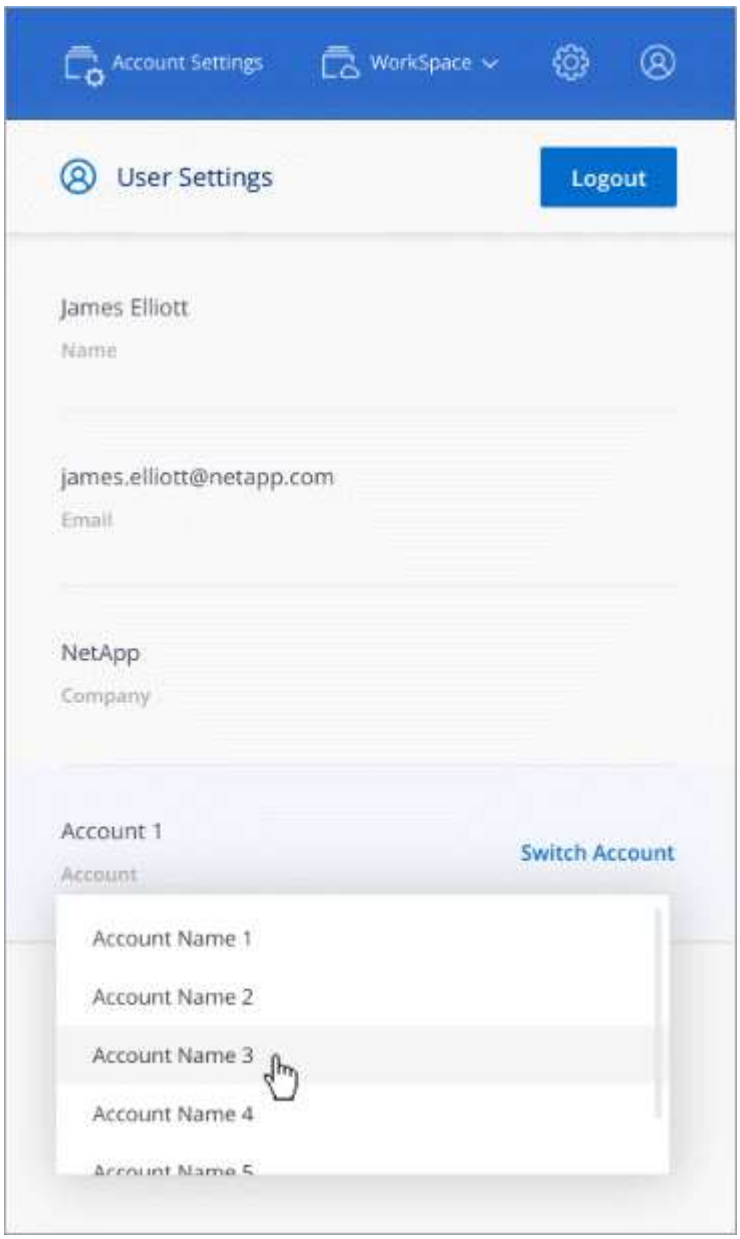
En la mayoría de los casos, necesita poner en marcha un *Connector* en su red local o en el cloud. El conector es un software necesario para gestionar Cloud Volumes ONTAP y otros servicios de datos en el cloud. (En realidad, el conector es el mismo que el software de Cloud Manager existente que ha instalado).

Beneficios

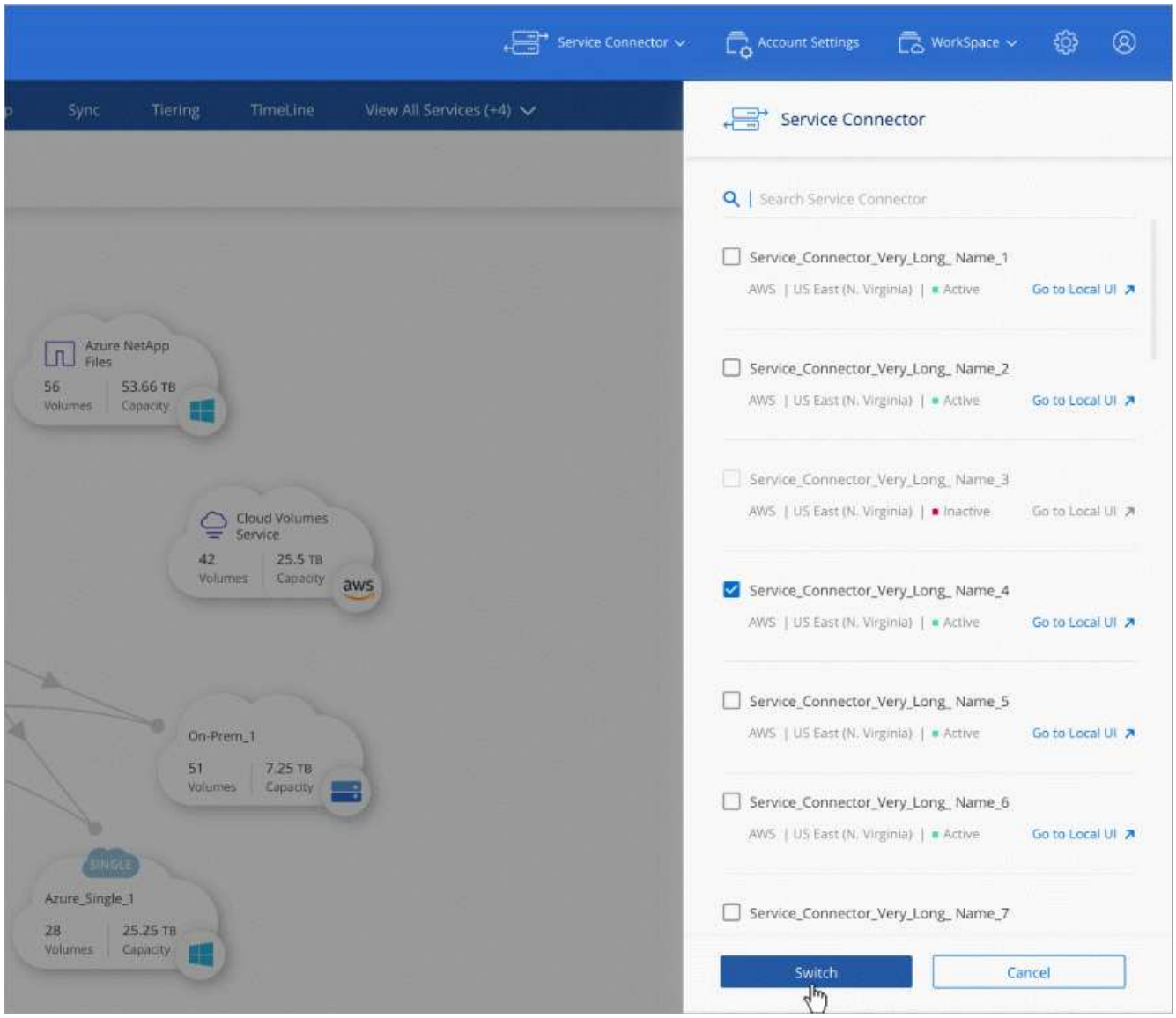
Este método basado en SaaS ofrece varias ventajas:

- Nos permite ofrecer funcionalidades de gestión adicionales para Azure NetApp Files y Cloud Volumes Service sin tener que poner en marcha software en su entorno.
- Puede cambiar fácilmente entre sus cuentas de Cloud Central.

  Si un usuario está asociado a varias cuentas de Cloud Central, puede cambiar a una cuenta diferente en cualquier momento desde el menú Configuración de usuario. A continuación, pueden ver los conectores y los entornos de trabajo asociados a esa cuenta.



- Puede cambiar fácilmente entre conectores (lo que conoce hoy como el software Cloud Manager) que están instalados en redes diferentes o en diferentes proveedores de cloud.

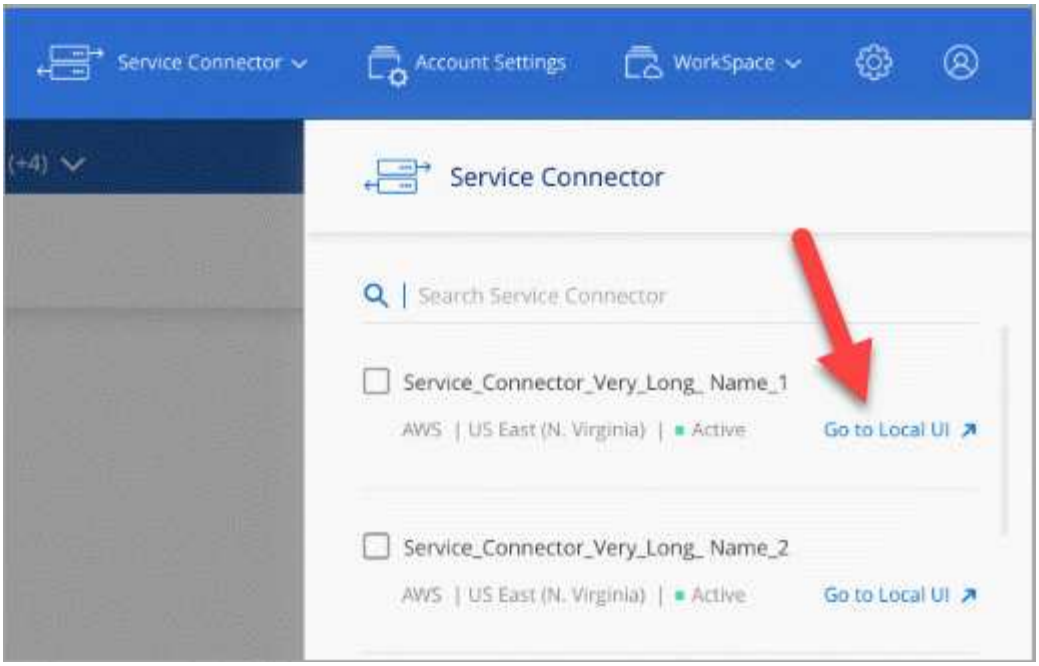


La interfaz de usuario local

Aunque debe realizar casi todas las tareas desde la interfaz de usuario de SaaS, todavía hay disponible una interfaz de usuario local en el conector. Esta interfaz es necesaria para algunas tareas que se deben realizar desde el propio conector:

- Establecimiento de un servidor proxy
- Instalación de un parche
- Descargando mensajes de AutoSupport

Puede acceder a la interfaz de usuario local directamente desde la interfaz de usuario de SaaS:



Cambios de tipo de máquina, máquina virtual y instancia

Para garantizar que haya recursos adecuados disponibles para las funciones nuevas y próximas en Cloud Manager, hemos cambiado el tipo de instancia, máquina virtual y máquina mínimo necesario de la siguiente manera:

- AWS: t3.xlarge
- Azure: DS3 v2
- GCP: n1-estándar-4

Cuando actualice el tipo de máquina, tendrá acceso a funciones como una nueva experiencia de Kubernetes, la caché global de archivos, la supervisión, etc.

Los tamaños predeterminados son el mínimo admitido "Según los requisitos de CPU y RAM".

Cloud Manager le pedirá instrucciones para cambiar el tipo de máquina del conector.

Problemas conocidos

Los problemas conocidos identifican problemas por los que el uso correcto de esta versión del producto puede resultar imposible.

No existen problemas conocidos en esta versión de Cloud Manager.

Es posible encontrar problemas conocidos de Cloud Volumes ONTAP en la "Notas de la versión de Cloud Volumes ONTAP" Y para el software ONTAP en general en la "Notas de la versión de ONTAP".

Limitaciones conocidas

Las limitaciones conocidas identifican plataformas, dispositivos o funciones que no son compatibles con esta versión del producto o cuya interoperabilidad con esta no es óptima. Revise estas limitaciones detenidamente.

Los conectores deben permanecer en funcionamiento

Un conector debe permanecer en funcionamiento en todo momento. Es importante para la salud y el funcionamiento continuos de los servicios que usted habilita.

Por ejemplo, un conector es un componente clave en la salud y el funcionamiento de los sistemas de Cloud Volumes ONTAP PAYGO. Si el conector está apagado, los sistemas de Cloud Volumes ONTAP PAYGO se apagarán tras perder la comunicación con un conector durante más de 14 días.

La plataforma SaaS está deshabilitada para las regiones gubernamentales

Si implementa un conector en una región de AWS GovCloud, una región de Azure Gov o una región de Azure DoD, el acceso a Cloud Manager solo está disponible a través de la dirección IP de host de un conector. El acceso a la plataforma SaaS está desactivado para toda la cuenta.

Esto significa que solo los usuarios con privilegios que pueden acceder al VPC/vnet interno del usuario final pueden usar la IU o la API de Cloud Manager.

También significa que Cloud Manager no ofrece los siguientes servicios:

- Cumplimiento de normativas en el cloud
- Kubernetes
- Organización en niveles del cloud
- Caché de archivos global
- Supervisión (Cloud Insights)

Se requiere la plataforma SaaS para usar estos servicios.

No se admiten los hosts Linux compartidos

El conector no es compatible con un host compartido con otras aplicaciones. El host debe ser un host dedicado.

Cloud Manager no es compatible con FlexGroup Volumes

Aunque Cloud Volumes ONTAP es compatible con FlexGroup Volumes, Cloud Manager no lo hace. Si crea un volumen de FlexGroup desde System Manager o desde la interfaz de línea de comandos, debe configurar el modo de gestión de capacidad de Cloud Manager en Manual. El modo automático puede no funcionar correctamente con volúmenes de FlexGroup.

Cambios importantes en Cloud Manager

En esta página, se destacan cambios importantes en Cloud Manager que pueden ayudarle a utilizar el servicio a medida que presentamos nuevas mejoras. Debe seguir leyendo el "Novedades" página para obtener información sobre las nuevas funciones y mejoras.

Cambios en SaaS

Hemos introducido una experiencia de software como servicio para Cloud Manager. Esta nueva experiencia le facilita el uso de Cloud Manager y nos permite proporcionar funciones adicionales para gestionar su infraestructura de cloud híbrido.

- "Cloud Manager realiza la transición a SaaS"
- "Descubra cómo funciona Cloud Manager"

Cambios de tipo de máquina

Para garantizar que haya recursos adecuados disponibles para las funciones nuevas y próximas en Cloud Manager, hemos cambiado el tipo de instancia, máquina virtual y máquina mínimo necesario de la siguiente manera:

- AWS: t3.xlarge
- Azure: DS3 v2
- GCP: n1-estándar-4

Cuando actualice el tipo de máquina, tendrá acceso a funciones como una nueva experiencia de Kubernetes, la caché global de archivos, la supervisión, etc.

Los tamaños predeterminados son el mínimo admitido "Según los requisitos de CPU y RAM".

Cloud Manager le pedirá instrucciones para cambiar el tipo de máquina del conector.

Configuración de la cuenta

Presentamos las cuentas de Cloud Central para proporcionar multi-tenancy, para ayudarle a organizar usuarios y recursos en espacios de trabajo aislados y para gestionar el acceso a conectores y suscripciones.

- "Obtenga información acerca de las cuentas de Cloud Central: Usuarios, espacios de trabajo, conectores y suscripciones"
- "Aprenda cómo empezar a utilizar su cuenta"
- "Aprenda a administrar su cuenta después de configurarla arriba"

Nuevos permisos

De vez en cuando, Cloud Manager requiere permisos adicionales de proveedores de cloud, ya que presentamos nuevas funciones y mejoras. Esta sección identifica los nuevos permisos que ahora son necesarios.

Puede encontrar la lista más reciente de permisos en "Políticas de Cloud Manager".

AWS

A partir de la versión 3.8.1, se necesitan los siguientes permisos para utilizar Backup en la nube con Cloud Volumes ONTAP. "Leer más".

```
{
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws:s3:::netapp-backup-*"
            ]
        },
```

Azure

- Para evitar que se produzcan errores en la implementación de Azure, asegúrese de que su política de Cloud Manager en Azure incluya el siguiente permiso:

```
"Microsoft.Resources/deployments/operationStatuses/read"
```

- A partir de la versión 3.8.7, se requiere el siguiente permiso para cifrar los discos gestionados de Azure en sistemas Cloud Volumes ONTAP de un solo nodo mediante claves externas de otra cuenta. "Leer más".

```
"Microsoft.Compute/diskEncryptionSets/read"
```

- Se requieren los siguientes permisos para habilitar la caché de archivos global en Cloud Volumes ONTAP. "Leer más".

```
"Microsoft.Resources/deployments/operationStatuses/read",
"Microsoft.Insights/Metrics/Read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/extensions/delete",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
```

GCP

Nuevos permisos para la gestión de Kubernetes

A partir del lanzamiento de la versión 3.8.8, la cuenta de servicio de un conector requiere los siguientes permisos para detectar y gestionar clústeres de Kubernetes que se ejecutan en Google Kubernetes Engine (GKE):

```
- container.*
```

Nuevos permisos para organización en niveles de los datos

A partir de la versión 3.8, se necesitan los siguientes permisos para utilizar una cuenta de servicio para la organización en niveles de datos. "Leer más".

```
- storage.buckets.update
- compute.instances.setServiceAccount
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
```

Nuevos puntos finales

El conector requiere acceso saliente a Internet para gestionar recursos y procesos dentro de su entorno de nube pública. En esta sección se identifican los nuevos puntos finales que ahora se requieren.

Puede encontrar el "lista completa de puntos finales a los que se accede desde su navegador web aquí" y la "Lista completa de puntos finales a los que accede el conector aquí".

- Los usuarios deben acceder a Cloud Manager desde un explorador web mediante la contacto con el siguiente extremo:

  https://cloudmanager.netapp.com

- Los conectores requieren acceso al siguiente extremo para obtener imágenes de software de componentes de contenedor para una infraestructura Docker:

  https://cloudmanagerinfraprod.azurecr.io

  Asegúrese de que el firewall permite el acceso a este extremo desde el conector.

Comience a usar Cloud Manager

Obtenga más información sobre Cloud Manager

Cloud Manager permite que los expertos EN TECNOLOGÍA y los arquitectos de cloud gestionen de forma centralizada su infraestructura multicloud híbrida mediante las soluciones cloud de NetApp.

Funciones

Cloud Manager es una plataforma de gestión basada en SaaS empresarial que le mantiene el control de sus datos independientemente de dónde estén.

- Configuración y uso "Cloud Volumes ONTAP" para lograr una gestión de datos eficiente con varios protocolos en todos los clouds.
- Configure y utilice los servicios de almacenamiento de archivos: "Azure NetApp Files", "Cloud Volumes Service para AWS", y. "Cloud Volumes Service para Google Cloud".
- Descubra y gestione sus clústeres de ONTAP en las instalaciones creando volúmenes, realizando backups en el cloud, replicando datos en el cloud híbrido y organizando en niveles los datos inactivos en el cloud.
- Habilite software y servicios cloud integrados como "Cumplimiento de normativas en el cloud", "Cloud Insights", "Cloud Backup Service", "Trident", y más.

"Obtenga más información sobre Cloud Manager".

Proveedores de almacenamiento de objetos admitidos

Cloud Manager le permite gestionar el almacenamiento en cloud y usar servicios cloud en Amazon Web Services, Microsoft Azure y Google Cloud.

Coste

El software Cloud Manager es gratuito en NetApp.

Para la mayoría de tareas, Cloud Manager solicita que ponga en marcha un conector en la red de cloud, lo cual da como resultado cargos del proveedor de cloud por la instancia de computación y el almacenamiento asociado. Tiene la opción de ejecutar el software Connector en sus instalaciones.

Cómo funciona Cloud Manager

Cloud Manager incluye una interfaz basada en SaaS integrada con Cloud Central de NetApp y conectores que gestionan Cloud Volumes ONTAP y otros servicios de cloud.

Software como servicio

Se puede acceder a Cloud Manager a través de una "Interfaz de usuario basada en SaaS" Y API. Esta experiencia SaaS le permite acceder automáticamente a las últimas funciones a medida que se publican y cambiar fácilmente entre las cuentas y conectores de Cloud Central.

Cloud Central de NetApp

"Cloud Central de NetApp" proporciona una ubicación centralizada para acceder y gestionar "Servicios en nube de NetApp". Con la autenticación de usuario centralizada, puede usar el mismo conjunto de credenciales para acceder a Cloud Manager y otros servicios cloud como Cloud Insights.

Cuando inicia sesión en Cloud Manager por primera vez, se le solicita que cree una cuenta *Cloud Central*. Esta cuenta proporciona multi-tenancy y le permite organizar usuarios y recursos en espacios de trabajo aislados.

Conectores

En la mayoría de los casos, un administrador de cuentas tendrá que poner en marcha un *Connector* en su red local o en la nube. El conector permite a Cloud Manager gestionar recursos y procesos dentro de su entorno de cloud público.

Un conector debe permanecer en funcionamiento en todo momento. Es importante para la salud y el funcionamiento continuos de los servicios que usted habilita.

Por ejemplo, un conector es un componente clave en la salud y el funcionamiento de los sistemas de Cloud Volumes ONTAP PAYGO. Si el conector está apagado, los sistemas de Cloud Volumes ONTAP PAYGO se apagarán tras perder la comunicación con un conector durante más de 14 días.

"Obtenga más información sobre cuándo se necesitan los conectores y cómo trabajo".

Información general sobre redes

Antes de que los usuarios inicien sesión en Cloud Manager, tendrá que asegurarse de que sus exploradores web pueden acceder a determinados extremos. Después de esto, debe verificar los requisitos de red para el tipo específico de entorno de trabajo y servicios que se utilizarán.

Puntos finales a los que se accede desde su navegador web

Los usuarios deben acceder a Cloud Manager desde un explorador web. La máquina que ejecuta el explorador Web debe tener conexiones con los siguientes puntos finales:

Puntos finales	Específico
https://cloudmanager.cloud.netapp.com	Para conectarlo a la interfaz SaaS de Cloud Manager.
https://api.services.cloud.netapp.com	Para ponerse en contacto con las API de Cloud Central.
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	El explorador web se conecta con estos extremos para conseguir una autenticación de usuario centralizada mediante NetApp Cloud Central.
https://widget.intercom.io	Si busca un chat integrado en los productos que le permita hablar con expertos en cloud de NetApp.

Índice de requisitos de red

- "Conectores"

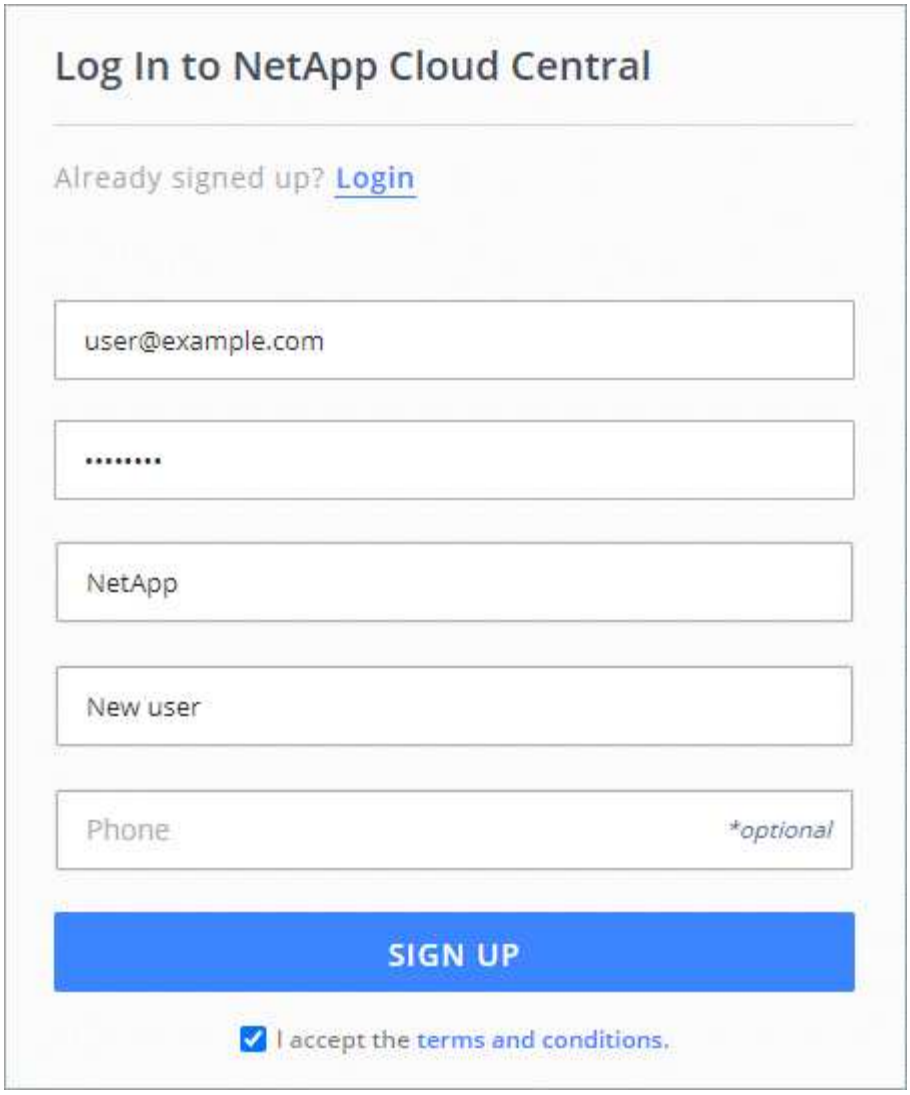
- "Cloud Volumes ONTAP para AWS"
- "Cloud Volumes ONTAP para Azure"
- "Cloud Volumes ONTAP para GCP"
- "Replicación de datos entre sistemas ONTAP"
- "Cloud Compliance para Cloud Volumes ONTAP o Azure NetApp Files"
- "Cloud Compliance para Amazon S3"
- "Clústeres de ONTAP en las instalaciones"
  - "Organización en niveles de los datos desde clústeres de ONTAP a Amazon S3"
  - "Organización en niveles de los datos desde los clústeres de ONTAP hasta el almacenamiento de Azure Blob"
  - "Organización en niveles de los datos desde clústeres de ONTAP a Google Cloud Storage"
  - "Organización en niveles de los datos desde clústeres de ONTAP a StorageGRID"

Suscripción a NetApp Cloud Central

Regístrese en Cloud Central de NetApp para acceder a los servicios cloud de NetApp.

Pasos

1. Abra un explorador web y vaya a. "Cloud Central de NetApp".
2. Haga clic en **Registrarse**.
3. Rellene el formulario y haga clic en **Registrarse**.



4. Espere a que aparezca un correo electrónico de NetApp Cloud Central.
5. Haga clic en el vínculo del correo electrónico para verificar su dirección de correo electrónico.

Resultado

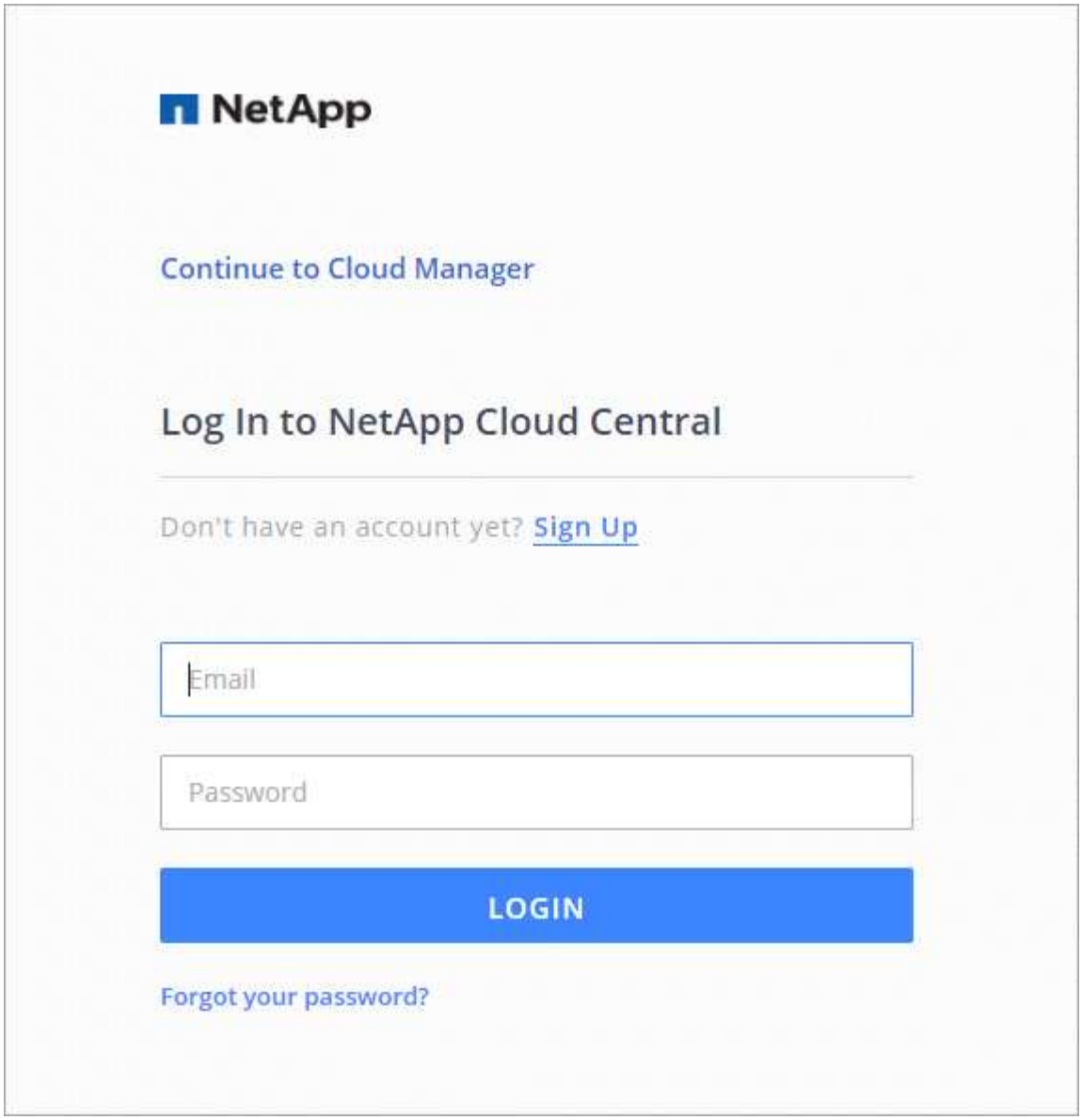
Ahora tiene un inicio de sesión de usuario activo de Cloud Central.

Inicio de sesión en Cloud Manager

Un usuario basado en SaaS puede acceder a la interfaz de Cloud Manager interfaz vaya a. https://cloudmanager.netapp.com.

Pasos

1. Abra un explorador web y vaya a. https://cloudmanager.netapp.com.
2. Inicie sesión con sus credenciales de Cloud Central de NetApp.



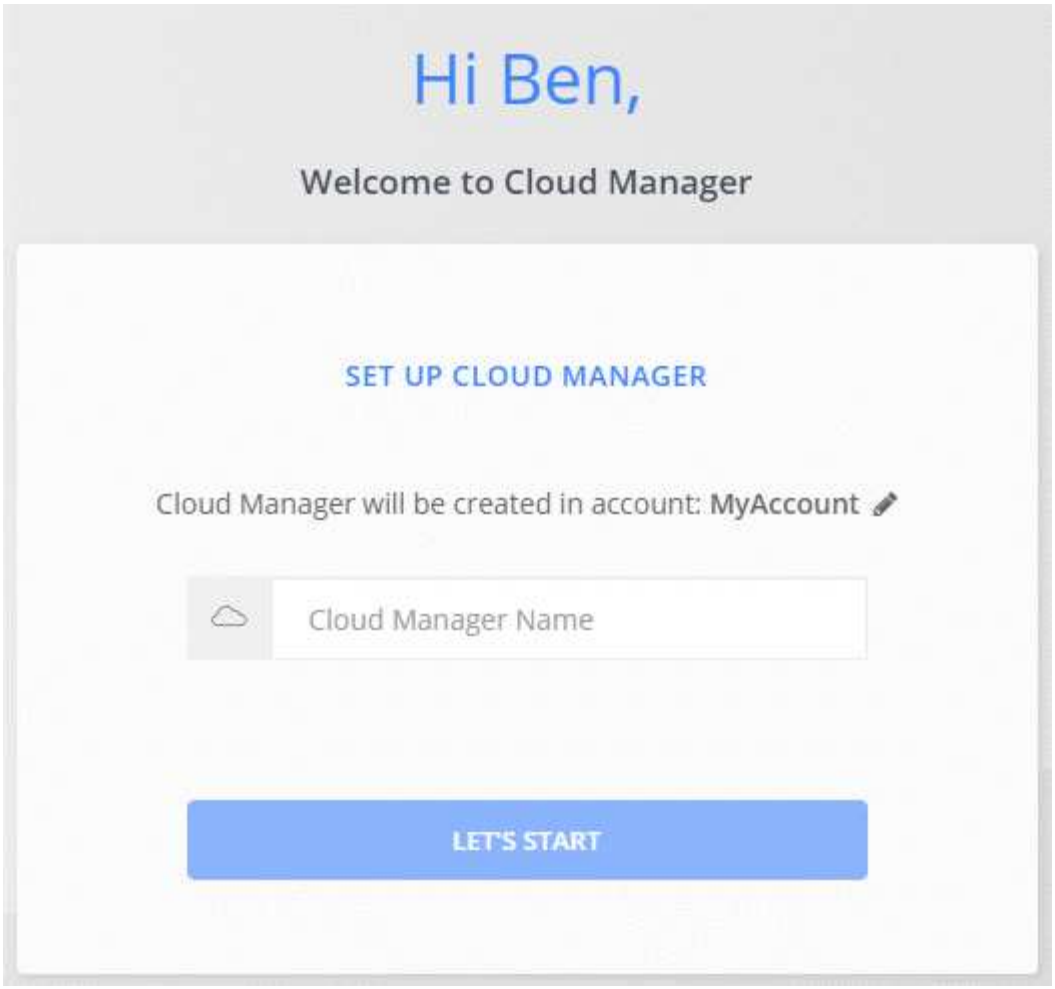
Configure una cuenta de Cloud Central

Configuración de cuentas: Usuarios, espacios de trabajo, conectores y suscripciones

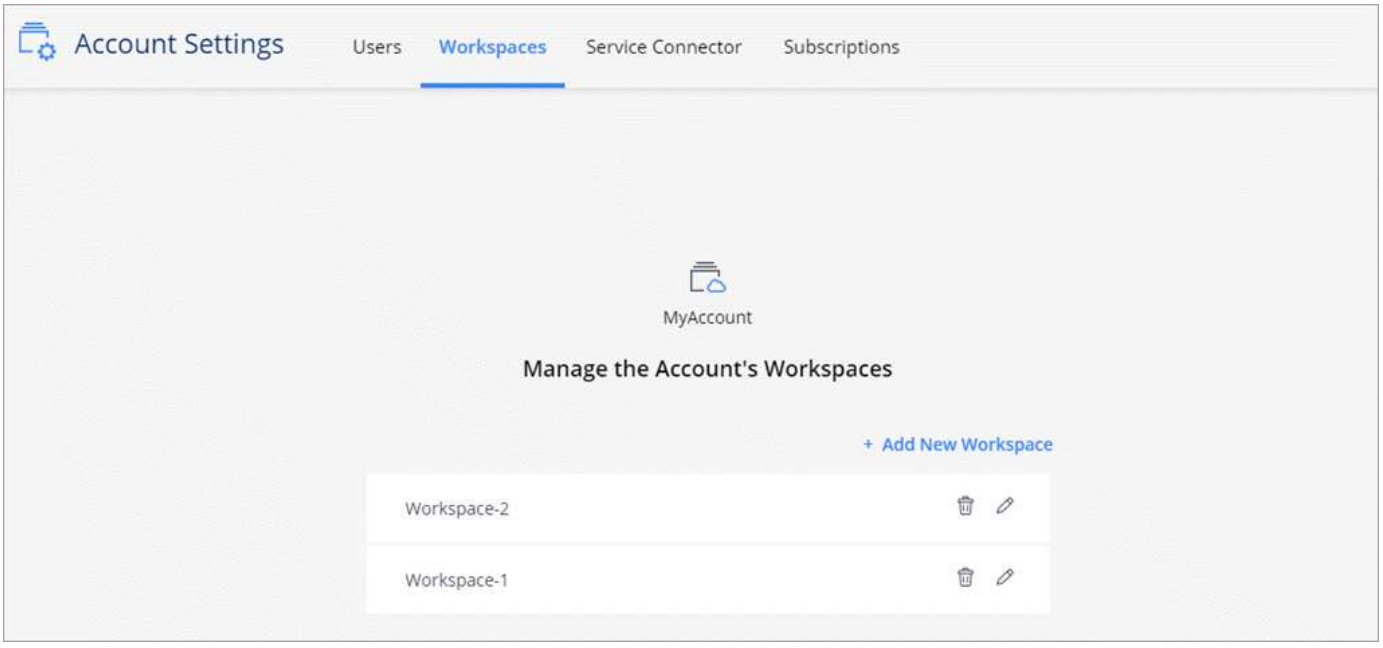
Una cuenta *Cloud Central* proporciona multi-tenancy y le permite organizar usuarios y recursos en espacios de trabajo aislados desde Cloud Manager.

Por ejemplo, varios usuarios pueden implementar y administrar sistemas Cloud Volumes ONTAP en entornos aislados denominados *espacios de trabajo*. Estos espacios de trabajo son invisibles para otros usuarios, a menos que se compartan.

Cuando acceda por primera vez a Cloud Manager, se le pedirá que seleccione o cree una cuenta de Cloud Central:



A continuación, los administradores de cuentas pueden modificar la configuración de esta cuenta mediante la administración de usuarios, áreas de trabajo, conectores y suscripciones:



Para obtener instrucciones paso a paso, consulte "Configurar la cuenta de Cloud Central".

Configuración de la cuenta

El widget Configuración de cuenta de Cloud Manager permite a los administradores de cuentas administrar una cuenta de Cloud Central. Si acaba de crear su cuenta, entonces comenzará desde cero. Pero si ya ha configurado una cuenta, verá *All* los usuarios, espacios de trabajo, conectores y suscripciones asociados a la cuenta.

Usuarios

Los usuarios que se muestran en la Configuración de la cuenta son usuarios de NetApp Cloud Central que está asociado a la cuenta de Cloud Central. La asociación de un usuario con una cuenta y uno o varios espacios de trabajo de esa cuenta permite a esos usuarios crear y administrar entornos de trabajo en Cloud Manager.

Al asociar un usuario, debe asignarles un rol:

- *Account Admin*: Puede realizar cualquier acción en Cloud Manager.
- *Workspace Admin*: Puede crear y administrar recursos en el área de trabajo asignada.
- *Cloud Compliance Viewer*: Sólo puede ver la información de cumplimiento y generar informes para los sistemas a los que tienen permiso para acceder.

Espacios de trabajo

En Cloud Manager, un espacio de trabajo aísla cualquier número de *entornos de trabajo* de otros entornos de trabajo. Los administradores de área de trabajo no pueden acceder a los entornos de trabajo de un área de trabajo a menos que el administrador de cuentas asocie el administrador a ese espacio de trabajo.

Un entorno de trabajo representa un sistema de almacenamiento:

- Un sistema Cloud Volumes ONTAP de un único nodo o un par de alta disponibilidad
- Un clúster ONTAP en las instalaciones de la red
- Un clúster de ONTAP en una configuración de almacenamiento privado de NetApp

Conectores

Un conector permite a Cloud Manager gestionar recursos y procesos dentro de su entorno de cloud público. El conector se ejecuta en una instancia de máquina virtual que se implementa en su proveedor de cloud o en un host en las instalaciones que configuró.

Puede utilizar un conector con más de un servicio de datos en cloud de NetApp. Por ejemplo, si ya tiene un conector para Cloud Manager, puede seleccionarlo cuando configura el servicio Cloud Tiering.

Suscripciones

El widget Account Settings muestra las suscripciones de NetApp asociadas con la cuenta seleccionada.

Al suscribirse a Cloud Manager desde el mercado de un proveedor de cloud, se le redirigirá a Cloud Central, donde necesita guardar su suscripción y asociarla a cuentas específicas.

Una vez que se haya suscrito, todas las suscripciones estarán disponibles en el widget Configuración de la cuenta. Solo verá las suscripciones asociadas a la cuenta que está viendo actualmente.

Puede cambiar el nombre de una suscripción y desasociar la suscripción de una o más cuentas.

Por ejemplo, digamos que tiene dos cuentas y cada una se factura mediante suscripciones independientes. Puede desasociar una suscripción de una de las cuentas para que los usuarios de esa cuenta no elijan accidentalmente la suscripción incorrecta al crear un entorno de trabajo de Cloud Volume ONTAP.

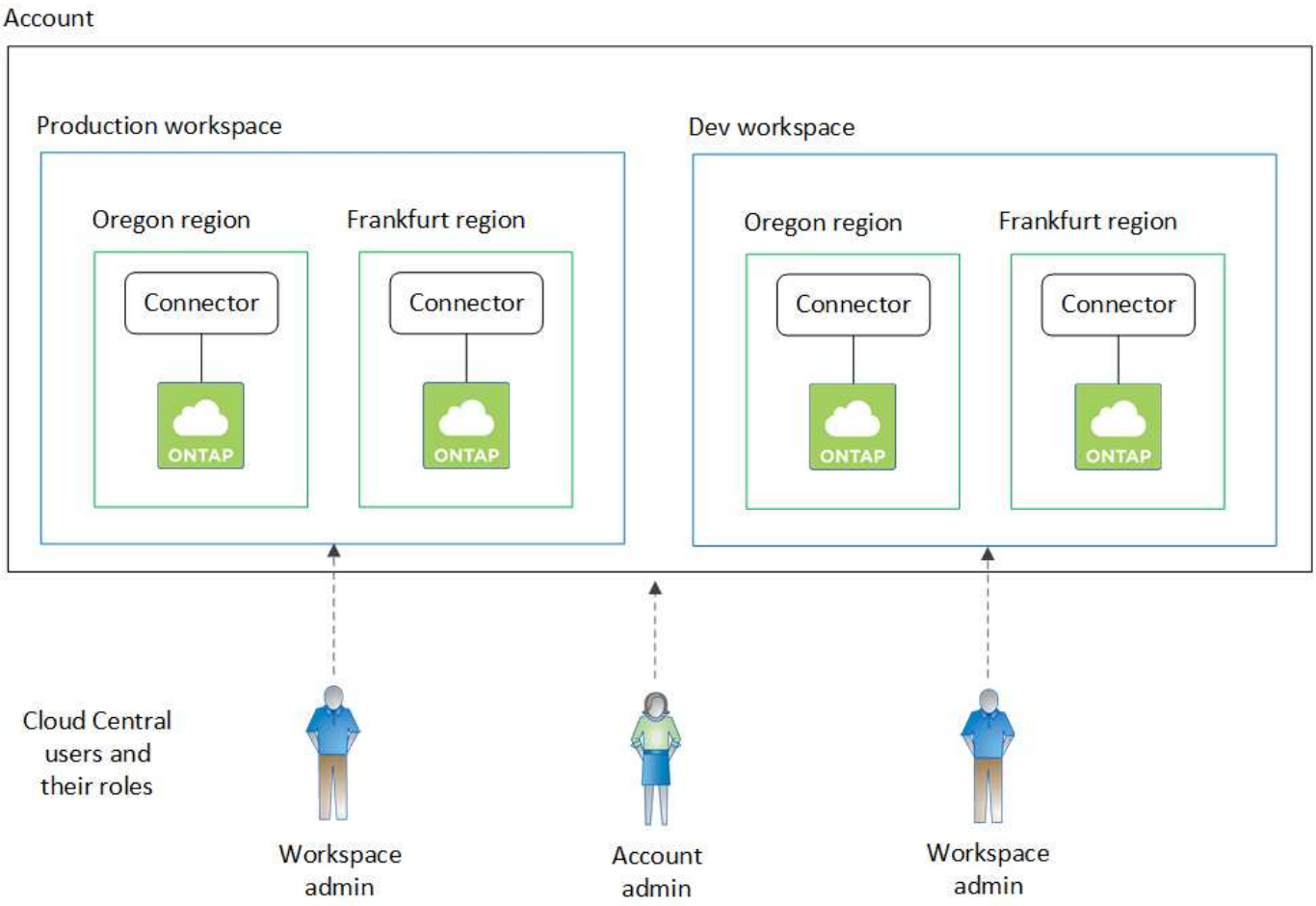
Ejemplos

Los siguientes ejemplos muestran cómo se pueden configurar las cuentas.

> En las dos imágenes de ejemplo siguientes, el conector y los sistemas Cloud Volumes ONTAP no residen en la cuenta de Cloud Central de NetApp, que se ejecutan en un proveedor de cloud. Ésta es una representación conceptual de la relación entre cada componente.

Ejemplo 1

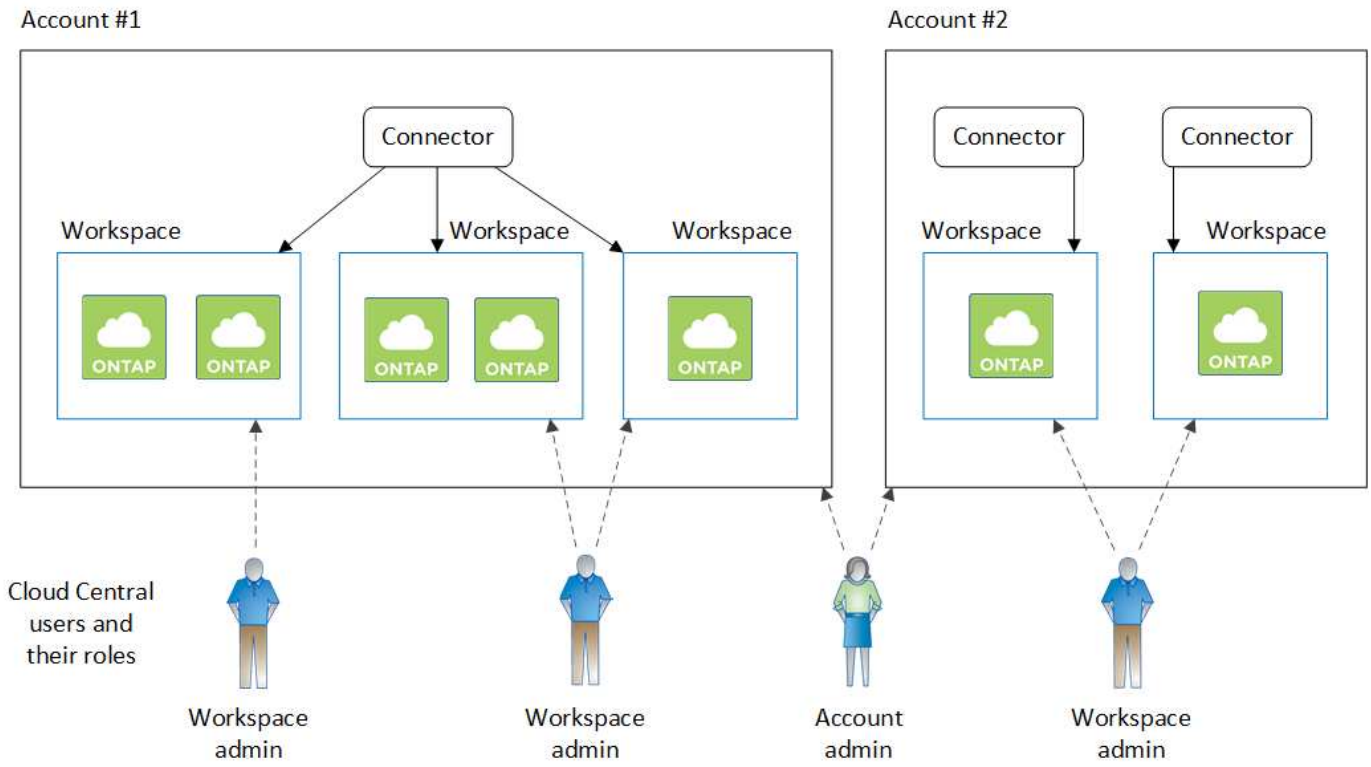
En el ejemplo siguiente se muestra una cuenta que utiliza dos espacios de trabajo para crear entornos aislados. El primer espacio de trabajo es para un entorno de producción y el segundo para un entorno de desarrollo.



Ejemplo 2

Aquí tenemos otro ejemplo que muestra el máximo nivel de multi-tenancy utilizando dos cuentas de Cloud Central separadas. Por ejemplo, un proveedor de servicios puede usar Cloud Manager en una cuenta para proporcionar servicios a sus clientes, mientras que otro utiliza para proporcionar recuperación ante desastres para una de sus unidades de negocio.

Tenga en cuenta que la cuenta 2 incluye dos conectores independientes. Esto puede suceder si tiene sistemas en regiones independientes o en proveedores de cloud independientes.



Configuración de espacios de trabajo y usuarios en la cuenta de Cloud Central

Cuando inicie sesión en Cloud Manager por primera vez, se le solicitará que cree una cuenta *Cloud Central de NetApp*. Esta cuenta proporciona multi-tenancy y le permite organizar usuarios y recursos en espacios de trabajo aislados.

"Obtenga más información sobre cómo funcionan las cuentas de Cloud Central".

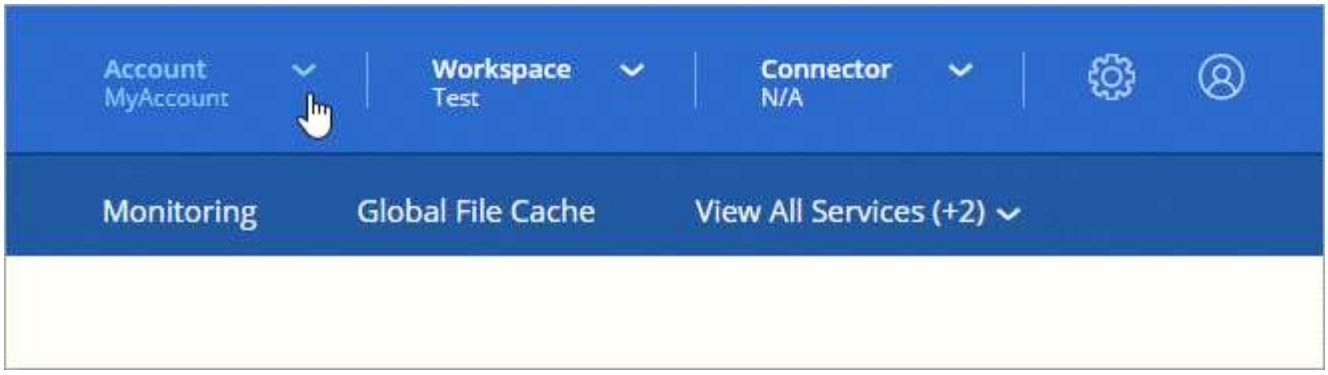
Configure su cuenta de Cloud Central para que los usuarios puedan acceder a Cloud Manager y a los entornos de trabajo de un espacio de trabajo. Solo tiene que añadir un único usuario o añadir varios usuarios y espacios de trabajo.

Agregar espacios de trabajo

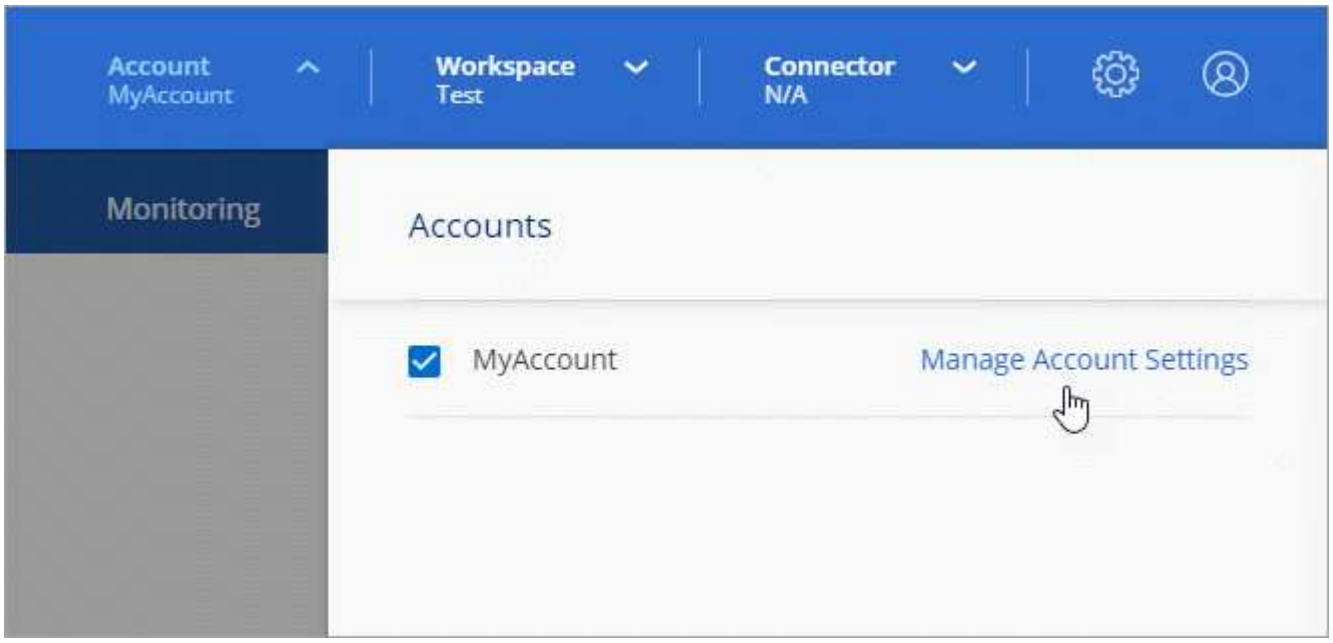
En Cloud Manager, los espacios de trabajo permiten aislar un conjunto de entornos de trabajo de otros entornos de trabajo y de otros usuarios. Por ejemplo, puede crear dos espacios de trabajo y asociar usuarios independientes a cada espacio de trabajo.

Pasos

1. En la parte superior de Cloud Manager, haga clic en el menú desplegable **cuenta**.



2. Haga clic en **Administrar cuenta** junto a la cuenta seleccionada actualmente.



3. Haga clic en **espacios de trabajo**.
4. Haga clic en **Agregar nuevo espacio de trabajo**.
5. Introduzca un nombre para el área de trabajo y haga clic en **Agregar**.

Después de terminar

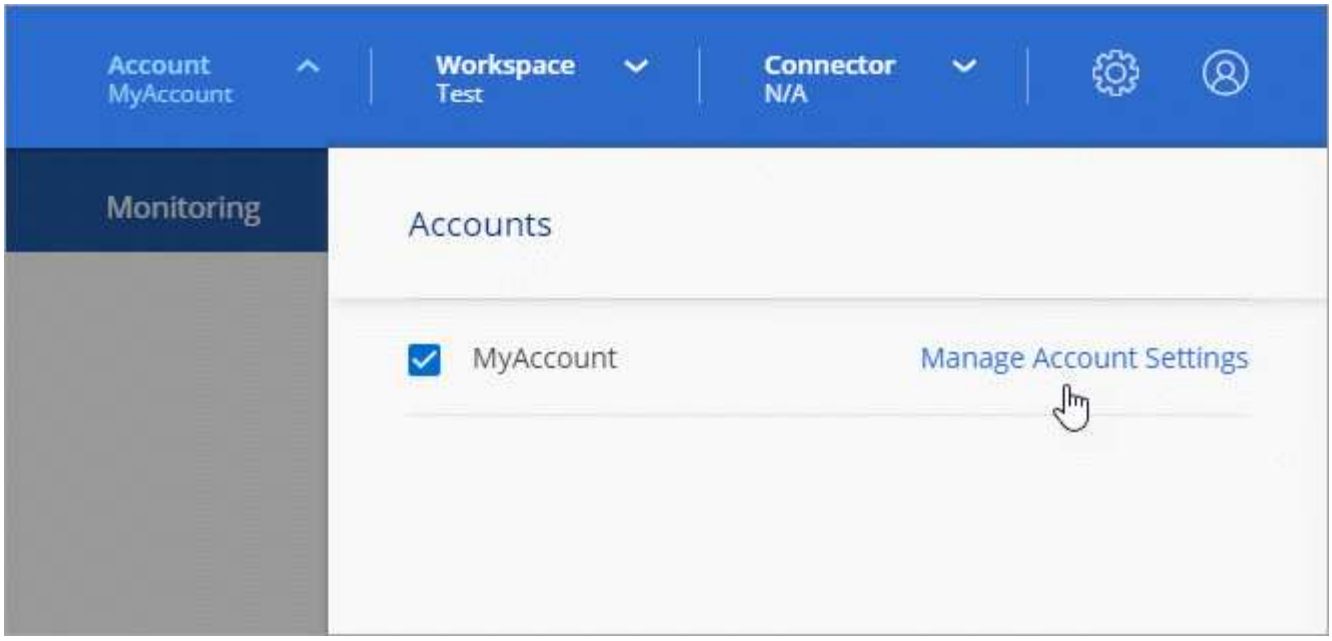
Si un administrador de área de trabajo necesita acceso a este área de trabajo, deberá asociarlo al usuario. También deberá asociar conectores al espacio de trabajo para que los administradores del área de trabajo puedan utilizar dichos conectores.

Adición de usuarios

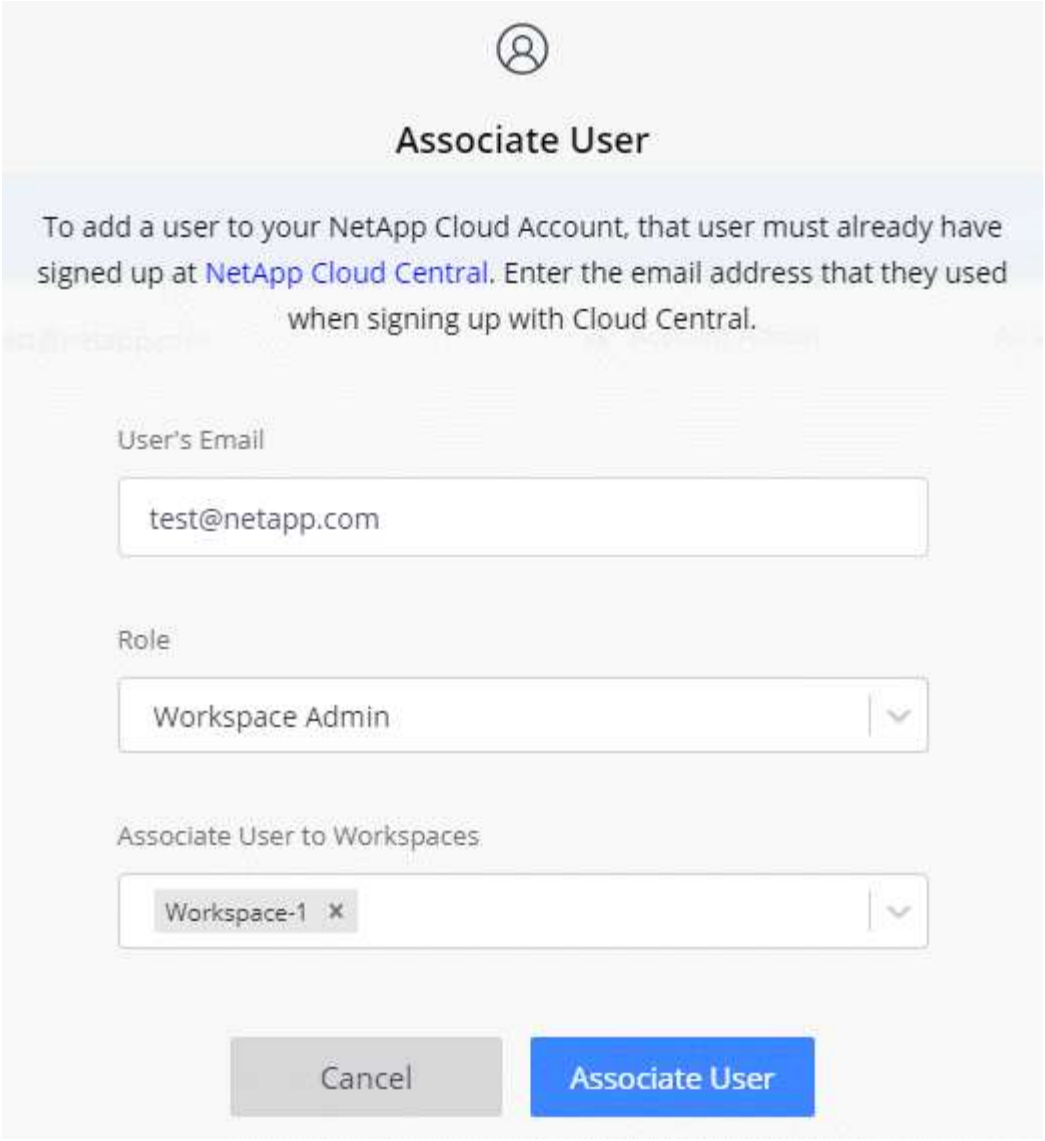
Asocie los usuarios de Cloud Central a la cuenta de Cloud Central para que esos usuarios puedan crear y gestionar entornos de trabajo en Cloud Manager.

Pasos

1. Si el usuario aún no lo ha hecho, pida al usuario que vaya a. "Cloud Central de NetApp" y regístrese.
2. En la parte superior de Cloud Manager, haga clic en el menú desplegable **cuenta** y haga clic en **gestionar cuenta**.



3. En la ficha usuarios, haga clic en **Usuario asociado**.
4. Introduzca la dirección de correo electrónico del usuario y seleccione un rol para el usuario:
   - **Administrador de cuentas**: Puede realizar cualquier acción en Cloud Manager.
   - **Administración de área de trabajo**: Puede crear y administrar recursos en áreas de trabajo asignadas.
   - **Visor de cumplimiento**: Sólo puede ver información de cumplimiento y generar informes para áreas de trabajo a las que tienen permiso para acceder.
5. Si ha seleccionado Administrador de área de trabajo o Visor de cumplimiento, seleccione uno o varios espacios de trabajo para asociarlos con ese usuario.



6. Haga clic en **Usuario asociado**.

Resultado

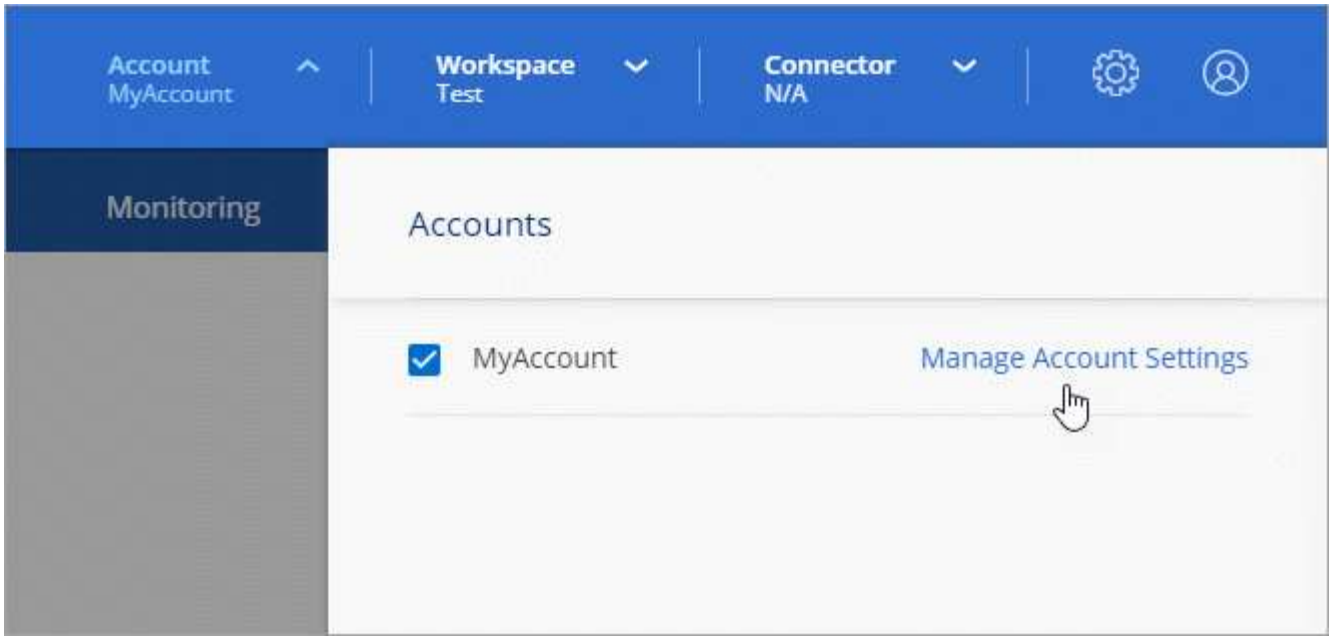
El usuario debe recibir un correo electrónico de Cloud Central de NetApp titulado "Account Association". El correo electrónico incluye la información necesaria para acceder a Cloud Manager.

Asociación de administradores de área de trabajo con áreas de trabajo

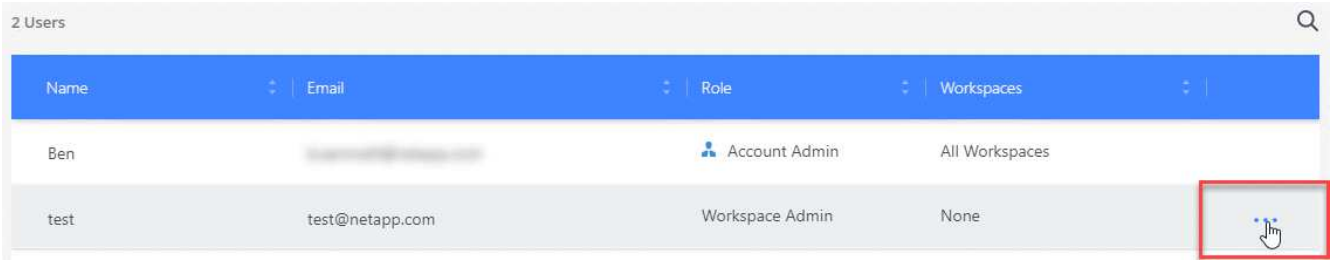
Puede asociar los administradores de área de trabajo a espacios de trabajo adicionales en cualquier momento. La asociación del usuario les permite crear y ver los entornos de trabajo en ese espacio de trabajo.

Pasos

1. En la parte superior de Cloud Manager, haga clic en el menú desplegable **cuenta** y haga clic en **gestionar cuenta**.



2. En la ficha usuarios , haga clic en el menú acción de la fila correspondiente al usuario.



3. Haga clic en **Administrar espacios de trabajo**.
4. Seleccione uno o más espacios de trabajo y haga clic en **aplicar**.

Resultado

Ahora el usuario puede acceder a esos espacios de trabajo desde Cloud Manager, siempre que el conector también esté asociado a los espacios de trabajo.

Asociación de conectores con áreas de trabajo

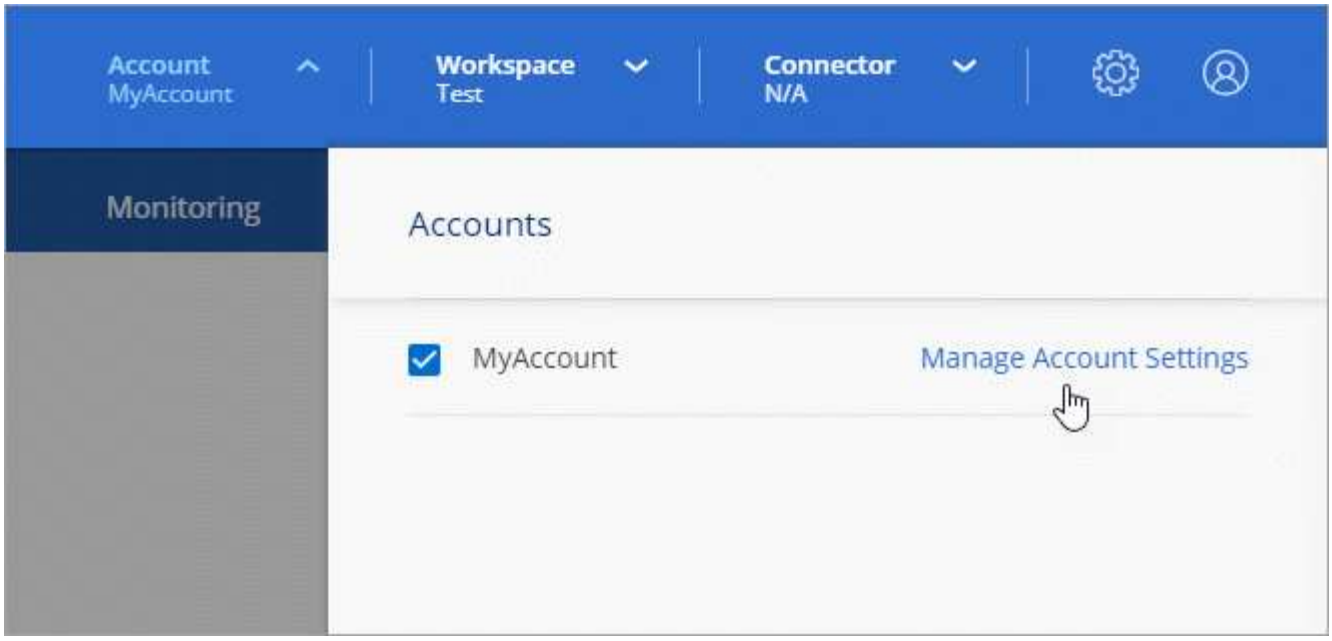
Debe asociar un conector a áreas de trabajo para que los administradores del área de trabajo puedan utilizar estos conectores para crear sistemas Cloud Volumes ONTAP.

Si sólo tiene Administradores de cuentas, no es necesario asociar el conector a áreas de trabajo. Los administradores de cuentas tienen la posibilidad de acceder a todos los espacios de trabajo de Cloud Manager de forma predeterminada.

"Obtenga más información sobre usuarios, áreas de trabajo y conectores".

Pasos

1. En la parte superior de Cloud Manager, haga clic en el menú desplegable **cuenta** y haga clic en **gestionar cuenta**.



2. Haga clic en **conector**.
3. Haga clic en **Administrar áreas de trabajo** para el conector que desea asociar.
4. Seleccione uno o más espacios de trabajo y haga clic en **aplicar**.

Resultado

Los administradores de área de trabajo ahora pueden usar estos conectores para crear sistemas Cloud Volumes ONTAP.

El futuro

Ahora que ha configurado su cuenta, puede administrarla en cualquier momento eliminando usuarios, gestionando áreas de trabajo, conectores y suscripciones. "Leer más".

Configure un conector

Más información sobre conectores

En la mayoría de los casos, un administrador de cuentas tendrá que poner en marcha un *Connector* en su red local o en la nube. El conector permite a Cloud Manager gestionar recursos y procesos dentro de su entorno de cloud público.

Cuando se necesita un conector

Se requiere un conector para utilizar cualquiera de las siguientes funciones en Cloud Manager:

- Cloud Volumes ONTAP
- Clústeres de ONTAP en las instalaciones
- Cumplimiento de normativas en el cloud
- Kubernetes
- Backup a cloud

- Supervisión
- Organización en niveles en las instalaciones
- Caché de archivos global
- Detección de bloques de Amazon S3

Se requiere un conector ***no*** para Azure NetApp Files, Cloud Volumes Service o Cloud Sync.

Mientras que un conector no es necesario para configurar y administrar Azure NetApp Files, es necesario un conector si desea utilizar Cloud Compliance para analizar datos de Azure NetApp Files.

Ubicaciones admitidas

Se admite un conector en las siguientes ubicaciones:

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- En sus instalaciones

Si desea crear un sistema Cloud Volumes ONTAP en Google Cloud, también debe tener un conector en Google Cloud. No puede utilizar un conector que se ejecute en otra ubicación.

Los conectores deben permanecer en funcionamiento

Un conector debe permanecer en funcionamiento en todo momento. Es importante para la salud y el funcionamiento continuos de los servicios que usted habilita.

Por ejemplo, un conector es un componente clave en la salud y el funcionamiento de los sistemas de Cloud Volumes ONTAP PAYGO. Si el conector está apagado, los sistemas de Cloud Volumes ONTAP PAYGO se apagarán tras perder la comunicación con un conector durante más de 14 días.

Cómo crear un conector

Un administrador de cuentas debe crear un conector antes de que un administrador de área de trabajo pueda crear un entorno de trabajo Cloud Volumes ONTAP y utilizar cualquiera de las demás funciones enumeradas anteriormente.

Un administrador de cuentas puede crear un conector de varias maneras:

- Directamente desde Cloud Manager (recomendado)
  - "Cree en AWS"
  - "Cree en Azure"
  - "Crear en GCP"
- "Desde el AWS Marketplace"
- "Desde Azure Marketplace"
- "Descargando e instalando el software en un Linux existente host"

Al crear su primer entorno de trabajo de Cloud Volumes ONTAP, Cloud Manager le solicitará que cree un conector si aún no lo tiene.

Permisos

Se necesitan permisos específicos para crear el conector y se necesita otro conjunto de permisos para la propia instancia del conector.

Permisos para crear un conector

El usuario que crea un conector desde Cloud Manager necesita permisos específicos para implementar la instancia en el proveedor de cloud que usted elija. Cloud Manager le recordará los requisitos de permisos al crear un conector.

"Vea políticas para cada proveedor de cloud".

Permisos para la instancia de conector

El conector necesita permisos específicos de proveedor de cloud para realizar operaciones en su nombre. Por ejemplo, para poner en marcha y gestionar Cloud Volumes ONTAP.

Al crear un conector directamente desde Cloud Manager, Cloud Manager crea el conector con los permisos que necesita. No hay nada que usted necesita hacer.

Si crea el conector usted mismo desde AWS Marketplace, Azure Marketplace o mediante la instalación manual del software, tendrá que asegurarse de que cuenta con los permisos adecuados.

"Vea políticas para cada proveedor de cloud".

Cuándo usar varios conectores

En algunos casos, es posible que sólo necesite un conector, pero es posible que necesite dos o más conectores.

A continuación, se muestran algunos ejemplos:

- Utiliza un entorno multicloud (AWS y Azure), por lo que tiene un conector en AWS y otro en Azure. Cada una de ellas gestiona los sistemas Cloud Volumes ONTAP que se ejecutan en estos entornos.
- Un proveedor de servicios puede utilizar una cuenta de Cloud Central para proporcionar servicios a sus clientes mientras utiliza otra cuenta para proporcionar recuperación ante desastres para una de sus unidades de negocio. Cada cuenta tendría conectores independientes.

Cuándo cambiar entre conectores

Al crear el primer conector, Cloud Manager utiliza automáticamente ese conector para cada entorno de trabajo adicional que cree. Una vez creado un conector adicional, deberá cambiar entre ellos para ver los entornos de trabajo específicos de cada conector.

"Aprenda a cambiar entre conectores".

La interfaz de usuario local

Mientras debe realizar casi todas las tareas de la "Interfaz de usuario de SaaS", una interfaz de usuario local todavía está disponible en el conector. Esta interfaz es necesaria para algunas tareas que se deben realizar desde el propio conector:

- "Establecimiento de un servidor proxy"
- Instalación de un parche (Normalmente, trabajará con el personal de NetApp para instalar un parche).
- Descargando mensajes de AutoSupport (Normalmente dirigido por el personal de NetApp cuando tiene problemas)

"Aprenda a acceder a la interfaz de usuario local".

Actualizaciones de conectores

El conector actualiza automáticamente su software a la última versión, siempre que lo haya hecho "acceso a internet de salida" para obtener la actualización de software.

Requisitos de red para el conector

Configure su red de modo que Connector pueda gestionar recursos y procesos en su entorno de cloud público. El paso más importante es garantizar el acceso saliente a Internet a varios puntos finales.

Si la red utiliza un servidor proxy para toda la comunicación a Internet, puede especificar el servidor proxy en la página Configuración. Consulte "Configuración del conector para utilizar un servidor proxy".

Conexión a redes de destino

Un conector requiere una conexión de red al tipo de entorno de trabajo que está creando y a los servicios que está planeando habilitar.

Por ejemplo, si instala un conector en la red corporativa, debe configurar una conexión VPN al VPC o a vnet en el que inicie Cloud Volumes ONTAP.

Acceso a Internet de salida

El conector requiere acceso saliente a Internet para gestionar recursos y procesos dentro de su entorno de nube pública. El acceso saliente a Internet también es necesario si desea instalar manualmente el conector en un host Linux o acceder a la interfaz de usuario local que se ejecuta en el conector.

En las siguientes secciones se identifican los puntos finales específicos.

Extremos para gestionar recursos en AWS

Un conector se pone en contacto con los siguientes extremos cuando se gestionan recursos en AWS:

Puntos finales	Específico
Servicios de AWS (amazonaws.com): • Formación CloudFormation • Cloud computing elástico (EC2) • Servicio de gestión de claves (KMS) • Servicio de token de seguridad (STS) • Simple Storage Service (S3) El extremo exacto depende de la región en la que se implemente Cloud Volumes ONTAP. "Consulte la documentación de AWS para obtener más detalles."	Permite al conector poner en marcha y gestionar Cloud Volumes ONTAP en AWS.
https://api.services.cloud.netapp.com:443	Solicitudes de API a Cloud Central de NetApp.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Proporciona acceso a imágenes, manifiestos y plantillas de software.
https://repo.cloud.support.netapp.com	Se utiliza para descargar las dependencias de Cloud Manager.
http://repo.mysql.com/	Se utiliza para descargar MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Permite al conector acceder y descargar manifiestos, plantillas e imágenes de actualización de Cloud Volumes ONTAP.
https://cloudmanagerinfraprod.azurecr.io	Acceso a imágenes de software de componentes de contenedor para una infraestructura que ejecuta Docker y proporciona una solución para las integraciones de servicios con Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Permite a NetApp transmitir datos desde registros de auditoría.
https://cloudmanager.cloud.netapp.com	Comunicación con el servicio Cloud Manager, que incluye cuentas de Cloud Central.
https://netapp-cloud-account.auth0.com	Comunicación con Cloud Central de NetApp para la autenticación de usuario centralizada.
https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist	Se utiliza para añadir su ID de cuenta de AWS a la lista de usuarios permitidos para Backup en S3.
https://support.netapp.com/aods/asupmessage https://support.netapp.com/asupprod/post/1.0/postAsup	Comunicación con AutoSupport de NetApp.

Puntos finales	Específico
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Comunicación con NetApp para la licencia del sistema y el registro de soporte.
https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com	Permite a NetApp recopilar la información necesaria para resolver problemas de soporte.
https://ipa-signer.cloudmanager.netapp.com	Permite que Cloud Manager genere licencias (por ejemplo, una licencia de FlexCache para Cloud Volumes ONTAP).
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Necesario para conectar los sistemas Cloud Volumes ONTAP con un clúster de Kubernetes. Los extremos permiten la instalación de Trident de NetApp.
Diversas ubicaciones de terceros, por ejemplo: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.com Las ubicaciones de terceros están sujetas a cambios.	Durante las actualizaciones, Cloud Manager descarga los paquetes más recientes para dependencias de terceros.

Extremos para gestionar recursos en Azure

Un conector se pone en contacto con los siguientes extremos al gestionar recursos en Azure:

Puntos finales	Específico
https://management.azure.com https://login.microsoftonline.com	Permite que Cloud Manager ponga en marcha y gestione Cloud Volumes ONTAP en la mayoría de las regiones de Azure.
https://management.microsoftazure.de https://login.microsoftonline.de	Permite que Cloud Manager ponga en marcha y gestione Cloud Volumes ONTAP en las regiones de Azure Alemania.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Permite a Cloud Manager implementar y gestionar Cloud Volumes ONTAP en las regiones de Azure US Gov.
https://api.services.cloud.netapp.com:443	Solicitudes de API a Cloud Central de NetApp.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Proporciona acceso a imágenes, manifiestos y plantillas de software.

Puntos finales	Específico
https://repo.cloud.support.netapp.com	Se utiliza para descargar las dependencias de Cloud Manager.
http://repo.mysql.com/	Se utiliza para descargar MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Permite al conector acceder y descargar manifiestos, plantillas e imágenes de actualización de Cloud Volumes ONTAP.
https://cloudmanagerinfraprod.azurecr.io	Acceso a imágenes de software de componentes de contenedor para una infraestructura que ejecuta Docker y proporciona una solución para las integraciones de servicios con Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Permite a NetApp transmitir datos desde registros de auditoría.
https://cloudmanager.cloud.netapp.com	Comunicación con el servicio Cloud Manager, que incluye cuentas de Cloud Central.
https://netapp-cloud-account.auth0.com	Comunicación con Cloud Central de NetApp para la autenticación de usuario centralizada.
https://mysupport.netapp.com	Comunicación con AutoSupport de NetApp.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Comunicación con NetApp para la licencia del sistema y el registro de soporte.
https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com	Permite a NetApp recopilar la información necesaria para resolver problemas de soporte.
https://ipa-signer.cloudmanager.netapp.com	Permite que Cloud Manager genere licencias (por ejemplo, una licencia de FlexCache para Cloud Volumes ONTAP).
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Necesario para conectar los sistemas Cloud Volumes ONTAP con un clúster de Kubernetes. Los extremos permiten la instalación de Trident de NetApp.
*.blob.core.windows.net	Necesario para pares de alta disponibilidad cuando se utiliza un proxy.

Puntos finales	Específico
Diversas ubicaciones de terceros, por ejemplo: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.com Las ubicaciones de terceros están sujetas a cambios.	Durante las actualizaciones, Cloud Manager descarga los paquetes más recientes para dependencias de terceros.

Extremos para gestionar recursos en GCP

Un conector se pone en contacto con los siguientes extremos al gestionar recursos en GCP:

Puntos finales	Específico
https://www.googleapis.com	Permite que el conector se ponga en contacto con las API de Google para poner en marcha y gestionar Cloud Volumes ONTAP en GCP.
https://api.services.cloud.netapp.com:443	Solicitudes de API a Cloud Central de NetApp.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Proporciona acceso a imágenes, manifiestos y plantillas de software.
https://repo.cloud.support.netapp.com	Se utiliza para descargar las dependencias de Cloud Manager.
http://repo.mysql.com/	Se utiliza para descargar MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Permite al conector acceder y descargar manifiestos, plantillas e imágenes de actualización de Cloud Volumes ONTAP.
https://cloudmanagerinfraprod.azurecr.io	Acceso a imágenes de software de componentes de contenedor para una infraestructura que ejecuta Docker y proporciona una solución para las integraciones de servicios con Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Permite a NetApp transmitir datos desde registros de auditoría.
https://cloudmanager.cloud.netapp.com	Comunicación con el servicio Cloud Manager, que incluye cuentas de Cloud Central.
https://netapp-cloud-account.auth0.com	Comunicación con Cloud Central de NetApp para la autenticación de usuario centralizada.
https://mysupport.netapp.com	Comunicación con AutoSupport de NetApp.

Puntos finales	Específico
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Comunicación con NetApp para la licencia del sistema y el registro de soporte.
https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com	Permite a NetApp recopilar la información necesaria para resolver problemas de soporte.
https://ipa-signer.cloudmanager.netapp.com	Permite que Cloud Manager genere licencias (por ejemplo, una licencia de FlexCache para Cloud Volumes ONTAP).
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Necesario para conectar los sistemas Cloud Volumes ONTAP con un clúster de Kubernetes. Los extremos permiten la instalación de Trident de NetApp.
Diversas ubicaciones de terceros, por ejemplo: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.com Las ubicaciones de terceros están sujetas a cambios.	Durante las actualizaciones, Cloud Manager descarga los paquetes más recientes para dependencias de terceros.

Extremos para instalar el conector en un host Linux

Tiene la opción de instalar manualmente el software Connector en su propio host Linux. Si lo hace, el instalador del conector debe acceder a las siguientes direcciones URL durante el proceso de instalación:

- http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm
- https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
- https://s3.amazonaws.com/aws-cli/awscli-bundle.zip

Es posible que el host intente actualizar paquetes de sistema operativo durante la instalación. El host puede ponerse en contacto con diferentes sitios de duplicación para estos paquetes de SO.

Puntos finales a los que se accede desde el explorador Web cuando se utiliza el local UI

Aunque debe realizar casi todas las tareas desde la interfaz de usuario de SaaS, todavía hay disponible una interfaz de usuario local en el conector. La máquina que ejecuta el explorador Web debe tener conexiones con los siguientes puntos finales:

Puntos finales	Específico
El host del conector	Debe introducir la dirección IP del host desde un explorador web para cargar la consola de Cloud Manager. Según su conectividad con el proveedor de cloud, puede usar la IP privada o una IP pública asignada al host: • Una IP privada funciona si dispone de una VPN y. acceso directo a la red virtual • Una IP pública funciona en cualquier situación de red En cualquier caso, debe proteger el acceso a la red garantizando que las reglas de grupo de seguridad permiten el acceso sólo desde IP o subredes autorizadas.
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	El explorador web se conecta con estos extremos para conseguir una autenticación de usuario centralizada mediante NetApp Cloud Central.
https://widget.intercom.io	Si busca un chat integrado en los productos que le permita hablar con expertos en cloud de NetApp.

Puertos y grupos de seguridad

No hay tráfico entrante en el conector, a menos que lo inicie. HTTP y HTTPS proporcionan acceso al "Interfaz de usuario local", que utilizará en raras circunstancias. SSH solo es necesario si necesita conectarse al host para la solución de problemas.

Reglas para el conector en AWS

El grupo de seguridad del conector requiere reglas entrantes y salientes.

Reglas de entrada

El origen de las reglas entrantes en el grupo de seguridad predefinido es 0.0.0.0/0.

Protocolo	Puerto	Específico
SSH	22	Proporciona acceso SSH al host de Connector
HTTP	80	Proporciona acceso HTTP desde navegadores web de cliente al local Interfaz de usuario y conexiones desde Cloud Compliance
HTTPS	443	Proporciona acceso HTTPS desde exploradores web de cliente al local interfaz de usuario
TCP	3128	Proporciona a la instancia de Cloud Compliance acceso a Internet si la red AWS no utiliza NAT o proxy

Reglas de salida

El grupo de seguridad predefinido para el conector abre todo el tráfico saliente. Si eso es aceptable, siga las reglas básicas de la salida. Si necesita más reglas rígidas, utilice las reglas avanzadas de salida.

Reglas de salida básicas

El grupo de seguridad predefinido para el conector incluye las siguientes reglas de salida.

Protocolo	Puerto	Específico
Todos los TCP	Todo	Todo el tráfico saliente
Todas las UDP	Todo	Todo el tráfico saliente

Reglas salientes avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede utilizar la siguiente información para abrir sólo los puertos necesarios para la comunicación saliente por parte del conector.

La dirección IP de origen es el host del conector.

Servicio	Protocolo	Puerto	Destino	Específico
Active Directory	TCP	88	Bosque de Active Directory	Autenticación Kerberos V.
	TCP	139	Bosque de Active Directory	Sesión de servicio NetBIOS
	TCP	389	Bosque de Active Directory	LDAP
	TCP	445	Bosque de Active Directory	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
	TCP	464	Bosque de Active Directory	Kerberos V cambiar y establecer contraseña (SET_CHANGE)
	TCP	749	Bosque de Active Directory	Contraseña de modificación y definición de Kerberos V de Active Directory (RPCSEC_GSS)
	UDP	137	Bosque de Active Directory	Servicio de nombres NetBIOS
	UDP	138	Bosque de Active Directory	Servicio de datagramas NetBIOS
	UDP	464	Bosque de Active Directory	Administración de claves Kerberos

Servicio	Protocolo	Puerto	Destino	Específico
Llamadas API y AutoSupport	HTTPS	443	LIF de gestión de clústeres de ONTAP y Internet saliente	API llama a AWS y ONTAP y envía mensajes de AutoSupport a NetApp
Llamadas API	TCP	3000	LIF de gestión de clústeres de ONTAP	Llamadas API a ONTAP
	TCP	8088	Backup en S3	Llamadas API a Backup en S3
DNS	UDP	53	DNS	Utilizado para resolver DNS por Cloud Manager
Cumplimiento de normativas en el cloud	HTTP	80	Instancia de cumplimiento de normativas cloud	Cumplimiento de normativas cloud para Cloud Volumes ONTAP

Reglas para Connector en Azure

El grupo de seguridad del conector requiere reglas entrantes y salientes.

Reglas de entrada

El origen de las reglas entrantes en el grupo de seguridad predefinido es 0.0.0.0/0.

Puerto	Protocolo	Específico
22	SSH	Proporciona acceso SSH al host de Connector
80	HTTP	Proporciona acceso HTTP desde navegadores web de cliente al local interfaz de usuario
443	HTTPS	Proporciona acceso HTTPS desde exploradores web de cliente al local interfaz de usuario

Reglas de salida

El grupo de seguridad predefinido para el conector abre todo el tráfico saliente. Si eso es aceptable, siga las reglas básicas de la salida. Si necesita más reglas rígidas, utilice las reglas avanzadas de salida.

Reglas de salida básicas

El grupo de seguridad predefinido para el conector incluye las siguientes reglas de salida.

Puerto	Protocolo	Específico
Todo	Todos los TCP	Todo el tráfico saliente

Puerto	Protocolo	Específico
Todo	Todas las UDP	Todo el tráfico saliente

Reglas salientes avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede utilizar la siguiente información para abrir sólo los puertos necesarios para la comunicación saliente por parte del conector.

La dirección IP de origen es el host del conector.

Servicio	Puerto	Protocolo	Destino	Específico
Active Directory	88	TCP	Bosque de Active Directory	Autenticación Kerberos V.
	139	TCP	Bosque de Active Directory	Sesión de servicio NetBIOS
	389	TCP	Bosque de Active Directory	LDAP
	445	TCP	Bosque de Active Directory	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
	464	TCP	Bosque de Active Directory	Kerberos V cambiar y establecer contraseña (SET_CHANGE)
	749	TCP	Bosque de Active Directory	Contraseña de modificación y definición de Kerberos V de Active Directory (RPCSEC_GSS)
	137	UDP	Bosque de Active Directory	Servicio de nombres NetBIOS
	138	UDP	Bosque de Active Directory	Servicio de datagramas NetBIOS
	464	UDP	Bosque de Active Directory	Administración de claves Kerberos
Llamadas API y AutoSupport	443	HTTPS	LIF de gestión de clústeres de ONTAP y Internet saliente	API llama a AWS y ONTAP y envía mensajes de AutoSupport a NetApp
Llamadas API	3000	TCP	LIF de gestión de clústeres de ONTAP	Llamadas API a ONTAP

Servicio	Puerto	Protocolo	Destino	Específico
DNS	53	UDP	DNS	Utilizado para resolver DNS por Cloud Manager

Reglas para el conector en GCP

Las reglas de firewall para el conector requieren reglas de entrada y salida.

Reglas de entrada

El origen de las reglas de entrada en las reglas de firewall predefinidas es 0.0.0.0/0.

Protocolo	Puerto	Específico
SSH	22	Proporciona acceso SSH al host de Connector
HTTP	80	Proporciona acceso HTTP desde navegadores web de cliente al local interfaz de usuario
HTTPS	443	Proporciona acceso HTTPS desde exploradores web de cliente al local interfaz de usuario

Reglas de salida

Las reglas de firewall predefinidas para el conector abren todo el tráfico saliente. Si eso es aceptable, siga las reglas básicas de la salida. Si necesita más reglas rígidas, utilice las reglas avanzadas de salida.

Reglas de salida básicas

Las reglas de firewall predefinidas para el conector incluyen las siguientes reglas de salida.

Protocolo	Puerto	Específico
Todos los TCP	Todo	Todo el tráfico saliente
Todas las UDP	Todo	Todo el tráfico saliente

Reglas salientes avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede utilizar la siguiente información para abrir sólo los puertos necesarios para la comunicación saliente por parte del conector.

La dirección IP de origen es el host del conector.

Servicio	Protocolo	Puerto	Destino	Específico
Active Directory	TCP	88	Bosque de Active Directory	Autenticación Kerberos V.
	TCP	139	Bosque de Active Directory	Sesión de servicio NetBIOS
	TCP	389	Bosque de Active Directory	LDAP
	TCP	445	Bosque de Active Directory	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
	TCP	464	Bosque de Active Directory	Kerberos V cambiar y establecer contraseña (SET_CHANGE)
	TCP	749	Bosque de Active Directory	Contraseña de modificación y definición de Kerberos V de Active Directory (RPCSEC_GSS)
	UDP	137	Bosque de Active Directory	Servicio de nombres NetBIOS
	UDP	138	Bosque de Active Directory	Servicio de datagramas NetBIOS
	UDP	464	Bosque de Active Directory	Administración de claves Kerberos
Llamadas API y AutoSupport	HTTPS	443	LIF de gestión de clústeres de ONTAP y Internet saliente	API llama a GCP y ONTAP, y envía mensajes de AutoSupport a NetApp
Llamadas API	TCP	3000	LIF de gestión de clústeres de ONTAP	Llamadas API a ONTAP
DNS	UDP	53	DNS	Utilizado para resolver DNS por Cloud Manager

Crear un conector en AWS desde Cloud Manager

Un administrador de cuentas debe implementar un *Connector* antes de poder utilizar la mayoría de las funciones de Cloud Manager. "Aprender cuando se necesita un conector". El conector permite a Cloud Manager gestionar recursos y procesos dentro de su entorno de cloud público.

En esta página se describe cómo crear un conector en AWS directamente desde Cloud Manager. También

tiene la opción a. "Cree el conector desde el AWS Marketplace", o. "descargue el software e instálelo en su propio host".

Estos pasos deben ser completados por un usuario que tenga la función de administrador de cuentas. Un administrador de área de trabajo no puede crear un conector.

Al crear su primer entorno de trabajo de Cloud Volumes ONTAP, Cloud Manager le solicitará que cree un conector si aún no lo tiene.

Configuración de permisos de AWS para crear un conector

Antes de poder implementar un conector desde Cloud Manager, debe asegurarse de que su cuenta de AWS tenga los permisos correctos.

Pasos

1. Descargue la política del IAM del conector desde la siguiente ubicación:

   "NetApp Cloud Manager: Políticas de AWS, Azure y GCP"

2. Desde la consola del IAM de AWS, cree su propia política copiando y pegando el texto de la política IAM del conector.
3. Adjunte la política que creó en el paso anterior al usuario IAM que creará el conector desde Cloud Manager.

Resultado

El usuario de AWS ahora tiene los permisos necesarios para crear el conector desde Cloud Manager. Deberá especificar las claves de acceso de AWS para este usuario cuando se le solicite Cloud Manager.

Creación de un conector en AWS

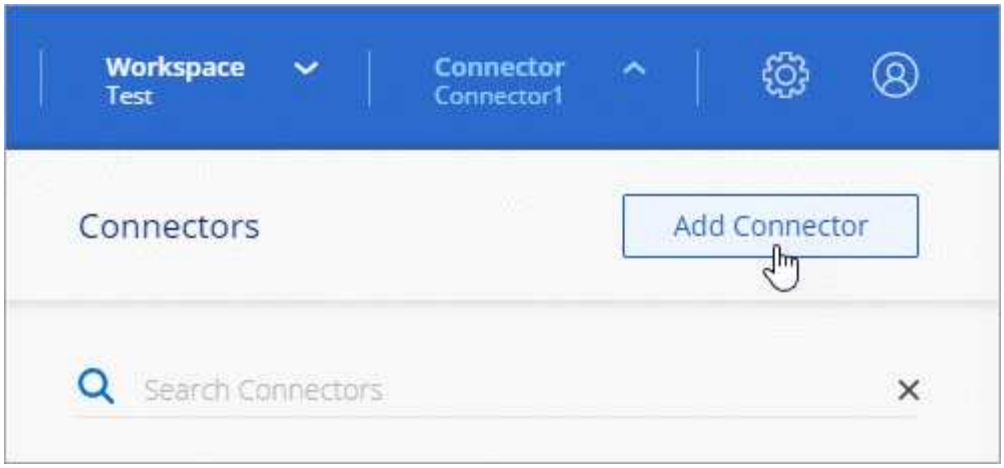
Cloud Manager permite crear un conector en AWS directamente desde su interfaz de usuario.

Lo que necesitará

- Una clave secreta y de acceso AWS para un IAM usuario que tiene la "permisos necesarios".
- Un VPC, una subred y un teclados en la región de AWS que usted elija.

Pasos

1. Si está creando su primer entorno de trabajo, haga clic en **Agregar entorno de trabajo** y siga las indicaciones. De lo contrario, haga clic en el menú desplegable **conector** y seleccione **Agregar conector**.



2. Haga clic en **Iniciar**.
3. Elija **Amazon Web Services** como su proveedor de cloud.

   Recuerde que el conector debe tener una conexión de red al tipo de entorno de trabajo que está creando y a los servicios que está planeando habilitar.

   "Obtenga más información sobre los requisitos de red del conector".

4. Revise lo que necesitará y haga clic en **continuar**.
5. Proporcione la información necesaria:
   - **credenciales de AWS**: Introduzca un nombre para la instancia y especifique la clave de acceso y la clave secreta de AWS que cumplan los requisitos de permisos.
   - **ubicación**: Especifique una región, VPC y subred de AWS para la instancia.
   - **Red**: Seleccione el par de claves que se va a utilizar con la instancia, si desea activar una dirección IP pública y, opcionalmente, especifique una configuración de proxy.
   - **Grupo de seguridad**: Elija si desea crear un nuevo grupo de seguridad o si desea seleccionar un grupo de seguridad existente que permita el acceso entrante HTTP, HTTPS y SSH.

     No hay tráfico entrante en el conector, a menos que lo inicie. HTTP y HTTPS proporcionan acceso al "Interfaz de usuario local", que utilizará en raras circunstancias. SSH solo es necesario si necesita conectarse al host para la solución de problemas.

6. Haga clic en **Crear**.

   La instancia debe estar lista en unos 7 minutos. Debe permanecer en la página hasta que el proceso se complete.

Después de terminar

Debe asociar un conector a áreas de trabajo para que los administradores del área de trabajo puedan utilizar estos conectores para crear sistemas Cloud Volumes ONTAP. Si sólo tiene Administradores de cuentas, no es necesario asociar el conector a áreas de trabajo. Los administradores de cuentas tienen la posibilidad de acceder a todos los espacios de trabajo de Cloud Manager de forma predeterminada. "Leer más".

Crear un conector en Azure desde Cloud Manager

Un administrador de cuentas debe implementar un *Connector* antes de poder utilizar la

mayoría de las funciones de Cloud Manager. "Aprender cuando se necesita un conector". El conector permite a Cloud Manager gestionar recursos y procesos dentro de su entorno de cloud público.

En esta página se describe cómo crear un conector en Azure directamente desde Cloud Manager. También tiene la opción a. "Cree el conector desde Azure Marketplace", o. "descargue el software e instálelo en su propio host".

Estos pasos deben ser completados por un usuario que tenga la función de administrador de cuentas. Un administrador de área de trabajo no puede crear un conector.

Al crear su primer entorno de trabajo de Cloud Volumes ONTAP, Cloud Manager le solicitará que cree un conector si aún no lo tiene.

Configurar permisos de Azure para crear un conector

Antes de poder implementar un conector desde Cloud Manager, debe asegurarse de que su cuenta de Azure tenga los permisos correctos.

Pasos

1. Cree un rol personalizado con la política de Azure para Connector:

   a. Descargue el "Política de Azure para Connector".

      Haga clic con el botón derecho del ratón en el enlace y haga clic en **Guardar enlace como…** para descargar el archivo.

   b. Modifique el archivo JSON añadiendo su ID de suscripción de Azure al ámbito asignable.

      ejemplo

      ```
      "AssignableScopes": [
      "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
      ],
      ```

   c. Use el archivo JSON para crear una función personalizada en Azure.

      El ejemplo siguiente muestra cómo crear una función personalizada con la CLI de Azure 2.0:

      ```
      az role definition create --role-definition
      C:\Policy_for_Setup_As_Service_Azure.json
      ```

   Ahora debería tener una función personalizada denominada *Azure SetupAsService*.

2. Asigne el rol al usuario que implementará Connector desde Cloud Manager:

   a. Abra el servicio **Suscripciones** y seleccione la suscripción del usuario.

   b. Haga clic en **Control de acceso (IAM)**.

   c. Haga clic en **Agregar** > **Agregar asignación de rol** y, a continuación, agregue los permisos:

      - Seleccione el rol **Azure SetupAsService**.

Azure SetupAsService es el nombre predeterminado que se proporciona en "Política de implementación de conectores para Azure". Si seleccionó otro nombre para el rol, seleccione ese nombre.

- Asigne acceso a un usuario, grupo o aplicación **AD de Azure**.
- Seleccione la cuenta de usuario.
- Haga clic en **Guardar**.

Resultado

El usuario de Azure ahora tiene los permisos necesarios para implementar Connector desde Cloud Manager.

Creación de un conector en Azure

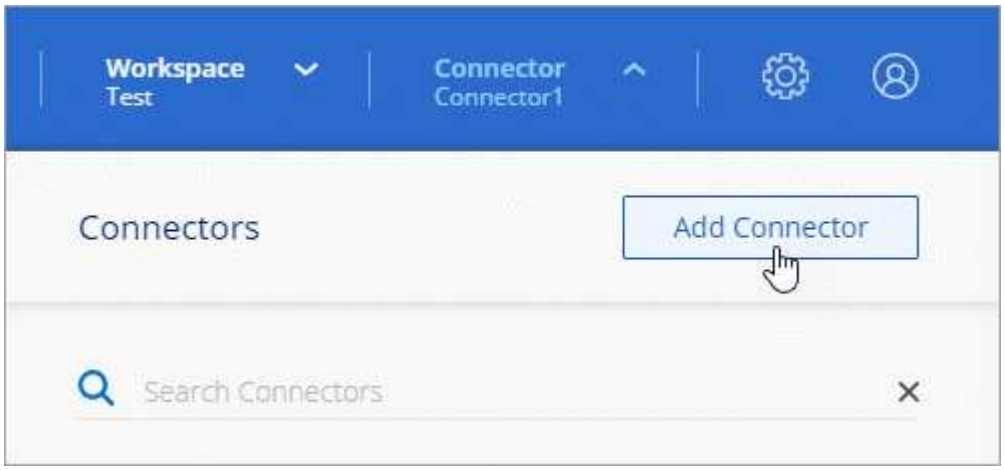
Cloud Manager permite crear un conector en Azure directamente desde su interfaz de usuario.

Lo que necesitará

- La "permisos necesarios" Para su cuenta de Azure.
- Una suscripción a Azure.
- Una red virtual y una subred en su región de Azure preferida.

Pasos

1. Si está creando su primer entorno de trabajo, haga clic en **Agregar entorno de trabajo** y siga las indicaciones. De lo contrario, haga clic en el menú desplegable **conector** y seleccione **Agregar conector**.



2. Haga clic en **Iniciar**.
3. Elija **Microsoft Azure** como proveedor de cloud.

   Recuerde que el conector debe tener una conexión de red al tipo de entorno de trabajo que está creando y a los servicios que está planeando habilitar.

   "Obtenga más información sobre los requisitos de red del conector".

4. Revise lo que necesitará y haga clic en **continuar**.
5. Si se le solicita, inicie sesión en su cuenta de Microsoft, que debería tener los permisos necesarios para crear la máquina virtual.

El formulario es propiedad de Microsoft y está alojado en él. Sus credenciales no se proporcionan a NetApp.

Si ya ha iniciado sesión en una cuenta de Azure, Cloud Manager utilizará esa cuenta automáticamente. Si tiene varias cuentas, es posible que deba cerrar la sesión primero para asegurarse de utilizar la cuenta correcta.

6. Proporcione la información necesaria:
   - **autenticación de VM**: Introduzca un nombre para la máquina virtual y un nombre de usuario y contraseña o clave pública.
   - **Configuración básica**: Elija una suscripción a Azure, una región de Azure y si desea crear un nuevo grupo de recursos o utilizar un grupo de recursos existente.
   - **Red**: Elija un vnet y una subred, si desea activar una dirección IP pública y, opcionalmente, especifique una configuración de proxy.
   - **Grupo de seguridad**: Elija si desea crear un nuevo grupo de seguridad o si desea seleccionar un grupo de seguridad existente que permita el acceso entrante HTTP, HTTPS y SSH.

No hay tráfico entrante en el conector, a menos que lo inicie. HTTP y HTTPS proporcionan acceso al "Interfaz de usuario local", que utilizará en raras circunstancias. SSH solo es necesario si necesita conectarse al host para la solución de problemas.

7. Haga clic en **Crear**.

   La máquina virtual debe estar lista en unos 7 minutos. Debe permanecer en la página hasta que el proceso se complete.

Después de terminar

Debe asociar un conector a áreas de trabajo para que los administradores del área de trabajo puedan utilizar estos conectores para crear sistemas Cloud Volumes ONTAP. Si sólo tiene Administradores de cuentas, no es necesario asociar el conector a áreas de trabajo. Los administradores de cuentas tienen la posibilidad de acceder a todos los espacios de trabajo de Cloud Manager de forma predeterminada. "Leer más".

Creación de un conector en GCP desde Cloud Manager

Un administrador de cuentas debe implementar un *Connector* antes de poder utilizar la mayoría de las funciones de Cloud Manager. "Aprender cuando se necesita un conector". El conector permite a Cloud Manager gestionar recursos y procesos dentro de su entorno de cloud público.

En esta página se describe cómo crear un conector en GCP directamente desde Cloud Manager. También tiene la opción a. "descargue el software e instálelo en su propio host".

Estos pasos deben ser completados por un usuario que tenga la función de administrador de cuentas. Un administrador de área de trabajo no puede crear un conector.

Al crear su primer entorno de trabajo de Cloud Volumes ONTAP, Cloud Manager le solicitará que cree un conector si aún no lo tiene.

Configuración de los permisos de GCP para crear un conector

Antes de poder implementar un conector desde Cloud Manager, debe asegurarse de que su cuenta de GCP tiene los permisos correctos y de que se haya configurado una cuenta de servicio para la máquina virtual Connector.

Pasos

1. Compruebe que el usuario de GCP que implementa Cloud Manager desde NetApp Cloud Central tiene los permisos en el "Política de implementación de conectores para GCP".

   "Puede crear una función personalizada con el archivo YAML" y, a continuación, adjuntarlo al usuario. Deberá utilizar la línea de comandos gcloud para crear la función.

2. Configure una cuenta de servicio con los permisos que Cloud Manager necesita para crear y gestionar sistemas Cloud Volumes ONTAP en los proyectos.

   Asociará esta cuenta de servicio con Connector VM al crearla desde Cloud Manager.

   a. "Crear un rol en GCP" esto incluye los permisos definidos en la "Política de Cloud Manager para GCP". De nuevo, deberá utilizar la línea de comandos gcloud.

      Los permisos contenidos en este archivo YAML son diferentes a los del paso 2a.

   b. "Cree una cuenta de servicio de GCP y aplique el rol personalizado que acaba de crear".

   c. Si desea poner en marcha Cloud Volumes ONTAP en otros proyectos, "Conceda el acceso añadiendo la cuenta de servicio con la nube La función de gerente de ese proyecto". Deberá repetir este paso con cada proyecto.

Resultado

El usuario GCP ahora tiene los permisos necesarios para crear el conector desde Cloud Manager y se configura la cuenta de servicio para el conector VM.

Habilitar las API de Google Cloud

Se necesitan varias API para implementar el conector y Cloud Volumes ONTAP.

Paso

1. "Habilite las siguientes API de Google Cloud en su proyecto".
   - API de Cloud Deployment Manager V2
   - API de registro en la nube
   - API de Cloud Resource Manager
   - API del motor de computación
   - API de gestión de acceso e identidad (IAM)

Creación de un conector en GCP

Cloud Manager le permite crear un conector en GCP directamente desde su interfaz de usuario.

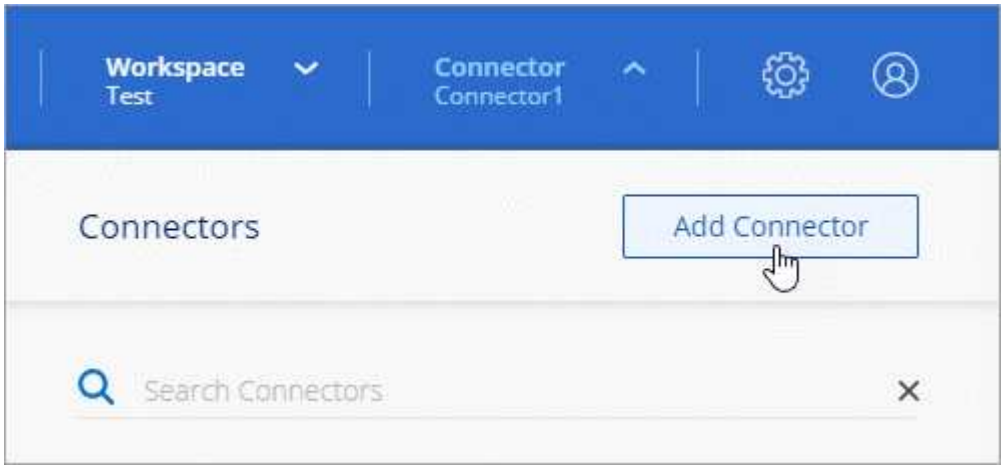
Lo que necesitará

- La "permisos necesarios" Para su cuenta de Google Cloud.
- Un proyecto de Google Cloud.

- Cuenta de servicio con los permisos necesarios para crear y gestionar Cloud Volumes ONTAP.
- VPC y una subred en la región de su elección de Google Cloud.

Pasos

1. Si está creando su primer entorno de trabajo, haga clic en **Agregar entorno de trabajo** y siga las indicaciones. De lo contrario, haga clic en el menú desplegable **conector** y seleccione **Agregar conector**.



2. Haga clic en **Iniciar**.
3. Elija **Google Cloud Platform** como su proveedor de cloud.

   Recuerde que el conector debe tener una conexión de red al tipo de entorno de trabajo que está creando y a los servicios que está planeando habilitar.

   "Obtenga más información sobre los requisitos de red del conector".

4. Revise lo que necesitará y haga clic en **continuar**.
5. Si se le solicita, inicie sesión en su cuenta de Google, que debería tener los permisos necesarios para crear la instancia de la máquina virtual.

   El formulario es propiedad de Google y está alojado en él. Sus credenciales no se proporcionan a NetApp.

6. Proporcione la información necesaria:
   - **Configuración básica**: Escriba un nombre para la instancia de la máquina virtual y especifique un proyecto y una cuenta de servicio que tenga los permisos necesarios.
   - **ubicación**: Especifique una región, zona, VPC y subred para la instancia.
   - **Red**: Elija si desea activar una dirección IP pública y, opcionalmente, especifique una configuración de proxy.
   - **Directiva de firewall**: Elija si desea crear una nueva directiva de firewall o si desea seleccionar una directiva de firewall existente que permita el acceso entrante HTTP, HTTPS y SSH.

     No hay tráfico entrante en el conector, a menos que lo inicie. HTTP y HTTPS proporcionan acceso al "Interfaz de usuario local", que utilizará en raras circunstancias. SSH solo es necesario si necesita conectarse al host para la solución de problemas.

7. Haga clic en **Crear**.

La instancia debe estar lista en unos 7 minutos. Debe permanecer en la página hasta que el proceso se complete.

Después de terminar

Debe asociar un conector a áreas de trabajo para que los administradores del área de trabajo puedan utilizar estos conectores para crear sistemas Cloud Volumes ONTAP. Si sólo tiene Administradores de cuentas, no es necesario asociar el conector a áreas de trabajo. Los administradores de cuentas tienen la posibilidad de acceder a todos los espacios de trabajo de Cloud Manager de forma predeterminada. "Leer más".

A continuación, ¿dónde ir

Ahora que ha iniciado sesión y configurado Cloud Manager, los usuarios pueden comenzar a crear y detectar entornos de trabajo.

- "Empiece a usar Cloud Volumes ONTAP para AWS"
- "Empiece a usar Cloud Volumes ONTAP para Azure"
- "Empiece a usar Cloud Volumes ONTAP para Google Cloud"
- "Configure Azure NetApp Files"
- "Configure Cloud Volumes Service para AWS"
- "Detectar un clúster de ONTAP en las instalaciones"
- "Descubra sus buckets de Amazon S3"

Si es administrador, puede gestionar la configuración de Cloud Manager después de crear el primer conector.

- "Más información sobre conectores"
- "Gestione un certificado HTTPS para un acceso seguro"
- "Configure los ajustes de proxy"

Gestione Cloud Volumes ONTAP

Aprenda

Más información sobre Cloud Volumes ONTAP

Cloud Volumes ONTAP le permite optimizar los costes y el rendimiento del almacenamiento en cloud, a la vez que mejora la protección de datos, la seguridad y el cumplimiento de normativas.

Cloud Volumes ONTAP es un dispositivo de almacenamiento exclusivamente de software que ejecuta el software de gestión de datos ONTAP en el cloud. Ofrece almacenamiento empresarial con las siguientes funciones clave:

- Eficiencias del almacenamiento

  Aproveche las funciones integradas de deduplicación de datos, compresión de datos, thin provisioning y clonado para minimizar los costes en almacenamiento.

- Alta disponibilidad

  Garantice la fiabilidad de su empresa y la continuidad de las operaciones en caso de fallos en su entorno cloud.

- Protección de datos

  Cloud Volumes ONTAP aprovecha SnapMirror, la tecnología de replicación líder del sector de NetApp, para replicar los datos en las instalaciones al cloud para que sea fácil disponer de copias secundarias para varios casos de uso.

  Cloud Volumes ONTAP también se integra con Cloud Backup Service para proporcionar funcionalidades de backup y restauración para la protección y archivado de datos en el cloud a largo plazo.

- Organización en niveles de los datos

  Cambie entre pools de almacenamiento de alto y bajo rendimiento bajo demanda sin desconectar las aplicaciones.

- Consistencia de las aplicaciones

  Garantice la consistencia de las copias Snapshot de NetApp mediante SnapCenter de NetApp.

- Seguridad de datos

  Cloud Volumes ONTAP admite el cifrado de datos y proporciona protección contra virus y ransomware.

- Controles de cumplimiento de normas de privacidad

  La integración con Cloud Compliance le ayuda a comprender el contexto de los datos e identificar datos confidenciales.

Con Cloud Volumes ONTAP se incluyen las licencias para funciones de ONTAP.

"Consulte las configuraciones de Cloud Volumes ONTAP admitidas"

"Obtenga más información acerca de Cloud Volumes ONTAP"

Reducida

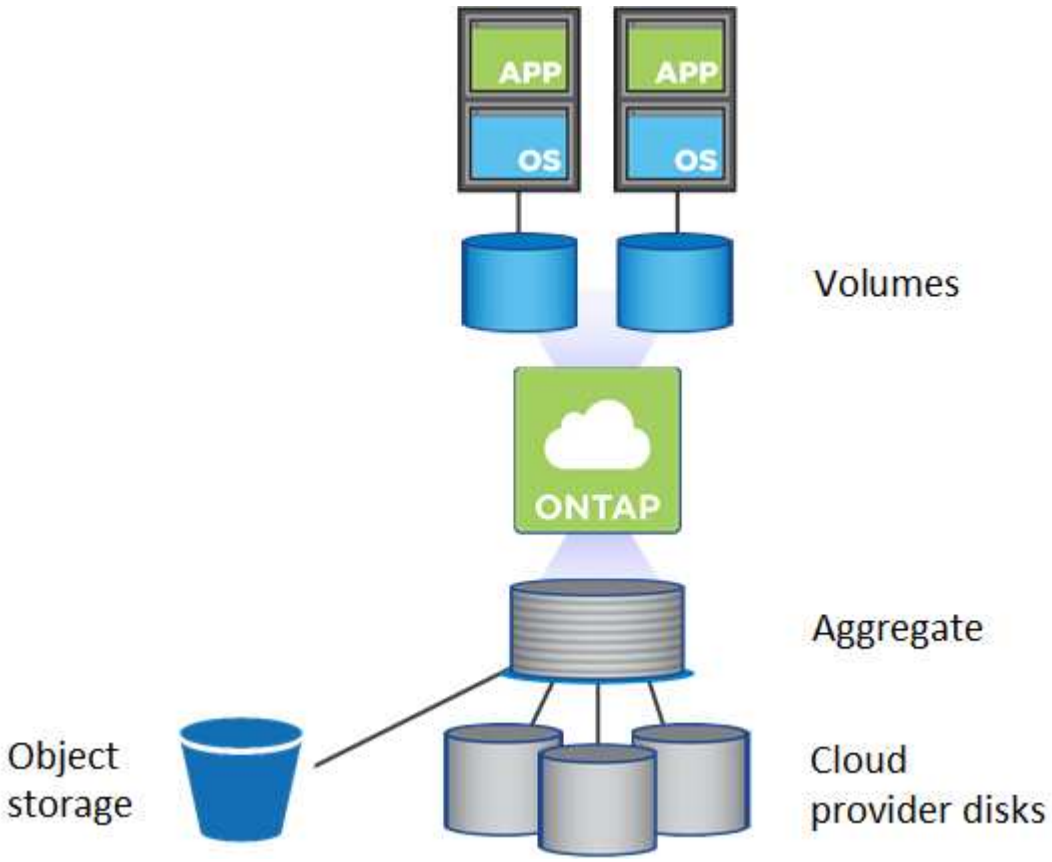
Discos y agregados

Comprender cómo utiliza Cloud Volumes ONTAP el almacenamiento en cloud puede ayudarle a comprender los costes de almacenamiento.

Todos los discos y agregados deben crearse y eliminarse directamente desde Cloud Manager. No debe realizar estas acciones desde otra herramienta de gestión. De esta manera, se puede afectar a la estabilidad del sistema, se puede obstaculizar la capacidad de añadir discos en el futuro y generar potencialmente cuotas redundantes para proveedores de cloud.

Descripción general

Cloud Volumes ONTAP usa el almacenamiento del proveedor de cloud como discos y los agrupa en uno o más agregados. Los agregados proporcionan almacenamiento a uno o varios volúmenes.



Se admiten varios tipos de discos de cloud. Al crear un volumen y el tamaño de disco predeterminado al implementar Cloud Volumes ONTAP, elija el tipo de disco.

La cantidad total de almacenamiento comprado a un proveedor de cloud es la *raw Capacity*. El *capacidad utilizable* es menor porque aproximadamente del 12 al 14 % es la sobrecarga reservada para el uso de Cloud Volumes ONTAP. Por ejemplo, si Cloud Manager crea un agregado de 500 GB, la capacidad utilizable es de 442.94 GB.

Almacenamiento AWS

En AWS, Cloud Volumes ONTAP utiliza almacenamiento EBS para datos de usuario y almacenamiento NVMe local como Flash Cache en algunos tipos de instancias de EC2.

Almacenamiento de EBS

En AWS, un agregado puede contener hasta 6 discos con el mismo tamaño. El tamaño máximo de disco es 16 TB.

El tipo de disco EBS subyacente puede ser SSD de uso general, SSD de IOPS aprovisionado, HDD de rendimiento optimizado o HDD en frío. Es posible emparejar un disco de EBS con Amazon S3 a. "organice en niveles los datos inactivos en almacenamiento de objetos de bajo coste".

En líneas generales, las diferencias entre los tipos de discos EBS son las siguientes:

- *SSD* los discos de uso general equilibran el coste y el rendimiento de una amplia gama de cargas de trabajo. El rendimiento se define en términos de IOPS.
- Los discos SSD_ aprovisionados de _IOPS se utilizan para aplicaciones esenciales que requieren el mayor rendimiento a un coste más elevado.
- *los discos HDD* optimizados para rendimiento se utilizan para cargas de trabajo de acceso frecuente que requieren un rendimiento rápido y constante a un precio más bajo.
- *HDD* los discos están diseñados para realizar backups o datos a los que se accede con poca frecuencia porque el rendimiento es muy bajo. Al igual que los discos HDD optimizados para el rendimiento, el rendimiento se define en términos de rendimiento.

Los discos HDD de datos fríos no son compatibles con configuraciones de alta disponibilidad ni con niveles de datos.

Almacenamiento NVMe local

Algunos tipos de instancias de EC2 incluyen almacenamiento NVMe local, que Cloud Volumes ONTAP utiliza como "Flash Cache".

Enlaces relacionados

- "Documentación de AWS: Tipos de volúmenes de EBS"
- "Aprenda a elegir tipos de disco y tamaños de disco para Sus sistemas en AWS"
- "Revise los límites de almacenamiento de Cloud Volumes ONTAP en AWS"
- "Revise las configuraciones compatibles para Cloud Volumes ONTAP en AWS"

Almacenamiento Azure

En Azure, un agregado puede contener hasta 12 discos con el mismo tamaño. El tipo de disco y el tamaño máximo del disco dependen de si se utiliza un sistema de nodo único o un par de alta disponibilidad:

Sistemas de un solo nodo

Los sistemas de un solo nodo pueden usar tres tipos de discos gestionados de Azure:

- *Premium SSD Managed Disks* proporciona un alto rendimiento para cargas de trabajo con un gran volumen de I/o a un coste más elevado.
- *Standard SSD Managed Disks* proporciona un rendimiento constante para cargas de trabajo que requieren un bajo nivel de IOPS.
- *Standard HDD Managed Disks* es una buena opción si no necesita un alto nivel de IOPS y desea reducir sus costes.

  Cada tipo de disco gestionado tiene un tamaño máximo de disco de 32 TB.

  Puede emparejar un disco gestionado con el almacenamiento de Azure Blob para "organice en niveles los datos inactivos en almacenamiento de objetos de bajo coste".

Parejas de HA

Los pares de ALTA DISPONIBILIDAD usan los blobs de página Premium, que tienen un tamaño de disco máximo de 8 TB.

Enlaces relacionados

- "Documentación de Microsoft Azure: Introducción a Microsoft Azure Storage"
- "Aprenda a elegir tipos de disco y tamaños de disco para Sus sistemas en Azure"
- "Revise los límites de almacenamiento de Cloud Volumes ONTAP en Azure"

Almacenamiento para GCP

En GCP, un agregado puede contener hasta 6 discos con el mismo tamaño. El tamaño máximo de disco es 16 TB.

El tipo de disco puede ser *Zonal SSD persistent disks* o *Zonal standard persistent disks*. Puede emparejar discos persistentes con un bloque de Google Storage para "organice en niveles los datos inactivos en almacenamiento de objetos de bajo coste".

Enlaces relacionados

- "Documentación de Google Cloud Platform: Opciones de almacenamiento"
- "Revise los límites de almacenamiento de Cloud Volumes ONTAP en GCP"

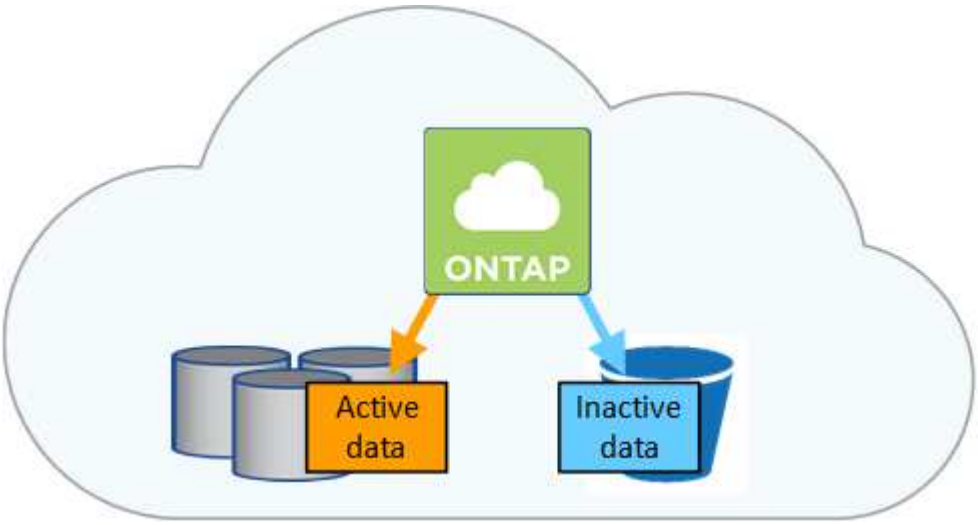
Tipo de RAID

El tipo RAID para cada agregado de Cloud Volumes ONTAP es RAID0 (segmentación). No se admite ningún otro tipo de RAID. Cloud Volumes ONTAP confía en el proveedor cloud para garantizar la disponibilidad de disco y la durabilidad.

Información general sobre organización en niveles de datos

Reduzca los costes de almacenamiento al permitir un almacenamiento de objetos de bajo coste mediante la segmentación automatizada de los datos inactivos. Los datos activos permanecen en unidades SSD o HDD de alto rendimiento, mientras que los datos inactivos se organizan en niveles en almacenamiento de objetos de bajo coste. De

este modo, podrá recuperar espacio en el almacenamiento primario y reducir el almacenamiento secundario.



Cloud Volumes ONTAP admite la organización en niveles de datos en AWS, Azure y Google Cloud Platform. La organización en niveles de datos utiliza la tecnología FabricPool.

No es necesario instalar una licencia de funciones para habilitar la organización en niveles de datos (FabricPool).

Organización en niveles de los datos en AWS

Al habilitar la organización en niveles de datos en AWS, Cloud Volumes ONTAP utiliza EBS como nivel de rendimiento para los datos activos y AWS S3 como nivel de capacidad para los datos inactivos.

Nivel de rendimiento

El nivel de rendimiento puede ser SSD de uso general, SSD de IOPS aprovisionados o HDD optimizados para el rendimiento.

Nivel de capacidad

Un sistema Cloud Volumes ONTAP organiza los datos inactivos en niveles en un único bloque de S3 utilizando la clase de almacenamiento *Standard*. El estándar es ideal para datos a los que se accede con frecuencia almacenados en múltiples zonas de disponibilidad.

Cloud Manager crea un único bloque de S3 para cada entorno laboral y lo nombra identificador único de estructura-pool-_clúster. No se crea otro bloque de S3 para cada volumen.

Clases de almacenamiento

La clase de almacenamiento predeterminada para los datos por niveles en AWS es *Standard*. Si no tiene previsto acceder a los datos inactivos, puede reducir sus costes de almacenamiento cambiando la clase de almacenamiento por una de las siguientes opciones: *Intelligent Tiering*, *One-Zone Infrecuente Access* o *Standard-Infrecuente Access*. Al cambiar la clase de almacenamiento, los datos inactivos se inician en la clase de almacenamiento estándar y se pasan a la clase de almacenamiento seleccionada si no se accede a los datos después de 30 días.

Los costes de acceso son más elevados si se accede a los datos, por lo que hay que tener en cuenta antes de cambiar la clase de almacenamiento. "Obtenga más información acerca de las clases de

almacenamiento de Amazon S3".

Puede seleccionar una clase de almacenamiento cuando cree el entorno de trabajo y puede cambiarla en cualquier momento. Para obtener información detallada sobre cómo cambiar la clase de almacenamiento, consulte "Organización en niveles de los datos inactivos en almacenamiento de objetos de bajo coste".

La clase de almacenamiento para la organización en niveles de los datos es de todo el sistema, pero no por volumen.

Organización en niveles de los datos en Azure

Cuando se habilita la organización en niveles de datos en Azure, Cloud Volumes ONTAP utiliza discos gestionados de Azure como nivel de rendimiento para los datos activos y el almacenamiento de Azure Blob como nivel de capacidad para los datos inactivos.

Nivel de rendimiento

El nivel de rendimiento puede ser SSD o HDD.

Nivel de capacidad

Un sistema Cloud Volumes ONTAP organiza los datos inactivos en niveles en un único contenedor BLOB utilizando el nivel de almacenamiento Azure *hot*. El nivel activo es ideal para los datos a los que se accede con frecuencia.

Cloud Manager crea una nueva cuenta de almacenamiento con un único contenedor para cada entorno de trabajo de Cloud Volumes ONTAP. El nombre de la cuenta de almacenamiento es aleatorio. No se crea un contenedor diferente para cada volumen.

Niveles de acceso al almacenamiento

El nivel de acceso al almacenamiento predeterminado para los datos por niveles en Azure es el nivel *hot*. Si no tiene pensado acceder a los datos inactivos, puede reducir sus costes de almacenamiento cambiando al nivel de almacenamiento *COOL*. Cuando cambia el nivel de almacenamiento, los datos inactivos se inician en el nivel de almacenamiento activo y se pasan a la capa de almacenamiento frío, si no se accede a los datos después de 30 días.

Los costes de acceso son más elevados si accede a los datos, por lo que tenga en cuenta antes de cambiar el nivel de almacenamiento. "Obtenga más información acerca de los niveles de acceso al almacenamiento de Azure Blob".

Es posible seleccionar un nivel de almacenamiento al crear el entorno de trabajo y cambiarlo siempre que se desee. Para obtener más información sobre cómo cambiar el nivel de almacenamiento, consulte "Organización en niveles de los datos inactivos en almacenamiento de objetos de bajo coste".

El nivel de acceso al almacenamiento para la organización en niveles de los datos es de todo el sistema, pero no lo es por volumen.

Organización en niveles de los datos en GCP

Cuando se habilita la organización en niveles de datos en GCP, Cloud Volumes ONTAP utiliza discos persistentes como nivel de rendimiento para los datos activos y un cubo de Google Cloud Storage como nivel de capacidad para los datos inactivos.

Nivel de rendimiento

El nivel de rendimiento puede ser SSD o HDD (discos estándar).

Nivel de capacidad

Un sistema Cloud Volumes ONTAP organiza los datos inactivos en niveles en un único bucket de Google Cloud Storage mediante la clase de almacenamiento *Regional*.

Cloud Manager crea un único bloque para cada entorno de trabajo y lo nombra identificador único de estructura-pool-_clúster. No se crea otro bloque para cada volumen.

Clases de almacenamiento

La clase de almacenamiento predeterminada para los datos por niveles es la clase *Standard Storage*. Si se accede a los datos con poca frecuencia, puede reducir los costes de almacenamiento cambiando a *Nearline Storage* o *Coldline Storage*. Al cambiar la clase de almacenamiento, los datos inactivos se inician en la clase de almacenamiento estándar y se pasan a la clase de almacenamiento seleccionada si no se accede a los datos después de 30 días.

Los costes de acceso son más elevados si se accede a los datos, por lo que hay que tener en cuenta antes de cambiar la clase de almacenamiento. "Obtenga más información sobre clases de almacenamiento para Google Cloud Storage".

Es posible seleccionar un nivel de almacenamiento al crear el entorno de trabajo y cambiarlo siempre que se desee. Para obtener información detallada sobre cómo cambiar la clase de almacenamiento, consulte "Organización en niveles de los datos inactivos en almacenamiento de objetos de bajo coste".

La clase de almacenamiento para la organización en niveles de los datos es de todo el sistema, pero no por volumen.

Organización en niveles de los datos y límites de capacidad

Si se habilita la organización en niveles de datos, el límite de capacidad de un sistema sigue siendo el mismo. El límite se distribuye entre el nivel de rendimiento y el nivel de capacidad.

Políticas de organización en niveles del volumen

Para habilitar la organización en niveles de datos, es necesario seleccionar una política de organización en niveles de volumen cuando se crea, se modifica o se replica un volumen. Puede seleccionar una política diferente para cada volumen.

Algunas políticas de organización en niveles tienen un período de refrigeración mínimo asociado, que establece el tiempo en el que los datos de un volumen deben permanecer inactivos para que los datos se consideren "inactivos" y moverse al nivel de capacidad.

Cloud Manager permite elegir entre las siguientes políticas de organización en niveles del volumen al crear o modificar un volumen:

Solo Snapshot

Cuando un agregado ha alcanzado la capacidad del 50%, Cloud Volumes ONTAP genera datos de usuarios inactivos de copias Snapshot que no están asociadas con el sistema de archivos activo al nivel de capacidad. El período de enfriamiento es de aproximadamente 2 días.

Si se leen, los bloques de datos inactivos del nivel de capacidad se activan y se mueven al nivel de rendimiento.

Todo

Todos los datos (no incluidos los metadatos) se marcan inmediatamente como fríos y por niveles en el almacenamiento de objetos lo antes posible. No es necesario esperar 48 horas hasta que se enfrían los

bloques nuevos en un volumen. Tenga en cuenta que los bloques ubicados en el volumen antes de ajustar la normativa de todo requieren 48 horas de frío.

Si se leen, los bloques de datos inactivos del nivel de cloud permanecen activos y no se vuelven a escribir en el nivel de rendimiento. Esta política está disponible a partir de ONTAP 9.6.

Automático

Después de que un agregado ha alcanzado la capacidad del 50 %, Cloud Volumes ONTAP organiza en niveles bloques de datos inactivos en un volumen en un nivel de capacidad. Los datos inactivos incluyen no solo copias snapshot, sino también datos de usuarios inactivos del sistema de archivos activo. El período de enfriamiento es de aproximadamente 31 días.

Esta política es compatible a partir de Cloud Volumes ONTAP 9.4.

Si las lecturas aleatorias las leen, los bloques de datos fríos del nivel de capacidad se activan y se mueven al nivel de rendimiento. Si las lecturas secuenciales se leen, como las asociadas con el índice y los análisis antivirus, los bloques de datos inactivos permanecen inactivos y no se mueven al nivel de rendimiento.

Ninguno

Mantiene datos de un volumen en el nivel de rendimiento, lo que impide que se mueva al nivel de capacidad.

Al replicar un volumen, se puede elegir si se van a organizar los datos en niveles en el almacenamiento de objetos. Si lo hace, Cloud Manager aplica la directiva **Backup** al volumen de protección de datos. A partir de Cloud Volumes ONTAP 9.6, la política de organización en niveles **todo** sustituye a la política de copia de seguridad.

La desactivación de Cloud Volumes ONTAP afecta al período de refrigeración

Los bloques de datos se enfrían mediante exploraciones de refrigeración. Durante este proceso, los bloques que no se han utilizado han movido la temperatura del bloque (enfriado) al siguiente valor más bajo. El tiempo de refrigeración predeterminado depende de la política de organización en niveles del volumen:

- Auto: 31 días
- Snapshot Only: 2 días

Cloud Volumes ONTAP debe estar en ejecución para que funcione la exploración de refrigeración. Si el Cloud Volumes ONTAP está apagado, la refrigeración también se detendrá. Como consecuencia, podría experimentar tiempos de refrigeración más largos.

Configuración de la organización en niveles de los datos

Para obtener instrucciones y una lista de las configuraciones compatibles, consulte "Organización en niveles de los datos inactivos en almacenamiento de objetos de bajo coste".

Gestión del almacenamiento

Cloud Manager proporciona una gestión simplificada y avanzada del almacenamiento de Cloud Volumes ONTAP.

Todos los discos y agregados deben crearse y eliminarse directamente desde Cloud Manager. No debe realizar estas acciones desde otra herramienta de gestión. De esta manera, se puede afectar a la estabilidad del sistema, se puede obstaculizar la capacidad de añadir discos en el futuro y generar potencialmente cuotas redundantes para proveedores de cloud.

Aprovisionamiento de almacenamiento

Cloud Manager facilita el aprovisionamiento de almacenamiento para Cloud Volumes ONTAP al comprar discos y gestionar agregados. Solo tiene que crear volúmenes. Puede utilizar una opción de asignación avanzada para aprovisionar los agregados por sí mismo, si lo desea.

Aprovisionamiento simplificado

Los agregados proporcionan almacenamiento en cloud a volúmenes. Cloud Manager crea agregados para el usuario cuando inicia una instancia y cuando aprovisiona volúmenes adicionales.

Al crear un volumen, Cloud Manager lleva a cabo una de estas tres cosas:

- Coloca el volumen en un agregado existente que tiene suficiente espacio libre.
- Coloca el volumen en una agrupación existente al comprar más discos para esa agrupación.
- Compra discos para un nuevo agregado y coloca el volumen en ese agregado.

Cloud Manager determina dónde colocar un nuevo volumen examinando varios factores: El tamaño máximo de un agregado, si está habilitado el aprovisionamiento ligero y los umbrales de espacio libre para los agregados.

El administrador de cuentas puede modificar los umbrales de espacio libre desde la página **Configuración**.

Selección de tamaño de disco para agregados en AWS

Cuando Cloud Manager crea nuevos agregados para Cloud Volumes ONTAP en AWS, aumenta gradualmente el tamaño del disco en un agregado, a medida que aumenta el número de agregados del sistema. Cloud Manager logra esto para garantizar que la capacidad máxima del sistema se pueda utilizar antes de que alcance el número máximo de discos de datos permitidos en AWS.

Por ejemplo, Cloud Manager podría elegir los siguientes tamaños de disco para los agregados en un sistema Premium o BYOL de Cloud Volumes ONTAP:

Número de agregado	Tamaño de disco	Capacidad máxima de agregado
1	500 MB	3 TB
4	1 TB	6 TB
6	2 TB	12 TB

Puede elegir el tamaño del disco usted mismo utilizando la opción de asignación avanzada.

Asignación avanzada

En lugar de dejar que Cloud Manager gestione agregados, puede hacerlo usted mismo. "Desde la página **asignación avanzada**", puede crear nuevos agregados que incluyan un número específico de discos, agregar

discos a un agregado existente y crear volúmenes en agregados específicos.

Gestión de la capacidad

El administrador de cuentas puede elegir si Cloud Manager notifica las decisiones sobre capacidad de almacenamiento o si Cloud Manager gestiona automáticamente los requisitos de capacidad. Puede que le resulte útil comprender cómo funcionan estos modos.

Gestión de la capacidad automática

El modo de gestión de la capacidad se establece como automático de manera predeterminada. En este modo, Cloud Manager adquiere automáticamente discos nuevos para instancias de Cloud Volumes ONTAP cuando se necesita más capacidad, elimina las colecciones de discos (agregados) no utilizadas, mueve volúmenes entre agregados cuando es necesario e intenta dejar los discos sin fallo.

A continuación se muestran ejemplos de cómo funciona este modo:

- Si un agregado con 5 o menos discos EBS llega al umbral de capacidad, Cloud Manager compra automáticamente nuevos discos para ese agregado, de modo que los volúmenes puedan seguir creciendo.
- Si un agregado con 12 discos de Azure alcanza el umbral de capacidad, Cloud Manager mueve automáticamente un volumen de ese agregado a un agregado con capacidad disponible o a un nuevo agregado.

  Si Cloud Manager crea un nuevo agregado para el volumen, elige un tamaño de disco que aloja el tamaño de ese volumen.

  Tenga en cuenta que ahora hay espacio libre disponible en el agregado original. Los volúmenes existentes o los volúmenes nuevos pueden usar ese espacio. En este escenario, no se puede devolver el espacio a AWS, Azure o GCP.

- Si un agregado no contiene volúmenes durante más de 12 horas, Cloud Manager los elimina.

Gestión de LUN con gestión de la capacidad automática

La gestión automática de la capacidad de Cloud Manager no se aplica a las LUN. Cuando Cloud Manager crea un LUN, deshabilita la función de crecimiento automático.

Gestión de inodos con gestión automática de la capacidad

Cloud Manager supervisa el uso de nodos de información en un volumen. Cuando se utiliza el 85 % de los inodos, Cloud Manager aumenta el tamaño del volumen para aumentar el número de inodos disponibles. El número de archivos que puede contener un volumen está determinado por la cantidad de inodos que tiene.

Gestión manual de la capacidad

Si el administrador de cuentas establece el modo de gestión de la capacidad en manual, Cloud Manager muestra los mensajes de acción necesarios cuando se deben tomar decisiones sobre la capacidad. Los mismos ejemplos descritos en el modo automático se aplican al modo manual, pero depende de usted aceptar las acciones.

Flash Cache

Algunas configuraciones de Cloud Volumes ONTAP en AWS y Azure incluyen

almacenamiento NVMe local, que Cloud Volumes ONTAP utiliza como *Flash Cache* para mejorar el rendimiento.

¿Qué es Flash Cache?

Flash Cache acelera el acceso a los datos mediante el almacenamiento en caché inteligente en tiempo real de datos recientes de usuarios y metadatos de NetApp. Es eficaz para cargas de trabajo de lectura intensiva aleatoria, como bases de datos, correo electrónico y servicios de archivos.

Instancias compatibles en AWS

Seleccione uno de los siguientes tipos de instancia de EC2 con un sistema Cloud Volumes ONTAP Premium o BYOL nuevo o existente:

- c5d.4 x grande
- c5d.9xlarge
- c5d.18xlarge
- m5d.8xgrande
- m5d.12xlarge
- r5d.2xgrande

Tipo de máquina virtual compatible en Azure

Seleccione el tipo de máquina virtual Standard_L8S_v2 con un sistema BYOL de Cloud Volumes ONTAP de un solo nodo en Azure.

Limitaciones

- La compresión debe deshabilitarse en todos los volúmenes para aprovechar las mejoras de rendimiento de Flash Cache.

  No seleccione ninguna eficiencia de almacenamiento cuando cree un volumen desde Cloud Manager, ni cree un volumen y, a continuación, "Deshabilite la compresión de datos mediante la CLI".

- Cloud Volumes ONTAP no admite el recalentamiento de la caché después de un reinicio.

Almacenamiento WORM

Puede activar el almacenamiento de escritura única y lectura múltiple (WORM) en un sistema Cloud Volumes ONTAP para conservar los archivos en forma no modificada durante un período de retención específico. El almacenamiento WORM cuenta con la tecnología SnapLock en el modo empresarial, lo que significa que los archivos WORM están protegidos a nivel de archivo.

Una vez comprometido un archivo con el almacenamiento WORM, no se podrá modificar, ni siquiera después de que haya caducado el período de retención. Un reloj a prueba de manipulaciones determina cuándo ha transcurrido el período de retención de un archivo WORM.

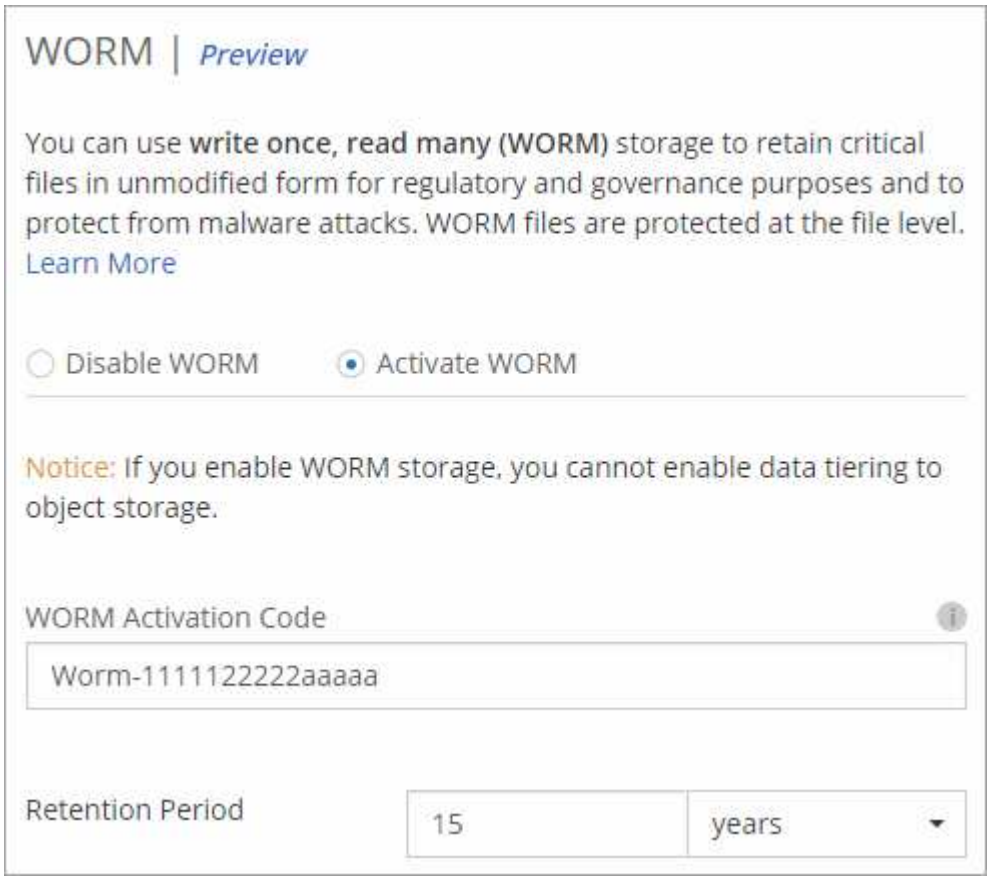
Una vez transcurrido el período de retención, es responsable de eliminar los archivos que ya no se necesiten.

Activación del almacenamiento WORM

Puede activar el almacenamiento WORM en un sistema Cloud Volumes ONTAP cuando crea un nuevo entorno de trabajo. Esto incluye especificar un código de activación y establecer el período de retención predeterminado para los archivos. Puede obtener un código de activación mediante el icono de chat de la parte inferior derecha de la interfaz de Cloud Manager.

No puede activar el almacenamiento WORM en volúmenes individuales; debe activarse WORM en el nivel de sistema.

En la siguiente imagen, se muestra cómo activar el almacenamiento WORM durante la creación de un entorno de trabajo:



Conserva archivos en WORM

Puede utilizar una aplicación para confirmar los archivos a WORM a través de NFS o CIFS, o utilizar la interfaz de línea de comandos de ONTAP para confirmar automáticamente los archivos a WORM. También puede utilizar un archivo WORM ampliable para conservar datos que se escriben de forma incremental, como la información de registro.

Después de activar el almacenamiento WORM en un sistema Cloud Volumes ONTAP, debe utilizar la CLI de ONTAP para toda la gestión del almacenamiento WORM. Para obtener instrucciones, consulte "Documentación de ONTAP".

La compatibilidad con Cloud Volumes ONTAP para el almacenamiento WORM equivale al modo empresarial de SnapLock.

Limitaciones

- Si elimina o mueve un disco directamente de AWS o Azure, puede eliminar un volumen antes de su fecha de caducidad.
- Cuando se activa el almacenamiento WORM, no se puede habilitar la organización en niveles de datos en el almacenamiento de objetos.
- Es necesario deshabilitar el backup en el cloud para poder habilitar el almacenamiento WORM.

Pares de alta disponibilidad

Pares de alta disponibilidad en AWS

Una configuración de alta disponibilidad de Cloud Volumes ONTAP proporciona operaciones no disruptivas y tolerancia a fallos. En AWS, los datos se replican de forma síncrona entre los dos nodos.

Descripción general

En AWS, las configuraciones de alta disponibilidad de Cloud Volumes ONTAP incluyen los siguientes componentes:

- Dos nodos Cloud Volumes ONTAP cuyos datos se reflejan de forma síncrona entre sí.
- Una instancia de mediador que proporciona un canal de comunicación entre los nodos para ayudar a tomar la toma de control y los procesos de devolución del almacenamiento.

> La instancia del mediador ejecuta el sistema operativo Linux en una instancia t2.micro y utiliza un disco magnético EBS de aproximadamente 8 GB.

Toma de control y retorno al nodo primario del almacenamiento

Si un nodo se cae, el otro nodo puede proporcionar datos a su partner para proporcionar un servicio de datos continuado. Los clientes pueden acceder a los mismos datos desde el nodo del partner porque los datos se duplicaron de forma síncrona al partner.

Cuando el nodo se haya reiniciado, el partner debe realizar una resincronización de los datos antes de que pueda devolver el almacenamiento. El tiempo que se tarda en resincronizar los datos depende de cuántos datos han cambiado con el nodo inactivo.

RPO y RTO

Una configuración de alta disponibilidad mantiene una alta disponibilidad de los datos de la siguiente manera:

- El objetivo de punto de recuperación (RPO) es 0 segundos. Sus datos son coherentes transcionalmente sin pérdida de datos.
- El objetivo de tiempo de recuperación (RTO) es de 60 segundos. En el caso de que se produzca una interrupción del servicio, los datos deben estar disponibles en 60 segundos o menos.

Modelos de puesta en marcha de ALTA DISPONIBILIDAD

Puede garantizar la alta disponibilidad de sus datos mediante la implementación de una configuración de alta disponibilidad en varias zonas de disponibilidad (AZs) o en un único AZ. Debe consultar más detalles sobre cada configuración para elegir la que mejor se ajuste a sus necesidades.

Alta disponibilidad de Cloud Volumes ONTAP en múltiples zonas de disponibilidad

La implementación de una configuración de alta disponibilidad en varias zonas de disponibilidad (AZs) garantiza una alta disponibilidad de los datos en caso de que se produzca un fallo con una zona de disponibilidad o una instancia que ejecute un nodo Cloud Volumes ONTAP. Debe comprender cómo las direcciones IP de NAS afectan al acceso a los datos y a la conmutación por error del almacenamiento.

Acceso a datos NFS y CIFS

Cuando una configuración de alta disponibilidad se distribuye por varias zonas de disponibilidad, *direcciones IP flotantes* permiten el acceso de clientes NAS. Las direcciones IP flotantes, que deben estar fuera de los bloques CIDR para todas las VPC de la región, pueden migrar entre nodos cuando se producen fallos. A los clientes que no pertenecen al VPC, no les podrán acceder de forma nativa "Configure una puerta de enlace de tránsito de AWS".

Si no puede configurar una puerta de enlace de tránsito, existen direcciones IP privadas disponibles para clientes NAS que se encuentran fuera del VPC. Sin embargo, estas direcciones IP son estáticas, no pueden realizar una conmutación por error entre nodos.

Debe revisar los requisitos para direcciones IP flotantes y tablas de rutas antes de implementar una configuración de alta disponibilidad en varias zonas de disponibilidad. Es necesario especificar las direcciones IP flotantes al implementar la configuración. Cloud Manager crea automáticamente las direcciones IP privadas.

Para obtener más información, consulte "Requisitos de red de AWS para alta disponibilidad de Cloud Volumes ONTAP en múltiples AZS".

Acceso a datos iSCSI

La comunicación de datos entre VPC no es un problema, ya que iSCSI no utiliza direcciones IP flotantes.

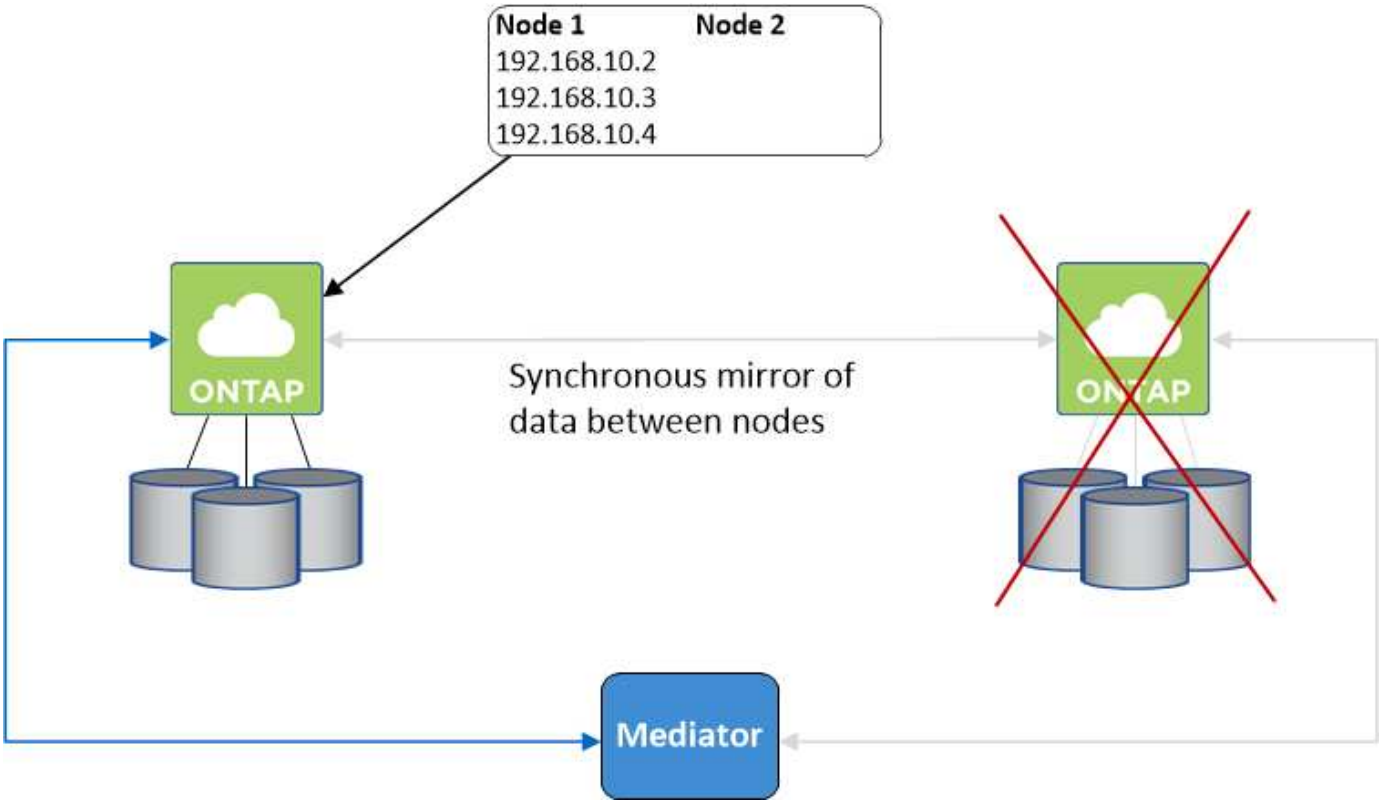
Toma de control y retorno del almacenamiento para iSCSI

Para iSCSI, Cloud Volumes ONTAP utiliza I/o multivía (MPIO) y ALUA (Asymmetric Logical Unit Access) para gestionar la conmutación por error de ruta entre las rutas activas y no optimizadas.

Para obtener información sobre qué configuraciones de host específicas admiten ALUA, consulte "Herramienta de matriz de interoperabilidad de NetApp" Y la guía de instalación y configuración de las utilidades de host para el sistema operativo host.

Toma de control y retorno del almacenamiento para NAS

Cuando la toma de control se produce en una configuración NAS mediante IP flotantes, la dirección IP flotante del nodo que los clientes usan para acceder a datos se mueve al otro nodo. La siguiente imagen muestra la toma de control del almacenamiento en una configuración NAS mediante IP flotantes. Si el nodo 2 cae, la dirección IP flotante del nodo 2 se mueve al nodo 1.



Las IP de datos NAS que se usan para el acceso al VPC externo no se pueden migrar de un nodo a otro en caso de que se produzcan fallos. Si un nodo se desconecta, debe volver a montar manualmente los volúmenes en clientes fuera del VPC mediante la dirección IP del otro nodo.

Una vez que el nodo con errores vuelva a estar en línea, vuelva a montar los clientes en los volúmenes con la dirección IP original. Este paso es necesario para evitar la transferencia de datos innecesarios entre dos nodos de alta disponibilidad, lo que puede causar un impacto significativo en el rendimiento y la estabilidad.

Puede identificar fácilmente la dirección IP correcta desde Cloud Manager seleccionando el volumen y haciendo clic en **Mount Command**.

Alta disponibilidad de Cloud Volumes ONTAP en una única zona de disponibilidad

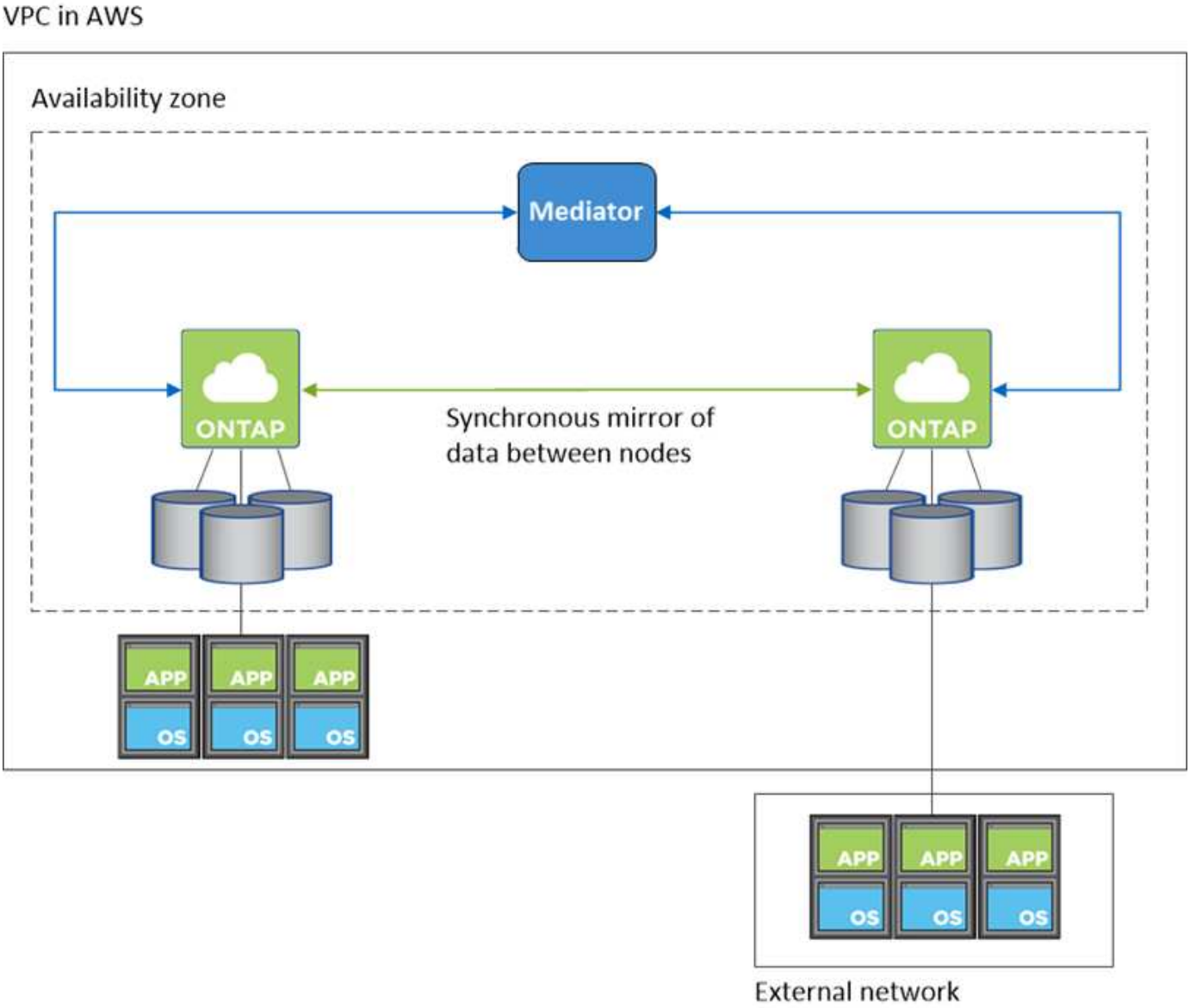
La implementación de una configuración de alta disponibilidad en una única zona de disponibilidad (AZ) puede garantizar una alta disponibilidad de los datos en caso de que falle una instancia que ejecute un nodo de Cloud Volumes ONTAP. Fuera del VPC, se puede acceder a todos los datos de forma nativa.

> Cloud Manager crea un "Grupo de colocación extendido de AWS" E inicia los dos nodos de alta disponibilidad en ese grupo de colocación. El grupo de colocación reduce el riesgo de fallos simultáneos al distribuir las instancias entre el hardware subyacente distinto. Esta función mejora la redundancia desde el punto de vista de la informática, no desde la perspectiva del fallo de disco.

Acceso a los datos

Debido a que esta configuración está en una sola unidad AZ, no requiere direcciones IP flotantes. Puede usar la misma dirección IP para el acceso a datos desde el VPC y desde fuera del VPC.

En la siguiente imagen se muestra una configuración de alta disponibilidad en un único entorno de disponibilidad. Se puede acceder a los datos desde el VPC y desde fuera del VPC.



Toma de control y retorno al nodo primario del almacenamiento

Para iSCSI, Cloud Volumes ONTAP utiliza I/o multivía (MPIO) y ALUA (Asymmetric Logical Unit Access) para gestionar la conmutación por error de ruta entre las rutas activas y no optimizadas.

Para obtener información sobre qué configuraciones de host específicas admiten ALUA, consulte "Herramienta de matriz de interoperabilidad de NetApp" Y la guía de instalación y configuración de las utilidades de host para el sistema operativo host.

En el caso de configuraciones NAS, las direcciones IP de datos pueden migrar entre nodos de alta disponibilidad si se produce un fallo. De este modo se garantiza el acceso del cliente al almacenamiento.

Cómo funciona el almacenamiento en una pareja de alta disponibilidad

A diferencia de un clúster de ONTAP, el almacenamiento de un par de alta disponibilidad de Cloud Volumes ONTAP no se comparte entre los nodos. En su lugar, los datos se reflejan de forma síncrona entre los nodos, de modo que los datos estén disponibles en caso de fallo.

La asignación de almacenamiento

Cuando se crea un volumen nuevo y se requieren discos adicionales, Cloud Manager asigna el mismo número de discos a ambos nodos, crea un agregado reflejado y, a continuación, crea el nuevo volumen. Por ejemplo, si se requieren dos discos para el volumen, Cloud Manager asigna dos discos por nodo para un total de cuatro discos.

Configuraciones de almacenamiento

Puede utilizar un par de alta disponibilidad como configuración activo-activo, en el cual ambos nodos sirven datos a los clientes o como una configuración activo-pasivo, en la cual el nodo pasivo responde a las solicitudes de datos únicamente si ha tomado almacenamiento para el nodo activo.

Solo puede configurar una configuración activo-activo cuando utiliza Cloud Manager en la vista del sistema de almacenamiento.

Expectativas de rendimiento para una configuración de alta disponibilidad

Una configuración de alta disponibilidad de Cloud Volumes ONTAP replica de forma síncrona datos entre los nodos, lo que consume ancho de banda de red. Como resultado, se puede esperar el siguiente rendimiento en comparación con una configuración de Cloud Volumes ONTAP de un solo nodo:

- En el caso de configuraciones de alta disponibilidad que solo proporcionan datos de un nodo, el rendimiento de lectura es comparable al rendimiento de lectura de una configuración con un solo nodo, mientras que el rendimiento de escritura es inferior.
- En el caso de configuraciones de alta disponibilidad que sirven datos de ambos nodos, el rendimiento de lectura es superior al rendimiento de lectura de una configuración de un solo nodo, y el rendimiento de escritura es igual o superior.

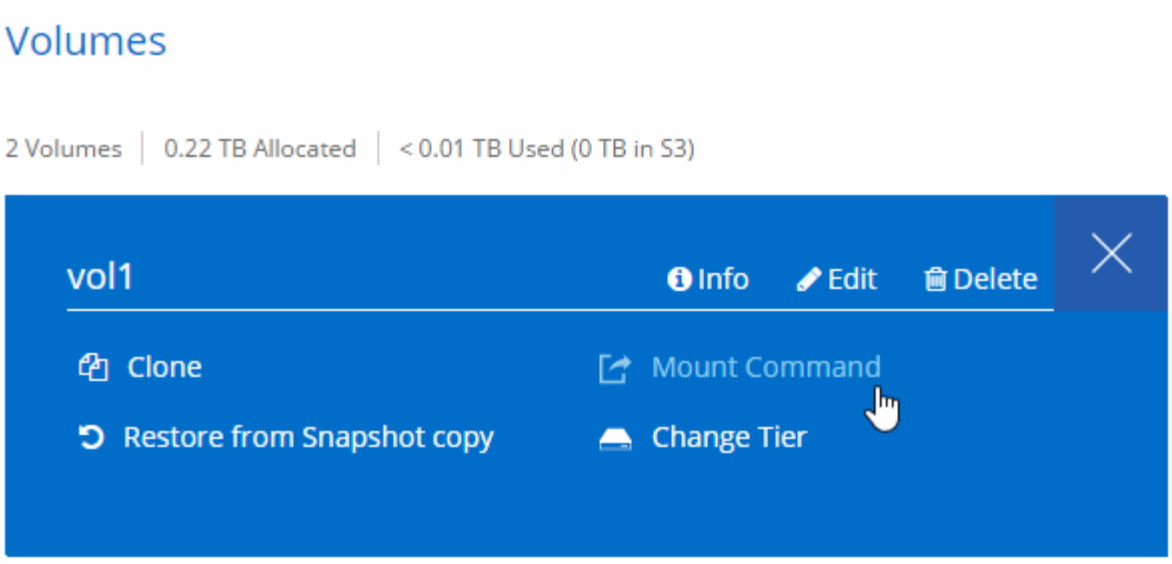
Para obtener más información sobre el rendimiento de Cloud Volumes ONTAP, consulte "Rendimiento".

Acceso de clientes al almacenamiento

Los clientes deben acceder a los volúmenes NFS y CIFS mediante la dirección IP de datos del nodo en el que reside el volumen. Si los clientes NAS acceden a un volumen utilizando la dirección IP del nodo del partner, el tráfico se dirige entre ambos nodos, lo que reduce el rendimiento.

Si mueve un volumen entre nodos de una pareja de ha, debe volver a montar el volumen con la dirección IP del otro nodo. De lo contrario, puede experimentar un rendimiento reducido. Si los clientes admiten las referencias de NFSv4 o la redirección de carpetas para CIFS, puede activar estas funciones en los sistemas de Cloud Volumes ONTAP para evitar el remontaje del volumen. Para obtener más detalles, consulte la documentación de ONTAP.

Puede identificar fácilmente la dirección IP correcta desde Cloud Manager:

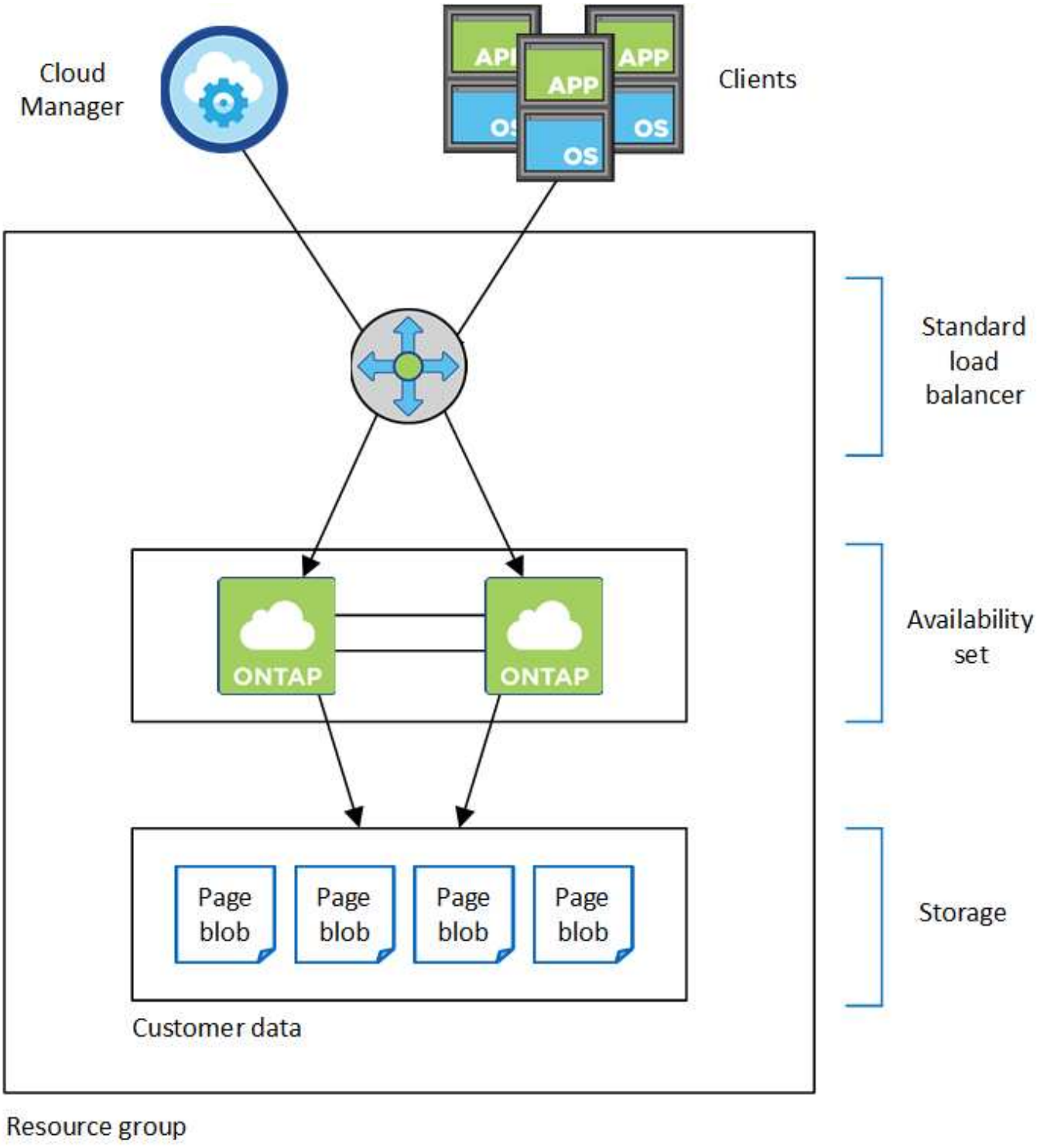


Pares de alta disponibilidad en Azure

Una pareja de alta disponibilidad (ha) Cloud Volumes ONTAP proporciona fiabilidad empresarial y operaciones continuas en caso de fallos en su entorno de cloud. En Azure, el almacenamiento se comparte entre los dos nodos.

Componentes DE ALTA DISPONIBILIDAD

Una configuración de alta disponibilidad de Cloud Volumes ONTAP en Azure incluye los siguientes componentes:



Tenga en cuenta lo siguiente acerca de los componentes de Azure que Cloud Manager pone en marcha para usted:

Equilibrador de carga estándar de Azure

El equilibrador de carga gestiona el tráfico entrante en el par ha de Cloud Volumes ONTAP.

Conjunto de disponibilidad

El conjunto de disponibilidad garantiza que los nodos se encuentren en diferentes dominios de actualización y fallo.

Discos

Los datos del cliente residen en Blobs de la página de Premium Storage. Cada nodo tiene acceso al almacenamiento del otro nodo. También se requiere almacenamiento adicional para "datos sobre el arranque, la raíz y el núcleo".

Cuentas de almacenamiento

- Se necesita una cuenta de almacenamiento para los discos gestionados.
- Se requieren una o más cuentas de almacenamiento para los BLOB de la página Premium Storage, ya que se alcanza el límite de capacidad de disco por cuenta de almacenamiento.

  "Documentación de Azure: Objetivos de escalabilidad y rendimiento de Azure Storage para cuentas de almacenamiento".

- Se necesita una cuenta de almacenamiento para la organización en niveles de los datos en el almacenamiento de Azure Blob.
- A partir de Cloud Volumes ONTAP 9.7, las cuentas de almacenamiento que crea Cloud Manager para los pares de alta disponibilidad son cuentas de almacenamiento de versión 2 generales.
- Puede habilitar una conexión HTTPS de una pareja de ha Cloud Volumes ONTAP 9.7 a cuentas de almacenamiento Azure al crear un entorno de trabajo. Tenga en cuenta que al habilitar esta opción, el rendimiento de escritura puede afectar. No se puede cambiar la configuración después de crear el entorno de trabajo.

RPO y RTO

Una configuración de alta disponibilidad mantiene una alta disponibilidad de los datos de la siguiente manera:

- El objetivo de punto de recuperación (RPO) es 0 segundos. Sus datos son coherentes transcionalmente sin pérdida de datos.
- El objetivo de tiempo de recuperación (RTO) es de 60 segundos. En el caso de que se produzca una interrupción del servicio, los datos deben estar disponibles en 60 segundos o menos.

Toma de control y retorno al nodo primario del almacenamiento

De forma similar a un clúster de ONTAP físico, el almacenamiento en un par de alta disponibilidad de Azure se comparte entre los nodos. Las conexiones con el almacenamiento del partner permiten a cada nodo acceder al almacenamiento del otro en caso de que se produzca un *takeover*. Los mecanismos de conmutación al nodo de respaldo de ruta de red garantizan que los clientes y los hosts sigan comunicarse con el nodo superviviente. El partner *devuelve* el almacenamiento cuando el nodo vuelve a estar online.

En el caso de configuraciones NAS, las direcciones IP de datos migran automáticamente entre nodos de alta disponibilidad si se dan fallos.

Para iSCSI, Cloud Volumes ONTAP utiliza I/o multivía (MPIO) y ALUA (Asymmetric Logical Unit Access) para gestionar la conmutación por error de ruta entre las rutas activas y no optimizadas.

Para obtener información sobre qué configuraciones de host específicas admiten ALUA, consulte "Herramienta de matriz de interoperabilidad de NetApp" Y la guía de instalación y configuración de las utilidades de host para el sistema operativo host.

Configuraciones de almacenamiento

Puede utilizar un par de alta disponibilidad como configuración activo-activo, en el cual ambos nodos sirven

datos a los clientes o como una configuración activo-pasivo, en la cual el nodo pasivo responde a las solicitudes de datos únicamente si ha tomado almacenamiento para el nodo activo.

Limitaciones de ALTA DISPONIBILIDAD

Las siguientes limitaciones afectan a las parejas de alta disponibilidad de Cloud Volumes ONTAP en Azure:

- Los pares de ALTA DISPONIBILIDAD son compatibles con Cloud Volumes ONTAP Standard, Premium y BYOL. No se admite la exploración.
- NFSv4 no es compatible. NFSv3 es compatible.
- En algunas regiones no se admiten pares DE HA.

  "Consulte la lista de regiones de Azure admitidas".

"Descubra cómo implementar un sistema de alta disponibilidad en Azure".

Evaluación

Puede evaluar Cloud Volumes ONTAP antes de pagar por el software. La forma más común es lanzar la versión de PAYGO de su primer sistema Cloud Volumes ONTAP para obtener una prueba gratuita de 30 días. Una licencia BYOL de evaluación es también una opción.

Si necesita ayuda con su prueba de concepto, póngase en contacto con "El equipo de ventas" o póngase en contacto con la opción de chat disponible en "Cloud Central de NetApp" Y desde dentro de Cloud Manager.

Pruebas gratuitas de 30 días para PAYGO

Hay disponible una prueba gratuita de 30 días si planea pagar por Cloud Volumes ONTAP mientras usa. Puede iniciar una prueba gratuita de 30 días de Cloud Volumes ONTAP desde Cloud Manager creando el primer sistema Cloud Volumes ONTAP en la cuenta de un pagador.

Para la instancia no se cobran horas de licencia de software, pero siguen siendo aplicables los costes de infraestructura del proveedor de cloud.

Una prueba gratuita se convierte automáticamente en una suscripción por hora de pago cuando expira. Si termina la instancia dentro del límite de tiempo, la siguiente instancia que implemente no forma parte de la prueba gratuita (aunque se despliegue dentro de esos 30 días).

Las pruebas de pago por uso se otorgan a través de un proveedor de cloud y no se pueden utilizar por ningún medio.

Licencias de evaluación para BYOL

Una licencia BYOL de evaluación es una opción para los clientes que esperan pagar por Cloud Volumes ONTAP comprando una licencia llamada de NetApp. Puede obtener una licencia de evaluación de su equipo de cuentas, de su ingeniero de ventas o de su partner.

La clave de evaluación es válida durante 30 días y puede usarse varias veces, cada una durante 30 días (independientemente del día de creación).

Al final de los 30 días, se producirán apagados diarios, por lo que es mejor planificar con antelación. Puede aplicar una nueva licencia BYOL sobre la licencia de evaluación para una actualización in situ (esto requiere el

reinicio de los sistemas de un solo nodo). Los datos alojados se eliminan **no** al final del período de prueba.

No se puede actualizar el software de Cloud Volumes ONTAP cuando se usa una licencia de evaluación.

Licencia

Cada sistema BYOL de Cloud Volumes ONTAP debe tener una licencia del sistema instalada con una suscripción activa. Cloud Manager simplifica el proceso al gestionar las licencias para usted y notificar antes de que caduquen. Las licencias BYOL también están disponibles para backup en el cloud.

Licencias de sistema BYOL

Puede comprar varias licencias para un sistema BYOL de Cloud Volumes ONTAP con el fin de asignar más de 368 TB de capacidad. Por ejemplo, puede adquirir dos licencias para asignar hasta 736 TB de capacidad a Cloud Volumes ONTAP. O bien podría comprar cuatro licencias para obtener hasta 1.4 PB.

El número de licencias que se pueden comprar para un único sistema de nodo o par de alta disponibilidad es ilimitado.

Tenga en cuenta que los límites de disco pueden impedir que llegue al límite de capacidad utilizando solo discos. Puede superar el límite de discos mediante "organización en niveles de los datos inactivos en el almacenamiento de objetos". Para obtener más información acerca de los límites de disco, consulte "Límites de almacenamiento en las notas de la versión de Cloud Volumes ONTAP".

Gestión de licencias para un nuevo sistema

Cuando crea un sistema BYOL, Cloud Manager le solicita el número de serie de la licencia y su cuenta del sitio de soporte de NetApp. Cloud Manager utiliza la cuenta para descargar el archivo de licencia de NetApp e instalarlo en el sistema Cloud Volumes ONTAP.

"Aprenda a añadir cuentas del sitio de soporte de NetApp a cloud Gerente".

Si Cloud Manager no puede acceder al archivo de licencia a través de la conexión segura a Internet, puede obtener el archivo usted mismo y, a continuación, cargarlo manualmente en Cloud Manager. Para ver instrucciones, consulte "Gestión de licencias BYOL para Cloud Volumes ONTAP".

Aviso de caducidad de la licencia

Cloud Manager le advierte de 30 días antes de que caduque una licencia para volver a expirar la licencia. La siguiente imagen muestra una advertencia de caducidad de 30 días:

Puede seleccionar el entorno de trabajo para revisar el mensaje.

Si no renueva la licencia a tiempo, el sistema Cloud Volumes ONTAP se apaga automáticamente. Si lo reinicia, se apaga de nuevo.

> Cloud Volumes ONTAP también es posible notificar por correo electrónico, un host de capturas de SNMP o un servidor de syslog mediante las notificaciones de eventos de EMS (Event Management System). Para ver instrucciones, consulte "Guía exprés de configuración de EMS de ONTAP 9".

Renovación de la licencia

Cuando renueve una suscripción de BYOL con un representante de NetApp, Cloud Manager obtiene automáticamente la nueva licencia de NetApp y la instala en el sistema Cloud Volumes ONTAP.

Si Cloud Manager no puede acceder al archivo de licencia a través de la conexión segura a Internet, puede obtener el archivo usted mismo y, a continuación, cargarlo manualmente en Cloud Manager. Para ver instrucciones, consulte "Gestión de licencias BYOL para Cloud Volumes ONTAP".

Licencias de backup BYOL

Una licencia de backup BYOL le permite comprar una licencia de NetApp para usar Backup en cloud por un periodo determinado de tiempo y por una cantidad máxima de espacio de backup. Cuando se alcance cualquiera de los límites, deberá renovar la licencia.

"Obtenga más información acerca de la licencia BYOL de backup en cloud".

Seguridad

Cloud Volumes ONTAP admite el cifrado de datos y proporciona protección contra virus y ransomware.

Cifrado de datos en reposo

Cloud Volumes ONTAP admite las siguientes tecnologías de cifrado:

- Soluciones de cifrado de NetApp (NVE y NAE)
- Servicio de gestión de claves de AWS
- Cifrado del servicio de almacenamiento de Azure
- Cifrado predeterminado de la plataforma Google Cloud

Puede utilizar las soluciones de cifrado de NetApp con el cifrado nativo de AWS, Azure o GCP, que cifran datos a nivel de hipervisor. De esta manera, se proporcionaría un cifrado doble, que puede resultar deseable para datos muy confidenciales. Cuando se accede a los datos cifrados, se descifra dos veces: Una a nivel de hipervisor (mediante claves del proveedor de cloud) y, a continuación, se utilizan de nuevo soluciones de cifrado de NetApp (mediante claves de un gestor de claves externo).

Soluciones de cifrado de NetApp (NVE y NAE)

Cloud Volumes ONTAP es compatible tanto con el cifrado de volúmenes de NetApp (NVE) como con el cifrado de agregados de NetApp (NAE) con un gestor de claves externo. NVE y NAE son soluciones basadas en software que permiten (FIPS) cifrado de volúmenes para datos en reposo conforme a la normativa 140-2.

- NVE cifra los datos en reposo un volumen por vez. Cada volumen de datos tiene su propia clave de

cifrado única.

- NAE es una extensión de NVE: Cifra los datos para cada volumen y los volúmenes comparten una clave en todo el agregado. NAE también permite deduplicar bloques comunes en todos los volúmenes del agregado.

Tanto NVE como NAE utilizan el cifrado AES de 256 bits.

"Obtenga más información sobre el cifrado de volumen de NetApp y el cifrado de agregados de NetApp".

A partir de Cloud Volumes ONTAP 9.7, los nuevos agregados tendrán el cifrado de agregados de NetApp (NAE) habilitado de forma predeterminada tras la configuración de un gestor de claves externo. Los volúmenes nuevos que no forman parte de un agregado de NAE tendrán habilitado el cifrado de volúmenes de NetApp (NVE) de forma predeterminada (por ejemplo, si tiene agregados existentes que se crearon antes de configurar un gestor de claves externo).

La configuración de un gestor de claves compatible es el único paso necesario. Para obtener instrucciones de configuración, consulte "Cifrar volúmenes con soluciones de cifrado de NetApp".

Servicio de gestión de claves de AWS

Cuando inicia un sistema Cloud Volumes ONTAP en AWS, puede habilitar el cifrado de datos mediante el "Servicio de gestión de claves AWS (KMS)". Cloud Manager solicita claves de datos mediante una clave maestra de cliente (CMK).

No puede cambiar el método de cifrado de datos de AWS después de crear un sistema Cloud Volumes ONTAP.

Si desea usar esta opción de cifrado, debe asegurarse de que el KMS de AWS esté configurado adecuadamente. Para obtener más información, consulte "Configuración de AWS KMS".

Cifrado del servicio de almacenamiento de Azure

"Cifrado del servicio de almacenamiento de Azure" Para los datos en reposo está habilitado de forma predeterminada para los datos de Cloud Volumes ONTAP en Azure. No se requiere configuración.

Puede cifrar discos gestionados de Azure en sistemas Cloud Volumes ONTAP de un solo nodo mediante claves externas de otra cuenta. Esta función es compatible con las API de Cloud Manager.

Solo tiene que agregar lo siguiente a la solicitud API cuando crea el sistema de un solo nodo:

```
"azureEncryptionParameters": {
      "key": <azure id of encryptionset>
  }
```

Las claves gestionadas por el cliente no son compatibles con los pares de alta disponibilidad Cloud Volumes ONTAP.

Cifrado predeterminado de la plataforma Google Cloud

"Cifrado de datos en reposo de la plataforma Google Cloud" Está habilitado de forma predeterminada para Cloud Volumes ONTAP. No se requiere configuración.

Mientras Google Cloud Storage siempre cifra sus datos antes de escribirlos en el disco, podrá utilizar las API de Cloud Manager para crear un sistema de Cloud Volumes ONTAP que utilice *claves de cifrado gestionadas por el cliente*. Estas son claves que genera y gestiona en GCP mediante el servicio Cloud Key Management Service. "Leer más".

Detección de virus de ONTAP

Puede utilizar la funcionalidad antivirus integrada en los sistemas ONTAP para proteger los datos frente a amenazas de virus u otro código malintencionado.

El análisis de virus de ONTAP, denominado *Vscan*, combina el mejor software antivirus de terceros con funciones de ONTAP que le proporcionan la flexibilidad que necesita para controlar qué archivos se analizan y cuándo.

Para obtener información acerca de los proveedores, software y versiones compatibles con Vscan, consulte "Matriz de interoperabilidad de NetApp".

Para obtener información acerca de cómo configurar y administrar la funcionalidad antivirus en los sistemas ONTAP, consulte "Guía de configuración de antivirus de ONTAP 9".

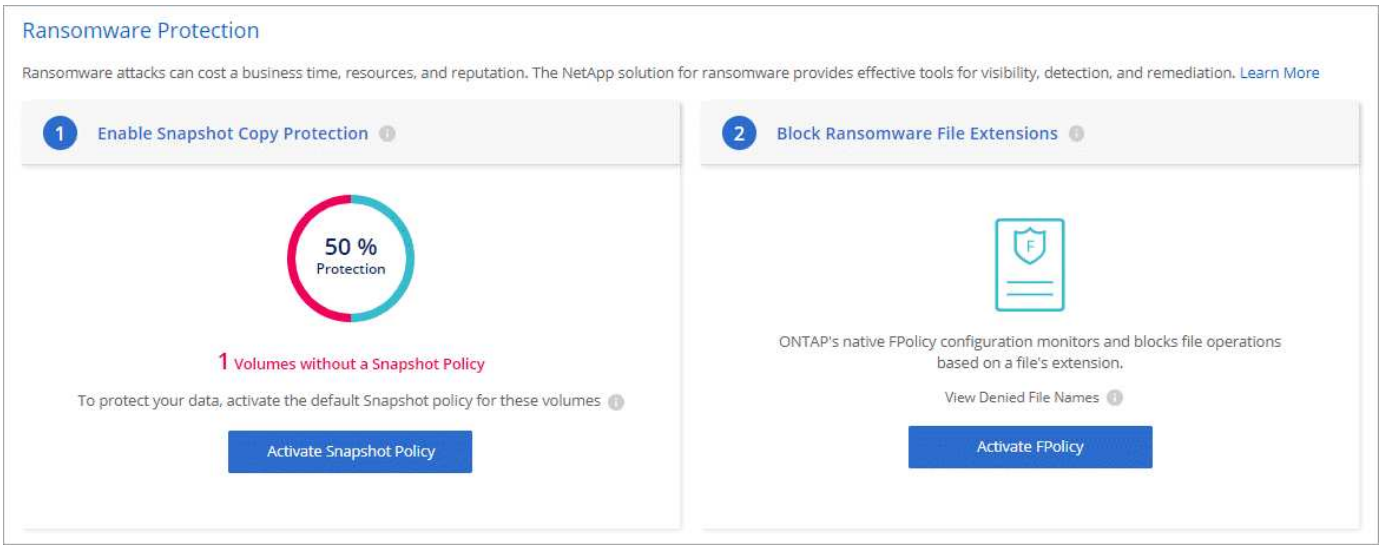
Protección contra ransomware

Los ataques de ransomware pueden suponer un coste comercial, recursos y reputación. Cloud Manager le ayuda a implementar la solución de NetApp para el ransomware, que proporciona herramientas eficaces para la visibilidad, la detección y la corrección.

- Cloud Manager identifica los volúmenes que no están protegidos por una política de Snapshot y le permite activar la política de Snapshot predeterminada en esos volúmenes.

  Las copias Snapshot son de solo lectura, lo que evita que se dañen el ransomware. También pueden proporcionar granularidad para crear imágenes de una sola copia de archivos o una solución completa de recuperación tras desastres.

- Cloud Manager también le permite bloquear extensiones de archivos ransomware comunes mediante la solución FPolicy de ONTAP.



"Aprenda a implementar la solución de NetApp para ransomware".

Rendimiento

Es posible revisar los resultados de rendimiento con el fin de ayudarle a decidir qué cargas de trabajo son las adecuadas para Cloud Volumes ONTAP.

- Cloud Volumes ONTAP para AWS

  "Informe técnico de NetApp 4383: Caracterización del rendimiento de Cloud Volumes ONTAP en Amazon Web Services con cargas de trabajo de las aplicaciones".

- Cloud Volumes ONTAP para Microsoft Azure

  "Informe técnico de NetApp 4671: Caracterización del rendimiento de Cloud Volumes ONTAP en Azure con cargas de trabajo de aplicaciones".

- Cloud Volumes ONTAP para Google Cloud

  "Informe técnico de NetApp 4816: Caracterización del rendimiento de Cloud Volumes ONTAP para Google Cloud".

Configuración predeterminada de Cloud Volumes ONTAP

Comprender cómo se configura Cloud Volumes ONTAP de forma predeterminada puede ayudarle a configurar y administrar los sistemas, especialmente si está familiarizado con ONTAP porque la configuración predeterminada para Cloud Volumes ONTAP es diferente de ONTAP.

Valores predeterminados

- Cloud Volumes ONTAP está disponible como un sistema de un solo nodo en AWS, Azure y GCP, así como como una pareja de alta disponibilidad en AWS y Azure.
- Cloud Manager crea una máquina virtual de almacenamiento que sirve datos cuando pone en marcha Cloud Volumes ONTAP. Algunas configuraciones admiten máquinas virtuales de almacenamiento adicionales. "Obtenga más información sobre la gestión de máquinas virtuales de almacenamiento".
- Cloud Manager instala automáticamente las siguientes licencias de funciones de ONTAP en Cloud Volumes ONTAP:
  - CIFS
  - FlexCache
  - FlexClone
  - ISCSI
  - Cifrado de volúmenes de NetApp (solo para sistemas BYOL o registrados de PAYGO)
  - NFS
  - SnapMirror
  - SnapRestore
  - SnapVault
- De forma predeterminada, se crean varias interfaces de red:

- Una LIF de gestión de clústeres
- Una LIF de interconexión de clústeres
- Una LIF de gestión SVM en sistemas de alta disponibilidad en Azure, sistemas de un solo nodo en AWS y, opcionalmente, en sistemas de alta disponibilidad en varias zonas de disponibilidad de AWS
- Una LIF de gestión de nodos
- Una LIF de datos iSCSI
- Un LIF de datos CIFS y NFS

> La conmutación por error de LIF está deshabilitada de forma predeterminada para Cloud Volumes ONTAP debido a los requisitos de EC2. Al migrar una LIF a otro puerto, se interrumpe la asignación externa entre direcciones IP e interfaces de red en la instancia, lo que hace que la LIF no sea accesible.

- Cloud Volumes ONTAP envía backups de configuración al conector mediante HTTPS.

  Se puede acceder a los backups desde https://ipaddress/occm/offboxconfig/ Donde *ipaddress* es la dirección IP del host del conector.

- Cloud Manager establece algunos atributos de volumen de manera diferente a los de otras herramientas de gestión (por ejemplo, System Manager o la CLI).

  En la siguiente tabla, se enumeran los atributos de volúmenes que Cloud Manager establece de manera diferente a los valores predeterminados:

Atributo	Valor definido por Cloud Manager
Modo de ajuste automático de tamaño	crezca
tamaño automático máximo	1,000 por ciento El administrador de cuentas puede modificar este valor en la página Configuración.
Estilo de seguridad	NTFS para volúmenes CIFS UNIX para volúmenes NFS
Estilo de garantía de espacio	ninguno
Permisos de UNIX (solo NFS)	777

  Consulte la página del comando man *volume create* para obtener información sobre estos atributos.

Datos raíz y de arranque para Cloud Volumes ONTAP

Además del almacenamiento de los datos de usuario, Cloud Manager también adquiere almacenamiento en cloud para el arranque y los datos raíz en cada sistema Cloud Volumes ONTAP.

AWS

- Dos discos por nodo para arranque y datos raíz:
  - 9.7: Disco io1 de 160 GB para datos de arranque y un disco gp2 de 220 GB para datos raíz
  - 9.6: Disco io1 de 93 GB para datos de arranque y un disco gp2 de 140 GB para datos raíz
  - 9.5: Disco io1 de 45 GB para datos de arranque y un disco gp2 de 140 GB para datos raíz
- Una instantánea de EBS para cada disco de arranque y disco raíz
- Para los pares de alta disponibilidad, un volumen de EBS para la instancia de Mediator, que es aproximadamente 8 GB

Azure (nodo único)

- Tres discos SSD premium:
  - Un disco de 10 GB para los datos de arranque
  - Un disco de 140 GB para datos raíz
  - Un disco de 128 GB para NVRAM

    Si la máquina virtual elegida para Cloud Volumes ONTAP admite Ultra SSD, el sistema utiliza un Ultra SSD para NVRAM, en lugar de un SSD Premium.
- Un disco duro estándar de 1024 GB para ahorrar núcleos
- Una instantánea de Azure para cada disco de arranque y disco raíz

Azure (parejas de alta disponibilidad)

- Dos discos SSD Premium de 10 GB para el volumen de arranque (uno por nodo)
- Dos Blobs de página de almacenamiento Premium de 140 GB para la raíz volumen (uno por nodo)
- Dos discos HDD estándar de 1024 GB para ahorrar núcleos (uno por nodo)
- Dos discos SSD Premium de 128 GB para NVRAM (uno por nodo)
- Una instantánea de Azure para cada disco de arranque y disco raíz

GCP

- Un disco persistente estándar de 10 GB para datos de arranque
- Un disco persistente estándar de 64 GB para datos raíz
- Un disco persistente estándar de 500 GB para NVRAM
- Un disco persistente estándar de 216 GB para ahorrar núcleos
- Una instantánea de GCP para el disco de arranque y la raíz disco

La ubicación de los discos

Cloud Manager establece el almacenamiento de la siguiente manera:

- Los datos de arranque residen en un disco asociado a la instancia o a la máquina virtual.

  Este disco, que contiene la imagen de arranque, no está disponible para Cloud Volumes ONTAP.

- Los datos raíz, que contienen la configuración y los registros del sistema, residen en aggr0.
- El volumen raíz de la máquina virtual de almacenamiento (SVM) reside en aggr1.
- Los volúmenes de datos también residen en aggr1.

Cifrado

Los discos de arranque y raíz siempre se cifran en Azure y Google Cloud Platform, ya que el cifrado está habilitado de forma predeterminada en esos proveedores de cloud.

Cuando habilita el cifrado de datos en AWS mediante el Servicio de gestión de claves (KMS), los discos de arranque y raíz para Cloud Volumes ONTAP también se cifran. Esto incluye el disco de arranque para la instancia del mediador en una pareja de alta disponibilidad. Los discos se cifran utilizando el CMK que seleccione al crear el entorno de trabajo.

Empiece a usar AWS

Introducción a Cloud Volumes ONTAP para AWS

Empiece a usar Cloud Volumes ONTAP para AWS en unos pasos.

Cree un conector

Si usted no tiene un "Conector" Sin embargo, un administrador de cuentas necesita crear uno. "Aprenda a crear un conector en AWS".

Al crear el primer entorno de trabajo de Cloud Volumes ONTAP, Cloud Manager le solicitará que implemente un conector si aún no lo tiene.

Planificación de la configuración

Cloud Manager ofrece paquetes preconfigurados que se ajustan a sus requisitos de carga de trabajo, o bien puede crear su propia configuración. Si elige su propia configuración, debe conocer las opciones disponibles. "Leer más".

Configure su red

1. Asegúrese de que VPC y las subredes admitan la conectividad entre el conector y Cloud Volumes ONTAP.
2. Habilite el acceso a Internet de salida desde el VPC de destino para que el conector y Cloud Volumes ONTAP puedan ponerse en contacto con varios extremos.

   Este paso es importante porque el conector no puede administrar Cloud Volumes ONTAP sin acceso saliente a Internet. Si necesita limitar la conectividad saliente, consulte la lista de puntos finales para "El conector y Cloud Volumes ONTAP".

3. Configure un extremo de VPC con el servicio S3.

   Se requiere un extremo de VPC si desea organizar en niveles los datos inactivos de Cloud Volumes ONTAP en el almacenamiento de objetos de bajo coste.

"Obtenga más información sobre los requisitos de red".

Configure el KMS de AWS

Si desea utilizar el cifrado de Amazon con Cloud Volumes ONTAP, debe asegurarse de que existe una clave maestra de cliente (CMK) activa. También debe modificar la política de claves para cada CMK agregando la función IAM que proporciona permisos al conector como *Key user*. "Leer más".

Inicie Cloud Volumes ONTAP mediante Cloud Manager

Haga clic en **Agregar entorno de trabajo**, seleccione el tipo de sistema que desea implementar y complete los pasos del asistente. "Lea las instrucciones paso a paso".

Enlaces relacionados

- "Evaluación"
- "Creación de un conector desde Cloud Manager"
- "Inicio de un conector desde AWS Marketplace"
- "Instalar el software del conector en un host Linux"
- "Qué hace Cloud Manager con los permisos de AWS"

Planificar la configuración de Cloud Volumes ONTAP en AWS

Al poner en marcha Cloud Volumes ONTAP en AWS, puede elegir un sistema preconfigurado que se ajuste a los requisitos de la carga de trabajo, o bien puede crear su propia configuración. Si elige su propia configuración, debe conocer las opciones disponibles.

Seleccione un tipo de licencia

Cloud Volumes ONTAP está disponible en dos opciones de precios: De pago por uso y con su propia licencia (BYOL). En el modelo de pago por uso, puede elegir entre tres licencias: Explorar, Standard o Premium. Cada licencia proporciona distintas opciones de computación y capacidad.

"Configuraciones compatibles para Cloud Volumes ONTAP 9.7 en AWS"

Comprender los límites de almacenamiento

El límite de capacidad bruta de un sistema de Cloud Volumes ONTAP está relacionado con la licencia. Los límites adicionales afectan al tamaño de los agregados y los volúmenes. Debe conocer estos límites a medida que planifique la configuración.

"Límites de almacenamiento para Cloud Volumes ONTAP 9.7 en AWS"

Ajuste de tamaño de su sistema en AWS

Configurar el tamaño de su sistema Cloud Volumes ONTAP puede ayudarle a cumplir los requisitos de rendimiento y capacidad. Al elegir un tipo de instancia, tipo de disco y tamaño de disco, debe tener en cuenta algunos puntos clave:

Tipo de instancia

- Relacione los requisitos de carga de trabajo con el rendimiento máximo y las IOPS para cada tipo de instancia de EC2.
- Si varios usuarios escriben en el sistema al mismo tiempo, elija un tipo de instancia que tenga suficientes CPU para administrar las solicitudes.
- Si tiene una aplicación que está mayormente en lectura, elija un sistema con suficiente RAM.
  - "Documentación de AWS: Tipos de instancias de Amazon EC2"
  - "Documentación de AWS: Instancias optimizadas para Amazon EBS"

Tipo de disco de EBS

Los SSD de uso general son el tipo de disco más común para Cloud Volumes ONTAP. Para ver los casos de uso de discos EBS, consulte "Documentación de AWS: Tipos de volúmenes de EBS".

Tamaño del disco de EBS

Es necesario seleccionar un tamaño de disco inicial al iniciar un sistema Cloud Volumes ONTAP. Después de eso, usted puede "Permita que Cloud Manager gestione la capacidad de un sistema por usted", pero si lo desea "cree agregados usted mismo", tenga en cuenta lo siguiente:

- Todos los discos de un agregado deben tener el mismo tamaño.
- El rendimiento de los discos EBS está relacionado con el tamaño del disco. El tamaño determina la tasa de IOPS de base y la duración máxima de ráfaga para discos SSD, así como el rendimiento de línea base y de ráfaga para discos HDD.
- En última instancia, debe elegir el tamaño del disco que le proporcione el *rendimiento sostenido* que necesita.
- Aunque se elijan discos más grandes (por ejemplo, seis discos de 4 TB), es posible que no se obtengan todas las IOPS porque la instancia de EC2 puede alcanzar su límite de ancho de banda.

  Para obtener más información sobre el rendimiento del disco EBS, consulte "Documentación de AWS: Tipos de volúmenes de EBS".

Consulte el siguiente vídeo para obtener más información acerca de cómo ajustar el tamaño de su sistema Cloud Volumes ONTAP en AWS:

[] | *https://img.youtube.com/vi/GELcXmOuYPw/maxresdefault.jpg*

Elegir una configuración compatible con Flash Cache

Algunas configuraciones de Cloud Volumes ONTAP en AWS incluyen almacenamiento NVMe local, que Cloud Volumes ONTAP utiliza como *Flash Cache* para mejorar el rendimiento. "Obtenga más información sobre Flash Cache".

Hoja de trabajo de información de red de AWS

Al iniciar Cloud Volumes ONTAP en AWS, tiene que especificar detalles acerca de la red VPC. Puede utilizar una hoja de cálculo para recopilar la información del administrador.

Información de red para Cloud Volumes ONTAP

Información de AWS	Su valor
Región	
VPC	
Subred	
Grupo de seguridad (si utiliza el suyo propio)	

Información de red para un par de alta disponibilidad en varios AZs

Información de AWS	Su valor
Región	
VPC	
Grupo de seguridad (si utiliza el suyo propio)	
Nodo 1 zona de disponibilidad	
Subred nodo 1	
Zona de disponibilidad del nodo 2	
Subred nodo 2	
Zona de disponibilidad del mediador	
Subred del mediador	
Par clave para el mediador	
Dirección IP flotante para el puerto de gestión del clúster	
Dirección IP flotante para datos en el nodo 1	
Dirección IP flotante para datos en el nodo 2	
Tablas de rutas para direcciones IP flotantes	

Elegir una velocidad de escritura

Cloud Manager le permite elegir una configuración de velocidad de escritura para sistemas Cloud Volumes ONTAP de un solo nodo. Antes de elegir una velocidad de escritura, debe comprender las diferencias entre la configuración normal y la alta, así como los riesgos y recomendaciones cuando utilice la alta velocidad de escritura.

Diferencia entre la velocidad de escritura normal y la alta velocidad de escritura

Al elegir la velocidad de escritura normal, los datos se escriben directamente en el disco, lo que reduce la probabilidad de que se pierdan los datos en caso de que se produzca una interrupción del servicio no planificada del sistema.

Al elegir una alta velocidad de escritura, los datos se guardan en búfer en la memoria antes de que se escriban en el disco, lo que proporciona un rendimiento de escritura más rápido. Gracias al almacenamiento en caché, existe la posibilidad de perder datos en caso de que se produzca una interrupción no planificada del sistema.

La cantidad de datos que se pueden perder en caso de una interrupción imprevista del sistema es el plazo de dos últimos puntos de coherencia. Un punto de coherencia es el acto de escribir datos en el búfer en el disco. Un punto de coherencia se produce cuando el registro de escritura está completo o después de 10 segundos (lo que ocurra primero). Sin embargo, el rendimiento del volumen de AWS EBS puede afectar el tiempo de procesamiento del punto de consistencia.

Cuándo utilizar alta velocidad de escritura

La alta velocidad de escritura es una buena opción si es necesario un rendimiento de escritura rápido para su carga de trabajo, y puede resistir el riesgo de pérdida de datos en caso de una interrupción del servicio del sistema no planificada.

Recomendaciones cuando se utiliza una alta velocidad de escritura

Si habilita una alta velocidad de escritura, debe garantizar la protección de escritura en la capa de la aplicación.

Selección de un perfil de uso de volumen

ONTAP incluye varias funciones de eficiencia del almacenamiento que pueden reducir la cantidad total de almacenamiento que necesita. Al crear un volumen en Cloud Manager, puede seleccionar un perfil que habilite estas funciones o un perfil que las deshabilite. Debe obtener más información sobre estas funciones para ayudarle a decidir qué perfil utilizar.

Las funciones de eficiencia del almacenamiento de NetApp ofrecen las siguientes ventajas:

Aprovisionamiento ligero
: Presenta más almacenamiento lógico a hosts o usuarios del que realmente hay en el pool de almacenamiento físico. En lugar de asignar previamente espacio de almacenamiento, el espacio de almacenamiento se asigna de forma dinámica a cada volumen a medida que se escriben los datos.

Deduplicación
: Mejora la eficiencia al localizar bloques de datos idénticos y sustituirlos con referencias a un único bloque compartido. Esta técnica reduce los requisitos de capacidad de almacenamiento al eliminar los bloques de datos redundantes que se encuentran en un mismo volumen.

Compresión
: Reduce la capacidad física requerida para almacenar datos al comprimir los datos de un volumen en almacenamiento primario, secundario y de archivado.

Configure su red

Requisitos de red para Cloud Volumes ONTAP en AWS

Configurar las redes de AWS para que los sistemas Cloud Volumes ONTAP funcionen correctamente.

Requisitos generales para Cloud Volumes ONTAP

Los siguientes requisitos deben satisfacerse en AWS.

Acceso a Internet saliente para nodos Cloud Volumes ONTAP

Los nodos Cloud Volumes ONTAP requieren acceso saliente a Internet para enviar mensajes a NetApp AutoSupport, que supervisa proactivamente el estado del almacenamiento.

Las políticas de enrutamiento y firewall deben permitir el tráfico HTTP/HTTPS de AWS a los siguientes extremos para que Cloud Volumes ONTAP pueda enviar mensajes de AutoSupport:

- https://support.netapp.com/aods/asupmessage
- https://support.netapp.com/asupprod/post/1.0/postAsup

  Si tiene una instancia NAT, debe definir una regla de grupo de seguridad entrante que permita el tráfico HTTPS desde la subred privada hasta Internet.

  "Aprenda a configurar AutoSupport".

Acceso saliente a Internet para el mediador de alta disponibilidad

La instancia del mediador de alta disponibilidad debe tener una conexión saliente al servicio EC2 de AWS para que pueda ayudar a recuperarse de la recuperación tras fallos del almacenamiento. Para proporcionar la conexión, puede agregar una dirección IP pública, especificar un servidor proxy o utilizar una opción manual.

La opción manual puede ser una puerta de enlace NAT o un extremo de la interfaz VPC desde la subred de destino al servicio AWS EC2. Para obtener más detalles sobre los extremos VPC, consulte "Documentación de AWS: Extremos de VPC de la interfaz (AWS PrivateLink)".

Número de direcciones IP

Cloud Manager asigna el siguiente número de direcciones IP a Cloud Volumes ONTAP en AWS:

- Nodo único: Direcciones IP de 6
- Pares DE ALTA DISPONIBILIDAD en AZs individuales: 15 direcciones
- Pares DE ALTA DISPONIBILIDAD en varios AZs: Direcciones IP 15 o 16

  Tenga en cuenta que Cloud Manager crea un LIF de gestión de SVM en sistemas de un solo nodo, pero no en pares de alta disponibilidad en una única zona de disponibilidad. Puede elegir si desea crear una LIF de gestión de SVM en parejas de alta disponibilidad en múltiples AZs.

  Una LIF es una dirección IP asociada con un puerto físico. Se requiere una LIF de gestión de SVM para herramientas de gestión como SnapCenter.

Grupos de seguridad

No necesita crear grupos de seguridad porque Cloud Manager lo hace por usted. Si necesita utilizar el suyo propio, consulte "Reglas de grupo de seguridad".

Conexión de Cloud Volumes ONTAP a AWS S3 para los datos organización en niveles

Si desea usar EBS como nivel de rendimiento y AWS S3 como nivel de capacidad, debe asegurarse de que Cloud Volumes ONTAP tenga una conexión con S3. La mejor forma de proporcionar esa conexión es crear un extremo de VPC con el servicio S3. Para ver instrucciones, consulte "Documentación de AWS: Crear un extremo de puerta de enlace".

Al crear el extremo VPC, asegúrese de seleccionar la región, VPC y tabla de rutas que correspondan a la instancia de Cloud Volumes ONTAP. También debe modificar el grupo de seguridad para añadir una regla de HTTPS de salida que habilite el tráfico hacia el extremo de S3. De lo contrario, Cloud Volumes ONTAP no puede conectarse con el servicio S3.

Si experimenta algún problema, consulte "Centro de conocimientos de soporte de AWS: ¿por qué no puedo conectarme a un bloque de S3 mediante un extremo de VPC de puerta de enlace?"

Conexiones a sistemas ONTAP en otras redes

Para replicar datos entre un sistema Cloud Volumes ONTAP en AWS y sistemas ONTAP en otras redes, debe tener una conexión VPN entre el VPC de AWS y la otra red, por ejemplo, un vnet de Azure o una red corporativa. Para ver instrucciones, consulte "Documentación de AWS: Configuración de una conexión VPN de AWS".

DNS y Active Directory para CIFS

Si desea aprovisionar almacenamiento CIFS, debe configurar DNS y Active Directory en AWS o ampliar la configuración de sus instalaciones a AWS.

El servidor DNS debe proporcionar servicios de resolución de nombres para el entorno de Active Directory. Puede configurar los conjuntos de opciones DHCP para que utilicen el servidor DNS EC2 predeterminado, que no debe ser el servidor DNS utilizado por el entorno de Active Directory.

Para obtener instrucciones, consulte "Documentación de AWS: Active Directory Domain Services en AWS Cloud: Implementación de referencia de inicio rápido".

Requisitos para pares de alta disponibilidad en varios AZs

Los requisitos de red adicionales de AWS se aplican a configuraciones de alta disponibilidad de Cloud Volumes ONTAP que utilizan varias zonas de disponibilidad (AZs). Debe revisar estos requisitos antes de iniciar una pareja de ha porque debe introducir los detalles de redes en Cloud Manager.

Para comprender cómo funcionan los pares de alta disponibilidad, consulte "Pares de alta disponibilidad".

Zonas de disponibilidad

Este modelo de puesta en marcha de alta disponibilidad utiliza varios AZs para garantizar una alta disponibilidad de sus datos. Debería utilizar una zona de disponibilidad dedicada para cada instancia de Cloud Volumes ONTAP y la instancia de mediador, que proporciona un canal de comunicación entre el par de alta disponibilidad.

Direcciones IP flotantes para datos de NAS y gestión de clústeres/SVM

Las configuraciones de ALTA DISPONIBILIDAD de varios AZs utilizan direcciones IP flotantes que migran entre nodos en caso de que se produzcan fallos. No se puede acceder a ellos de forma nativa desde fuera del VPC, a menos que usted "Configure una puerta de enlace de tránsito de AWS".

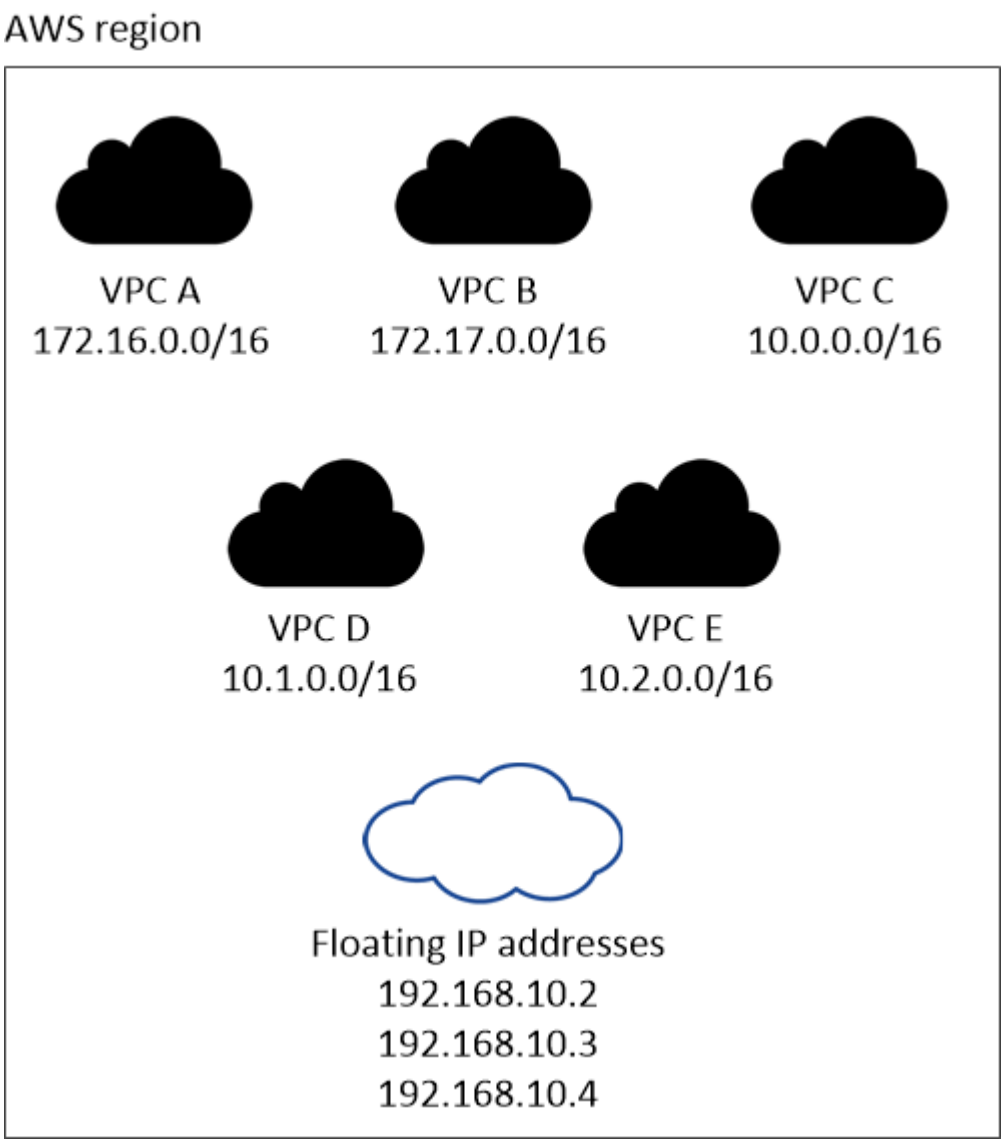
Una dirección IP flotante es para la gestión del clúster, otra para los datos NFS/CIFS del nodo 1 y otra para los datos NFS/CIFS del nodo 2. Una cuarta dirección IP flotante para la gestión de SVM es opcional.

Se requiere una dirección IP flotante para el LIF de gestión de SVM si se usa SnapDrive para Windows o SnapCenter con el par de alta disponibilidad. Si no especifica la dirección IP al implementar el sistema, puede crear la LIF más adelante. Para obtener más información, consulte "Configurar Cloud Volumes ONTAP".

Debe introducir las direcciones IP flotantes en Cloud Manager cuando crea un entorno de trabajo de alta disponibilidad de Cloud Volumes ONTAP. Cloud Manager asigna las direcciones IP a la pareja de alta disponibilidad cuando arranca el sistema.

Las direcciones IP flotantes deben estar fuera de los bloques CIDR para todas las VPC de la región AWS en la que se implemente la configuración de alta disponibilidad. Piense en las direcciones IP flotantes como una subred lógica que está fuera de las VPC en su región.

En el siguiente ejemplo se muestra la relación entre las direcciones IP flotantes y las VPC en una región de AWS. Mientras las direcciones IP flotantes están fuera de los bloques CIDR para todos los VPC, se pueden enrutar a subredes a través de tablas de ruta.



Cloud Manager crea automáticamente direcciones IP estáticas para el acceso iSCSI y para el acceso NAS desde clientes fuera de VPC. No es necesario cumplir ningún requisito para estos tipos de direcciones IP.

Puerta de enlace de tránsito para habilitar el acceso de IP flotante desde fuera del VPC

"Configure una puerta de enlace de tránsito de AWS" Para habilitar el acceso a las direcciones IP flotantes de una pareja de alta disponibilidad desde fuera del VPC, donde reside el par de alta disponibilidad.

Tablas de rutas

Después de especificar las direcciones IP flotantes en Cloud Manager, debe seleccionar las tablas de rutas que deberían incluir rutas a las direcciones IP flotantes. Esto permite el acceso de los clientes al par de alta disponibilidad.

Si sólo tiene una tabla de rutas para las subredes en el VPC (la tabla de rutas principal), Cloud Manager agrega automáticamente las direcciones IP flotantes a esa tabla de rutas. Si dispone de más de una tabla de rutas, es muy importante seleccionar las tablas de rutas correctas al iniciar el par ha. De lo contrario, es posible que algunos clientes no tengan acceso a Cloud Volumes ONTAP.

Por ejemplo, puede tener dos subredes asociadas a diferentes tablas de rutas. Si selecciona la tabla DE rutas A, pero no la tabla de rutas B, los clientes de la subred asociada a la tabla DE rutas A pueden acceder al par de alta disponibilidad, pero los clientes de la subred asociada a la tabla de rutas B no pueden.

Para obtener más información sobre las tablas de rutas, consulte "Documentación de AWS: Tablas de rutas".

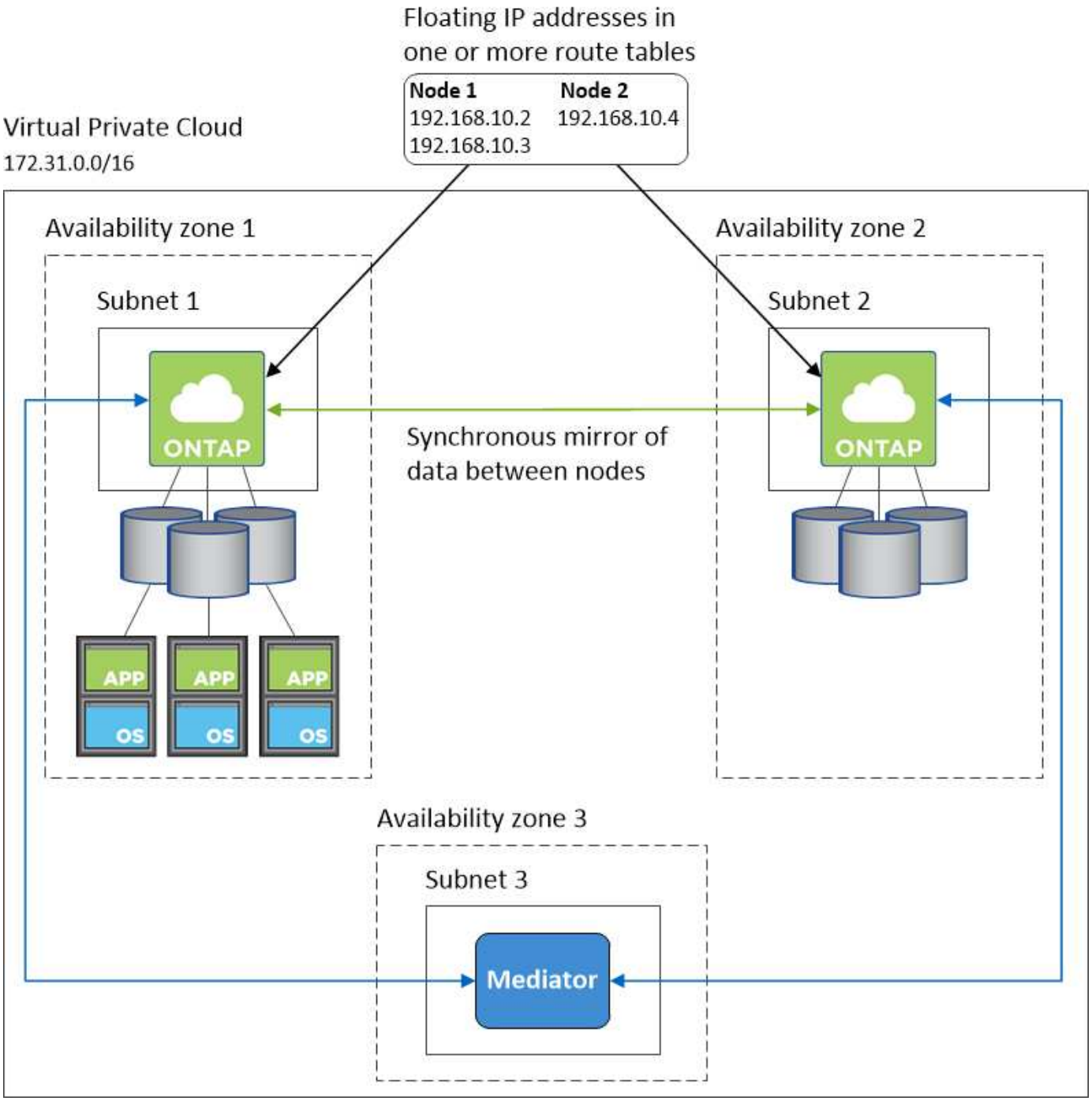
Conexión a herramientas de gestión de NetApp

Para utilizar las herramientas de gestión de NetApp con configuraciones de alta disponibilidad que se encuentran en múltiples AZs, tiene dos opciones de conexión:

1. Puesta en marcha de las herramientas de gestión de NetApp en otro VPC y otras "Configure una puerta de enlace de tránsito de AWS". La puerta de enlace permite el acceso a la dirección IP flotante para la interfaz de gestión del clúster desde fuera del VPC.
2. Ponga en marcha las herramientas de gestión de NetApp en el mismo VPC con una configuración de enrutamiento similar a las de los clientes NAS.

Ejemplo de configuración de alta disponibilidad

En la siguiente imagen, se muestra una configuración de alta disponibilidad óptima en AWS que funciona como una configuración activo-pasivo:



Requisitos para el conector

Configure su red de modo que el conector pueda gestionar recursos y procesos en su entorno de cloud público. El paso más importante es garantizar el acceso saliente a Internet a varios puntos finales.

Si la red utiliza un servidor proxy para toda la comunicación a Internet, puede especificar el servidor proxy en la página Configuración. Consulte "Configuración del conector para utilizar un servidor proxy".

Conexión a redes de destino

Un conector requiere una conexión de red a los VPC y VNets en los que desea implementar Cloud Volumes

ONTAP.

Por ejemplo, si instala un conector en la red corporativa, debe configurar una conexión VPN al VPC o a vnet en el que inicie Cloud Volumes ONTAP.

Acceso a Internet de salida

El conector requiere acceso saliente a Internet para gestionar recursos y procesos dentro de su entorno de nube pública. Un conector se pone en contacto con los siguientes extremos cuando se gestionan recursos en AWS:

Puntos finales	Específico
Servicios de AWS (amazonaws.com): • Formación CloudFormation • Cloud computing elástico (EC2) • Servicio de gestión de claves (KMS) • Servicio de token de seguridad (STS) • Simple Storage Service (S3) El extremo exacto depende de la región en la que se implemente Cloud Volumes ONTAP. "Consulte la documentación de AWS para obtener más detalles."	Permite que Cloud Manager ponga en marcha y gestione Cloud Volumes ONTAP en AWS.
https://api.services.cloud.netapp.com:443	Solicitudes de API a Cloud Central de NetApp.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Proporciona acceso a imágenes, manifiestos y plantillas de software.
https://repo.cloud.support.netapp.com	Se utiliza para descargar las dependencias de Cloud Manager.
http://repo.mysql.com/	Se utiliza para descargar MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Permite a Cloud Manager acceder y descargar manifiestos, plantillas e imágenes de actualización de Cloud Volumes ONTAP.
https://cloudmanagerinfraprod.azurecr.io	Acceso a imágenes de software de componentes de contenedor para una infraestructura que ejecuta Docker y proporciona una solución para las integraciones de servicios con Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Permite a NetApp transmitir datos desde registros de auditoría.
https://cloudmanager.cloud.netapp.com	Comunicación con el servicio Cloud Manager, que incluye cuentas de Cloud Central.
https://netapp-cloud-account.auth0.com	Comunicación con Cloud Central de NetApp para la autenticación de usuario centralizada.

Puntos finales	Específico
https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist	Se utiliza para añadir su ID de cuenta de AWS a la lista de usuarios permitidos para Backup en S3.
https://support.netapp.com/aods/asupmessage https://support.netapp.com/asupprod/post/1.0/postAsup	Comunicación con AutoSupport de NetApp.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Comunicación con NetApp para la licencia del sistema y el registro de soporte.
https://ipa-signer.cloudmanager.netapp.com	Permite que Cloud Manager genere licencias (por ejemplo, una licencia de FlexCache para Cloud Volumes ONTAP).
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Necesario para conectar los sistemas Cloud Volumes ONTAP con un clúster de Kubernetes. Los extremos permiten la instalación de Trident de NetApp.
Diversas ubicaciones de terceros, por ejemplo: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org Las ubicaciones de terceros están sujetas a cambios.	Durante las actualizaciones, Cloud Manager descarga los paquetes más recientes para dependencias de terceros.

Aunque debe realizar casi todas las tareas desde la interfaz de usuario de SaaS, todavía hay disponible una interfaz de usuario local en el conector. La máquina que ejecuta el explorador Web debe tener conexiones con los siguientes puntos finales:

Puntos finales	Específico
El host del conector	Debe introducir la dirección IP del host desde un explorador web para cargar la consola de Cloud Manager. Según su conectividad con el proveedor de cloud, puede usar la IP privada o una IP pública asignada al host: • Una IP privada funciona si dispone de una VPN y. acceso directo a la red virtual • Una IP pública funciona en cualquier situación de red En cualquier caso, debe proteger el acceso a la red garantizando que las reglas de grupo de seguridad permiten el acceso sólo desde IP o subredes autorizadas.

Puntos finales	Específico
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	El explorador web se conecta con estos extremos para conseguir una autenticación de usuario centralizada mediante NetApp Cloud Central.
https://widget.intercom.io	Si busca un chat integrado en los productos que le permita hablar con expertos en cloud de NetApp.

Configuración de una puerta de enlace de tránsito de AWS para parejas de alta disponibilidad en AZs múltiples

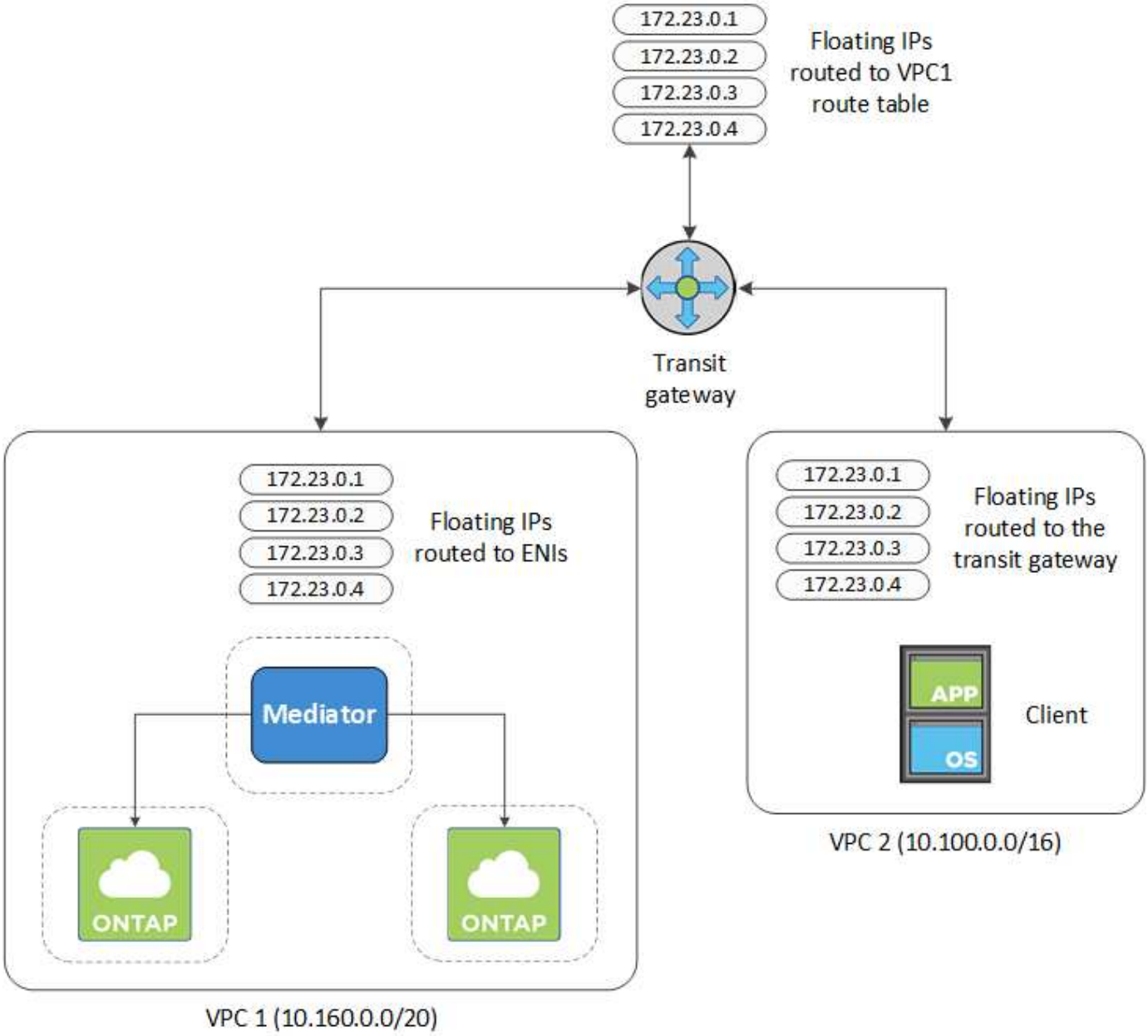
Configure una puerta de enlace de tránsito de AWS para permitir el acceso a. Pares de alta disponibilidad "Direcciones IP flotantes" Desde fuera del VPC, donde reside el par de alta disponibilidad.

Cuando una configuración de alta disponibilidad de Cloud Volumes ONTAP se distribuye por varias zonas de disponibilidad de AWS, se necesitan direcciones IP flotantes para el acceso a datos de NAS desde el VPC. Estas direcciones IP flotantes pueden migrar entre nodos cuando se producen fallos, pero no están accesibles desde fuera del VPC de forma nativa. Las direcciones IP privadas independientes proporcionan acceso a los datos desde fuera del VPC, pero no proporcionan una recuperación tras fallos automática.

Las direcciones IP flotantes también se requieren para la interfaz de gestión de clústeres y la LIF de gestión de SVM opcional.

Si configura una puerta de enlace de tránsito de AWS, debe habilitar el acceso a las direcciones IP flotantes desde fuera del VPC donde reside el par de alta disponibilidad. Esto significa que los clientes NAS y las herramientas de gestión de NetApp fuera del VPC pueden acceder a las IP flotantes.

Este es un ejemplo que muestra dos VPC conectados por una puerta de enlace de tránsito. Un sistema de alta disponibilidad reside en un VPC, mientras que un cliente reside en el otro. A continuación, podría montar un volumen NAS en el cliente mediante la dirección IP flotante.

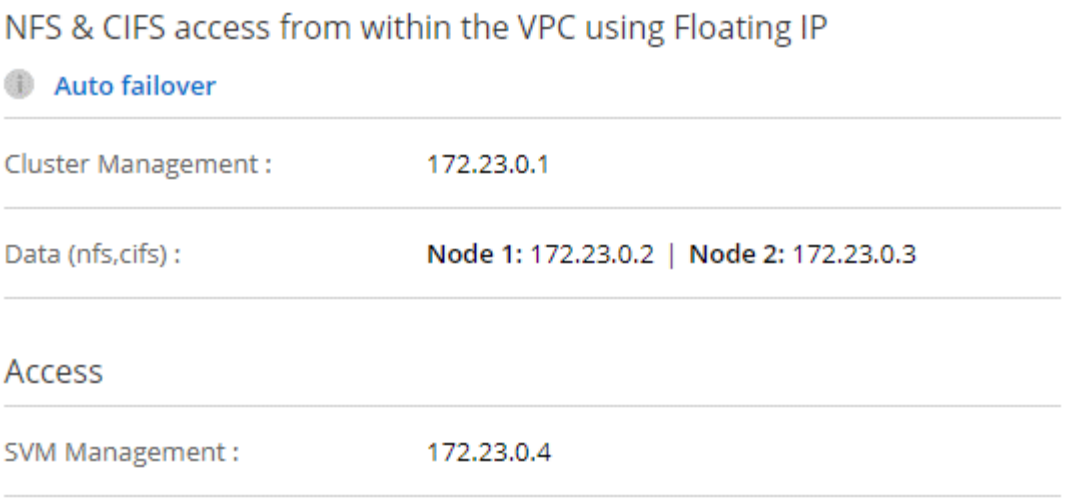


Los siguientes pasos ilustran cómo configurar una configuración similar.

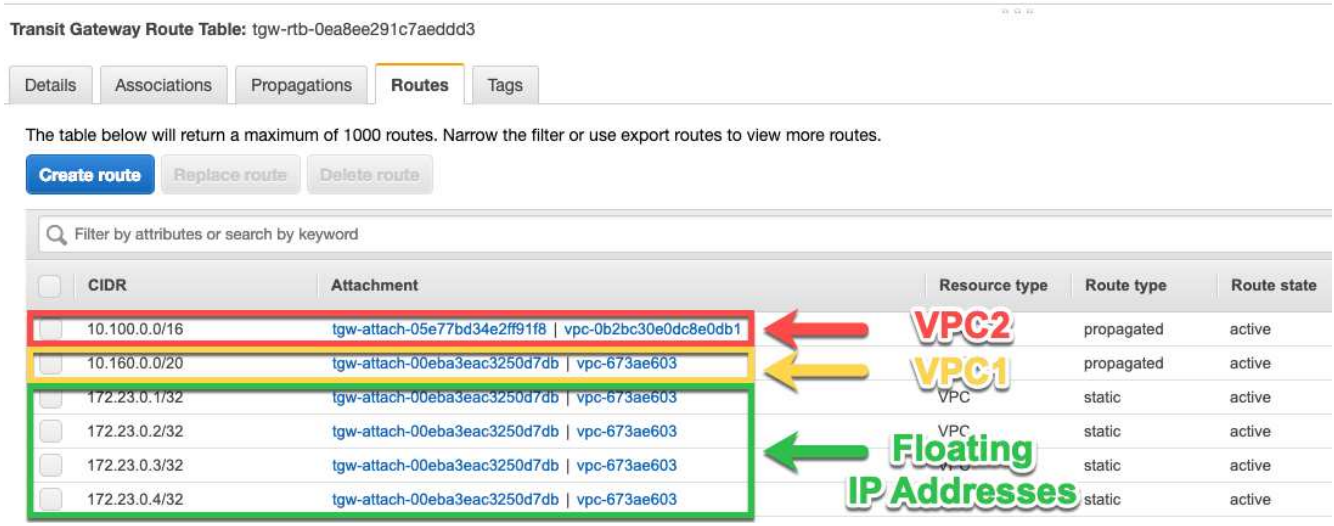
Pasos

1. "Cree una puerta de enlace de tránsito y conecte las VPC al puerta de enlace".
2. Cree rutas en la tabla de rutas de la puerta de enlace de tránsito especificando las direcciones IP flotantes del par de alta disponibilidad.

   Puede encontrar las direcciones IP flotantes en la página Información del entorno de trabajo de Cloud Manager. Veamos un ejemplo:

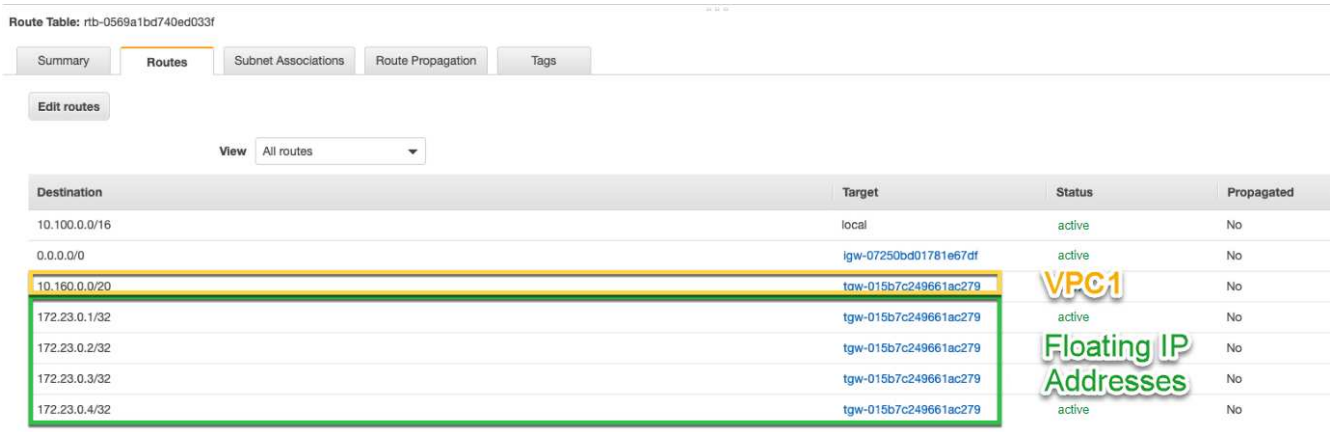


La siguiente imagen de ejemplo muestra la tabla de rutas para la puerta de enlace de tránsito. Incluye rutas a los bloques CIDR de las dos VPC y cuatro direcciones IP flotantes utilizadas por Cloud Volumes ONTAP.



3. Modifique la tabla de rutas de las VPC que necesitan acceder a las direcciones IP flotantes.
   a. Agregar entradas de ruta a las direcciones IP flotantes.
   b. Añada una entrada de ruta al bloque CIDR del VPC donde reside el par de alta disponibilidad.

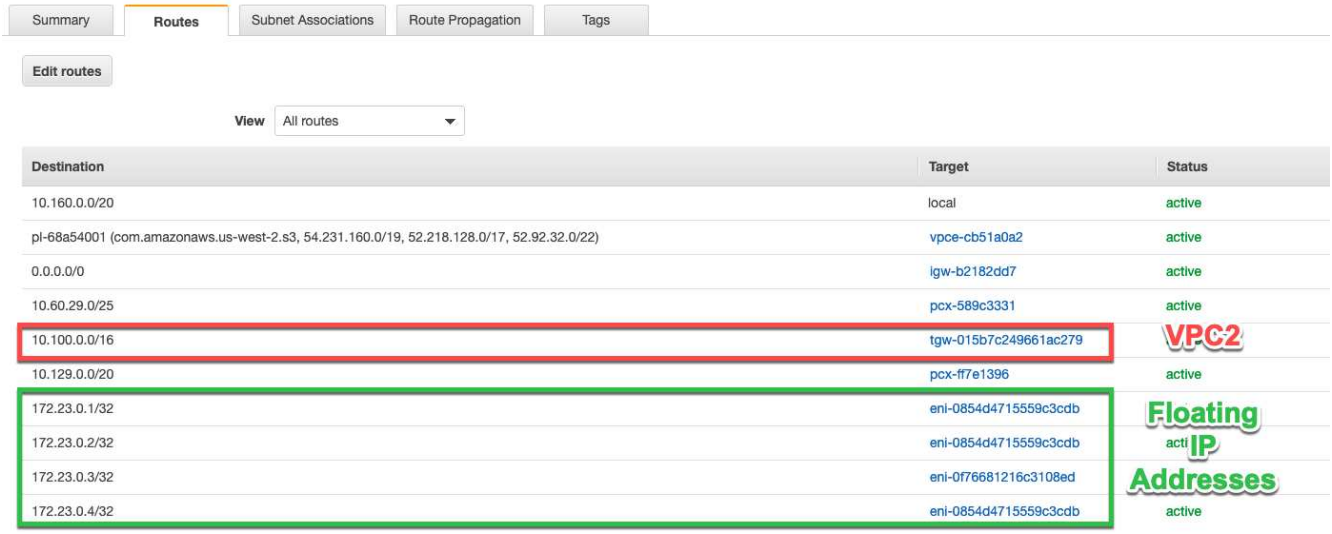
      La siguiente imagen de ejemplo muestra la tabla de rutas para VPC 2, que incluye las rutas hasta VPC 1 y las direcciones IP flotantes.



4. Modifique la tabla de rutas del VPC del par de alta disponibilidad añadiendo una ruta al VPC que necesite acceso a las direcciones IP flotantes.

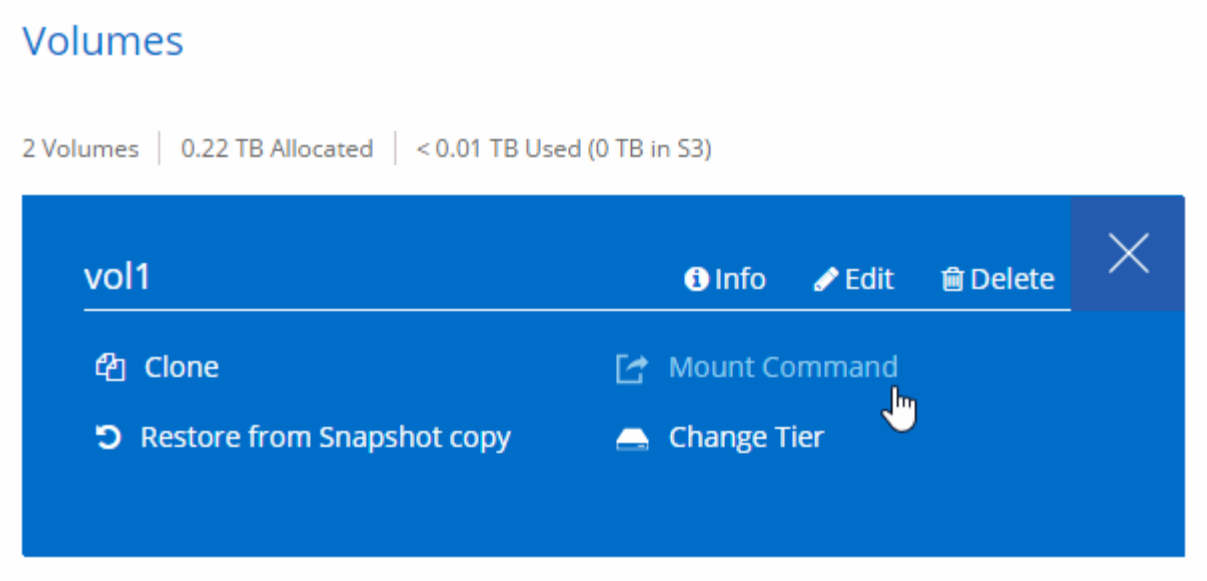
   Este paso es importante porque completa el enrutamiento entre las VPC.

   La siguiente imagen de ejemplo muestra la tabla de rutas para VPC 1. Incluye una ruta a las direcciones IP flotantes y al VPC 2, que es donde reside un cliente. Cloud Manager añadió automáticamente las IP flotantes a la tabla de rutas cuando puso en marcha el par de alta disponibilidad.



5. Montar volúmenes en clientes con la dirección IP flotante.

   Puede encontrar la dirección IP correcta en Cloud Manager seleccionando un volumen y haciendo clic en **Mount Command**.



Enlaces relacionados

- "Pares de alta disponibilidad en AWS"
- "Requisitos de red para Cloud Volumes ONTAP en AWS"

Reglas de grupos de seguridad para AWS

Cloud Manager crea grupos de seguridad de AWS que incluyen las reglas entrantes y salientes que Connector y Cloud Volumes ONTAP necesitan para funcionar correctamente. Tal vez desee consultar los puertos para fines de prueba o si prefiere utilizar sus propios grupos de seguridad.

Reglas para Cloud Volumes ONTAP

El grupo de seguridad para Cloud Volumes ONTAP requiere reglas tanto entrantes como salientes.

Reglas de entrada

El origen de las reglas entrantes en el grupo de seguridad predefinido es 0.0.0.0/0.

Protocolo	Puerto	Específico
Todos los ICMP	Todo	Hacer ping a la instancia
HTTP	80	Acceso HTTP a la consola web de System Manager mediante el La dirección IP de la LIF de gestión del clúster
HTTPS	443	Acceso HTTPS a la consola web de System Manager mediante el La dirección IP de la LIF de gestión del clúster
SSH	22	Acceso SSH a la dirección IP de administración del clúster LIF o una LIF de gestión de nodos
TCP	111	Llamada a procedimiento remoto para NFS

Protocolo	Puerto	Específico
TCP	139	Sesión de servicio NetBIOS para CIFS
TCP	161-162	Protocolo simple de gestión de red
TCP	445	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
TCP	635	Montaje NFS
TCP	749	Kerberos
TCP	2049	Daemon del servidor NFS
TCP	3260	Acceso iSCSI mediante la LIF de datos iSCSI
TCP	4045	Daemon de bloqueo NFS
TCP	4046	Supervisor de estado de red para NFS
TCP	10000	Backup con NDMP
TCP	11104	Gestión de sesiones de comunicación de interconexión de clústeres para SnapMirror
TCP	11105	Transferencia de datos de SnapMirror mediante LIF de interconexión de clústeres
UDP	111	Llamada a procedimiento remoto para NFS
UDP	161-162	Protocolo simple de gestión de red
UDP	635	Montaje NFS
UDP	2049	Daemon del servidor NFS
UDP	4045	Daemon de bloqueo NFS
UDP	4046	Supervisor de estado de red para NFS
UDP	4049	Protocolo rquotad NFS

Reglas de salida

El grupo de seguridad predefinido para Cloud Volumes ONTAP abre todo el tráfico saliente. Si eso es aceptable, siga las reglas básicas de la salida. Si necesita más reglas rígidas, utilice las reglas avanzadas de salida.

Reglas de salida básicas

El grupo de seguridad predefinido para Cloud Volumes ONTAP incluye las siguientes reglas de salida.

Protocolo	Puerto	Específico
Todos los ICMP	Todo	Todo el tráfico saliente
Todos los TCP	Todo	Todo el tráfico saliente
Todas las UDP	Todo	Todo el tráfico saliente

Reglas salientes avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede utilizar la siguiente información para abrir sólo los

puertos necesarios para la comunicación saliente por Cloud Volumes ONTAP.

El origen es la interfaz (dirección IP) en el sistema Cloud Volumes ONTAP.

Servicio	Protocolo	Puerto	Origen	Destino	Específico
Active Directory	TCP	88	LIF de gestión de nodos	Bosque de Active Directory	Autenticación Kerberos V.
	UDP	137	LIF de gestión de nodos	Bosque de Active Directory	Servicio de nombres NetBIOS
	UDP	138	LIF de gestión de nodos	Bosque de Active Directory	Servicio de datagramas NetBIOS
	TCP	139	LIF de gestión de nodos	Bosque de Active Directory	Sesión de servicio NetBIOS
	TCP Y UDP	389	LIF de gestión de nodos	Bosque de Active Directory	LDAP
	TCP	445	LIF de gestión de nodos	Bosque de Active Directory	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
	TCP	464	LIF de gestión de nodos	Bosque de Active Directory	Kerberos V cambiar y establecer contraseña (SET_CHANGE)
	UDP	464	LIF de gestión de nodos	Bosque de Active Directory	Administración de claves Kerberos
	TCP	749	LIF de gestión de nodos	Bosque de Active Directory	Contraseña de Kerberos V Change & Set (RPCSEC_GSS)
	TCP	88	LIF de datos (NFS, CIFS e iSCSI)	Bosque de Active Directory	Autenticación Kerberos V.
	UDP	137	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Servicio de nombres NetBIOS
	UDP	138	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Servicio de datagramas NetBIOS
	TCP	139	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Sesión de servicio NetBIOS
	TCP Y UDP	389	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	LDAP
	TCP	445	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
	TCP	464	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Kerberos V cambiar y establecer contraseña (SET_CHANGE)
	UDP	464	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Administración de claves Kerberos
	TCP	749	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Contraseña de Kerberos V change & set (RPCSEC_GSS)

Servicio	Protocolo	Puerto	Origen	Destino	Específico
Backup en S3	TCP	5010	LIF entre clústeres	Extremo de backup o extremo de restauración	Realizar backups y restaurar operaciones para el backup en S3 función
Clúster	Todo el tráfico	Todo el tráfico	Todos los LIF de un nodo	Todas las LIF del otro nodo	Comunicaciones de interconexión de clústeres (solo Cloud Volumes ONTAP de alta disponibilidad)
	TCP	3000	LIF de gestión de nodos	Mediador DE ALTA DISPONIBILIDAD	Llamadas ZAPI (solo alta disponibilidad de Cloud Volumes ONTAP)
	ICMP	1	LIF de gestión de nodos	Mediador DE ALTA DISPONIBILIDAD	Mantener activos (solo alta disponibilidad de Cloud Volumes ONTAP)
DHCP	UDP	68	LIF de gestión de nodos	DHCP	Cliente DHCP para la configuración inicial
DHCPS	UDP	67	LIF de gestión de nodos	DHCP	Servidor DHCP
DNS	UDP	53	LIF de gestión de nodos y LIF de datos (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	LIF de gestión de nodos	Servidores de destino	Copia NDMP
SMTP	TCP	25	LIF de gestión de nodos	Servidor de correo	Alertas SMTP, que se pueden utilizar para AutoSupport
SNMP	TCP	161	LIF de gestión de nodos	Servidor de supervisión	Supervisión mediante capturas SNMP
	UDP	161	LIF de gestión de nodos	Servidor de supervisión	Supervisión mediante capturas SNMP
	TCP	162	LIF de gestión de nodos	Servidor de supervisión	Supervisión mediante capturas SNMP
	UDP	162	LIF de gestión de nodos	Servidor de supervisión	Supervisión mediante capturas SNMP
SnapMirror	TCP	11104	LIF entre clústeres	LIF de interconexión de clústeres de ONTAP	Gestión de sesiones de comunicación de interconexión de clústeres para SnapMirror
	TCP	11105	LIF entre clústeres	LIF de interconexión de clústeres de ONTAP	Transferencia de datos de SnapMirror
Syslog	UDP	514	LIF de gestión de nodos	Servidor de syslog	Mensajes de syslog Reenviar

Reglas para el grupo de seguridad externo de mediador de alta disponibilidad

El grupo de seguridad externo predefinido para el mediador de alta disponibilidad de Cloud Volumes ONTAP incluye las siguientes reglas de entrada y salida.

Reglas de entrada

La fuente de las reglas entrantes es 0.0.0.0/0.

Protocolo	Puerto	Específico
SSH	22	Conexiones SSH al mediador de alta disponibilidad
TCP	3000	Acceso a API RESTful desde el conector

Reglas de salida

El grupo de seguridad predefinido para el mediador ha abre todo el tráfico saliente. Si eso es aceptable, siga las reglas básicas de la salida. Si necesita más reglas rígidas, utilice las reglas avanzadas de salida.

Reglas de salida básicas

El grupo de seguridad predefinido para el mediador ha incluye las siguientes reglas de salida.

Protocolo	Puerto	Específico
Todos los TCP	Todo	Todo el tráfico saliente
Todas las UDP	Todo	Todo el tráfico saliente

Reglas salientes avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede utilizar la siguiente información para abrir sólo los puertos necesarios para la comunicación saliente por parte del mediador ha.

Protocolo	Puerto	Destino	Específico
HTTP	80	Dirección IP del conector	Descargar actualizaciones para el mediador
HTTPS	443	Servicios API de AWS	Ayudar en la recuperación tras fallos de almacenamiento
UDP	53	Servicios API de AWS	Ayudar en la recuperación tras fallos de almacenamiento

En lugar de abrir los puertos 443 y 53, puede crear un extremo de la interfaz VPC desde la subred de destino al servicio AWS EC2.

Reglas para el grupo de seguridad interna de mediador de alta disponibilidad

El grupo de seguridad interna predefinido para el mediador de alta disponibilidad de Cloud Volumes ONTAP incluye las siguientes reglas. Cloud Manager siempre crea este grupo de seguridad. No tiene la opción de utilizar la suya propia.

Reglas de entrada

El grupo de seguridad predefinido incluye las siguientes reglas entrantes.

Protocolo	Puerto	Específico
Todo el tráfico	Todo	Comunicación entre el mediador de alta disponibilidad y los nodos de alta disponibilidad

Reglas de salida

El grupo de seguridad predefinido incluye las siguientes reglas de salida.

Protocolo	Puerto	Específico
Todo el tráfico	Todo	Comunicación entre el mediador de alta disponibilidad y los nodos de alta disponibilidad

Reglas para el conector

El grupo de seguridad del conector requiere reglas entrantes y salientes.

Reglas de entrada

El origen de las reglas entrantes en el grupo de seguridad predefinido es 0.0.0.0/0.

Protocolo	Puerto	Específico
SSH	22	Proporciona acceso SSH al host de Connector
HTTP	80	Proporciona acceso HTTP desde navegadores web de cliente al local Interfaz de usuario y conexiones desde Cloud Compliance
HTTPS	443	Proporciona acceso HTTPS desde exploradores web de cliente al local interfaz de usuario
TCP	3128	Proporciona a la instancia de Cloud Compliance acceso a Internet si la red AWS no utiliza NAT o proxy

Reglas de salida

El grupo de seguridad predefinido para el conector abre todo el tráfico saliente. Si eso es aceptable, siga las reglas básicas de la salida. Si necesita más reglas rígidas, utilice las reglas avanzadas de salida.

Reglas de salida básicas

El grupo de seguridad predefinido para el conector incluye las siguientes reglas de salida.

Protocolo	Puerto	Específico
Todos los TCP	Todo	Todo el tráfico saliente
Todas las UDP	Todo	Todo el tráfico saliente

Reglas salientes avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede utilizar la siguiente información para abrir sólo los puertos necesarios para la comunicación saliente por parte del conector.

La dirección IP de origen es el host del conector.

Servicio	Protocolo	Puerto	Destino	Específico
Active Directory	TCP	88	Bosque de Active Directory	Autenticación Kerberos V.
	TCP	139	Bosque de Active Directory	Sesión de servicio NetBIOS
	TCP	389	Bosque de Active Directory	LDAP
	TCP	445	Bosque de Active Directory	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
	TCP	464	Bosque de Active Directory	Kerberos V cambiar y establecer contraseña (SET_CHANGE)
	TCP	749	Bosque de Active Directory	Contraseña de modificación y definición de Kerberos V de Active Directory (RPCSEC_GSS)
	UDP	137	Bosque de Active Directory	Servicio de nombres NetBIOS
	UDP	138	Bosque de Active Directory	Servicio de datagramas NetBIOS
	UDP	464	Bosque de Active Directory	Administración de claves Kerberos
Llamadas API y AutoSupport	HTTPS	443	LIF de gestión de clústeres de ONTAP y Internet saliente	API llama a AWS y ONTAP y envía mensajes de AutoSupport a NetApp
Llamadas API	TCP	3000	LIF de gestión de clústeres de ONTAP	Llamadas API a ONTAP
	TCP	8088	Backup en S3	Llamadas API a Backup en S3
DNS	UDP	53	DNS	Utilizado para resolver DNS por Cloud Manager

Servicio	Protocolo	Puerto	Destino	Específico
Cumplimiento de normativas en el cloud	HTTP	80	Instancia de cumplimiento de normativas cloud	Cumplimiento de normativas cloud para Cloud Volumes ONTAP

Configuración de AWS KMS

Si desea usar el cifrado de Amazon con Cloud Volumes ONTAP, debe configurar el servicio de gestión de claves (KMS) de AWS.

Pasos

1. Asegúrese de que existe una clave maestra de cliente (CMK) activa.

   El CMK puede ser un CMK gestionado por AWS o un CMK gestionado por el cliente. Puede encontrarse en la misma cuenta de AWS que Cloud Manager y Cloud Volumes ONTAP, o en una cuenta de AWS diferente.

   "Documentación de AWS: Claves maestras de clientes (CMKs)"

2. Modifique la política de claves de cada CMK añadiendo el rol IAM que proporciona permisos a Cloud Manager como *key user*.

   La adición del rol IAM como usuario clave permite a Cloud Manager utilizar el CMK con Cloud Volumes ONTAP.

   "Documentación de AWS: Editar claves"

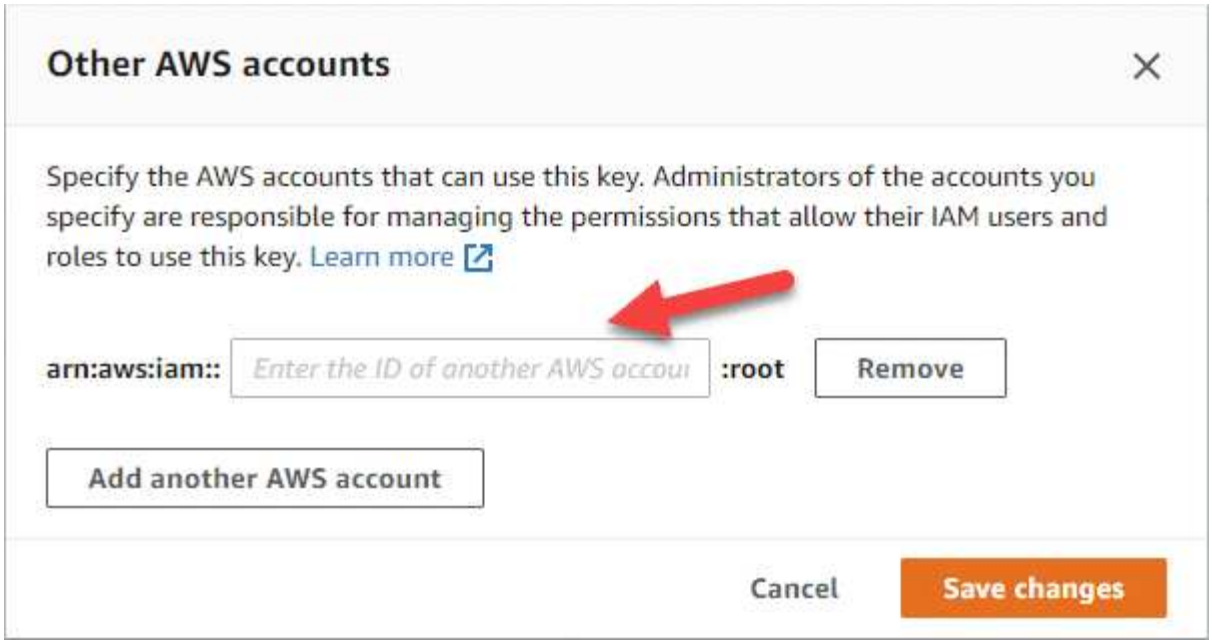
3. Si el CMK se encuentra en una cuenta de AWS diferente, realice los pasos siguientes:

   a. Vaya a la consola KMS desde la cuenta donde reside el CMK.
   b. Seleccione la tecla.
   c. En el panel **Configuración general**, copie el ARN de la clave.

      Deberá proporcionar el ARN al Cloud Manager cuando cree el sistema Cloud Volumes ONTAP.

   d. En el panel **otras cuentas de AWS**, agregue la cuenta de AWS que proporciona permisos a Cloud Manager.

      En la mayoría de los casos, esta es la cuenta en la que reside Cloud Manager. Si Cloud Manager no se instaló en AWS, sería la cuenta para la que proporcionó las claves de acceso de AWS a Cloud Manager.



e. Cambie ahora a la cuenta de AWS que proporciona permisos a Cloud Manager y abra la consola IAM.

f. Cree una política de IAM que incluya los permisos que se indican a continuación.

g. Asocie la política al rol de IAM o al usuario IAM que proporciona permisos a Cloud Manager.

   La siguiente directiva proporciona los permisos que Cloud Manager necesita para utilizar CMK desde la cuenta de AWS externa. Asegúrese de modificar la región y el ID de cuenta en las secciones "Recursos".

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowUseOfTheKey",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalkeyid"
            ]
        },
        {
            "Sid": "AllowAttachmentOfPersistentResources",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalaccountid"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

+
Para obtener más información sobre este proceso, consulte "Documentación de AWS: Permitir que las cuentas de AWS externas puedan acceder a un CMK".

Inicio de Cloud Volumes ONTAP en AWS

Puede iniciar Cloud Volumes ONTAP en una configuración con un único sistema o como par de alta disponibilidad en AWS.

Lanzar un sistema Cloud Volumes ONTAP de un único nodo en AWS

Si desea iniciar Cloud Volumes ONTAP en AWS, tiene que crear un nuevo entorno de trabajo en Cloud Manager.

Antes de empezar

- Usted debe tener un "Conector asociado al área de trabajo".

> Debe ser un administrador de cuentas para crear un conector. Al crear el primer entorno de trabajo de Cloud Volumes ONTAP, Cloud Manager le solicita que cree un conector si todavía no lo tiene.

- "Debe estar preparado para dejar el conector funcionando en en todo momento".
- Debe haberse preparado eligiendo una configuración y obteniendo información de red de AWS de su administrador. Para obtener más información, consulte "Planificación de la configuración de Cloud Volumes ONTAP".
- Si desea iniciar un sistema BYOL, debe tener el número de serie de 20 dígitos (clave de licencia).
- Si desea usar CIFS, debe haber configurado DNS y Active Directory. Para obtener más información, consulte "Requisitos de red para Cloud Volumes ONTAP en AWS".

Acerca de esta tarea

Inmediatamente después de crear el entorno de trabajo, Cloud Manager inicia una instancia de prueba en el VPC especificado para verificar la conectividad. Si se realiza correctamente, Cloud Manager finaliza inmediatamente la instancia y después inicia la implementación del sistema Cloud Volumes ONTAP. Si Cloud Manager no puede verificar la conectividad, se produce un error en la creación del entorno de trabajo. La instancia de prueba es t2.nano (para el tenancy por defecto de VPC) o m3.medium (para el uso dedicado de VPC).

Pasos

1. En la página entornos de trabajo, haga clic en **Agregar entorno de trabajo** y siga las indicaciones.
2. **Elija una ubicación**: Seleccione **Amazon Web Services** y **Cloud Volumes ONTAP Single Node**.
3. **Detalles y credenciales**: Si lo desea, puede cambiar las credenciales y la suscripción de AWS, introducir un nombre de entorno de trabajo, agregar etiquetas y, a continuación, introducir una contraseña.

   Algunos de los campos en esta página son claros y explicativos. En la siguiente tabla se describen los campos que podrían presentar dificultades:

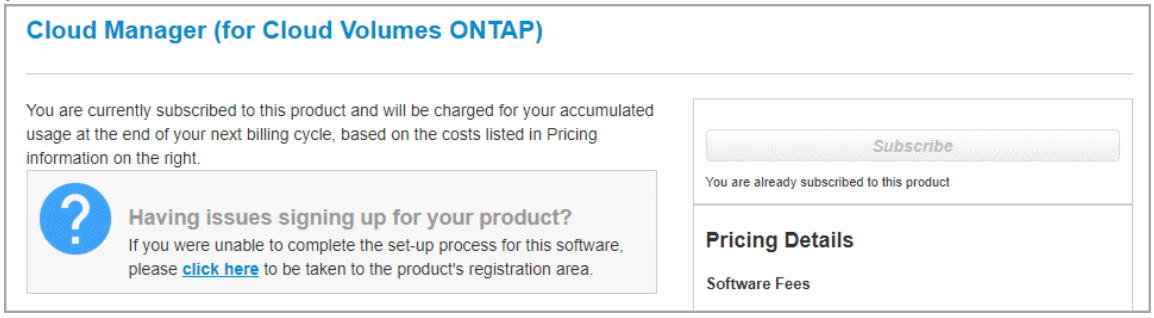
Campo	Descripción
Nombre del entorno de trabajo	Cloud Manager utiliza el nombre del entorno de trabajo para asignar un nombre tanto al sistema Cloud Volumes ONTAP como a la instancia de Amazon EC2. También utiliza el nombre como prefijo para el grupo de seguridad predefinido si selecciona esa opción.

Campo	Descripción
Agregar etiquetas	Las etiquetas de AWS son metadatos para sus recursos de AWS. Cloud Manager agrega las etiquetas a la instancia de Cloud Volumes ONTAP y a cada recurso de AWS asociado con la instancia. Puede agregar hasta cuatro etiquetas desde la interfaz de usuario al crear un entorno de trabajo y, a continuación, puede agregar más después de crear. Tenga en cuenta que la API no le limita a cuatro etiquetas al crear un entorno de trabajo. Para obtener información sobre etiquetas, consulte "Documentación de AWS: Etiquetado de los recursos de Amazon EC2".
Nombre de usuario y contraseña	Estas son las credenciales de la cuenta de administrador del clúster de Cloud Volumes ONTAP. Puede usar estas credenciales para conectarse a Cloud Volumes ONTAP a través de OnCommand System Manager o de su CLI.
Editar credenciales	Elija las credenciales de AWS y la suscripción al mercado para utilizar con este sistema Cloud Volumes ONTAP. Haga clic en **Agregar suscripción** para asociar las credenciales seleccionadas a una suscripción. Para crear un sistema Cloud Volumes ONTAP de pago por uso, debe seleccionar las credenciales de AWS asociadas con una suscripción a Cloud Volumes ONTAP desde AWS Marketplace. Se le cobrará de esta suscripción por cada sistema Cloud Volumes ONTAP 9.6 y posterior de PAYGO que cree y cada función complementaria que habilite."Aprenda a añadir credenciales de AWS adicionales a Cloud Manager".

En el siguiente vídeo se muestra cómo asociar una suscripción de pago por uso a Marketplace en sus credenciales de AWS:

► https://docs.netapp.com/es-es/occm38//media/video_subscribing_aws.mp4 *(video)*

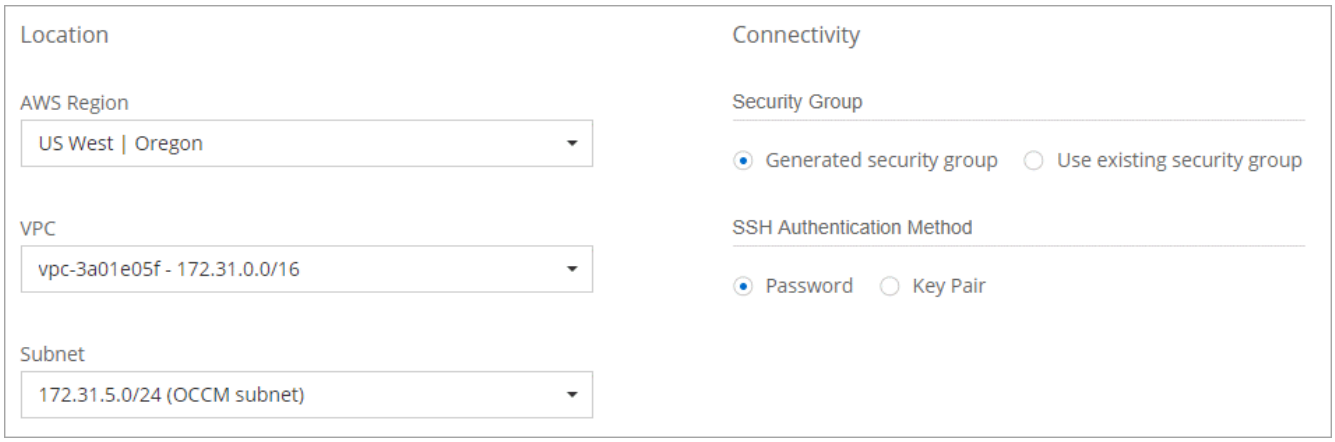
Si varios usuarios de IAM trabajan en la misma cuenta de AWS, cada usuario debe suscribirse. Una vez que el primer usuario se haya suscrito, AWS Marketplace informa a los usuarios posteriores de que ya están suscritos, tal como se muestra en la siguiente imagen. Mientras se ha establecido una suscripción para la cuenta *de AWS*, cada usuario de IAM debe asociarse a dicha suscripción. Si ve el mensaje que aparece a continuación, haga clic en el enlace **haga clic aquí** para ir a Cloud Central y completar el proceso.



4. **Servicios**: Mantenga activados los servicios o desactive los servicios individuales que no desea utilizar con Cloud Volumes ONTAP.
   - "Más información sobre Cloud Compliance".
   - "Más información sobre el backup en el cloud".
   - "Más información sobre la supervisión".

5. **ubicación y conectividad**: Introduzca la información de red que ha grabado en la hoja de trabajo de AWS.

   La siguiente imagen muestra la página llena:



6. **cifrado de datos**: Elija sin cifrado de datos o cifrado gestionado por AWS.

   Para el cifrado gestionado por AWS, puede elegir una clave maestra de cliente (CMK) diferente de su cuenta u otra cuenta de AWS.

   No puede cambiar el método de cifrado de datos de AWS después de crear un sistema Cloud Volumes ONTAP.

   "Aprenda a configurar AWS KMS para el cloud Volumes ONTAP".

   "Obtenga más información sobre las tecnologías de cifrado compatibles".

7. **cuenta del sitio de soporte y licencia**: Indique si desea usar el modelo de pago por uso o con su licencia y, a continuación, especifique una cuenta del sitio de soporte de NetApp.

   Para comprender cómo funcionan las licencias, consulte "Licencia".

   Una cuenta del sitio de soporte de NetApp es opcional para el pago por uso, pero obligatoria para los sistemas BYOL. "Aprenda a añadir cuentas del sitio de soporte de NetApp".

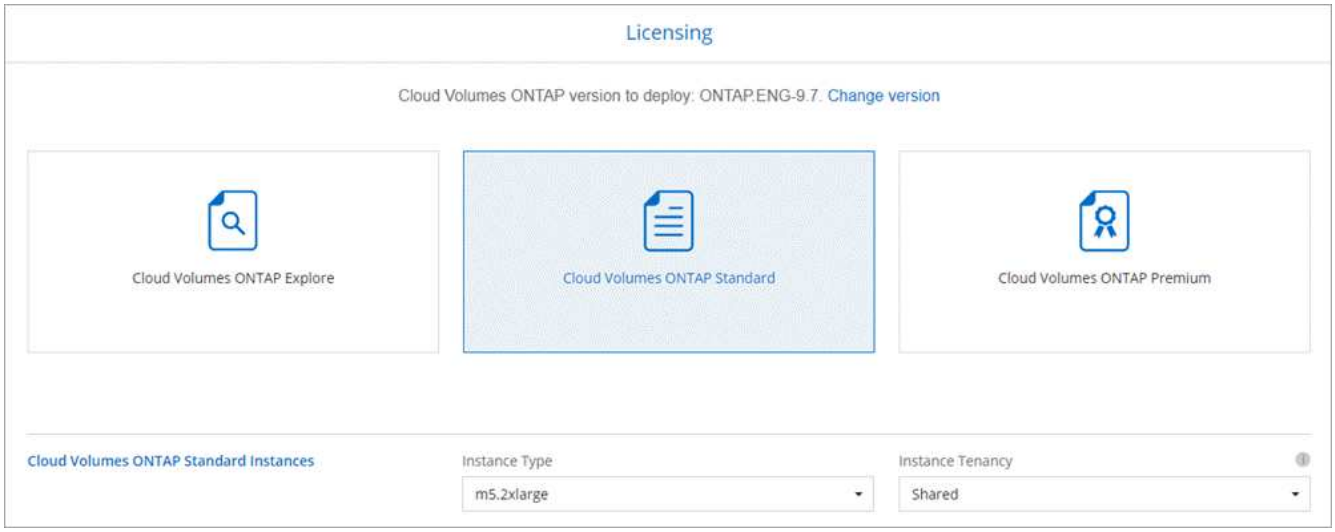
8. **Paquetes preconfigurados**: Seleccione uno de los paquetes para iniciar rápidamente Cloud Volumes ONTAP, o haga clic en **Crear mi propia configuración**.

   Si selecciona uno de los paquetes, solo tiene que especificar un volumen y, a continuación, revisar y aprobar la configuración.

9. **función IAM**: Debe mantener la opción predeterminada para que Cloud Manager pueda crear la función que le corresponde.

   Si prefiere utilizar su propia política, debe cumplirla "Requisitos de políticas para los nodos Cloud Volumes ONTAP".

10. **Licencia**: Cambie la versión de Cloud Volumes ONTAP según sea necesario, seleccione una licencia, un tipo de instancia y el uso de la instancia.



Si sus necesidades cambian después de iniciar la instancia, puede modificar la licencia o el tipo de instancia más adelante.

> Si hay disponible un candidato de versión, disponibilidad general o versión de revisión más reciente para la versión seleccionada, Cloud Manager actualiza el sistema a esa versión al crear el entorno de trabajo. Por ejemplo, la actualización se produce si selecciona Cloud Volumes ONTAP 9.6 RC1 y 9.6 GA está disponible. La actualización no se produce de una versión a otra; por ejemplo, de 9.6 a 9.7.

11. **Recursos de almacenamiento subyacentes**: Elija la configuración para el agregado inicial: Un tipo de disco, un tamaño para cada disco y si la organización en niveles de datos debe estar activada.

    Tenga en cuenta lo siguiente:

    - El tipo de disco es para el volumen inicial. Es posible seleccionar un tipo de disco diferente para volúmenes posteriores.
    - El tamaño de disco es para todos los discos del agregado inicial y para cualquier agregado adicional que Cloud Manager cree cuando utilice la opción de aprovisionamiento simple. Puede crear agregados que utilicen un tamaño de disco diferente mediante la opción de asignación avanzada.

      Para obtener ayuda a elegir el tipo y el tamaño de disco, consulte "Ajuste de tamaño de su sistema en AWS".

    - Se puede elegir una política de organización en niveles de volumen específica cuando se crea o se edita un volumen.
    - Si deshabilita la organización en niveles de datos, puede habilitarla en agregados posteriores.

      "Descubra cómo funciona la organización en niveles de datos".

12. **escribir velocidad y GUSANO**: Elija **velocidad de escritura normal** o **Alta**, y active el almacenamiento de escritura única, lectura múltiple (WORM), si lo desea.

    Además, es posible seleccionar una velocidad de escritura con sistemas de un solo nodo.

    "Más información sobre la velocidad de escritura".

    NO se puede habilitar WORM si la organización en niveles de datos está habilitada.

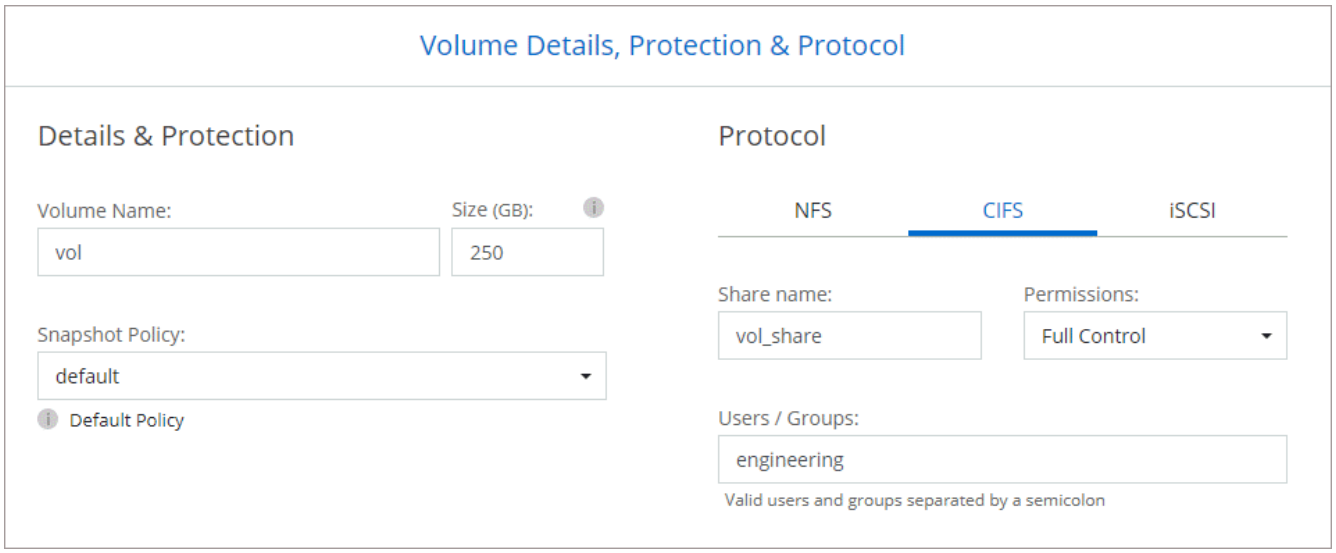
"Más información acerca del almacenamiento WORM".

13. **Crear volumen**: Introduzca los detalles del nuevo volumen o haga clic en **Omitir**.

    Algunos de los campos en esta página son claros y explicativos. En la siguiente tabla se describen los campos que podrían presentar dificultades:

Campo	Descripción
Tamaño	El tamaño máximo que puede introducir depende en gran medida de si habilita thin provisioning, lo que le permite crear un volumen que sea mayor que el almacenamiento físico que hay disponible actualmente.
Control de acceso (solo para NFS)	Una política de exportación define los clientes de la subred que pueden acceder al volumen. De forma predeterminada, Cloud Manager introduce un valor que proporciona acceso a todas las instancias de la subred.
Permisos y usuarios/grupos (solo para CIFS)	Estos campos permiten controlar el nivel de acceso a un recurso compartido para usuarios y grupos (también denominados listas de control de acceso o ACL). Es posible especificar usuarios o grupos de Windows locales o de dominio, o usuarios o grupos de UNIX. Si especifica un nombre de usuario de Windows de dominio, debe incluir el dominio del usuario con el formato domain\username.
Política de Snapshot	Una política de copia de Snapshot especifica la frecuencia y el número de copias de Snapshot de NetApp creadas automáticamente. Una copia snapshot de NetApp es una imagen del sistema de archivos puntual que no afecta al rendimiento y requiere un almacenamiento mínimo. Puede elegir la directiva predeterminada o ninguna. Es posible que no elija ninguno para los datos transitorios: Por ejemplo, tempdb para Microsoft SQL Server.
Opciones avanzadas (solo para NFS)	Seleccione una versión de NFS para el volumen: NFSv3 o NFSv4.
Grupo del iniciador y IQN (solo para iSCSI)	Los destinos de almacenamiento iSCSI se denominan LUN (unidades lógicas) y se presentan a los hosts como dispositivos de bloque estándar. Los iGroups son tablas de los nombres de los nodos de host iSCSI y controlan qué iniciadores tienen acceso a qué LUN. Los destinos iSCSI se conectan a la red a través de adaptadores de red Ethernet (NIC) estándar, tarjetas DEL motor de descarga TCP (TOE) con iniciadores de software, adaptadores de red convergente (CNA) o adaptadores de host de salida dedicados (HBA) y se identifican mediante nombres cualificados de iSCSI (IQN). Cuando se crea un volumen iSCSI, Cloud Manager crea automáticamente un LUN. Lo hemos hecho sencillo creando sólo una LUN por volumen, por lo que no hay que realizar ninguna gestión. Después de crear el volumen, "Utilice el IQN para conectarse con la LUN del hosts".

    En la siguiente imagen, se muestra la página volumen rellenada para el protocolo CIFS:



14. **Configuración CIFS**: Si elige el protocolo CIFS, configure un servidor CIFS.

Campo	Descripción
DNS Dirección IP principal y secundaria	Las direcciones IP de los servidores DNS que proporcionan resolución de nombres para el servidor CIFS. Los servidores DNS enumerados deben contener los registros de ubicación de servicio (SRV) necesarios para localizar los servidores LDAP de Active Directory y los controladores de dominio del dominio al que se unirá el servidor CIFS.
Dominio de Active Directory al que unirse	El FQDN del dominio de Active Directory (AD) al que desea que se una el servidor CIFS.
Credenciales autorizadas para unirse al dominio	Nombre y contraseña de una cuenta de Windows con privilegios suficientes para agregar equipos a la unidad organizativa (OU) especificada dentro del dominio AD.
Nombre NetBIOS del servidor CIFS	Nombre de servidor CIFS que es único en el dominio de AD.
Unidad organizacional	La unidad organizativa del dominio AD para asociarla con el servidor CIFS. El valor predeterminado es CN=Computers. Si configura Microsoft AD administrado de AWS como servidor AD para Cloud Volumes ONTAP, debe introducir **OU=equipos,OU=corp** en este campo.
Dominio DNS	El dominio DNS para la máquina virtual de almacenamiento (SVM) de Cloud Volumes ONTAP. En la mayoría de los casos, el dominio es el mismo que el dominio de AD.
Servidor NTP	Seleccione **usar dominio de Active Directory** para configurar un servidor NTP mediante el DNS de Active Directory. Si necesita configurar un servidor NTP con una dirección diferente, debe usar la API. Consulte "Guía para desarrolladores de API de Cloud Manager" para obtener más detalles.

15. **Perfil de uso, Tipo de disco y Directiva de organización en niveles**: Elija si desea activar las funciones de eficiencia del almacenamiento y editar la política de organización en niveles de volumen, si es necesario.

    Para obtener más información, consulte "Descripción de los perfiles de uso de volumen" y.. "Información general sobre organización en niveles de datos".

16. **revisar y aprobar**: Revise y confirme sus selecciones.
    a. Consulte los detalles de la configuración.
    b. Haga clic en **más información** para consultar detalles sobre el soporte técnico y los recursos de AWS que adquirirá Cloud Manager.
    c. Active las casillas de verificación **comprendo…**.
    d. Haga clic en **Ir**.

Resultado

Cloud Manager inicia la instancia de Cloud Volumes ONTAP. Puede realizar un seguimiento del progreso en la línea de tiempo.

Si tiene algún problema con el inicio de la instancia de Cloud Volumes ONTAP, revise el mensaje de error. También puede seleccionar el entorno de trabajo y hacer clic en Volver a crear entorno.

Para obtener más ayuda, vaya a. "Soporte Cloud Volumes ONTAP de NetApp".

Después de terminar

- Si ha aprovisionado un recurso compartido CIFS, proporcione permisos a usuarios o grupos a los archivos y carpetas y compruebe que esos usuarios pueden acceder al recurso compartido y crear un archivo.
- Si desea aplicar cuotas a los volúmenes, use System Manager o la interfaz de línea de comandos.

  Las cuotas le permiten restringir o realizar un seguimiento del espacio en disco y del número de archivos que usan un usuario, un grupo o un qtree.

Iniciar una pareja de alta disponibilidad de Cloud Volumes ONTAP en AWS

Si desea iniciar un par de alta disponibilidad de Cloud Volumes ONTAP en AWS, debe crear un entorno de trabajo de alta disponibilidad en Cloud Manager.

Antes de empezar

- Usted debe tener un "Conector asociado al área de trabajo".

  > Debe ser un administrador de cuentas para crear un conector. Al crear el primer entorno de trabajo de Cloud Volumes ONTAP, Cloud Manager le solicita que cree un conector si todavía no lo tiene.

- "Debe estar preparado para dejar el conector funcionando en en todo momento".
- Debe haberse preparado eligiendo una configuración y obteniendo información de red de AWS de su administrador. Para obtener más información, consulte "Planificación de la configuración de Cloud Volumes ONTAP".
- Si ha adquirido licencias BYOL, debe tener un número de serie (clave de licencia) de 20 dígitos para cada nodo.
- Si desea usar CIFS, debe haber configurado DNS y Active Directory. Para obtener más información, consulte "Requisitos de red para Cloud Volumes ONTAP en AWS".

Limitación

En este momento, no se admiten pares de alta disponibilidad con entradas externas de AWS.

Acerca de esta tarea

Inmediatamente después de crear el entorno de trabajo, Cloud Manager inicia una instancia de prueba en el VPC especificado para verificar la conectividad. Si se realiza correctamente, Cloud Manager finaliza inmediatamente la instancia y después inicia la implementación del sistema Cloud Volumes ONTAP. Si Cloud Manager no puede verificar la conectividad, se produce un error en la creación del entorno de trabajo. La instancia de prueba es t2.nano (para el tenancy por defecto de VPC) o m3.medium (para el uso dedicado de VPC).

Pasos

1. En la página entornos de trabajo, haga clic en **Agregar entorno de trabajo** y siga las indicaciones.
2. **Elija una ubicación**: Seleccione **Amazon Web Services** y **Cloud Volumes ONTAP Single Node**.
3. **Detalles y credenciales**: Si lo desea, puede cambiar las credenciales y la suscripción de AWS, introducir un nombre de entorno de trabajo, agregar etiquetas y, a continuación, introducir una contraseña.

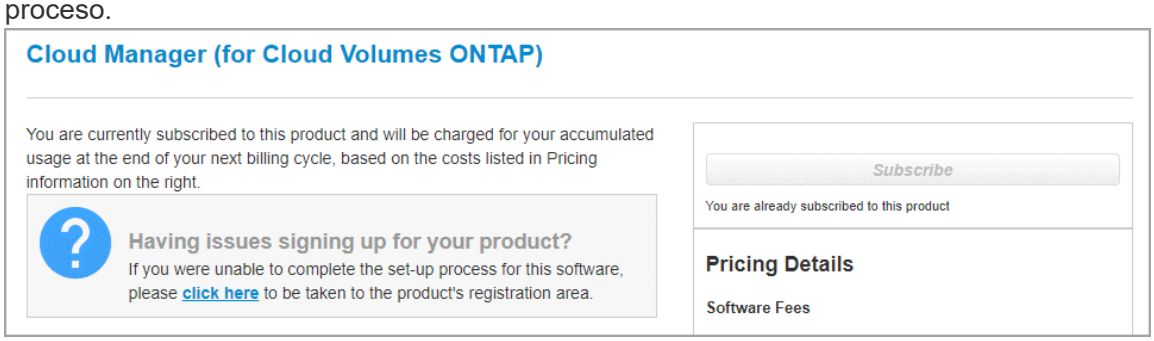
   Algunos de los campos en esta página son claros y explicativos. En la siguiente tabla se describen los campos que podrían presentar dificultades:

Campo	Descripción
Nombre del entorno de trabajo	Cloud Manager utiliza el nombre del entorno de trabajo para asignar un nombre tanto al sistema Cloud Volumes ONTAP como a la instancia de Amazon EC2. También utiliza el nombre como prefijo para el grupo de seguridad predefinido si selecciona esa opción.
Agregar etiquetas	Las etiquetas de AWS son metadatos para sus recursos de AWS. Cloud Manager agrega las etiquetas a la instancia de Cloud Volumes ONTAP y a cada recurso de AWS asociado con la instancia. Puede agregar hasta cuatro etiquetas desde la interfaz de usuario al crear un entorno de trabajo y, a continuación, puede agregar más después de crear. Tenga en cuenta que la API no le limita a cuatro etiquetas al crear un entorno de trabajo. Para obtener información sobre etiquetas, consulte "Documentación de AWS: Etiquetado de los recursos de Amazon EC2".
Nombre de usuario y contraseña	Estas son las credenciales de la cuenta de administrador del clúster de Cloud Volumes ONTAP. Puede usar estas credenciales para conectarse a Cloud Volumes ONTAP a través de OnCommand System Manager o de su CLI.
Editar credenciales	Elija las credenciales de AWS y la suscripción al mercado para utilizar con este sistema Cloud Volumes ONTAP. Haga clic en **Agregar suscripción** para asociar las credenciales seleccionadas a una suscripción. Para crear un sistema Cloud Volumes ONTAP de pago por uso, debe seleccionar las credenciales de AWS asociadas con una suscripción a Cloud Volumes ONTAP desde AWS Marketplace. Se le cobrará de esta suscripción por cada sistema Cloud Volumes ONTAP 9.6 y posterior de PAYGO que cree y cada función complementaria que habilite."Aprenda a añadir credenciales de AWS adicionales a Cloud Manager".

   En el siguiente vídeo se muestra cómo asociar una suscripción de pago por uso a Marketplace en sus credenciales de AWS:

   ► https://docs.netapp.com/es-es/occm38//media/video_subscribing_aws.mp4 *(video)*

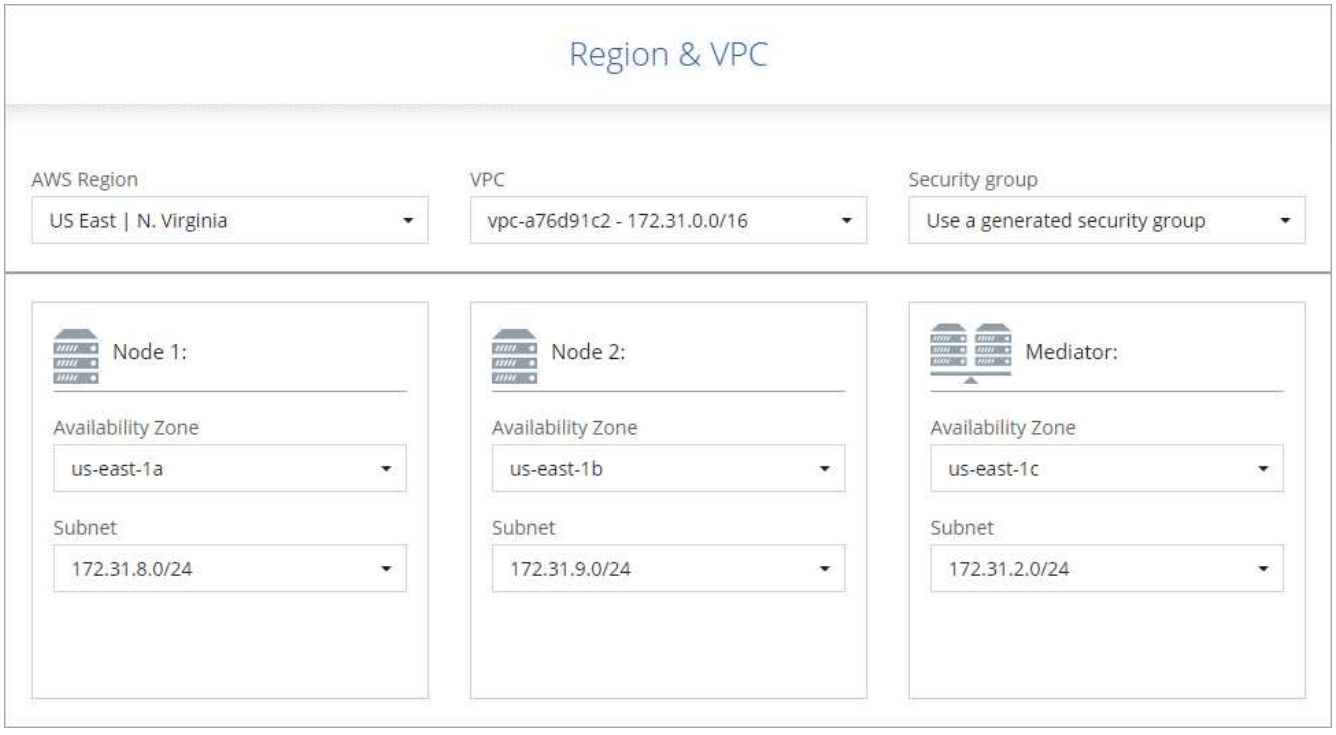
Si varios usuarios de IAM trabajan en la misma cuenta de AWS, cada usuario debe suscribirse. Una vez que el primer usuario se haya suscrito, AWS Marketplace informa a los usuarios posteriores de que ya están suscritos, tal como se muestra en la siguiente imagen. Mientras se ha establecido una suscripción para la cuenta *de AWS*, cada usuario de IAM debe asociarse a dicha suscripción. Si ve el mensaje que aparece a continuación, haga clic en el enlace **haga clic aquí** para ir a Cloud Central y completar el proceso.



4. **Servicios**: Mantenga activados o desactive los servicios individuales que no desea utilizar con este sistema Cloud Volumes ONTAP.
   - "Más información sobre Cloud Compliance".
   - "Más información sobre el backup en el cloud".
   - "Más información sobre la supervisión".
5. **modelos de implementación de alta disponibilidad**: Elija una configuración de alta disponibilidad.

   Para obtener información general sobre los modelos de puesta en marcha, consulte "Alta disponibilidad de Cloud Volumes ONTAP para AWS".
6. **Región y VPC**: Introduzca la información de red que ha grabado en la hoja de cálculo de AWS.

   La siguiente imagen muestra la página rellenada para una configuración de AZ múltiple:



7. **conectividad y autenticación SSH**: Elija los métodos de conexión para el par ha y el mediador.
8. **IP flotantes**: Si elige varios AZs, especifique las direcciones IP flotantes.

   Las direcciones IP deben estar fuera del bloque CIDR para todas las VPC de la región. Para obtener detalles adicionales, consulte "Requisitos de red de AWS para alta disponibilidad de Cloud Volumes ONTAP en múltiples AZS".

9. * tablas de rutas*: Si elige varios AZs, seleccione las tablas de rutas que deben incluir rutas a las direcciones IP flotantes.

   Si tiene más de una tabla de rutas, es muy importante seleccionar las tablas de rutas correctas. De lo contrario, es posible que algunos clientes no tengan acceso al par de alta disponibilidad de Cloud Volumes ONTAP. Para obtener más información sobre las tablas de rutas, consulte "Documentación de AWS: Tablas de rutas".

10. **cifrado de datos**: Elija sin cifrado de datos o cifrado gestionado por AWS.

    Para el cifrado gestionado por AWS, puede elegir una clave maestra de cliente (CMK) diferente de su cuenta u otra cuenta de AWS.

    No puede cambiar el método de cifrado de datos de AWS después de crear un sistema Cloud Volumes ONTAP.

    "Aprenda a configurar AWS KMS para el cloud Volumes ONTAP".

    "Obtenga más información sobre las tecnologías de cifrado compatibles".

11. **cuenta del sitio de soporte y licencia**: Indique si desea usar el modelo de pago por uso o con su licencia y, a continuación, especifique una cuenta del sitio de soporte de NetApp.

    Para comprender cómo funcionan las licencias, consulte "Licencia".

    Una cuenta del sitio de soporte de NetApp es opcional para el pago por uso, pero obligatoria para los sistemas BYOL. "Aprenda a añadir cuentas del sitio de soporte de NetApp".

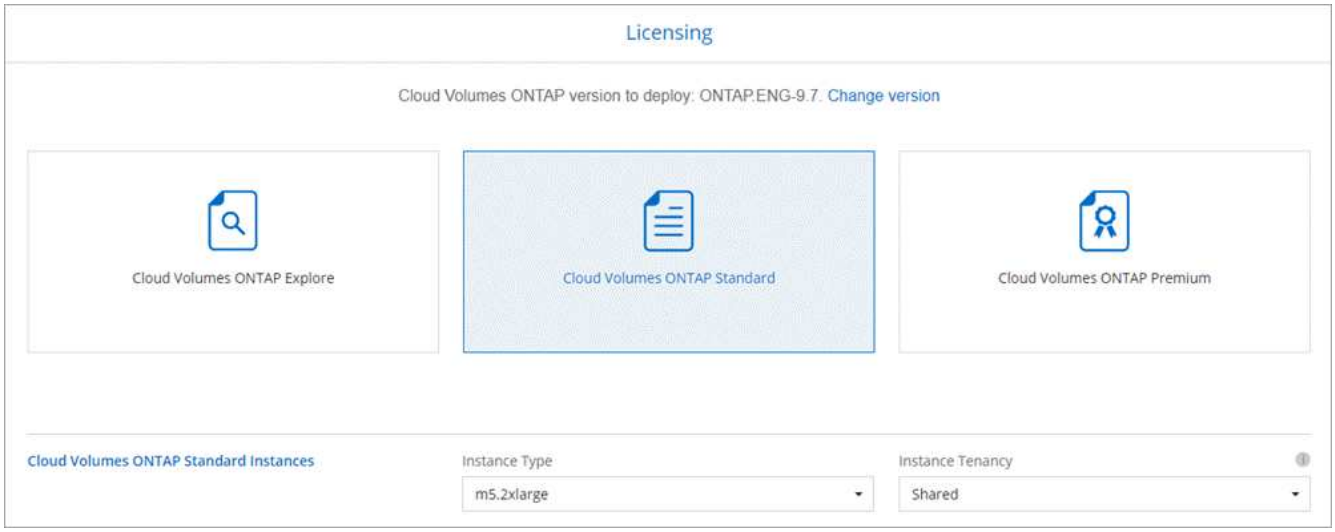
12. **Paquetes preconfigurados**: Seleccione uno de los paquetes para iniciar rápidamente un sistema Cloud Volumes ONTAP, o haga clic en **Crear mi propia configuración**.

    Si selecciona uno de los paquetes, solo tiene que especificar un volumen y, a continuación, revisar y aprobar la configuración.

13. **función IAM**: Debe mantener la opción predeterminada para que Cloud Manager pueda crear las funciones que le corresponde.

    Si prefiere utilizar su propia política, debe cumplirla "Requisitos normativos para los nodos Cloud Volumes ONTAP y la alta disponibilidad mediador".

14. **Licencia**: Cambie la versión de Cloud Volumes ONTAP según sea necesario, seleccione una licencia, un tipo de instancia y el uso de la instancia.



Si sus necesidades cambian después de iniciar las instancias, puede modificar la licencia o el tipo de instancia más adelante.

> Si hay disponible un candidato de versión, disponibilidad general o versión de revisión más reciente para la versión seleccionada, Cloud Manager actualiza el sistema a esa versión al crear el entorno de trabajo. Por ejemplo, la actualización se produce si selecciona Cloud Volumes ONTAP 9.6 RC1 y 9.6 GA está disponible. La actualización no se produce de una versión a otra; por ejemplo, de 9.6 a 9.7.

15. **Recursos de almacenamiento subyacentes**: Elija la configuración para el agregado inicial: Un tipo de disco, un tamaño para cada disco y si la organización en niveles de datos debe estar activada.

    Tenga en cuenta lo siguiente:

    - El tipo de disco es para el volumen inicial. Es posible seleccionar un tipo de disco diferente para volúmenes posteriores.
    - El tamaño de disco es para todos los discos del agregado inicial y para cualquier agregado adicional que Cloud Manager cree cuando utilice la opción de aprovisionamiento simple. Puede crear agregados que utilicen un tamaño de disco diferente mediante la opción de asignación avanzada.

      Para obtener ayuda a elegir el tipo y el tamaño de disco, consulte "Ajuste de tamaño de su sistema en AWS".

    - Se puede elegir una política de organización en niveles de volumen específica cuando se crea o se edita un volumen.
    - Si deshabilita la organización en niveles de datos, puede habilitarla en agregados posteriores.

      "Descubra cómo funciona la organización en niveles de datos".

16. **WORM**: Active el almacenamiento de escritura única y lectura múltiple (WORM), si lo desea.

    NO se puede habilitar WORM si la organización en niveles de datos está habilitada.

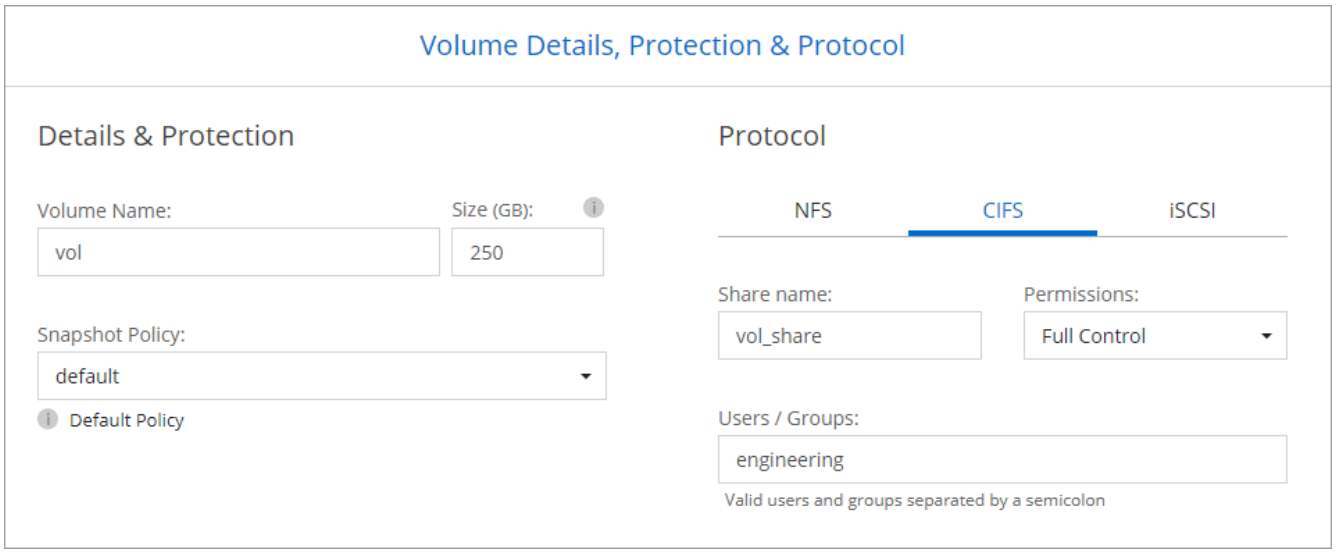
    "Más información acerca del almacenamiento WORM".

17. **Crear volumen**: Introduzca los detalles del nuevo volumen o haga clic en **Omitir**.

Algunos de los campos en esta página son claros y explicativos. En la siguiente tabla se describen los campos que podrían presentar dificultades:

Campo	Descripción
Tamaño	El tamaño máximo que puede introducir depende en gran medida de si habilita thin provisioning, lo que le permite crear un volumen que sea mayor que el almacenamiento físico que hay disponible actualmente.
Control de acceso (solo para NFS)	Una política de exportación define los clientes de la subred que pueden acceder al volumen. De forma predeterminada, Cloud Manager introduce un valor que proporciona acceso a todas las instancias de la subred.
Permisos y usuarios/grupos (solo para CIFS)	Estos campos permiten controlar el nivel de acceso a un recurso compartido para usuarios y grupos (también denominados listas de control de acceso o ACL). Es posible especificar usuarios o grupos de Windows locales o de dominio, o usuarios o grupos de UNIX. Si especifica un nombre de usuario de Windows de dominio, debe incluir el dominio del usuario con el formato domain\username.
Política de Snapshot	Una política de copia de Snapshot especifica la frecuencia y el número de copias de Snapshot de NetApp creadas automáticamente. Una copia snapshot de NetApp es una imagen del sistema de archivos puntual que no afecta al rendimiento y requiere un almacenamiento mínimo. Puede elegir la directiva predeterminada o ninguna. Es posible que no elija ninguno para los datos transitorios: Por ejemplo, tempdb para Microsoft SQL Server.
Opciones avanzadas (solo para NFS)	Seleccione una versión de NFS para el volumen: NFSv3 o NFSv4.
Grupo del iniciador y IQN (solo para iSCSI)	Los destinos de almacenamiento iSCSI se denominan LUN (unidades lógicas) y se presentan a los hosts como dispositivos de bloque estándar. Los iGroups son tablas de los nombres de los nodos de host iSCSI y controlan qué iniciadores tienen acceso a qué LUN. Los destinos iSCSI se conectan a la red a través de adaptadores de red Ethernet (NIC) estándar, tarjetas DEL motor de descarga TCP (TOE) con iniciadores de software, adaptadores de red convergente (CNA) o adaptadores de host de salida dedicados (HBA) y se identifican mediante nombres cualificados de iSCSI (IQN). Cuando se crea un volumen iSCSI, Cloud Manager crea automáticamente un LUN. Lo hemos hecho sencillo creando sólo una LUN por volumen, por lo que no hay que realizar ninguna gestión. Después de crear el volumen, "Utilice el IQN para conectarse con la LUN del hosts".

En la siguiente imagen, se muestra la página volumen rellenada para el protocolo CIFS:



18. **Configuración CIFS**: Si ha seleccionado el protocolo CIFS, configure un servidor CIFS.

Campo	Descripción
DNS Dirección IP principal y secundaria	Las direcciones IP de los servidores DNS que proporcionan resolución de nombres para el servidor CIFS. Los servidores DNS enumerados deben contener los registros de ubicación de servicio (SRV) necesarios para localizar los servidores LDAP de Active Directory y los controladores de dominio del dominio al que se unirá el servidor CIFS.
Dominio de Active Directory al que unirse	El FQDN del dominio de Active Directory (AD) al que desea que se una el servidor CIFS.
Credenciales autorizadas para unirse al dominio	Nombre y contraseña de una cuenta de Windows con privilegios suficientes para agregar equipos a la unidad organizativa (OU) especificada dentro del dominio AD.
Nombre NetBIOS del servidor CIFS	Nombre de servidor CIFS que es único en el dominio de AD.
Unidad organizacional	La unidad organizativa del dominio AD para asociarla con el servidor CIFS. El valor predeterminado es CN=Computers. Si configura Microsoft AD administrado de AWS como servidor AD para Cloud Volumes ONTAP, debe introducir **OU=equipos,OU=corp** en este campo.
Dominio DNS	El dominio DNS para la máquina virtual de almacenamiento (SVM) de Cloud Volumes ONTAP. En la mayoría de los casos, el dominio es el mismo que el dominio de AD.
Servidor NTP	Seleccione **usar dominio de Active Directory** para configurar un servidor NTP mediante el DNS de Active Directory. Si necesita configurar un servidor NTP con una dirección diferente, debe usar la API. Consulte "Guía para desarrolladores de API de Cloud Manager" para obtener más detalles.

19. **Perfil de uso, Tipo de disco y Directiva de organización en niveles**: Elija si desea activar las funciones de eficiencia del almacenamiento y editar la política de organización en niveles de volumen, si es necesario.

    Para obtener más información, consulte "Descripción de los perfiles de uso de volumen" y.. "Información general sobre organización en niveles de datos".

20. **revisar y aprobar**: Revise y confirme sus selecciones.
    a. Consulte los detalles de la configuración.
    b. Haga clic en **más información** para consultar detalles sobre el soporte técnico y los recursos de AWS que adquirirá Cloud Manager.
    c. Active las casillas de verificación **comprendo…**.
    d. Haga clic en **Ir**.

Resultado

Cloud Manager inicia el par de alta disponibilidad de Cloud Volumes ONTAP. Puede realizar un seguimiento del progreso en la línea de tiempo.

Si tiene algún problema con el inicio de la pareja de alta disponibilidad, revise el mensaje de error. También puede seleccionar el entorno de trabajo y hacer clic en Volver a crear entorno.

Para obtener más ayuda, vaya a. "Soporte Cloud Volumes ONTAP de NetApp".

Después de terminar

- Si ha aprovisionado un recurso compartido CIFS, proporcione permisos a usuarios o grupos a los archivos y carpetas y compruebe que esos usuarios pueden acceder al recurso compartido y crear un archivo.
- Si desea aplicar cuotas a los volúmenes, use System Manager o la interfaz de línea de comandos.

  Las cuotas le permiten restringir o realizar un seguimiento del espacio en disco y del número de archivos que usan un usuario, un grupo o un qtree.

Empiece a usar Azure

Introducción a Cloud Volumes ONTAP para Azure

Empiece a usar Cloud Volumes ONTAP para Azure en unos pasos.

Cree un conector

Si usted no tiene un "Conector" Sin embargo, un administrador de cuentas necesita crear uno. "Aprenda a crear un conector en Azure".

Al crear el primer entorno de trabajo de Cloud Volumes ONTAP, Cloud Manager le solicitará que implemente un conector si aún no lo tiene.

Planificación de la configuración

Cloud Manager ofrece paquetes preconfigurados que se ajustan a sus requisitos de carga de trabajo, o bien puede crear su propia configuración. Si elige su propia configuración, debe conocer las opciones disponibles. "Leer más".

Configure su red

1. Asegúrese de que vnet y las subredes admitan la conectividad entre el conector y Cloud Volumes ONTAP.
2. Habilite el acceso saliente a Internet desde la red virtual de destino para que el conector y Cloud Volumes ONTAP puedan ponerse en contacto con varios puntos finales.

   Este paso es importante porque el conector no puede administrar Cloud Volumes ONTAP sin acceso saliente a Internet. Si necesita limitar la conectividad saliente, consulte la lista de puntos finales para "El conector y Cloud Volumes ONTAP".

"Obtenga más información sobre los requisitos de red".

Inicie Cloud Volumes ONTAP mediante Cloud Manager

Haga clic en **Agregar entorno de trabajo**, seleccione el tipo de sistema que desea implementar y complete los pasos del asistente. "Lea las instrucciones paso a paso".

Enlaces relacionados

- "Evaluación"
- "Creación de un conector desde Cloud Manager"
- "Creación de un conector desde Azure Marketplace"
- "Instalar el software del conector en un host Linux"
- "Qué hace Cloud Manager con permisos de Azure"

Planificar la configuración de Cloud Volumes ONTAP en Azure

Al poner en marcha Cloud Volumes ONTAP en Azure, puede elegir un sistema preconfigurado que se ajuste a los requisitos de la carga de trabajo, o bien puede crear su propia configuración. Si elige su propia configuración, debe conocer las opciones disponibles.

Seleccione un tipo de licencia

Cloud Volumes ONTAP está disponible en dos opciones de precios: De pago por uso y con su propia licencia (BYOL). En el modelo de pago por uso, puede elegir entre tres licencias: Explorar, Standard o Premium. Cada licencia proporciona distintas opciones de computación y capacidad.

"Configuraciones compatibles para Cloud Volumes ONTAP 9.7 en Azure"

Comprender los límites de almacenamiento

El límite de capacidad bruta de un sistema de Cloud Volumes ONTAP está relacionado con la licencia. Los límites adicionales afectan al tamaño de los agregados y los volúmenes. Debe conocer estos límites a medida que planifique la configuración.

"Límites de almacenamiento para Cloud Volumes ONTAP 9.7 en Azure"

Ajuste de tamaño de su sistema en Azure

Configurar el tamaño de su sistema Cloud Volumes ONTAP puede ayudarle a cumplir los requisitos de rendimiento y capacidad. Al elegir un tipo de máquina virtual, un tipo de disco y un tamaño de disco, es necesario tener en cuenta algunos puntos clave:

Tipo de máquina virtual

Observe los tipos de máquina virtual admitidos en la "Notas de la versión de Cloud Volumes ONTAP" Y, a continuación, revise los detalles sobre cada tipo de máquina virtual admitido. Tenga en cuenta que cada tipo de máquina virtual admite un número específico de discos de datos.

- "Documentación de Azure: Tamaños de máquinas virtuales de uso general"
- "Documentación de Azure: Tamaños de máquinas virtuales optimizadas con memoria"

Tipo de disco de Azure

Cuando crea volúmenes para Cloud Volumes ONTAP, debe elegir el almacenamiento en cloud subyacente que Cloud Volumes ONTAP utiliza como disco.

Los sistemas HA utilizan Blobs de página Premium. Mientras tanto, los sistemas de un solo nodo pueden usar dos tipos de discos gestionados de Azure:

- *Premium SSD Managed Disks* proporciona un alto rendimiento para cargas de trabajo con un gran volumen de I/o a un coste más elevado.
- *Standard SSD Managed Disks* proporciona un rendimiento constante para cargas de trabajo que requieren un bajo nivel de IOPS.
- *Standard HDD Managed Disks* es una buena opción si no necesita un alto nivel de IOPS y desea reducir sus costes.

  Si quiere más información sobre los casos de uso de estos discos, consulte "Documentación de Microsoft Azure: ¿qué tipos de discos están disponibles en Azure?".

Tamaño de disco de Azure

Al iniciar las instancias de Cloud Volumes ONTAP, debe elegir el tamaño de disco predeterminado para los agregados. Cloud Manager utiliza este tamaño de disco para el agregado inicial y para cualquier agregado adicional que cree cuando utilice la opción de aprovisionamiento simple. Puede crear agregados con un tamaño de disco diferente desde el valor predeterminado por "mediante la opción de asignación avanzada".

Todos los discos de un agregado deben tener el mismo tamaño.

Al elegir un tamaño de disco, se deben tener en cuenta varios factores. El tamaño del disco afecta a la cantidad de almacenamiento que se paga, el tamaño de los volúmenes que se pueden crear en un agregado, la capacidad total disponible para Cloud Volumes ONTAP y el rendimiento del almacenamiento.

El rendimiento del almacenamiento Premium de Azure está ligado al tamaño del disco. Los discos más grandes permiten mejorar la tasa de IOPS y el rendimiento. Por ejemplo, elegir discos de 1 TB puede proporcionar un mejor rendimiento que los discos de 500 GB a un coste mayor.

No existen diferencias de rendimiento entre los tamaños de disco para Standard Storage. Debe elegir el tamaño del disco en función de la capacidad que necesite.

Consulte Azure para obtener información sobre IOPS y rendimiento por tamaño de disco:

- "Microsoft Azure: Precios de discos gestionados"
- "Microsoft Azure: Precios para Blobs de página"

Elegir una configuración compatible con Flash Cache

Una configuración de Cloud Volumes ONTAP en Azure incluye almacenamiento NVMe local, que Cloud Volumes ONTAP utiliza como *Flash Cache* para mejorar el rendimiento. "Obtenga más información sobre Flash Cache".

Hoja de trabajo de información de red de Azure

Al implementar Cloud Volumes ONTAP en Azure, tiene que especificar detalles acerca de su red virtual. Puede utilizar una hoja de cálculo para recopilar la información del administrador.

Información de Azure	Su valor
Región	
Red virtual (vnet)	
Subred	
Grupo de seguridad de red (si utiliza el suyo propio)	

Elegir una velocidad de escritura

Cloud Manager le permite elegir una configuración de velocidad de escritura para sistemas Cloud Volumes ONTAP de un solo nodo. Antes de elegir una velocidad de escritura, debe comprender las diferencias entre la configuración normal y la alta, así como los riesgos y recomendaciones cuando utilice la alta velocidad de escritura.

Diferencia entre la velocidad de escritura normal y la alta velocidad de escritura

Al elegir la velocidad de escritura normal, los datos se escriben directamente en el disco, lo que reduce la probabilidad de que se pierdan los datos en caso de que se produzca una interrupción del servicio no planificada del sistema.

Al elegir una alta velocidad de escritura, los datos se guardan en búfer en la memoria antes de que se escriban en el disco, lo que proporciona un rendimiento de escritura más rápido. Gracias al almacenamiento en caché, existe la posibilidad de perder datos en caso de que se produzca una interrupción no planificada del sistema.

La cantidad de datos que se pueden perder en caso de una interrupción imprevista del sistema es el plazo de dos últimos puntos de coherencia. Un punto de coherencia es el acto de escribir datos en el búfer en el disco. Un punto de coherencia se produce cuando el registro de escritura está completo o después de 10 segundos (lo que ocurra primero). Sin embargo, el rendimiento del volumen de AWS EBS puede afectar el tiempo de procesamiento del punto de consistencia.

Cuándo utilizar alta velocidad de escritura

La alta velocidad de escritura es una buena opción si es necesario un rendimiento de escritura rápido para su carga de trabajo, y puede resistir el riesgo de pérdida de datos en caso de una interrupción del servicio del sistema no planificada.

Recomendaciones cuando se utiliza una alta velocidad de escritura

Si habilita una alta velocidad de escritura, debe garantizar la protección de escritura en la capa de la aplicación.

Selección de un perfil de uso de volumen

ONTAP incluye varias funciones de eficiencia del almacenamiento que pueden reducir la cantidad total de almacenamiento que necesita. Al crear un volumen en Cloud Manager, puede seleccionar un perfil que habilite estas funciones o un perfil que las deshabilite. Debe obtener más información sobre estas funciones para ayudarle a decidir qué perfil utilizar.

Las funciones de eficiencia del almacenamiento de NetApp ofrecen las siguientes ventajas:

Aprovisionamiento ligero
: Presenta más almacenamiento lógico a hosts o usuarios del que realmente hay en el pool de almacenamiento físico. En lugar de asignar previamente espacio de almacenamiento, el espacio de almacenamiento se asigna de forma dinámica a cada volumen a medida que se escriben los datos.

Deduplicación
: Mejora la eficiencia al localizar bloques de datos idénticos y sustituirlos con referencias a un único bloque compartido. Esta técnica reduce los requisitos de capacidad de almacenamiento al eliminar los bloques de datos redundantes que se encuentran en un mismo volumen.

Compresión
: Reduce la capacidad física requerida para almacenar datos al comprimir los datos de un volumen en almacenamiento primario, secundario y de archivado.

Requisitos de red para poner en marcha y gestionar Cloud Volumes ONTAP en Azure

Configure sus redes de Azure para que los sistemas Cloud Volumes ONTAP funcionen correctamente. Esto incluye la conexión a redes para el conector y Cloud Volumes ONTAP.

Requisitos para Cloud Volumes ONTAP

Los siguientes requisitos de red deben satisfacerse en Azure.

Acceso saliente a Internet para Cloud Volumes ONTAP
: Cloud Volumes ONTAP requiere acceso saliente a Internet para enviar mensajes a NetApp AutoSupport, que supervisa proactivamente el estado del almacenamiento.

  Las políticas de enrutamiento y firewall deben permitir el tráfico HTTP/HTTPS a los siguientes extremos para que Cloud Volumes ONTAP pueda enviar mensajes de AutoSupport:

  - https://support.netapp.com/aods/asupmessage
  - https://support.netapp.com/asupprod/post/1.0/postAsup

    "Aprenda a configurar AutoSupport".

Grupos de seguridad

No necesita crear grupos de seguridad porque Cloud Manager lo hace por usted. Si necesita utilizar el suyo propio, consulte las reglas de grupo de seguridad que se enumeran a continuación.

Número de direcciones IP

Cloud Manager asigna el siguiente número de direcciones IP a Cloud Volumes ONTAP en Azure:

- Nodo único: Direcciones IP de 5
- Par DE ALTA DISPONIBILIDAD: 16 direcciones IP

Tenga en cuenta que Cloud Manager crea una LIF de gestión de SVM en parejas de alta disponibilidad, pero no en sistemas de un único nodo en Azure.

Una LIF es una dirección IP asociada con un puerto físico. Se requiere una LIF de gestión de SVM para herramientas de gestión como SnapCenter.

Conexión de Cloud Volumes ONTAP a Azure Blob Storage para organización en niveles de los datos

Si desea organizar en niveles datos fríos en almacenamiento de Azure Blob, no necesita configurar una conexión entre el nivel de rendimiento y el nivel de capacidad mientras Cloud Manager tenga los permisos necesarios Cloud Manager habilita un extremo de servicio vnet para usted si la política de Cloud Manager tiene estos permisos:

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

Estos permisos se incluyen en el último "Política de Cloud Manager".

Para obtener más información sobre la configuración de la organización en niveles de datos, consulte "Organización en niveles de los datos inactivos en almacenamiento de objetos de bajo coste".

Conexiones a sistemas ONTAP en otras redes

Para replicar datos entre un sistema Cloud Volumes ONTAP en Azure y sistemas ONTAP en otras redes, debe tener una conexión VPN entre el vnet de Azure y la otra red, por ejemplo, un VPC de AWS o una red de su empresa.

Para obtener instrucciones, consulte "Documentación de Microsoft Azure: Cree una conexión de sitio a sitio en el portal de Azure".

Requisitos para el conector

Configure su red de modo que el conector pueda gestionar recursos y procesos en su entorno de cloud público. El paso más importante es garantizar el acceso saliente a Internet a varios puntos finales.

Si la red utiliza un servidor proxy para toda la comunicación a Internet, puede especificar el servidor proxy en la página Configuración. Consulte "Configuración del conector para utilizar un servidor proxy".

Conexiones a redes de destino

Un conector requiere una conexión de red a los VPC y VNets en los que desea implementar Cloud Volumes

ONTAP.

Por ejemplo, si instala un conector en la red corporativa, debe configurar una conexión VPN al VPC o a vnet en el que inicie Cloud Volumes ONTAP.

Acceso a Internet de salida

El conector requiere acceso saliente a Internet para gestionar recursos y procesos dentro de su entorno de nube pública. Un conector se pone en contacto con los siguientes extremos al gestionar recursos en Azure:

Puntos finales	Específico
https://management.azure.com https://login.microsoftonline.com	Permite que Cloud Manager ponga en marcha y gestione Cloud Volumes ONTAP en la mayoría de las regiones de Azure.
https://management.microsoftazure.de https://login.microsoftonline.de	Permite que Cloud Manager ponga en marcha y gestione Cloud Volumes ONTAP en las regiones de Azure Alemania.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Permite a Cloud Manager implementar y gestionar Cloud Volumes ONTAP en las regiones de Azure US Gov.
https://api.services.cloud.netapp.com:443	Solicitudes de API a Cloud Central de NetApp.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Proporciona acceso a imágenes, manifiestos y plantillas de software.
https://repo.cloud.support.netapp.com	Se utiliza para descargar las dependencias de Cloud Manager.
http://repo.mysql.com/	Se utiliza para descargar MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Permite a Cloud Manager acceder y descargar manifiestos, plantillas e imágenes de actualización de Cloud Volumes ONTAP.
https://cloudmanagerinfraprod.azurecr.io	Acceso a imágenes de software de componentes de contenedor para una infraestructura que ejecuta Docker y proporciona una solución para las integraciones de servicios con Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Permite a NetApp transmitir datos desde registros de auditoría.
https://cloudmanager.cloud.netapp.com	Comunicación con el servicio Cloud Manager, que incluye cuentas de Cloud Central.
https://netapp-cloud-account.auth0.com	Comunicación con Cloud Central de NetApp para la autenticación de usuario centralizada.
https://mysupport.netapp.com	Comunicación con AutoSupport de NetApp.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Comunicación con NetApp para la licencia del sistema y el registro de soporte.

Puntos finales	Específico
https://ipa-signer.cloudmanager.netapp.com	Permite que Cloud Manager genere licencias (por ejemplo, una licencia de FlexCache para Cloud Volumes ONTAP).
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Necesario para conectar los sistemas Cloud Volumes ONTAP con un clúster de Kubernetes. Los extremos permiten la instalación de Trident de NetApp.
*.blob.core.windows.net	Necesario para pares de alta disponibilidad cuando se utiliza un proxy.
Diversas ubicaciones de terceros, por ejemplo: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org Las ubicaciones de terceros están sujetas a cambios.	Durante las actualizaciones, Cloud Manager descarga los paquetes más recientes para dependencias de terceros.

Aunque debe realizar casi todas las tareas desde la interfaz de usuario de SaaS, todavía hay disponible una interfaz de usuario local en el conector. La máquina que ejecuta el explorador Web debe tener conexiones con los siguientes puntos finales:

Puntos finales	Específico
El host del conector	Debe introducir la dirección IP del host desde un explorador web para cargar la consola de Cloud Manager. Según su conectividad con el proveedor de cloud, puede usar la IP privada o una IP pública asignada al host: • Una IP privada funciona si dispone de una VPN y. acceso directo a la red virtual • Una IP pública funciona en cualquier situación de red En cualquier caso, debe proteger el acceso a la red garantizando que las reglas de grupo de seguridad permiten el acceso sólo desde IP o subredes autorizadas.
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	El explorador web se conecta con estos extremos para conseguir una autenticación de usuario centralizada mediante NetApp Cloud Central.
https://widget.intercom.io	Si busca un chat integrado en los productos que le permita hablar con expertos en cloud de NetApp.

Reglas de grupo de seguridad para Cloud Volumes ONTAP

Cloud Manager crea grupos de seguridad de Azure que incluyen las reglas de entrada y salida que Cloud Volumes ONTAP necesita para funcionar correctamente. Tal vez desee consultar los puertos para fines de prueba o si prefiere utilizar sus propios grupos de seguridad.

El grupo de seguridad para Cloud Volumes ONTAP requiere reglas tanto entrantes como salientes.

Reglas de entrada para sistemas de un solo nodo

Las reglas que se enumeran a continuación permiten el tráfico, a menos que la descripción indique que bloquea el tráfico entrante específico.

Prioridad y nombre	Puerto y protocolo	Origen y destino	Descripción
1000 inbound_ssh	22 TCP	De cualquiera a cualquiera	Acceso SSH a la dirección IP de administración del clúster LIF o una LIF de gestión de nodos
1001 inbound_http	80 TCP	De cualquiera a cualquiera	Acceso HTTP a la consola web de System Manager mediante el La dirección IP de la LIF de gestión del clúster
1002 inbound_111_tcp	111 TCP	De cualquiera a cualquiera	Llamada a procedimiento remoto para NFS
1003 inbound_111_udp	111 UDP	De cualquiera a cualquiera	Llamada a procedimiento remoto para NFS
1004 inbound_139	139 TCP	De cualquiera a cualquiera	Sesión de servicio NetBIOS para CIFS
1005 inbound_161-162 _tcp	161-162 TCP	De cualquiera a cualquiera	Protocolo simple de gestión de red
1006 inbound_161-162 _udp	161-162 UDP	De cualquiera a cualquiera	Protocolo simple de gestión de red
1007 inbound_443	443 TCP	De cualquiera a cualquiera	Acceso HTTPS a la consola web de System Manager mediante el La dirección IP de la LIF de gestión del clúster
1008 inbound_445	445 TCP	De cualquiera a cualquiera	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
1009 inbound_635_tcp	635 TCP	De cualquiera a cualquiera	Montaje NFS
1010 inbound_635_udp	635 UDP	De cualquiera a cualquiera	Montaje NFS
1011 inbound_749	749 TCP	De cualquiera a cualquiera	Kerberos

Prioridad y nombre	Puerto y protocolo	Origen y destino	Descripción
1012 inbound_2049_tcp	2049 TCP	De cualquiera a cualquiera	Daemon del servidor NFS
1013 inbound_2049_udp	2049 UDP	De cualquiera a cualquiera	Daemon del servidor NFS
1014 inbound_3260	3260 TCP	De cualquiera a cualquiera	Acceso iSCSI mediante la LIF de datos iSCSI
1015 inbound_4045-4046_tcp	4045-4046 TCP	De cualquiera a cualquiera	Daemon de bloqueo NFS y monitor de estado de red
1016 inbound_4045-4046_udp	4045-4046 UDP	De cualquiera a cualquiera	Daemon de bloqueo NFS y monitor de estado de red
1017 inbound_10000	10000 TCP	De cualquiera a cualquiera	Backup con NDMP
1018 inbound_11104-11105	11104-11105 TCP	De cualquiera a cualquiera	Transferencia de datos de SnapMirror
3000 inbound_deny _all_tcp	Cualquier puerto TCP	De cualquiera a cualquiera	Bloquear el resto del tráfico entrante TCP
3001 inbound_deny _all_udp	Cualquier puerto UDP	De cualquiera a cualquiera	Bloquee el resto del tráfico de entrada UDP
65000 AllowVnetInBound	Cualquier protocolo	VirtualNetwork para VirtualNetwork	Tráfico entrante desde dentro del vnet
65001 AllowAzureLoad Balance InBound	Cualquier protocolo	AzureLoadBalancer a cualquiera	Tráfico de datos del balanceador de carga estándar de Azure
65500 DenyAllInBound	Cualquier protocolo	De cualquiera a cualquiera	Bloquear el resto del tráfico entrante

Reglas de entrada para sistemas de alta disponibilidad

Las reglas que se enumeran a continuación permiten el tráfico, a menos que la descripción indique que bloquea el tráfico entrante específico.

> Los sistemas de ALTA DISPONIBILIDAD tienen menos reglas entrantes que los sistemas de un solo nodo, porque el tráfico de datos entrantes pasa por el balanceador de carga estándar de Azure. Debido a esto, el tráfico del equilibrador de carga debe estar abierto, como se muestra en la regla "AllowAzureLoadBalance InBound".

Prioridad y nombre	Puerto y protocolo	Origen y destino	Descripción
100 inbound_443	443 cualquier protocolo	De cualquiera a cualquiera	Acceso HTTPS a la consola web de System Manager mediante el La dirección IP de la LIF de gestión del clúster

Prioridad y nombre	Puerto y protocolo	Origen y destino	Descripción
101 inbound_111_tcp	111 cualquier protocolo	De cualquiera a cualquiera	Llamada a procedimiento remoto para NFS
102 inbound_2049_tcp	2049 cualquier protocolo	De cualquiera a cualquiera	Daemon del servidor NFS
111 inbound_ssh	22 cualquier protocolo	De cualquiera a cualquiera	Acceso SSH a la dirección IP de administración del clúster LIF o una LIF de gestión de nodos
121 inbound_53	53 cualquier protocolo	De cualquiera a cualquiera	DNS y CIFS
65000 AllowVnetInBound	Cualquier protocolo	VirtualNetwork para VirtualNetwork	Tráfico entrante desde dentro del vnet
65001 AllowAzureLoad Balance InBound	Cualquier protocolo	AzureLoadBalancer a cualquiera	Tráfico de datos del balanceador de carga estándar de Azure
65500 DenyAllInBound	Cualquier protocolo	De cualquiera a cualquiera	Bloquear el resto del tráfico entrante

Reglas de salida

El grupo de seguridad predefinido para Cloud Volumes ONTAP abre todo el tráfico saliente. Si eso es aceptable, siga las reglas básicas de la salida. Si necesita más reglas rígidas, utilice las reglas avanzadas de salida.

Reglas de salida básicas

El grupo de seguridad predefinido para Cloud Volumes ONTAP incluye las siguientes reglas de salida.

Puerto	Protocolo	Específico
Todo	Todos los TCP	Todo el tráfico saliente
Todo	Todas las UDP	Todo el tráfico saliente

Reglas salientes avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede utilizar la siguiente información para abrir sólo los puertos necesarios para la comunicación saliente por Cloud Volumes ONTAP.

El origen es la interfaz (dirección IP) en el sistema Cloud Volumes ONTAP.

Servicio	Puerto	Protocolo	Origen	Destino	Específico
Active Directory	88	TCP	LIF de gestión de nodos	Bosque de Active Directory	Autenticación Kerberos V.
	137	UDP	LIF de gestión de nodos	Bosque de Active Directory	Servicio de nombres NetBIOS
	138	UDP	LIF de gestión de nodos	Bosque de Active Directory	Servicio de datagramas NetBIOS
	139	TCP	LIF de gestión de nodos	Bosque de Active Directory	Sesión de servicio NetBIOS
	389	TCP Y UDP	LIF de gestión de nodos	Bosque de Active Directory	LDAP
	445	TCP	LIF de gestión de nodos	Bosque de Active Directory	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
	464	TCP	LIF de gestión de nodos	Bosque de Active Directory	Kerberos V cambiar y establecer contraseña (SET_CHANGE)
	464	UDP	LIF de gestión de nodos	Bosque de Active Directory	Administración de claves Kerberos
	749	TCP	LIF de gestión de nodos	Bosque de Active Directory	Contraseña de Kerberos V Change & Set (RPCSEC_GSS)
	88	TCP	LIF de datos (NFS, CIFS e iSCSI)	Bosque de Active Directory	Autenticación Kerberos V.
	137	UDP	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Servicio de nombres NetBIOS
	138	UDP	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Servicio de datagramas NetBIOS
	139	TCP	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Sesión de servicio NetBIOS
	389	TCP Y UDP	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	LDAP
	445	TCP	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
	464	TCP	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Kerberos V cambiar y establecer contraseña (SET_CHANGE)
	464	UDP	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Administración de claves Kerberos
	749	TCP	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Contraseña de Kerberos V change & set (RPCSEC_GSS)
DHCP	68	UDP	LIF de gestión de nodos	DHCP	Cliente DHCP para la configuración inicial

Servicio	Puerto	Protocolo	Origen	Destino	Específico
DHCPS	67	UDP	LIF de gestión de nodos	DHCP	Servidor DHCP
DNS	53	UDP	LIF de gestión de nodos y LIF de datos (NFS, CIFS)	DNS	DNS
NDMP	18600–18699	TCP	LIF de gestión de nodos	Servidores de destino	Copia NDMP
SMTP	25	TCP	LIF de gestión de nodos	Servidor de correo	Alertas SMTP, que se pueden utilizar para AutoSupport
SNMP	161	TCP	LIF de gestión de nodos	Servidor de supervisión	Supervisión mediante capturas SNMP
	161	UDP	LIF de gestión de nodos	Servidor de supervisión	Supervisión mediante capturas SNMP
	162	TCP	LIF de gestión de nodos	Servidor de supervisión	Supervisión mediante capturas SNMP
	162	UDP	LIF de gestión de nodos	Servidor de supervisión	Supervisión mediante capturas SNMP
SnapMirror	11104	TCP	LIF entre clústeres	LIF de interconexión de clústeres de ONTAP	Gestión de sesiones de comunicación de interconexión de clústeres para SnapMirror
	11105	TCP	LIF entre clústeres	LIF de interconexión de clústeres de ONTAP	Transferencia de datos de SnapMirror
Syslog	514	UDP	LIF de gestión de nodos	Servidor de syslog	Mensajes de syslog Reenviar

Reglas de grupo de seguridad para el conector

El grupo de seguridad del conector requiere reglas entrantes y salientes.

Reglas de entrada

El origen de las reglas entrantes en el grupo de seguridad predefinido es 0.0.0.0/0.

Puerto	Protocolo	Específico
22	SSH	Proporciona acceso SSH al host de Connector
80	HTTP	Proporciona acceso HTTP desde navegadores web de cliente al local interfaz de usuario

Puerto	Protocolo	Específico
443	HTTPS	Proporciona acceso HTTPS desde exploradores web de cliente al local interfaz de usuario

Reglas de salida

El grupo de seguridad predefinido para el conector abre todo el tráfico saliente. Si eso es aceptable, siga las reglas básicas de la salida. Si necesita más reglas rígidas, utilice las reglas avanzadas de salida.

Reglas de salida básicas

El grupo de seguridad predefinido para el conector incluye las siguientes reglas de salida.

Puerto	Protocolo	Específico
Todo	Todos los TCP	Todo el tráfico saliente
Todo	Todas las UDP	Todo el tráfico saliente

Reglas salientes avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede utilizar la siguiente información para abrir sólo los puertos necesarios para la comunicación saliente por parte del conector.

La dirección IP de origen es el host del conector.

Servicio	Puerto	Protocolo	Destino	Específico
Active Directory	88	TCP	Bosque de Active Directory	Autenticación Kerberos V.
	139	TCP	Bosque de Active Directory	Sesión de servicio NetBIOS
	389	TCP	Bosque de Active Directory	LDAP
	445	TCP	Bosque de Active Directory	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
	464	TCP	Bosque de Active Directory	Kerberos V cambiar y establecer contraseña (SET_CHANGE)
	749	TCP	Bosque de Active Directory	Contraseña de modificación y definición de Kerberos V de Active Directory (RPCSEC_GSS)
	137	UDP	Bosque de Active Directory	Servicio de nombres NetBIOS
	138	UDP	Bosque de Active Directory	Servicio de datagramas NetBIOS
	464	UDP	Bosque de Active Directory	Administración de claves Kerberos
Llamadas API y AutoSupport	443	HTTPS	LIF de gestión de clústeres de ONTAP y Internet saliente	API llama a AWS y ONTAP y envía mensajes de AutoSupport a NetApp
Llamadas API	3000	TCP	LIF de gestión de clústeres de ONTAP	Llamadas API a ONTAP
DNS	53	UDP	DNS	Utilizado para resolver DNS por Cloud Manager

Inicio de Cloud Volumes ONTAP en Azure

Puede iniciar un sistema de un solo nodo o un par de alta disponibilidad en Azure mediante la creación de un entorno de trabajo de Cloud Volumes ONTAP en Cloud Manager.

Antes de empezar

- Usted debe tener un "Conector asociado al área de trabajo".

> Debe ser un administrador de cuentas para crear un conector. Al crear el primer entorno de trabajo de Cloud Volumes ONTAP, Cloud Manager le solicita que cree un conector si todavía no lo tiene.

- "Debe estar preparado para dejar el conector funcionando en en todo momento".
- Debe haber elegido una configuración y obtener información de redes de Azure de su administrador. Para obtener más información, consulte "Planificación de la configuración de Cloud Volumes ONTAP".
- Para poner en marcha un sistema BYOL, necesita el número de serie (clave de licencia) de 20 dígitos para cada nodo.

Acerca de esta tarea

Cuando Cloud Manager crea un sistema Cloud Volumes ONTAP en Azure, crea varios objetos de Azure, como un grupo de recursos, interfaces de red y cuentas de almacenamiento. Puede revisar un resumen de los recursos al final del asistente.

> **Potencial de pérdida de datos**
>
> No se recomienda la implementación de Cloud Volumes ONTAP en un grupo de recursos compartidos existente debido al riesgo de pérdida de datos. Mientras que la reversión está deshabilitada de forma predeterminada cuando se usa la API para implementar en un grupo de recursos existente, la eliminación de Cloud Volumes ONTAP potencialmente elimina otros recursos de ese grupo compartido.
>
> La mejor práctica es utilizar un nuevo grupo de recursos dedicado para Cloud Volumes ONTAP. Esta es la opción predeterminada y solo recomendada cuando implemente Cloud Volumes ONTAP en Azure desde Cloud Manager.

Pasos

1. En la página entornos de trabajo, haga clic en **Agregar entorno de trabajo** y siga las indicaciones.
2. **Elija una ubicación**: Seleccione **Microsoft Azure** y **Cloud Volumes ONTAP Single Node** o **Cloud Volumes ONTAP High Availability**.
3. **Detalles y credenciales**: De forma opcional, cambie las credenciales y la suscripción de Azure, especifique un nombre de clúster y un nombre de grupo de recursos, añada etiquetas si es necesario y, a continuación, especifique credenciales.

   En la siguiente tabla se describen los campos que podrían presentar dificultades:

Campo	Descripción
Nombre del entorno de trabajo	Cloud Manager utiliza el nombre de entorno de trabajo para nombrar tanto el sistema Cloud Volumes ONTAP como la máquina virtual de Azure. También utiliza el nombre como prefijo para el grupo de seguridad predefinido si selecciona esa opción.

Campo	Descripción
Nombre del grupo de recursos	Conserve el nombre predeterminado para el nuevo grupo de recursos o desactive **Use Default** e introduzca su propio nombre para el nuevo grupo de recursos. La mejor práctica es utilizar un nuevo grupo de recursos dedicado para Cloud Volumes ONTAP. Aunque es posible implementar Cloud Volumes ONTAP en un grupo de recursos compartidos existente mediante la API, no se recomienda debido al riesgo de pérdida de datos. Consulte la advertencia anterior para obtener más detalles.
Etiquetas	Las etiquetas son metadatos para sus recursos de Azure. Cuando introduce etiquetas en este campo, Cloud Manager las añade al grupo de recursos asociado con el sistema Cloud Volumes ONTAP. Puede agregar hasta cuatro etiquetas desde la interfaz de usuario al crear un entorno de trabajo y, a continuación, puede agregar más después de crear. Tenga en cuenta que la API no le limita a cuatro etiquetas al crear un entorno de trabajo. Para obtener información sobre etiquetas, consulte "Documentación de Microsoft Azure: Uso de etiquetas para organizar los recursos de Azure".
Nombre de usuario y contraseña	Estas son las credenciales de la cuenta de administrador del clúster de Cloud Volumes ONTAP. Puede usar estas credenciales para conectarse a Cloud Volumes ONTAP a través de OnCommand System Manager o de su CLI.
Editar credenciales	Puede elegir diferentes credenciales de Azure y una suscripción de Azure diferente para utilizarlo con este sistema de Cloud Volumes ONTAP. Tiene que asociar una suscripción a Azure Marketplace con la suscripción de Azure seleccionada para poner en marcha un sistema Cloud Volumes ONTAP de pago por uso. "Aprenda a añadir credenciales".

En el siguiente vídeo se muestra cómo asociar una suscripción de Marketplace a una suscripción de Azure:

► https://docs.netapp.com/es-es/occm38//media/video_subscribing_azure.mp4 *(video)*

4. **Servicios**: Mantenga activados los servicios o desactive los servicios individuales que no desea utilizar con Cloud Volumes ONTAP.
   - "Más información sobre Cloud Compliance".
   - "Más información sobre el backup en el cloud".
5. **Ubicación y conectividad**: Seleccione una ubicación y un grupo de seguridad y active la casilla de verificación para confirmar la conectividad de red entre Cloud Manager y la ubicación de destino.
6. **cuenta del sitio de soporte y licencia**: Indique si desea usar el modelo de pago por uso o con su licencia y, a continuación, especifique una cuenta del sitio de soporte de NetApp.

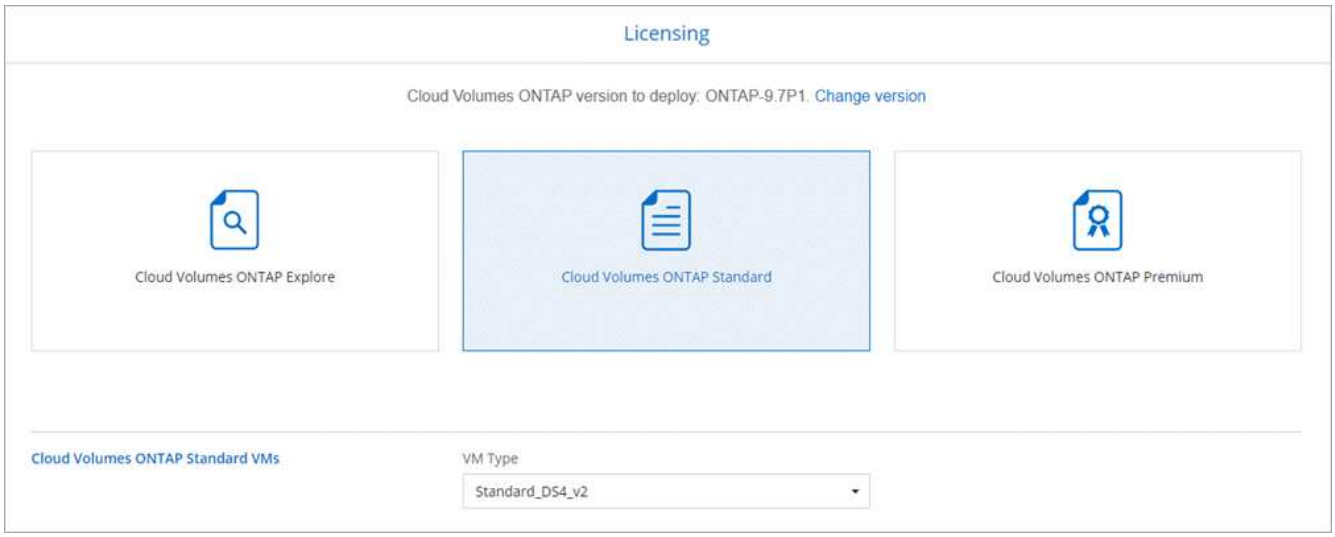
   Para comprender cómo funcionan las licencias, consulte "Licencia".

   Una cuenta del sitio de soporte de NetApp es opcional para el pago por uso, pero obligatoria para los sistemas BYOL. "Aprenda a añadir cuentas del sitio de soporte de NetApp".

7. **Paquetes preconfigurados**: Cree uno de los paquetes para implementar rápidamente un sistema Cloud Volumes ONTAP, o haga clic en **cree mi propia configuración**.

   Si selecciona uno de los paquetes, solo tiene que especificar un volumen y, a continuación, revisar y aprobar la configuración.

8. **Licencia**: Cambie la versión de Cloud Volumes ONTAP según sea necesario, seleccione una licencia y seleccione un tipo de máquina virtual.



Si sus necesidades cambian después de iniciar el sistema, puede modificar la licencia o el tipo de máquina virtual más adelante.

> Si hay disponible un candidato de versión, disponibilidad general o versión de revisión más reciente para la versión seleccionada, Cloud Manager actualiza el sistema a esa versión al crear el entorno de trabajo. Por ejemplo, la actualización se produce si selecciona Cloud Volumes ONTAP 9.6 RC1 y 9.6 GA está disponible. La actualización no se produce de una versión a otra; por ejemplo, de 9.6 a 9.7.

9. **Suscribirse desde el mercado de Azure**: Siga los pasos si Cloud Manager no pudo permitir implementaciones programáticas de Cloud Volumes ONTAP.
10. **Recursos de almacenamiento subyacentes**: Elija la configuración para el agregado inicial: Un tipo de disco, un tamaño para cada disco y si se debe habilitar la organización en niveles de datos para el almacenamiento BLOB.

    Tenga en cuenta lo siguiente:

    - El tipo de disco es para el volumen inicial. Es posible seleccionar un tipo de disco diferente para volúmenes posteriores.
    - El tamaño de disco es para todos los discos del agregado inicial y para cualquier agregado adicional que Cloud Manager cree cuando utilice la opción de aprovisionamiento simple. Puede crear agregados que utilicen un tamaño de disco diferente mediante la opción de asignación avanzada.

      Para obtener ayuda a elegir el tipo y el tamaño de disco, consulte "Ajuste de tamaño de su sistema en Azure".

    - Se puede elegir una política de organización en niveles de volumen específica cuando se crea o se edita un volumen.
    - Si deshabilita la organización en niveles de datos, puede habilitarla en agregados posteriores.

      "Más información acerca de la organización en niveles de los datos".

11. **escribir velocidad y GUSANO** (sólo sistemas de un solo nodo): Elija **velocidad de escritura normal** o **Alta** y active el almacenamiento de escritura única, lectura múltiple (WORM), si lo desea.

Además, es posible seleccionar una velocidad de escritura con sistemas de un solo nodo.

"Más información sobre la velocidad de escritura".

NO se puede habilitar WORM si la organización en niveles de datos está habilitada.

"Más información acerca del almacenamiento WORM".

12. **Secure Communication to Storage & WORM** (sólo ha): Si desea activar una conexión HTTPS a cuentas de almacenamiento de Azure y activar el almacenamiento de escritura única y lectura múltiple (WORM).

    La conexión HTTPS es de un par de alta disponibilidad de Cloud Volumes ONTAP 9.7 a las cuentas de almacenamiento de Azure. Tenga en cuenta que al habilitar esta opción, el rendimiento de escritura puede afectar. No se puede cambiar la configuración después de crear el entorno de trabajo.

    "Más información acerca del almacenamiento WORM".

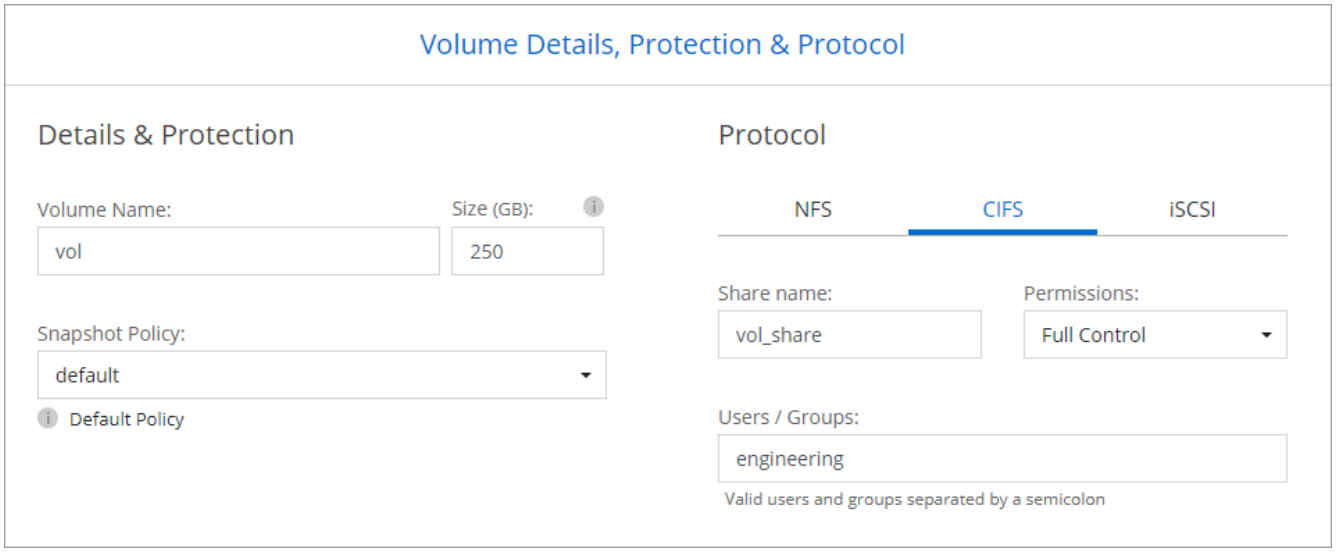
13. **Crear volumen**: Introduzca los detalles del nuevo volumen o haga clic en **Omitir**.

    Algunos de los campos en esta página son claros y explicativos. En la siguiente tabla se describen los campos que podrían presentar dificultades:

Campo	Descripción
Tamaño	El tamaño máximo que puede introducir depende en gran medida de si habilita thin provisioning, lo que le permite crear un volumen que sea mayor que el almacenamiento físico que hay disponible actualmente.
Control de acceso (solo para NFS)	Una política de exportación define los clientes de la subred que pueden acceder al volumen. De forma predeterminada, Cloud Manager introduce un valor que proporciona acceso a todas las instancias de la subred.
Permisos y usuarios/grupos (solo para CIFS)	Estos campos permiten controlar el nivel de acceso a un recurso compartido para usuarios y grupos (también denominados listas de control de acceso o ACL). Es posible especificar usuarios o grupos de Windows locales o de dominio, o usuarios o grupos de UNIX. Si especifica un nombre de usuario de Windows de dominio, debe incluir el dominio del usuario con el formato domain\username.
Política de Snapshot	Una política de copia de Snapshot especifica la frecuencia y el número de copias de Snapshot de NetApp creadas automáticamente. Una copia snapshot de NetApp es una imagen del sistema de archivos puntual que no afecta al rendimiento y requiere un almacenamiento mínimo. Puede elegir la directiva predeterminada o ninguna. Es posible que no elija ninguno para los datos transitorios: Por ejemplo, tempdb para Microsoft SQL Server.
Opciones avanzadas (solo para NFS)	Seleccione una versión de NFS para el volumen: NFSv3 o NFSv4.

Campo	Descripción
Grupo del iniciador y IQN (solo para iSCSI)	Los destinos de almacenamiento iSCSI se denominan LUN (unidades lógicas) y se presentan a los hosts como dispositivos de bloque estándar. Los iGroups son tablas de los nombres de los nodos de host iSCSI y controlan qué iniciadores tienen acceso a qué LUN. Los destinos iSCSI se conectan a la red a través de adaptadores de red Ethernet (NIC) estándar, tarjetas DEL motor de descarga TCP (TOE) con iniciadores de software, adaptadores de red convergente (CNA) o adaptadores de host de salida dedicados (HBA) y se identifican mediante nombres cualificados de iSCSI (IQN). Cuando se crea un volumen iSCSI, Cloud Manager crea automáticamente un LUN. Lo hemos hecho sencillo creando sólo una LUN por volumen, por lo que no hay que realizar ninguna gestión. Después de crear el volumen, "Utilice el IQN para conectarse con la LUN del hosts".

En la siguiente imagen, se muestra la página volumen rellenada para el protocolo CIFS:



14. **Configuración CIFS**: Si elige el protocolo CIFS, configure un servidor CIFS.

Campo	Descripción
DNS Dirección IP principal y secundaria	Las direcciones IP de los servidores DNS que proporcionan resolución de nombres para el servidor CIFS. Los servidores DNS enumerados deben contener los registros de ubicación de servicio (SRV) necesarios para localizar los servidores LDAP de Active Directory y los controladores de dominio del dominio al que se unirá el servidor CIFS.
Dominio de Active Directory al que unirse	El FQDN del dominio de Active Directory (AD) al que desea que se una el servidor CIFS.
Credenciales autorizadas para unirse al dominio	Nombre y contraseña de una cuenta de Windows con privilegios suficientes para agregar equipos a la unidad organizativa (OU) especificada dentro del dominio AD.
Nombre NetBIOS del servidor CIFS	Nombre de servidor CIFS que es único en el dominio de AD.

Campo	Descripción
Unidad organizacional	La unidad organizativa del dominio AD para asociarla con el servidor CIFS. El valor predeterminado es CN=Computers. Para configurar los Servicios de dominio de Azure AD como servidor AD para Cloud Volumes ONTAP, debe introducir **OU=equipos ADDC** o **OU=usuarios ADDC** en este campo.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Documentación de Azure: Cree una unidad organizativa (OU) en un dominio gestionado de Azure AD Domain Services"^]
Dominio DNS	El dominio DNS para la máquina virtual de almacenamiento (SVM) de Cloud Volumes ONTAP. En la mayoría de los casos, el dominio es el mismo que el dominio de AD.
Servidor NTP	Seleccione **usar dominio de Active Directory** para configurar un servidor NTP mediante el DNS de Active Directory. Si necesita configurar un servidor NTP con una dirección diferente, debe usar la API. Consulte "Guía para desarrolladores de API de Cloud Manager" para obtener más detalles.

15. **Perfil de uso, Tipo de disco y Directiva de organización en niveles**: Elija si desea activar las funciones de eficiencia del almacenamiento y cambiar la política de organización en niveles de volumen, si es necesario.

    Para obtener más información, consulte "Descripción de los perfiles de uso de volumen" y.. "Información general sobre organización en niveles de datos".

16. **revisar y aprobar**: Revise y confirme sus selecciones.
    a. Consulte los detalles de la configuración.
    b. Haga clic en **más información** para consultar detalles sobre el soporte técnico y los recursos de Azure que adquirirá Cloud Manager.
    c. Active las casillas de verificación **comprendo…**.
    d. Haga clic en **Ir**.

Resultado

Cloud Manager pone en marcha el sistema Cloud Volumes ONTAP. Puede realizar un seguimiento del progreso en la línea de tiempo.

Si tiene algún problema con la implementación del sistema Cloud Volumes ONTAP, revise el mensaje de error. También puede seleccionar el entorno de trabajo y hacer clic en **Volver a crear entorno**.

Para obtener más ayuda, vaya a. "Soporte Cloud Volumes ONTAP de NetApp".

Después de terminar

- Si ha aprovisionado un recurso compartido CIFS, proporcione permisos a usuarios o grupos a los archivos y carpetas y compruebe que esos usuarios pueden acceder al recurso compartido y crear un archivo.
- Si desea aplicar cuotas a los volúmenes, use System Manager o la interfaz de línea de comandos.

  Las cuotas le permiten restringir o realizar un seguimiento del espacio en disco y del número de archivos que usan un usuario, un grupo o un qtree.

Empiece a usar GCP

Introducción a Cloud Volumes ONTAP para Google Cloud

Empiece a usar Cloud Volumes ONTAP para GCP en unos pasos.

Cree un conector

Si usted no tiene un "Conector" Sin embargo, un administrador de cuentas necesita crear uno. "Aprenda a crear un conector en GCP".

Al crear el primer entorno de trabajo de Cloud Volumes ONTAP, Cloud Manager le solicitará que implemente un conector si aún no lo tiene.

Planificación de la configuración

Cloud Manager ofrece paquetes preconfigurados que se ajustan a sus requisitos de carga de trabajo, o bien puede crear su propia configuración. Si elige su propia configuración, debe conocer las opciones disponibles. "Leer más".

Configure su red

1. Asegúrese de que VPC y las subredes admitan la conectividad entre el conector y Cloud Volumes ONTAP.
2. Habilite el acceso a Internet de salida desde el VPC de destino para que el conector y Cloud Volumes ONTAP puedan ponerse en contacto con varios extremos.

   Este paso es importante porque el conector no puede administrar Cloud Volumes ONTAP sin acceso saliente a Internet. Si necesita limitar la conectividad saliente, consulte la lista de puntos finales para "El conector y Cloud Volumes ONTAP".

"Obtenga más información sobre los requisitos de red".

Configure GCP para la organización en niveles de datos

Deben cumplirse dos requisitos para organizar los datos fríos en niveles del Cloud Volumes ONTAP en un almacenamiento de objetos de bajo coste (un bucket de almacenamiento en cloud de Google):

1. "Configure la subred de Cloud Volumes ONTAP para acceso privado a Google".
2. "Configure una cuenta de servicio para la organización en niveles de los datos":
   - Asigne el rol *Storage Admin* predefinido a la cuenta del servicio de organización en niveles.
   - Agregue la cuenta de servicio conector como un *Usuario de cuenta de servicio* a la cuenta de servicio de organización en niveles.

     Puede proporcionar el rol de usuario "en el paso 3 del asistente al crear el cuenta de servicio de

organización en niveles", o. "otorgue el rol después de crear la cuenta de servicio".

Deberá seleccionar más adelante la cuenta del servicio de organización en niveles cuando cree un entorno de trabajo de Cloud Volumes ONTAP.

Si no habilita la organización en niveles de datos y selecciona una cuenta de servicio al crear el sistema Cloud Volumes ONTAP, tendrá que desactivar el sistema y añadir la cuenta de servicio a Cloud Volumes ONTAP desde la consola de GCP.

Habilite las API de Google Cloud

"Habilite las siguientes API de Google Cloud en su proyecto". Estas API son necesarias para poner en marcha el conector y Cloud Volumes ONTAP.

- API de Cloud Deployment Manager V2
- API de registro en la nube
- API de Cloud Resource Manager
- API del motor de computación
- API de gestión de acceso e identidad (IAM)

Inicie Cloud Volumes ONTAP mediante Cloud Manager

Haga clic en **Agregar entorno de trabajo**, seleccione el tipo de sistema que desea implementar y complete los pasos del asistente. "Lea las instrucciones paso a paso".

Enlaces relacionados

- "Evaluación"
- "Creación de un conector desde Cloud Manager"
- "Instalar el software del conector en un host Linux"
- "Qué hace Cloud Manager con los permisos de GCP"

Planificación de la configuración de Cloud Volumes ONTAP en Google Cloud

Al poner en marcha Cloud Volumes ONTAP en Google Cloud, puede elegir un sistema preconfigurado que se ajuste a los requisitos de la carga de trabajo, o puede crear su propia configuración. Si elige su propia configuración, debe conocer las opciones disponibles.

Seleccione un tipo de licencia

Cloud Volumes ONTAP está disponible en dos opciones de precios: De pago por uso y con su propia licencia (BYOL). En el modelo de pago por uso, puede elegir entre tres licencias: Explorar, Standard o Premium. Cada licencia proporciona distintas opciones de computación y capacidad.

"Configuraciones admitidas para Cloud Volumes ONTAP 9.7 en GCP"

Comprender los límites de almacenamiento

El límite de capacidad bruta de un sistema de Cloud Volumes ONTAP está relacionado con la licencia. Los límites adicionales afectan al tamaño de los agregados y los volúmenes. Debe conocer estos límites a medida que planifique la configuración.

"Límites de almacenamiento para Cloud Volumes ONTAP 9.7 en GCP"

Ajuste de tamaño de su sistema en GCP

Configurar el tamaño de su sistema Cloud Volumes ONTAP puede ayudarle a cumplir los requisitos de rendimiento y capacidad. Al elegir un tipo de máquina, un tipo de disco y un tamaño de disco, es necesario tener en cuenta algunos puntos clave:

Tipo de máquina

Observe los tipos de máquina admitidos en la "Notas de la versión de Cloud Volumes ONTAP" Y luego revise los detalles de Google sobre cada tipo de máquina compatible. Haga coincidir los requisitos de carga de trabajo con el número de vCPU y memoria para el tipo de máquina. Tenga en cuenta que cada núcleo de CPU aumenta el rendimiento de la red.

Consulte lo siguiente para obtener más información:

- "Documentación de Google Cloud: Tipos de máquina estándar N1"
- "Documentación de Google Cloud: Rendimiento"

Tipo de disco para GCP

Cuando crea volúmenes para Cloud Volumes ONTAP, debe elegir el almacenamiento en cloud subyacente que utiliza Cloud Volumes ONTAP para un disco. El tipo de disco puede ser *Zonal SSD persistent disks* o *Zonal standard persistent disks*.

Los discos persistentes de SSD son la mejor opción para cargas de trabajo que requieren altas tasas de IOPS aleatorias, mientras que los discos persistentes estándar son económicos y pueden gestionar operaciones de lectura/escritura secuenciales. Para obtener información detallada, consulte "Documentación de Google Cloud: Discos persistentes zonal (Standard y SSD)".

Tamaño de discos para GCP

Debe seleccionar un tamaño de disco inicial al poner en marcha un sistema Cloud Volumes ONTAP. Después puede dejar que Cloud Manager gestione la capacidad de un sistema para usted, pero si desea crear agregados por su cuenta, tenga en cuenta lo siguiente:

- Todos los discos de un agregado deben tener el mismo tamaño.
- Determine el espacio que necesita, teniendo en cuenta el rendimiento.
- El rendimiento de los discos persistentes se amplía automáticamente con el tamaño del disco y el número de vCPU disponibles para el sistema.

  Consulte lo siguiente para obtener más información:

  - "Documentación de Google Cloud: Discos persistentes zonal (Standard y SSD)"
  - "Documentación de Google Cloud: Optimización del rendimiento de discos persistentes y SSD locales"

Hoja de trabajo de información de red para GCP

Al implementar Cloud Volumes ONTAP en GCP, debe especificar los detalles de su red virtual. Puede utilizar una hoja de cálculo para recopilar la información del administrador.

Información para GCP	Su valor
Región	
Zona	
Red VPC	
Subred	
Política de firewall (si utiliza la suya propia)	

Elegir una velocidad de escritura

Cloud Manager le permite elegir una configuración de velocidad de escritura para sistemas Cloud Volumes ONTAP de un solo nodo. Antes de elegir una velocidad de escritura, debe comprender las diferencias entre la configuración normal y la alta, así como los riesgos y recomendaciones cuando utilice la alta velocidad de escritura.

Diferencia entre la velocidad de escritura normal y la alta velocidad de escritura

Al elegir la velocidad de escritura normal, los datos se escriben directamente en el disco, lo que reduce la probabilidad de que se pierdan los datos en caso de que se produzca una interrupción del servicio no planificada del sistema.

Al elegir una alta velocidad de escritura, los datos se guardan en búfer en la memoria antes de que se escriban en el disco, lo que proporciona un rendimiento de escritura más rápido. Gracias al almacenamiento en caché, existe la posibilidad de perder datos en caso de que se produzca una interrupción no planificada del sistema.

La cantidad de datos que se pueden perder en caso de una interrupción imprevista del sistema es el plazo de dos últimos puntos de coherencia. Un punto de coherencia es el acto de escribir datos en el búfer en el disco. Un punto de coherencia se produce cuando el registro de escritura está completo o después de 10 segundos (lo que ocurra primero). Sin embargo, el rendimiento del volumen de AWS EBS puede afectar el tiempo de procesamiento del punto de consistencia.

Cuándo utilizar alta velocidad de escritura

La alta velocidad de escritura es una buena opción si es necesario un rendimiento de escritura rápido para su carga de trabajo, y puede resistir el riesgo de pérdida de datos en caso de una interrupción del servicio del sistema no planificada.

Recomendaciones cuando se utiliza una alta velocidad de escritura

Si habilita una alta velocidad de escritura, debe garantizar la protección de escritura en la capa de la aplicación.

Selección de un perfil de uso de volumen

ONTAP incluye varias funciones de eficiencia del almacenamiento que pueden reducir la cantidad total de

almacenamiento que necesita. Al crear un volumen en Cloud Manager, puede seleccionar un perfil que habilite estas funciones o un perfil que las deshabilite. Debe obtener más información sobre estas funciones para ayudarle a decidir qué perfil utilizar.

Las funciones de eficiencia del almacenamiento de NetApp ofrecen las siguientes ventajas:

Aprovisionamiento ligero

Presenta más almacenamiento lógico a hosts o usuarios del que realmente hay en el pool de almacenamiento físico. En lugar de asignar previamente espacio de almacenamiento, el espacio de almacenamiento se asigna de forma dinámica a cada volumen a medida que se escriben los datos.

Deduplicación

Mejora la eficiencia al localizar bloques de datos idénticos y sustituirlos con referencias a un único bloque compartido. Esta técnica reduce los requisitos de capacidad de almacenamiento al eliminar los bloques de datos redundantes que se encuentran en un mismo volumen.

Compresión

Reduce la capacidad física requerida para almacenar datos al comprimir los datos de un volumen en almacenamiento primario, secundario y de archivado.

Requisitos de red para poner en marcha y gestionar Cloud Volumes ONTAP en GCP

Configure sus redes de Google Cloud Platform para que los sistemas Cloud Volumes ONTAP puedan funcionar correctamente. Esto incluye la conexión a redes para el conector y Cloud Volumes ONTAP.

Requisitos para Cloud Volumes ONTAP

En GCP deben cumplirse los siguientes requisitos.

Cloud privado virtual

Cloud Volumes ONTAP y el conector son compatibles con un VPC compartido de Google Cloud y también en PCs no compartidos.

Un VPC compartido permite configurar y gestionar de forma centralizada las redes virtuales de varios proyectos. Puede configurar redes VPC compartidas en el *proyecto host* e implementar las instancias de máquina virtual de conector y Cloud Volumes ONTAP en un *proyecto de servicio*. "Documentación de Google Cloud: Información general sobre VPC compartido".

El único requisito al usar un VPC compartido es a. proporcione el "Rol de usuario de red de computación" A la cuenta de servicio conector. Cloud Manager necesita estos permisos para consultar los firewalls, VPC y subredes del proyecto de host.

Acceso saliente a Internet para Cloud Volumes ONTAP

Cloud Volumes ONTAP requiere acceso saliente a Internet para enviar mensajes a NetApp AutoSupport, que supervisa proactivamente el estado del almacenamiento.

Las políticas de enrutamiento y firewall deben permitir el tráfico HTTP/HTTPS a los siguientes extremos para que Cloud Volumes ONTAP pueda enviar mensajes de AutoSupport:

- https://support.netapp.com/aods/asupmessage

- https://support.netapp.com/asupprod/post/1.0/postAsup

  "Aprenda a configurar AutoSupport".

Número de direcciones IP

Cloud Manager asigna 5 direcciones IP a Cloud Volumes ONTAP en GCP.

Tenga en cuenta que Cloud Manager no crea una LIF de gestión de SVM para Cloud Volumes ONTAP en GCP.

Una LIF es una dirección IP asociada con un puerto físico. Se requiere una LIF de gestión de SVM para herramientas de gestión como SnapCenter.

Reglas del firewall

No necesita crear reglas de firewall, ya que Cloud Manager lo hace por usted. Si necesita utilizar el suyo propio, consulte las reglas de firewall que se enumeran a continuación.

Conexión de Cloud Volumes ONTAP a Google Cloud Storage para organización en niveles de los datos

Si desea organizar los datos inactivos en niveles en un bucket de Google Cloud Storage, la subred en la que reside Cloud Volumes ONTAP debe estar configurada para Private Google Access. Para obtener instrucciones, consulte "Documentación de Google Cloud: Configuración de Private Google Access".

Si quiere ver los pasos adicionales necesarios para configurar la organización en niveles de los datos en Cloud Manager, consulte "Organización en niveles de los datos inactivos en almacenamiento de objetos de bajo coste".

Conexiones a sistemas ONTAP en otras redes

Para replicar datos entre un sistema Cloud Volumes ONTAP en GCP y los sistemas ONTAP de otras redes, debe tener una conexión VPN entre el VPC y la otra red, por ejemplo, su red corporativa.

Para obtener instrucciones, consulte "Documentación de Google Cloud: Información general sobre Cloud VPN".

Requisitos para el conector

Configure su red de modo que el conector pueda gestionar recursos y procesos en su entorno de cloud público. El paso más importante es garantizar el acceso saliente a Internet a varios puntos finales.

Si la red utiliza un servidor proxy para toda la comunicación a Internet, puede especificar el servidor proxy en la página Configuración. Consulte "Configuración del conector para utilizar un servidor proxy".

Conexión a redes de destino

Un conector requiere una conexión de red a los VPC y VNets en los que desea implementar Cloud Volumes ONTAP.

Por ejemplo, si instala un conector en la red corporativa, debe configurar una conexión VPN al VPC o a vnet en el que inicie Cloud Volumes ONTAP.

Acceso a Internet de salida

El conector requiere acceso saliente a Internet para gestionar recursos y procesos dentro de su entorno de nube pública. Un conector se pone en contacto con los siguientes extremos al gestionar recursos en GCP:

Puntos finales	Específico
https://www.googleapis.com	Permite que el conector se ponga en contacto con las API de Google para poner en marcha y gestionar Cloud Volumes ONTAP en GCP.
https://api.services.cloud.netapp.com:443	Solicitudes de API a Cloud Central de NetApp.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Proporciona acceso a imágenes, manifiestos y plantillas de software.
https://repo.cloud.support.netapp.com	Se utiliza para descargar las dependencias de Cloud Manager.
http://repo.mysql.com/	Se utiliza para descargar MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Permite al conector acceder y descargar manifiestos, plantillas e imágenes de actualización de Cloud Volumes ONTAP.
https://cloudmanagerinfraprod.azurecr.io	Acceso a imágenes de software de componentes de contenedor para una infraestructura que ejecuta Docker y proporciona una solución para las integraciones de servicios con Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Permite a NetApp transmitir datos desde registros de auditoría.
https://cloudmanager.cloud.netapp.com	Comunicación con el servicio Cloud Manager, que incluye cuentas de Cloud Central.
https://netapp-cloud-account.auth0.com	Comunicación con Cloud Central de NetApp para la autenticación de usuario centralizada.
https://mysupport.netapp.com	Comunicación con AutoSupport de NetApp.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Comunicación con NetApp para la licencia del sistema y el registro de soporte.
https://ipa-signer.cloudmanager.netapp.com	Permite que Cloud Manager genere licencias (por ejemplo, una licencia de FlexCache para Cloud Volumes ONTAP).
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Necesario para conectar los sistemas Cloud Volumes ONTAP con un clúster de Kubernetes. Los extremos permiten la instalación de Trident de NetApp.

Puntos finales	Específico
Diversas ubicaciones de terceros, por ejemplo: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org Las ubicaciones de terceros están sujetas a cambios.	Durante las actualizaciones, Cloud Manager descarga los paquetes más recientes para dependencias de terceros.

Aunque debe realizar casi todas las tareas desde la interfaz de usuario de SaaS, todavía hay disponible una interfaz de usuario local en el conector. La máquina que ejecuta el explorador Web debe tener conexiones con los siguientes puntos finales:

Puntos finales	Específico
El host del conector	Debe introducir la dirección IP del host desde un explorador web para cargar la consola de Cloud Manager. Según su conectividad con el proveedor de cloud, puede usar la IP privada o una IP pública asignada al host: • Una IP privada funciona si dispone de una VPN y. acceso directo a la red virtual • Una IP pública funciona en cualquier situación de red En cualquier caso, debe proteger el acceso a la red garantizando que las reglas de grupo de seguridad permiten el acceso sólo desde IP o subredes autorizadas.
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	El explorador web se conecta con estos extremos para conseguir una autenticación de usuario centralizada mediante NetApp Cloud Central.
https://widget.intercom.io	Si busca un chat integrado en los productos que le permita hablar con expertos en cloud de NetApp.

Reglas de firewall para Cloud Volumes ONTAP

Cloud Manager crea reglas de firewall de GCP que incluyen las reglas entrantes y salientes que Cloud Manager y Cloud Volumes ONTAP necesitan para funcionar correctamente. Tal vez desee consultar los puertos para fines de prueba o si prefiere utilizar sus propios grupos de seguridad.

Las reglas de firewall para Cloud Volumes ONTAP requieren reglas tanto entrantes como salientes.

Reglas de entrada

El origen de las reglas entrantes en el grupo de seguridad predefinido es 0.0.0.0/0.

Protocolo	Puerto	Específico
Todos los ICMP	Todo	Hacer ping a la instancia
HTTP	80	Acceso HTTP a la consola web de System Manager mediante el La dirección IP de la LIF de gestión del clúster
HTTPS	443	Acceso HTTPS a la consola web de System Manager mediante el La dirección IP de la LIF de gestión del clúster
SSH	22	Acceso SSH a la dirección IP de administración del clúster LIF o una LIF de gestión de nodos
TCP	111	Llamada a procedimiento remoto para NFS
TCP	139	Sesión de servicio NetBIOS para CIFS
TCP	161-162	Protocolo simple de gestión de red
TCP	445	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
TCP	635	Montaje NFS
TCP	749	Kerberos
TCP	2049	Daemon del servidor NFS
TCP	3260	Acceso iSCSI mediante la LIF de datos iSCSI
TCP	4045	Daemon de bloqueo NFS
TCP	4046	Supervisor de estado de red para NFS
TCP	10000	Backup con NDMP
TCP	11104	Gestión de sesiones de comunicación de interconexión de clústeres para SnapMirror
TCP	11105	Transferencia de datos de SnapMirror mediante LIF de interconexión de clústeres
UDP	111	Llamada a procedimiento remoto para NFS
UDP	161-162	Protocolo simple de gestión de red
UDP	635	Montaje NFS
UDP	2049	Daemon del servidor NFS
UDP	4045	Daemon de bloqueo NFS
UDP	4046	Supervisor de estado de red para NFS
UDP	4049	Protocolo rquotad NFS

Reglas de salida

El grupo de seguridad predefinido para Cloud Volumes ONTAP abre todo el tráfico saliente. Si eso es aceptable, siga las reglas básicas de la salida. Si necesita más reglas rígidas, utilice las reglas avanzadas de salida.

Reglas de salida básicas

El grupo de seguridad predefinido para Cloud Volumes ONTAP incluye las siguientes reglas de salida.

Protocolo	Puerto	Específico
Todos los ICMP	Todo	Todo el tráfico saliente
Todos los TCP	Todo	Todo el tráfico saliente
Todas las UDP	Todo	Todo el tráfico saliente

Reglas salientes avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede utilizar la siguiente información para abrir sólo los puertos necesarios para la comunicación saliente por Cloud Volumes ONTAP.

El origen es la interfaz (dirección IP) en el sistema Cloud Volumes ONTAP.

Servicio	Protocolo	Puerto	Origen	Destino	Específico
Active Directory	TCP	88	LIF de gestión de nodos	Bosque de Active Directory	Autenticación Kerberos V.
	UDP	137	LIF de gestión de nodos	Bosque de Active Directory	Servicio de nombres NetBIOS
	UDP	138	LIF de gestión de nodos	Bosque de Active Directory	Servicio de datagramas NetBIOS
	TCP	139	LIF de gestión de nodos	Bosque de Active Directory	Sesión de servicio NetBIOS
	TCP Y UDP	389	LIF de gestión de nodos	Bosque de Active Directory	LDAP
	TCP	445	LIF de gestión de nodos	Bosque de Active Directory	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
	TCP	464	LIF de gestión de nodos	Bosque de Active Directory	Kerberos V cambiar y establecer contraseña (SET_CHANGE)
	UDP	464	LIF de gestión de nodos	Bosque de Active Directory	Administración de claves Kerberos
	TCP	749	LIF de gestión de nodos	Bosque de Active Directory	Contraseña de Kerberos V Change & Set (RPCSEC_GSS)
	TCP	88	LIF de datos (NFS, CIFS e iSCSI)	Bosque de Active Directory	Autenticación Kerberos V.
	UDP	137	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Servicio de nombres NetBIOS
	UDP	138	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Servicio de datagramas NetBIOS
	TCP	139	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Sesión de servicio NetBIOS
	TCP Y UDP	389	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	LDAP
	TCP	445	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
	TCP	464	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Kerberos V cambiar y establecer contraseña (SET_CHANGE)
	UDP	464	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Administración de claves Kerberos
	TCP	749	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Contraseña de Kerberos V change & set (RPCSEC_GSS)

Servicio	Protocolo	Puerto	Origen	Destino	Específico
Clúster	Todo el tráfico	Todo el tráfico	Todos los LIF de un nodo	Todas las LIF del otro nodo	Comunicaciones de interconexión de clústeres (solo Cloud Volumes ONTAP de alta disponibilidad)
	TCP	3000	LIF de gestión de nodos	Mediador DE ALTA DISPONIBILIDAD	Llamadas ZAPI (solo alta disponibilidad de Cloud Volumes ONTAP)
	ICMP	1	LIF de gestión de nodos	Mediador DE ALTA DISPONIBILIDAD	Mantener activos (solo alta disponibilidad de Cloud Volumes ONTAP)
DHCP	UDP	68	LIF de gestión de nodos	DHCP	Cliente DHCP para la configuración inicial
DHCPS	UDP	67	LIF de gestión de nodos	DHCP	Servidor DHCP
DNS	UDP	53	LIF de gestión de nodos y LIF de datos (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	LIF de gestión de nodos	Servidores de destino	Copia NDMP
SMTP	TCP	25	LIF de gestión de nodos	Servidor de correo	Alertas SMTP, que se pueden utilizar para AutoSupport
SNMP	TCP	161	LIF de gestión de nodos	Servidor de supervisión	Supervisión mediante capturas SNMP
	UDP	161	LIF de gestión de nodos	Servidor de supervisión	Supervisión mediante capturas SNMP
	TCP	162	LIF de gestión de nodos	Servidor de supervisión	Supervisión mediante capturas SNMP
	UDP	162	LIF de gestión de nodos	Servidor de supervisión	Supervisión mediante capturas SNMP
SnapMirror	TCP	11104	LIF entre clústeres	LIF de interconexión de clústeres de ONTAP	Gestión de sesiones de comunicación de interconexión de clústeres para SnapMirror
	TCP	11105	LIF entre clústeres	LIF de interconexión de clústeres de ONTAP	Transferencia de datos de SnapMirror
Syslog	UDP	514	LIF de gestión de nodos	Servidor de syslog	Mensajes de syslog Reenviar

Reglas de firewall para el conector

Las reglas de firewall para el conector requieren reglas de entrada y salida.

Reglas de entrada

El origen de las reglas de entrada en las reglas de firewall predefinidas es 0.0.0.0/0.

Protocolo	Puerto	Específico
SSH	22	Proporciona acceso SSH al host de Connector
HTTP	80	Proporciona acceso HTTP desde navegadores web de cliente al local interfaz de usuario
HTTPS	443	Proporciona acceso HTTPS desde exploradores web de cliente al local interfaz de usuario

Reglas de salida

Las reglas de firewall predefinidas para el conector abren todo el tráfico saliente. Si eso es aceptable, siga las reglas básicas de la salida. Si necesita más reglas rígidas, utilice las reglas avanzadas de salida.

Reglas de salida básicas

Las reglas de firewall predefinidas para el conector incluyen las siguientes reglas de salida.

Protocolo	Puerto	Específico
Todos los TCP	Todo	Todo el tráfico saliente
Todas las UDP	Todo	Todo el tráfico saliente

Reglas salientes avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede utilizar la siguiente información para abrir sólo los puertos necesarios para la comunicación saliente por parte del conector.

La dirección IP de origen es el host del conector.

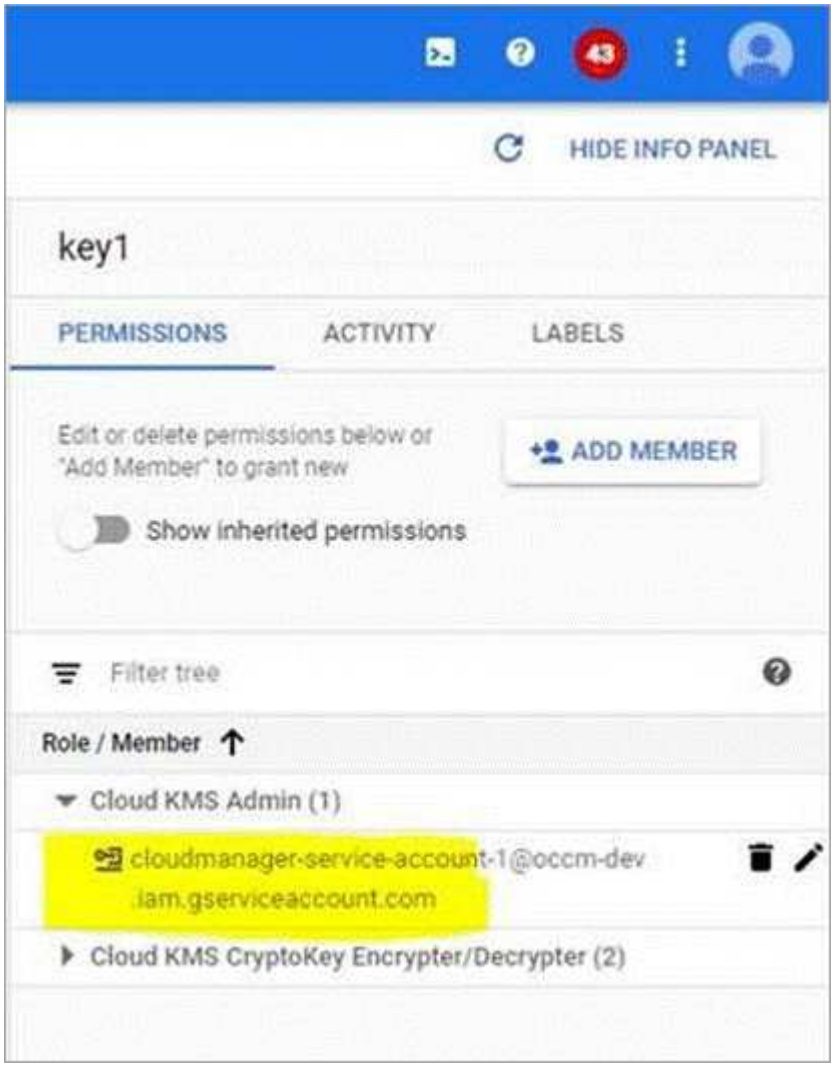
Servicio	Protocolo	Puerto	Destino	Específico
Active Directory	TCP	88	Bosque de Active Directory	Autenticación Kerberos V.
	TCP	139	Bosque de Active Directory	Sesión de servicio NetBIOS
	TCP	389	Bosque de Active Directory	LDAP
	TCP	445	Bosque de Active Directory	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
	TCP	464	Bosque de Active Directory	Kerberos V cambiar y establecer contraseña (SET_CHANGE)
	TCP	749	Bosque de Active Directory	Contraseña de modificación y definición de Kerberos V de Active Directory (RPCSEC_GSS)
	UDP	137	Bosque de Active Directory	Servicio de nombres NetBIOS
	UDP	138	Bosque de Active Directory	Servicio de datagramas NetBIOS
	UDP	464	Bosque de Active Directory	Administración de claves Kerberos
Llamadas API y AutoSupport	HTTPS	443	LIF de gestión de clústeres de ONTAP y Internet saliente	API llama a GCP y ONTAP, y envía mensajes de AutoSupport a NetApp
Llamadas API	TCP	3000	LIF de gestión de clústeres de ONTAP	Llamadas API a ONTAP
DNS	UDP	53	DNS	Utilizado para resolver DNS por Cloud Manager

Utiliza claves de cifrado gestionadas por el cliente con Cloud Volumes ONTAP

Aunque Google Cloud Storage siempre cifra los datos antes de que se escriban en el disco, puede utilizar las API de Cloud Manager para crear un sistema Cloud Volumes ONTAP que utilice *claves de cifrado gestionadas por el cliente*. Estas son claves que genera y gestiona en GCP mediante el servicio Cloud Key Management Service.

Pasos

1. Conceda permiso a la cuenta de servicio conector para utilizar la clave de cifrado.



2. Obtenga el "id" de la clave invocando el comando get de la API /gcp/vsa/Metadata/gcp-Encryption-keys.
3. Utilice el parámetro "GcpEncryption" con la solicitud de API al crear un entorno de trabajo.

ejemplo

```
"gcpEncryptionParameters": {
    "key": "projects/tlv-support/locations/us-
east4/keyRings/Nikiskeys/cryptoKeys/generatedkey1"
  }
```

Consulte la "Guía para desarrolladores de API" Para obtener más detalles sobre el uso del parámetro "GcpEncryption".

Lanzamiento de Cloud Volumes ONTAP en GCP

Puede iniciar un sistema Cloud Volumes ONTAP de un solo nodo en GCP creando un entorno de trabajo.

Lo que necesitará

- Usted debe tener un "Conector asociado al área de trabajo".

> Debe ser un administrador de cuentas para crear un conector. Al crear el primer entorno de trabajo de Cloud Volumes ONTAP, Cloud Manager le solicita que cree un conector si todavía no lo tiene.

- "Debe estar preparado para dejar el conector funcionando en en todo momento".
- Debe haber elegido una configuración y haber obtenido la información de red de GCP de su administrador. Para obtener más información, consulte "Planificación de la configuración de Cloud Volumes ONTAP".
- Para poner en marcha un sistema BYOL, necesita el número de serie (clave de licencia) de 20 dígitos para cada nodo.
- Deben estar las siguientes API de Google Cloud "habilitado en el proyecto":
  - API de Cloud Deployment Manager V2
  - API de registro en la nube
  - API de Cloud Resource Manager
  - API del motor de computación
  - API de gestión de acceso e identidad (IAM)

Pasos

1. En la página entornos de trabajo, haga clic en **Agregar entorno de trabajo** y siga las indicaciones.
2. **Elija una ubicación**: Seleccione **Google Cloud** y **Cloud Volumes ONTAP**.
3. **Detalles y credenciales**: Seleccione un proyecto, especifique un nombre de clúster, añada etiquetas de manera opcional y especifique las credenciales.

   En la siguiente tabla se describen los campos que podrían presentar dificultades:

Campo	Descripción
Nombre del entorno de trabajo	Cloud Manager utiliza el nombre del entorno de trabajo para nombrar tanto el sistema Cloud Volumes ONTAP como la instancia de GCP VM. También utiliza el nombre como prefijo para el grupo de seguridad predefinido si selecciona esa opción.
Agregar etiquetas	Las etiquetas son metadatos para sus recursos de GCP. Cloud Manager añade las etiquetas al sistema Cloud Volumes ONTAP y a los recursos de GCP asociados con el sistema. Puede añadir hasta cuatro etiquetas desde la interfaz de usuario al crear un entorno de trabajo y, después, puede agregar más. Tenga en cuenta que la API no le limita a cuatro etiquetas al crear un entorno de trabajo. Para obtener más información sobre las etiquetas, consulte "Documentación de Google Cloud: Etiquetado de recursos".
Nombre de usuario y contraseña	Estas son las credenciales de la cuenta de administrador del clúster de Cloud Volumes ONTAP. Puede usar estas credenciales para conectarse a Cloud Volumes ONTAP a través de System Manager o de la CLI.

Campo	Descripción
Editar proyecto	Seleccione el proyecto en el que desea que resida Cloud Volumes ONTAP. El proyecto predeterminado es el proyecto en el que reside Cloud Manager. Si no ve ningún proyecto adicional en la lista desplegable, aún no ha asociado la cuenta de servicio de Cloud Manager con otros proyectos. Vaya a la consola de Google Cloud, abra el servicio IAM y seleccione el proyecto. Añada la cuenta de servicio con la función Cloud Manager a ese proyecto. Deberá repetir este paso con cada proyecto. Esta es la cuenta de servicio que configuró para Cloud Manager "como se describe en el paso 2b de esta página". Haga clic en **Agregar suscripción** para asociar las credenciales seleccionadas a una suscripción. Para crear un sistema Cloud Volumes ONTAP de pago por uso, debe seleccionar un proyecto de GCP asociado con una suscripción a Cloud Volumes ONTAP desde el mercado de GCP.

En el siguiente vídeo se muestra cómo asociar una suscripción de mercado de pago por uso a su proyecto de GCP:

► https://docs.netapp.com/es-es/occm38//media/video_subscribing_gcp.mp4 *(video)*

4. **ubicación y conectividad**: Seleccione una ubicación, elija una política de firewall y seleccione la casilla de verificación para confirmar la conectividad de red al almacenamiento de Google Cloud para la organización en niveles de datos.

   Si desea organizar los datos inactivos en niveles en un bucket de Google Cloud Storage, la subred en la que reside Cloud Volumes ONTAP debe estar configurada para Private Google Access. Para obtener instrucciones, consulte "Documentación de Google Cloud: Configuración de Private Google Access".

5. **cuenta del sitio de soporte y licencia**: Indique si desea usar el modelo de pago por uso o con su propia licencia y, a continuación, especifique una cuenta del sitio de soporte de NetApp.

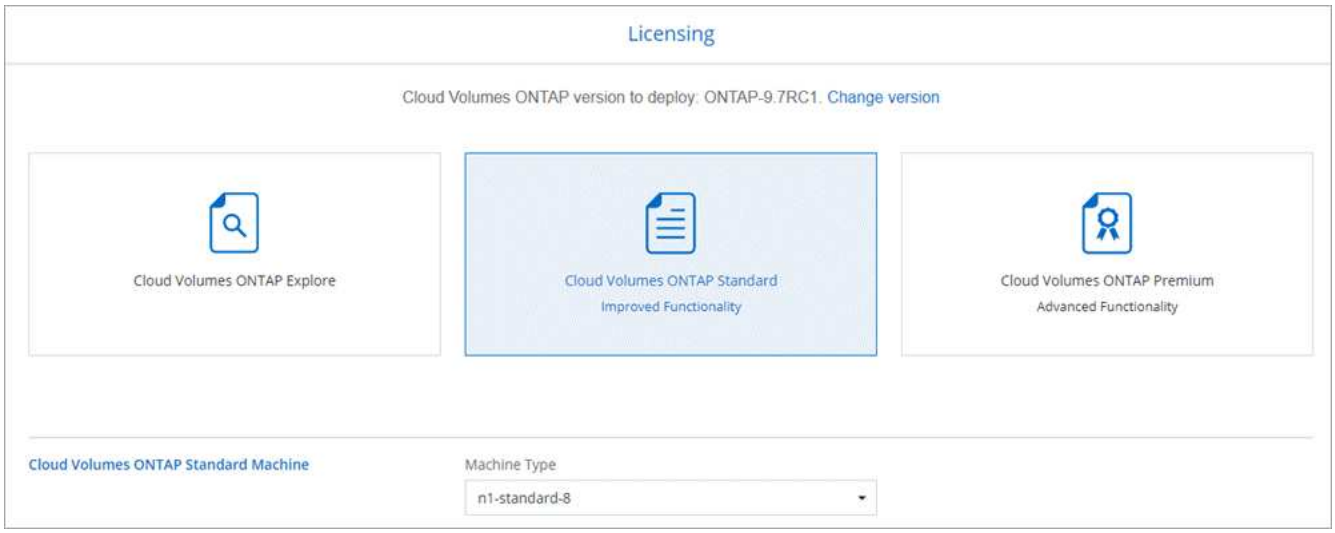
   Para comprender cómo funcionan las licencias, consulte "Licencia".

   Una cuenta del sitio de soporte de NetApp es opcional para el pago por uso, pero obligatoria para los sistemas BYOL. "Aprenda a añadir cuentas del sitio de soporte de NetApp".

6. **Paquetes preconfigurados**: Seleccione uno de los paquetes para implementar rápidamente un sistema Cloud Volumes ONTAP, o haga clic en **Crear mi propia configuración**.

   Si selecciona uno de los paquetes, solo tiene que especificar un volumen y, a continuación, revisar y aprobar la configuración.

7. **Licencia**: Cambie la versión de Cloud Volumes ONTAP según sea necesario, seleccione una licencia y seleccione un tipo de máquina virtual.



Si sus necesidades cambian después de iniciar el sistema, puede modificar la licencia o el tipo de máquina virtual más adelante.

> Si hay disponible un candidato de versión, disponibilidad general o versión de revisión más reciente para la versión seleccionada, Cloud Manager actualiza el sistema a esa versión al crear el entorno de trabajo. Por ejemplo, la actualización se produce si selecciona Cloud Volumes ONTAP 9.6 RC1 y 9.6 GA está disponible. La actualización no se produce de una versión a otra; por ejemplo, de 9.6 a 9.7.

8. **Recursos de almacenamiento subyacentes**: Elija la configuración del agregado inicial: Un tipo de disco y el tamaño de cada disco.

   El tipo de disco es para el volumen inicial. Es posible seleccionar un tipo de disco diferente para volúmenes posteriores.

   El tamaño de disco es para todos los discos del agregado inicial y para cualquier agregado adicional que Cloud Manager cree cuando utilice la opción de aprovisionamiento simple. Puede crear agregados que utilicen un tamaño de disco diferente mediante la opción de asignación avanzada.

   Para obtener ayuda a elegir el tipo y el tamaño de disco, consulte "Ajuste de tamaño de su sistema en GCP".

9. **escribir velocidad y GUSANO**: Elija **velocidad de escritura normal** o **Alta**, y active el almacenamiento de escritura única, lectura múltiple (WORM), si lo desea.

   Además, es posible seleccionar una velocidad de escritura con sistemas de un solo nodo.

   "Más información sobre la velocidad de escritura".

   NO se puede habilitar WORM si la organización en niveles de datos está habilitada.

   "Más información acerca del almacenamiento WORM".

10. **Segmentación de datos en Google Cloud Platform**: Elija si desea habilitar la organización en niveles de los datos en el agregado inicial, elija una clase de almacenamiento para los datos almacenados en niveles y, a continuación, seleccione una cuenta de servicio con el rol de administrador de almacenamiento predefinido (se requiere para Cloud Volumes ONTAP 9.7) o seleccione una cuenta de GCP (se requiere para Cloud Volumes ONTAP 9.6).

Tenga en cuenta lo siguiente:

- Cloud Manager establece la cuenta de servicio en la instancia de Cloud Volumes ONTAP. Esta cuenta de servicio proporciona permisos para organizar los datos en niveles en un bloque de Google Cloud Storage. Asegúrese de añadir la cuenta del servicio Cloud Manager como usuario de la cuenta del servicio de organización en niveles. De lo contrario, no puede seleccionarla en Cloud Manager.
- Si necesita ayuda para añadir una cuenta de GCP, consulte "Configuración y adición de cuentas de GCP para la organización de datos en niveles con 9.6".
- Se puede elegir una política de organización en niveles de volumen específica cuando se crea o se edita un volumen.
- Si deshabilita la organización en niveles de datos, puede habilitarla en agregados posteriores, pero tendrá que apagar el sistema y agregar una cuenta de servicio desde la consola de GCP.

  "Más información acerca de la organización en niveles de los datos".

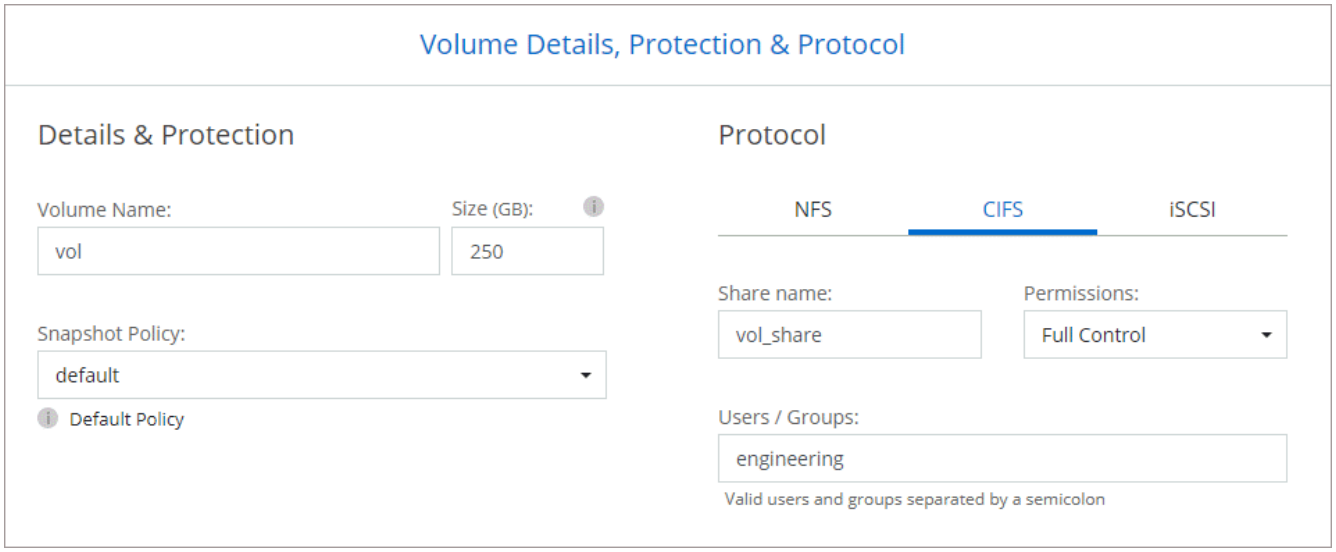
11. **Crear volumen**: Introduzca los detalles del nuevo volumen o haga clic en **Omitir**.

    Algunos de los campos en esta página son claros y explicativos. En la siguiente tabla se describen los campos que podrían presentar dificultades:

Campo	Descripción
Tamaño	El tamaño máximo que puede introducir depende en gran medida de si habilita thin provisioning, lo que le permite crear un volumen que sea mayor que el almacenamiento físico que hay disponible actualmente.
Control de acceso (solo para NFS)	Una política de exportación define los clientes de la subred que pueden acceder al volumen. De forma predeterminada, Cloud Manager introduce un valor que proporciona acceso a todas las instancias de la subred.
Permisos y usuarios/grupos (solo para CIFS)	Estos campos permiten controlar el nivel de acceso a un recurso compartido para usuarios y grupos (también denominados listas de control de acceso o ACL). Es posible especificar usuarios o grupos de Windows locales o de dominio, o usuarios o grupos de UNIX. Si especifica un nombre de usuario de Windows de dominio, debe incluir el dominio del usuario con el formato domain\username.
Política de Snapshot	Una política de copia de Snapshot especifica la frecuencia y el número de copias de Snapshot de NetApp creadas automáticamente. Una copia snapshot de NetApp es una imagen del sistema de archivos puntual que no afecta al rendimiento y requiere un almacenamiento mínimo. Puede elegir la directiva predeterminada o ninguna. Es posible que no elija ninguno para los datos transitorios: Por ejemplo, tempdb para Microsoft SQL Server.
Opciones avanzadas (solo para NFS)	Seleccione una versión de NFS para el volumen: NFSv3 o NFSv4.

Campo	Descripción
Grupo del iniciador y IQN (solo para iSCSI)	Los destinos de almacenamiento iSCSI se denominan LUN (unidades lógicas) y se presentan a los hosts como dispositivos de bloque estándar. Los iGroups son tablas de los nombres de los nodos de host iSCSI y controlan qué iniciadores tienen acceso a qué LUN. Los destinos iSCSI se conectan a la red a través de adaptadores de red Ethernet (NIC) estándar, tarjetas DEL motor de descarga TCP (TOE) con iniciadores de software, adaptadores de red convergente (CNA) o adaptadores de host de salida dedicados (HBA) y se identifican mediante nombres cualificados de iSCSI (IQN). Cuando se crea un volumen iSCSI, Cloud Manager crea automáticamente un LUN. Lo hemos hecho sencillo creando sólo una LUN por volumen, por lo que no hay que realizar ninguna gestión. Después de crear el volumen, "Utilice el IQN para conectarse con la LUN del hosts".

En la siguiente imagen, se muestra la página volumen rellenada para el protocolo CIFS:



12. **Configuración CIFS**: Si elige el protocolo CIFS, configure un servidor CIFS.

Campo	Descripción
DNS Dirección IP principal y secundaria	Las direcciones IP de los servidores DNS que proporcionan resolución de nombres para el servidor CIFS. Los servidores DNS enumerados deben contener los registros de ubicación de servicio (SRV) necesarios para localizar los servidores LDAP de Active Directory y los controladores de dominio del dominio al que se unirá el servidor CIFS.
Dominio de Active Directory al que unirse	El FQDN del dominio de Active Directory (AD) al que desea que se una el servidor CIFS.
Credenciales autorizadas para unirse al dominio	Nombre y contraseña de una cuenta de Windows con privilegios suficientes para agregar equipos a la unidad organizativa (OU) especificada dentro del dominio AD.
Nombre NetBIOS del servidor CIFS	Nombre de servidor CIFS que es único en el dominio de AD.
Unidad organizacional	La unidad organizativa del dominio AD para asociarla con el servidor CIFS. El valor predeterminado es CN=Computers.

Campo	Descripción
Dominio DNS	El dominio DNS para la máquina virtual de almacenamiento (SVM) de Cloud Volumes ONTAP. En la mayoría de los casos, el dominio es el mismo que el dominio de AD.
Servidor NTP	Seleccione **usar dominio de Active Directory** para configurar un servidor NTP mediante el DNS de Active Directory. Si necesita configurar un servidor NTP con una dirección diferente, debe usar la API. Consulte "Guía para desarrolladores de API de Cloud Manager" para obtener más detalles.

13. **Perfil de uso, Tipo de disco y Directiva de organización en niveles**: Elija si desea activar las funciones de eficiencia del almacenamiento y cambiar la política de organización en niveles de volumen, si es necesario.

    Para obtener más información, consulte "Descripción de los perfiles de uso de volumen" y.. "Información general sobre organización en niveles de datos".

14. **revisar y aprobar**: Revise y confirme sus selecciones.
    a. Consulte los detalles de la configuración.
    b. Haga clic en **más información** para revisar los detalles sobre el soporte técnico y los recursos de GCP que adquirirá Cloud Manager.
    c. Active las casillas de verificación **comprendo…**.
    d. Haga clic en **Ir**.

Resultado

Cloud Manager pone en marcha el sistema Cloud Volumes ONTAP. Puede realizar un seguimiento del progreso en la línea de tiempo.

Si tiene algún problema con la implementación del sistema Cloud Volumes ONTAP, revise el mensaje de error. También puede seleccionar el entorno de trabajo y hacer clic en **Volver a crear entorno**.

Para obtener más ayuda, vaya a. "Soporte Cloud Volumes ONTAP de NetApp".

Después de terminar

- Si ha aprovisionado un recurso compartido CIFS, proporcione permisos a usuarios o grupos a los archivos y carpetas y compruebe que esos usuarios pueden acceder al recurso compartido y crear un archivo.
- Si desea aplicar cuotas a los volúmenes, use System Manager o la interfaz de línea de comandos.

  Las cuotas le permiten restringir o realizar un seguimiento del espacio en disco y del número de archivos que usan un usuario, un grupo o un qtree.

Aprovisione y gestione el almacenamiento

Aprovisionar almacenamiento

Puede aprovisionar almacenamiento adicional para los sistemas Cloud Volumes ONTAP desde Cloud Manager mediante la gestión de volúmenes y agregados.

Todos los discos y agregados deben crearse y eliminarse directamente desde Cloud Manager. No debe realizar estas acciones desde otra herramienta de gestión. De esta manera, se puede afectar a la estabilidad del sistema, se puede obstaculizar la capacidad de añadir discos en el futuro y generar potencialmente cuotas redundantes para proveedores de cloud.

Creación de volúmenes de FlexVol

Si necesita más almacenamiento después de iniciar un sistema Cloud Volumes ONTAP, puede crear nuevos volúmenes FlexVol para NFS, CIFS o iSCSI desde Cloud Manager.

Acerca de esta tarea

Cuando se crea un volumen iSCSI, Cloud Manager crea automáticamente un LUN. Lo hemos hecho sencillo creando sólo una LUN por volumen, por lo que no hay que realizar ninguna gestión. Después de crear el volumen, Utilice el IQN para conectarse con la LUN del hosts.

Puede crear LUN adicionales desde System Manager o desde la CLI.

Antes de empezar

Si desea usar CIFS en AWS, debe haber configurado DNS y Active Directory. Para obtener más información, consulte "Requisitos de red para Cloud Volumes ONTAP para AWS".

Pasos

1. En la página Working Environments, haga doble clic en el nombre del sistema Cloud Volumes ONTAP donde desea aprovisionar los volúmenes de FlexVol.
2. Cree un nuevo volumen en cualquier agregado o en un agregado específico:

Acción	Pasos
Cree un nuevo volumen y deje que Cloud Manager elija el con el agregado	Haga clic en **Añadir nuevo volumen**.
Cree un nuevo volumen en un agregado específico	a. Haga clic en el icono de menú y, a continuación, haga clic en **Avanzado > asignación avanzada**. b. Haga clic en el menú de un agregado. c. Haga clic en **Crear volumen**.

3. Introduzca los detalles del nuevo volumen y, a continuación, haga clic en **continuar**.

   Algunos de los campos en esta página son claros y explicativos. En la siguiente tabla se describen los campos que podrían presentar dificultades:

Campo	Descripción
Tamaño	El tamaño máximo que puede introducir depende en gran medida de si habilita thin provisioning, lo que le permite crear un volumen que sea mayor que el almacenamiento físico que hay disponible actualmente.
Control de acceso (solo para NFS)	Una política de exportación define los clientes de la subred que pueden acceder al volumen. De forma predeterminada, Cloud Manager introduce un valor que proporciona acceso a todas las instancias de la subred.

Campo	Descripción
Permisos y usuarios/grupos (solo para CIFS)	Estos campos permiten controlar el nivel de acceso a un recurso compartido para usuarios y grupos (también denominados listas de control de acceso o ACL). Es posible especificar usuarios o grupos de Windows locales o de dominio, o usuarios o grupos de UNIX. Si especifica un nombre de usuario de Windows de dominio, debe incluir el dominio del usuario con el formato domain\username.
Política de Snapshot	Una política de copia de Snapshot especifica la frecuencia y el número de copias de Snapshot de NetApp creadas automáticamente. Una copia snapshot de NetApp es una imagen del sistema de archivos puntual que no afecta al rendimiento y requiere un almacenamiento mínimo. Puede elegir la directiva predeterminada o ninguna. Es posible que no elija ninguno para los datos transitorios: Por ejemplo, tempdb para Microsoft SQL Server.
Opciones avanzadas (solo para NFS)	Seleccione una versión de NFS para el volumen: NFSv3 o NFSv4.
Grupo del iniciador y IQN (solo para iSCSI)	Los destinos de almacenamiento iSCSI se denominan LUN (unidades lógicas) y se presentan a los hosts como dispositivos de bloque estándar. Los iGroups son tablas de los nombres de los nodos de host iSCSI y controlan qué iniciadores tienen acceso a qué LUN. Los destinos iSCSI se conectan a la red a través de adaptadores de red Ethernet (NIC) estándar, tarjetas DEL motor de descarga TCP (TOE) con iniciadores de software, adaptadores de red convergente (CNA) o adaptadores de host de salida dedicados (HBA) y se identifican mediante nombres cualificados de iSCSI (IQN). Cuando se crea un volumen iSCSI, Cloud Manager crea automáticamente un LUN. Lo hemos hecho sencillo creando sólo una LUN por volumen, por lo que no hay que realizar ninguna gestión. Después de crear el volumen, "Utilice el IQN para conectarse con la LUN del hosts".

4. Si ha elegido el protocolo CIFS y no se ha configurado el servidor CIFS, especifique los detalles del servidor en el cuadro de diálogo Crear un servidor CIFS y, a continuación, haga clic en **Guardar y continuar**:

Campo	Descripción
DNS Dirección IP principal y secundaria	Las direcciones IP de los servidores DNS que proporcionan resolución de nombres para el servidor CIFS. Los servidores DNS enumerados deben contener los registros de ubicación de servicio (SRV) necesarios para localizar los servidores LDAP de Active Directory y los controladores de dominio del dominio al que se unirá el servidor CIFS.
Dominio de Active Directory al que unirse	El FQDN del dominio de Active Directory (AD) al que desea que se una el servidor CIFS.
Credenciales autorizadas para unirse al dominio	Nombre y contraseña de una cuenta de Windows con privilegios suficientes para agregar equipos a la unidad organizativa (OU) especificada dentro del dominio AD.
Nombre NetBIOS del servidor CIFS	Nombre de servidor CIFS que es único en el dominio de AD.

Campo	Descripción
Unidad organizacional	La unidad organizativa del dominio AD para asociarla con el servidor CIFS. El valor predeterminado es CN=Computers. • Para configurar Microsoft AD administrado de AWS como el servidor AD para Cloud Volumes ONTAP, debe introducir **OU=equipos,OU=corp** en este campo. • Para configurar los Servicios de dominio de Azure AD como servidor AD para Cloud Volumes ONTAP, debe introducir **OU=equipos ADDC** o **OU=usuarios ADDC** en este campo.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Documentación de Azure: Cree una unidad organizativa (OU) en un dominio gestionado de Azure AD Domain Services"^]
Dominio DNS	El dominio DNS para la máquina virtual de almacenamiento (SVM) de Cloud Volumes ONTAP. En la mayoría de los casos, el dominio es el mismo que el dominio de AD.
Servidor NTP	Seleccione **usar dominio de Active Directory** para configurar un servidor NTP mediante el DNS de Active Directory. Si necesita configurar un servidor NTP con una dirección diferente, debe usar la API. Consulte "Guía para desarrolladores de API de Cloud Manager" para obtener más detalles.

5. En la página Usage Profile, Disk Type y Tiering Policy, elija si desea habilitar las funciones de eficiencia del almacenamiento, elija un tipo de disco y edite la política de organización en niveles, si es necesario.

   Si necesita ayuda, consulte lo siguiente:

   - "Descripción de los perfiles de uso de volumen"
   - "Ajuste de tamaño de su sistema en AWS"
   - "Ajuste de tamaño de su sistema en Azure"
   - "Información general sobre organización en niveles de datos"

6. Haga clic en **Ir**.

Resultado

Cloud Volumes ONTAP aprovisiona el volumen.

Después de terminar

Si ha aprovisionado un recurso compartido CIFS, proporcione permisos a usuarios o grupos a los archivos y carpetas y compruebe que esos usuarios pueden acceder al recurso compartido y crear un archivo.

Si desea aplicar cuotas a volúmenes, debe usar System Manager o la interfaz de línea de comandos. Las cuotas le permiten restringir o realizar un seguimiento del espacio en disco y del número de archivos que usan un usuario, un grupo o un qtree.

Creación de volúmenes de FlexVol en el segundo nodo de una alta disponibilidad configuración

De forma predeterminada, Cloud Manager crea volúmenes en el primer nodo de una configuración de alta disponibilidad. Si necesita una configuración activo-activo, en la que ambos nodos sirven datos a los clientes, debe crear agregados y volúmenes en el segundo nodo.

Pasos

1. En la página entornos de trabajo, haga doble clic en el nombre del entorno de trabajo de Cloud Volumes ONTAP en el que desea gestionar agregados.
2. Haga clic en el icono de menú y, a continuación, haga clic en **Avanzado > asignación avanzada**.
3. Haga clic en **Agregar agregado** y, a continuación, cree el agregado.
4. Para Home Node, elija el segundo nodo del par de alta disponibilidad.
5. Después de que Cloud Manager cree el agregado, selecciónelo y, a continuación, haga clic en **Crear volumen**.
6. Introduzca los detalles del nuevo volumen y, a continuación, haga clic en **Crear**.

Después de terminar

Puede crear volúmenes adicionales en este agregado si es necesario.

> En el caso de parejas de alta disponibilidad implementadas en varias zonas de disponibilidad de AWS, debe montar el volumen en clientes mediante la dirección IP flotante del nodo en el que reside el volumen.

Creación de agregados

Puede crear agregados usted mismo o dejar que Cloud Manager lo haga por usted cuando cree volúmenes. La ventaja de crear los agregados usted mismo es que puede elegir el tamaño de disco subyacente, lo que le permite configurar el agregado para la capacidad o el rendimiento que necesita.

Pasos

1. En la página entornos de trabajo, haga doble clic en el nombre de la instancia de Cloud Volumes ONTAP en la que desea gestionar agregados.
2. Haga clic en el icono de menú y, a continuación, haga clic en **Avanzado > asignación avanzada**.
3. Haga clic en **Agregar agregado** y, a continuación, especifique los detalles para el agregado.

   Para obtener ayuda con el tipo de disco y el tamaño de disco, consulte "Planificación de la configuración".

4. Haga clic en **Ir** y, a continuación, haga clic en **aprobar y adquirir**.

Conectar una LUN a un host

Cuando se crea un volumen iSCSI, Cloud Manager crea automáticamente un LUN. Lo hemos hecho sencillo creando sólo una LUN por volumen, por lo que no hay que realizar ninguna gestión. Después de crear el volumen, utilice el IQN para conectarse con el LUN desde los hosts.

Tenga en cuenta lo siguiente:

1. La gestión automática de la capacidad de Cloud Manager no se aplica a las LUN. Cuando Cloud Manager crea un LUN, deshabilita la función de crecimiento automático.
2. Puede crear LUN adicionales desde System Manager o desde la CLI.

Pasos

1. En la página Working Environments, haga doble clic en el entorno de trabajo de Cloud Volumes ONTAP en el que desea gestionar los volúmenes.
2. Seleccione un volumen y, a continuación, haga clic en **IQN objetivo**.

3. Haga clic en **Copiar** para copiar el nombre del IQN.
4. Configurar una conexión iSCSI desde el host al LUN.
    - "Configuración exprés de iSCSI de ONTAP 9 para Red Hat Enterprise Linux: Iniciar las sesiones iSCSI con el destino"
    - "Configuración exprés de iSCSI para Windows de ONTAP 9: Iniciar sesiones iSCSI con el destino"

Uso de volúmenes de FlexCache para acelerar el acceso a los datos

Un volumen FlexCache es un volumen de almacenamiento que almacena en caché datos de lectura NFS de un volumen de origen (o origen). Las lecturas posteriores a los datos almacenados en caché hacen que el acceso a los datos sea más rápido.

Puede usar volúmenes de FlexCache para acelerar el acceso a los datos o para descargar el tráfico de volúmenes con un acceso frecuente. Los volúmenes FlexCache ayudan a mejorar el rendimiento, en especial cuando los clientes necesitan acceder a los mismos datos en repetidas ocasiones, ya que los datos pueden ofrecerse directamente sin tener que acceder al volumen de origen. Los volúmenes FlexCache funcionan bien con cargas de trabajo del sistema que requieren una gran cantidad de lecturas.

Cloud Manager no proporciona gestión de volúmenes de FlexCache en este momento, pero se puede usar la interfaz de línea de comandos de ONTAP o ONTAP System Manager para crear y gestionar volúmenes de FlexCache:

- "Guía completa de volúmenes de FlexCache para un acceso más rápido a los datos"
- "Creación de volúmenes de FlexCache en System Manager"

A partir del lanzamiento de la versión 3.7.2, Cloud Manager genera una licencia de FlexCache para todos los nuevos sistemas de Cloud Volumes ONTAP. La licencia incluye un límite de uso de 500 GB.

Para generar la licencia, Cloud Manager necesita acceder a https://ipa-signer.cloudmanager.netapp.com. Asegúrese de que se puede acceder a esta URL desde el firewall.

Gestión del almacenamiento existente

Cloud Manager le permite gestionar volúmenes, agregados y servidores CIFS. También indica que se deben mover los volúmenes para evitar problemas de capacidad.

Gestión de los volúmenes existentes

Puede gestionar los volúmenes existentes a medida que cambien sus necesidades de almacenamiento. Es posible ver, editar, clonar, restaurar y eliminar volúmenes.

Pasos

1. En la página Working Environments, haga doble clic en el entorno de trabajo de Cloud Volumes ONTAP en el que desea gestionar los volúmenes.
2. Gestione sus volúmenes:

Tarea	Acción
Permite ver la información de un volumen	Seleccione un volumen y, a continuación, haga clic en **Info**.
Editar un volumen (solo volúmenes de lectura y escritura)	a. Seleccione un volumen y, a continuación, haga clic en **Editar**. b. Modifique la directiva Snapshot del volumen, la versión del protocolo NFS, la lista de control de acceso NFS o los permisos de uso compartido y, a continuación, haga clic en **Actualizar**. Si necesita políticas de Snapshot personalizadas, puede crearlas mediante System Manager.

Tarea	Acción
Clonar un volumen	a. Seleccione un volumen y, a continuación, haga clic en **Clonar**. b. Modifique el nombre del clon según sea necesario y, a continuación, haga clic en **Clonar**. Este proceso crea un volumen FlexClone. Un volumen FlexClone es una copia editable, de un momento específico, que gestiona el espacio de forma eficiente, porque utiliza una pequeña cantidad de espacio para los metadatos y, a continuación, solo consume espacio adicional a medida que se modifican o agregan datos. Para obtener más información sobre los volúmenes FlexClone, consulte "Guía de gestión de almacenamiento lógico de ONTAP 9".
Restaurar datos de una copia Snapshot en un volumen nuevo	a. Seleccione un volumen y, a continuación, haga clic en **Restaurar desde copia Snapshot**. b. Seleccione una copia Snapshot, introduzca un nombre para el nuevo volumen y, a continuación, haga clic en **Restaurar**.
Cree una copia Snapshot bajo demanda	a. Seleccione un volumen y, a continuación, haga clic en **Crear una copia Snapshot**. b. Si es necesario, cambie el nombre y, a continuación, haga clic en **Crear**.
Obtenga el comando de montaje NFS	a. Seleccione un volumen y, a continuación, haga clic en **comando de montaje**. b. Haga clic en **Copiar**.
Vea el IQN objetivo para un volumen iSCSI	a. Seleccione un volumen y, a continuación, haga clic en **IQN objetivo**. b. Haga clic en **Copiar**. c. "Utilice el IQN para conectarse con la LUN del hosts".
Cambie el tipo de disco subyacente	a. Seleccione un volumen y, a continuación, haga clic en **Cambiar tipo de disco y directiva de organización en niveles**. b. Seleccione el tipo de disco y, a continuación, haga clic en **Cambiar**. Cloud Manager mueve el volumen a un agregado existente que utiliza el tipo de disco seleccionado o crea un nuevo agregado para el volumen.

Tarea	Acción
Cambie la política de organización en niveles	a. Seleccione un volumen y, a continuación, haga clic en **Cambiar tipo de disco y directiva de organización en niveles**. b. Haga clic en **Editar directiva**. c. Seleccione una directiva diferente y haga clic en **Cambiar**. Cloud Manager mueve el volumen a un agregado existente que utiliza el tipo de disco seleccionado con organización en niveles o crea un nuevo agregado para el volumen.
Eliminar un volumen	a. Seleccione un volumen y, a continuación, haga clic en **Eliminar**. b. Vuelva a hacer clic en **Eliminar** para confirmar.

Gestión de los agregados existentes

Gestione los agregados usted mismo añadiendo discos, visualizando información sobre los agregados y suprimiéndolos.

Antes de empezar

Si desea eliminar un agregado, primero debe haber eliminado los volúmenes del agregado.

Acerca de esta tarea

Si se está quedando sin espacio un agregado, puede mover volúmenes a otro agregado mediante System Manager de OnCommand.

Pasos

1. En la página entornos de trabajo, haga doble clic en el entorno de trabajo de Cloud Volumes ONTAP en el que desea gestionar agregados.
2. Haga clic en el icono de menú y, a continuación, haga clic en **Avanzado > asignación avanzada**.
3. Gestione los agregados:

Tarea	Acción
Ver información sobre un agregado	Seleccione un agregado y haga clic en **Info**.
Cree un volumen en un agregado específico	Seleccione un agregado y haga clic en **Crear volumen**.

Tarea	Acción
Añada discos a un agregado	a. Seleccione un agregado y haga clic en **Agregar discos de AWS** o **Agregar discos de Azure**. b. Seleccione el número de discos que desea agregar y haga clic en **Agregar**. Todos los discos de un agregado deben tener el mismo tamaño.
Eliminar un agregado	a. Seleccione un agregado que no contenga ningún volumen y haga clic en **Eliminar**. b. Vuelva a hacer clic en **Eliminar** para confirmar.

Modificación del servidor CIFS

Si cambia sus servidores DNS o dominio de Active Directory, debe modificar el servidor CIFS en Cloud Volumes ONTAP para seguir sirviendo almacenamiento a los clientes.

Pasos

1. En el entorno de trabajo, haga clic en el icono de menú y, a continuación, haga clic en **Avanzado > Configuración CIFS**.
2. Especifique la configuración del servidor CIFS:

Tarea	Acción
DNS Dirección IP principal y secundaria	Las direcciones IP de los servidores DNS que proporcionan resolución de nombres para el servidor CIFS. Los servidores DNS enumerados deben contener los registros de ubicación de servicio (SRV) necesarios para localizar los servidores LDAP de Active Directory y los controladores de dominio del dominio al que se unirá el servidor CIFS.
Dominio de Active Directory al que unirse	El FQDN del dominio de Active Directory (AD) al que desea que se una el servidor CIFS.
Credenciales autorizadas para unirse al dominio	Nombre y contraseña de una cuenta de Windows con privilegios suficientes para agregar equipos a la unidad organizativa (OU) especificada dentro del dominio AD.
Nombre NetBIOS del servidor CIFS	Nombre de servidor CIFS que es único en el dominio de AD.
Unidad organizacional	La unidad organizativa del dominio AD para asociarla con el servidor CIFS. El valor predeterminado es CN=Computers. Si configura Microsoft AD administrado de AWS como servidor AD para Cloud Volumes ONTAP, debe introducir **OU=equipos,OU=corp** en este campo.
Dominio DNS	El dominio DNS para la máquina virtual de almacenamiento (SVM) de Cloud Volumes ONTAP. En la mayoría de los casos, el dominio es el mismo que el dominio de AD.

Tarea	Acción
Servidor NTP	Seleccione **usar dominio de Active Directory** para configurar un servidor NTP mediante el DNS de Active Directory. Si necesita configurar un servidor NTP con una dirección diferente, debe usar la API. Consulte "Guía para desarrolladores de API de Cloud Manager" para obtener más detalles.

3. Haga clic en **Guardar**.

Resultado

Cloud Volumes ONTAP actualiza el servidor CIFS con los cambios.

Mover un volumen

Mueva volúmenes para mejorar el aprovechamiento de la capacidad, mejorar el rendimiento y cumplir los acuerdos de nivel de servicio.

Puede mover un volumen en System Manager seleccionando un volumen y el agregado de destino, iniciando la operación de movimiento de volúmenes y, opcionalmente, supervisando el trabajo de movimiento de volúmenes. Cuando se usa System Manager, una operación de movimiento de volúmenes se completa automáticamente.

Pasos

1. Utilice System Manager o la interfaz de línea de comandos para mover los volúmenes al agregado.

   En la mayoría de las situaciones, se puede usar System Manager para mover volúmenes.

   Para ver instrucciones, consulte "Guía exprés de traslado de volúmenes de ONTAP 9".

Movimiento de un volumen cuando Cloud Manager muestra una acción requerida mensaje

Cloud Manager puede mostrar un mensaje de acción obligatorio que dice que es necesario mover un volumen para evitar problemas de capacidad, pero que no puede ofrecer recomendaciones para corregir el problema. Si sucede esto, debe identificar cómo corregir el problema y luego mover uno o más volúmenes.

Pasos

1. Identificar cómo se corrige el problema.
2. Según su análisis, mueva volúmenes para evitar problemas de capacidad:
   - Mueva volúmenes a otro sistema.
   - Mueva volúmenes a otro agregado del mismo sistema.

Identificación de cómo corregir los problemas de capacidad

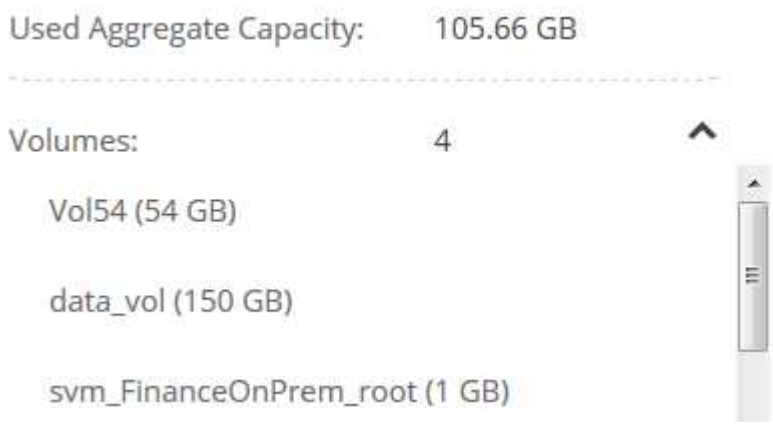
Si Cloud Manager no puede proporcionar recomendaciones para mover un volumen para evitar problemas de capacidad, debe identificar los volúmenes que debe mover y si debe moverlos a otro agregado del mismo sistema o a otro sistema.

Pasos

1. Consulte la información avanzada en el mensaje Action Required para identificar el agregado que ha alcanzado su límite de capacidad.

Por ejemplo, la información avanzada debería decir algo similar a lo siguiente: La agrupación aggr1 ha alcanzado su límite de capacidad.

2. Identifique uno o varios volúmenes para mover fuera del agregado:
   a. En el entorno de trabajo, haga clic en el icono de menú y, a continuación, haga clic en **Avanzado > asignación avanzada**.
   b. Seleccione el agregado y, a continuación, haga clic en **Info**.
   c. Expanda la lista de volúmenes.



   d. Revise el tamaño de cada volumen y seleccione uno o varios volúmenes para mover fuera del agregado.

      Debe elegir volúmenes que sean lo suficientemente grandes como para liberar espacio en el agregado para evitar problemas de capacidad adicionales en el futuro.

3. Si el sistema no ha alcanzado el límite de discos, debe mover los volúmenes a un agregado existente o a un nuevo agregado del mismo sistema.

   Para obtener más información, consulte "Mover volúmenes a otro agregado para evitar problemas de capacidad".

4. Si el sistema ha alcanzado el límite de discos, realice una de las siguientes acciones:
   a. Elimine los volúmenes que no se utilizan.
   b. Reorganice los volúmenes para liberar espacio en un agregado.

      Para obtener más información, consulte "Mover volúmenes a otro agregado para evitar problemas de capacidad".

   c. Mueva dos o más volúmenes a otro sistema que tenga espacio.

      Para obtener más información, consulte "Mover volúmenes a otro sistema para evitar problemas de capacidad".

Mover volúmenes a otro sistema para evitar problemas de capacidad

Es posible mover uno o más volúmenes a otro sistema Cloud Volumes ONTAP para evitar problemas de capacidad. Es posible que deba hacer esto si el sistema alcanzó su límite de discos.

Acerca de esta tarea

Puede seguir los pasos de esta tarea para corregir el siguiente mensaje Acción necesaria:

```
 Moving a volume is necessary to avoid capacity issues; however, Cloud
Manager cannot perform this action for you because the system has reached
the disk limit.
.Pasos
. Identifique un sistema Cloud Volumes ONTAP con capacidad disponible o
implemente un nuevo sistema.
. Arrastre y suelte el entorno de trabajo de origen en el entorno de
trabajo de destino para realizar una replicación de datos única del
volumen.
```

+
Para obtener más información, consulte "Replicación de datos entre sistemas".

1. Vaya a la página Replication Status y, a continuación, rompa la relación de SnapMirror para convertir el volumen replicado de un volumen de protección de datos a un volumen de lectura/escritura.

   Para obtener más información, consulte "Gestionar programaciones y relaciones de replicación de datos".

2. Configure el volumen para el acceso a los datos.

   Para obtener información sobre la configuración de un volumen de destino para el acceso a los datos, consulte "Guía exprés de recuperación de desastres de volúmenes de ONTAP 9".

3. Elimine el volumen original.

   Para obtener más información, consulte "Gestión de los volúmenes existentes".

Mover volúmenes a otro agregado para evitar problemas de capacidad

Puede mover uno o varios volúmenes a otro agregado para evitar problemas de capacidad.

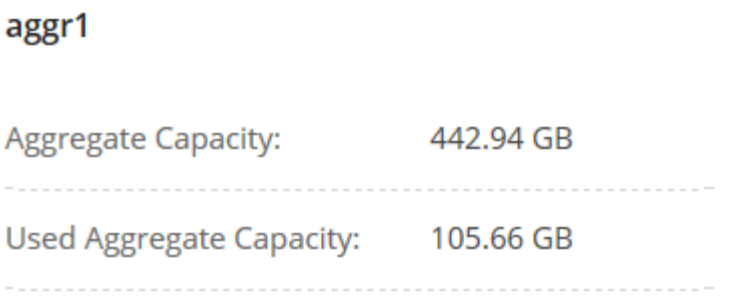
Acerca de esta tarea

Puede seguir los pasos de esta tarea para corregir el siguiente mensaje Acción necesaria:

```
 Moving two or more volumes is necessary to avoid capacity issues;
however, Cloud Manager cannot perform this action for you.
.Pasos
. Compruebe si un agregado existente tiene capacidad disponible para los
volúmenes que se necesitan mover:
```

+
.. En el entorno de trabajo, haga clic en el icono de menú y, a continuación, haga clic en **Avanzado > asignación avanzada**.
.. Seleccione cada agregado, haga clic en **Info** y, a continuación, vea la capacidad disponible (capacidad agregada menos capacidad agregada utilizada).

+



1. Si es necesario, añada discos a un agregado existente:
   a. Seleccione el agregado y, a continuación, haga clic en **Agregar discos**.
   b. Seleccione el número de discos que desea agregar y, a continuación, haga clic en **Agregar**.
2. Si no hay agregados con capacidad disponible, cree un nuevo agregado.

   Para obtener más información, consulte "Creación de agregados".
3. Utilice System Manager o la interfaz de línea de comandos para mover los volúmenes al agregado.
4. En la mayoría de las situaciones, se puede usar System Manager para mover volúmenes.

   Para ver instrucciones, consulte "Guía exprés de traslado de volúmenes de ONTAP 9".

Motivos por los que es posible que un movimiento de volumen sea lento

El movimiento de un volumen puede tardar más de lo esperado si se da alguna de las siguientes condiciones en el caso de Cloud Volumes ONTAP:

- El volumen es un clon.
- El volumen es el elemento principal de un clon.
- Los agregados de origen o destino tienen un único disco HDD de rendimiento optimizado (st1).
- El sistema Cloud Volumes ONTAP está en AWS y un agregado utiliza un esquema de nomenclatura anterior para los objetos. Ambos agregados tienen que utilizar el mismo formato de nombre.

  Se utiliza un esquema de nomenclatura anterior si se habilitó la organización en niveles de datos en un agregado de la versión 9.4 o anterior.
- La configuración de cifrado no coincide con los agregados de origen y destino; o bien, hay una nueva clave en curso.
- Se especificó la opción *-Tiering-policy* en el movimiento del volumen para cambiar la política de organización en niveles.
- Se especificó la opción *-generate-destination-key* en el movimiento de volúmenes.

Organización en niveles de los datos inactivos en almacenamiento de objetos de bajo coste

Puede reducir los costes de almacenamiento de Cloud Volumes ONTAP combinando un nivel de rendimiento de SSD o HDD para datos activos con un nivel de capacidad de almacenamiento de objetos para los datos inactivos. Para obtener información general de alto nivel, consulte "Información general sobre organización en niveles de datos".

Para configurar la organización en niveles de los datos, solo tiene que hacer lo siguiente:

Elija una configuración compatible

La mayoría de configuraciones son compatibles. Si tiene un sistema Cloud Volumes ONTAP estándar, Premium o BYOL con la versión más reciente, debería ser bueno. "Leer más".

Garantice la conectividad entre Cloud Volumes ONTAP y el almacenamiento de objetos

- Para AWS, necesitará un extremo de VPC a S3. Leer más.
- Para Azure, ya no tendrá que hacer nada mientras Cloud Manager tenga los permisos necesarios. Leer más.
- Para GCP, necesita configurar la subred para Google Access privado y configurar una cuenta de servicio. Leer más.

Elija una política de organización en niveles cuando cree, modifique o replique un volumen

Cloud Manager le solicita que elija una política de organización en niveles al crear, modificar o replicar un volumen.

- "Organización en niveles de los datos en volúmenes de lectura y escritura"
- "Organización en niveles de los datos en los volúmenes de protección de datos"

Qué'no se requiere para la organización en niveles de datos

- No es necesario instalar una licencia de funciones para habilitar la organización en niveles de datos.
- No necesita crear el nivel de capacidad (un bloque de S3, un contenedor de Azure Blob o un bloque de GCP). Cloud Manager lo hace por usted.

Configuraciones compatibles con la organización en niveles de los datos

Puede habilitar la organización en niveles de los datos al utilizar configuraciones y funciones específicas:

- La organización en niveles de los datos es compatible con Cloud Volumes ONTAP Standard, Premium y BYOL, a partir de las siguientes versiones:
  - La versión 9.2 en AWS
  - Versión 9.4 en Azure con sistemas de un solo nodo
  - Versión 9.6 en Azure con parejas de alta disponibilidad
  - Versión 9.6 en GCP

  No se admite la organización en niveles de datos en Azure con el tipo de máquina virtual DS3_v2.

- En AWS, el nivel de rendimiento puede ser SSD de uso general, SSD con aprovisionamiento IOPS o HDD optimizados para el rendimiento.

- En Azure, el nivel de rendimiento puede ser discos gestionados por SSD Premium, discos gestionados por SSD estándar o discos gestionados por HDD estándar.
- En GCP, el nivel de rendimiento puede ser SSD o HDD (discos estándar).
- Las tecnologías de cifrado admiten la organización en niveles de datos.
- Debe estar habilitado thin provisioning en los volúmenes.

Requisitos para organizar en niveles los datos fríos en AWS S3

Compruebe que Cloud Volumes ONTAP tenga una conexión con S3. La mejor forma de proporcionar esa conexión es crear un extremo de VPC con el servicio S3. Para ver instrucciones, consulte "Documentación de AWS: Crear un extremo de puerta de enlace".

Al crear el extremo VPC, asegúrese de seleccionar la región, VPC y tabla de rutas que correspondan a la instancia de Cloud Volumes ONTAP. También debe modificar el grupo de seguridad para añadir una regla de HTTPS de salida que habilite el tráfico hacia el extremo de S3. De lo contrario, Cloud Volumes ONTAP no puede conectarse con el servicio S3.

Si experimenta algún problema, consulte "Centro de conocimientos de soporte de AWS: ¿por qué no puedo conectarme a un bloque de S3 mediante un extremo de VPC de puerta de enlace?".

Requisitos para organizar los datos fríos en niveles en almacenamiento de Azure Blob

No es necesario configurar una conexión entre el nivel de rendimiento y el nivel de capacidad siempre que Cloud Manager tenga los permisos necesarios. Cloud Manager habilita un extremo de servicio vnet para usted si la política de Cloud Manager tiene estos permisos:

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

Los permisos se incluyen en el último "Política de Cloud Manager".

Requisitos para organizar los datos inactivos en niveles en Google Cloud Storage cucharón

- La subred en la que reside Cloud Volumes ONTAP debe estar configurada para acceso privado a Google. Para obtener instrucciones, consulte "Documentación de Google Cloud: Configuración de Private Google Access".
- Se necesita una cuenta de servicio que tenga el rol predefinido Storage Admin. Deberá seleccionar esta cuenta de servicio al crear un entorno de trabajo de Cloud Volumes ONTAP.

  "Configure esta cuenta de servicio de organización en niveles del siguiente modo":

  a. Asigne el rol *Storage Admin* predefinido a la cuenta del servicio de organización en niveles.
  b. Agregue la cuenta de servicio conector como un *Usuario de cuenta de servicio* a la cuenta de servicio de organización en niveles.

     Puede proporcionar el rol de usuario "en el paso 3 del asistente al crear el cuenta de servicio de organización en niveles", o. "otorgue el rol después de crear la cuenta de servicio".

     Deberá seleccionar más adelante la cuenta del servicio de organización en niveles cuando cree un entorno de trabajo de Cloud Volumes ONTAP.

Si no habilita la organización en niveles de datos y selecciona una cuenta de servicio al crear el sistema Cloud Volumes ONTAP, tendrá que desactivar el sistema y añadir la cuenta de servicio a Cloud Volumes ONTAP desde la consola de GCP.

Organización en niveles de los datos de volúmenes de lectura y escritura

Cloud Volumes ONTAP puede organizar los datos inactivos en niveles en volúmenes de lectura y escritura para un almacenamiento de objetos rentable, liberando al nivel de rendimiento de los datos activos.

Pasos

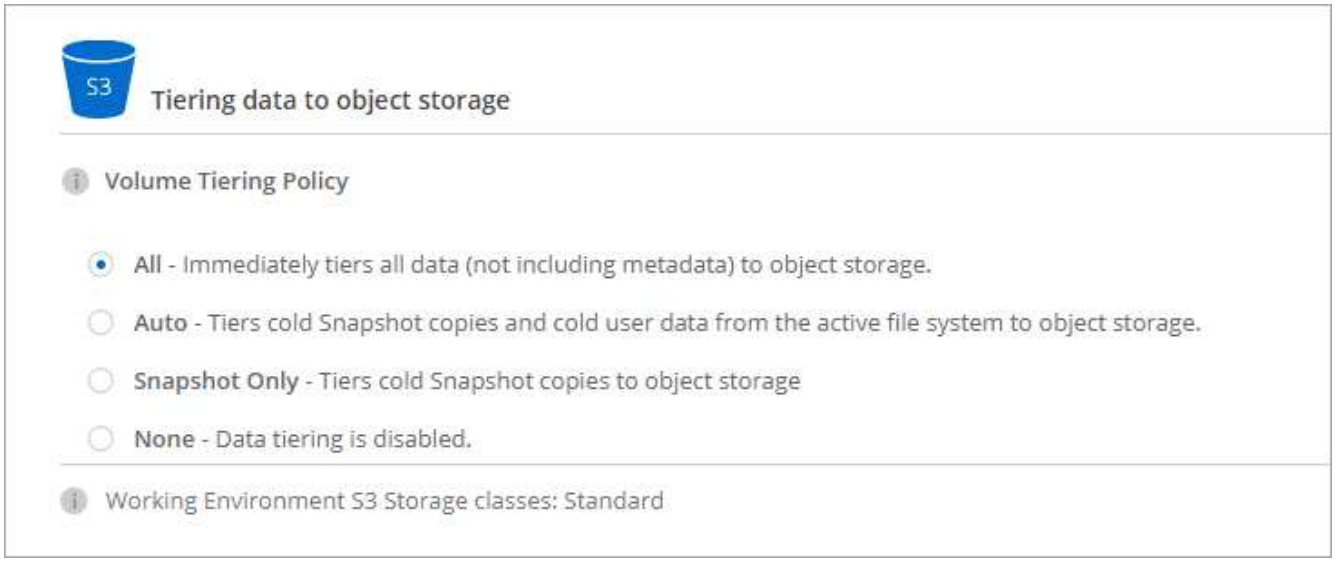
1. En el entorno de trabajo, cree un volumen nuevo o cambie el nivel de un volumen existente:

Tarea	Acción
Cree un nuevo volumen	Haga clic en **Añadir nuevo volumen**.
Modifique un volumen existente	Seleccione el volumen y haga clic en **Change Disk Type & Tiering Policy**.

2. Seleccione una política de organización en niveles.

   Para obtener una descripción de estas políticas, consulte "Información general sobre organización en niveles de datos".

   ejemplo



   Cloud Manager crea un nuevo agregado para el volumen si aún no existe un agregado con organización en niveles de datos habilitada.

   Si prefiere crear agregados usted mismo, puede habilitar la organización en niveles de datos en los agregados al crearlos.

Organización en niveles de los datos de los volúmenes de protección de datos

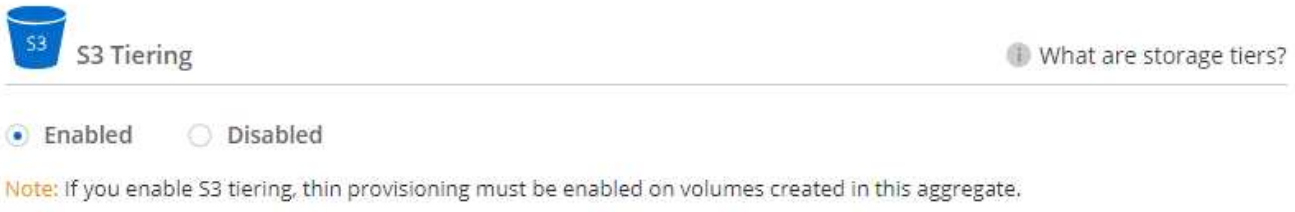
Cloud Volumes ONTAP puede organizar los datos en niveles desde un volumen de protección de datos a un nivel de capacidad. Si activa el volumen de destino, los datos se mueven gradualmente al nivel de rendimiento

a medida que se leen.

Pasos

1. En la página entornos de trabajo, seleccione el entorno de trabajo que contiene el volumen de origen y, a continuación, arrástrelo al entorno de trabajo al que desea replicar el volumen.
2. Siga las indicaciones hasta llegar a la página Tiering y habilitar la organización en niveles de datos en el almacenamiento de objetos.

   ejemplo



   Para obtener ayuda sobre la replicación de datos, consulte "Replicar datos hacia y desde el cloud".

Cambio del tipo de almacenamiento para datos organizados por niveles

Después de poner en marcha Cloud Volumes ONTAP, puede reducir sus costes de almacenamiento cambiando la clase de almacenamiento para los datos inactivos a los que no se ha accedido durante 30 días. Los costes de acceso son más elevados si se accede a los datos, por lo que debe tener en cuenta antes de cambiar la clase de almacenamiento.

El tipo de almacenamiento para los datos por niveles es de amplio alcance del sistema: it no por volumen.

Para obtener más información sobre las clases de almacenamiento compatibles, consulte "Información general sobre organización en niveles de datos".

Pasos

1. En el entorno de trabajo, haga clic en el icono de menú y, a continuación, haga clic en **clases de almacenamiento** o **almacenamiento en blob**.
2. Elija una clase de almacenamiento y, a continuación, haga clic en **Guardar**.

¿Puedo habilitar la organización en niveles de los datos en un agregado existente?

No, no es posible habilitar la organización en niveles de datos en un agregado existente. Solo puede habilitar la organización en niveles de datos en nuevos agregados.

Tampoco puede habilitar la organización en niveles de los datos en un agregado nuevo "creando usted mismo un agregado" o. mediante la creación de un volumen nuevo con la función de organización en niveles de datos habilitada. A continuación, Cloud Manager crearía un nuevo agregado para el volumen en caso de que no existiera un agregado con organización en niveles de datos habilitada.

Gestionar máquinas virtuales de almacenamiento

Una máquina virtual de almacenamiento es un equipo virtual que se ejecuta en ONTAP y proporciona servicios de datos y almacenamiento a sus clientes. Puede que lo sepa como un *SVM* o un *vserver*. Cloud Volumes ONTAP se configura con una máquina virtual

de almacenamiento de forma predeterminada, pero algunas configuraciones admiten máquinas virtuales de almacenamiento adicionales.

Número admitido de máquinas virtuales de almacenamiento

Cloud Volumes ONTAP 9.7 admite varios equipos virtuales de almacenamiento en AWS con determinadas configuraciones y una licencia complementaria. "Vea el número de máquinas virtuales de almacenamiento compatibles en AWS". Póngase en contacto con el equipo de cuenta para obtener una licencia adicional SVM.

Todas las demás configuraciones de Cloud Volumes ONTAP admiten un equipo virtual de almacenamiento que sirve datos y un equipo virtual de almacenamiento de destino utilizado para la recuperación ante desastres. Puede activar el equipo virtual de almacenamiento de destino para acceder a los datos si se produce una interrupción en el equipo virtual de almacenamiento de origen.

Una máquina virtual de almacenamiento abarca todo el sistema Cloud Volumes ONTAP (par de alta disponibilidad o nodo único).

Creación de máquinas virtuales de almacenamiento adicionales

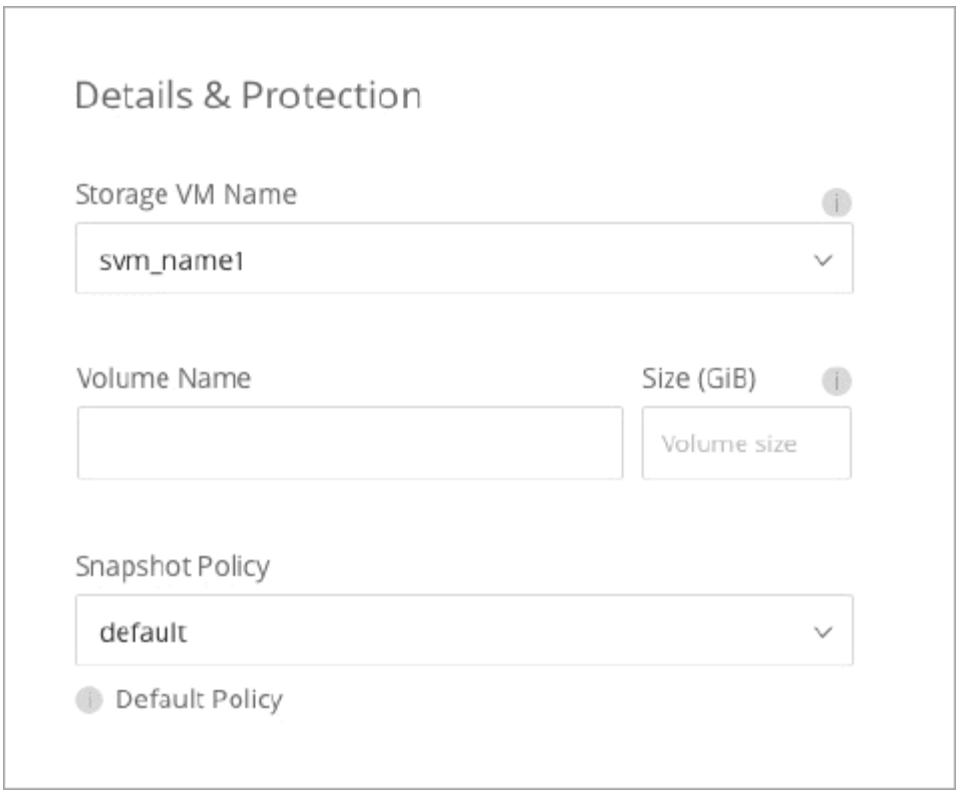
Si es compatible con su configuración, puede crear equipos virtuales de almacenamiento adicionales mediante "System Manager o CLI".

- "Creación de una SVM para el acceso de SMB"
- "Creación de una SVM para acceso NFS"
- "Creación de una SVM para acceso iSCSI"
- "Creación de una SVM de destino para recuperación ante desastres"

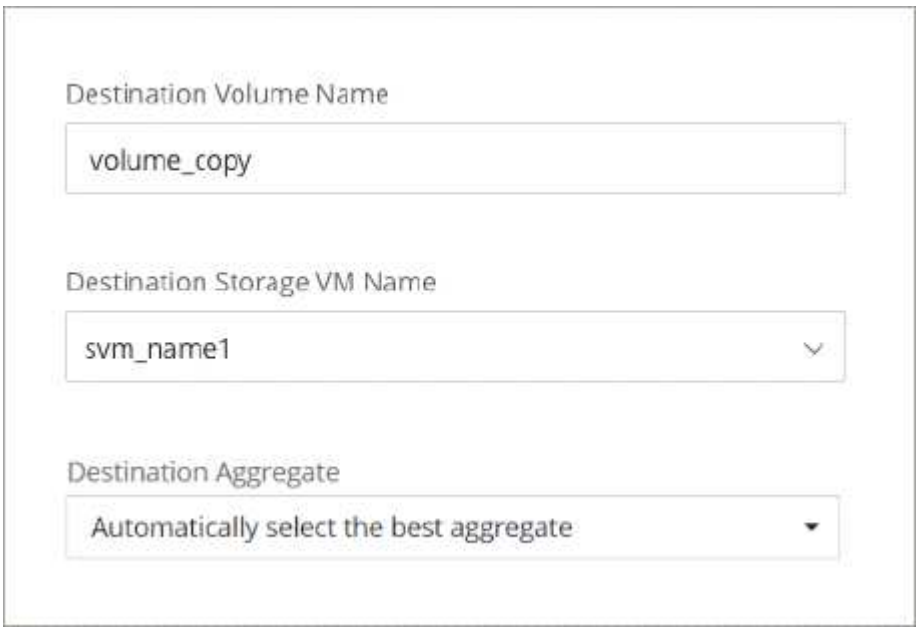
Trabajar con varias máquinas virtuales de almacenamiento en Cloud Manager

Cloud Manager admite todas las máquinas virtuales de almacenamiento adicionales que se creen desde System Manager o desde la interfaz de línea de comandos.

Por ejemplo, la siguiente imagen muestra cómo puede elegir una máquina virtual de almacenamiento al crear un volumen.



Y la siguiente imagen muestra cómo puede elegir una máquina virtual de almacenamiento cuando se replica un volumen en otro sistema.



Gestionar la recuperación ante desastres de equipos virtuales de almacenamiento

Cloud Manager no ofrece ningún tipo de configuración ni orquestación para la recuperación ante desastres de máquinas virtuales de almacenamiento. Se debe usar System Manager o la CLI.

- "Guía exprés de preparación para la recuperación de desastres de SVM"
- "Guía exprés de recuperación ante desastres de SVM"

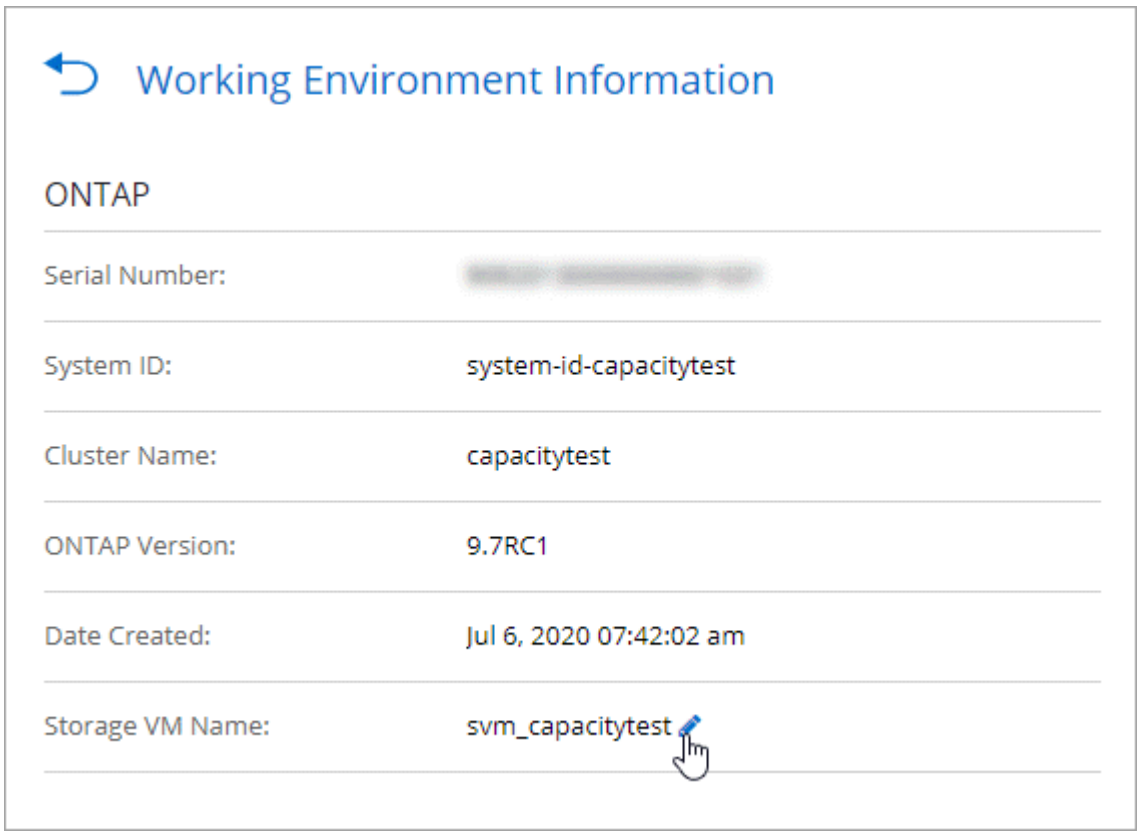
Modificación del nombre de la máquina virtual de almacenamiento

Cloud Manager nombra automáticamente a la máquina virtual de almacenamiento única que crea para Cloud Volumes ONTAP. Puede modificar el nombre de la máquina virtual de almacenamiento si tiene estrictos estándares de nomenclatura. Por ejemplo, podría que el nombre coincida con el nombre que se le da a las máquinas virtuales de almacenamiento de los clústeres de ONTAP.

Si creó cualquier máquina virtual de almacenamiento adicional para Cloud Volumes ONTAP, no podrá cambiar el nombre de las máquinas virtuales de almacenamiento desde Cloud Manager. Tendrá que hacerlo directamente desde Cloud Volumes ONTAP mediante System Manager o la CLI.

Pasos

1. En el entorno de trabajo, haga clic en el icono de menú y, a continuación, haga clic en **Información**.
2. Haga clic en el icono de edición a la derecha del nombre de la máquina virtual de almacenamiento.



3. En el cuadro de diálogo Modificar nombre de SVM, cambie el nombre y, a continuación, haga clic en **Guardar**.

Use Cloud Volumes ONTAP como almacenamiento persistente para Kubernetes

Cloud Manager puede automatizar la puesta en marcha de Trident de NetApp en clústeres de Kubernetes para que pueda usar Cloud Volumes ONTAP como almacenamiento persistente para contenedores.

Trident es un proyecto de código abierto totalmente compatible y mantenido por NetApp. Trident se integra de forma nativa con Kubernetes y su marco de trabajo de volumen persistente para aprovisionar y gestionar volúmenes desde sistemas que ejecutan cualquier combinación de plataformas de almacenamiento de NetApp. "Más información sobre Trident".

La función Kubernetes no es compatible con los clústeres de ONTAP en las instalaciones. Solo es compatible con Cloud Volumes ONTAP.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

Revise los requisitos previos

Compruebe que el entorno pueda cumplir con los requisitos previos, que incluyen conectividad entre los clústeres de Kubernetes y Cloud Volumes ONTAP, conectividad entre los clústeres de Kubernetes y un conector, una versión mínima de Kubernetes de 1.14, al menos un nodo de trabajo de un clúster y varios. Vea la lista completa.

Añada los clústeres de Kubernetes a Cloud Manager

En Cloud Manager, haga clic en **Kubernetes** y descubra los clústeres directamente desde el servicio gestionado de su proveedor de cloud o importe un clúster proporcionando un archivo kubeconfig.

Conecte los clústeres a Cloud Volumes ONTAP

Después de agregar un clúster de Kubernetes, haga clic en **conectar al entorno de trabajo** para conectar el clúster a uno o más sistemas Cloud Volumes ONTAP.

Inicie el aprovisionamiento de volúmenes persistentes

Solicite y gestione volúmenes persistentes mediante construcciones e interfaces de Kubernetes nativas. Cloud Manager crea clases de almacenamiento NFS e iSCSI que se pueden usar cuando se aprovisionan volúmenes persistentes.

"Más información sobre el aprovisionamiento de su primer volumen con Trident para Kubernetes".

Revisión de requisitos previos

Antes de empezar, compruebe que el conector y los clústeres de Kubernetes cumplen con los requisitos específicos.

Requisitos del clúster de Kubernetes

- Se requiere conectividad de red entre un clúster de Kubernetes y el conector, y entre un clúster de Kubernetes y Cloud Volumes ONTAP.

  Tanto el conector como el Cloud Volumes ONTAP necesitan una conexión con el extremo de la API de Kubernetes:

  - En el caso de clústeres gestionados, configure una ruta entre el VPC de un clúster y el VPC donde

residen el conector y Cloud Volumes ONTAP.

    - Para otros clústeres, el conector y Cloud Volumes ONTAP deben tener acceso a la dirección IP del nodo maestro o del equilibrador de carga (como se indica en el archivo kubeconfig) y debe presentar un certificado TLS válido.

- Un clúster de Kubernetes puede estar en cualquier ubicación que tenga la conectividad de red indicada anteriormente.
- Un clúster de Kubernetes debe ejecutar la versión 1.14 como mínimo.

  La versión máxima admitida es definida por Trident. "Haga clic aquí para ver la versión de Kubernetes máxima admitida".

- Un clúster de Kubernetes debe tener al menos un nodo de trabajo.
- En el caso de clústeres que se ejecutan en Amazon Elastic Kubernetes Service (Amazon EKS), cada clúster necesita un rol de IAM añadido para poder resolver un error de permiso. Después de agregar el clúster, Cloud Manager le pedirá el comando eksctl exacto que resuelve el error.

  "Obtenga información acerca de los límites de permisos de IAM".

- Para los clústeres que se ejecutan en Azure Kubernetes Service (AKS), esos clústeres deben tener asignado el rol *Azure Kubernetes Service RBAC Cluster Admin*. Esto es necesario para que Cloud Manager pueda instalar Trident y configurar las clases de almacenamiento en el clúster.
- Para los clústeres que se ejecutan en Google Kubernetes Engine (GKE), esos clústeres no deben usar el sistema operativo Container Optimized predeterminado. Debe cambiarlos para usar Ubuntu.

  De forma predeterminada, GKE utiliza Google "imagen optimizada para contenedor", que no tiene las utilidades que Trident necesita para montar volúmenes.

Requisitos del conector

Asegúrese de que se han establecido las siguientes redes y permisos para el conector.

Redes

- El conector necesita una conexión a Internet de salida para acceder a los siguientes extremos al instalar Trident:

  https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/

  Cloud Manager instala Trident en un clúster de Kubernetes cuando se conecta un entorno de trabajo al clúster.

Permisos necesarios para detectar y gestionar clústeres EKS

El conector necesita permisos de administrador para detectar y gestionar clústeres de Kubernetes que se ejecutan en Amazon Elastic Kubernetes Service (EKS):

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "eks:*",
            "Resource": "*"
        }
    ]
}
```

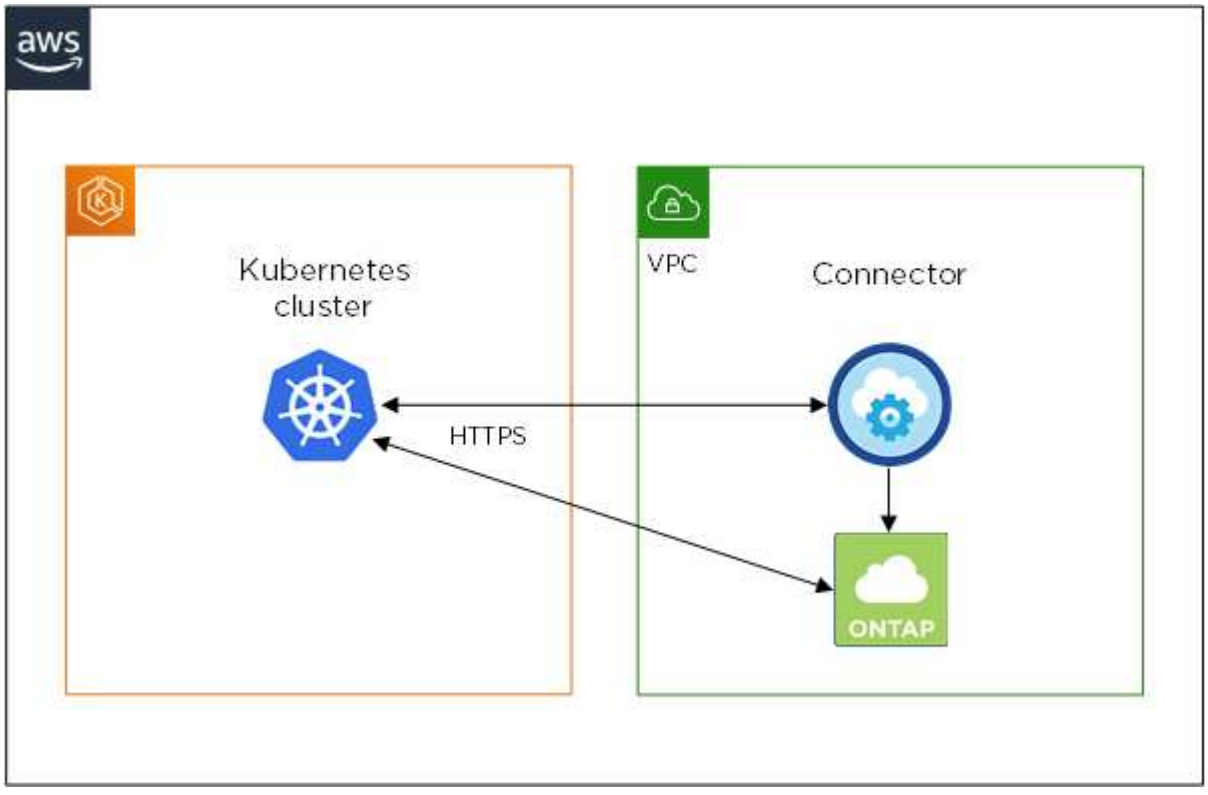
Permisos necesarios para detectar y gestionar clústeres GKE

El conector necesita los siguientes permisos para detectar y gestionar clústeres de Kubernetes que se ejecutan en Google Kubernetes Engine (GKE):

```
container.*
```

Configuración de ejemplo

En la siguiente imagen, se muestra un ejemplo de un clúster de Kubernetes que se ejecuta en Amazon Elastic Kubernetes Service (Amazon EKS) y sus conexiones a Connector y Cloud Volumes ONTAP.



Añadir clústeres de Kubernetes

Añada clústeres de Kubernetes a Cloud Manager detectando los clústeres que se ejecutan en el servicio Kubernetes gestionado por el proveedor de cloud o importando el archivo kubeconfig de un clúster.

Pasos

1. En la parte superior de Cloud Manager, haga clic en **Kubernetes**.
2. Haga clic en **Agregar clúster**.
3. Elija una de las opciones disponibles:
   - Haga clic en **detectar clústeres** para descubrir los clústeres administrados a los que Cloud Manager tiene acceso en función de los permisos que proporcionó al conector.

     Por ejemplo, si su conector se ejecuta en Google Cloud, Cloud Manager utiliza los permisos de la cuenta de servicio del conector para detectar clústeres que se ejecutan en Google Kubernetes Engine (GKE).

   - Haga clic en **Importar clúster** para importar un clúster mediante un archivo kubeconfig.

     Después de cargar el archivo, Cloud Manager verifica la conectividad al clúster y guarda una copia cifrada del archivo kubeconfig.

Resultado

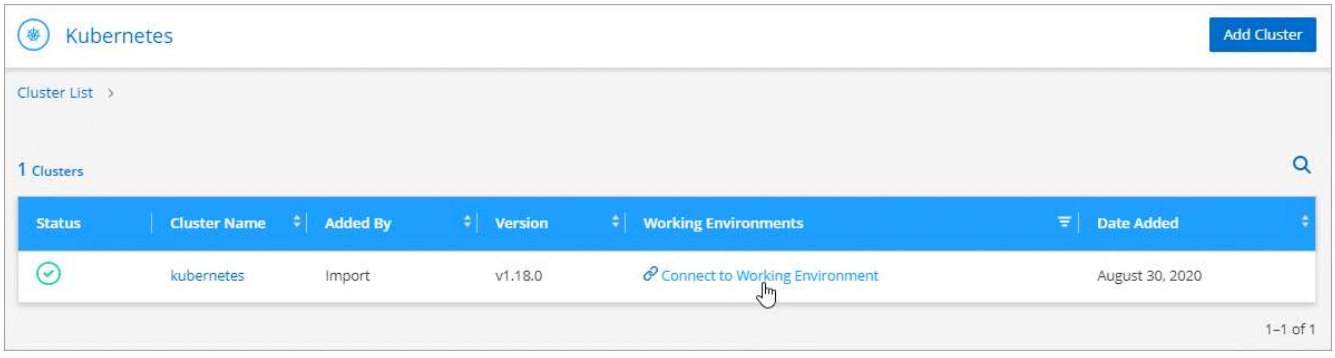
Cloud Manager agrega el clúster de Kubernetes. Ahora puede conectar el clúster a Cloud Volumes ONTAP.

Conectar un clúster a Cloud Volumes ONTAP

Conecte un clúster de Kubernetes a Cloud Volumes ONTAP para que pueda usar Cloud Volumes ONTAP como almacenamiento persistente para contenedores.

Pasos

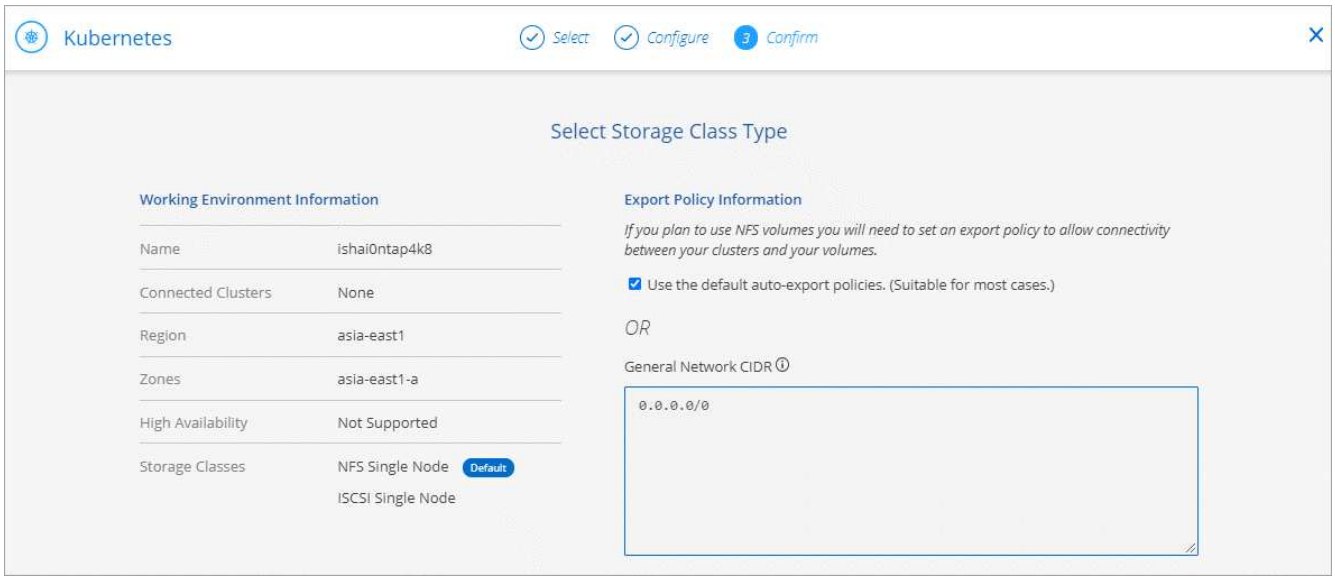
1. En la parte superior de Cloud Manager, haga clic en **Kubernetes**.
2. Haga clic en **conectar al entorno de trabajo** para el clúster que acaba de agregar.



3. Seleccione un entorno de trabajo y haga clic en **continuar**.
4. Elija la clase de almacenamiento de NetApp que se utilizará como clase de almacenamiento predeterminada para el clúster de Kubernetes y haga clic en **continuar**.

   Cuando un usuario crea un volumen persistente, el clúster de Kubernetes puede utilizar esta clase de almacenamiento como almacenamiento back-end de forma predeterminada.

5. Elija si desea utilizar directivas de exportación automática predeterminadas o si desea añadir un bloque CIDR personalizado.



6. Haga clic en **Agregar entorno de trabajo**.

Resultado

Cloud Manager conecta el entorno de trabajo al clúster, que puede tardar hasta 15 minutos.

Gestione los clústeres

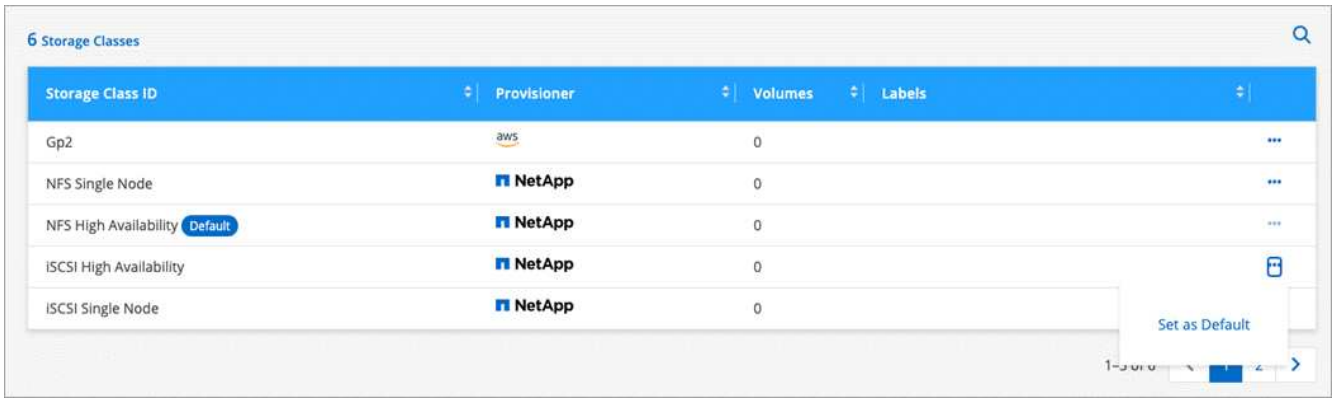
Cloud Manager le permite gestionar los clústeres de Kubernetes cambiando el tipo de almacenamiento predeterminado, actualizando Trident, etc.

Cambiando la clase de almacenamiento predeterminada

Asegúrese de haber establecido una clase de almacenamiento Cloud Volumes ONTAP como la clase de almacenamiento predeterminada para que los clústeres utilicen Cloud Volumes ONTAP como almacenamiento back-end.

Pasos

1. En la parte superior de Cloud Manager, haga clic en **Kubernetes**.
2. Haga clic en el nombre del clúster de Kubernetes.
3. En la tabla **clases de almacenamiento**, haga clic en el menú acciones situado en el extremo derecho de la clase de almacenamiento que desea establecer como predeterminada.



4. Haga clic en **establecer como predeterminado**.

Actualización de Trident

Es posible actualizar Trident desde Cloud Manager cuando hay una nueva versión de Trident disponible.

Pasos

1. En la parte superior de Cloud Manager, haga clic en **Kubernetes**.
2. Haga clic en el nombre del clúster de Kubernetes.
3. Si hay una nueva versión disponible, haga clic en **Actualizar** junto a la versión Trident.

Actualizando el archivo kubeconfig

Si agregó el clúster a Cloud Manager importando el archivo kubeconfig, puede cargar el archivo más reciente kubeconfig en Cloud Manager en cualquier momento. Puede hacer esto si actualizó las credenciales, si ha cambiado usuarios o roles, o si algo cambió que afecta el clúster, el usuario, los espacios de nombres o la autenticación.

Pasos

1. En la parte superior de Cloud Manager, haga clic en **Kubernetes**.
2. Haga clic en el nombre del clúster de Kubernetes.
3. Haga clic en **Actualizar Kubeconfig**.
4. Cuando se le solicite a través del explorador Web, seleccione el archivo kubeconfig actualizado y haga clic en **Abrir**.

Resultado

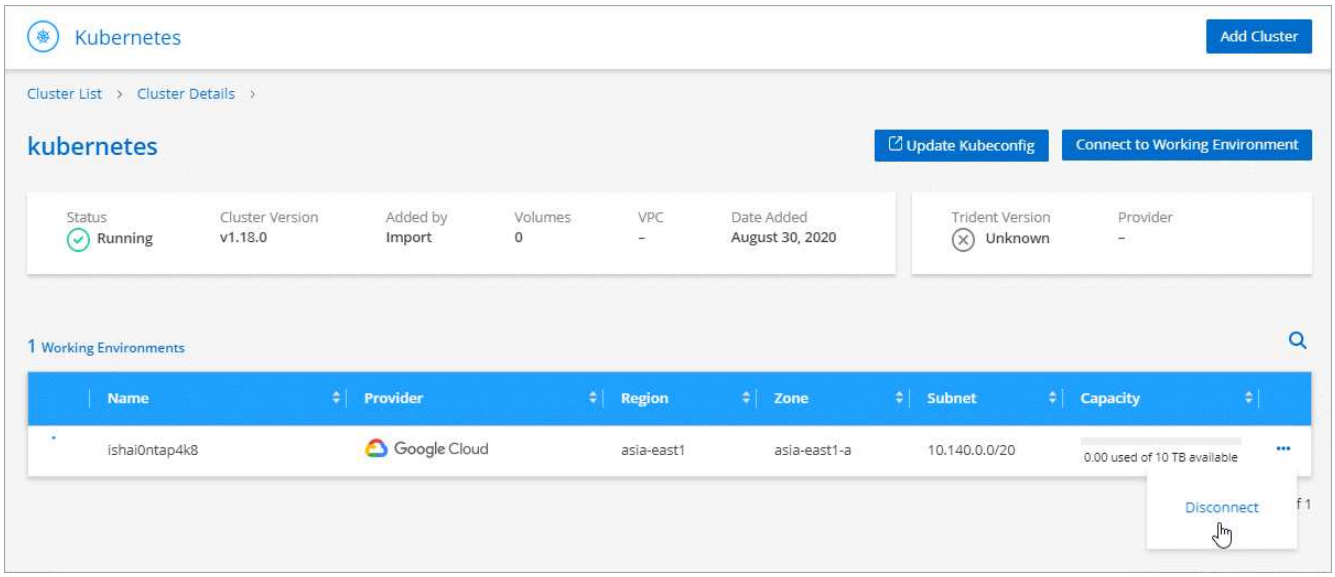
Cloud Manager actualiza la información sobre el clúster de Kubernetes en función del archivo más reciente kubeconfig.

Desconectar un clúster

Cuando se desconecta un clúster de Cloud Volumes ONTAP, ya no se puede usar ese sistema Cloud Volumes ONTAP como almacenamiento persistente para contenedores. No se eliminan los volúmenes persistentes existentes.

Pasos

1. En la parte superior de Cloud Manager, haga clic en **Kubernetes**.
2. Haga clic en el nombre del clúster de Kubernetes.
3. En la tabla **entornos de trabajo**, haga clic en el menú acciones situado en el extremo derecho del entorno de trabajo que desea desconectar.



4. Haga clic en **desconectar**.

Resultado

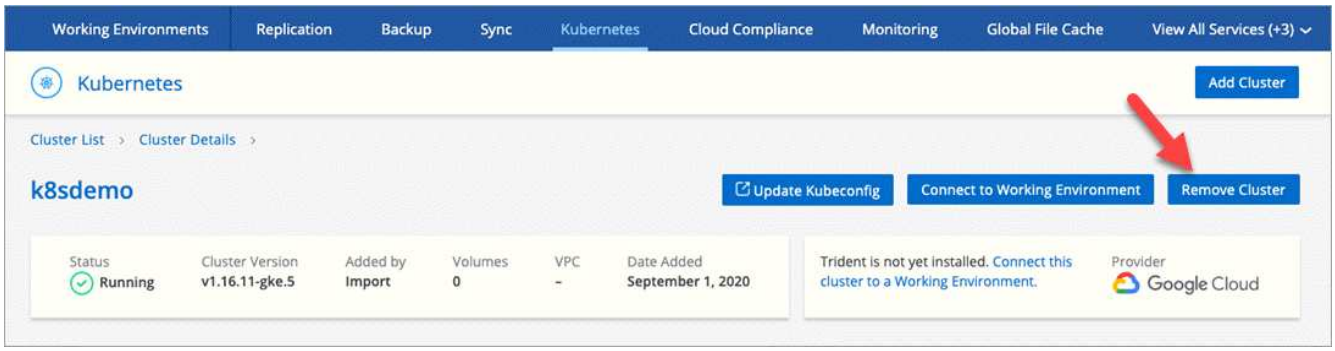
Cloud Manager desconecta el clúster del sistema Cloud Volumes ONTAP.

Quitar un clúster

Quite los clústeres retirados del servicio de Cloud Manager después de desconectar todos los entornos de trabajo del clúster.

Pasos

1. En la parte superior de Cloud Manager, haga clic en **Kubernetes**.
2. Haga clic en el nombre del clúster de Kubernetes.
3. Haga clic en **Quitar clúster**.



Cifrar volúmenes con soluciones de cifrado de NetApp

Cloud Volumes ONTAP es compatible tanto con el cifrado de volúmenes de NetApp (NVE) como con el cifrado de agregados de NetApp (NAE) con un gestor de claves externo. NVE y NAE son soluciones basadas en software que permiten (FIPS) cifrado de volúmenes para datos en reposo conforme a la normativa 140-2. "Obtenga más información sobre estas soluciones de cifrado".

A partir de Cloud Volumes ONTAP 9.7, los nuevos agregados tendrán NAE habilitado de forma predeterminada después de configurar un gestor de claves externo. Los volúmenes nuevos que no forman parte de un agregado de NAE tendrán el valor de NVE habilitado de forma predeterminada (por ejemplo, si tiene agregados existentes que se crearon antes de configurar un gestor de claves externo).

Cloud Volumes ONTAP no admite la gestión de claves incorporada.

Lo que necesitará

Su sistema Cloud Volumes ONTAP debe registrarse con el soporte de NetApp. A partir de Cloud Manager 3.7.1, se instala automáticamente una licencia de cifrado de volúmenes de NetApp en cada sistema Cloud Volumes ONTAP registrado en el servicio de soporte de NetApp.

- "Adición de cuentas del sitio de soporte de NetApp a Cloud Manager"
- "Registro de sistemas de pago por uso"

Cloud Manager no instala la licencia NVE en sistemas que residen en la región China.

Pasos

1. Revise la lista de administradores de claves compatibles en la "Herramienta de matriz de interoperabilidad de NetApp".

   Busque la solución **Key Managers**.

2. "Conéctese a la CLI de Cloud Volumes ONTAP".
3. Instale certificados SSL y conéctese a los servidores de gestión de claves externos.

   "Guía completa de cifrado de NetApp para ONTAP 9: Configuración de gestión de claves externas"

Replicación de datos entre sistemas

Puede replicar datos entre entornos de trabajo eligiendo una replicación de datos única para la transferencia de datos, o una programación recurrente para la recuperación ante desastres o la retención a largo plazo. Por ejemplo, puede configurar la replicación de datos desde un sistema ONTAP en las instalaciones a Cloud Volumes ONTAP para la recuperación ante desastres.

Cloud Manager simplifica la replicación de datos entre volúmenes en sistemas independientes con tecnologías SnapMirror y SnapVault. Solo tiene que identificar el volumen de origen y el de destino y, a continuación, elegir una programación y una política de replicación. Cloud Manager compra los discos necesarios, configura las relaciones, aplica la política de replicación y, a continuación, inicia la transferencia básica entre los volúmenes.

La transferencia básica incluye una copia completa de los datos de origen. Las transferencias posteriores contienen copias diferenciales de los datos de origen.

Cloud Manager permite la replicación de datos entre los siguientes tipos de entornos de trabajo:

- De un sistema Cloud Volumes ONTAP a otro Cloud Volumes Sistema ONTAP
- Entre un sistema Cloud Volumes ONTAP y un ONTAP en las instalaciones clúster
- De un clúster de ONTAP en las instalaciones a otro clúster de ONTAP en las instalaciones

Requisitos de replicación de datos

Antes de poder replicar datos, debe confirmar que se cumplen requisitos específicos tanto para los sistemas Cloud Volumes ONTAP como para los clústeres de ONTAP.

Requisitos de versión

Debe verificar que los volúmenes de origen y destino ejecutan versiones de ONTAP compatibles antes de replicar los datos. Para obtener más detalles, consulte "Guía completa de protección de datos".

Requisitos específicos de Cloud Volumes ONTAP

- El grupo de seguridad de la instancia debe incluir las reglas de entrada y salida necesarias: Específicamente, reglas para ICMP y los puertos 11104 y 11105.

  Estas reglas se incluyen en el grupo de seguridad predefinido.

- Para replicar datos entre dos sistemas Cloud Volumes ONTAP en subredes diferentes, las subredes deben enrutarse juntas (esta es la configuración predeterminada).
- Para replicar datos entre un sistema Cloud Volumes ONTAP en AWS y un sistema en Azure, debe tener una conexión VPN entre el VPC de AWS y la vnet de Azure.

Requisitos específicos de los clústeres de ONTAP

- Debe instalarse una licencia de SnapMirror activa.
- Si el clúster está en sus instalaciones, debe tener una conexión desde la red corporativa a AWS o Azure, que suele ser una conexión de VPN.
- Los clústeres de ONTAP deben cumplir con requisitos adicionales de subred, puerto, firewall y clúster.

  Para obtener detalles, consulte la Guía exprés de paridad de clústeres y SVM para su versión de ONTAP.

Configurar la replicación de datos entre sistemas

Puede replicar datos entre sistemas Cloud Volumes ONTAP y clústeres ONTAP eligiendo una replicación de datos única, que puede ayudarle a mover datos hacia y desde el cloud, o una programación recurrente, que puede ayudar con la recuperación ante desastres o la retención a largo plazo.

Acerca de esta tarea

Cloud Manager admite configuraciones sencillas, con ventilador y de protección de datos en cascada:

- En una configuración sencilla, la replicación se produce del volumen A al volumen B.
- En una configuración de fanout, la replicación se produce del volumen A a varios destinos.
- En una configuración en cascada, la replicación ocurre del volumen A al volumen B y del volumen B al volumen C.

Puede configurar las configuraciones de fanout y cascada en Cloud Manager configurando múltiples replicaciones de datos entre sistemas. Por ejemplo, replicando un volumen del sistema A al sistema B y, a continuación, replicando el mismo volumen del sistema B al sistema C.

Pasos

1. En la página entornos de trabajo, seleccione el entorno de trabajo que contiene el volumen de origen y, a continuación, arrástrelo al entorno de trabajo al que desea replicar el volumen:

2. Si aparecen las páginas Source y Destination peering Setup, seleccione todas las LIF de interconexión de clústeres para la relación de paridad de clústeres.

   La red de interconexión de clústeres se debe configurar de modo que los pares de clústeres tengan una conectividad de malla completa en función de par, lo que significa que cada par de clústeres de una relación de paridad de clústeres tiene conectividad entre todas sus LIF de interconexión de clústeres.

   Estas páginas aparecen si un clúster ONTAP que tiene varias LIF es el origen o el destino.

3. En la página Source Volume Selection, seleccione el volumen que desea replicar.
4. En la página Nombre del volumen de destino y clasificación por niveles, especifique el nombre del volumen de destino, elija un tipo de disco subyacente, cambie cualquiera de las opciones avanzadas y, a continuación, haga clic en **continuar**.

   Si el destino es un clúster de ONTAP, también debe especificar la SVM de destino y el agregado.

5. En la página Max Transfer Rate, especifique la velocidad máxima (en megabytes por segundo) a la que se pueden transferir los datos.
6. En la página Directiva de replicación, elija una de las directivas predeterminadas o haga clic en * Directivas adicionales* y, a continuación, seleccione una de las directivas avanzadas.

Para obtener ayuda, consulte "Elegir una política de replicación".

Si selecciona una política de backup (SnapVault) personalizada, las etiquetas asociadas con la política deben coincidir con las etiquetas de las copias de Snapshot en el volumen de origen. Para obtener más información, consulte "Cómo funcionan las políticas de backup".

7. En la página Schedule, seleccione una copia única o una programación recurrente.

   Hay varios horarios predeterminados disponibles. Si desea crear una programación diferente, debe crear una nueva en el clúster *Destination* mediante System Manager.

8. En la página Review, revise las selecciones y, a continuación, haga clic en **Go**.

Resultado

Cloud Manager inicia el proceso de replicación de datos. Puede ver detalles sobre la replicación en la página Replication Status.

Gestionar programaciones y relaciones de replicación de datos

Después de configurar la replicación de datos entre dos sistemas, puede gestionar la programación y la relación de replicación de datos desde Cloud Manager.

Pasos

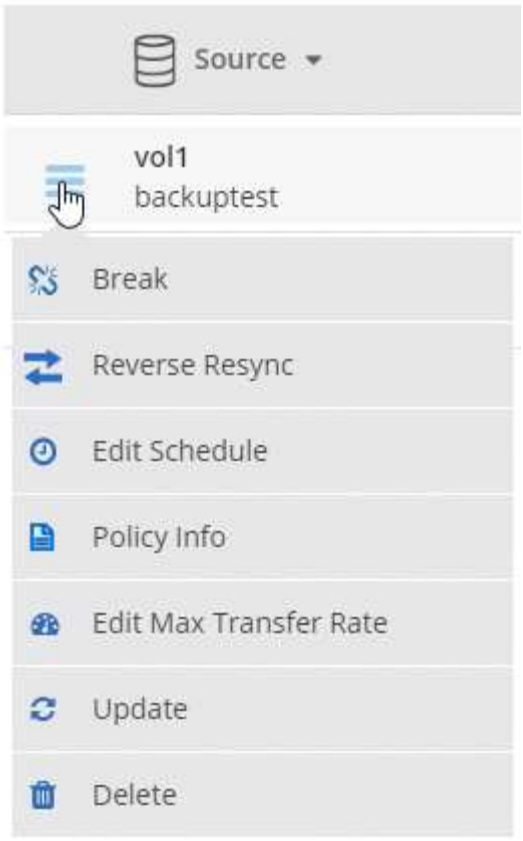
1. En la página entornos de trabajo, consulte el estado de replicación de todos los entornos de trabajo del área de trabajo o de un entorno de trabajo específico:

Opción	Acción
Todos los entornos de trabajo del espacio de trabajo	En la parte superior de Cloud Manager, haga clic en **replicación**.
Un entorno de trabajo específico	Abra el entorno de trabajo y haga clic en **replicaciones**.

2. Revisar el estado de las relaciones de replicación de datos para verificar que están en buen estado.

   Si el estado de una relación está inactivo y el estado de reflejo no se ha inicializado, debe inicializar la relación desde el sistema de destino para que la replicación de datos se realice de acuerdo con la programación definida. Puede inicializar la relación mediante System Manager o la interfaz de línea de comandos (CLI). Estos estados pueden aparecer cuando el sistema de destino falla y, a continuación, vuelve a estar online.

3. Seleccione el icono de menú junto al volumen de origen y, a continuación, elija una de las acciones disponibles.



En la siguiente tabla se describen las acciones disponibles:

Acción	Descripción
Interrumpir	Rompe la relación entre los volúmenes de origen y de destino, y activa el volumen de destino para acceder a los datos. Esta opción suele utilizarse cuando el volumen de origen no puede servir datos debido a eventos como datos dañados, una eliminación accidental o un estado sin conexión. Para obtener información sobre la configuración de un volumen de destino para el acceso a los datos y la reactivación de un volumen de origen, consulte la Guía exprés de recuperación de desastres de volúmenes de ONTAP 9.
Resincronizcar	Vuelve a establecer una relación rota entre volúmenes y reanuda la replicación de datos de acuerdo con la programación definida. Cuando se resincronizan los volúmenes, el contenido del volumen de destino se sobrescribe con el contenido del volumen de origen. Para realizar una resincronización inversa, que resincronizará los datos del volumen de destino con el volumen de origen, consulte "Guía exprés de recuperación de desastres de volúmenes de ONTAP 9".
Resincronización inversa	Revierte los roles de los volúmenes de origen y destino. El contenido del volumen de origen original se sobrescribe con el contenido del volumen de destino. Esto es útil cuando se desea reactivar un volumen de origen que se desconectó. No se conservan todos los datos escritos en el volumen de origen original entre la última replicación de datos y la hora en la que se deshabilitó el volumen de origen.

Acción	Descripción
Editar programación	Le permite elegir una programación diferente para la replicación de datos.
Información sobre políticas	Muestra la política de protección asignada a la relación de replicación de datos.
Editar velocidad máxima de transferencia	Permite editar la frecuencia máxima (en kilobytes por segundo) a la que se pueden transferir los datos.
Actualizar	Inicia una transferencia incremental para actualizar el volumen de destino.
Eliminar	Elimina la relación de protección de datos entre los volúmenes de origen y de destino, lo que significa que ya no se produce la replicación de datos entre los volúmenes. Esta acción no activa el volumen de destino para acceder a los datos. Esta acción también elimina la relación de paridad entre clústeres y la relación entre iguales de máquinas virtuales de almacenamiento (SVM), si no hay otras relaciones de protección de datos entre los sistemas.

Resultado

Después de seleccionar una acción, Cloud Manager actualiza la relación o la programación.

Elegir una política de replicación

Es posible que necesite ayuda para elegir una política de replicación al configurar la replicación de datos en Cloud Manager. Una política de replicación define cómo el sistema de almacenamiento replica los datos de un volumen de origen a un volumen de destino.

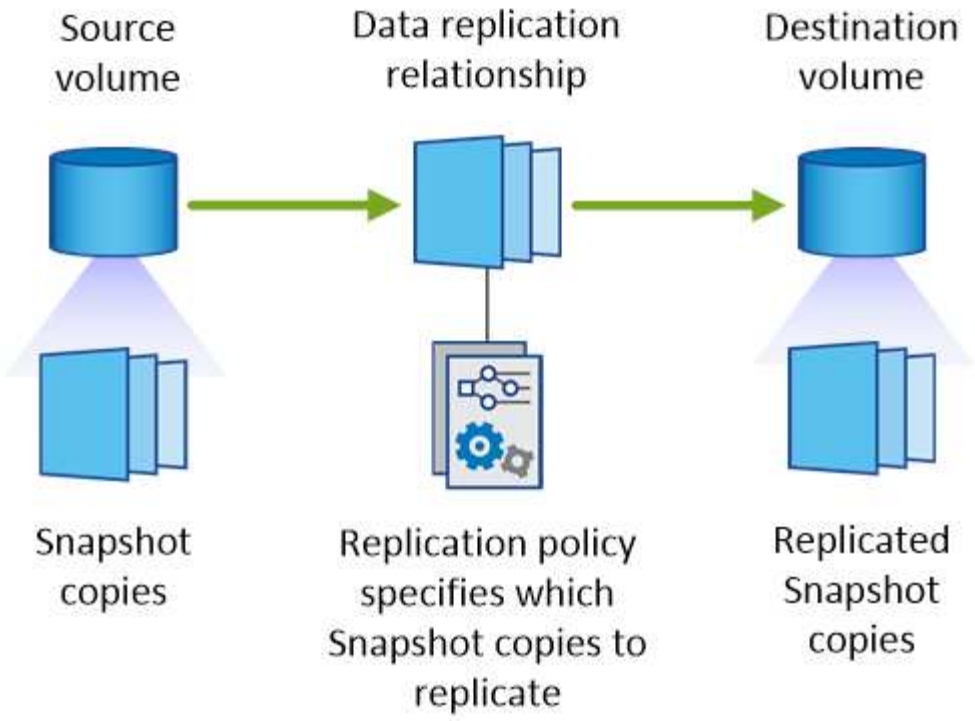
Lo que hacen las políticas de replicación

El sistema operativo ONTAP crea automáticamente backups llamados copias snapshot. Una copia Snapshot es una imagen de solo lectura de un volumen que captura el estado del sistema de archivos en un momento específico.

Cuando se replican datos entre sistemas, se replican copias Snapshot de un volumen de origen a un volumen de destino. Una política de replicación especifica las copias de Snapshot que se van a replicar del volumen de origen al volumen de destino.

Las normativas de replicación también se conocen como políticas de *protection* porque se alimentan de las tecnologías SnapMirror y SnapVault, que proporcionan protección de recuperación ante desastres y backup y recuperación de datos de disco a disco.

En la siguiente imagen, se muestra la relación entre las copias Snapshot y las políticas de replicación:



Tipos de políticas de replicación

Existen tres tipos de políticas de replicación:

- Una directiva *Mirror* replica las copias Snapshot recién creadas en un volumen de destino.

  Es posible usar estas copias Snapshot para proteger el volumen de origen como preparación para la recuperación ante desastres o para la replicación de datos que se realiza una vez. Puede activar el volumen de destino para acceder a los datos en cualquier momento.

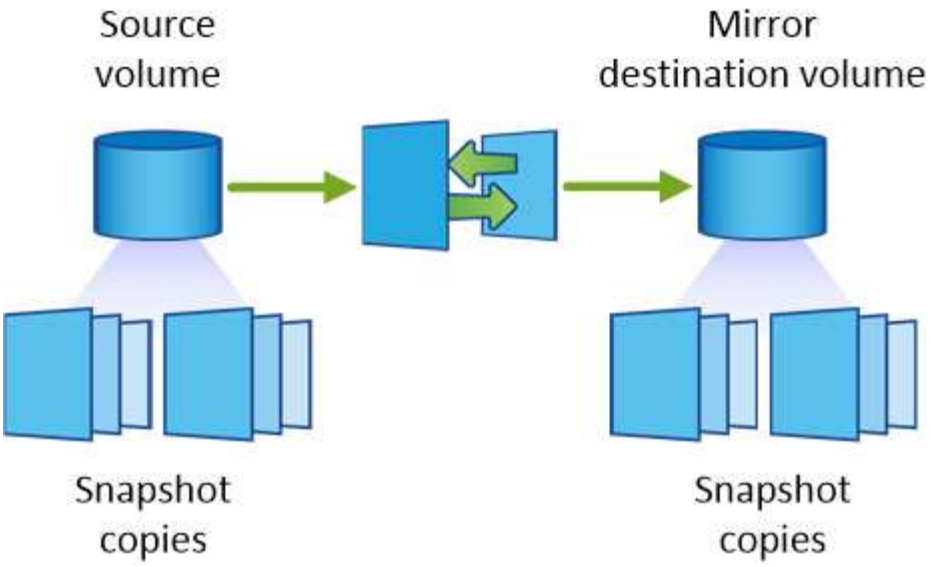
- Una política de *Backup* replica copias Snapshot específicas a un volumen de destino y, normalmente, las conserva durante un período de tiempo más largo del que tendría en el volumen de origen.

  Puede restaurar datos de estas copias Snapshot cuando se dañen o se pierdan datos, y conservarlas para cumplir los estándares y otros fines relacionados con la regulación.

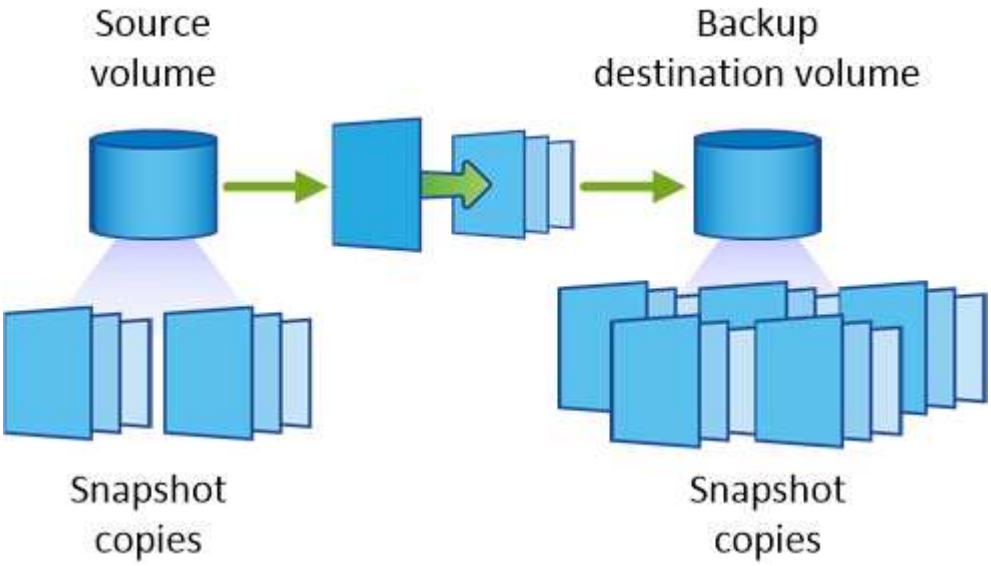
- Una política de *Mirror and Backup* proporciona recuperación ante desastres y retención a largo plazo.

  Cada sistema incluye una política predeterminada de copia de seguridad y copia de seguridad, que funciona bien en muchas situaciones. Si necesita políticas personalizadas, puede crear propias con System Manager.

En las siguientes imágenes, se muestra la diferencia entre las políticas de reflejo y backup. Una política de mirroring refleja las copias Snapshot disponibles en el volumen de origen.



Normalmente, una política de backup retiene copias Snapshot durante más tiempo del que se conservan en el volumen de origen:



Cómo funcionan las políticas de backup

A diferencia de las políticas de mirroring, las políticas de backup (SnapVault) replican copias Snapshot específicas a un volumen de destino. Es importante comprender cómo funcionan las políticas de backup si desea utilizar sus propias políticas en lugar de las predeterminadas.

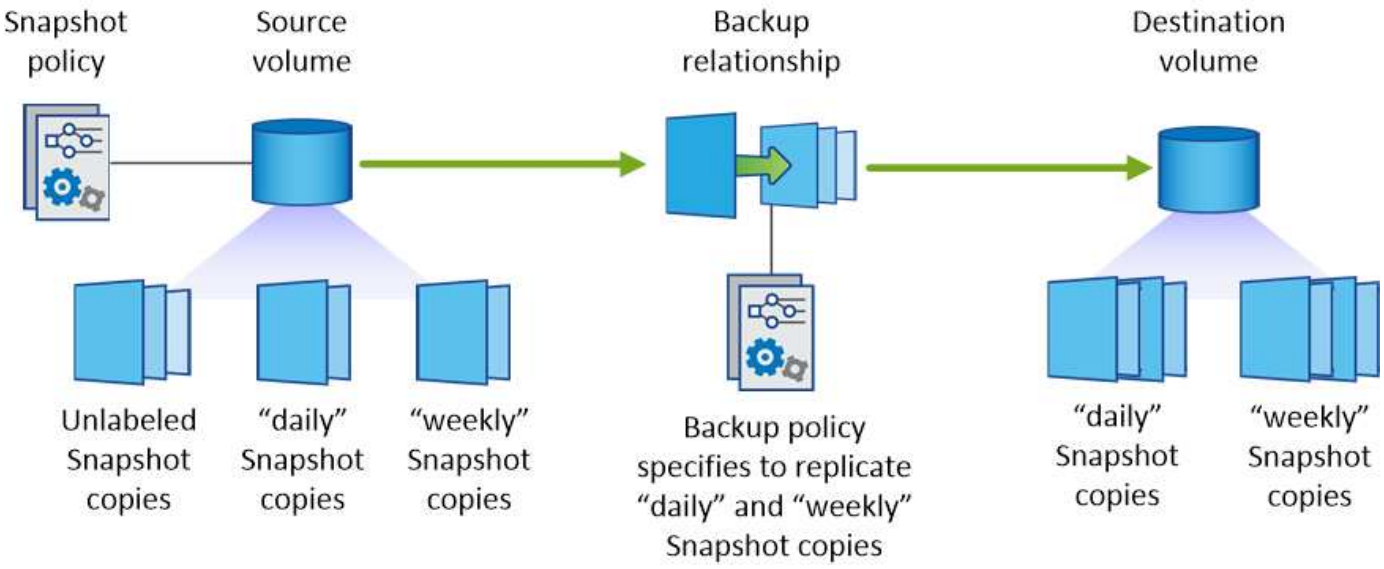
Descripción de la relación entre las etiquetas de copia de Snapshot y las políticas de backup

Una política de Snapshot define el modo en que el sistema crea copias Snapshot de los volúmenes. La política especifica cuándo crear las copias Snapshot, cuántas copias se deben conservar y cómo etiquetarlas. Por ejemplo, un sistema puede crear una copia Snapshot todos los días a las 12:10 a.m., retener las dos copias más recientes y etiquetarlas "diarias".

Una política de backup incluye reglas que especifican las etiquetas que las copias Snapshot se replican en un volumen de destino y cuántas copias se retendrán. Las etiquetas definidas en una política de backup deben coincidir con una o más etiquetas definidas en una política de Snapshot. De lo contrario, el sistema no puede

replicar ninguna copia Snapshot.

Por ejemplo, una política de backup que incluya las etiquetas "diaria" y "semanal" provoca la replicación de copias Snapshot que solo incluyen esas etiquetas. No se replican ninguna otra copia Snapshot, como se muestra en la siguiente imagen:



Directivas predeterminadas y personalizadas

La política de Snapshot predeterminada crea copias de SnapVault cada hora, cada día y cada semana, y conserva seis copias de Snapshot cada hora, dos días y dos semanas.

Puede utilizar fácilmente una política de backup predeterminada con la política de Snapshot predeterminada. Las normativas de backup predeterminadas replican las copias snapshot diarias y semanales, y conservan siete copias snapshot diarias y 52 semanales.

Si crea directivas personalizadas, las etiquetas definidas por dichas directivas deben coincidir. Puede crear políticas personalizadas mediante System Manager.

Replicación de datos de NetApp HCI a Cloud Volumes ONTAP

Si intenta replicar datos de NetApp HCI en Cloud Volumes ONTAP, puede hacerlo en un sistema NetApp HCI que ejecuta el software NetApp Element mediante SnapMirror. También puede replicar datos en volúmenes creados en un sistema ONTAP Select que se ejecuta como invitado virtual de una solución de NetApp HCI en Cloud Volumes ONTAP.

Consulte los siguientes informes técnicos para obtener detalles:

- "Informe técnico 4641: Protección de datos de NetApp HCI"
- "Informe técnico 4651: Arquitectura y configuración de SnapMirror para SolidFire de NetApp"

Supervisión del rendimiento

Obtenga más información sobre el servicio Supervisión

Aprovechando la "Servicio Cloud Insights de NetApp", Cloud Manager le proporciona

información sobre el estado y el rendimiento de sus instancias de Cloud Volumes ONTAP y le ayuda a solucionar problemas y optimizar el rendimiento de su entorno de almacenamiento en cloud.

Funciones

- Supervise automáticamente todos los volúmenes
- Puede ver datos de rendimiento de volúmenes en términos de IOPS, rendimiento y latencia
- Identifique los problemas de rendimiento para minimizar el impacto en sus usuarios y y. aplicaciones

Proveedores de cloud compatibles

El servicio de supervisión es compatible con Cloud Volumes ONTAP para AWS.

Coste

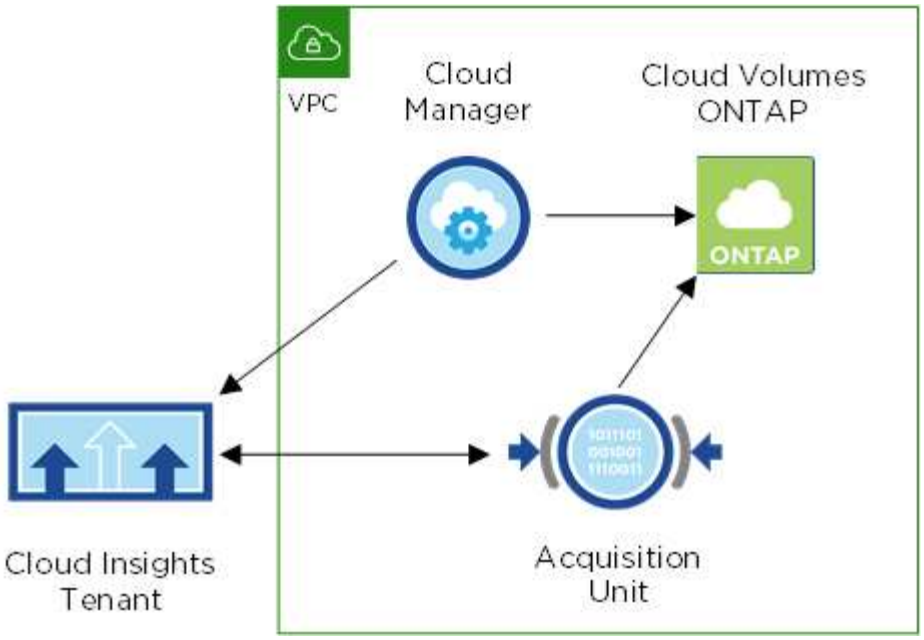
La supervisión está disponible actualmente como una vista previa. La activación es gratuita, pero Cloud Manager lanza una máquina virtual en su VPC para facilitar la supervisión. Esta máquina virtual cobra a su proveedor de cloud.

Funcionamiento de Cloud Insights con Cloud Manager

En un nivel superior, la integración de Cloud Insights con Cloud Manager funciona como el siguiente:

1. El servicio de supervisión se habilita en Cloud Volumes ONTAP.
2. Cloud Manager configura su entorno. Realiza lo siguiente:
    a. Crea un inquilino Cloud Insights (también llamado *Environment*) y asocia todos los usuarios de la cuenta de Cloud Central al inquilino.
    b. Permite una prueba gratuita de 30 días de Cloud Insights.
    c. Pone en marcha una máquina virtual en su VPC denominada unidad de adquisición, que facilita la supervisión de los volúmenes (a este respecto, la VM mencionada en la sección de costes anterior).
    d. Conecta la unidad de adquisición a Cloud Volumes ONTAP y al inquilino Cloud Insights.
3. En Cloud Manager, haga clic en Monitoring y utilice los datos de rendimiento para solucionar problemas y optimizar el rendimiento.

En la siguiente imagen se muestra la relación entre estos componentes:



La Unidad de adquisición

Al habilitar Supervisión, Cloud Manager implementa una unidad de adquisición en la misma subred que el conector.

Una *Unidad de adquisición* recopila datos de rendimiento de Cloud Volumes ONTAP y los envía al arrendatario Cloud Insights. Cloud Manager, después, consulta esos datos y los presenta.

Tenga en cuenta lo siguiente acerca de la instancia de Unidad de adquisición:

- La Unidad de adquisición se ejecuta en una instancia t3.xlarge con un volumen GP2 de 100 GB.
- La instancia se denomina *AcquisitionUnit* con un hash generado (UUID) concatenado. Por ejemplo: *AcquisitionUnit-FAN7FqeH*
- Sólo se despliega una unidad de adquisición por conector.
- La instancia debe estar en ejecución para acceder a la información de rendimiento en la pestaña Supervisión.

Cliente Cloud Insights

Cloud Manager configura un *inquilino* para usted al habilitar Monitoring. Un inquilino de Cloud Insights le permite acceder a los datos de rendimiento que recopila la unidad de adquisición. El inquilino es una partición de datos segura dentro del servicio Cloud Insights de NetApp.

Interfaz web de Cloud Insights

La pestaña Monitoring de Cloud Manager proporciona datos de rendimiento básicos para los volúmenes. Desde el explorador, puede ir a la interfaz web de Cloud Insights para realizar supervisión más profunda y configurar alertas para sus sistemas Cloud Volumes ONTAP.

Prueba y suscripción gratuitas

Cloud Manager permite una prueba gratuita de 30 días de Cloud Insights para proporcionar datos de rendimiento en Cloud Manager y para que pueda explorar las funciones que ofrece la edición estándar de Cloud Insights.

Debe suscribirse al final de la prueba gratuita o su inquilino de Cloud Insights se eliminará al final. Puede suscribirse a la edición Basic, Standard o Premium para continuar usando la función Monitoring en Cloud Manager.

"Obtenga más información sobre cómo suscribirse a Cloud Insights".

Supervisión de Cloud Volumes ONTAP en AWS

Complete unos pasos para empezar a supervisar el rendimiento de Cloud Volumes ONTAP.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

Verifique la compatibilidad con la configuración

Necesita una nueva instalación de Cloud Manager 3.8.4 o posterior en AWS o Cloud Volumes ONTAP en AWS, y debe ser un nuevo cliente de Cloud Insights.

Active la supervisión en su sistema nuevo o existente

- Nuevos entornos de trabajo: Asegúrese de mantener la monitorización activada al crear el entorno de trabajo (está activada de forma predeterminada).
- Entornos de trabajo existentes: Seleccione un entorno de trabajo y haga clic en **Iniciar supervisión**.

Ver los datos de rendimiento

Haga clic en **Supervisión** y vea los datos de rendimiento de sus volúmenes.

Suscríbase a Cloud Insights

Suscríbase antes de finalizar su prueba gratuita de 30 días para seguir viendo datos de rendimiento en Cloud Manager y Cloud Insights. "Aprenda a suscribirse".

Requisitos

Lea los siguientes requisitos para asegurarse de tener una configuración compatible.

Versiones de Cloud Manager compatibles

Necesita una nueva instalación de Cloud Manager 3.8.4 o posterior. Se necesita una nueva instalación porque se necesita una nueva infraestructura para habilitar el servicio de supervisión. Esta infraestructura está disponible a partir de nuevas instalaciones de Cloud Manager 3.8.4.

Versiones de Cloud Volumes ONTAP compatibles

Cualquier versión de Cloud Volumes ONTAP en AWS.

Requisito de Cloud Insights

Debe ser un nuevo cliente de Cloud Insights. La supervisión no se admite si ya tiene un inquilino Cloud Insights.

Dirección de correo electrónico de Cloud Central

La dirección de correo electrónico de su cuenta de usuario de Cloud Central debe ser la dirección de correo electrónico de su empresa. Los dominios de correo electrónico gratuitos como gmail y hotmail no son compatibles al crear un inquilino Cloud Insights.

Conexión de red para la unidad de adquisición

La unidad de adquisición utiliza autenticación bidireccional/mutua para conectarse al servidor Cloud Insights. El certificado de cliente debe pasarse al servidor Cloud Insights para autenticarse. Para ello, el proxy debe configurarse para reenviar la solicitud http al servidor Cloud Insights sin descifrarse los datos.

La unidad de adquisición utiliza los dos puntos finales siguientes para comunicarse con Cloud Insights. Si tiene un firewall entre el servidor de la unidad de adquisición y Cloud Insights, necesitará estos puntos finales al configurar las reglas de firewall:

```
https://aulogin.<Cloud Insights Domain>
https://<your-tenant-ID>.<Cloud Insights Domain>
```

Por ejemplo:

```
https://aulogin.c01.cloudinsights.netapp.com
https://cg0c586a-ee05-45rb-a5ac-
333b5ae7718d7.c01.cloudinsights.netapp.com
```

Póngase en contacto con nosotros a través del chat en el producto si necesita ayuda para identificar su dominio de Cloud Insights y su ID de inquilino.

Conexión en red para el conector

De forma similar a la unidad de adquisición, el conector debe tener conectividad de salida al inquilino Cloud Insights. Pero el extremo que los contactos del conector son ligeramente diferentes. Se pone en contacto con la URL del host de inquilino mediante el ID de inquilino acortado:

```
 https://<your-short-tenant-ID>.<Cloud Insights Domain>
Por ejemplo:
```

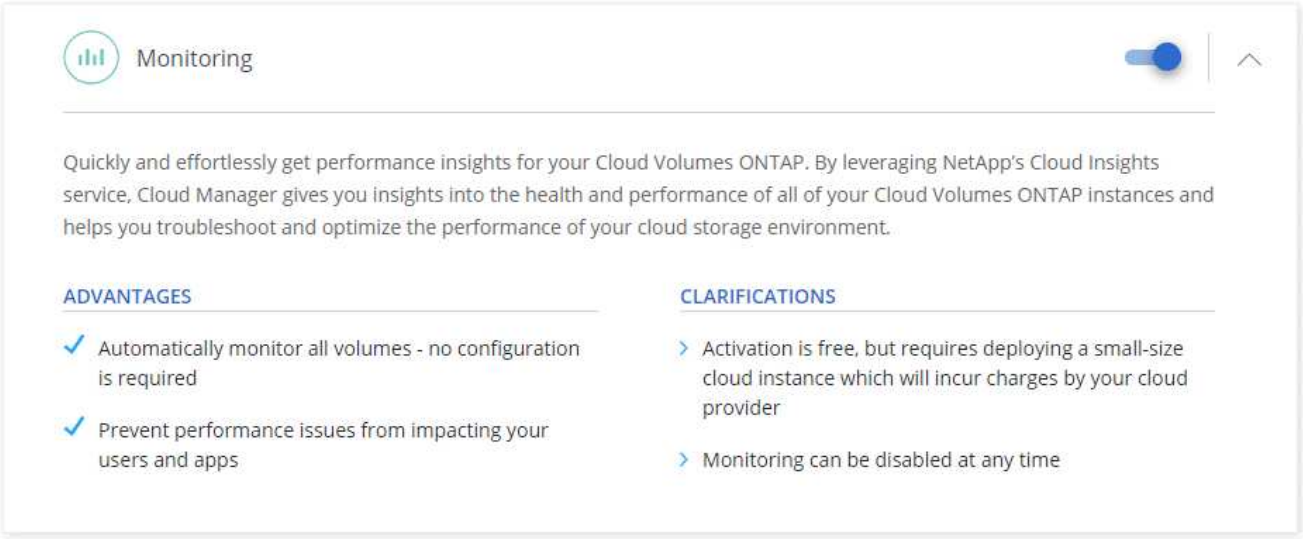
```
 https://abcd12345.c01.cloudinsights.netapp.com
De nuevo, puede ponerse en contacto con nosotros a través del chat de
producto si necesita ayuda para identificar la URL del host de
inquilinos.
```

Activación de la supervisión en un sistema nuevo

El servicio Supervisión está activado de forma predeterminada en el asistente del entorno de trabajo. Asegúrese de mantener la opción habilitada.

Pasos

1. Haga clic en **Crear Cloud Volumes ONTAP**.
2. Seleccione Amazon Web Services como proveedor de cloud y, a continuación, elija un único nodo o sistema de alta disponibilidad.
3. Rellene la página Details & Credentials.
4. En la página Servicios, deje el servicio activado y haga clic en **continuar**.

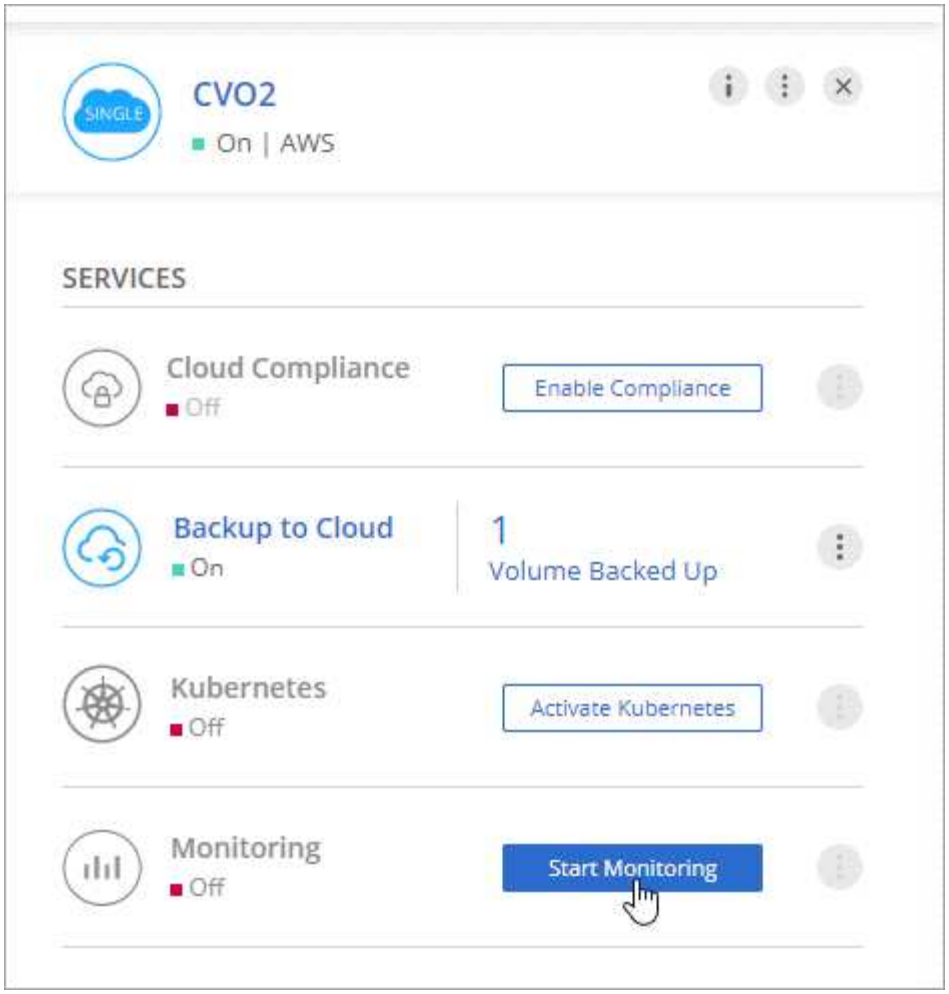


Activación de la supervisión en un sistema existente

Active la supervisión en cualquier momento desde el entorno de trabajo.

Pasos

1. En la parte superior de Cloud Manager, haga clic en **entornos de trabajo**.
2. Seleccione un entorno de trabajo.
3. En el panel de la derecha, haga clic en **Iniciar supervisión**.



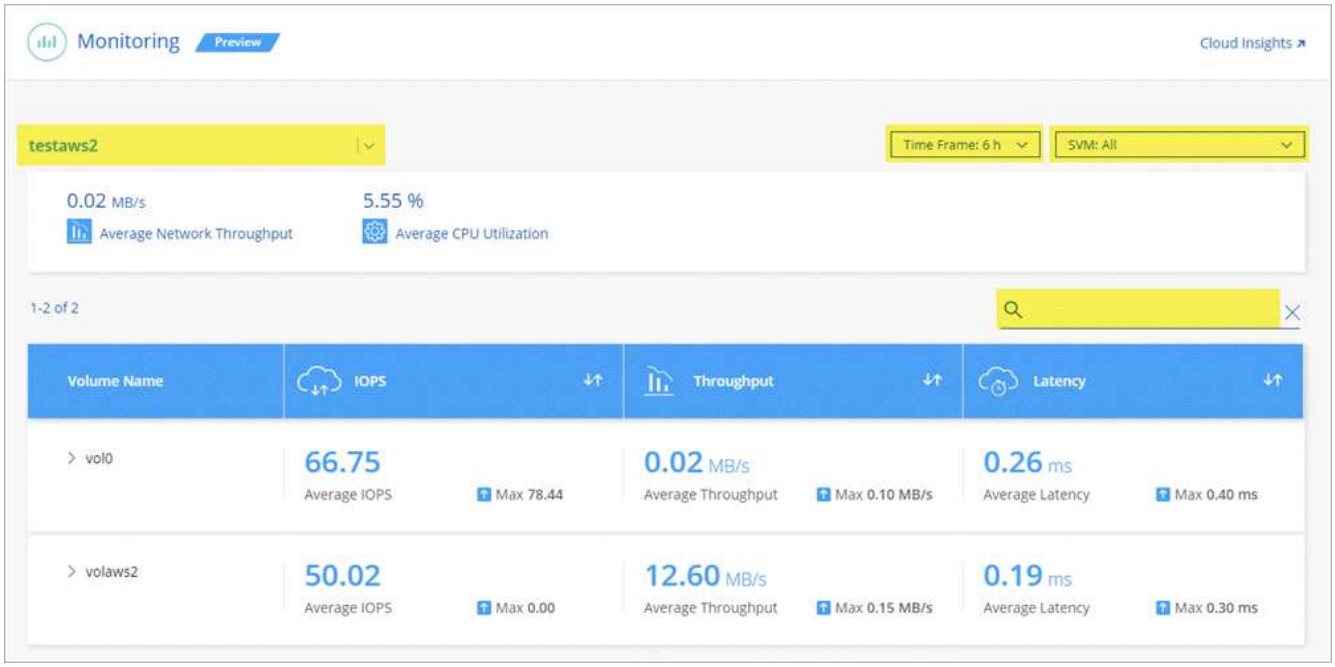
Supervisar los volúmenes

Supervise el rendimiento viendo las IOPS, el rendimiento y la latencia de cada volumen.

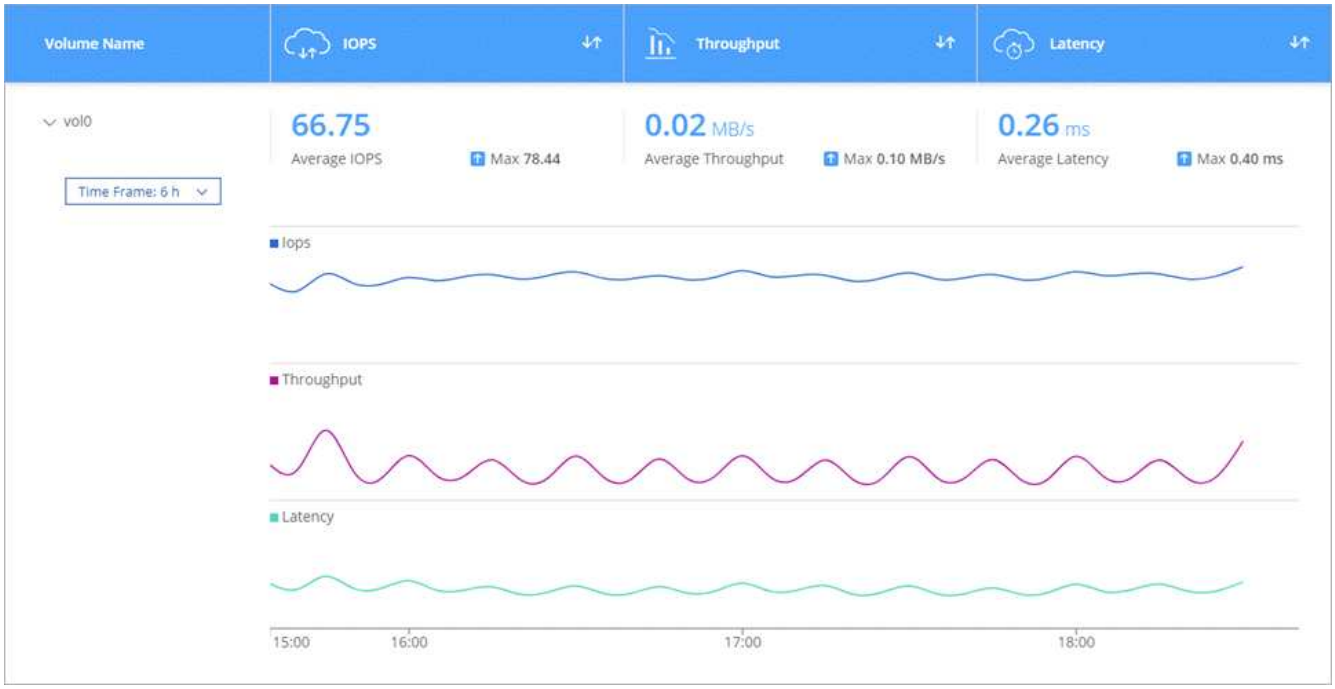
Pasos

1. En la parte superior de Cloud Manager, haga clic en **Supervisión**.
2. Filtre el contenido de la consola para obtener la información necesaria.
   - Seleccione un entorno de trabajo específico.
   - Seleccione un período de tiempo diferente.
   - Seleccione una SVM específica.
   - Busque un volumen específico.

     La siguiente imagen resalta cada una de estas opciones:



3. Haga clic en un volumen de la tabla para expandir la fila y ver una escala de tiempo para IOPS, rendimiento y latencia.



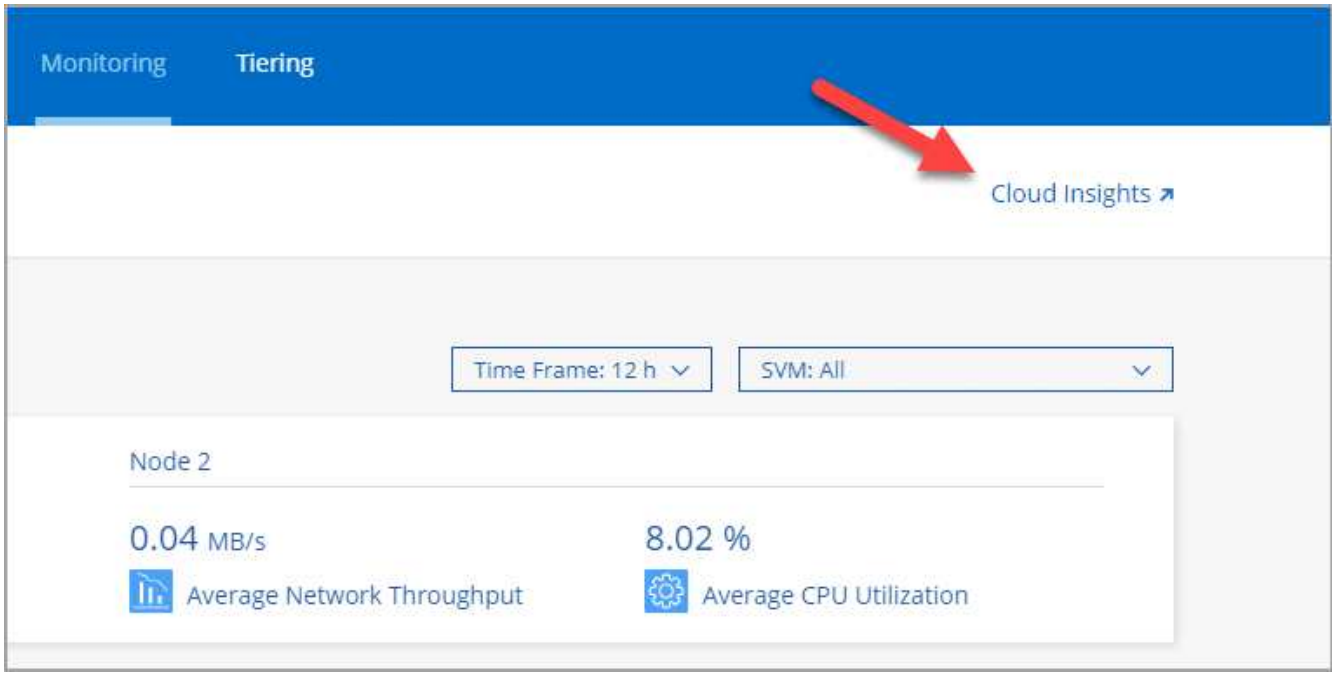
4. Utilice los datos para identificar problemas de rendimiento y minimizar el impacto en sus usuarios y aplicaciones.

Obtener más información de Cloud Insights

La pestaña Monitoring de Cloud Manager proporciona datos de rendimiento básicos para los volúmenes. Desde el explorador, puede ir a la interfaz web de Cloud Insights para realizar supervisión más profunda y configurar alertas para sus sistemas Cloud Volumes ONTAP.

Pasos

1. En la parte superior de Cloud Manager, haga clic en **Supervisión**.
2. Haga clic en el enlace **Cloud Insights**.



Resultado

Cloud Insights se abre en una nueva pestaña del navegador. Si necesita ayuda, consulte "Documentación de Cloud Insights".

Deshabilitar la supervisión

Si ya no desea supervisar Cloud Volumes ONTAP, puede deshabilitar el servicio en cualquier momento.

> Si deshabilita la supervisión desde cada uno de los entornos de trabajo, deberá eliminar la instancia de EC2 usted mismo. La instancia se denomina *AcquisitionUnit* con un hash generado (UUID) concatenado. Por ejemplo: *AcquisitionUnit-FAN7FqeH*

Pasos

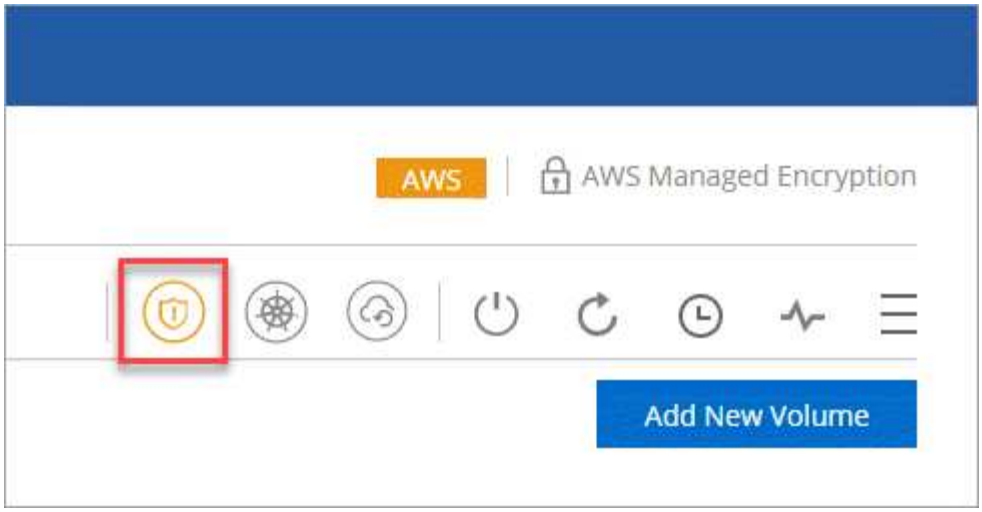
1. En la parte superior de Cloud Manager, haga clic en **entornos de trabajo**.
2. Seleccione un entorno de trabajo.
3. En el panel de la derecha, haga clic en Y seleccione **Desactivar escaneado**.

Mejorar la protección contra el ransomware

Los ataques de ransomware pueden suponer un coste comercial, recursos y reputación. Cloud Manager le ayuda a implementar la solución de NetApp para el ransomware, que proporciona herramientas eficaces para la visibilidad, la detección y la corrección.

Pasos

1. En el entorno de trabajo, haga clic en el icono **Ransomware**.

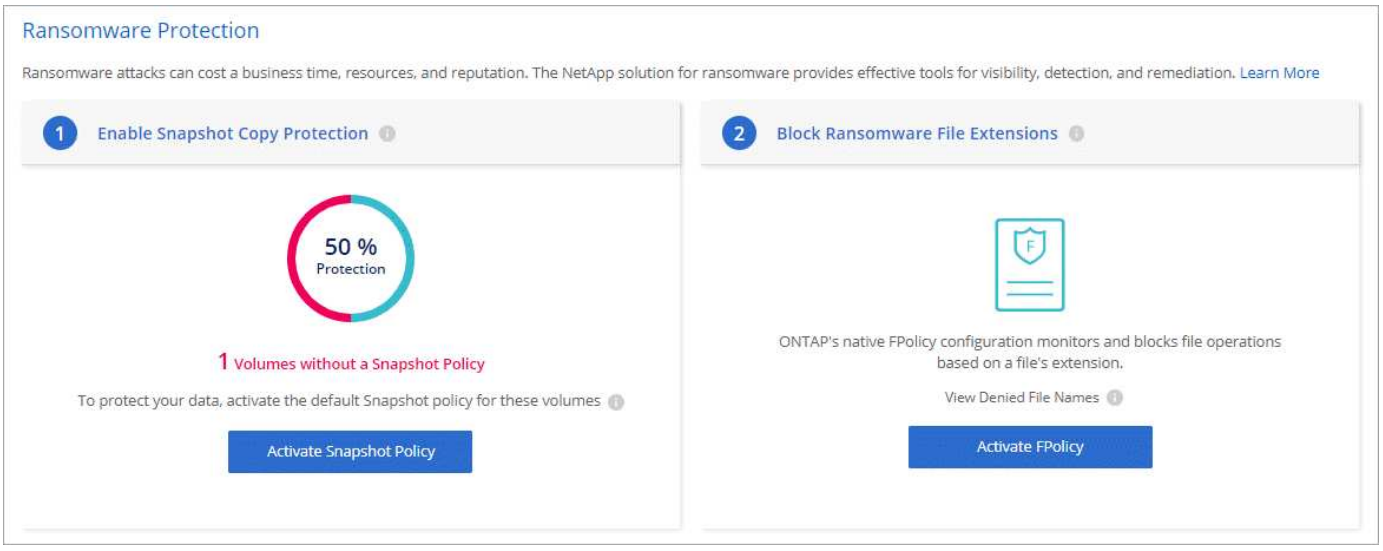


2. Implemente la solución de NetApp para ransomware:
   a. Haga clic en **Activar política de instantánea** si tiene volúmenes que no tienen activada una directiva de instantánea.

      La tecnología Snapshot de NetApp proporciona la mejor solución del sector para la reparación de ransomware. La clave para una recuperación correcta es restaurar a partir de backups no infectados. Las copias Snapshot son de solo lectura, lo que evita que se dañen el ransomware. También pueden proporcionar granularidad para crear imágenes de una sola copia de archivos o una solución completa de recuperación tras desastres.

   b. Haga clic en **Activar FPolicy** para habilitar la solución FPolicy de ONTAP, que puede bloquear las operaciones de archivos según la extensión de un archivo.

      Esta solución preventiva mejora la protección contra ataques de ransomware bloqueando tipos de archivos comunes de ransomware.



Administración

Registro de sistemas de pago por uso

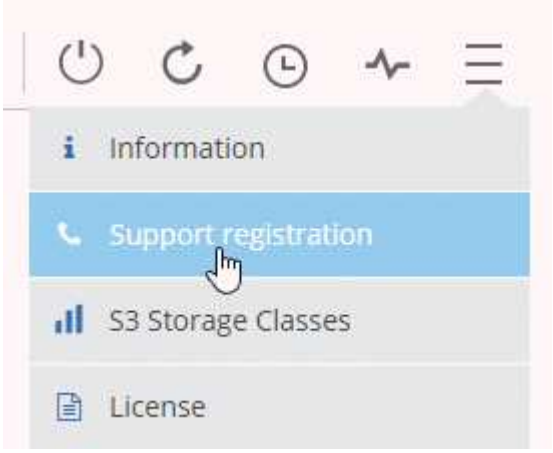
El soporte de NetApp se incluye en los sistemas Explore, estándar y Premium de Cloud Volumes ONTAP, pero primero debe activar el soporte registrando los sistemas en NetApp.

Pasos

1. Si todavía no ha añadido su cuenta del sitio de soporte de NetApp a Cloud Manager, vaya a **Configuración de cuenta** y añádalo ahora.

   "Aprenda a añadir cuentas del sitio de soporte de NetApp".

2. En la página entornos de trabajo, haga doble clic en el nombre del sistema que desea registrar.
3. Haga clic en el icono de menú y, a continuación, haga clic en **Registro de soporte**:



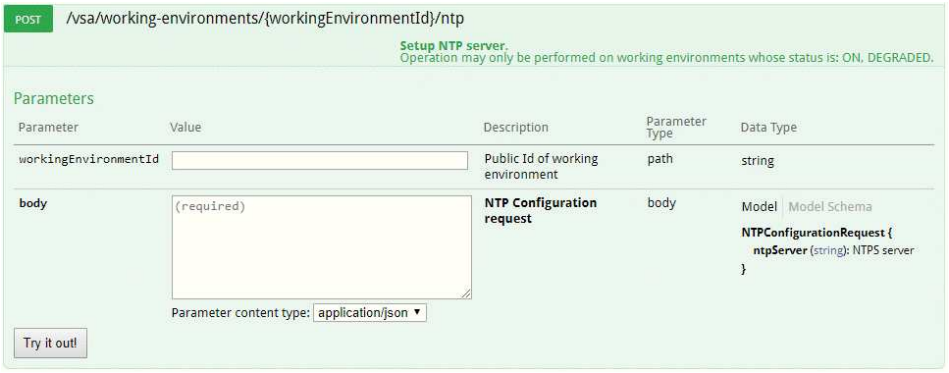
4. Seleccione una cuenta en la página de soporte de NetApp y haga clic en **Register**.

Resultado

Cloud Manager registra el sistema con NetApp.

Configurar Cloud Volumes ONTAP

Después de implementar Cloud Volumes ONTAP, puede configurarlo mediante la sincronización de la hora del sistema con NTP y ejecutando algunas tareas opcionales desde System Manager o desde la CLI.

Tarea	Descripción
Sincronice la hora del sistema con NTP	Al especificar un servidor NTP se sincroniza el tiempo entre los sistemas de la red, lo que puede ayudar a prevenir problemas debido a las diferencias de tiempo. Especifique un servidor NTP con la API de Cloud Manager o desde la interfaz de usuario al configurar un servidor CIFS. • "Modificación del servidor CIFS" • "Guía para desarrolladores de API de Cloud Manager" Por ejemplo, aquí tiene la API para un sistema de un solo nodo en AWS: 
Opcional: Configure AutoSupport	AutoSupport supervisa de manera proactiva el estado del sistema y envía automáticamente mensajes al soporte técnico de NetApp de forma predeterminada. Si el administrador de cuentas agregó un servidor proxy a Cloud Manager antes de iniciar la instancia, Cloud Volumes ONTAP está configurado para utilizar ese servidor proxy para mensajes de AutoSupport. Debe probar AutoSupport para asegurarse de que puede enviar mensajes. Para obtener instrucciones, consulte la ayuda de System Manager o la "Referencia de administración del sistema de ONTAP 9".
Opcional: Configure Cloud Manager como proxy AutoSupport	Si su entorno requiere que un servidor proxy envíe mensajes de AutoSupport, puede configurar Cloud Manager para que actúe como proxy. No es necesario configurar Cloud Manager aparte del acceso a Internet. Simplemente tiene que ir a la CLI para Cloud Volumes ONTAP y ejecutar el siguiente comando: `system node autosupport modify -proxy-url <cloud-manager-ip-address>`
Opcional: Configure EMS	El sistema de gestión de eventos (EMS) recopila y muestra información sobre los eventos que se producen en los sistemas Cloud Volumes ONTAP. Para recibir notificaciones de eventos, es posible establecer destinos de eventos (direcciones de correo electrónico, hosts de captura SNMP o servidores de syslog) y rutas de eventos para una gravedad de eventos en particular. Puede configurar EMS con la CLI. Para ver instrucciones, consulte "Guía exprés de configuración de EMS de ONTAP 9".

Tarea	Descripción
Opcional: Cree una interfaz de red de gestión (LIF) SVM para sistemas de alta disponibilidad en varias zonas de disponibilidad de AWS	Se requiere una interfaz de red (LIF) de gestión de máquinas virtuales de almacenamiento si desea usar SnapCenter o SnapDrive para Windows con una pareja de alta disponibilidad. La LIF de gestión de SVM debe utilizar una dirección IP *flotante* cuando se utiliza un par de alta disponibilidad en varias zonas de disponibilidad de AWS. Cloud Manager le solicita que especifique la dirección IP flotante al iniciar el par de alta disponibilidad. Si no especificó la dirección IP, puede crear usted mismo la LIF de gestión de SVM desde System Manager o la CLI. El ejemplo siguiente muestra cómo crear la LIF a partir de la CLI: `network interface create -vserver svm_cloud -lif svm_mgmt -role data -data-protocol none -home-node cloud-01 -home-port e0a -address 10.0.2.126 -netmask 255.255.255.0 -status-admin up -firewall -policy mgmt`
Opcional: Cambie la ubicación de la copia de seguridad de los archivos de configuración	Cloud Volumes ONTAP crea automáticamente archivos de copia de seguridad de configuración que contienen información acerca de las opciones configurables que necesita para funcionar correctamente. De forma predeterminada, Cloud Volumes ONTAP realiza copias de seguridad de los archivos en el host del conector cada ocho horas. Si desea enviar las copias de seguridad a una ubicación alternativa, puede cambiar la ubicación a un servidor FTP o HTTP en el centro de datos o en AWS. Por ejemplo, es posible que ya tenga una ubicación de backup para los sistemas de almacenamiento de FAS. Es posible cambiar la ubicación del backup con la CLI. Consulte "Referencia de administración del sistema de ONTAP 9".

Gestión de licencias BYOL para Cloud Volumes ONTAP

Añada una licencia del sistema BYOL de Cloud Volumes ONTAP para añadir capacidad adicional, actualizar una licencia del sistema existente y gestionar las licencias BYOL para backup en el cloud.

Administrar las licencias del sistema

Puede comprar varias licencias para un sistema BYOL de Cloud Volumes ONTAP con el fin de asignar más de 368 TB de capacidad. Por ejemplo, puede adquirir dos licencias para asignar hasta 736 TB de capacidad a Cloud Volumes ONTAP. O bien podría comprar cuatro licencias para obtener hasta 1.4 PB.

El número de licencias que se pueden comprar para un único sistema de nodo o par de alta disponibilidad es ilimitado.

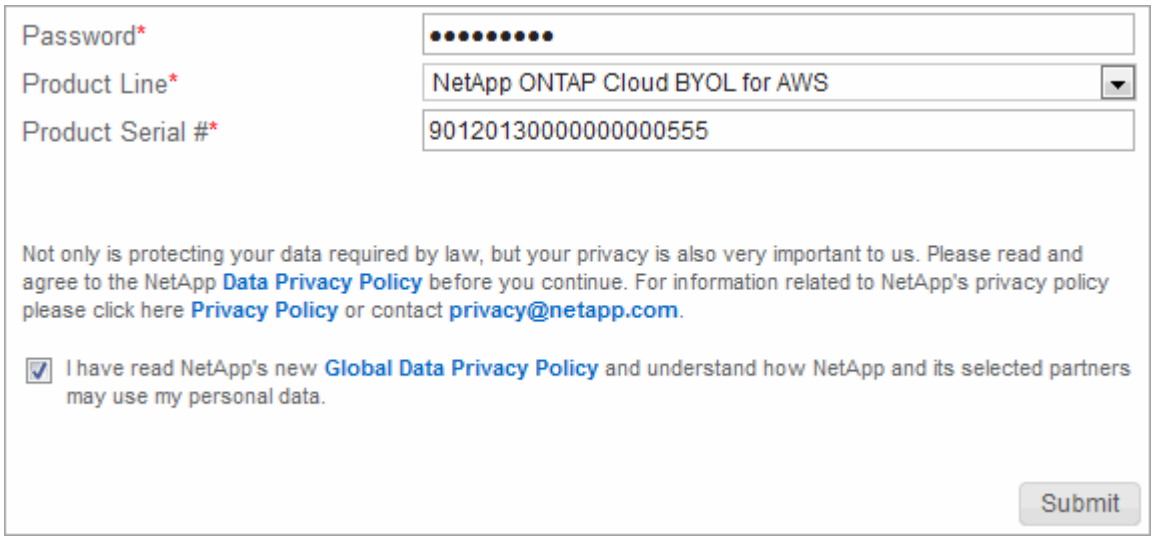
Obtención de un archivo de licencia del sistema

En la mayoría de los casos, Cloud Manager puede obtener automáticamente su archivo de licencia con su cuenta del sitio de soporte de NetApp. Pero si no puede, deberá cargar manualmente el archivo de licencia. Si no tiene el archivo de licencia, puede obtenerlo en netapp.com.

Pasos

1. Vaya a la "Generador de archivos de licencia de NetApp" E inicie sesión con sus credenciales del sitio de soporte de NetApp.
2. Introduzca su contraseña, elija su producto, introduzca el número de serie, confirme que ha leído y aceptado la política de privacidad y, a continuación, haga clic en **Enviar**.

   ejemplo



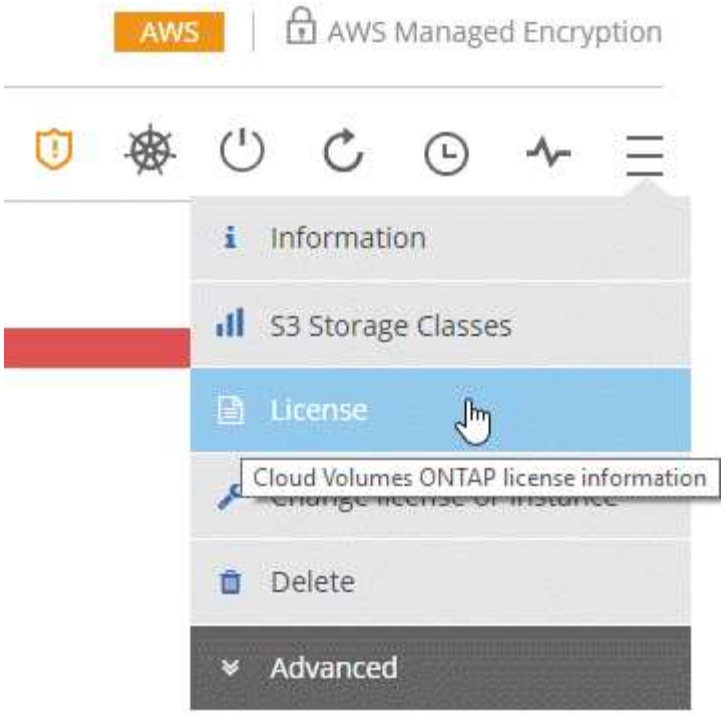
3. Elija si desea recibir el archivo serialnumber.NLF JSON a través del correo electrónico o la descarga directa.

Adición de una nueva licencia del sistema

Añada una nueva licencia de sistema BYOL en cualquier momento para asignar 368 TB adicionales de capacidad a su sistema BYOL de Cloud Volumes ONTAP.

Pasos

1. En Cloud Manager, abra el entorno de trabajo BYOL de Cloud Volumes ONTAP.
2. Haga clic en el icono de menú y, a continuación, haga clic en **Licencia**.



3. Haga clic en **Agregar licencia de sistema CVO**.

4. Elija introducir el número de serie o cargar el archivo de licencia.
5. Haga clic en **Agregar licencia**.

Resultado

Cloud Manager instala el nuevo archivo de licencia en el sistema Cloud Volumes ONTAP.

Actualizar una licencia del sistema

Cuando renueve una suscripción de BYOL con un representante de NetApp, Cloud Manager obtiene automáticamente la nueva licencia de NetApp y la instala en el sistema Cloud Volumes ONTAP.

Si Cloud Manager no puede acceder al archivo de licencia a través de la conexión segura a Internet, puede obtener el archivo usted mismo y, a continuación, cargarlo manualmente en Cloud Manager.

Pasos

1. En Cloud Manager, abra el entorno de trabajo BYOL de Cloud Volumes ONTAP.
2. Haga clic en el icono de menú y, a continuación, haga clic en **Licencia**.
3. Haga clic en **Actualizar licencia del sistema CVO**.

4. Haga clic en **cargar archivo** y seleccione el archivo de licencia.
5. Haga clic en **Actualizar licencia**.

Resultado

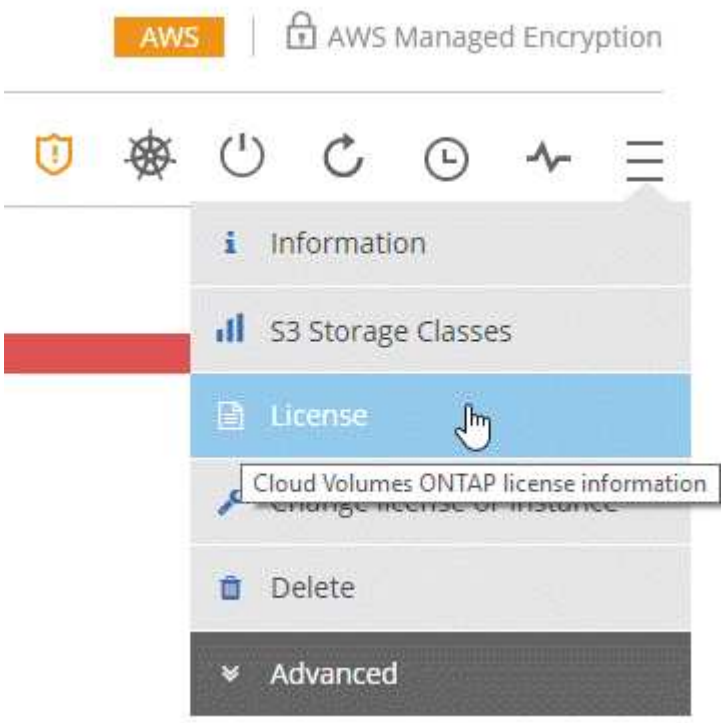
Cloud Manager actualiza la licencia del sistema Cloud Volumes ONTAP.

Adición y actualización de su licencia BYOL de copia de seguridad

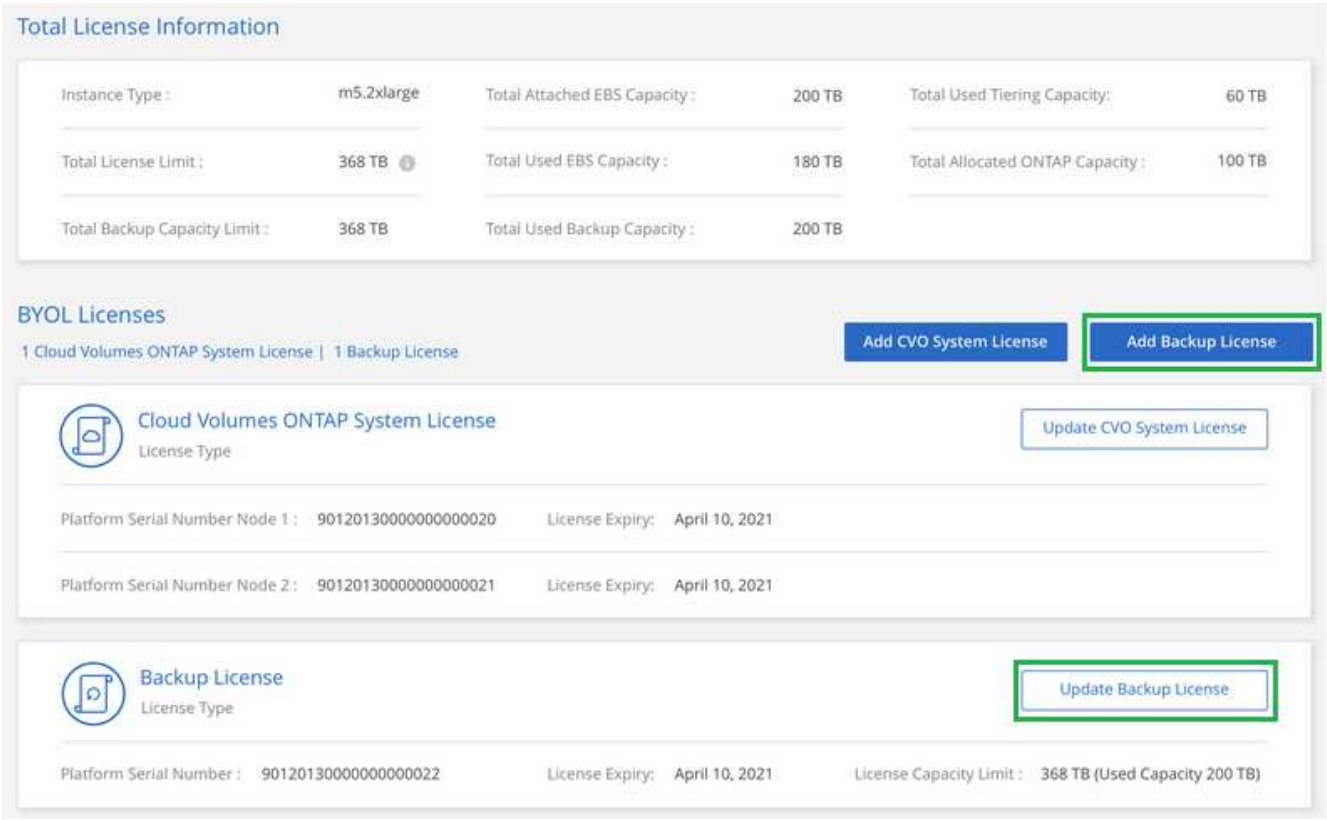
La página licencias BYOL se utiliza para añadir o actualizar la licencia BYOL de backup.

Pasos

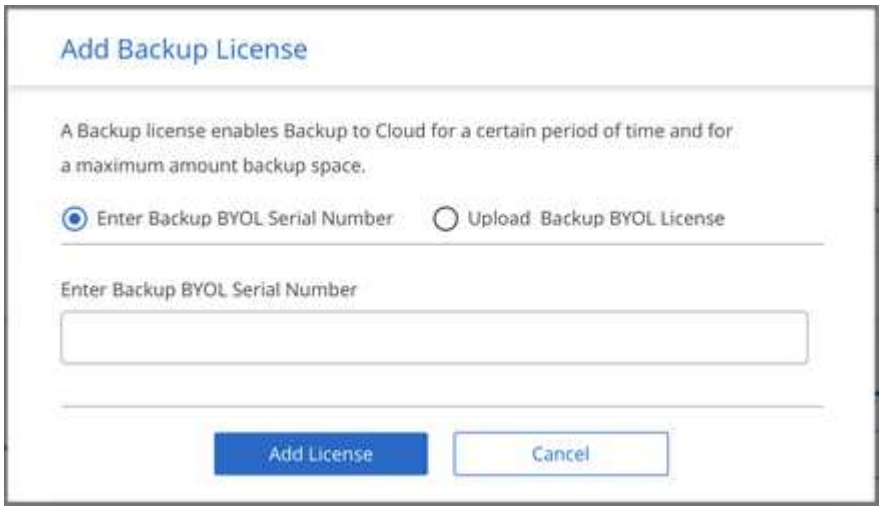
1. En Cloud Manager, abra el entorno de trabajo BYOL de Cloud Volumes ONTAP.
2. Haga clic en el icono de menú y, a continuación, haga clic en **Licencia**.



3. Haga clic en **Agregar licencia de copia de seguridad** o **Actualizar licencia de copia de seguridad** dependiendo de si va a añadir una licencia nueva o actualizar una licencia existente.



4. Introduzca la información de la licencia y haga clic en **Agregar licencia**:
   - Si tiene el número de serie, seleccione la opción **introducir número de serie BYOL** de copia de seguridad e introduzca el número de serie.
   - Si tiene el archivo de licencia de copia de seguridad, seleccione la opción **cargar licencia BYOL de copia de seguridad** y siga las indicaciones para adjuntar el archivo.



Resultado

Cloud Manager agrega o actualiza la licencia para que el servicio Backup to Cloud esté activo.

Actualización del software Cloud Volumes ONTAP

Cloud Manager incluye varias opciones que se pueden utilizar para actualizar a la

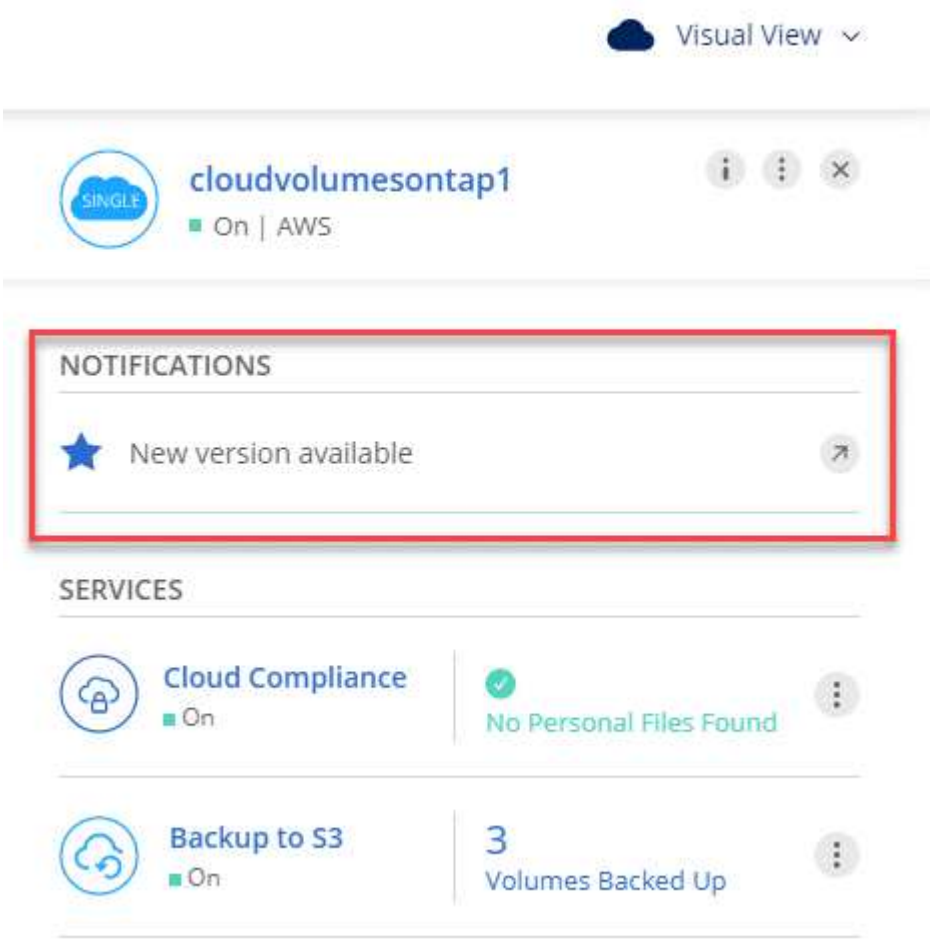
versión actual de Cloud Volumes ONTAP o degradar Cloud Volumes ONTAP a una versión anterior. Debe preparar los sistemas de Cloud Volumes ONTAP antes de actualizar o degradar el software.

Cloud Manager debe completar las actualizaciones de software

Las actualizaciones de Cloud Volumes ONTAP se deben completar desde Cloud Manager. No debe actualizar Cloud Volumes ONTAP con System Manager o CLI. Hacerlo puede afectar a la estabilidad del sistema.

Formas de actualizar Cloud Volumes ONTAP

Cloud Manager muestra una notificación en entornos de trabajo de Cloud Volumes ONTAP cuando hay disponible una nueva versión de Cloud Volumes ONTAP:



Puede iniciar el proceso de actualización a partir de esta notificación, que automatiza el proceso. Para ello, obtenga la imagen de software de un bloque de S3, instale la imagen y, a continuación, reinicie el sistema. Para obtener más información, consulte Actualizar Cloud Volumes ONTAP a partir de notificaciones de Cloud Manager.

Para los sistemas de alta disponibilidad de AWS, Cloud Manager puede actualizar al mediador de alta disponibilidad como parte del proceso de actualización.

Opciones avanzadas para actualizaciones de software

Cloud Manager también ofrece las siguientes opciones avanzadas para actualizar el software Cloud Volumes ONTAP:

- Actualizaciones de software mediante una imagen en una URL externa

  Esta opción resulta útil si Cloud Manager no puede acceder al bloque de S3 para actualizar el software, si se le proporcionó un parche o si desea degradar el software a una versión concreta.

  Para obtener más información, consulte Actualización o degradación de Cloud Volumes ONTAP mediante un servidor HTTP o FTP.

- Actualizaciones de software usando la imagen alternativa del sistema

  Puede utilizar esta opción para cambiar a la versión anterior haciendo que la imagen de software alternativa sea la predeterminada. Esta opción no está disponible para pares de alta disponibilidad.

  Para obtener más información, consulte Degradación de Cloud Volumes ONTAP mediante una imagen local.

Preparando la actualización del software Cloud Volumes ONTAP

Antes de realizar una actualización o una degradación, debe verificar que los sistemas estén preparados y realizar los cambios de configuración necesarios.

- Planificación de los tiempos de inactividad
- Revisión de los requisitos de versión
- Verificación de que la devolución automática sigue activada
- Suspensión de las transferencias de SnapMirror
- Verificación de que los agregados están en línea

Planificación de los tiempos de inactividad

Al actualizar un sistema de un solo nodo, el proceso de actualización desconecta el sistema durante un máximo de 25 minutos, durante el cual se interrumpen las operaciones de I/O.

Actualizar un par de alta disponibilidad no provoca interrupciones y la I/o se realiza de forma ininterrumpida. Durante este proceso de actualización no disruptiva, cada nodo se actualiza conjuntamente para seguir proporcionando I/o a los clientes.

Revisión de los requisitos de versión

La versión de ONTAP a la que se puede actualizar o degradar varía en función de la versión de ONTAP que esté ejecutándose actualmente en el sistema.

Para conocer los requisitos de la versión, consulte "Documentación de ONTAP 9: Requisitos de actualización del clúster".

Verificación de que la devolución automática sigue activada

La devolución automática debe estar habilitada en una pareja de ha de Cloud Volumes ONTAP (esta es la configuración predeterminada). Si no lo es, la operación fallará.

"Documentación de ONTAP 9: Comandos para configurar el retorno automático"

Suspensión de las transferencias de SnapMirror

Si un sistema Cloud Volumes ONTAP tiene relaciones SnapMirror activas, se recomienda suspender las transferencias antes de actualizar el software Cloud Volumes ONTAP. La suspensión de las transferencias evita que se produzcan fallos de SnapMirror. Debe suspender las transferencias del sistema de destino.

Acerca de esta tarea

Estos pasos describen cómo utilizar System Manager para la versión 9.3 y posteriores.

Pasos

1. "Inicie sesión en System Manager" desde el sistema de destino.
2. Haga clic en **Protección > Relaciones**.
3. Seleccione la relación y haga clic en **Operaciones > Quiesce**.

Verificación de que los agregados están en línea

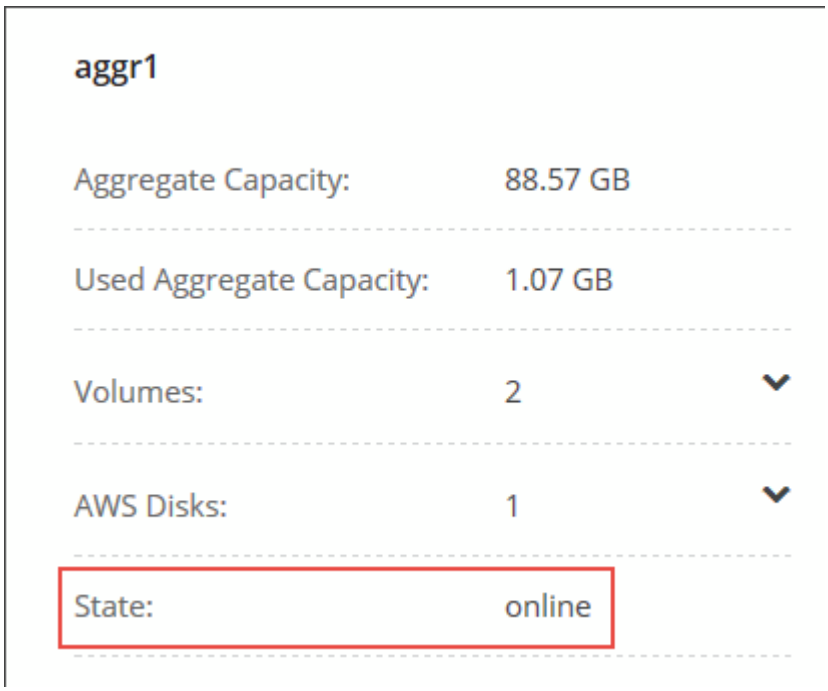
Los agregados para Cloud Volumes ONTAP deben estar en línea antes de actualizar el software. Los agregados deben estar en línea en la mayoría de las configuraciones, pero si no lo están, debe conectarlos conectados.

Acerca de esta tarea

Estos pasos describen cómo utilizar System Manager para la versión 9.3 y posteriores.

Pasos

1. En el entorno de trabajo, haga clic en el icono de menú y, a continuación, haga clic en **Avanzado > asignación avanzada**.
2. Seleccione un agregado, haga clic en **Info** y, a continuación, compruebe que el estado está en línea.



3. Si el agregado está sin conexión, use System Manager para conectar el agregado:

a. "Inicie sesión en System Manager".

b. Haga clic en **almacenamiento > agregados y discos > agregados**.

c. Seleccione el agregado y, a continuación, haga clic en **más acciones > Estado > en línea**.

Actualizar Cloud Volumes ONTAP a partir de notificaciones de Cloud Manager

Cloud Manager notifica el momento en que una nueva versión de Cloud Volumes ONTAP está disponible. Haga clic en la notificación para iniciar el proceso de actualización.

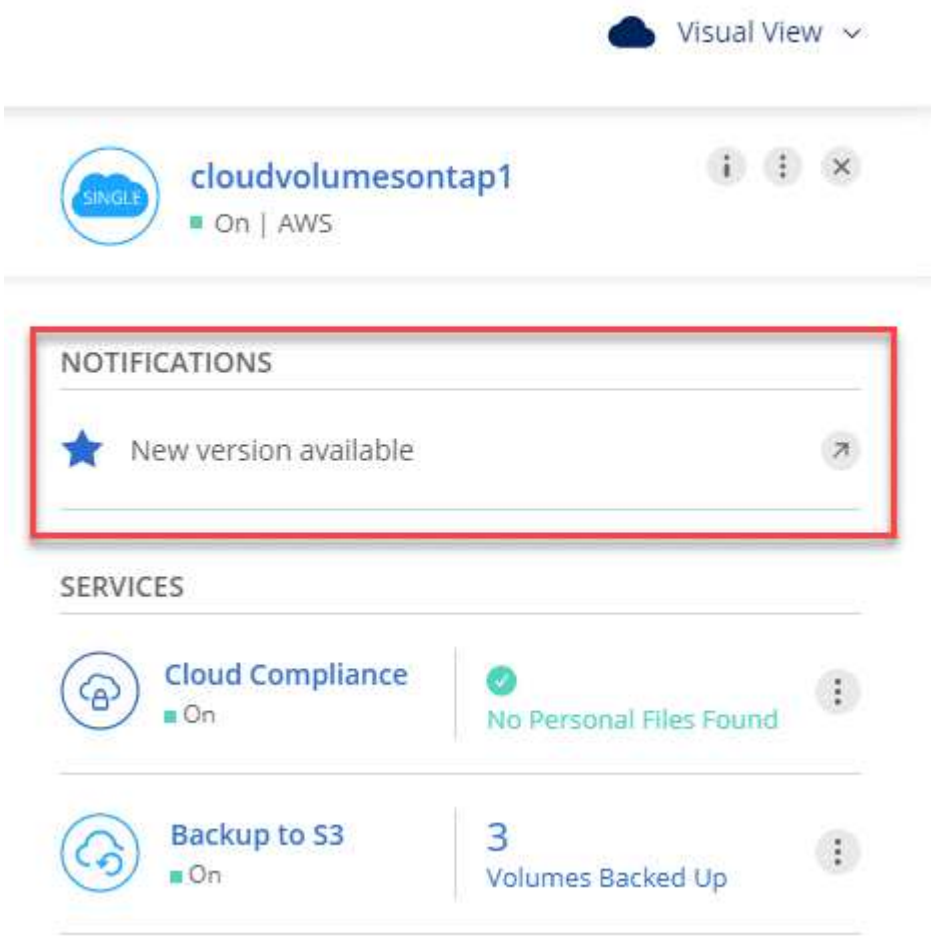
Antes de empezar

No deben estar en curso en el sistema de Cloud Volumes ONTAP operaciones de Cloud Manager, como la creación de volúmenes o agregados.

Pasos

1. Haga clic en **entornos de trabajo**.
2. Seleccione un entorno de trabajo.

   Aparece una notificación en el panel derecho si hay una nueva versión disponible:



3. Si hay una nueva versión disponible, haga clic en **Actualizar**.
4. En la página Información de versión, haga clic en el vínculo para leer las Notas de versión de la versión especificada y, a continuación, active la casilla de verificación **he leído…** .

5. En la página Contrato de licencia para el usuario final (EULA), lea el EULA y, a continuación, seleccione **he leído y aprobado el EULA**.
6. En la página revisar y aprobar, lea las notas importantes, seleccione **comprendo…** y, a continuación, haga clic en **Ir**.

Resultado

Cloud Manager inicia la actualización del software. Puede realizar acciones en el entorno de trabajo una vez completada la actualización de software.

Después de terminar

Si ha suspendido las transferencias de SnapMirror, use System Manager para reanudar las transferencias.

Actualización o degradación de Cloud Volumes ONTAP mediante un servidor HTTP o FTP

Puede colocar la imagen del software Cloud Volumes ONTAP en un servidor HTTP o FTP e iniciar la actualización del software desde Cloud Manager. Se puede usar esta opción si Cloud Manager no puede acceder al bloque de S3 para actualizar el software o si desea degradar el software.

Pasos

1. Configure un servidor HTTP o FTP que pueda alojar la imagen del software Cloud Volumes ONTAP.
2. Si tiene una conexión VPN a la red virtual, puede colocar la imagen del software Cloud Volumes ONTAP en un servidor HTTP o FTP en su propia red. De lo contrario, debe colocar el archivo en un servidor HTTP o FTP en la nube.
3. Si utiliza su propio grupo de seguridad para Cloud Volumes ONTAP, asegúrese de que las reglas salientes permiten conexiones HTTP o FTP para que Cloud Volumes ONTAP pueda acceder a la imagen del software.

   El grupo de seguridad Cloud Volumes ONTAP predefinido permite conexiones HTTP y FTP salientes de forma predeterminada.

4. Obtenga la imagen del software de "El sitio de soporte de NetApp".
5. Copie la imagen de software en el directorio del servidor HTTP o FTP a partir del que se servirá el archivo.
6. En el entorno de trabajo de Cloud Manager, haga clic en el icono de menú y, a continuación, haga clic en **Avanzado > Actualizar Cloud Volumes ONTAP**.
7. En la página de actualización del software, elija **Seleccione una imagen disponible en una dirección URL**, introduzca la dirección URL y, a continuación, haga clic en **Cambiar imagen**.
8. Haga clic en **continuar** para confirmar.

Resultado

Cloud Manager inicia la actualización de software. Puede realizar acciones en el entorno de trabajo una vez completada la actualización de software.

Después de terminar

Si ha suspendido las transferencias de SnapMirror, use System Manager para reanudar las transferencias.

Degradación de Cloud Volumes ONTAP mediante una imagen local

La transición de Cloud Volumes ONTAP a una versión anterior de la misma familia de versiones (por ejemplo, 9.5 a 9.4) se conoce como una degradación. Es posible degradar sin ayuda cuando se degrade un clúster nuevo o de prueba, pero debe ponerse en contacto con el soporte técnico si desea degradar un clúster de

producción.

Cada sistema Cloud Volumes ONTAP puede contener dos imágenes de software: La imagen actual en ejecución y una imagen alternativa que puede arrancar. Cloud Manager puede cambiar la imagen alternativa para que sea la imagen predeterminada. Puede utilizar esta opción para cambiar a la versión anterior de Cloud Volumes ONTAP si tiene problemas con la imagen actual.

Acerca de esta tarea

Este proceso de degradación solo está disponible para sistemas Cloud Volumes ONTAP individuales. No está disponible para pares de alta disponibilidad.

Pasos

1. En el entorno de trabajo, haga clic en el icono de menú y, a continuación, haga clic en **Avanzado > Actualizar Cloud Volumes ONTAP**.
2. En la página Actualizar software, seleccione la imagen alternativa y, a continuación, haga clic en **Cambiar imagen**.
3. Haga clic en **continuar** para confirmar.

Resultado

Cloud Manager inicia la actualización de software. Puede realizar acciones en el entorno de trabajo una vez completada la actualización de software.

Después de terminar

Si ha suspendido las transferencias de SnapMirror, use System Manager para reanudar las transferencias.

Modificación de sistemas Cloud Volumes ONTAP

Es posible que necesite cambiar la configuración de los sistemas Cloud Volumes ONTAP a medida que cambien sus necesidades de almacenamiento. Por ejemplo, es posible cambiar entre configuraciones de pago por uso, cambiar la instancia o el tipo de equipo virtual, etc.

Cambiar la instancia o el tipo de máquina de Cloud Volumes ONTAP

Puede elegir entre varios tipos de máquina o instancia al ejecutar Cloud Volumes ONTAP en AWS, Azure o GCP. Puede cambiar la instancia o el tipo de máquina en cualquier momento si determina que tiene un tamaño insuficiente o demasiado grande para sus necesidades.

Acerca de esta tarea

- La devolución automática debe estar habilitada en una pareja de ha de Cloud Volumes ONTAP (esta es la configuración predeterminada). Si no lo es, la operación fallará.

  "Documentación de ONTAP 9: Comandos para configurar el retorno automático"

- Al cambiar el tipo de instancia o máquina, se ven afectados los cargos por servicios del proveedor de cloud.
- La operación reinicia Cloud Volumes ONTAP.

  Para los sistemas de un solo nodo, la I/o se interrumpe.

  En el caso de los pares de alta disponibilidad, el cambio no es disruptivo. Los pares de ALTA

DISPONIBILIDAD siguen sirviendo datos.

> Cloud Manager cambia con dignidad un nodo a uno iniciando la toma de control y esperando que se produzca el fallo. El equipo de control de calidad de NetApp ha probado la escritura y lectura de ficheros durante este proceso y no ha visto ningún problema por parte del cliente. A medida que cambiaron las conexiones, observamos el número de reintentos en el nivel de I/o, pero la capa de aplicación superó esta corta "repetición de la conexión" de conexiones NFS/CIFS.

Pasos

1. En el entorno de trabajo, haga clic en el icono de menú y, a continuación, haga clic en **Cambiar licencia o instancia** para AWS, **Cambiar licencia o VM** para Azure, o **Cambiar licencia o máquina** para GCP.
2. Si utiliza una configuración de pago por uso, puede elegir una licencia diferente.
3. Seleccione una instancia o un tipo de máquina, active la casilla de verificación para confirmar que comprende las implicaciones del cambio y, a continuación, haga clic en **Aceptar**.

Resultado

Cloud Volumes ONTAP se reinicia con la nueva configuración.

Cambio entre configuraciones de pago por uso

Después de lanzar sistemas Cloud Volumes ONTAP de pago por uso, puede cambiar entre las configuraciones Explore, Estándar y Premium en cualquier momento modificando la licencia. Al cambiar la licencia, aumenta o disminuye el límite de capacidad bruta y le permite elegir entre diferentes tipos de instancia de AWS o tipos de máquina virtual de Azure.

> En GCP, hay un solo tipo de máquina disponible para cada configuración de pago por uso. No se puede elegir entre distintos tipos de máquinas.

Acerca de esta tarea

Tenga en cuenta lo siguiente sobre el cambio entre las licencias de pago por uso:

- La operación reinicia Cloud Volumes ONTAP.

  Para los sistemas de un solo nodo, la I/o se interrumpe.

  En el caso de los pares de alta disponibilidad, el cambio no es disruptivo. Los pares de ALTA DISPONIBILIDAD siguen sirviendo datos.

- Al cambiar el tipo de instancia o máquina, se ven afectados los cargos por servicios del proveedor de cloud.

Pasos

1. En el entorno de trabajo, haga clic en el icono de menú y, a continuación, haga clic en **Cambiar licencia o instancia** para AWS, **Cambiar licencia o VM** para Azure, o **Cambiar licencia o máquina** para GCP.
2. Seleccione un tipo de licencia y un tipo de instancia o de máquina, active la casilla de verificación para confirmar que comprende las implicaciones del cambio y, a continuación, haga clic en **Aceptar**.

Resultado

Cloud Volumes ONTAP se reinicia con la nueva licencia, el tipo de instancia o el tipo de máquina, o ambos.

Mover a una configuración de Cloud Volumes ONTAP alternativa

Si desea cambiar entre una suscripción de pago por uso y una suscripción BYOL o entre un único sistema Cloud Volumes ONTAP y un par de alta disponibilidad, tendrá que poner en marcha un nuevo sistema y replicar los datos del sistema existente al nuevo sistema.

Pasos

1. Crear un nuevo entorno de trabajo de Cloud Volumes ONTAP.

   "Inicio de Cloud Volumes ONTAP en AWS"
   "Inicio de Cloud Volumes ONTAP en Azure"
   "Lanzamiento de Cloud Volumes ONTAP en GCP"

2. "Configure la replicación de datos única" entre los sistemas para cada volumen que se debe replicar.
3. Finalice el sistema Cloud Volumes ONTAP que ya no utiliza ¿necesita "eliminación del entorno de trabajo original".

Cambio de la velocidad de escritura a normal o alta

Cloud Manager le permite elegir una configuración de velocidad de escritura para sistemas Cloud Volumes ONTAP de un solo nodo. La velocidad de escritura predeterminada es normal. Puede cambiar a una alta velocidad de escritura si es necesario un rendimiento de escritura rápido para su carga de trabajo. Antes de cambiar la velocidad de escritura, debe hacerlo "entender las diferencias entre los ajustes normal y alto".

Acerca de esta tarea

- Asegúrese de que no haya operaciones en curso como la creación de volúmenes o agregados.
- Tenga en cuenta que este cambio reinicia Cloud Volumes ONTAP, lo que significa que se interrumpe la I/O.

Pasos

1. En el entorno de trabajo, haga clic en el icono de menú y, a continuación, haga clic en **Avanzado > velocidad de escritura**.
2. Seleccione **normal** o **Alta**.

   Si elige Alto, tendrá que leer la sentencia "entiendo…" y confirmar marcando la casilla.

3. Haga clic en **Guardar**, revise el mensaje de confirmación y, a continuación, haga clic en **proseguir**.

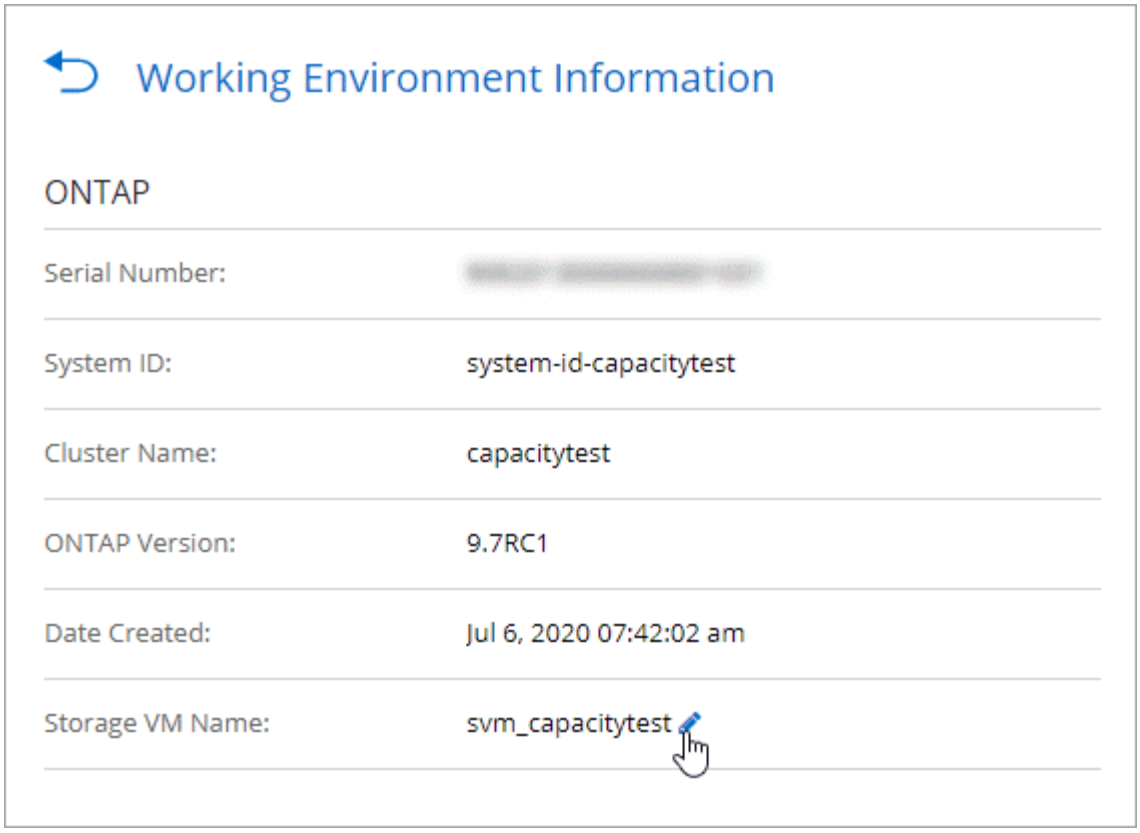
Modificación del nombre de la máquina virtual de almacenamiento

Cloud Manager nombra automáticamente a la máquina virtual de almacenamiento única (SVM) que crea para Cloud Volumes ONTAP. Puede modificar el nombre de la SVM si tiene estándares de nomenclatura estrictos. Por ejemplo, puede que el nombre coincida con el nombre que le da a las SVM de los clústeres de ONTAP.

Pero si ha creado cualquier SVM adicional para Cloud Volumes ONTAP, no puede cambiar el nombre de las SVM desde Cloud Manager. Tendrá que hacerlo directamente desde Cloud Volumes ONTAP mediante System Manager o la CLI.

Pasos

1. En el entorno de trabajo, haga clic en el icono de menú y, a continuación, haga clic en **Información**.
2. Haga clic en el icono de edición a la derecha del nombre de la máquina virtual de almacenamiento.



3. En el cuadro de diálogo Modificar nombre de SVM, cambie el nombre y, a continuación, haga clic en **Guardar**.

Cambiando la contraseña de Cloud Volumes ONTAP

Cloud Volumes ONTAP incluye una cuenta de administrador de clúster. Si es necesario, puede cambiar la contraseña de esta cuenta desde Cloud Manager.

No debe cambiar la contraseña de la cuenta de administrador mediante System Manager o la CLI. La contraseña no se reflejará en Cloud Manager. Como resultado, Cloud Manager no puede supervisar la instancia correctamente.

Pasos

1. En el entorno de trabajo, haga clic en el icono de menú y, a continuación, haga clic en **Avanzado > establecer contraseña**.
2. Introduzca la nueva contraseña dos veces y, a continuación, haga clic en **Guardar**.

   La nueva contraseña debe ser diferente de una de las últimas seis contraseñas que ha utilizado.

Cambiar la MTU de red para instancias c4.4xgrande y c4.8xgrande

De forma predeterminada, Cloud Volumes ONTAP se configura para utilizar 9,000 MTU (también denominado tramas gigantes) cuando se selecciona la instancia c4.4xgrande o la instancia c4.8xgrande en AWS. Puede cambiar el MTU de red a 1,500 bytes si es más adecuado para la configuración de red.

Acerca de esta tarea

Una unidad de transmisión máxima (MTU) de red de 9,000 bytes puede proporcionar el mayor rendimiento de red posible para configuraciones específicas.

El valor de MTU de 9,000 es una buena opción si los clientes del mismo VPC se comunican con el sistema de Cloud Volumes ONTAP y algunos de esos clientes también admiten 9,000 MTU. Si el tráfico abandona el VPC, se puede producir la fragmentación del paquete, lo que degrada el rendimiento.

Una MTU de red de 1,500 bytes es una buena opción si los clientes o sistemas fuera del VPC se comunican con el sistema de Cloud Volumes ONTAP.

Pasos

1. En el entorno de trabajo, haga clic en el icono de menú y, a continuación, haga clic en **Avanzado > utilización de red**.
2. Seleccione **Estándar** o **tramas jumbo**.
3. Haga clic en **Cambiar**.

Cambiar las tablas de rutas asociadas con pares de alta disponibilidad en varios AWS AZS

Puede modificar las tablas de rutas de AWS que incluyen las rutas a las direcciones IP flotantes de un par de alta disponibilidad. Puede hacerlo si los nuevos clientes NFS o CIFS necesitan acceder a un par de alta disponibilidad en AWS.

Pasos

1. En el entorno de trabajo, haga clic en el icono de menú y, a continuación, haga clic en **Información**.
2. Haga clic en **tablas de rutas**.
3. Modifique la lista de tablas de rutas seleccionadas y, a continuación, haga clic en **Guardar**.

Resultado

Cloud Manager envía una solicitud de AWS para modificar las tablas de rutas.

Administrar el estado de Cloud Volumes ONTAP

Puede parar y iniciar Cloud Volumes ONTAP desde Cloud Manager para gestionar sus costes de tecnología de cloud.

Programar apagados automáticos de Cloud Volumes ONTAP

Es posible que desee apagar Cloud Volumes ONTAP durante intervalos de tiempo específicos para reducir los costes de computación. En lugar de hacerlo manualmente, puede configurar Cloud Manager para que se apague automáticamente y, a continuación, reinicie los sistemas en momentos específicos.

Acerca de esta tarea

Cuando se programa un apagado automático del sistema de Cloud Volumes ONTAP, Cloud Manager pospone el apagado si hay una transferencia de datos activa en curso. Cloud Manager apaga el sistema una vez que finaliza la transferencia.

Esta tarea programa los apagados automáticos de ambos nodos en un par de alta disponibilidad.

Pasos

1. En el entorno de trabajo, haga clic en el icono del reloj:

2. Especifique la programación de apagado:

   a. Elija si desea apagar el sistema todos los días, todos los días de la semana, cada fin de semana o cualquier combinación de las tres opciones.

   b. Especifique cuándo desea apagar el sistema y durante cuánto tiempo desea apagarlo.

      ejemplo

      En la siguiente imagen, se muestra una programación que indica a Cloud Manager que apague el sistema todos los sábados a las 12:00 a. m. durante 48 horas. Cloud Manager reinicia el sistema cada lunes a las 12:00

3. Haga clic en **Guardar**.

Resultado

Cloud Manager guarda la programación. El icono de reloj cambia para indicar que se ha establecido una programación: 

Detener Cloud Volumes ONTAP

Detener Cloud Volumes ONTAP le ahorra acumular costes informáticos y crear snapshots de los discos raíz y de arranque, lo que puede ser útil para la solución de problemas.

Acerca de esta tarea

Cuando detiene una pareja de alta disponibilidad, Cloud Manager apaga ambos nodos.

Pasos

1. En el entorno de trabajo, haga clic en el icono **Apagar**.

2. Mantenga la opción de crear snapshots habilitadas porque las snapshots pueden habilitar la recuperación del sistema.
3. Haga clic en **Apagar**.

   Detener el sistema puede tardar hasta unos minutos. Puede reiniciar los sistemas más adelante desde la página del entorno de trabajo.

Supervisar los costes de recursos de AWS

Cloud Manager permite ver los costes de recursos asociados con la ejecución de Cloud Volumes ONTAP en AWS. También puede ver cuánto dinero ha ahorrado con las funciones de NetApp que pueden reducir los costes de almacenamiento.

Acerca de esta tarea

Cloud Manager actualiza los costes cuando se actualiza la página. Debería consultar AWS para obtener información sobre el coste final.

Paso

1. Compruebe que Cloud Manager puede obtener información de costes de AWS:
   a. Compruebe que la política de IAM que proporciona permisos a Cloud Manager incluye las siguientes acciones:

      ```
      "ce:GetReservationUtilization",
      "ce:GetDimensionValues",
      "ce:GetCostAndUsage",
      "ce:GetTags"
      ```

      Estas acciones se incluyen en las últimas novedades "Política de Cloud Manager". Los nuevos sistemas implementados desde Cloud Central de NetApp incluyen automáticamente estos permisos.

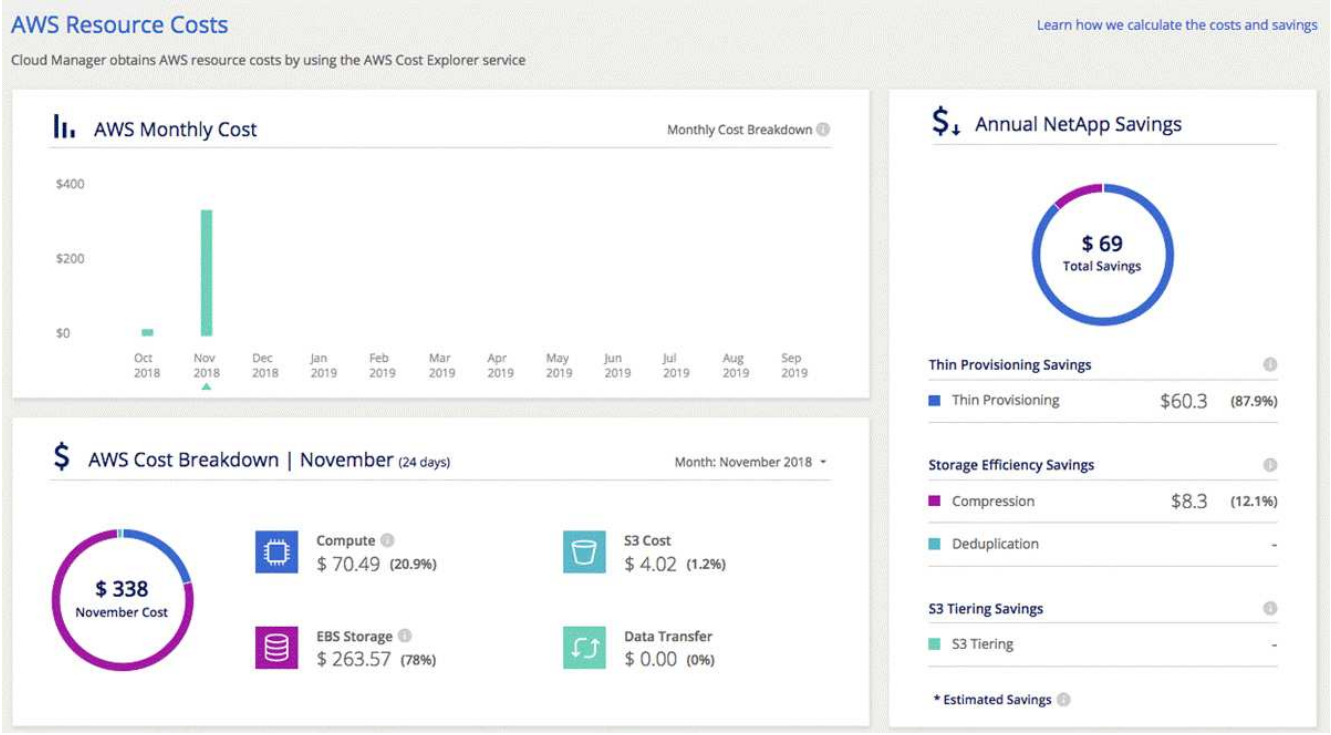
   b. "Active la etiqueta **WorkingEnvironmentId**".

      Para realizar un seguimiento de los costes de AWS, Cloud Manager asigna una etiqueta de asignación de costes a las instancias de Cloud Volumes ONTAP. Después de crear su primer entorno de trabajo, active la etiqueta **WorkingEnvironmentId**. Las etiquetas definidas por el usuario no aparecen en los informes de facturación de AWS hasta que las active en la consola de gestión de costes y facturación.

2. En la página entornos de trabajo, seleccione un entorno de trabajo Cloud Volumes ONTAP y, a continuación, haga clic en **costo**.

   La página de costes muestra los costes de los meses actuales y anteriores y muestra sus ahorros anuales de NetApp si habilitó las funciones de ahorro de costes en volúmenes de NetApp.

   La siguiente imagen muestra una página de costes de ejemplo:



Conectando a Cloud Volumes ONTAP

Si necesita realizar una gestión avanzada de Cloud Volumes ONTAP, puede hacerlo mediante System Manager de OnCommand o la interfaz de línea de comandos.

Conexión a System Manager

Es posible que deba realizar algunas tareas de Cloud Volumes ONTAP desde System Manager, que es una herramienta de gestión basada en explorador que se ejecuta en el sistema Cloud Volumes ONTAP. Por ejemplo, debe usar System Manager si desea crear LUN.

Antes de empezar

El equipo desde el que accede a Cloud Manager debe tener una conexión de red a Cloud Volumes ONTAP. Por ejemplo, es posible que tenga que iniciar sesión en Cloud Manager desde un host de salto en AWS o Azure.

> Cuando se implementa en varias zonas de disponibilidad de AWS, las configuraciones de alta disponibilidad de Cloud Volumes ONTAP utilizan una dirección IP flotante para la interfaz de gestión del clúster, lo que significa que no hay disponible el enrutamiento externo. Debe conectarse desde un host que forme parte del mismo dominio de enrutamiento.

Pasos

1. En la página Working Environments, haga doble clic en el sistema Cloud Volumes ONTAP que desea gestionar con System Manager.
2. Haga clic en el icono de menú y, a continuación, haga clic en **Avanzado > Administrador del sistema**.
3. Haga clic en **Iniciar**.

   System Manager se carga en una nueva pestaña del navegador.

4. En la pantalla de inicio de sesión, introduzca **admin** en el campo Nombre de usuario, introduzca la contraseña que especificó al crear el entorno de trabajo y, a continuación, haga clic en **Iniciar sesión**.

Resultado

Se carga la consola de System Manager. Ahora puede usarlo para gestionar Cloud Volumes ONTAP.

Conexión a la CLI de Cloud Volumes ONTAP

La CLI de Cloud Volumes ONTAP le permite ejecutar todos los comandos administrativos y es una buena opción para las tareas avanzadas o si se siente más cómodo mediante la CLI. Puede conectarse a la CLI mediante Secure Shell (SSH).

Antes de empezar

El host desde el que se utiliza SSH para conectarse a Cloud Volumes ONTAP debe tener una conexión de red a Cloud Volumes ONTAP. Por ejemplo, es posible que tenga que utilizar SSH desde un host de salto en AWS o Azure.

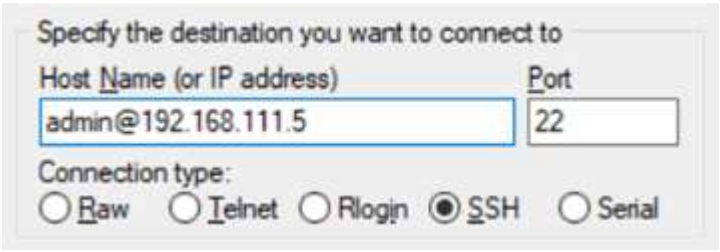
> Cuando se implementa en múltiples AZs, las configuraciones de alta disponibilidad de Cloud Volumes ONTAP utilizan una dirección IP flotante para la interfaz de gestión del clúster, lo que significa que el enrutamiento externo no está disponible. Debe conectarse desde un host que forme parte del mismo dominio de enrutamiento.

Pasos

1. En Cloud Manager, identifique la dirección IP de la interfaz de gestión de clústeres:
   a. En la página entornos de trabajo, seleccione el sistema Cloud Volumes ONTAP.
   b. Copie la dirección IP de gestión del clúster que aparece en el panel derecho.
2. Utilice SSH para conectarse a la dirección IP de la interfaz de gestión del clúster mediante la cuenta de administrador.

   ejemplo

   La siguiente imagen muestra un ejemplo con PuTTY:



3. En la solicitud de inicio de sesión de, introduzca la contraseña de la cuenta de administrador.

   ejemplo

```
Password: ********
COT2::>
```

Adición de sistemas de Cloud Volumes ONTAP existentes a Cloud Manager

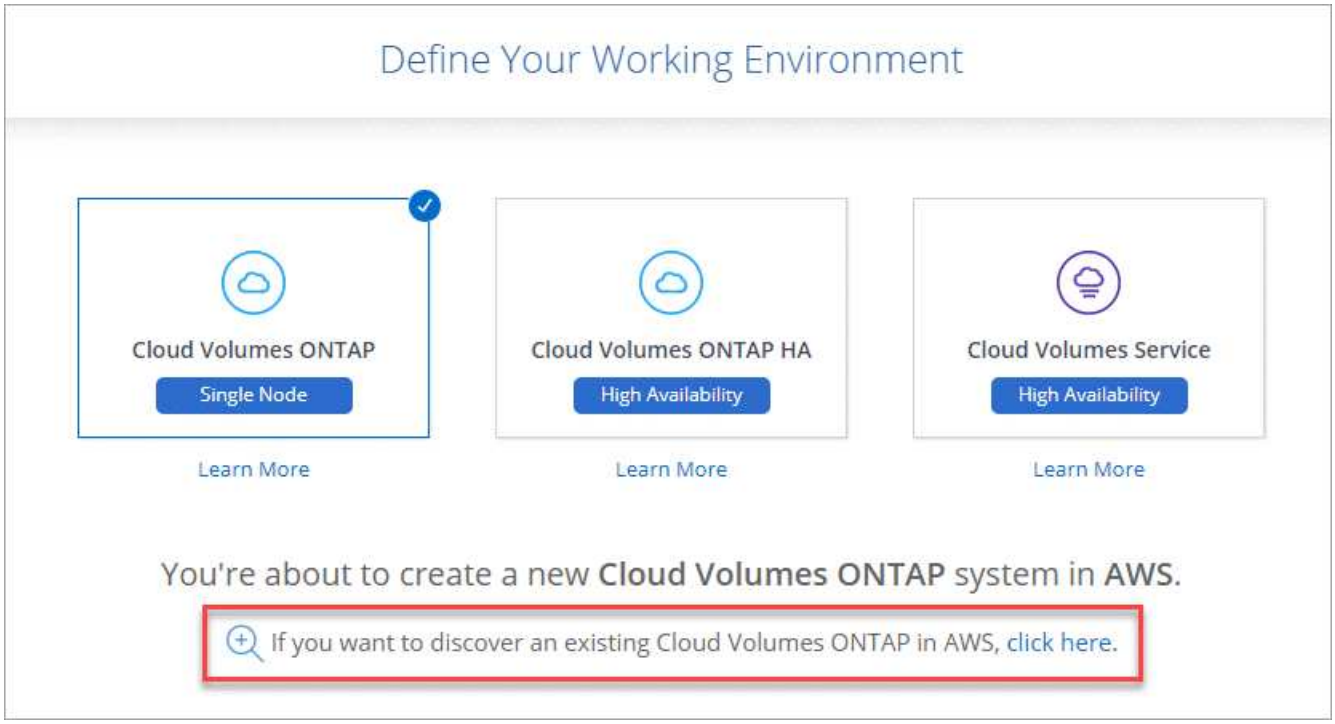
Puede detectar y añadir sistemas de Cloud Volumes ONTAP existentes a Cloud Manager. Puede hacer esto si se implementó un nuevo sistema Cloud Manager.

Antes de empezar

Debe conocer la contraseña de la cuenta de usuario administrador de Cloud Volumes ONTAP.

Pasos

1. En la página entornos de trabajo, haga clic en **Agregar entorno de trabajo**.
2. Seleccione el proveedor de cloud en el que reside el sistema.
3. Elija el tipo de sistema Cloud Volumes ONTAP.
4. Haga clic en el enlace para detectar un sistema existente.



5. En la página Región, seleccione la región donde se ejecutan las instancias y, a continuación, seleccione las instancias.
6. En la página credenciales, introduzca la contraseña para el usuario administrador de Cloud Volumes ONTAP y, a continuación, haga clic en **Ir**.

Resultado

Cloud Manager agrega las instancias de Cloud Volumes ONTAP al espacio de trabajo.

Eliminar un entorno de trabajo de Cloud Volumes ONTAP

Lo mejor es eliminar sistemas de Cloud Volumes ONTAP de Cloud Manager, en lugar de hacerlo de la consola de su proveedor de cloud. Por ejemplo, si termina una instancia de Cloud Volumes ONTAP con licencia desde AWS, no puede utilizar la clave de licencia para otra instancia. Debe eliminar el entorno de trabajo de Cloud Manager para liberar la

licencia.

Acerca de esta tarea

Cuando se elimina un entorno de trabajo, Cloud Manager termina las instancias, elimina discos y instantáneas.

> Las instancias de Cloud Volumes ONTAP tienen habilitada la protección de terminación para ayudar a evitar la terminación accidental de AWS. Sin embargo, si da por terminado una instancia de Cloud Volumes ONTAP desde AWS, debe ir a la consola de AWS CloudFormation y eliminar la pila de la instancia. El nombre de la pila es el nombre del entorno de trabajo.

Pasos

1. En el entorno de trabajo, haga clic en el icono de menú y, a continuación, haga clic en **Eliminar**.
2. Escriba el nombre del entorno de trabajo y, a continuación, haga clic en **Eliminar**.

   La eliminación del entorno de trabajo puede tardar hasta 5 minutos.

Aprovisionamiento de volúmenes mediante un servicio de archivos

Azure NetApp Files

Más información sobre Azure NetApp Files

Azure NetApp Files permite a las empresas migrar y ejecutar sus aplicaciones esenciales para la empresa, sensibles a la latencia y con un alto rendimiento en Azure sin necesidad de refactorizar el cloud.

Funciones

- La compatibilidad con varios protocolos permite que las aplicaciones de Linux y Windows se ejecuten sin problemas en Azure.
- Los múltiples niveles de rendimiento permiten alinear estrechamente con los requisitos de rendimiento de la carga de trabajo.
- Las certificaciones más importantes, incluidos SAP HANA, GDPR e HIPPA, permiten la migración de las cargas de trabajo más exigentes a Azure.

Funciones adicionales de Cloud Manager

- Migre datos de NFS o SMB a Azure NetApp Files directamente desde Cloud Manager. Las migraciones de datos se realizan a través del servicio Cloud Sync de NetApp. "Leer más".
- Con la tecnología impulsada por la inteligencia artificial (IA), Cloud Compliance puede ayudarle a comprender el contexto de los datos e identificar los datos confidenciales que residen en sus cuentas de Azure NetApp Files. "Leer más".

Coste

"Ver los precios de Azure NetApp Files".

Tenga en cuenta que el servicio de Azure NetApp Files y no Cloud Manager mantienen su suscripción y sus cargos.

Regiones admitidas

"Consulte las regiones de Azure admitidas".

Solicitando acceso

Debe tener acceso a Azure NetApp Files por "envío de una solicitud en línea". Tendrá que esperar la aprobación del equipo de Azure NetApp Files para poder continuar.

Obtener ayuda

En el caso de los problemas de soporte técnico asociados con Azure NetApp Files, use el portal de Azure para registrar una solicitud de soporte a Microsoft. Seleccione su suscripción de Microsoft asociada y seleccione el nombre de servicio **Azure NetApp Files** en **almacenamiento**. Proporcione la información restante necesaria para crear su solicitud de soporte técnico de Microsoft.

En el caso de problemas relacionados con Cloud Sync y Azure NetApp Files, puede empezar con NetApp utilizando su número de serie Cloud Sync directamente desde el servicio Cloud Sync. Deberá acceder al servicio Cloud Sync a través del enlace en Cloud Manager. "Consulte el proceso para habilitar la compatibilidad con Cloud Sync".

Enlaces relacionados

- "Cloud Central de NetApp: Azure NetApp Files"
- "Documentación de Azure NetApp Files"
- "Documentación de Cloud Sync"

Configurar Azure NetApp Files

Cree un entorno de trabajo de Azure NetApp Files en Cloud Manager para crear y gestionar cuentas, pools de capacidad, volúmenes y snapshots de NetApp.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

Solicitar acceso

"Enviar una solicitud en línea" Para que se le conceda acceso a Azure NetApp Files.

Configure una aplicación de Azure AD

En Azure, conceda permisos a una aplicación Azure AD y copie el ID de la aplicación (cliente), el ID de directorio (inquilino) y el valor de un secreto de cliente.

Crear un entorno de trabajo de Azure NetApp Files

En Cloud Manager, haga clic en **Agregar entorno de trabajo** > **Microsoft Azure** > **Azure NetApp Files** y, a continuación, proporcione detalles sobre la aplicación AD.

Solicitando acceso

Debe tener acceso a Azure NetApp Files por "envío de una solicitud en línea". Tendrá que esperar la aprobación del equipo de Azure NetApp Files para poder continuar.

Configuración de una aplicación Azure AD

Cloud Manager necesita permisos para configurar y gestionar Azure NetApp Files. Puede otorgar los permisos requeridos a una cuenta de Azure mediante la creación y configuración de una aplicación de Azure AD, así como la obtención de las credenciales de Azure que Cloud Manager necesita.

Creación de la aplicación AD

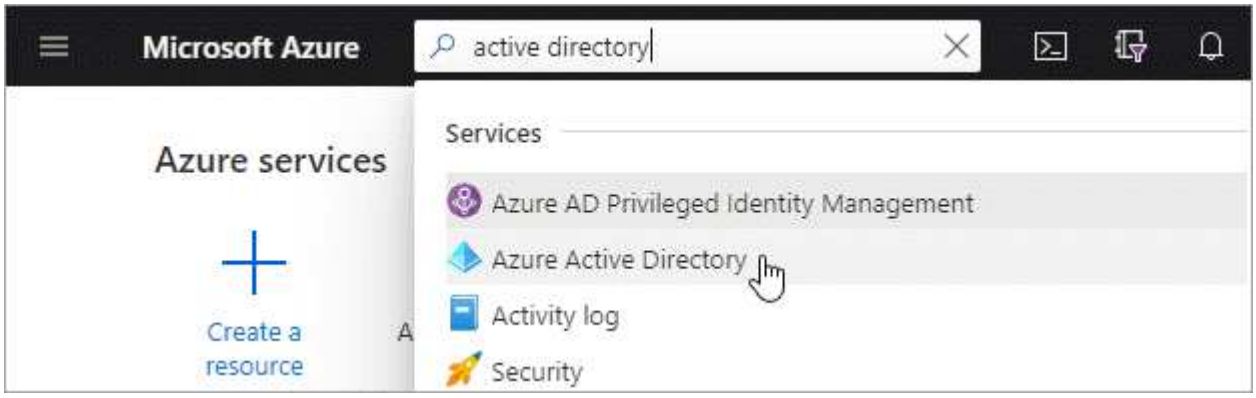
Cree una aplicación de Azure Active Directory (AD) y una entidad de servicio que Cloud Manager pueda usar para el control de acceso basado en roles.

Antes de empezar

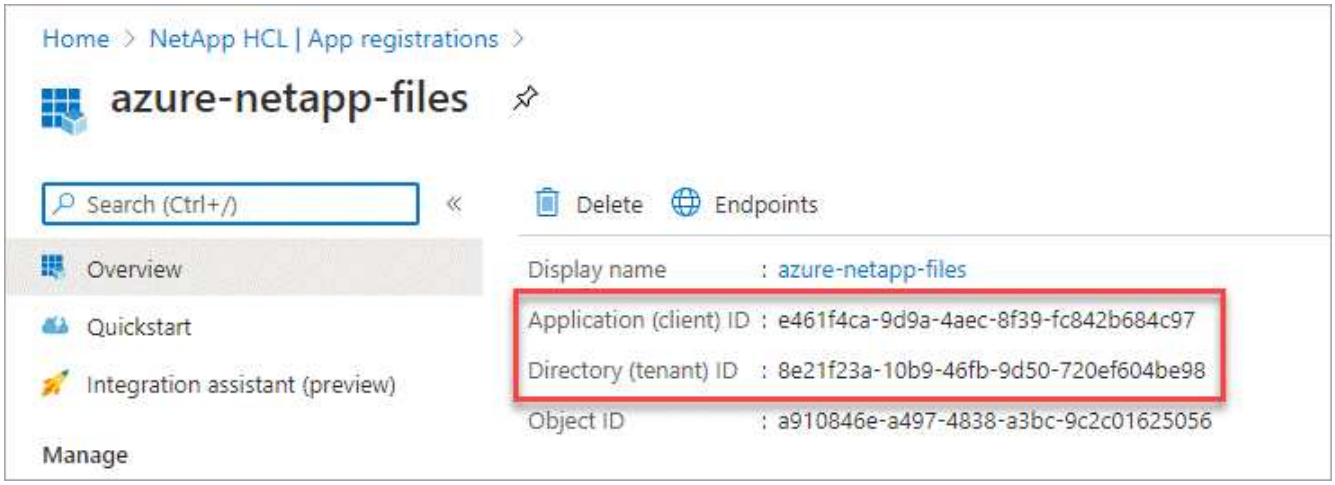
Debe tener los permisos adecuados en Azure para crear una aplicación de Active Directory y asignar la aplicación a un rol. Para obtener más información, consulte "Documentación de Microsoft Azure: Permisos necesarios".

Pasos

1. Desde el portal de Azure, abra el servicio **Azure Active Directory**.



2. En el menú, haga clic en **App registrs**.
3. Cree la aplicación:
   a. Haga clic en **Nuevo registro**.
   b. Especificar detalles acerca de la aplicación:
      - **Nombre**: Introduzca un nombre para la aplicación.
      - **Tipo de cuenta**: Seleccione un tipo de cuenta (cualquiera funcionará con Cloud Manager).
      - **Redirigir URI**: Puede dejar este espacio en blanco.
   c. Haga clic en **Registrar**.
4. Copie el **ID de aplicación (cliente)** y el **ID de directorio (inquilino)**.



Al crear el entorno de trabajo de Azure NetApp Files en Cloud Manager, debe proporcionar el ID de la aplicación (cliente) y el ID del directorio (inquilino) para la aplicación. Cloud Manager utiliza los ID para iniciar sesión mediante programación.

5. Cree un secreto de cliente para la aplicación de modo que Cloud Manager pueda utilizarlo para la autenticación de Azure AD:
   a. Haga clic en **certificados y secretos > Nuevo secreto de cliente**.
   b. Proporcione una descripción del secreto y una duración.
   c. Haga clic en **Agregar**.
   d. Copie el valor del secreto de cliente.

Resultado

La aplicación AD está configurada y debe haber copiado el ID de la aplicación (cliente), el ID del directorio (arrendatario) y el valor del secreto del cliente. Debe introducir esta información en Cloud Manager cuando añada un entorno de trabajo de Azure NetApp Files.

Asignación de la aplicación a una función

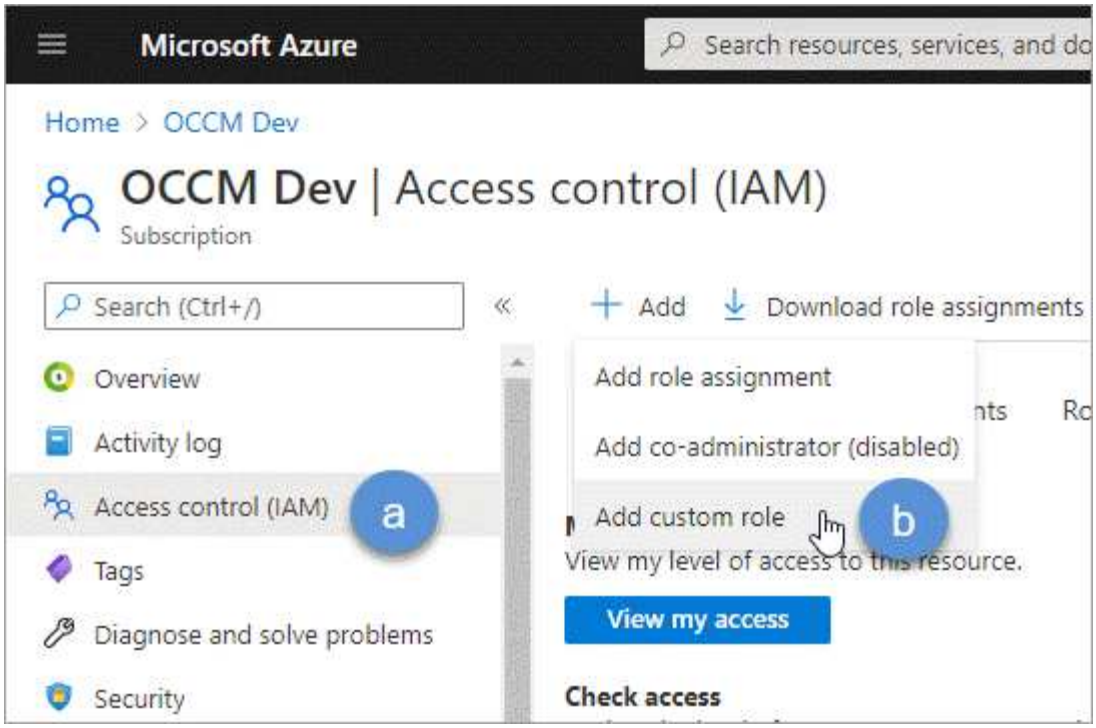
Debe enlazar el principal del servicio con la suscripción a Azure y asignarle una función personalizada que tenga los permisos necesarios.

Pasos

1. "Crear un rol personalizado en Azure".

   Los siguientes pasos describen cómo crear el rol desde el portal de Azure.

   a. Abra la suscripción y haga clic en **Control de acceso (IAM)**.
   b. Haga clic en **Agregar > Agregar rol personalizado**.



c. En la ficha **conceptos básicos**, escriba un nombre y una descripción para la función.

d. Haga clic en **JSON** y haga clic en **Editar**, que aparece en la parte superior derecha del formato JSON.

e. Agregue los siguientes permisos en *Actions*:

```
"actions": [
    "Microsoft.NetApp/*",
    "Microsoft.Resources/resources/read",
    "Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
    "Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Insights/Metrics/Read"
    ],
```

f. Haga clic en **Guardar**, haga clic en **Siguiente** y, a continuación, haga clic en **Crear**.

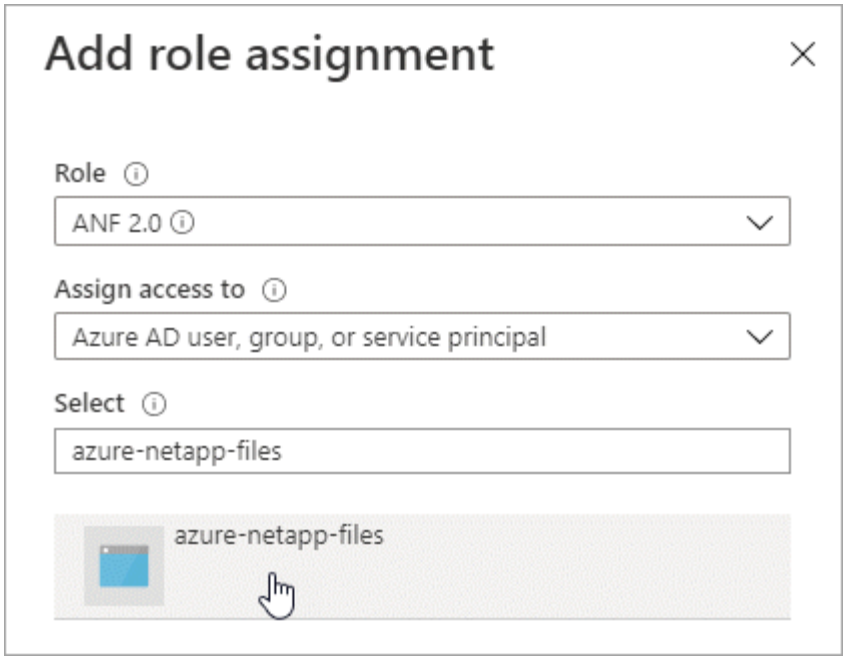
2. Ahora asigne la aplicación al rol que acaba de crear:

a. En el portal de Azure, abra la suscripción y haga clic en **Control de acceso (IAM) > Agregar > Agregar asignación de funciones**.

b. Seleccione la función personalizada que ha creado.

c. Mantener seleccionado **usuario, grupo o principal de servicio de Azure AD**.

d. Busque el nombre de la aplicación (no puede encontrarlo en la lista desplazándose).



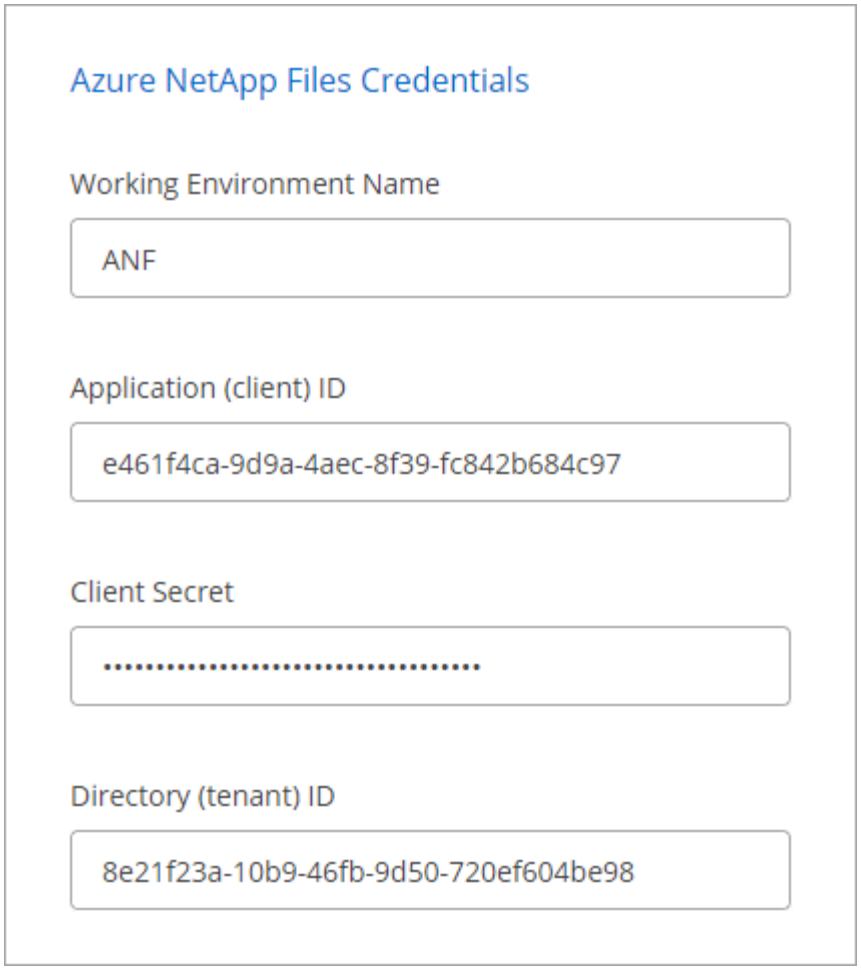
e. Seleccione la aplicación y haga clic en **Guardar**.

   El director de servicio de Cloud Manager ahora tiene los permisos de Azure necesarios para esa suscripción.

Crear un entorno de trabajo de Azure NetApp Files

Configure un entorno de trabajo de Azure NetApp Files en Cloud Manager para que pueda empezar a crear volúmenes.

1. En la página entornos de trabajo, haga clic en **Agregar entorno de trabajo**.
2. Seleccione **Microsoft Azure** y, a continuación, **Azure NetApp Files**.
3. Proporcione detalles acerca de la aplicación AD configurada anteriormente.



4. Haga clic en **Agregar**.

Resultado

Ahora debería tener un entorno de trabajo de Azure NetApp Files.

El futuro

"Comience a crear y gestionar volúmenes".

Crear y gestionar volúmenes para Azure NetApp Files

Después de configurar el entorno de trabajo, puede crear y gestionar cuentas de Azure NetApp Files, pools de capacidad, volúmenes y snapshots.

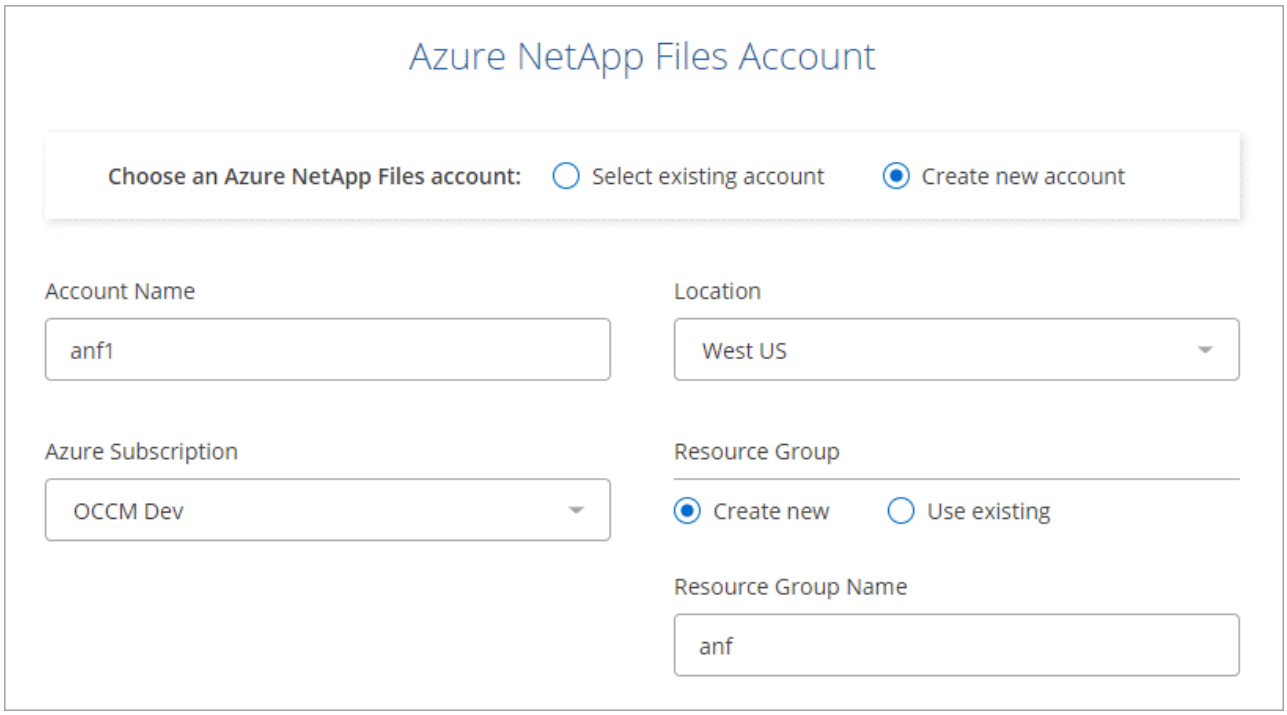
Crear volúmenes

Es posible crear volúmenes de NFS o SMB en una cuenta de Azure NetApp Files nueva o existente.

Pasos

1. Abra el entorno de trabajo de Azure NetApp Files.
2. Haga clic en **Añadir nuevo volumen**.
3. Proporcione la información necesaria en cada página:

   - **cuenta de Azure NetApp Files**: Elija una cuenta de Azure NetApp Files existente o cree una nueva cuenta.



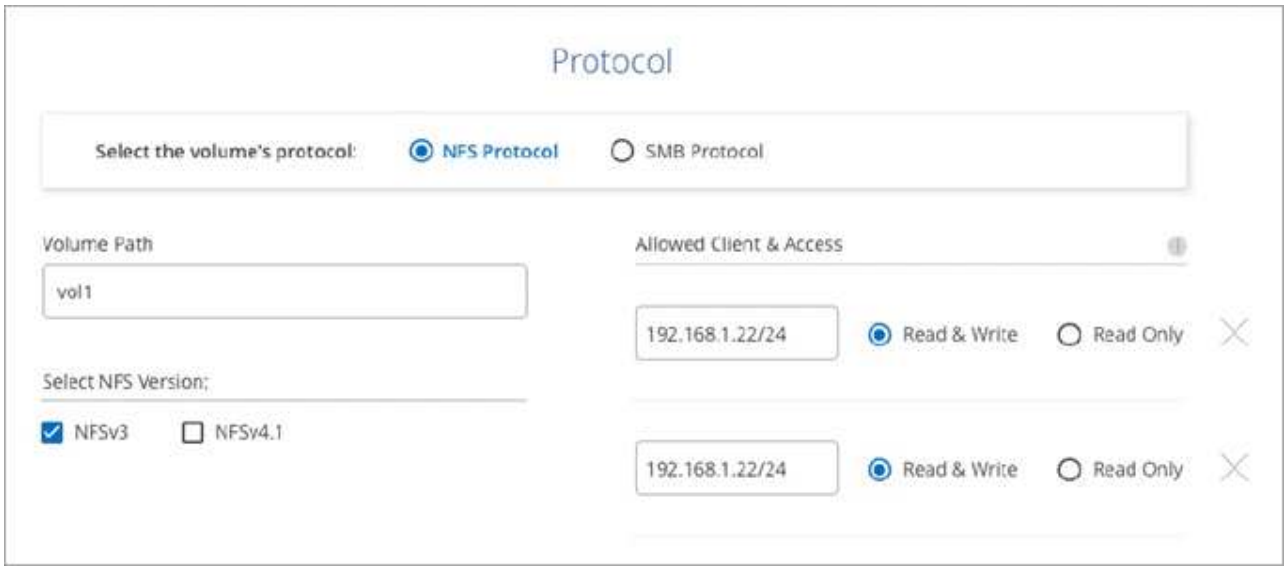
   - **capacidad Pool**: Seleccione un pool de capacidad existente o cree un nuevo pool de capacidad.

     Si crea un pool de capacidad nuevo, debe especificar un tamaño y seleccionar un "nivel de servicio".

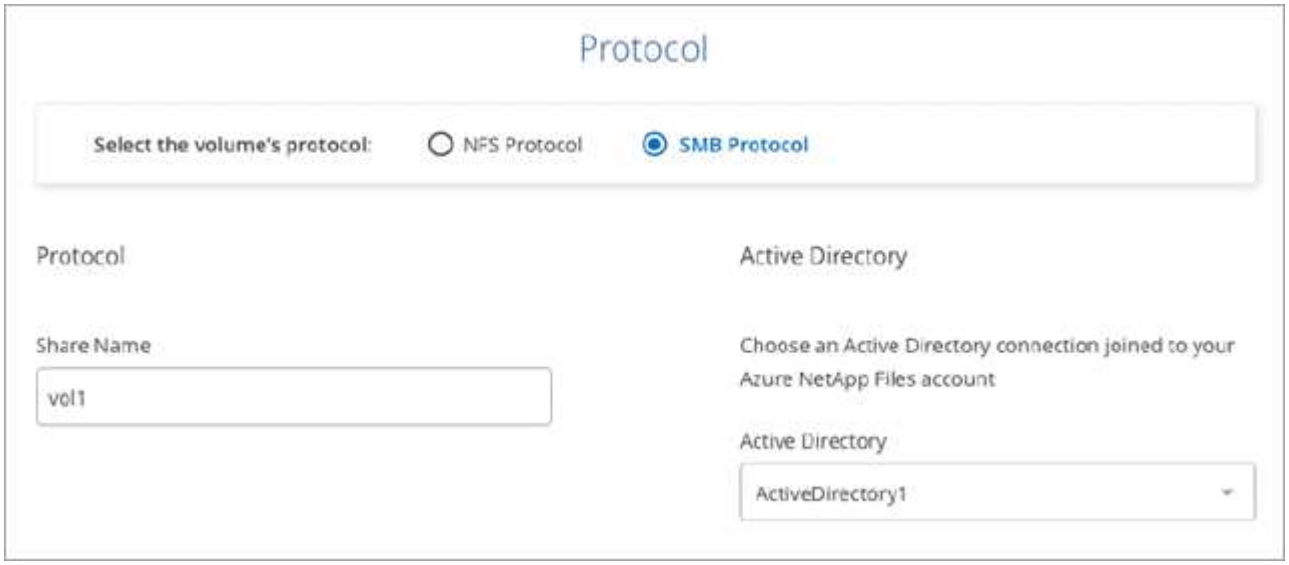
     El tamaño mínimo del pool de capacidad es de 4 TB. Es posible especificar un tamaño en múltiplos de 4 TB.

   - **Detalles y etiquetas**: Introduzca un nombre y un tamaño de volumen, el vnet y la subred donde debería residir el volumen y, opcionalmente, especifique etiquetas para el volumen.
   - **Protocolo**: Elija el protocolo NFS o SMB e introduzca la información necesaria.

     A continuación encontrará un ejemplo de detalles de NFS.



A continuación encontrará un ejemplo de detalles de SMB. Necesitará proporcionar información de Active Directory al configurar el primer volumen de SMB.



4. Haga clic en **Añadir volumen**.

Montaje de volúmenes

Acceda a instrucciones de montaje desde Cloud Manager para que pueda montar el volumen en un host.

Pasos

1. Abra el entorno de trabajo.
2. Pase el ratón sobre el volumen y seleccione **montar el volumen**.

3. Siga las instrucciones para montar el volumen.

Editar el tamaño y las etiquetas de un volumen

Después de crear un volumen, puede modificar su tamaño y sus etiquetas en cualquier momento.

Pasos

1. Abra el entorno de trabajo.
2. Pase el ratón sobre el volumen y seleccione **Editar**.
3. Modifique el tamaño y las etiquetas según sea necesario.
4. Haga clic en **aplicar**.

Gestione las copias Snapshot

Las copias Snapshot proporcionan una copia puntual de su volumen. Cree copias Snapshot, restaure los datos a un volumen nuevo y elimine copias Snapshot.

Pasos

1. Abra el entorno de trabajo.
2. Pase el ratón sobre el volumen y elija una de las opciones disponibles para gestionar las copias Snapshot:
   - **Crear una copia Snapshot**
   - **Restaurar a un nuevo volumen**
   - **Eliminar una copia snapshot**
3. Siga las indicaciones para completar la acción seleccionada.

Eliminar volúmenes

Elimine los volúmenes que ya no necesita.

Pasos

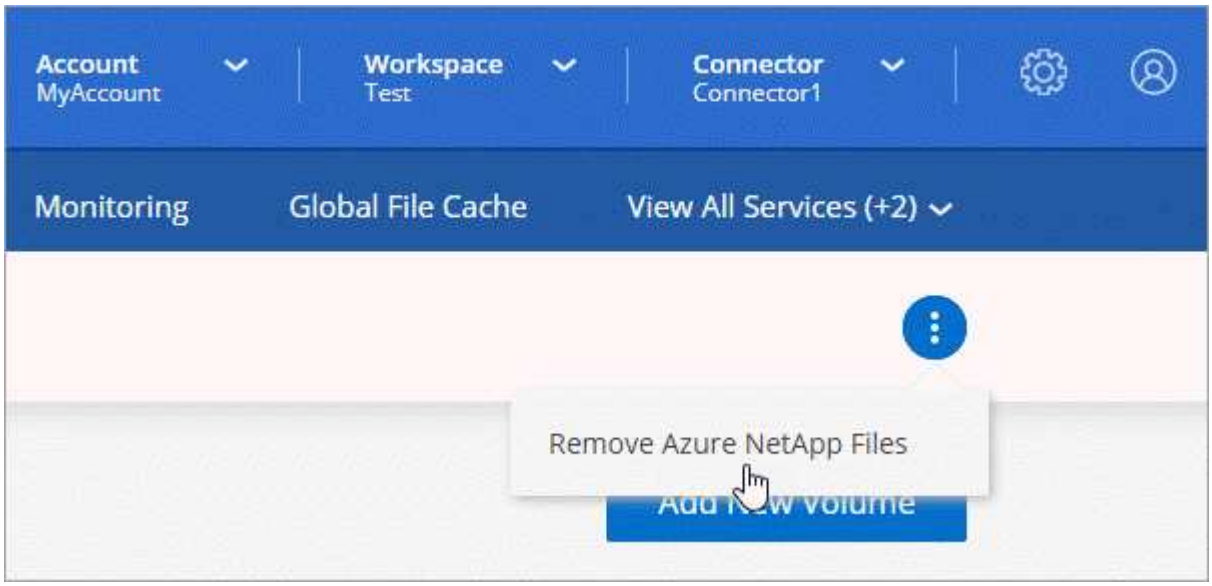
1. Abra el entorno de trabajo.
2. Pase el ratón sobre el volumen y haga clic en **Eliminar**.
3. Confirme que desea eliminar el volumen.

Quitando Azure NetApp Files

Esta acción quita Azure NetApp Files de Cloud Manager. No elimina tu cuenta ni los volúmenes de Azure NetApp Files. Puede volver a añadir Azure NetApp Files a Cloud Manager en cualquier momento.

Pasos

1. Abra el entorno de trabajo de Azure NetApp Files.
2. En la parte superior derecha de la página, seleccione el menú acciones y haga clic en **Quitar Azure NetApp Files**.



3. Haga clic en **Eliminar** para confirmar.

Cloud Volumes Service para AWS

Obtenga más información sobre Cloud Volumes Service para AWS

Cloud Volumes Service de NetApp para AWS es un servicio de archivos nativo del cloud que proporciona volúmenes NAS a través de NFS y SMB con rendimiento all-flash. Este servicio permite que cualquier carga de trabajo, incluidas aplicaciones heredadas, se ejecute en el cloud de AWS.

Ventajas de usar Cloud Volumes Service para AWS

Cloud Volumes Service para AWS ofrece las siguientes ventajas:

- Servicio totalmente gestionado, por lo tanto, no es necesario configurar ni gestionar dispositivos de almacenamiento
- Compatibilidad con NFSv3 y NFSv4.1, y los protocolos NAS de SMB 3.0 y 3.1.1
- Acceso seguro a instancias de Linux y de Windows Elastic Container Service (ECS), con soporte incluido:
  - Amazon Linux 2, Red Hat Enterprise Linux 7.5, SLES 12 SP3 y Ubuntu 16.04 LTS
  - Windows Server 2008 R2, Windows Server 2012 R2 y Windows Server 2016
- Opción de precios incluidos y de pago por uso

Coste

Los volúmenes creados por Cloud Volumes Service para AWS se cobran según su suscripción al servicio, no mediante Cloud Manager.

Cloud Manager no tiene ningún coste para descubrir un volumen o región de Cloud Volumes Service para AWS.

Antes de empezar

- Cloud Manager puede descubrir suscripciones y volúmenes existentes de Cloud Volumes Service para AWS. Consulte "Guía de configuración de la cuenta de Cloud Volumes Service para AWS de NetApp" si aún no ha configurado su suscripción. Debe seguir este proceso de configuración para cada región antes de poder añadir las suscripciones y volúmenes de AWS en Cloud Manager.
- Debe obtener la clave de API de Cloud Volumes y la clave secreta para poder proporcionarlas a Cloud Manager. "Para obtener instrucciones, consulte la documentación de Cloud Volumes Service para AWS".

Inicio rápido

Empiece rápidamente siguiendo estos pasos o vaya a la siguiente sección para obtener toda la información.

Verifique la compatibilidad con la configuración

Ha configurado AWS para Cloud Volumes Service y. debe haber suscrito a una de las "Cloud Volumes Service de NetApp en AWS Marketplace".

Añada su suscripción a Cloud Volumes Service para AWS

Debe crear un entorno de trabajo para los volúmenes según la suscripción a Cloud Volumes Service para AWS.

Cree un Cloud Volumes

Los Cloud Volumes que ya existen para esta suscripción aparecen en el nuevo entorno de trabajo. De lo contrario, creará volúmenes nuevos desde Cloud Manager.

Montar un volumen de cloud

Monte nuevos volúmenes de cloud en la instancia de AWS para que los usuarios puedan comenzar a utilizar el almacenamiento.

Obtener ayuda

Use el chat de Cloud Manager para formular preguntas generales de servicio.

Para los problemas de soporte técnico asociados con sus volúmenes de cloud, use su número de serie “930” de 20 dígitos que se encuentra en la pestaña "Soporte" de la interfaz de usuario de Cloud Volumes Service. Utilice este ID de soporte cuando abra un ticket web o llame para recibir asistencia. Asegúrese de activar el

número de serie de Cloud Volumes Service para recibir soporte desde la interfaz de usuario de Cloud Volumes Service. "Estos pasos se explican aquí".

Limitaciones

- Cloud Manager no admite la replicación de datos entre entornos de trabajo al usar volúmenes de Cloud Volumes Service.
- No es posible eliminar su suscripción a Cloud Volumes Service para AWS desde Cloud Manager. Solo puede hacerlo a través de la interfaz de Cloud Volumes Service para AWS.

Enlaces relacionados

- "NetApp Cloud Central: Cloud Volumes Service para AWS"
- "Documentación de Cloud Volumes Service de NetApp para AWS"

Gestionar Cloud Volumes Service para AWS

Cloud Manager le permite crear volúmenes de cloud basados en su "Cloud Volumes Service para AWS" suscripción. También puede detectar los volúmenes de cloud que ya se crearon desde la interfaz de Cloud Volumes Service y añadirlos a un entorno de trabajo.

Añada su suscripción a Cloud Volumes Service para AWS

Independientemente de si ya ha creado volúmenes desde la interfaz de usuario de Cloud Volumes Service o si acaba de suscribirse a Cloud Volumes Service para AWS y no tiene volúmenes, el primer paso es crear un entorno de trabajo para los volúmenes según su suscripción a AWS.

Si Cloud Volumes ya existen para esta suscripción, los volúmenes se añaden automáticamente al nuevo entorno de trabajo. Si todavía no ha añadido ningún volumen de cloud para la suscripción a AWS, podrá hacerlo después de crear el nuevo entorno de trabajo.

Si tiene suscripciones y volúmenes en varias regiones de AWS, debe realizar esta tarea en cada región.

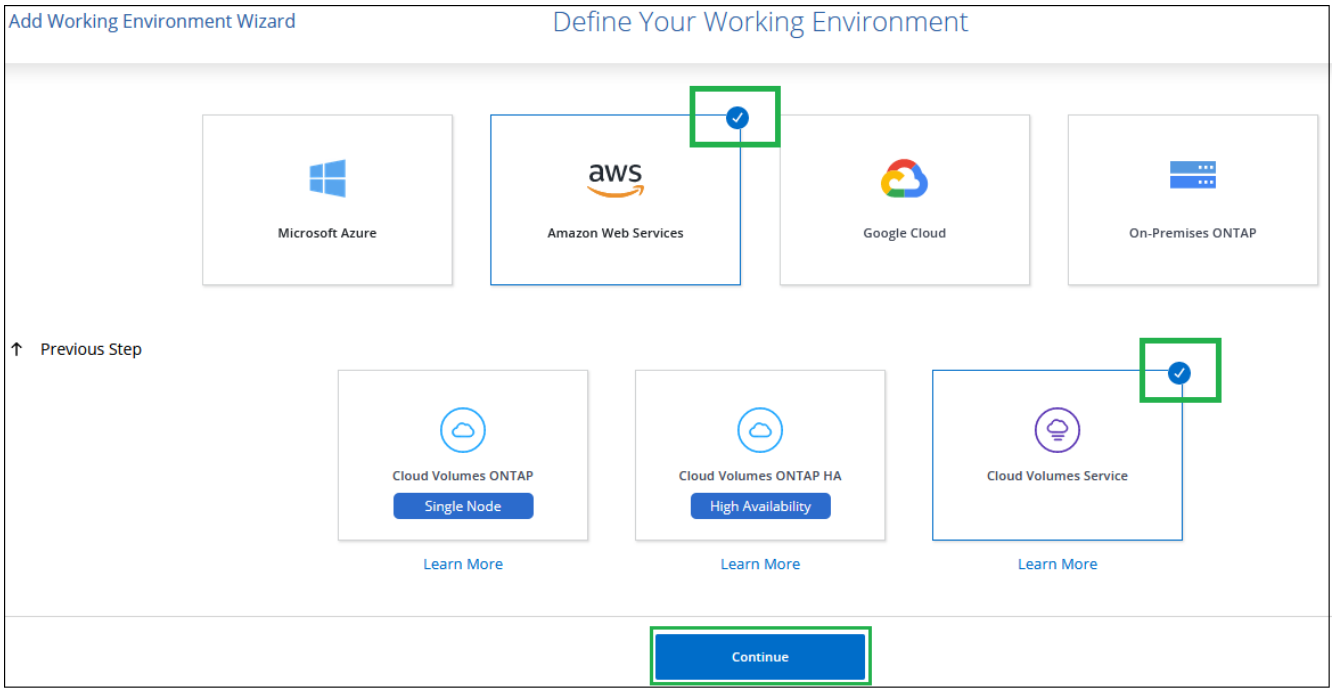
Antes de empezar

Debe disponer de la siguiente información al agregar una suscripción en cada región:

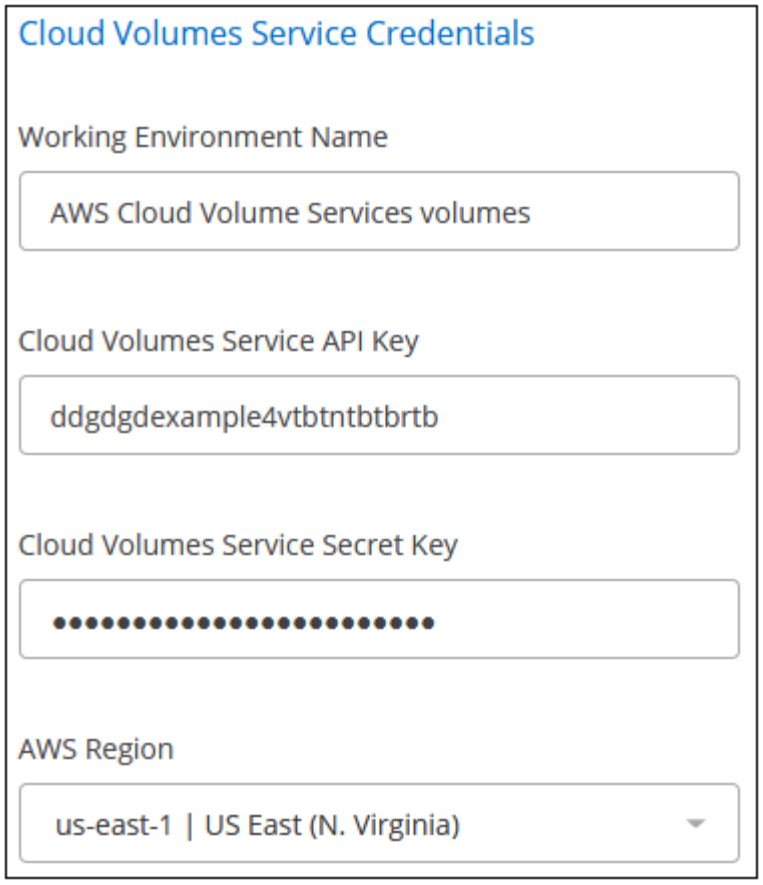
- Clave de API y clave secreta de Cloud Volumes: "Consulte la documentación de Cloud Volumes Service para AWS que desea obtener esta información".
- Región AWS donde se creó la suscripción.

Pasos

1. En Cloud Manager, agregue un nuevo entorno de trabajo, seleccione la ubicación **Amazon Web Services** y haga clic en **continuar**.
2. Seleccione **Cloud Volumes Service** y haga clic en **continuar**.



3. Proporcione información sobre su suscripción a Cloud Volumes Service:
   a. Introduzca el nombre del entorno de trabajo que desee utilizar.
   b. Introduzca la clave de API y la clave secreta de Cloud Volumes Service.
   c. Seleccione la región de AWS en la que residen los volúmenes de cloud o donde se pondrán en marcha.
   d. Haga clic en **Agregar**.



Resultado

Cloud Manager muestra la configuración de Cloud Volumes Service para AWS en la página entornos de trabajo.

Si ya existen volúmenes en la nube para esta suscripción, los volúmenes se agregan automáticamente al nuevo entorno de trabajo, como se muestra en la captura de pantalla. Puede añadir volúmenes de cloud adicionales desde Cloud Manager.

Si no existen Cloud Volumes para esta suscripción, puede crearlos ahora.

Cree Cloud Volumes

Para las configuraciones donde ya hay volúmenes en el entorno de trabajo de Cloud Volumes Service, puede usar estos pasos para añadir volúmenes nuevos.

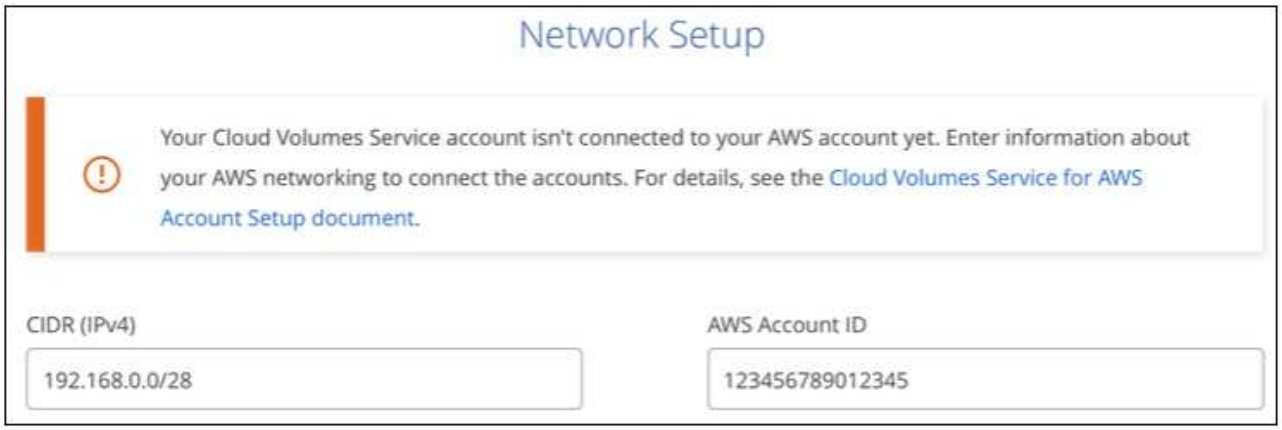
Para configuraciones donde no hay volúmenes, puede crear su primer volumen directamente desde Cloud Manager después de configurar la suscripción a Cloud Volumes Service para AWS. En el pasado, el primer volumen se debía crear directamente en la interfaz de usuario de Cloud Volumes Service.

Antes de empezar

- Si desea usar SMB en AWS, debe haber configurado DNS y Active Directory.
- Cuando planee crear un volumen SMB, debe tener un servidor de Windows Active Directory disponible para el que se pueda conectar. Deberá introducir esta información al crear el volumen. Además, asegúrese de que el usuario Admin puede crear una cuenta de equipo en la ruta de la unidad organizativa (OU) especificada.
- Necesitará esta información al crear el primer volumen en una nueva región/entorno de trabajo:
  - ID de cuenta de AWS: Identificador de cuenta de Amazon de 12 dígitos sin guiones. Para encontrar su ID de cuenta, consulte este "Tema de AWS".
  - Bloque InterDomain Routing (CIDR) sin clase: Bloque IPv4 CIDR sin usar. El prefijo de red debe estar comprendido entre /16 y /28, y también debe estar dentro de los rangos reservados para redes privadas (RFC 1918). No seleccione una red que se superponga con las asignaciones CIDR de VPC.

Pasos

1. Seleccione el nuevo entorno de trabajo y haga clic en **Agregar nuevo volumen**.
2. Si va a añadir el primer volumen al entorno de trabajo de la región, tendrá que añadir la información de red de AWS.
   a. Introduzca el rango de IPv4 (CIDR) para la región.
   b. Introduzca el ID de cuenta de AWS de 12 dígitos (sin guiones) para conectar su cuenta de Cloud Volumes a su cuenta de AWS.
   c. Haga clic en **continuar**.



3. En la página aceptando interfaces virtuales, se describen algunos pasos que deberá realizar después de agregar el volumen para que esté preparado para completar ese paso. Simplemente haga clic en **continuar** de nuevo.
4. En la página Details & Tags, introduzca detalles sobre el volumen:
   a. Escriba un nombre para el volumen.
   b. Especifique un tamaño dentro del intervalo de 100 GIB a 90,000 GIB (equivalente a 88 TIBs).

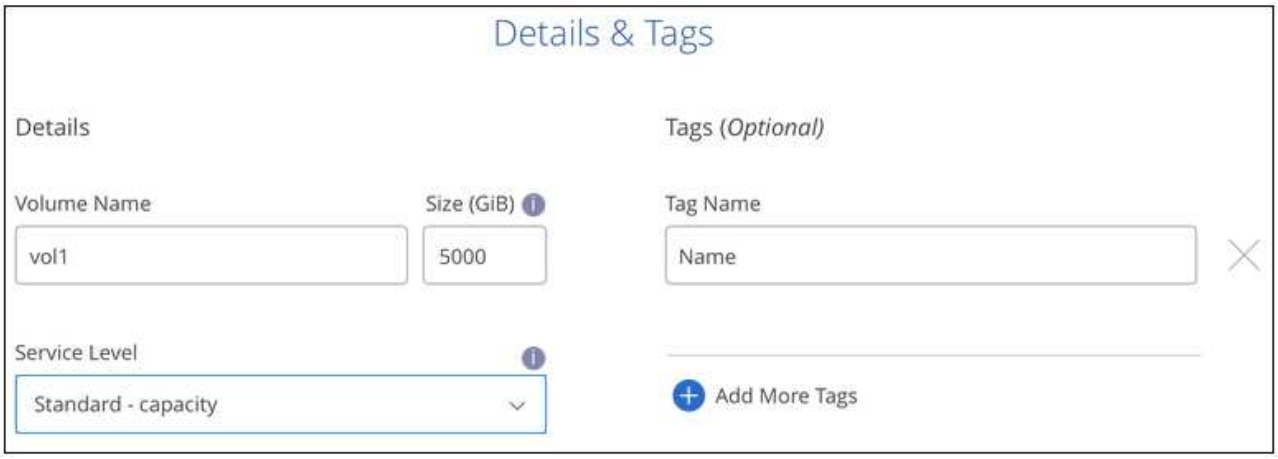
      "Más información sobre la capacidad asignada".

   c. Especifique un nivel de servicio: Standard, Premium o Extreme.

      "Obtenga más información sobre los niveles de servicio".

d. Introduzca uno o más nombres de etiqueta para clasificar el volumen si lo desea.

e. Haga clic en **continuar**.

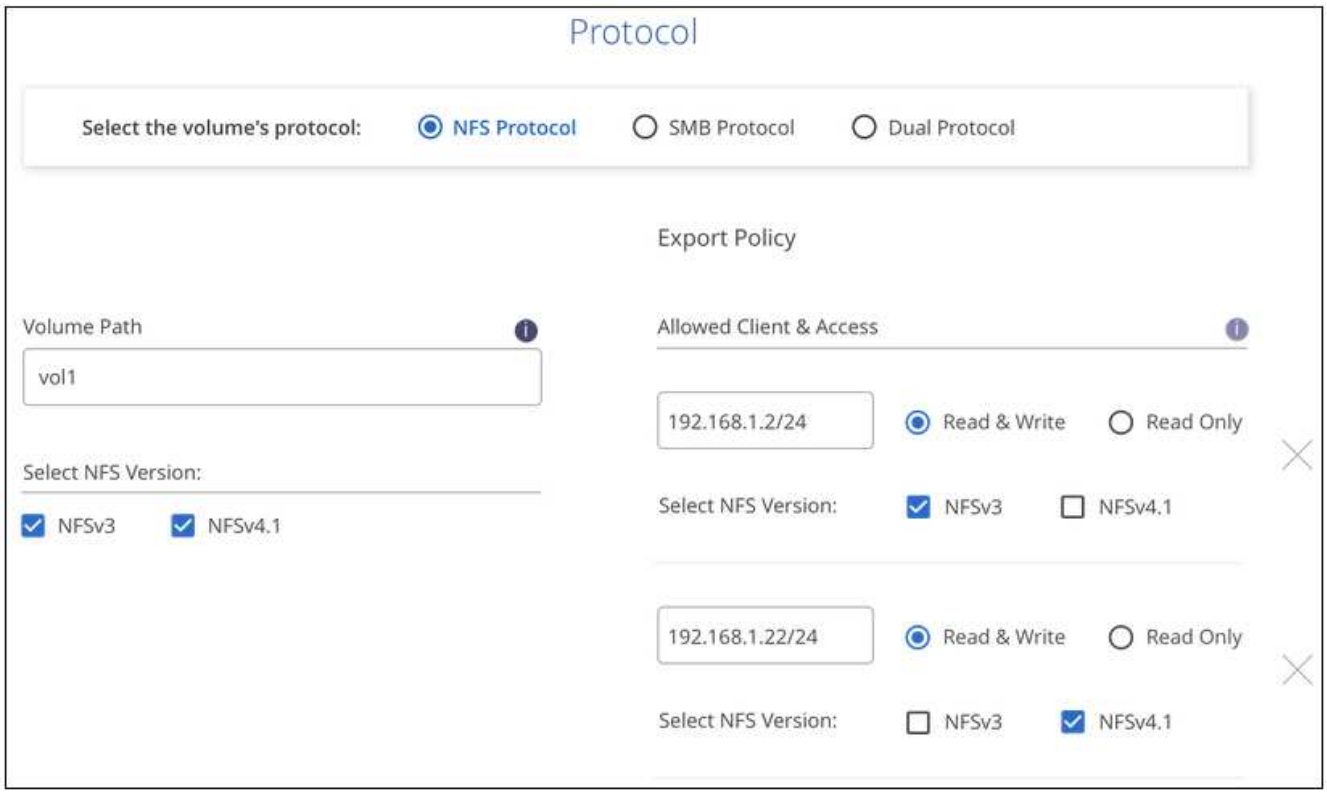


5. En la página Protocol, seleccione NFS, SMB o Dual Protocol y, a continuación, defina los detalles. Las entradas necesarias para NFS y SMB se muestran en secciones independientes a continuación.
6. En el campo Volume Path, especifique el nombre de la exportación de volumen que se verá cuando monte el volumen.
7. Si selecciona Protocolo dual, puede seleccionar el estilo de seguridad seleccionando NTFS o UNIX. Los estilos de seguridad afectan al tipo de permiso de archivo utilizado y cómo se pueden modificar los permisos.
   - UNIX utiliza bits del modo NFSv3 y solo los clientes NFS pueden modificar los permisos.
   - NTFS usa ACL de NTFS, y solo los clientes SMB pueden modificar los permisos.
8. Para NFS:

   a. En el campo NFS Version, seleccione NFSv3, NFSv4.1 o ambos en función de sus requisitos.

   b. De manera opcional, puede crear una política de exportación para identificar los clientes que pueden acceder al volumen. Especifique:
      - Clientes permitidos mediante una dirección IP o enrutamiento entre dominios sin clase (CIDR).
      - Derechos de acceso como sólo lectura y escritura o lectura.
      - Protocolo de acceso (o protocolos si el volumen permite el acceso NFSv3 y NFSv4.1) utilizado para los usuarios.
      - Haga clic en **+ Agregar regla de directiva de exportación** si desea definir reglas de política de exportación adicionales.

        En la siguiente imagen, se muestra la página Volume rellenada para el protocolo NFS:



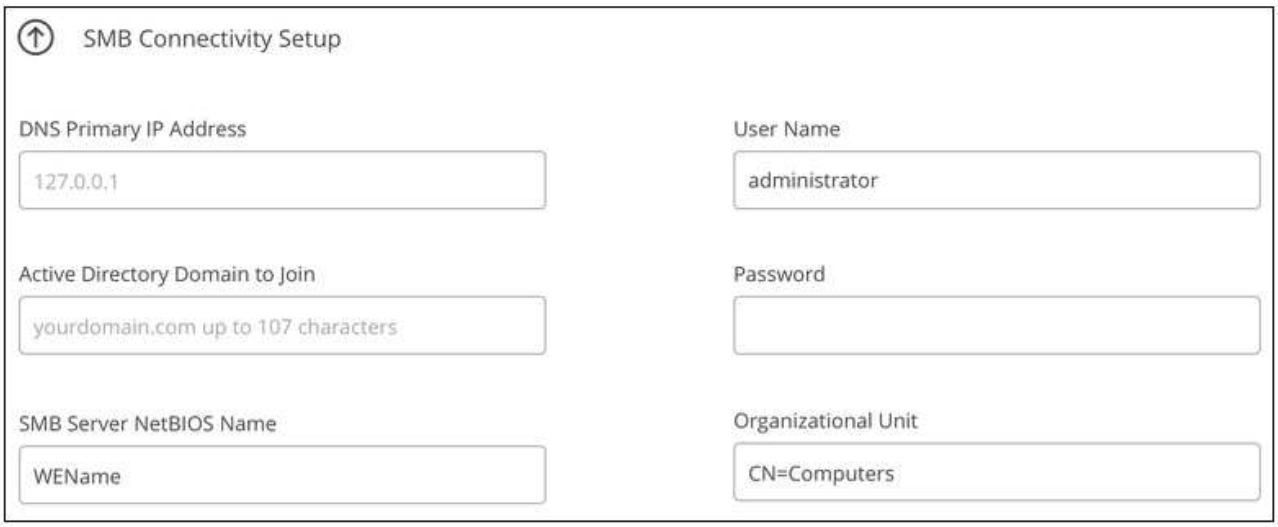
9. Para SMB:

   a. Puede habilitar el cifrado de sesión SMB marcando la casilla de cifrado de protocolo SMB.

   b. Puede integrar el volumen con un servidor de Windows Active Directory existente completando los campos de la sección Active Directory:

Campo	Descripción
Dirección IP primaria DNS	Las direcciones IP de los servidores DNS que proporcionan resolución de nombres para el servidor SMB. Utilice una coma para separar las direcciones IP cuando haga referencia a varios servidores, por ejemplo, 172.31.25.223, 172.31.2.74.
Dominio de Active Directory al que unirse	El FQDN del dominio de Active Directory (AD) al que desea que se una el servidor SMB. Cuando se utilice Microsoft AD gestionado por AWS, utilice el valor del campo "Nombre DNS de directorio".
Nombre NetBIOS del servidor SMB	Nombre NetBIOS para el servidor SMB que se va a crear.
Credenciales autorizadas para unirse al dominio	Nombre y contraseña de una cuenta de Windows con privilegios suficientes para agregar equipos a la unidad organizativa (OU) especificada dentro del dominio AD.
Unidad organizacional	La unidad organizativa del dominio AD para asociarla con el servidor SMB. El valor predeterminado es CN=equipos para las conexiones con su propio servidor de Windows Active Directory. Si configura Microsoft AD administrado de AWS como el servidor AD para Cloud Volumes Service, debe introducir **OU=equipos,OU=corp** en este campo.

   En la siguiente imagen, se muestra la página volumen llena para el protocolo SMB:



Debe seguir las directrices sobre la configuración del grupo de seguridad de AWS para habilitar volúmenes de cloud para que se integren correctamente con los servidores de Windows Active Directory. Consulte "Configuración del grupo de seguridad de AWS para servidores Windows AD" si quiere más información.

10. En la página Volume from Snapshot, si desea que este volumen se cree según una copia de Snapshot de un volumen existente, seleccione la copia de Snapshot en la lista desplegable Snapshot Name.
11. En la página Snapshot Policy, puede habilitar Cloud Volumes Service para crear copias Snapshot de los volúmenes según una programación. Puede hacer esto ahora o editar el volumen más tarde para definir la política de Snapshot.

    Consulte "Crear una política de Snapshot" para obtener más información sobre la funcionalidad snapshot.

12. Haga clic en **Añadir volumen**.

El nuevo volumen se agrega al entorno de trabajo.

Después de terminar

Si este es el primer volumen creado en esta suscripción a AWS, debe iniciar la consola de gestión de AWS para aceptar la interfaz virtual que se usará en esta región de AWS para conectar todos sus volúmenes de cloud. Consulte "Guía de configuración de la cuenta de Cloud Volumes Service para AWS de NetApp" para obtener más detalles.

Debe aceptar las interfaces en un plazo de 10 minutos después de hacer clic en el botón **Añadir volumen** o puede que se agote el tiempo de espera del sistema. Si esto sucede, envíe un correo electrónico a cvs-support@netapp.com con su ID de cliente de AWS y el número de serie de NetApp. El equipo de soporte solucionará el problema y puede reiniciar el proceso de incorporación.

A continuación, continúe con "Montaje del volumen de cloud".

Monte el volumen de cloud

Es posible montar un volumen de cloud en la instancia de AWS. Cloud Volumes admite actualmente NFSv3 y NFSv4.1 para clientes de Linux y UNIX, y SMB 3.0 y 3.1.1 para clientes de Windows.

Nota: por favor use el protocolo/dialecto resaltado soportado por su cliente.

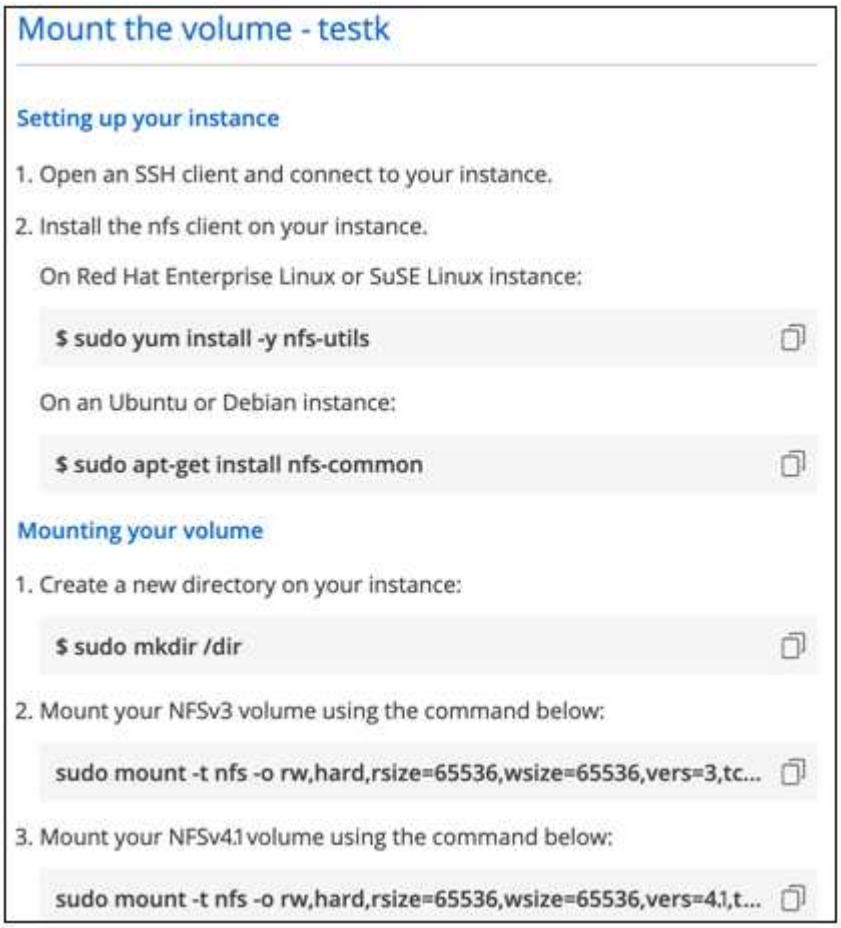
Pasos

1. Abra el entorno de trabajo.
2. Pase el ratón sobre el volumen y haga clic en **montar el volumen**.

   Los volúmenes NFS y SMB muestran instrucciones de montaje para ese protocolo. Los volúmenes de protocolo doble proporcionan ambos conjuntos de instrucciones.

3. Pase el ratón sobre los comandos y cópielos en el portapapeles para simplificar este proceso. Solo tiene que agregar el directorio de destino/punto de montaje al final del comando.

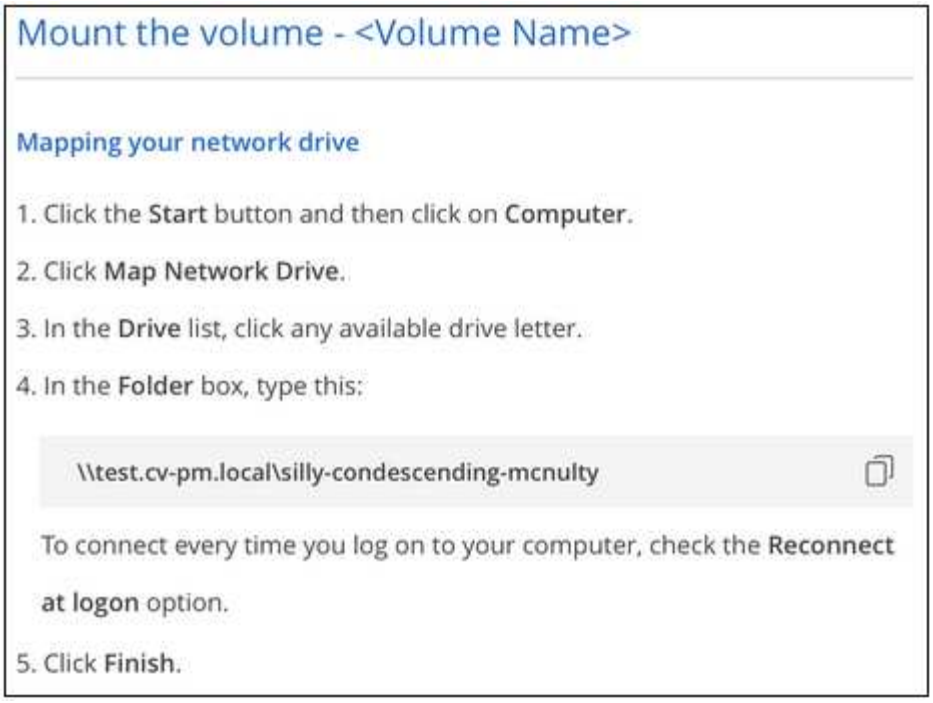
   ejemplo de NFS:



   El tamaño máximo de I/o definido por la `rsize` y.. `wsize` options es 1048576, sin embargo 65536 es el valor predeterminado recomendado para la mayoría de los casos de uso.

   Tenga en cuenta que los clientes de Linux tendrán NFSv4.1 de manera predeterminada a menos que se especifique la versión con `vers=<nfs_version>` opción.

   ejemplo SMB:



4. Conéctese a su instancia de Amazon Elastic Compute Cloud (EC2) mediante un cliente SSH o RDP y, a continuación, siga las instrucciones de montaje de su instancia.

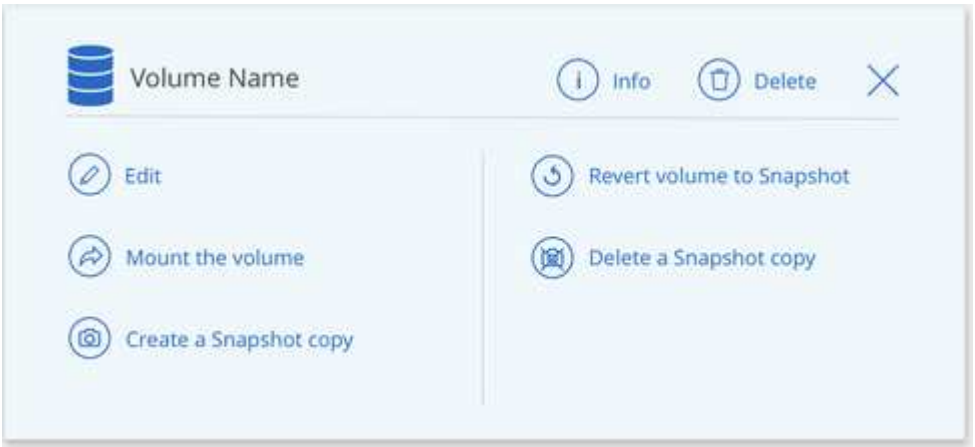
   Después de completar los pasos de las instrucciones de montaje, debe haber montado correctamente el volumen de cloud en la instancia de AWS.

Gestión de los volúmenes existentes

Puede gestionar los volúmenes existentes a medida que cambien sus necesidades de almacenamiento. Es posible ver, editar, restaurar y eliminar volúmenes.

Pasos

1. Abra el entorno de trabajo.
2. Pase el ratón sobre el volumen.



3. Gestione sus volúmenes:

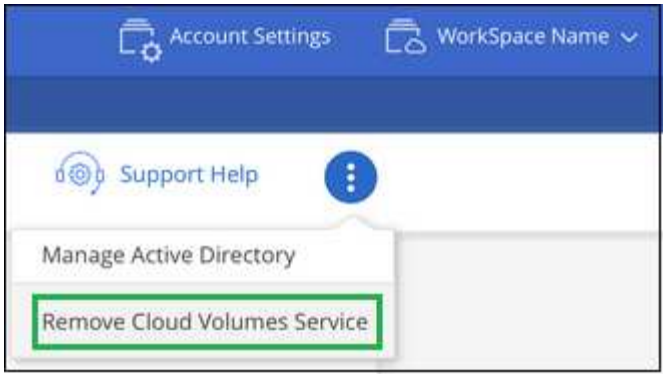
Tarea	Acción
Permite ver la información de un volumen	Seleccione un volumen y, a continuación, haga clic en **Info**.
Editar un volumen (incluida la política de Snapshot)	a. Seleccione un volumen y, a continuación, haga clic en **Editar**. b. Modifique las propiedades del volumen y haga clic en **Actualizar**.
Obtenga el comando de montaje NFS o SMB	a. Seleccione un volumen y, a continuación, haga clic en **montar el volumen**. b. Haga clic en **Copiar** para copiar los comandos.
Cree una copia Snapshot bajo demanda	a. Seleccione un volumen y, a continuación, haga clic en **Crear una copia Snapshot**. b. Si es necesario, cambie el nombre de la instantánea y, a continuación, haga clic en **Crear**.
Reemplace el volumen por el contenido de una copia Snapshot	a. Seleccione un volumen y, a continuación, haga clic en **revertir volumen a Snapshot**. b. Seleccione una copia Snapshot y haga clic en **revertir**.
Eliminar una copia Snapshot	a. Seleccione un volumen y, a continuación, haga clic en **Eliminar una copia Snapshot**. b. Seleccione la copia Snapshot que desea eliminar y haga clic en **Eliminar**. c. Vuelva a hacer clic en **Eliminar** para confirmar.
Eliminar un volumen	a. Desmonte el volumen de todos los clientes: ◦ En los clientes Linux, utilice `umount` comando. ◦ En clientes Windows, haga clic en **desconectar unidad de red**. b. Seleccione un volumen y, a continuación, haga clic en **Eliminar**. c. Vuelva a hacer clic en **Eliminar** para confirmar.

Quite Cloud Volumes Service de Cloud Manager

Puede eliminar una suscripción a Cloud Volumes Service para AWS y todos los volúmenes existentes de Cloud Manager. Los volúmenes no se eliminan; se acaban de quitar de la interfaz de Cloud Manager.

Pasos

1. Abra el entorno de trabajo.



2. Haga clic en la En la parte superior de la página y haga clic en **Quitar Cloud Volumes Service**.
3. En el cuadro de diálogo de confirmación, haga clic en **Quitar**.

Administrar la configuración de Active Directory

Si cambia sus servidores DNS o dominio de Active Directory, debe modificar el servidor SMB en Cloud Volumes Services para poder seguir sirviendo almacenamiento a los clientes.

También puede eliminar el vínculo a un Active Directory si ya no lo necesita.

Pasos

1. Abra el entorno de trabajo.
2. Haga clic en la En la parte superior de la página y haga clic en **Administrar Active Directory**.
3. Si no se ha configurado Active Directory, puede agregar uno ahora. Si se ha configurado uno, puede modificar los ajustes o eliminarlos utilizando botón.
4. Especifique la configuración de Active Directory a la que desea unirse:

Campo	Descripción
Dirección IP primaria DNS	Las direcciones IP de los servidores DNS que proporcionan resolución de nombres para el servidor SMB. Utilice comas para separar las direcciones IP al hacer referencia a varios servidores, por ejemplo, 172.31.25.223, 172.31.2.74.
Dominio de Active Directory al que unirse	El FQDN del dominio de Active Directory (AD) al que desea que se una el servidor SMB. Cuando se utilice Microsoft AD gestionado por AWS, utilice el valor del campo "Nombre DNS de directorio".
Nombre NetBIOS del servidor SMB	Nombre NetBIOS para el servidor SMB que se va a crear.
Credenciales autorizadas para unirse al dominio	Nombre y contraseña de una cuenta de Windows con privilegios suficientes para agregar equipos a la unidad organizativa (OU) especificada dentro del dominio AD.
Unidad organizacional	La unidad organizativa del dominio AD para asociarla con el servidor SMB. El valor predeterminado es CN=equipos para las conexiones con su propio servidor de Windows Active Directory. Si configura Microsoft AD administrado de AWS como el servidor AD para Cloud Volumes Service, debe introducir **OU=equipos,OU=corp** en este campo.

5. Haga clic en **Guardar** para guardar la configuración.

Permite gestionar snapshots de Cloud Volumes

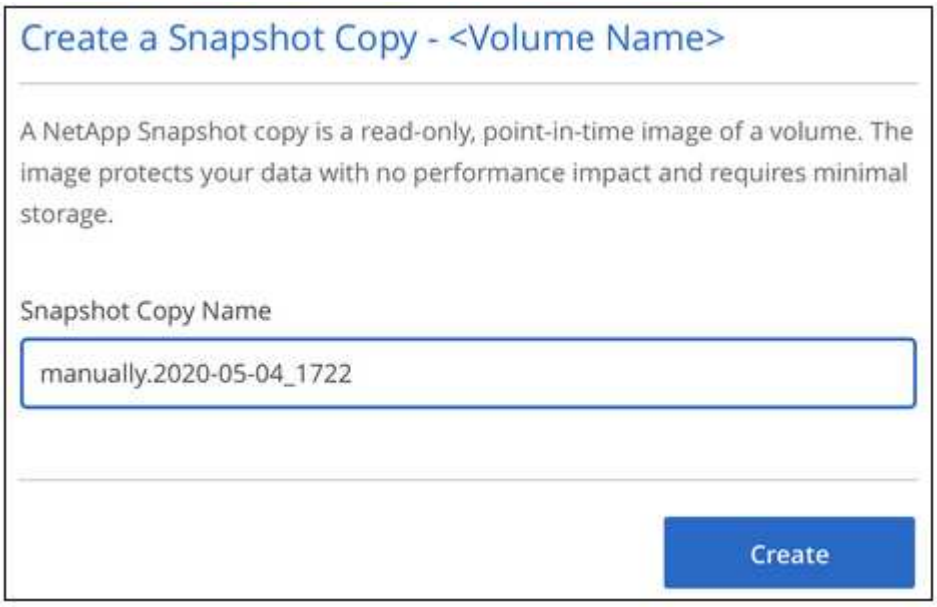
Es posible crear una política de Snapshot para cada volumen para recuperar o restaurar todo el contenido de un volumen desde un momento anterior. También puede crear una snapshot bajo demanda de un volumen de cloud cuando sea necesario.

Crear una snapshot bajo demanda

Es posible crear una copia de Snapshot bajo demanda de un volumen de cloud para crear una copia de Snapshot con el estado actual del volumen.

Pasos

1. Abra el entorno de trabajo.
2. Pase el ratón sobre el volumen y haga clic en **Crear una copia de instantánea**.
3. Introduzca un nombre para la instantánea o utilice el nombre generado automáticamente y haga clic en **Crear**.



Crear o modificar una política de Snapshot

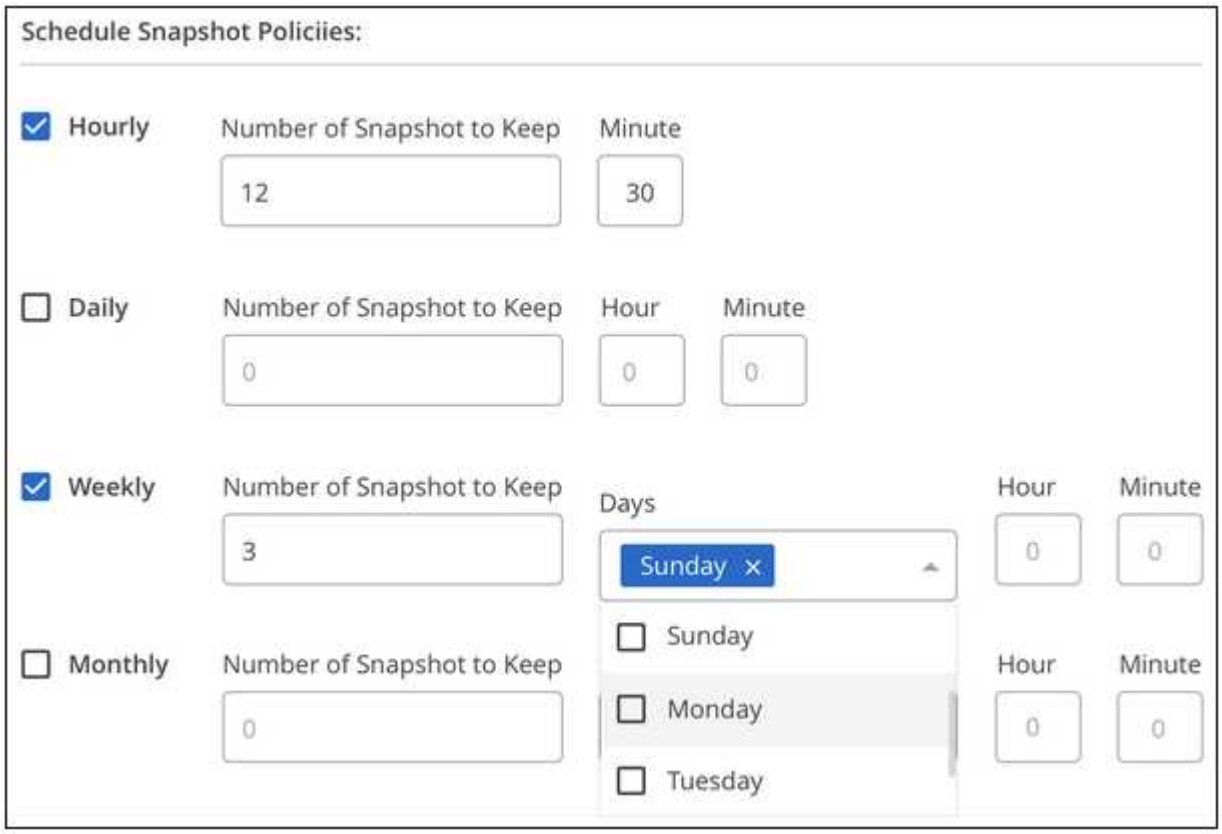
Es posible crear o modificar una política de Snapshot según sea necesario para un volumen de cloud. La política de Snapshot se define en la pestaña *Snapshot Policy* al crear un volumen o al editar un volumen.

Pasos

1. Abra el entorno de trabajo.
2. Pase el ratón sobre el volumen y haga clic en **Editar**.
3. En la ficha *Snapshot Policy*, mueva el control deslizante Habilitar instantáneas a la derecha.
4. Defina la programación para las Snapshot:
   a. Seleccione la frecuencia: **Hourly**, **Daily**, **Weekly** o **Monthly**

b. Seleccione el número de snapshots que desea conservar.

c. Seleccione el día, la hora y los minutos en que se debe realizar la copia de Snapshot.



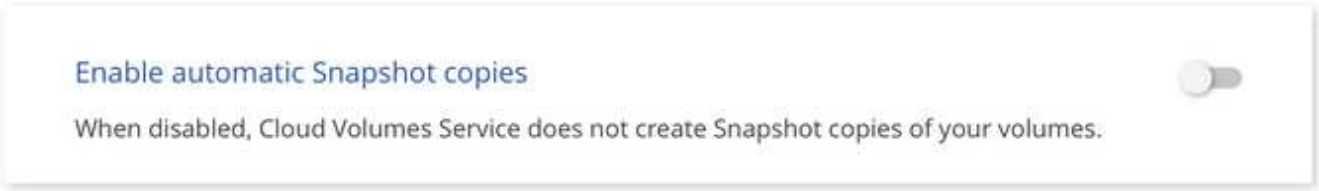
5. Haga clic en **Añadir volumen** o **Actualizar volumen** para guardar la configuración de la directiva.

Deshabilitar una política de Snapshot

Puede deshabilitar una política de Snapshot para detener la creación de copias Snapshot durante un breve período de tiempo mientras se conserva la configuración de la política de Snapshot.

Pasos

1. Abra el entorno de trabajo.
2. Pase el ratón sobre el volumen y haga clic en **Editar**.
3. En la ficha *Snapshot Policy*, mueva el control deslizante Habilitar instantáneas a la izquierda.



4. Haga clic en **Actualizar volumen**.

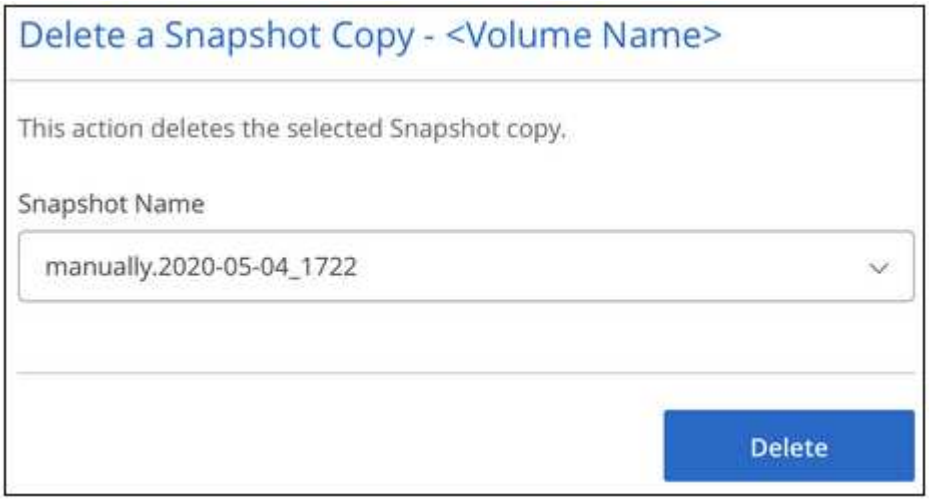
Si desea volver a activar la directiva de instantáneas, mueva el control deslizante Activar instantáneas a la derecha y haga clic en **Actualizar volumen**.

Eliminar una copia de Snapshot

Las snapshots se pueden eliminar de la página Volumes.

Pasos

1. Abra el entorno de trabajo.
2. Pase el ratón sobre el volumen y haga clic en **Eliminar una copia Snapshot**.
3. Seleccione la instantánea en la lista desplegable y haga clic en **Eliminar**.



4. En el cuadro de diálogo de confirmación, haga clic en **Eliminar**.

Revertir un volumen a partir de una copia de Snapshot

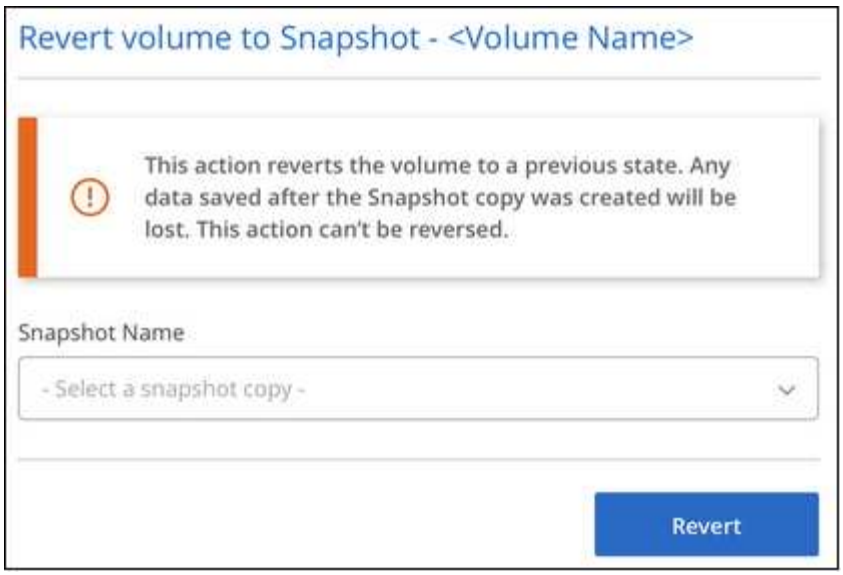
Es posible revertir un volumen a un momento específico anterior desde una snapshot existente.

Si se revierte un volumen, el contenido de la copia Snapshot sobrescribe la configuración de volumen existente. Se pierden todos los cambios que se realizaron en los datos del volumen después de la creación de la copia de Snapshot.

Tenga en cuenta que los clientes no necesitan volver a montar el volumen después de la operación de reversión.

Pasos

1. Abra el entorno de trabajo.
2. Pase el ratón sobre el volumen y haga clic en **revertir volumen a Snapshot**.
3. Seleccione la instantánea que desea utilizar para restaurar el volumen existente de la lista desplegable y haga clic en **revertir**.



Referencia

Los niveles de servicio y la capacidad asignada

El coste de Cloud Volumes Service para AWS se basa en el *nivel de servicio* y en el *capacidad asignada* que seleccione. Al seleccionar el nivel de servicio y la capacidad adecuados, podrá satisfacer sus necesidades de almacenamiento con el menor coste.

Consideraciones

Entre las necesidades de almacenamiento se encuentran dos aspectos fundamentales:

- El almacenamiento *Capacity* para retener datos
- El *Bandwidth* de almacenamiento para interactuar con datos

Si consume más espacio de almacenamiento que la capacidad seleccionada para el volumen, se deben tener en cuenta las siguientes consideraciones:

- Se le facturará la capacidad de almacenamiento adicional que use con el precio definido por su nivel de servicio.
- La cantidad de ancho de banda de almacenamiento disponible para el volumen no aumenta hasta que aumenta el tamaño de capacidad asignada o cambia el nivel de servicio.

Niveles de servicio

Cloud Volumes Service para AWS ofrece soporte a tres niveles de servicio. Debe especificar el nivel de servicio al crear o modificar el volumen.

Los niveles de servicio se ofrecen para distintas necesidades de capacidad de almacenamiento y ancho de banda de almacenamiento:

- **Estándar** (capacidad)

  Si desea capacidad con el menor costo y sus necesidades de ancho de banda son limitadas, el nivel de servicio estándar puede ser más adecuado para usted. Un ejemplo es el uso del volumen como destino de

backup.

    - Ancho de banda: 16 KB de ancho de banda por GB de capacidad aprovisionada

- **Premium** (un equilibrio entre capacidad y rendimiento)

  Si su aplicación tiene una necesidad equilibrada de capacidad de almacenamiento y ancho de banda, puede que el nivel de servicio Premium sea el más adecuado. Este nivel es menos costoso por MB/s que el nivel de servicio estándar, y también resulta más económico por GB de capacidad de almacenamiento que el nivel de servicio extremo.

    - Ancho de banda: 64 KB de ancho de banda por GB de capacidad aprovisionada

- **Extreme** (rendimiento)

  El nivel de servicio extremo es menos costoso en términos de ancho de banda de almacenamiento. Si su aplicación requiere ancho de banda de almacenamiento sin la demanda asociada de mucha capacidad de almacenamiento, puede que el nivel de servicio extremo sea más adecuado para usted.

    - Ancho de banda: 128 KB de ancho de banda por GB de capacidad aprovisionada

Capacidad asignada

Debe especificar la capacidad asignada para el volumen cuando cree o modifique el volumen.

Si bien debe seleccionar su nivel de servicio en función de sus necesidades empresariales generales de alto nivel, debe seleccionar su tamaño de capacidad asignada en función de las necesidades específicas de las aplicaciones, por ejemplo:

- Cantidad de espacio de almacenamiento que necesitan las aplicaciones
- ¿Cuánto ancho de banda del almacenamiento por segundo que requieren las aplicaciones o las los usuarios lo necesitan

La capacidad asignada se especifica en GBS. La capacidad asignada de un volumen se puede establecer entre 100 GB y 100,000 GB (equivalente a 100 TB).

Número de inodos

Volúmenes inferiores o iguales a 1 TB pueden usar hasta 20 millones de inodos. El número de inodos aumenta en 20 millones por cada TB que asigne, hasta un máximo de 100 millones de inodos.

- <= 1 TB = 20 millones de inodos
- >1 TB a 2 TB = 40 millones de inodos
- >2 TB a 3 TB = 60 millones de inodos
- >3 TB a 4 TB = 80 millones de inodos
- >4 TB a 100 TB = 100 millones de inodos

Ancho de banda

La combinación de tanto el nivel de servicio como la capacidad asignada que seleccione determina el ancho de banda máximo del volumen.

Si sus aplicaciones o usuarios necesitan más ancho de banda que las selecciones, puede cambiar el nivel de servicio o aumentar la capacidad asignada. Los cambios no interrumpen el acceso a los datos.

Selección del nivel de servicio y la capacidad asignada

Para seleccionar el nivel de servicio y la capacidad asignada que más se correspondan con sus necesidades, debe saber la capacidad y el ancho de banda que necesita en el extremo o en la periferia.

Lista de niveles de servicio y capacidad asignada

La columna situada más a la izquierda indica la capacidad y las demás columnas definen los MB/s disponibles en cada punto de capacidad en función del nivel de servicio.

Consulte "Precio de suscripción por contrato" y.. "Tarificación por suscripciones" para obtener información completa sobre los precios.

Capacidad (TB)	Estándar (MB/s)	Premium (MB/s)	Extremo (MB/s)
0.1 (100 GB)	1.6	6.4	12.8
1	16	64	128
2	32	128	256
3	48	192	384
4	64	256	512
5	80	320	640
6	96	384	768
7	112	448	896
8	128	512	1,024
9	144	576	1,152
10	160	640	1,280
11	176	704	1,408
12	192	768	1,536
13	208	832	1,664
14	224	896	1,792
15	240	960	1,920
16	256	1,024	2,048
17	272	1,088	2,176
18	288	1,152	2,304
19	304	1,216	2,432
20	320	1,280	2,560
21	336	1,344	2,688
22	352	1,408	2,816
23	368	1,472	2,944
24	384	1,536	3,072

Capacidad (TB)	Estándar (MB/s)	Premium (MB/s)	Extremo (MB/s)
25	400	1,600	3,200
26	416	1,664	3,328
27	432	1,728	3,456
28	448	1,792	3,584
29	464	1,856	3,712
30	480	1,920	3,840
31	496	1,984	3,968
32	512	2,048	4,096
33	528	2,112	4,224
34	544	2,176	4,352
35	560	2,240	4,480
36	576	2,304	4,500
37	592	2,368	4,500
38	608	2,432	4,500
39	624	2,496	4,500
40	640	2,560	4,500
41	656	2,624	4,500
42	672	2,688	4,500
43	688	2,752	4,500
44	704	2,816	4,500
45	720	2,880	4,500
46	736	2,944	4,500
47	752	3,008	4,500
48	768	3,072	4,500
49	784	3,136	4,500
50	800	3,200	4,500
51	816	3,264	4,500
52	832	3,328	4,500
53	848	3,392	4,500
54	864	3,456	4,500
55	880	3,520	4,500
56	896	3,584	4,500
57	912	3,648	4,500

Capacidad (TB)	Estándar (MB/s)	Premium (MB/s)	Extremo (MB/s)
58	928	3,712	4,500
59	944	3,776	4,500
60	960	3,840	4,500
61	976	3,904	4,500
62	992	3,968	4,500
63	1,008	4,032	4,500
64	1,024	4,096	4,500
65	1,040	4,160	4,500
66	1,056	4,224	4,500
67	1,072	4,288	4,500
68	1,088	4,352	4,500
69	1,104	4,416	4,500
70	1,120	4,480	4,500
71	1,136	4,500	4,500
72	1,152	4,500	4,500
73	1,168	4,500	4,500
74	1,184	4,500	4,500
75	1,200	4,500	4,500
76	1,216	4,500	4,500
77	1,232	4,500	4,500
78	1,248	4,500	4,500
79	1,264	4,500	4,500
80	1,280	4,500	4,500
81	1,296	4,500	4,500
82	1,312	4,500	4,500
83	1,328	4,500	4,500
84	1,344	4,500	4,500
85	1,360	4,500	4,500
86	1,376	4,500	4,500
87	1,392	4,500	4,500
88	1,408	4,500	4,500
89	1,424	4,500	4,500
90	1,440	4,500	4,500

Capacidad (TB)	Estándar (MB/s)	Premium (MB/s)	Extremo (MB/s)
91	1,456	4,500	4,500
92	1,472	4,500	4,500
93	1,488	4,500	4,500
94	1,504	4,500	4,500
95	1,520	4,500	4,500
96	1,536	4,500	4,500
97	1,552	4,500	4,500
98	1,568	4,500	4,500
99	1,584	4,500	4,500
100	1,600	4,500	4,500

Ejemplo 1

Por ejemplo, su aplicación requiere 25 TB de capacidad y 100 MB/s de ancho de banda. Con 25 TB de capacidad, el nivel de servicio estándar proporcionaría 400 MB/s de ancho de banda a un coste de 2,500 $ (estimación: Ver precio actual), lo que convierte a Standard en el nivel de servicio más adecuado en este caso.

	Standard		Premium		Extreme	
capacity	Bandwidth		Bandwidth		Bandwidth	
TB	MB/s	Cost	MB/s	Cost	MB/s	Cost
24	384	$2,400	1,536	$4,800	3,072	$7,200
25	400	$2,500	1,600	$5,000	3,200	$7,500
26	416	$2,600	1,664	$5,200	3,328	$7,800

Ejemplo 2

Por ejemplo, su aplicación requiere 12 TB de capacidad y 800 MB/s de ancho de banda máximo. Aunque el nivel de servicio extremo puede satisfacer las demandas de la aplicación con el objetivo de 12 TB, es más rentable (estimación: Consulte los precios actuales) seleccionar 13 TB en el nivel de servicio Premium.

	Standard		Premium		Extreme	
capacity	Bandwidth		Bandwidth		Bandwidth	
TB	MB/s	Cost	MB/s	Cost	MB/s	Cost
12	192	$1,200	768	$2,400	1,536	$3,600
13	208	$1,300	832	$2,600	1,664	$3,900
14	224	$1,400	896	$2,800	1,792	$4,200

Configuración del grupo de seguridad de AWS para servidores Windows AD

Si utiliza servidores de Windows Active Directory (AD) con volúmenes de cloud, debe familiarizarse con la guía de la configuración del grupo de seguridad de AWS. Los

ajustes permiten que los volúmenes de cloud se integren correctamente con AD.

De forma predeterminada, el grupo de seguridad de AWS aplicado a una instancia de EC2 Windows no contiene reglas entrantes para ningún protocolo excepto RDP. Debe agregar reglas a los grupos de seguridad asociados a cada instancia de Windows AD para habilitar la comunicación entrante desde Cloud Volumes Service. Los puertos necesarios son los siguientes:

Servicio	Puerto	Protocolo
Servicios web DE ANUNCIOS	9389	TCP
DNS	53	TCP
DNS	53	UDP
ICMPv4	N.A.	Respuesta de eco
Kerberos	464	TCP
Kerberos	464	UDP
Kerberos	88	TCP
Kerberos	88	UDP
LDAP	389	TCP
LDAP	389	UDP
LDAP	3268	TCP
Nombre NetBIOS	138	UDP
SAM/LSA	445	TCP
SAM/LSA	445	UDP
LDAP seguro	636	TCP
LDAP seguro	3269	TCP
w32time	123	UDP

Si va a implementar y administrar los controladores de dominio de instalación de AD y los servidores miembro en una instancia de AWS EC2, necesitará varias reglas de grupo de seguridad para permitir el tráfico de Cloud Volumes Service. A continuación se muestra un ejemplo de cómo implementar estas reglas para aplicaciones AD como parte de la plantilla AWS CloudFormation.

```
{
    "AWSTemplateFormatVersion" : "2010-09-09",
    "Description" : "Security Group for AD",
    "Parameters" :
    {
        "VPC" :
        {
            "Type" : "AWS::EC2::VPC::Id",
            "Description" : "VPC where the Security Group will belong:"
        },
```

```
        "Name" :
        {
            "Type" : "String",
            "Description" : "Name Tag of the Security Group:"
        },
        "Description" :
        {
            "Type" : "String",
            "Description" : "Description Tag of the Security Group:",
            "Default" : "Security Group for Active Directory for CVS "
        },
        "CIDRrangeforTCPandUDP" :
        {
            "Type" : "String",
            "Description" : "CIDR Range for the UDP ports
445,138,464,389,53,123 and for the TCP ports
464,339,3389,3268,88,636,9389,445 and 0-65535: *CIDR range format:
10.0.0.0/24"
        }
    },
    "Resources" :
    {
        "ADSGWest" :
        {
            "Type" : "AWS::EC2::SecurityGroup",
            "Properties" :
            {
                "GroupDescription" : {"Ref" : "Description"},
                "VpcId" : { "Ref" : "VPC" },
                "SecurityGroupIngress" : [
                    {
                        "IpProtocol" : "udp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "445",
                        "ToPort" : "445"
                    },
                    {
                        "IpProtocol" : "udp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "138",
                        "ToPort" : "138"
                    },
                    {
                        "IpProtocol" : "udp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "464",
```

```
                    "ToPort" : "464"
                },
                {
                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "464",
                    "ToPort" : "464"
                },
                {
                    "IpProtocol" : "udp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "389",
                    "ToPort" : "389"
                },
                {
                    "IpProtocol" : "udp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "53",
                    "ToPort" : "53"
                },
                {
                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "339",
                    "ToPort" : "339"
                },
                {
                    "IpProtocol" : "udp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "123",
                    "ToPort" : "123"
                },
                {
                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "3389",
                    "ToPort" : "3389"
                },
                {
                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "3268",
                    "ToPort" : "3268"
                },
                {
                    "IpProtocol" : "tcp",
```

```
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "88",
                        "ToPort" : "88"
                    },
                    {
                        "IpProtocol" : "tcp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "636",
                        "ToPort" : "636"
                    },
                    {
                        "IpProtocol" : "tcp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "3269",
                        "ToPort" : "3269"
                    },
                    {
                        "IpProtocol" : "tcp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "53",
                        "ToPort" : "53"
                    },
                    {
                        "IpProtocol" : "tcp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "0",
                        "ToPort" : "65535"
                    },
                    {
                        "IpProtocol" : "tcp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "9389",
                        "ToPort" : "9389"
                    },
                    {
                        "IpProtocol" : "tcp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "445",
                        "ToPort" : "445"
                    }
                ]
            }
        }
    },
    "Outputs" :
    {
```

```
        "SecurityGroupID" :
        {
            "Description" : "Security Group ID",
            "Value" : { "Ref" : "ADSGWest" }
        }
    }
}
```

Cloud Volumes Service para GCP

Más información sobre Cloud Volumes Service para Google Cloud

Cloud Volumes Service de NetApp para Google Cloud le permite agregar rápidamente cargas de trabajo multiprotocolo, así como crear y poner en marcha aplicaciones basadas en Windows y UNIX.

Características principales:

- Migre datos entre sus instalaciones y Google Cloud.
- Aprovisione volúmenes de 1 a 100 TIB en segundos.
- Compatibilidad con varios protocolos (puede crear un volumen NFS o SMB).
- Proteja los datos con copias snapshot eficientes y automatizadas.
- Acelere el desarrollo de aplicaciones con un clonado rápido.

Coste

Los volúmenes creados por Cloud Volumes Service para Google Cloud se cobran a su suscripción al servicio, no a través de Cloud Manager.

"Ver precios"

Cloud Manager no tiene ningún coste para descubrir una región o volumen de Cloud Volumes Service para Google Cloud.

Regiones admitidas

"Consulte las regiones de Google Cloud admitidas."

Antes de empezar

Cloud Manager puede descubrir las suscripciones y volúmenes existentes de Cloud Volumes Service para GCP. Consulte "Documentación de NetApp Cloud Volumes Service para Google Cloud" si aún no ha configurado su suscripción.

Obtener ayuda

Use el chat de Cloud Manager para preguntas generales acerca del funcionamiento de Cloud Volumes Service en Cloud Manager.

Si tiene alguna pregunta general sobre Cloud Volumes Service para Google Cloud, envíe un correo electrónico al equipo de Google Cloud de NetApp en gcinfo@netapp.com.

En el caso de los problemas técnicos asociados con sus volúmenes de cloud, puede crear un caso de soporte técnico desde la consola de Google Cloud. Consulte "obtención de soporte" para obtener más detalles.

Limitaciones

- Cloud Manager no admite la replicación de datos entre entornos de trabajo al usar volúmenes de Cloud Volumes Service.
- No se admite la eliminación de su suscripción a Cloud Volumes Service para Google Cloud de Cloud Manager. Solo puede hacerlo a través de la consola de Google Cloud.

Enlaces relacionados

- "NetApp Cloud Central: Cloud Volumes Service para Google Cloud"
- "Documentación de NetApp Cloud Volumes Service para Google Cloud"

Configure Cloud Volumes Service para Google Cloud

Cree un entorno de trabajo de Cloud Volumes Service para Google Cloud en Cloud Manager para crear y gestionar volúmenes y snapshots.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o vaya a la siguiente sección para obtener toda la información.

Habilite la API de Cloud Volumes Service

En Google, habilite la API de Cloud Volumes Service para GCP para que Cloud Manager pueda gestionar la suscripción y los volúmenes de cloud.

Cree una cuenta de servicio de GCP y descargue las credenciales

Desde Google, cree una cuenta de servicio y una función de GCP para que Cloud Manager pueda acceder a su cuenta de Cloud Volumes Service para GCP.

Crear un entorno de trabajo de Cloud Volumes Service para GCP

En Cloud Manager, haga clic en **Agregar entorno de trabajo** > **Google Cloud** > **Cloud Volumes Service** y, a continuación, proporcione detalles sobre la cuenta de servicio y el proyecto de Google Cloud.

Habilite la API de Cloud Volumes Service

En Google Cloud Shell, ejecute el siguiente comando para habilitar la API de Cloud Volumes Service:

```
gcloud --project=<my-cvs-project> services enable cloudvolumesgcp-api.netapp.com
```

Dé acceso a Cloud Manager a Cloud Volumes Service for Cuenta para GCP

Debe completar las siguientes tareas para que Cloud Manager pueda acceder a su proyecto de Google Cloud:

- Cree una nueva cuenta de servicio
- Agregue el nuevo miembro de la cuenta de servicio al proyecto y. asignar roles específicos de ti (permisos)
- Cree y descargue un par de claves para la cuenta de servicio Que se utiliza para autenticar en Google

Pasos

1. En Google Cloud Console, vaya a la página **Cuentas de servicio**.
2. Haga clic en **Seleccionar un proyecto**, elija su proyecto y haga clic en **Abrir**.
3. Haga clic en **Crear cuenta de servicio**, introduzca el nombre de la cuenta de servicio (nombre descriptivo para mostrar) y la descripción, y haga clic en **Crear**.
4. En la página *IAM* haga clic en **Agregar** y rellene los campos de la página *Add Members*:
   a. En el campo nuevos miembros, introduzca el ID de cuenta de servicio completo, por ejemplo, user1-service-account-cvs@project1.iam.gserviceaccount.com.
   b. Añada estos roles:
      - *NetApp Cloud Volumes Admin*
      - *Visor de redes de computación*
      - *Visor de carpetas*
   c. Haga clic en **Guardar**.
5. En la página *Service account details* haga clic en **Agregar clave > Crear nueva clave**.
6. Seleccione **JSON** como el tipo de clave y haga clic en **Crear**.

   Al hacer clic en **Crear** se genera y descarga en el sistema su nuevo par de claves públicas/privadas. Sirve como la única copia de la clave privada. Almacene este archivo de forma segura porque puede utilizarse para autenticarse como cuenta de servicio.

Si desea conocer los pasos detallados, consulte los temas de Google Cloud "Crear y administrar cuentas de servicio", "Otorgar, cambiar y revocar el acceso a los recursos", y. "Crear y administrar claves de cuenta de servicio".

Crear un entorno de trabajo de Cloud Volumes Service para GCP

Configure un entorno de trabajo de Cloud Volumes Service para GCP en Cloud Manager para que pueda empezar a crear volúmenes.

Independientemente de si ya ha creado volúmenes desde Google Cloud Console, o si acaba de suscribirse a Cloud Volumes Service para GCP y no tiene aún volúmenes, el primer paso es crear un entorno laboral para los volúmenes basados en su suscripción para GCP.

Si Cloud Volumes ya existen para esta suscripción, los volúmenes aparecerán en el nuevo entorno de trabajo. Si todavía no ha añadido ningún volumen de cloud para la suscripción a GCP, podrá hacerlo después de crear el nuevo entorno de trabajo.

Si tiene suscripciones y volúmenes en varios proyectos de GCP, deberá realizar esta tarea para cada proyecto.

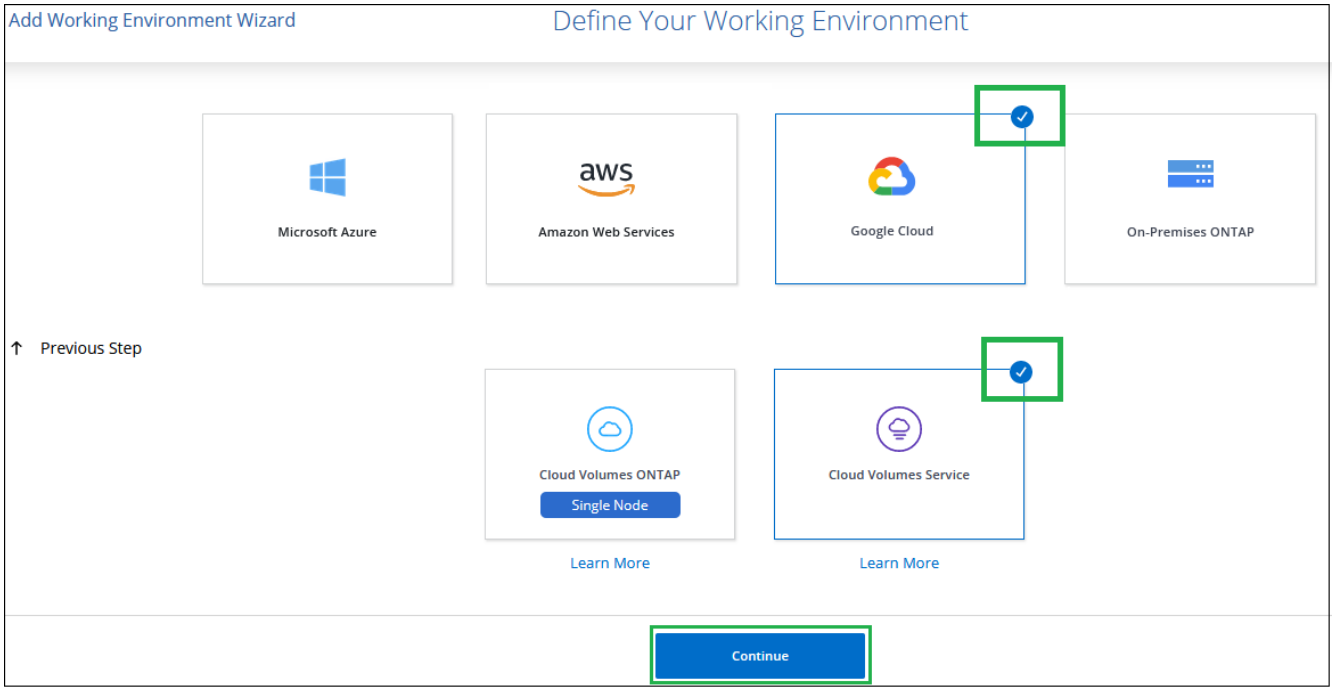
Antes de empezar

Debe disponer de la siguiente información al agregar una suscripción a cada proyecto:

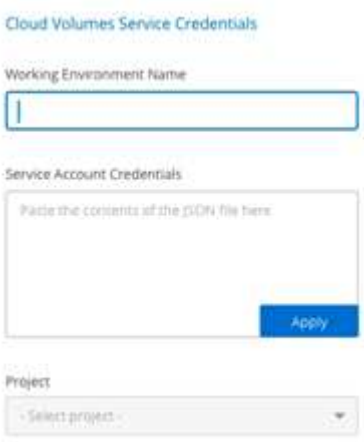
- Credenciales de cuenta de servicio (clave privada JSON que ha descargado)
- Nombre del proyecto

Pasos

1. En Cloud Manager, agregue un nuevo entorno de trabajo, seleccione la ubicación **Google Cloud** y haga clic en **continuar**.
2. Seleccione **Cloud Volumes Service** y haga clic en **continuar**.



3. Proporcione información sobre su suscripción a Cloud Volumes Service:
   a. Introduzca el nombre del entorno de trabajo que desee utilizar.
   b. Copie y pegue la clave privada JSON que ha descargado en los pasos anteriores.
   c. Seleccione el nombre de su proyecto de Google Cloud.
   d. Haga clic en **Agregar**.



Resultado

Cloud Manager muestra su entorno de trabajo de Cloud Volumes Service para Google Cloud.

Si Cloud Volumes ya existe para esta suscripción, los volúmenes aparecen en el nuevo entorno de trabajo, como se muestra en la captura de pantalla. Puede añadir volúmenes de cloud adicionales desde Cloud Manager.

Si no hay Cloud Volumes para esta suscripción, créelos ahora.

El futuro

"Comience a crear y gestionar volúmenes".

Cree y gestione volúmenes para Cloud Volumes Service para Google Cloud

Cloud Manager le permite crear volúmenes de cloud basados en su "Cloud Volumes Service para Google Cloud" suscripción. También puede editar ciertos atributos de un volumen, obtener los comandos de montaje pertinentes, crear copias Snapshot y eliminar volúmenes de cloud.

Cree Cloud Volumes

Puede crear NFS o volúmenes SMB en una cuenta nueva o existente de Cloud Volumes Service para Google Cloud. Cloud Volumes admite actualmente NFSv3 y NFSv4.1 para clientes de Linux y UNIX y SMB 3.x para clientes de Windows.

Antes de empezar

- Si desea utilizar SMB en GCP, debe haber configurado DNS y Active Directory.
- Cuando planee crear un volumen SMB, debe tener un servidor de Windows Active Directory disponible para el que se pueda conectar. Deberá introducir esta información al crear el volumen. Además, asegúrese de que el usuario Admin puede crear una cuenta de equipo en la ruta de la unidad organizativa (OU) especificada.

Pasos

1. Seleccione el entorno de trabajo y haga clic en **Añadir nuevo volumen**.
2. En la página Details & Location, introduzca detalles sobre el volumen:
   a. Escriba un nombre para el volumen.
   b. Especifique un tamaño dentro del intervalo de 1 TIB (1024 GIB) a 100 TIB.

      "Más información sobre la capacidad asignada".

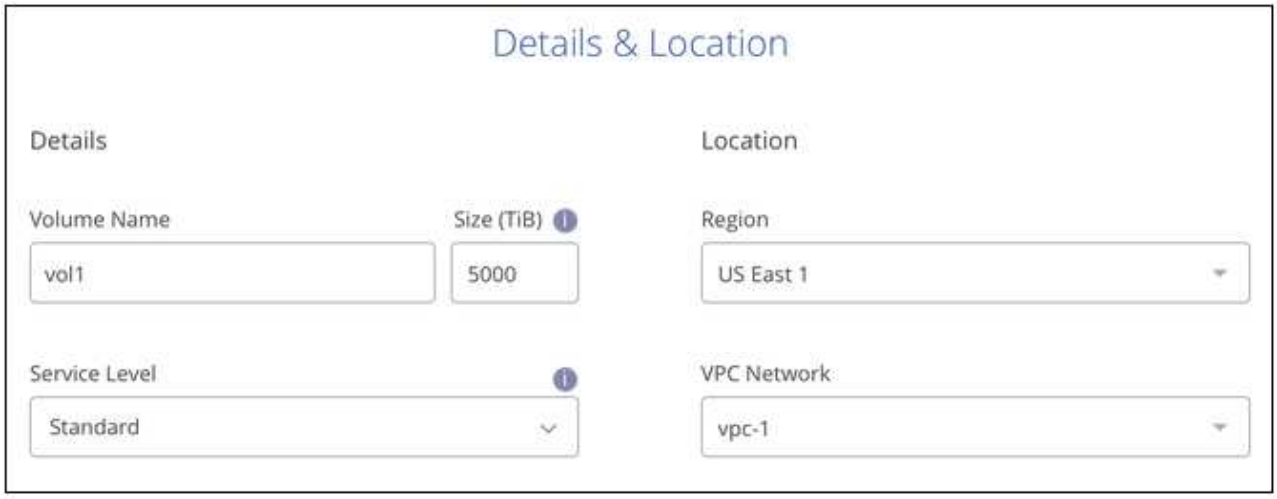
   c. Especifique un nivel de servicio: Standard, Premium o Extreme.

"Obtenga más información sobre los niveles de servicio".

d. Seleccione la región de Google Cloud.

e. Seleccione la red VPC a partir de la que se podrá acceder el volumen. Tenga en cuenta que el VPC no se puede cambiar ni editar después de que se cree el volumen.

f. Haga clic en **continuar**.



3. En la página Protocol, seleccione NFS o SMB y, a continuación, defina los detalles. Las entradas necesarias para NFS y SMB se muestran en secciones independientes a continuación.
4. Para NFS:

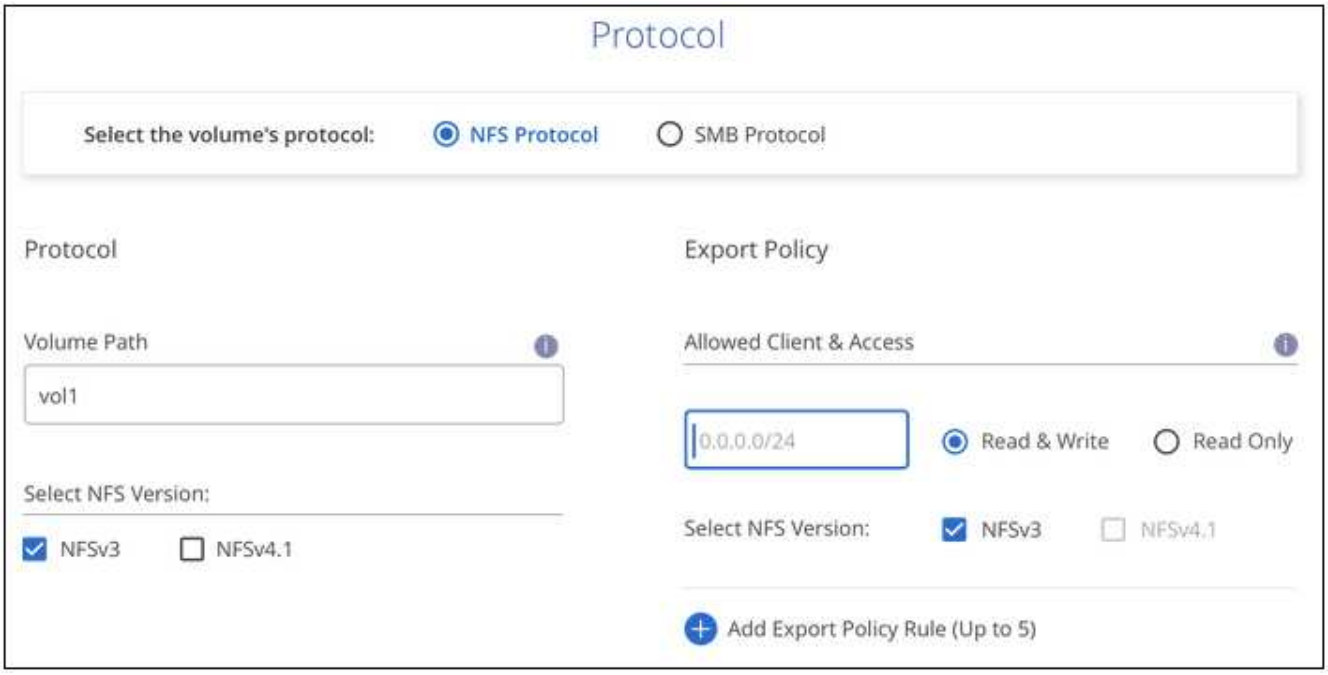
a. En el campo Volume Path, especifique el nombre de la exportación de volumen que se verá cuando monte el volumen.

b. Seleccione NFSv3, NFSv4.1 o ambos en función de sus requisitos.

c. De manera opcional, puede crear una política de exportación para identificar los clientes que pueden acceder al volumen. Especifique:

- Clientes permitidos mediante una dirección IP o enrutamiento entre dominios sin clase (CIDR).
- Derechos de acceso como sólo lectura y escritura o lectura.
- Protocolo de acceso (o protocolos si el volumen permite el acceso NFSv3 y NFSv4.1) utilizado para los usuarios.
- Haga clic en **+ Agregar regla de directiva de exportación** si desea definir reglas de política de exportación adicionales.

  En la siguiente imagen, se muestra la página Volume rellenada para el protocolo NFS:



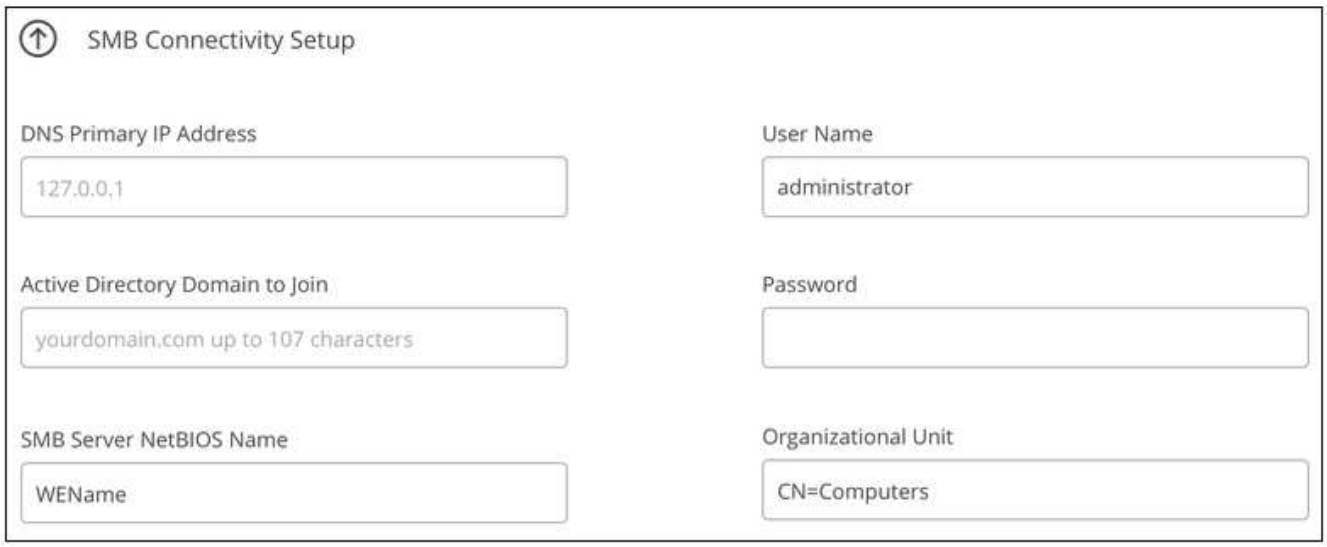
5. Para SMB:

   a. En el campo Volume Path (Ruta de volumen), especifique el nombre de la exportación de volumen que verá cuando monte el volumen y haga clic en **Continue** (continuar).

   b. Si se ha configurado Active Directory, verá la configuración. Si es el primer volumen que se está configurar y no se ha configurado ningún Active Directory, puede habilitar el cifrado de sesión SMB en la página SMB Connectivity Setup:

Campo	Descripción
Dirección IP primaria DNS	Las direcciones IP de los servidores DNS que proporcionan resolución de nombres para el servidor SMB. Utilice una coma para separar las direcciones IP cuando haga referencia a varios servidores, por ejemplo, 172.31.25.223, 172.31.2.74.
Dominio de Active Directory al que unirse	El FQDN del dominio de Active Directory (AD) al que desea que se una el servidor SMB.
Nombre NetBIOS del servidor SMB	Nombre NetBIOS para el servidor SMB que se va a crear.
Credenciales autorizadas para unirse al dominio	Nombre y contraseña de una cuenta de Windows con privilegios suficientes para agregar equipos a la unidad organizativa (OU) especificada dentro del dominio AD.
Unidad organizacional	La unidad organizativa del dominio AD para asociarla con el servidor SMB. El valor predeterminado es CN=equipos para las conexiones con su propio servidor de Windows Active Directory.

   En la siguiente imagen, se muestra la página volumen llena para el protocolo SMB:



6. Haga clic en **continuar**.
7. Si desea crear el volumen según una copia de Snapshot de un volumen existente, seleccione la copia de Snapshot en la lista desplegable Snapshot Name. De lo contrario, haga clic en **continuar**.
8. En la página Snapshot Policy, puede habilitar Cloud Volumes Service para crear copias Snapshot de los volúmenes según una programación. Puede hacerlo ahora moviendo el selector a la derecha o bien se puede editar el volumen más tarde para definir la política de snapshots.

   Consulte "Crear una política de Snapshot" para obtener más información sobre la funcionalidad snapshot.

9. Haga clic en **Añadir volumen**.

El nuevo volumen se agrega al entorno de trabajo.

Continúe con "Montaje del volumen de cloud".

Monte Cloud Volumes

Acceda a instrucciones de montaje desde Cloud Manager para que pueda montar el volumen en un host.

Nota: por favor use el protocolo/dialecto resaltado soportado por su cliente.

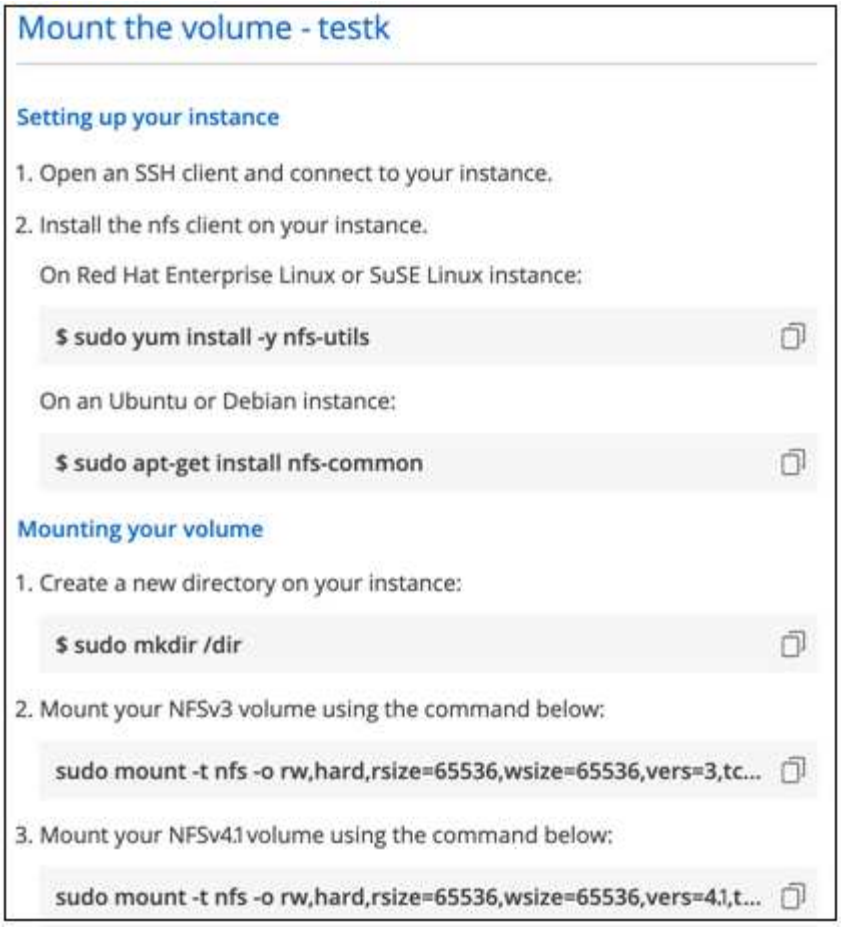
Pasos

1. Abra el entorno de trabajo.
2. Pase el ratón sobre el volumen y haga clic en **montar el volumen**.

   Los volúmenes NFS y SMB muestran instrucciones de montaje para ese protocolo.

3. Pase el ratón sobre los comandos y cópielos en el portapapeles para simplificar este proceso. Solo tiene que agregar el directorio de destino/punto de montaje al final del comando.

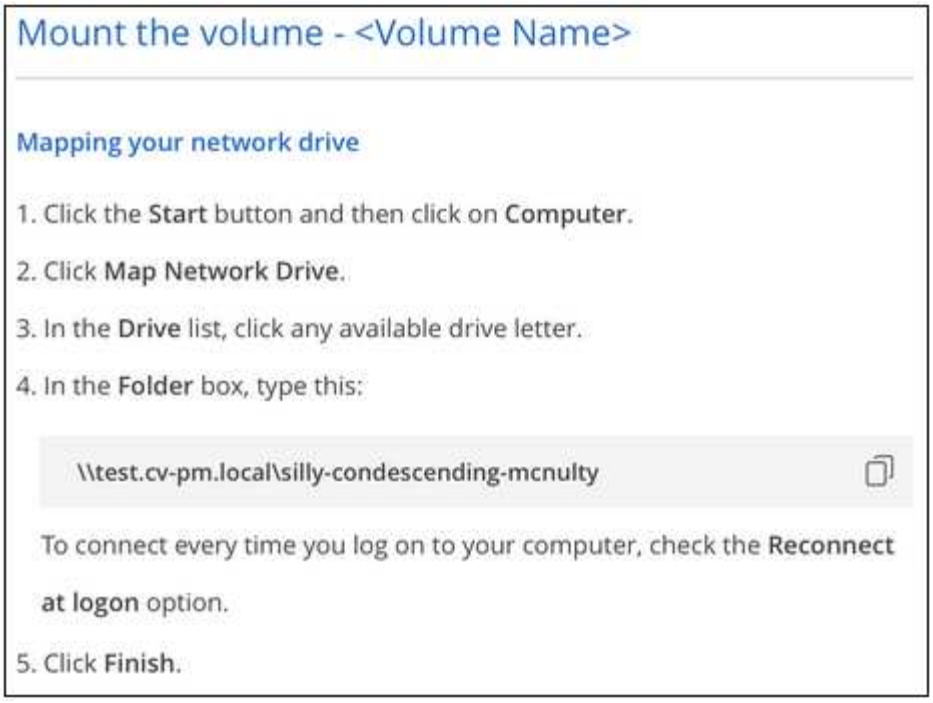
   ejemplo de NFS:



El tamaño máximo de I/o definido por la `rsize` y.. `wsize` options es 1048576, sin embargo 65536 es el valor predeterminado recomendado para la mayoría de los casos de uso.

Tenga en cuenta que los clientes de Linux tendrán NFSv4.1 de manera predeterminada a menos que se especifique la versión con `vers=<nfs_version>` opción.

ejemplo SMB:



4. Asigne la unidad de red siguiendo las instrucciones de montaje de su instancia.

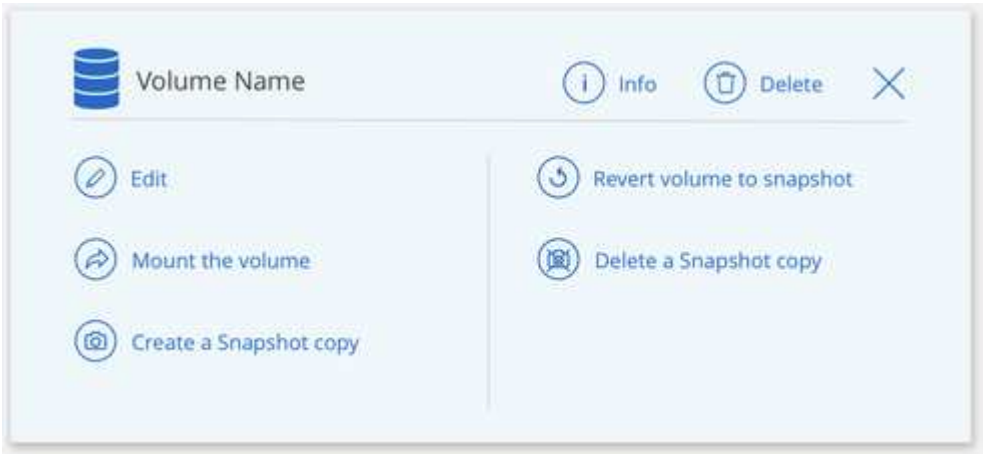
   Después de completar los pasos de las instrucciones de montaje, ha montado correctamente el volumen de cloud en su instancia de GCP.

Gestione los volúmenes existentes

Puede gestionar los volúmenes existentes a medida que cambien sus necesidades de almacenamiento. Es posible ver, editar, restaurar y eliminar volúmenes.

Pasos

1. Abra el entorno de trabajo.
2. Pase el ratón sobre el volumen.



3. Gestione sus volúmenes:

Tarea	Acción
Permite ver la información de un volumen	Haga clic en **Info**.
Editar un volumen (incluida la política de Snapshot)	a. Haga clic en **Editar**. b. Modifique las propiedades del volumen y haga clic en **Actualizar**.
Obtenga el comando de montaje NFS o SMB	a. Haga clic en **montar el volumen**. b. Haga clic en **Copiar** para copiar los comandos.
Cree una copia Snapshot bajo demanda	a. Haga clic en **Crear una copia Snapshot**. b. Si es necesario, cambie el nombre y, a continuación, haga clic en **Crear**.
Reemplace el volumen por el contenido de una copia Snapshot	a. Haga clic en **revertir volumen a instantánea**. b. Seleccione una copia Snapshot y haga clic en **Restaurar**.
Eliminar una copia Snapshot	a. Haga clic en **Eliminar una copia Snapshot**. b. Seleccione la instantánea y haga clic en **Eliminar**. c. Haga clic en **Eliminar** de nuevo cuando se le solicite confirmar.
Eliminar un volumen	a. Desmonte el volumen de todos los clientes: ◦ En los clientes Linux, utilice `umount` comando. ◦ En clientes Windows, haga clic en **desconectar unidad de red**. b. Seleccione un volumen y, a continuación, haga clic en **Eliminar**. c. Vuelva a hacer clic en **Eliminar** para confirmar.

Quite Cloud Volumes Service de Cloud Manager

Puede eliminar una suscripción a Cloud Volumes Service para Google Cloud y todos los volúmenes existentes de Cloud Manager. Los volúmenes no se eliminan; se acaban de quitar de la interfaz de Cloud Manager.

Pasos

1. Abra el entorno de trabajo.
2. Haga clic en la En la parte superior de la página y haga clic en **Quitar Cloud Volumes Service**.
3. En el cuadro de diálogo de confirmación, haga clic en **Quitar**.

Administrar la configuración de Active Directory

Si cambia sus servidores DNS o dominio de Active Directory, debe modificar el servidor SMB en Cloud Volumes Services para poder seguir sirviendo almacenamiento a los clientes.

Pasos

1. Abra el entorno de trabajo.
2. Haga clic en la En la parte superior de la página y haga clic en **Administrar Active Directory**. Si no se ha configurado Active Directory, puede agregar uno ahora. Si se ha configurado uno, puede modificar o eliminar los ajustes mediante el botón.
3. Especifique la configuración del servidor SMB:

Campo	Descripción
Dirección IP primaria DNS	Las direcciones IP de los servidores DNS que proporcionan resolución de nombres para el servidor SMB. Utilice comas para separar las direcciones IP al hacer referencia a varios servidores, por ejemplo, 172.31.25.223, 172.31.2.74.
Dominio de Active Directory al que unirse	El FQDN del dominio de Active Directory (AD) al que desea que se una el servidor SMB.
Nombre NetBIOS del servidor SMB	Nombre NetBIOS para el servidor SMB que se va a crear.
Credenciales autorizadas para unirse al dominio	Nombre y contraseña de una cuenta de Windows con privilegios suficientes para agregar equipos a la unidad organizativa (OU) especificada dentro del dominio AD.
Unidad organizacional	La unidad organizativa del dominio AD para asociarla con el servidor SMB. El valor predeterminado es CN=equipos para las conexiones con su propio servidor de Windows Active Directory.

4. Haga clic en **Guardar** para guardar la configuración.

Permite gestionar snapshots de Cloud Volumes

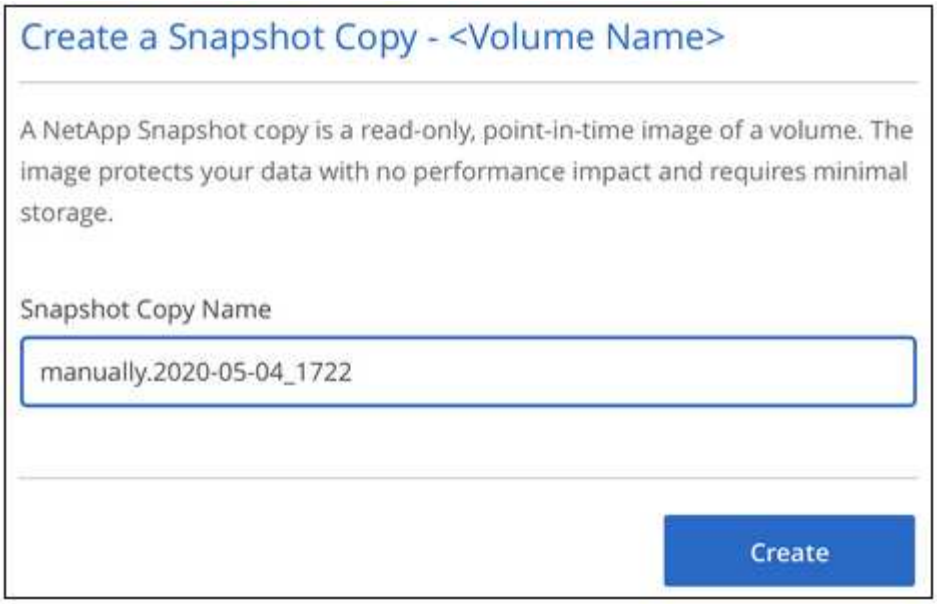
Es posible crear una política de Snapshot para cada volumen para recuperar o restaurar todo el contenido de un volumen desde un momento anterior. También puede crear una snapshot bajo demanda de un volumen de cloud cuando sea necesario.

Crear una snapshot bajo demanda

Es posible crear una copia de Snapshot bajo demanda de un volumen de cloud para crear una copia de Snapshot con el estado actual del volumen.

Pasos

1. Abra el entorno de trabajo.
2. Pase el ratón sobre el volumen y haga clic en **Crear una copia de instantánea**.
3. Introduzca un nombre para la instantánea o utilice el nombre generado automáticamente y haga clic en **Crear**.



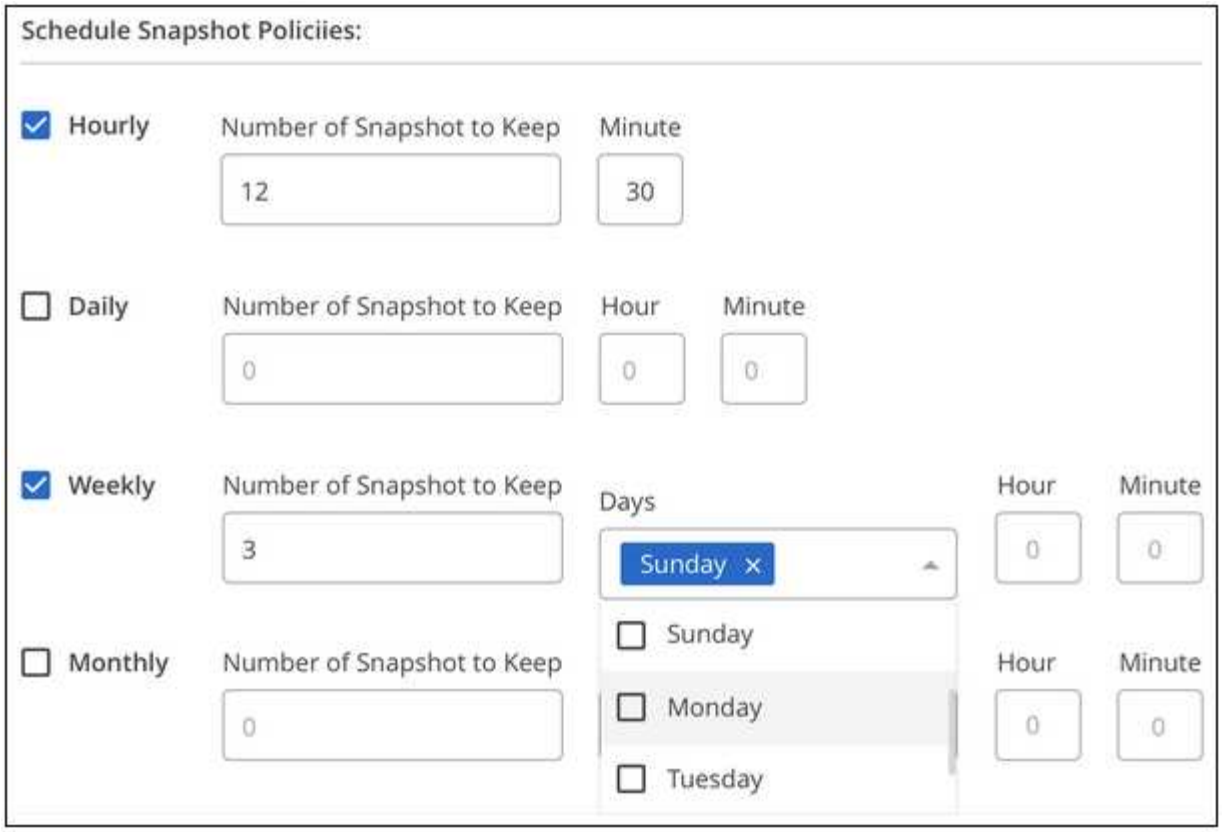
Se crea la copia de Snapshot.

Crear o modificar una política de Snapshot

Es posible crear o modificar una política de Snapshot según sea necesario para un volumen de cloud. La política de Snapshot se define en la pestaña *Snapshot Policy* al crear un volumen o al editar un volumen.

Pasos

1. Abra el entorno de trabajo.
2. Pase el ratón sobre el volumen y haga clic en **Editar**.
3. En la ficha *Snapshot Policy*, mueva el control deslizante Habilitar instantáneas a la derecha.
4. Defina la programación para las Snapshot:
   a. Seleccione la frecuencia: **Hourly**, **Daily**, **Weekly** o **Monthly**
   b. Seleccione el número de snapshots que desea conservar.
   c. Seleccione el día, la hora y los minutos en que se debe realizar la copia de Snapshot.



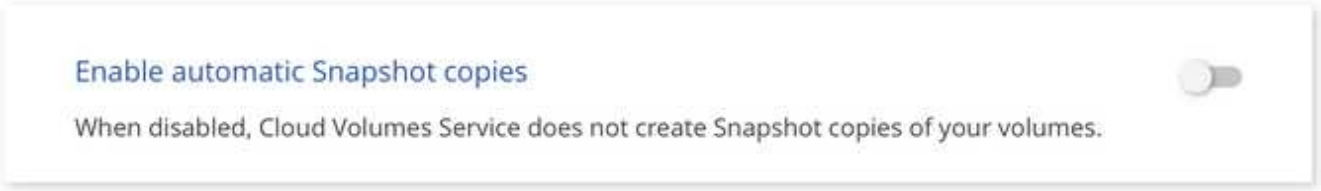
5. Haga clic en **Añadir volumen** o **Actualizar volumen** para guardar la configuración de la directiva.

Deshabilitar una política de Snapshot

Puede deshabilitar una política de Snapshot para detener la creación de copias Snapshot durante un breve período de tiempo mientras se conserva la configuración de la política de Snapshot.

Pasos

1. Abra el entorno de trabajo.
2. Pase el ratón sobre el volumen y haga clic en **Editar**.
3. En la ficha *Snapshot Policy*, mueva el control deslizante Habilitar instantáneas a la izquierda.



4. Haga clic en **Actualizar volumen**.

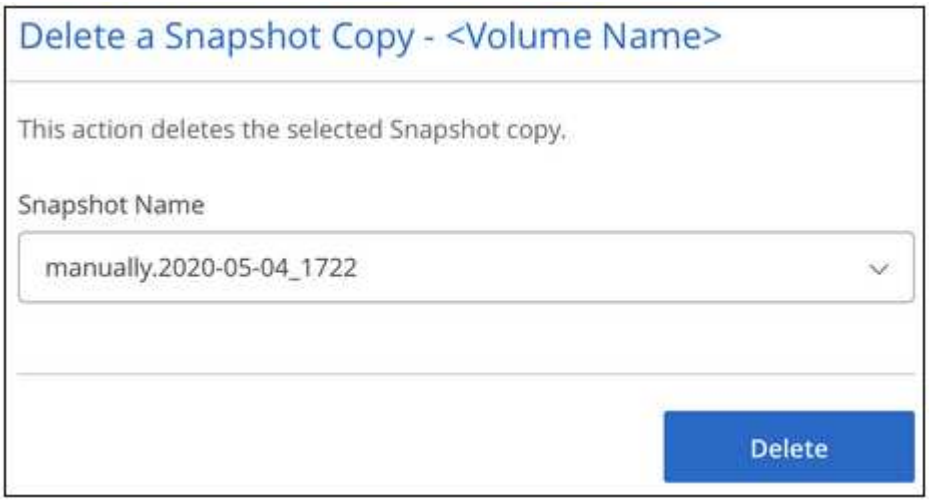
Si desea volver a activar la directiva de instantáneas, mueva el control deslizante Activar instantáneas a la derecha y haga clic en **Actualizar volumen**.

Eliminar una copia de Snapshot

Es posible eliminar una snapshot si ya no es necesaria.

Pasos

1. Abra el entorno de trabajo.
2. Pase el ratón sobre el volumen y haga clic en **Eliminar una copia Snapshot**.
3. Seleccione la instantánea en la lista desplegable y haga clic en **Eliminar**.



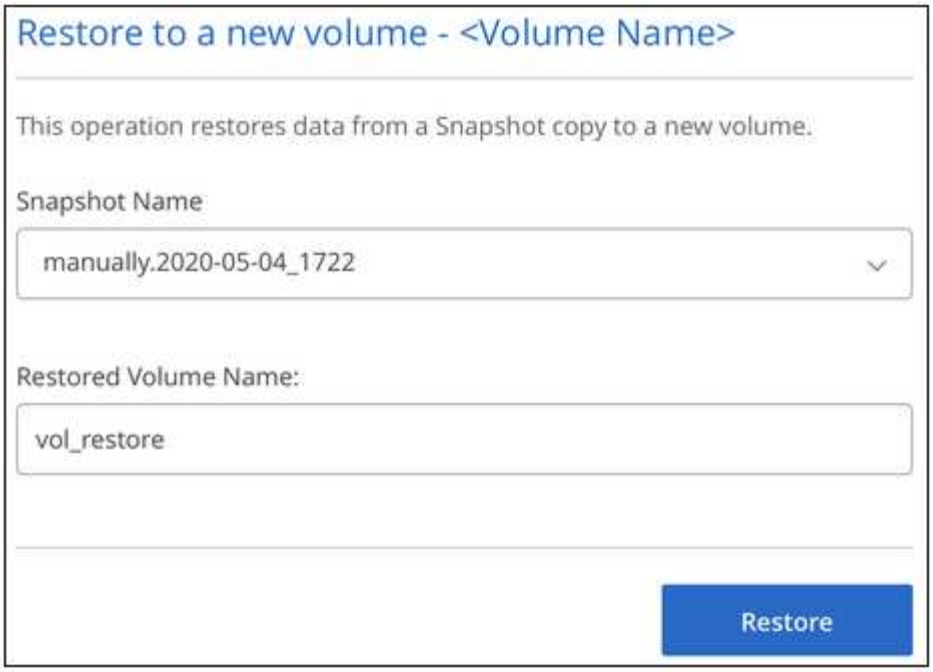
4. En el cuadro de diálogo de confirmación, haga clic en **Eliminar**.

Restaurar una copia de Snapshot en un volumen nuevo

Es posible restaurar una copia de Snapshot en un volumen nuevo si es necesario.

Pasos

1. Abra el entorno de trabajo.
2. Pase el ratón sobre el volumen y haga clic en **Restaurar a un nuevo volumen**.
3. Seleccione la copia de Snapshot que desea usar para crear el volumen nuevo de la lista desplegable.
4. Introduzca un nombre para el nuevo volumen y haga clic en **Restaurar**.



El volumen se crea en el entorno de trabajo.

5. Si necesita cambiar alguno de los atributos del volumen, como la ruta del volumen o el nivel de servicio:
   a. Pase el ratón sobre el volumen y haga clic en **Editar**.
   b. Realice los cambios y haga clic en **Actualizar volumen**.

Después de terminar

Continúe con "Montaje del volumen de cloud".

Gestione clústeres ONTAP de

Detección de clústeres de ONTAP

Cloud Manager puede detectar los clústeres de ONTAP en su entorno local, en una configuración de almacenamiento privado de NetApp y en IBM Cloud. Al detectar un clúster de ONTAP le permite aprovisionar almacenamiento, replicar datos, realizar backups de datos y organizar en niveles datos inactivos de un clúster en las instalaciones al cloud.

Lo que necesitará

- Un conector instalado en un proveedor de cloud o en sus instalaciones.

  Si desea organizar en niveles datos inactivos en el cloud, debe revisar los requisitos del conector en función de dónde tenga pensado organizar los datos inactivos.

  - "Más información sobre conectores"
  - "Cambio entre conectores"
  - "Más información acerca de Cloud Tiering"
- La dirección IP de administración del clúster y la contraseña de la cuenta de usuario administrador para añadir el clúster a Cloud Manager.

  Cloud Manager detecta los clústeres de ONTAP mediante HTTPS. Si utiliza directivas de firewall personalizadas, deben cumplir los siguientes requisitos:

  - El host del conector debe permitir el acceso HTTPS de salida a través del puerto 443.

    Si el conector está en la nube, el grupo de seguridad predefinido permite todas las comunicaciones salientes.

  - El clúster ONTAP debe permitir el acceso HTTPS de entrada a través del puerto 443.

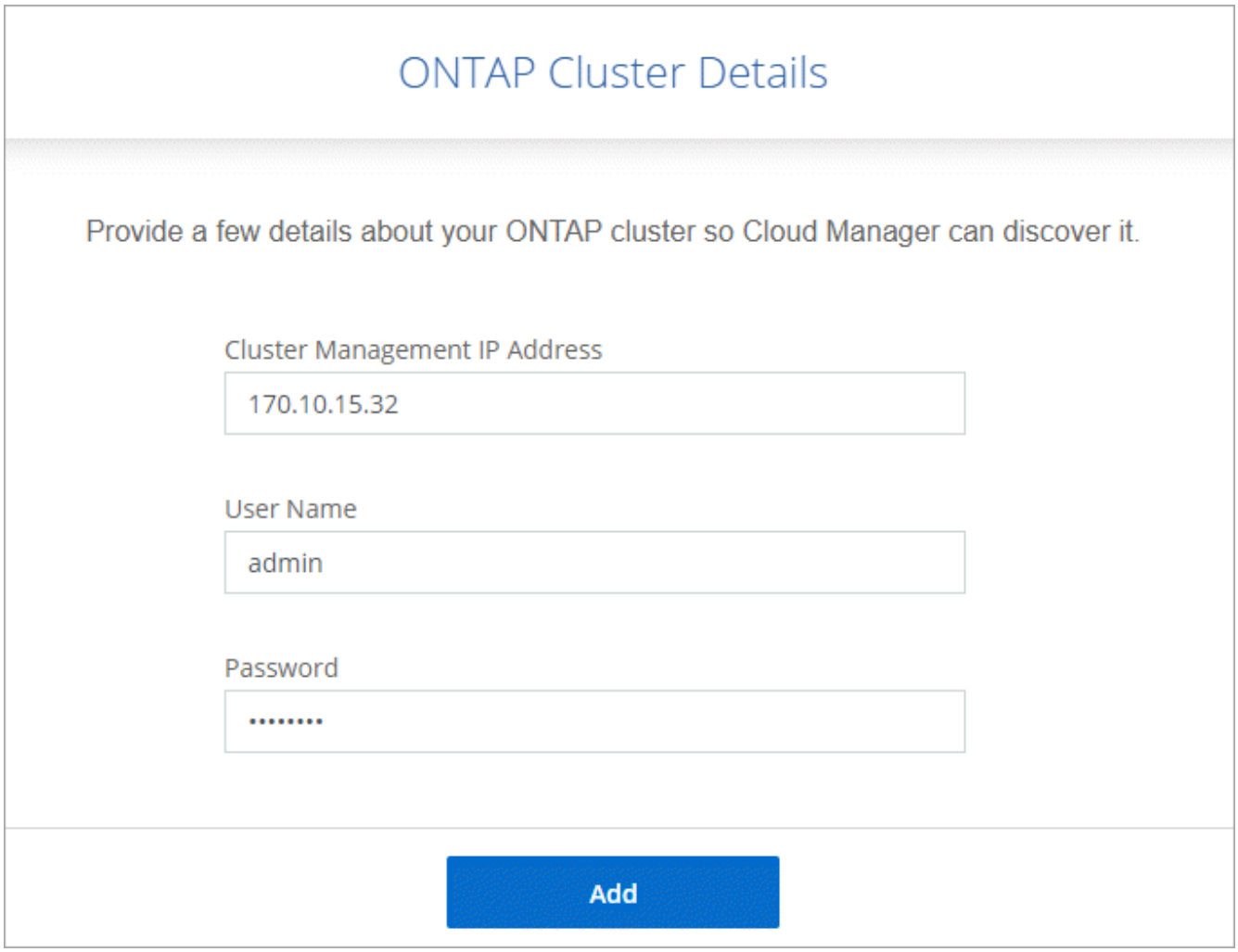
    La política de firewall "mgmt" predeterminada permite el acceso HTTPS entrante desde todas las direcciones IP. Si ha modificado esta directiva predeterminada o si ha creado su propia directiva de firewall, debe asociar el protocolo HTTPS con esa directiva y habilitar el acceso desde el host de Connector.

Pasos

1. En la página entornos de trabajo, haga clic en **Agregar entorno de trabajo** y seleccione **ONTAP** en las instalaciones.
2. Si se le solicita, cree un conector.

   Consulte los enlaces anteriores para obtener más información.

3. En la página **Detalles del clúster ONTAP**, introduzca la dirección IP de administración del clúster, la contraseña de la cuenta de usuario administrador y la ubicación del clúster.



4. En la página Detalles, introduzca un nombre y una descripción para el entorno de trabajo y, a continuación, haga clic en **Ir**.

Resultado

Cloud Manager detecta el clúster. Ahora puede crear volúmenes, replicar datos en el clúster y desde él, configurar la organización en niveles de datos en el cloud, realizar backups de volúmenes en el cloud e iniciar System Manager para realizar tareas avanzadas.

Gestionar el almacenamiento para clústeres de ONTAP

Después de detectar un clúster de ONTAP desde Cloud Manager, puede abrir el entorno de trabajo para aprovisionar y gestionar almacenamiento.

Creación de volúmenes para clústeres de ONTAP

Cloud Manager permite aprovisionar volúmenes NFS, CIFS e iSCSI en clústeres de ONTAP.

Antes de empezar

Los protocolos de datos deben configurarse en el clúster mediante System Manager o la CLI.

Acerca de esta tarea

Es posible crear volúmenes en agregados existentes. No se pueden crear nuevos agregados desde Cloud

Manager.

Pasos

1. En la página Working Environments, haga doble clic en el nombre del clúster de ONTAP en el que desea aprovisionar los volúmenes.
2. Haga clic en **Añadir nuevo volumen**.
3. En la página Crear nuevo volumen, introduzca los detalles del volumen y, a continuación, haga clic en **Crear**.

   Algunos de los campos en esta página son claros y explicativos. En la siguiente tabla se describen los campos que podrían presentar dificultades:

Campo	Descripción
Tamaño	El tamaño máximo que puede introducir depende en gran medida de si habilita thin provisioning, lo que le permite crear un volumen que sea mayor que el almacenamiento físico que hay disponible actualmente.
Política de Snapshot	Una política de copia de Snapshot especifica la frecuencia y el número de copias de Snapshot de NetApp creadas automáticamente. Una copia snapshot de NetApp es una imagen del sistema de archivos puntual que no afecta al rendimiento y requiere un almacenamiento mínimo. Puede elegir la directiva predeterminada o ninguna. Es posible que no elija ninguno para los datos transitorios: Por ejemplo, tempdb para Microsoft SQL Server.
Control de acceso (solo para NFS)	Una política de exportación define los clientes de la subred que pueden acceder al volumen. De forma predeterminada, Cloud Manager introduce un valor que proporciona acceso a todas las instancias de la subred.
Permisos y usuarios/grupos (solo para CIFS)	Estos campos permiten controlar el nivel de acceso a un recurso compartido para usuarios y grupos (también denominados listas de control de acceso o ACL). Es posible especificar usuarios o grupos de Windows locales o de dominio, o usuarios o grupos de UNIX. Si especifica un nombre de usuario de Windows de dominio, debe incluir el dominio del usuario con el formato domain\username.
Grupo del iniciador y IQN (solo para iSCSI)	Los destinos de almacenamiento iSCSI se denominan LUN (unidades lógicas) y se presentan a los hosts como dispositivos de bloque estándar. Los iGroups son tablas de los nombres de los nodos de host iSCSI y controlan qué iniciadores tienen acceso a qué LUN. Los destinos iSCSI se conectan a la red a través de adaptadores de red Ethernet (NIC) estándar, tarjetas DEL motor de descarga TCP (TOE) con iniciadores de software, adaptadores de red convergente (CNA) o adaptadores de host de salida dedicados (HBA) y se identifican mediante nombres cualificados de iSCSI (IQN). Cuando se crea un volumen iSCSI, Cloud Manager crea automáticamente un LUN. Lo hemos hecho sencillo creando sólo una LUN por volumen, por lo que no hay que realizar ninguna gestión. Después de crear el volumen, seleccione ese volumen, haga clic en Target IQN y luego use el IQN para conectarse con el LUN de los hosts.
Perfil de uso	Los perfiles de uso definen las funciones de eficiencia del almacenamiento de NetApp habilitadas para un volumen.

Replicando datos

Puede replicar datos entre sistemas Cloud Volumes ONTAP y clústeres ONTAP eligiendo una replicación de datos única, que puede ayudarle a mover datos hacia y desde el cloud, o una programación recurrente, que puede ayudar con la recuperación ante desastres o la retención a largo plazo.

"Haga clic aquí para obtener más información".

Copia de seguridad de los datos

Puede realizar backups de datos de su sistema ONTAP en las instalaciones en un almacenamiento de objetos de bajo coste en el cloud utilizando el servicio Cloud Manager Backup en el cloud. Este servicio proporciona funcionalidades de backup y restauración para protección y archivado a largo plazo de sus datos en el cloud.

"Haga clic aquí para obtener más información".

Organización de los datos en niveles en el cloud

Amplíe su centro de datos al cloud organizando en niveles los datos inactivos de los clústeres de ONTAP en el almacenamiento de objetos.

"Haga clic aquí para obtener más información".

Backup en el cloud

Más información sobre el backup en el cloud

Backup en cloud es un servicio complementario para clústeres ONTAP y Cloud Volumes ONTAP en las instalaciones que ofrece funcionalidades de backup y restauración para la protección, así como un archivado a largo plazo de sus datos en el cloud. Los backups se almacenan en un almacén de objetos en su cuenta de cloud, independientemente de las copias Snapshot de volumen que se utilicen para la recuperación o clonado a corto plazo.

El backup en el cloud utiliza tecnología "Cloud Backup Service".

> Debe usar Cloud Manager para todas las operaciones de backup y restauración. Cualquier acción que se haga directamente desde ONTAP o desde su proveedor de cloud tendrá como resultado una configuración no compatible.

Funciones

- Realice backups de copias independientes de sus volúmenes de datos en un almacenamiento de objetos de bajo coste en el cloud.
- Los datos de los backups se protegen con conexiones HTTPS en reposo con cifrado AES de 256 bits y TLS 1.2.
- Realice backups del cloud a cloud, y de sistemas ONTAP en las instalaciones al cloud.
- Permite hasta 1,019 backups de un único volumen.
- Restaure los datos de un momento específico.
- Restaure los datos a un volumen en el sistema de origen o a otro sistema.

Entornos de trabajo y proveedores de almacenamiento de objetos compatibles

Backup en Cloud es compatible con los siguientes tipos de entornos de trabajo:

- Cloud Volumes ONTAP en AWS
- Cloud Volumes ONTAP en Azure
- Clústeres de ONTAP en las instalaciones

Coste

El backup en el cloud está disponible en dos opciones de precio: Con su propia licencia (BYOL) y pago por uso (PAYGO).

Para su modelo BYOL, pagará a NetApp para que use el servicio por un periodo de tiempo, por ejemplo, 6 meses, y por una cantidad máxima de capacidad de backup, 10 GB (antes de las eficiencias del almacenamiento), y pagará a su proveedor cloud por los costes de almacenamiento de objetos. Recibirá un número de serie que introduzca en la página Cloud Manager Licensing para habilitar el servicio. Cuando se alcance cualquiera de los límites, deberá renovar la licencia. Consulte "Adición y actualización de su licencia BYOL de copia de seguridad". La licencia BYOL de backup se aplica a todos los sistemas Cloud Volumes

ONTAP asociados con su "Cuenta de Cloud Central".

Para PAYGO, tendrá que pagar a su proveedor de cloud por los costes de almacenamiento de objetos y NetApp por los costes de licencia de backup. Los costes de licencia se basan en la capacidad utilizada (antes de la eficiencia del almacenamiento):

- AWS: "Vaya a la oferta de Cloud Manager Marketplace para obtener información sobre los precios".
- Azure: "Vaya a la oferta de Cloud Manager Marketplace para obtener información sobre los precios".

Prueba gratuita

Se ofrece una prueba gratuita de 30 días. Al utilizar la versión de prueba, se le notifica el número de días de prueba gratuitos que quedan. Al final de su prueba gratuita, los backups dejan de crearse. Debe suscribirse al servicio o adquirir una licencia para seguir utilizando el servicio.

El backup no se elimina cuando el servicio está deshabilitado. El proveedor de cloud seguirá facturando los costes del almacenamiento de objetos por la capacidad que utilizan sus backups a menos que elimine los backups.

Funcionamiento del backup en cloud

Cuando habilita Backup en cloud en un sistema Cloud Volumes ONTAP o ONTAP en las instalaciones, el servicio realiza un backup completo de los datos. Las snapshots de volúmenes no están incluidas en la imagen de backup. Tras el primer backup, todos los backups adicionales son incrementales, lo que significa que solo se realiza un backup de los bloques modificados y los nuevos bloques.

La ubicación de los backups

Las copias de backup se almacenan en un bloque de S3 o en un contenedor de Azure Blob que Cloud Manager crea en su cuenta de cloud. Para los sistemas Cloud Volumes ONTAP, el almacén de objetos se crea en la misma región donde se encuentra el sistema Cloud Volumes ONTAP. Para sistemas ONTAP locales que identifica la región al habilitar el servicio.

Hay un almacén de objetos por Cloud Volumes ONTAP o sistema ONTAP en las instalaciones. Cloud Manager nombra el almacén de objetos de la siguiente manera: netapp-backup-*clusterUUID*

Asegúrese de no eliminar este almacén de objetos.

Notas:

- En AWS, Cloud Manager habilita el "Función de acceso público en bloque de Amazon S3" En el bloque de S3.
- En Azure, Cloud Manager utiliza un grupo de recursos nuevo o existente con una cuenta de almacenamiento para el contenedor Blob.

Clases de almacenamiento S3 compatibles

En Amazon S3, los backups se inician en la clase de almacenamiento *Standard* y se realizan la transición a la clase de almacenamiento *Standard-Infrecuente Access* tras 30 días.

Niveles de acceso de Azure Blob compatibles

En Azure, cada backup está asociado con el nivel de acceso *Cold*.

La configuración de backup es de todo el sistema

Al habilitar el backup en cloud, se realiza un backup en el cloud de todos los volúmenes que se identifican en el sistema.

La programación y la cantidad de backups que se retendrán se definen en el nivel del sistema. La configuración de backup afecta a todos los volúmenes del sistema.

La programación es diaria, semanal, mensual o combinada

Se pueden elegir backups diarios, semanales o mensuales de todos los volúmenes. También puede seleccionar una de las políticas definidas por el sistema que proporcione backups y retención durante 3 meses, 1 año y 7 años. Estas políticas son:

Nombre de la directiva	Backups por intervalo…			Capacidad Completos
	Diario	Semanal	mensual	
Netapp3MonthsRetention	30	13	3	46
Netapp1YearRetention	30	13	12	55
Retención de Netapp7YearsRetention	30	53	84	167

Una vez que haya alcanzado el número máximo de backups para una categoría o intervalo, se eliminan los backups más antiguos de modo que siempre tendrá los backups más recientes.

Tenga en cuenta que el período de retención para backups de volúmenes de protección de datos es el mismo que se define en la relación de SnapMirror de origen. Puede cambiar esto si lo desea con la API de.

Los backups se realizan a medianoche

- Los backups diarios comienzan justo después de la medianoche cada día.
- Los respaldos semanales comienzan justo después de la medianoche los domingos por la mañana.
- Los backups mensuales comienzan justo después de la medianoche del primer mes.

En este momento, no se pueden programar operaciones de copia de seguridad a una hora especificada por el usuario.

Las copias de backup están asociadas con su cuenta de Cloud Central

Las copias de backup se asocian con "Cuenta de Cloud Central" En el que reside Cloud Manager.

Si tiene varios sistemas Cloud Manager en la misma cuenta de Cloud Central, cada sistema Cloud Manager mostrará la misma lista de backups. Que incluye los backups asociados con Cloud Volumes ONTAP e instancias de ONTAP en las instalaciones desde otros sistemas de Cloud Manager.

Consideraciones sobre la licencia de BYOL

Cuando se usa una licencia BYOL de backup a cloud, Cloud Manager le notifica cuando los backups se acercan al límite de capacidad o se acercan a la fecha de vencimiento de la licencia. Recibe estas notificaciones:

- cuando los backups han alcanzado el 80 % de la capacidad con licencia y nuevamente cuando se ha

alcanzado el límite

- 30 días antes de que caduque una licencia, y de nuevo cuando caduque la licencia

Utilice el icono de chat de la parte inferior derecha de la interfaz de Cloud Manager para renovar su licencia cuando reciba estas notificaciones.

Pueden ocurrir dos cosas cuando caduca su licencia:

- Si la cuenta que está utilizando para sus sistemas ONTAP tiene una cuenta de mercado, el servicio de copia de seguridad continúa ejecutándose, pero se pasa a un modelo de licencia de PAYGO. Su proveedor de cloud le cobra por los costes de almacenamiento de objetos y por NetApp por los costes de licencias de backup por la capacidad que utilizan sus backups.
- Si la cuenta que está utilizando para sus sistemas ONTAP no tiene una cuenta de mercado, el servicio de backup sigue ejecutándose, pero seguirá recibiendo el mensaje de caducidad.

Una vez que renueve su suscripción BYOL, Cloud Manager obtiene automáticamente la nueva licencia de NetApp y la instala. Si Cloud Manager no puede acceder al archivo de licencia a través de la conexión segura a Internet, puede obtener el archivo usted mismo y cargarlo manualmente en Cloud Manager. Para ver instrucciones, consulte "Adición y actualización de su licencia BYOL de copia de seguridad".

Los sistemas que se han transferido a una licencia PAYGO se devuelven automáticamente a la licencia BYOL. Y los sistemas que se estaban ejecutando sin una licencia dejarán de recibir el mensaje de advertencia y se cobrarán por las copias de seguridad que se hayan producido mientras la licencia ha caducado.

Volúmenes compatibles

Backup en el cloud admite volúmenes de lectura/escritura y volúmenes de protección de datos (DP).

Los volúmenes FlexGroup no son compatibles actualmente.

Limitaciones

- No se admite el almacenamiento WORM (SnapLock) en un sistema Cloud Volumes ONTAP o en las instalaciones cuando se habilita el backup en el cloud.
- Restricciones de backup a cloud al realizar backups desde sistemas ONTAP en las instalaciones:
  - El clúster en las instalaciones debe ejecutar ONTAP 9.7P5 o una versión posterior.
  - Cloud Manager debe ponerse en marcha en Azure. No existe compatibilidad con puestas en marcha de Cloud Manager en las instalaciones.
  - La ubicación de destino de los backups solo es almacenamiento de objetos en Azure.
  - Los backups solo se pueden restaurar en sistemas Cloud Volumes ONTAP implementados en Azure. No es posible restaurar un backup en un sistema ONTAP en las instalaciones o en un sistema Cloud Volumes ONTAP que utilice un proveedor de cloud diferente.
- Al realizar una copia de seguridad de los volúmenes de protección de datos (DP), la regla definida para la política de SnapMirror en el volumen de origen debe utilizar una etiqueta que coincida con los nombres permitidos de la política de copia de seguridad en la nube de **diaria**, **semanal** o **mensual**. De lo contrario, se producirá un error en la copia de seguridad de ese volumen DP.
- En Azure, si habilita Backup en cloud cuando se implementa Cloud Volumes ONTAP, Cloud Manager crea el grupo de recursos para usted y no puede cambiarlo. Si desea elegir su propio grupo de recursos al habilitar Backup to Cloud, **deshabilite** Backup to Cloud al implementar Cloud Volumes ONTAP y, a continuación, active Backup to Cloud y elija el grupo de recursos en la página Backup to Cloud Settings.

- Cuando se realizan backups de volúmenes de sistemas Cloud Volumes ONTAP, no se crean backups de los volúmenes creados fuera de Cloud Manager automáticamente.

  Por ejemplo, si crea un volumen desde la CLI de ONTAP, la API de ONTAP o System Manager, no se creará un backup automático de ese volumen.

  Si desea realizar un backup de estos volúmenes, tendrá que deshabilitar la función Backup en el cloud y, a continuación, volver a habilitarla.

Manos a la obra

Realizar backups de datos en Amazon S3

Complete unos pasos para empezar a realizar backups de datos desde Cloud Volumes ONTAP en Amazon S3.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

Verifique la compatibilidad con la configuración

- Utiliza Cloud Volumes ONTAP 9.6 o posterior en AWS.
- Se ha suscrito a "Oferta de Cloud Manager Marketplace Backup", o usted ha comprado "y activado" Una licencia BYOL de backup en cloud de NetApp.
- El rol IAM que proporciona a Cloud Manager permisos incluye Permisos de S3 desde el más reciente "Política de Cloud Manager".

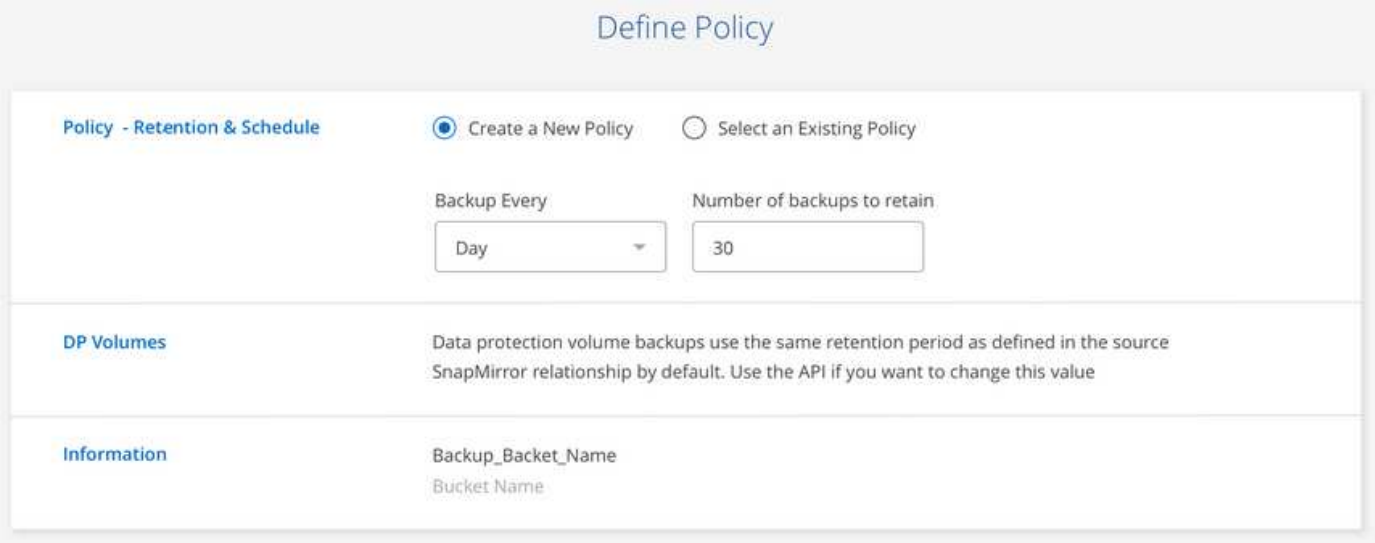
Habilite el backup en cloud en su sistema nuevo o existente

- Nuevos sistemas: El backup en el cloud está habilitado de forma predeterminada en el asistente del entorno de trabajo. Asegúrese de mantener la opción habilitada.
- Sistemas existentes: Seleccione el entorno de trabajo y haga clic en **Activar** junto al servicio copia de seguridad en la nube en el panel derecho y, a continuación, siga el asistente de configuración.

Defina la política de backup

La política predeterminada realiza backups de volúmenes todos los días y conserva las 30 copias de backup

más recientes de cada volumen. Cambie a backups semanales o mensuales, o seleccione una de las políticas definidas por el sistema que proporcionan más opciones. También es posible cambiar la cantidad de copias de backup que se conservan.

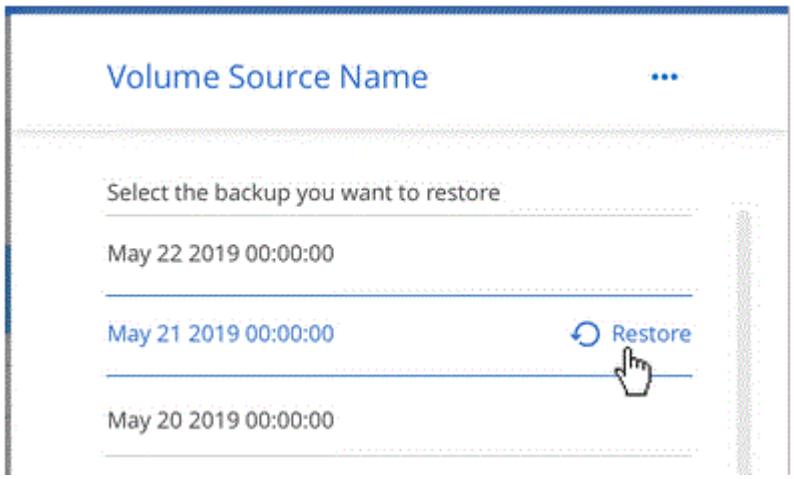


Seleccione los volúmenes de los que desea realizar el backup

Identificar los volúmenes de los que se desea realizar backup en la página Select Volumes.

Restaure sus datos, según sea necesario

En la lista de backups, seleccione un volumen, seleccione un backup y, a continuación, restaure datos del backup en un nuevo volumen.



Requisitos

Lea los siguientes requisitos para asegurarse de que tenga una configuración compatible antes de comenzar a realizar el backup de volúmenes en S3.

Versiones de ONTAP compatibles

Cloud Volumes ONTAP 9.6 y posteriores.

Regiones admitidas de AWS

El backup en cloud es compatible en todas las regiones de AWS "Donde se admite Cloud Volumes ONTAP".

Requisitos de licencia

Para las licencias de Backup to Cloud PAYGO, hay una suscripción a Cloud Manager disponible en AWS Marketplace que permite poner en marcha Cloud Volumes ONTAP 9.6 y versiones posteriores (PAYGO) y Backup en el cloud. Necesita hacerlo "suscríbase a esta suscripción a Cloud Manager" Antes de habilitar Backup en el cloud. La facturación de Backup en Cloud se realiza mediante esta suscripción.

Para las licencias BYOL de backup en cloud, no necesita una suscripción a AWS Backup en el cloud. Se necesita el número de serie de NetApp que le permite usar el servicio durante la duración y la capacidad de la licencia. Consulte "Adición y actualización de su licencia BYOL de copia de seguridad".

Además, necesita tener una suscripción a AWS para el espacio de almacenamiento donde se ubicará la copia de seguridad.

Se requieren permisos de AWS

El rol IAM que proporciona permisos a Cloud Manager Incluya los permisos de S3 desde el último "Política de Cloud Manager".

A continuación se muestran los permisos específicos de la directiva:

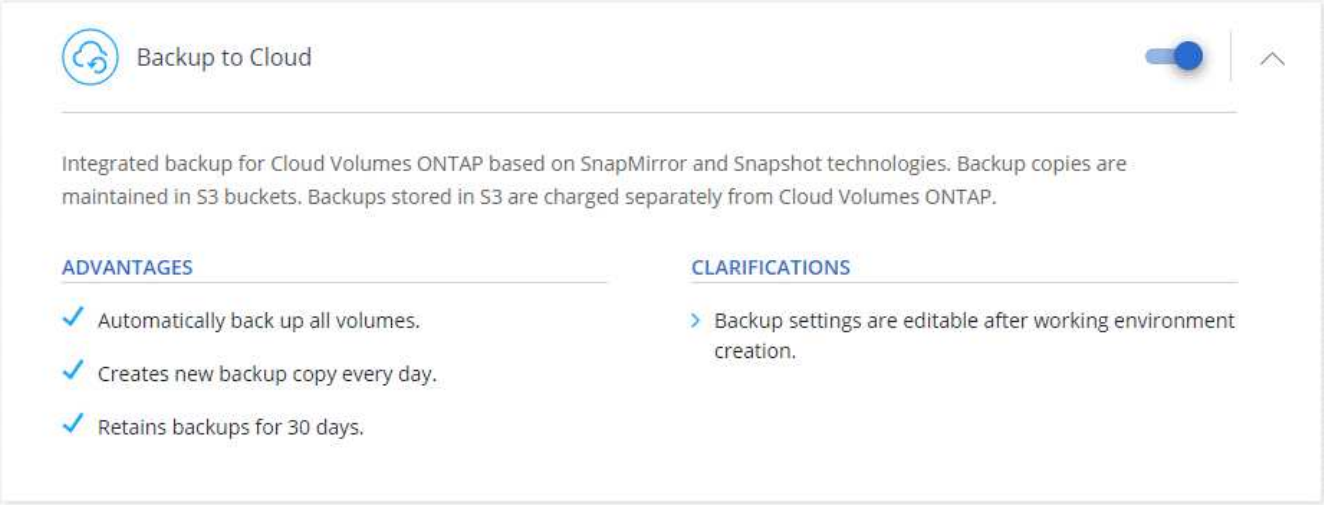
```
{
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws:s3:::netapp-backup-*"
            ]
        },
```

Habilitación de Backup en cloud en un nuevo sistema

De forma predeterminada, el backup en cloud está habilitado en el asistente de entorno de trabajo. Asegúrese de mantener la opción habilitada.

Pasos

1. Haga clic en **Crear Cloud Volumes ONTAP**.
2. Seleccione Amazon Web Services como proveedor de cloud y, a continuación, elija un único nodo o sistema de alta disponibilidad.
3. Rellene la página Details & Credentials.
4. En la página Servicios, deje el servicio activado y haga clic en **continuar**.



5. Complete las páginas del asistente para implementar el sistema.

Resultado

El backup en el cloud se habilita en el sistema y realiza backups de volúmenes cada día y retiene las 30 copias de backup más recientes.

El futuro

"Es posible gestionar backups si se cambia la programación de backup, se restauran los volúmenes, etc.".

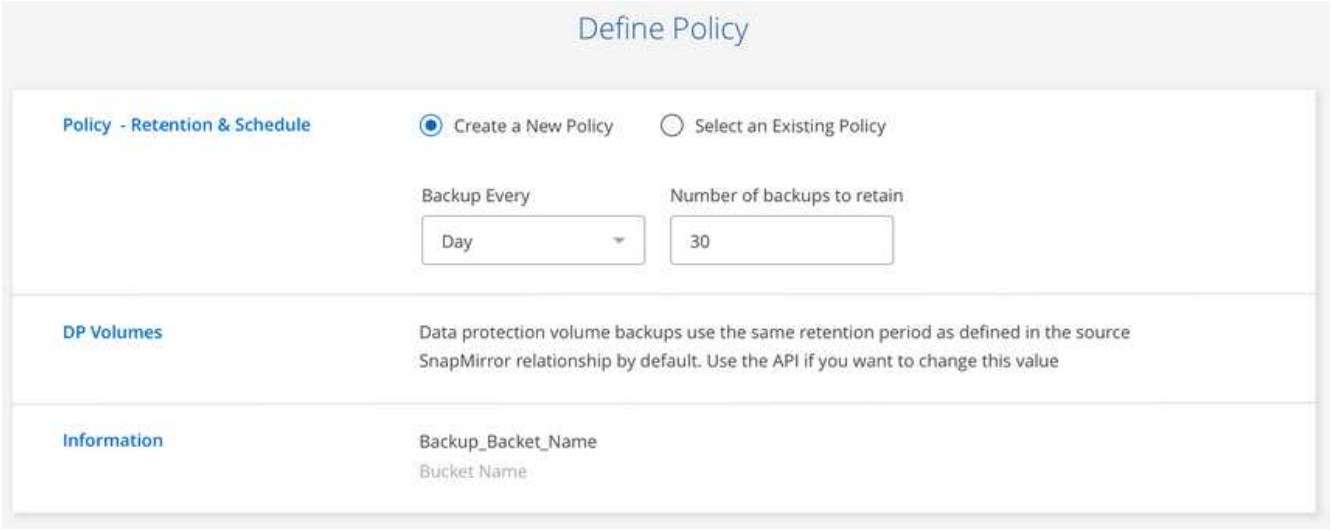
Habilitar Backup en el cloud en un sistema existente

Active Backup en el cloud en cualquier momento directamente desde el entorno de trabajo.

Pasos

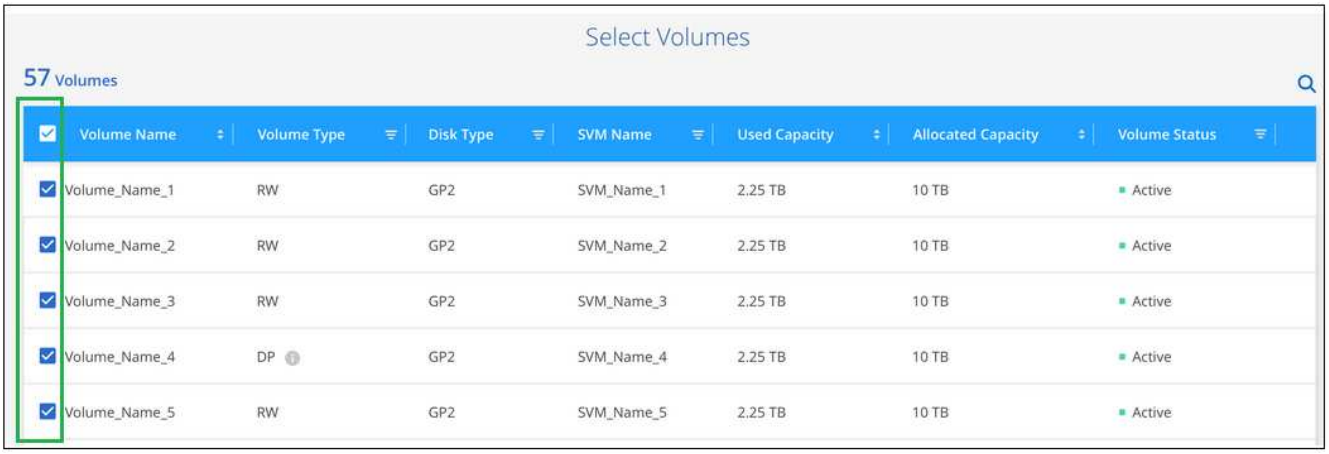
1. Seleccione el entorno de trabajo y haga clic en **Activar** junto al servicio copia de seguridad en la nube en el panel derecho.

2. Defina el programa de copia de seguridad y el valor de retención y haga clic en **continuar**.



Consulte "la lista de políticas existentes".

3. Seleccione los volúmenes de los que desea realizar una copia de seguridad y haga clic en **Activar**.



Resultado

Backup a cloud empieza a realizar los backups iniciales de cada volumen seleccionado.

El futuro

"Es posible gestionar backups si se cambia la programación de backup, se restauran los volúmenes, etc.".

Realizar backups de los datos en almacenamiento de Azure Blob

Complete unos pasos para empezar a realizar backups de datos de Cloud Volumes ONTAP a almacenamiento de Azure Blob.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

Verifique la compatibilidad con la configuración

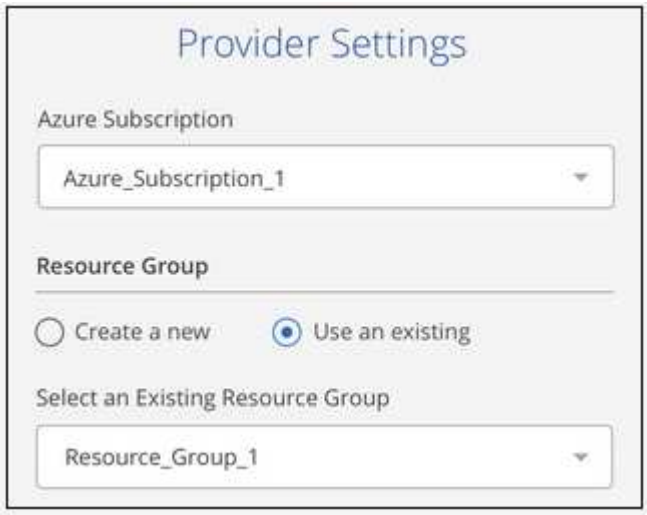
- Utiliza Cloud Volumes ONTAP 9.7 o posterior en Azure.
- Dispone de una suscripción de proveedor de cloud válida para el espacio de almacenamiento en el que se ubicará los backups.
- Se ha suscrito a "Oferta de Cloud Manager Marketplace Backup", o usted ha comprado "y activado" Una licencia BYOL de backup en cloud de NetApp.

Habilite el backup en cloud en su sistema nuevo o existente

- Nuevos sistemas: El backup en el cloud está habilitado de forma predeterminada en el asistente del entorno de trabajo. Asegúrese de mantener la opción habilitada.
- Sistemas existentes: Seleccione el entorno de trabajo y haga clic en **Activar** junto al servicio copia de seguridad en la nube en el panel derecho y, a continuación, siga el asistente de configuración.

Introduzca los detalles del proveedor

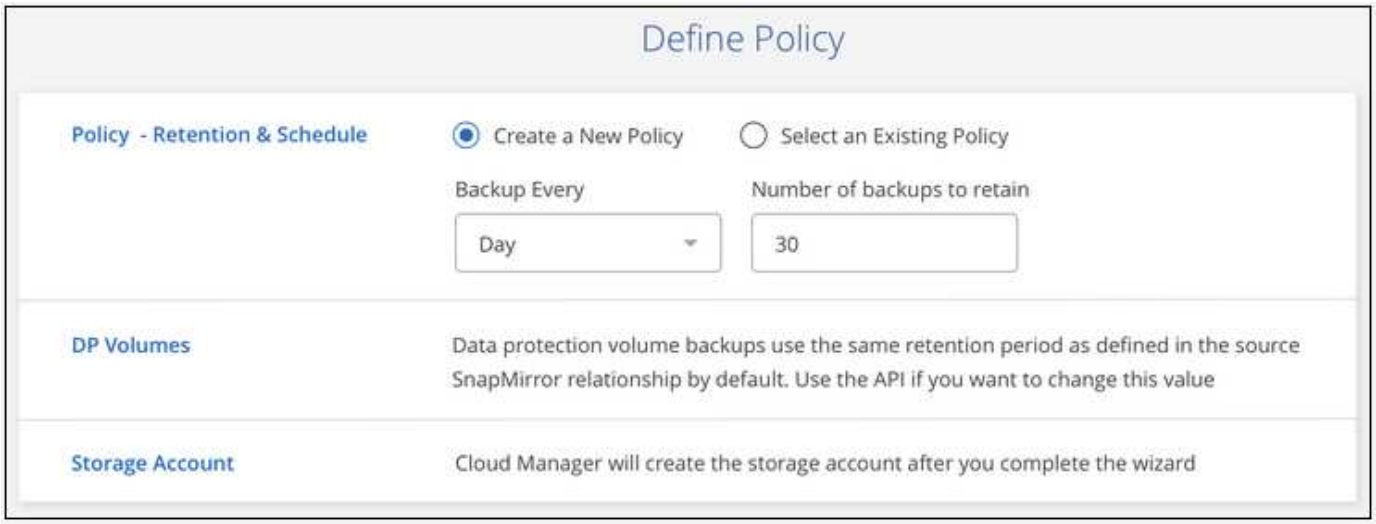
Seleccione la suscripción de proveedor y elija si desea crear un nuevo grupo de recursos o usar un grupo de recursos ya existente.



Defina la política de backup

La política predeterminada realiza backups de volúmenes todos los días y conserva las 30 copias de backup más recientes de cada volumen. Cambie a backups semanales o mensuales, o seleccione una de las políticas

definidas por el sistema que proporcionan más opciones.

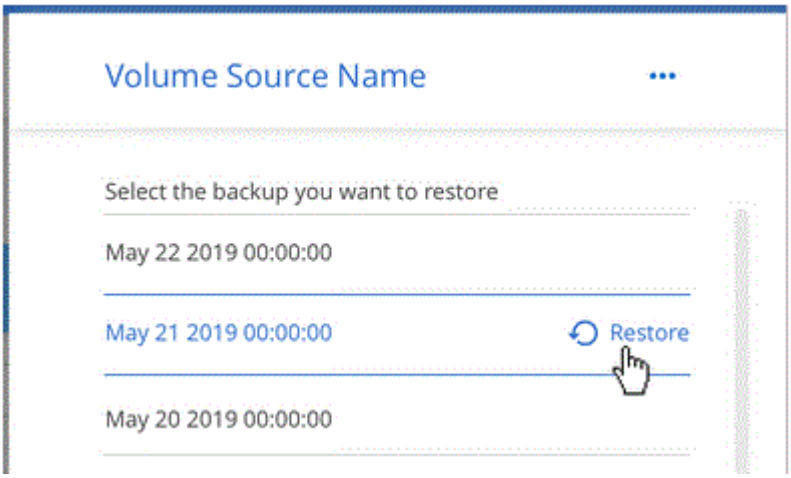


5 Seleccione los volúmenes de los que desea realizar el backup

Identificar los volúmenes de los que se desea realizar backup en la página Select Volumes.

6 Restaure sus datos, según sea necesario

En la lista de backups, seleccione un volumen, seleccione un backup y, a continuación, restaure datos del backup en un nuevo volumen.



Requisitos

Lea los siguientes requisitos para asegurarse de que tiene una configuración compatible antes de empezar a realizar backups de volúmenes en el almacenamiento de Azure Blob.

Versiones de ONTAP compatibles

Cloud Volumes ONTAP 9.7 y posteriores.

Regiones de Azure compatibles

El backup en cloud es compatible en todas las regiones de Azure "Donde se admite Cloud Volumes ONTAP".

Requisitos de licencia

Para las licencias de Backup to Cloud PAYGO, es necesario suscribirse a través de Azure Marketplace antes de habilitar Backup en el cloud. La facturación de Backup en Cloud se realiza mediante esta suscripción. "Puede suscribirse desde la página Detalles Credentials del asistente de entorno de trabajo".

Para las licencias de BYOL de backup a cloud, necesita el número de serie de NetApp que le permite usar el servicio durante la duración y la capacidad de la licencia. Consulte "Adición y actualización de su licencia BYOL de copia de seguridad".

Además, necesita tener una suscripción a Microsoft Azure para el espacio de almacenamiento en el que se ubicará los backups.

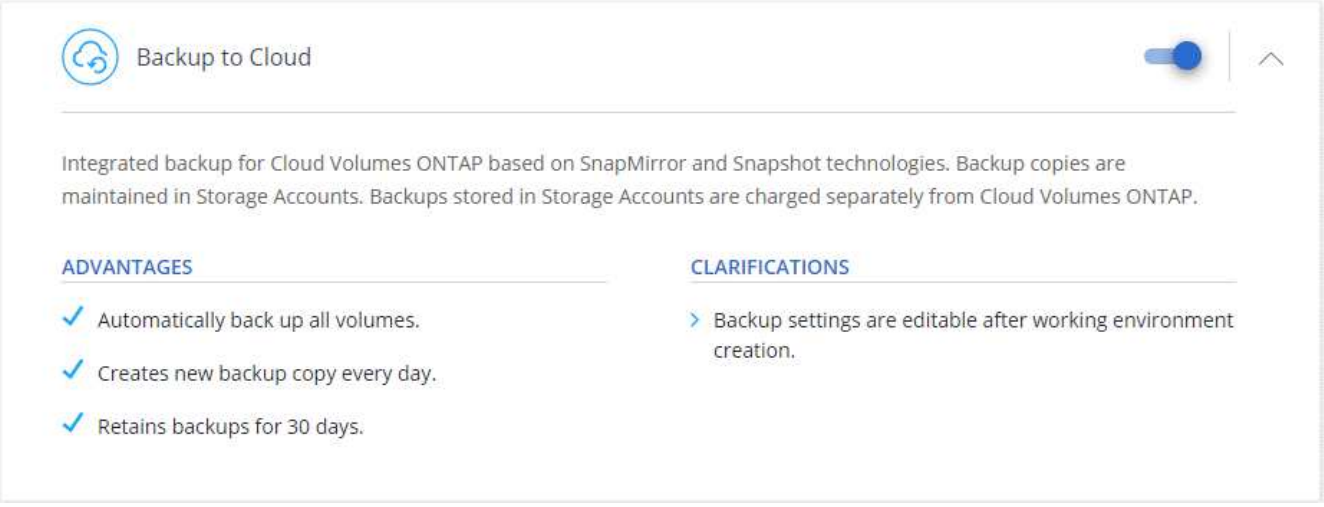
Habilitación de Backup en cloud en un nuevo sistema

De forma predeterminada, el backup en cloud está habilitado en el asistente de entorno de trabajo. Asegúrese de mantener la opción habilitada.

Si desea elegir el nombre del grupo de recursos, **deshabilite** copia de seguridad en la nube al implementar Cloud Volumes ONTAP. Siga los pasos de habilitar el backup en cloud en un sistema existente Para habilitar Backup en cloud y elegir el grupo de recursos.

Pasos

1. Haga clic en **Crear Cloud Volumes ONTAP**.
2. Seleccione Microsoft Azure como proveedor de cloud y, a continuación, elija un único nodo o sistema de alta disponibilidad.
3. Rellene la página Detalles y credenciales y asegúrese de que haya una suscripción a Azure Marketplace en su lugar.
4. En la página Servicios, deje el servicio activado y haga clic en **continuar**.



5. Complete las páginas del asistente para implementar el sistema.

Resultado

El backup en el cloud se habilita en el sistema y realiza backups de volúmenes cada día y retiene las 30 copias de backup más recientes.

El futuro

"Es posible gestionar backups si se cambia la programación de backup, se restauran los volúmenes, etc.".

Habilitar Backup en el cloud en un sistema existente

Active Backup en el cloud en cualquier momento directamente desde el entorno de trabajo.

Pasos

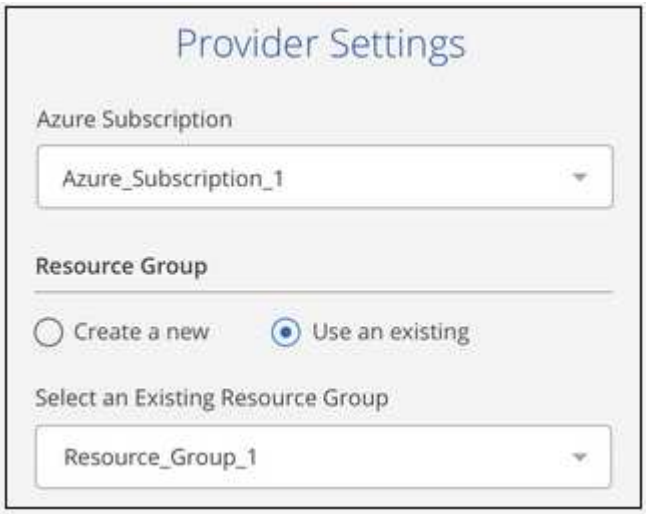
1. Seleccione el entorno de trabajo y haga clic en **Activar** junto al servicio copia de seguridad en la nube en el panel derecho.

2. Seleccione los detalles del proveedor:

   a. La suscripción de Azure utilizada para almacenar los backups.

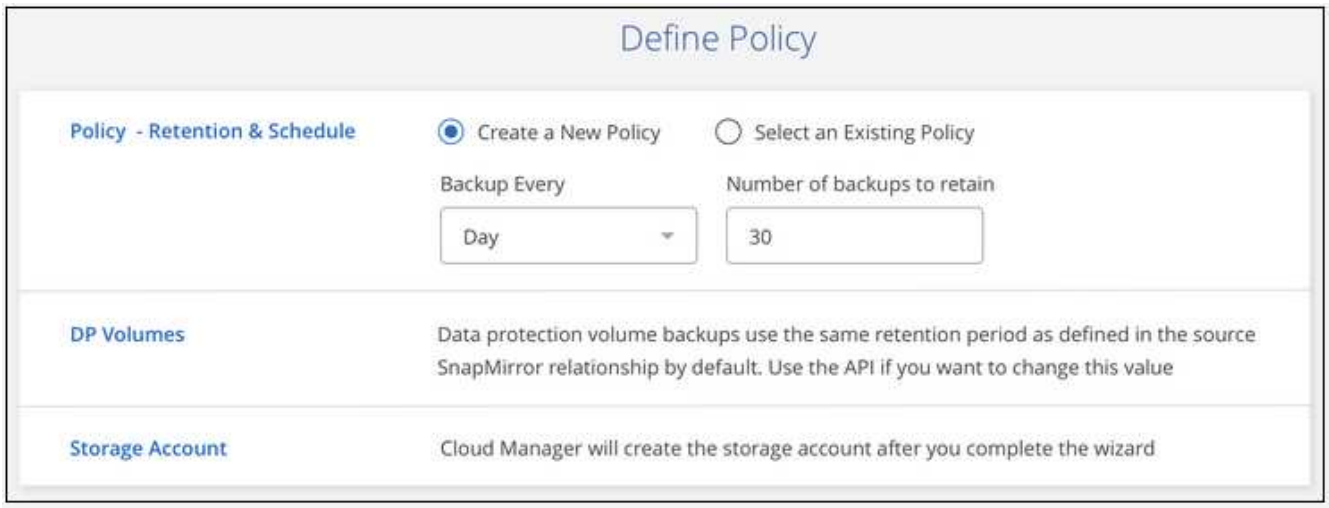
   b. El grupo de recursos: Es posible crear un nuevo grupo de recursos, o bien seleccionar y existente.

   c. Y, a continuación, haga clic en **continuar**.



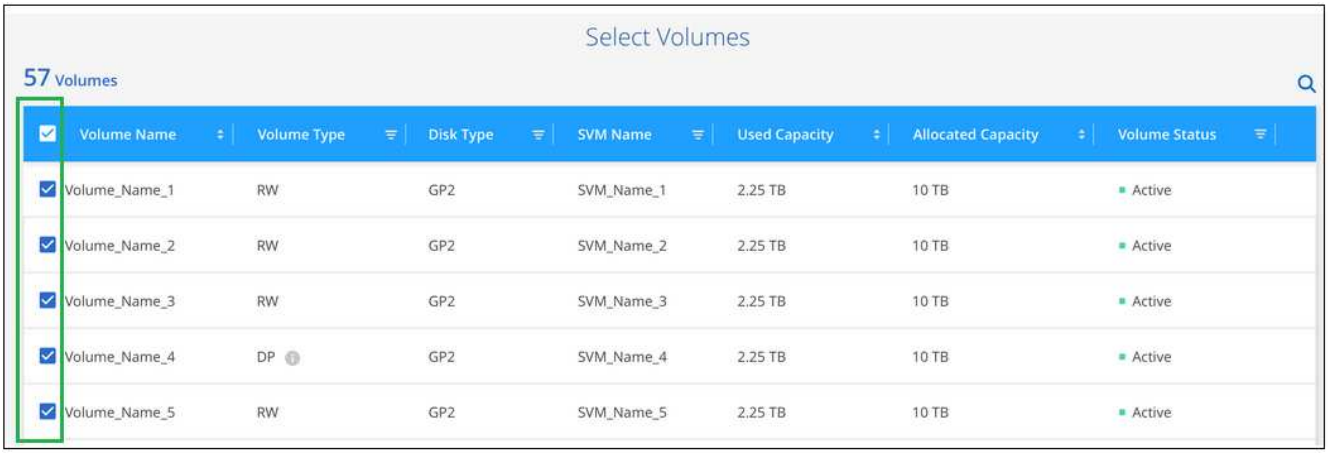
   Tenga en cuenta que no puede cambiar la suscripción ni el grupo de recursos después de que se hayan iniciado los servicios.

3. En la página *define Policy*, seleccione el programa de copia de seguridad y el valor de retención y haga clic en **continuar**.



Consulte "la lista de políticas existentes".

4. Seleccione los volúmenes de los que desea realizar una copia de seguridad y haga clic en **Activar**.



Resultado

Backup a cloud empieza a realizar los backups iniciales de cada volumen seleccionado.

El futuro

"Es posible gestionar backups si se cambia la programación de backup, se restauran los volúmenes, etc.".

Realizar backups de datos desde un sistema ONTAP en las instalaciones en la cloud

Complete algunos pasos para empezar a realizar backups de datos desde su sistema ONTAP en las instalaciones al almacenamiento de objetos de bajo coste en el cloud.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

Verifique la compatibilidad con la configuración

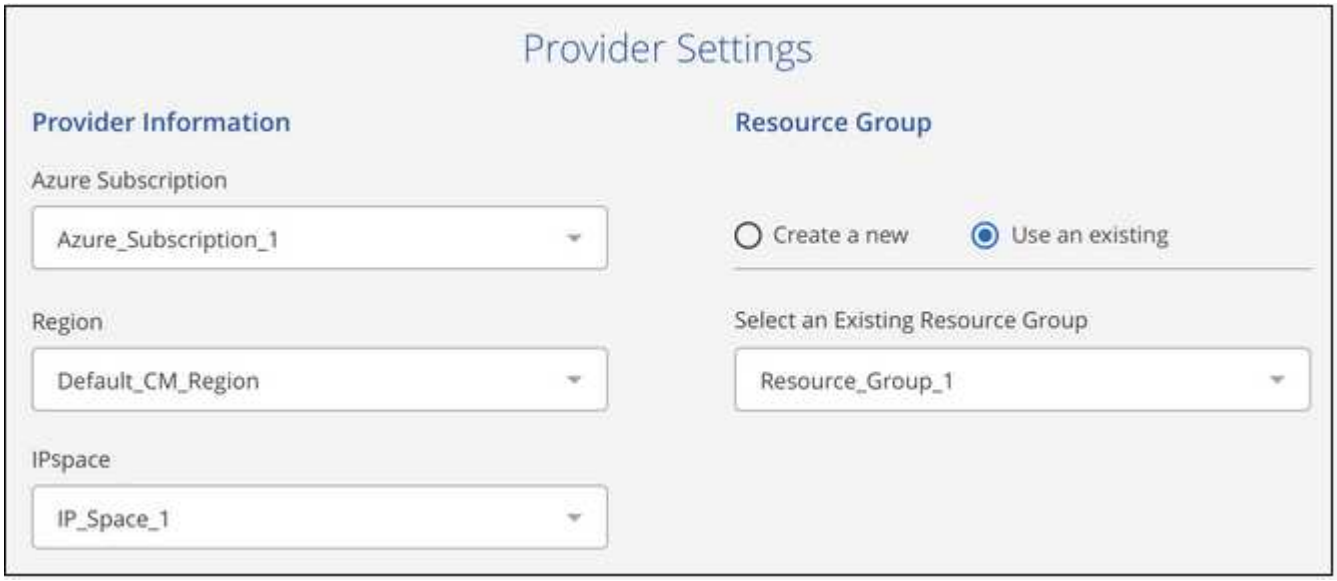
- Ha detectado el clúster en las instalaciones y lo ha añadido a un entorno de trabajo en Cloud Manager. Consulte "Detección de clústeres de ONTAP" para obtener más detalles.
- Utiliza ONTAP 9.7P5 o una versión posterior en el clúster.
- Dispone de una suscripción de proveedor de cloud válida para el espacio de almacenamiento en el que se ubicará los backups.
- Se ha suscrito a "Oferta de Cloud Manager Marketplace Backup", o usted ha comprado "y activado" Una licencia BYOL de backup en cloud de NetApp.

Habilite Backup en el sistema

Seleccione el entorno de trabajo y haga clic en **Activar** junto al servicio copia de seguridad en la nube en el panel derecho y, a continuación, siga el asistente de configuración.

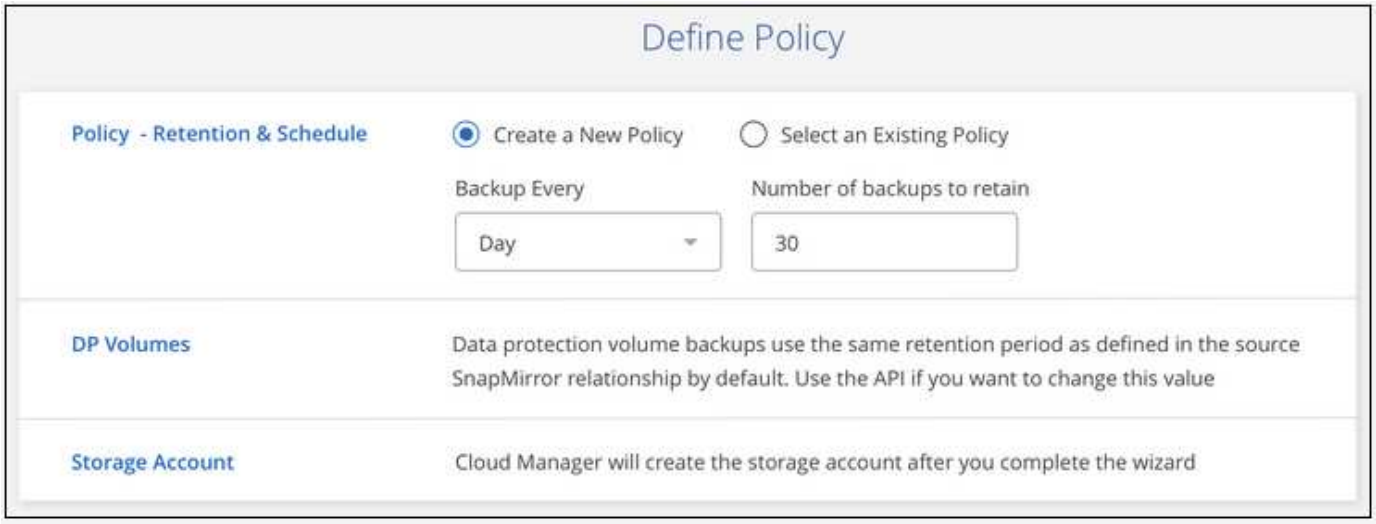
Seleccione el proveedor de cloud e introduzca los detalles del proveedor

Seleccione el proveedor y, a continuación, seleccione la suscripción al proveedor, la región y el grupo de recursos. También debe especificar el espacio IP del clúster de ONTAP en el que residen los volúmenes.



Defina la política de backup

La política predeterminada realiza backups de volúmenes todos los días y conserva las 30 copias de backup más recientes de cada volumen. Cambie a backups semanales o mensuales, o seleccione una de las políticas definidas por el sistema que proporcionan más opciones.

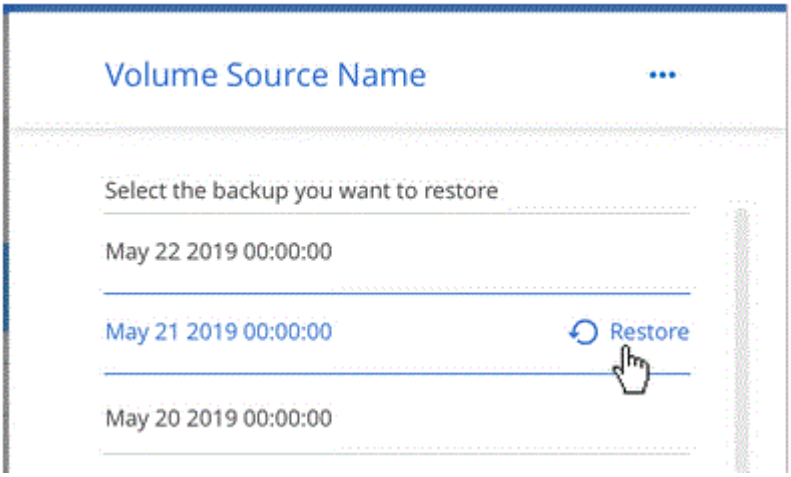


5 Seleccione los volúmenes de los que desea realizar el backup

Identifique los volúmenes de los que desea realizar backup desde el clúster.

6 Restaure sus datos, según sea necesario

En la lista de backups, seleccione un volumen, seleccione un backup y, a continuación, restaure datos del backup en un volumen nuevo en un sistema Cloud Volumes ONTAP que utilice el mismo proveedor de cloud.



Requisitos

Lea los siguientes requisitos para asegurarse de que tiene una configuración compatible antes de empezar a realizar backups de volúmenes en un almacenamiento de Azure Blob.

Versiones de ONTAP compatibles

ONTAP 9.7P5 y posterior.

Requisitos para la red de clúster

Se requiere una LIF de interconexión de clústeres en cada nodo ONTAP donde se alojan los volúmenes en los que se desea incluir. La LIF debe estar asociada al *IPspace* que ONTAP debería utilizar para conectarse al almacenamiento de objetos. La SVM de administrador debe residir en el espacio IP. "Obtenga más información acerca de los espacios IP".

Cuando configura el backup en la nube, se le solicita que utilice el espacio IP. Debe elegir el espacio IP al que está asociada cada LIF. Puede ser el espacio IP «predeterminado» o un espacio IP personalizado que haya creado.

Regiones de Azure compatibles

El backup en cloud es compatible en todas las regiones de Azure "donde se admiten cloud volumes".

Requisitos de licencia

Para las licencias de Backup to Cloud PAYGO, una suscripción a "Oferta de backup de Azure Marketplace Cloud Manager" Es necesario antes de habilitar Backup en el cloud. La facturación de Backup en Cloud se realiza mediante esta suscripción.

Para las licencias de BYOL de backup a cloud, necesita el número de serie de NetApp que le permite usar el servicio durante la duración y la capacidad de la licencia. Consulte "Adición y actualización de su licencia BYOL de copia de seguridad".

Además, necesita tener una suscripción a Microsoft Azure para el espacio de almacenamiento en el que se ubicará los backups.

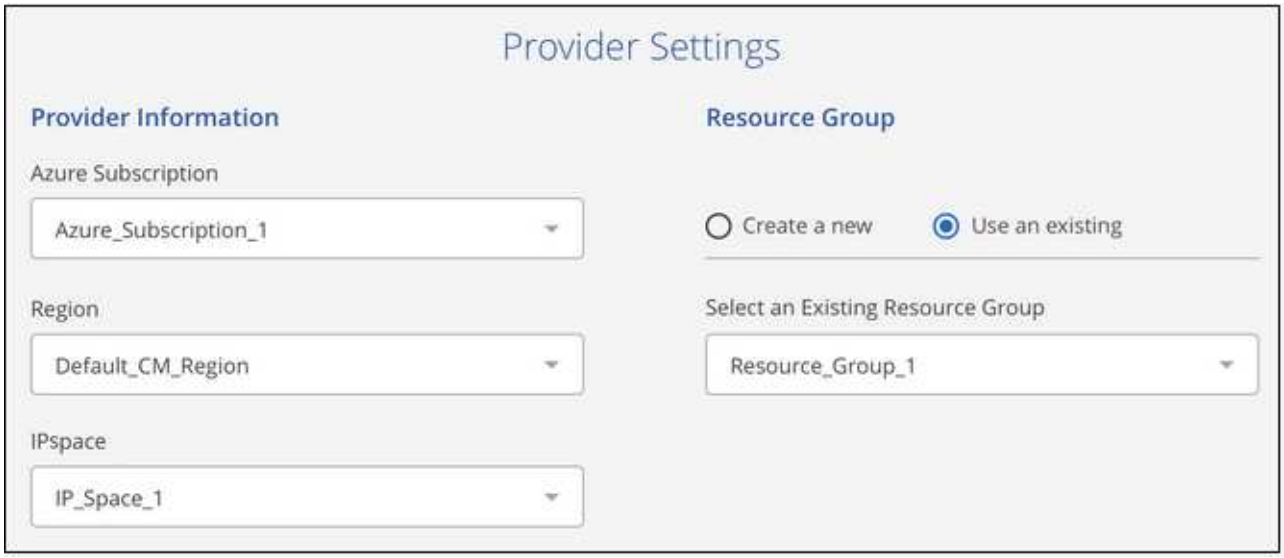
Habilitación de Backup en el cloud

Active Backup en el cloud en cualquier momento directamente desde el entorno de trabajo.

Pasos

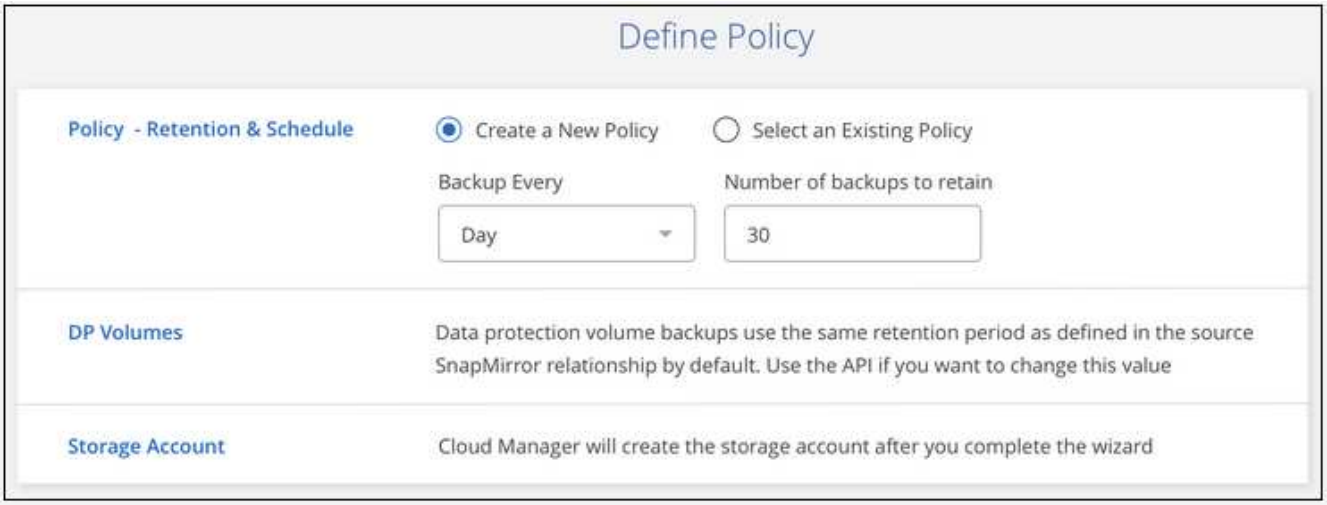
1. Seleccione el entorno de trabajo y haga clic en **Activar** junto al servicio copia de seguridad en la nube en el panel derecho.

2. Seleccione el proveedor y, a continuación, introduzca los detalles del proveedor:
   a. La suscripción de Azure utilizada para almacenar los backups.
   b. La región de Azure.
   c. El grupo de recursos: Es posible crear un nuevo grupo de recursos, o bien seleccionar y existente.
   d. El espacio IP del clúster de ONTAP en el que residen los volúmenes de los que desea realizar backup.
   e. Y, a continuación, haga clic en **continuar**.



Tenga en cuenta que no puede cambiar la suscripción ni el grupo de recursos después de que se hayan iniciado los servicios.

3. En la página *define Policy*, seleccione el programa de copia de seguridad y el valor de retención y haga clic en **continuar**.



Consulte "la lista de políticas existentes".

4. Seleccione los volúmenes de los que desea realizar una copia de seguridad y haga clic en **Activar**.

Resultado

Backup a cloud empieza a realizar los backups iniciales de cada volumen seleccionado.

El futuro

"Es posible gestionar backups si se cambia la programación de backup, se restauran los volúmenes, etc.".

Administración de backups para sistemas Cloud Volumes ONTAP y ONTAP en las instalaciones

Gestione backups para sistemas Cloud Volumes ONTAP y ONTAP en las instalaciones cambiando la programación de backup, restaurar volúmenes, eliminar backups, etc.

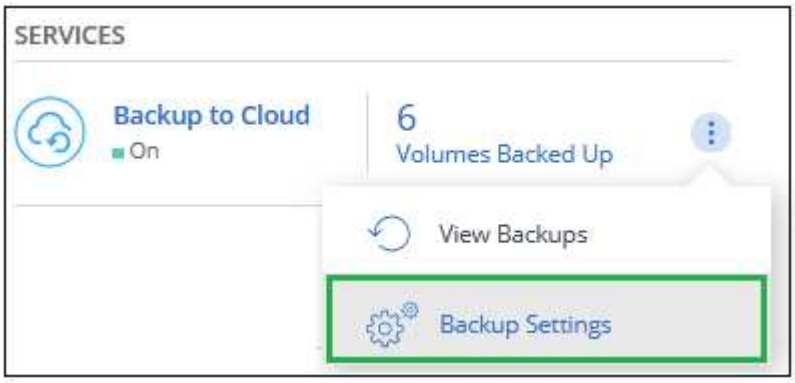
Cambiar la programación y la retención de backups

La política predeterminada realiza backups de volúmenes todos los días y conserva las 30 copias de backup más recientes de cada volumen. Puede cambiar a los backups semanales o mensuales y puede cambiar la cantidad de copias de backup que desea retener. También se puede seleccionar una de las políticas definidas por el sistema que proporcione backups programados para 3 meses, 1 año y 7 años.

Cambiar la política de backup afecta solo a los volúmenes nuevos creados después de cambiar la programación. No afecta a la programación de ningún volumen existente.

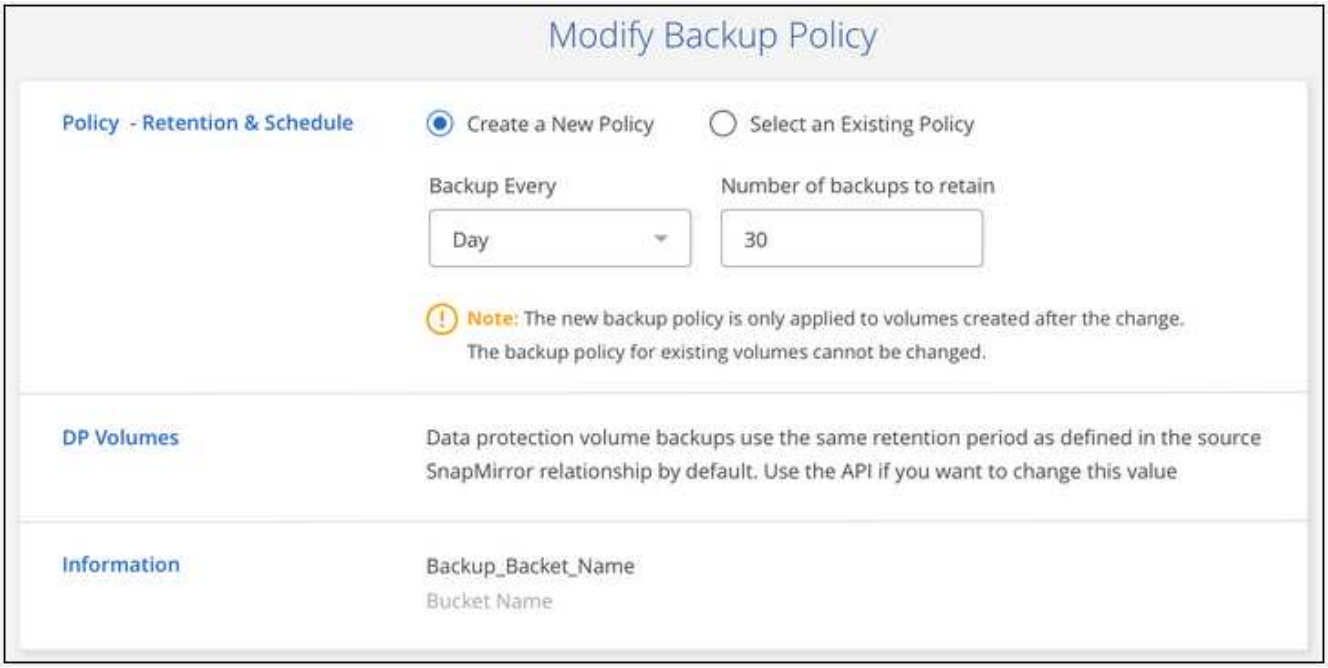
Pasos

1. Seleccione el entorno de trabajo.
2. Haga clic en Y seleccione **Configuración de copia de seguridad**.



3. En la página *Backup Settings*, haga clic en ••• Para el entorno de trabajo y seleccione **Modificar la política de copia de seguridad**.

4. En la página *Modify Backup Policy*, cambie la programación y la retención de copias de seguridad y, a continuación, haga clic en **Guardar**.



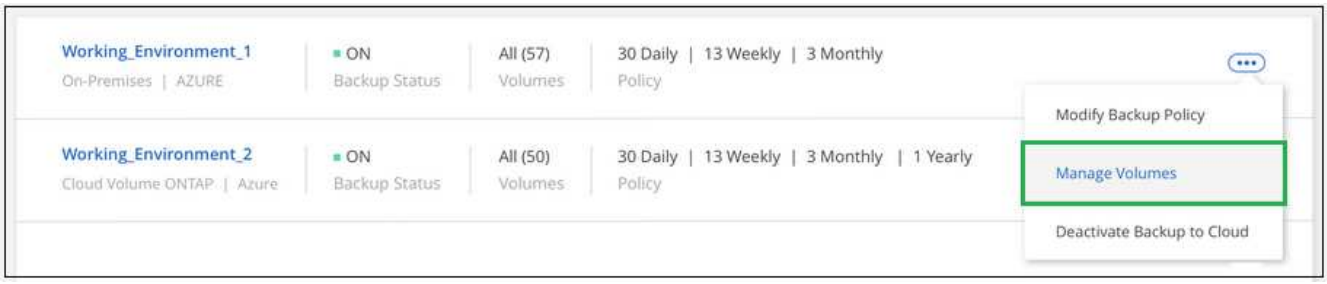
Iniciar y detener backups de volúmenes

Puede detener el backup de un volumen si no necesita copias de backup de ese volumen, y no quiere pagar por el coste de almacenar los backups. También puede añadir un nuevo volumen a la lista de backups si actualmente no se está realizando un backup.

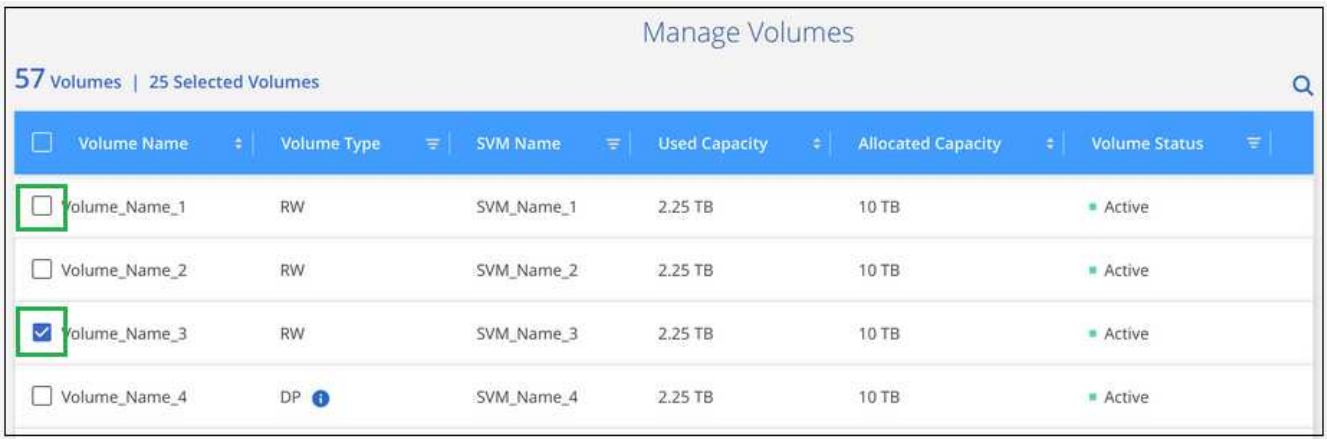
Pasos

1. Seleccione el entorno de trabajo.
2. Haga clic en Y seleccione **Configuración de copia de seguridad**.

3. En la página *Backup Settings*, haga clic en ••• Para el entorno de trabajo y seleccione **gestionar volúmenes**.



4. Seleccione la casilla de comprobación para los volúmenes que desea iniciar el backup y anule la selección de la casilla de comprobación para los volúmenes que desea detener el backup.



Nota: cuando detenga la copia de seguridad de un volumen, lo hará siga cobrándose por su proveedor de cloud por el objeto costes de almacenamiento de la capacidad que utilizan los backups a menos que usted eliminar los backups.

Restaurar un volumen a partir de un backup

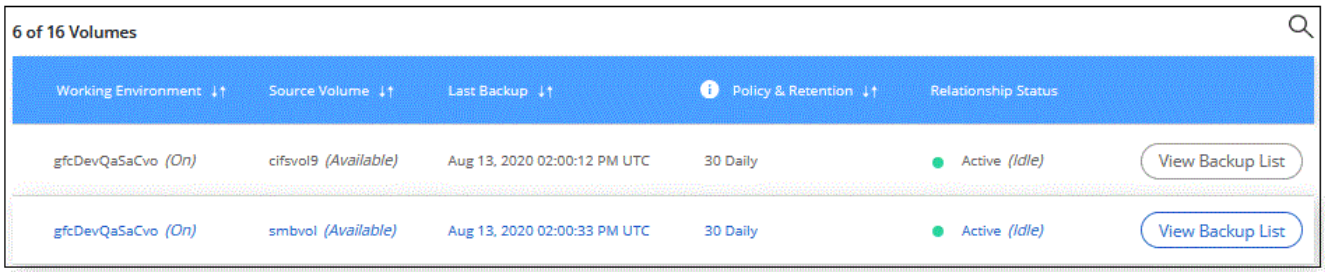
Al restaurar datos de una copia de seguridad, Cloud Manager crea un volumen *new* con los datos de la copia de seguridad. Puede restaurar los datos en un volumen del mismo entorno de trabajo o en otro entorno de trabajo ubicado en la misma cuenta de cloud que el entorno de trabajo de origen. Como el backup no contiene ninguna copia de Snapshot, el volumen recién restaurado tampoco.

Los backups creados a partir de sistemas ONTAP en las instalaciones solo se pueden restaurar en sistemas Cloud Volumes ONTAP que utilicen el mismo proveedor de cloud donde reside el backup.

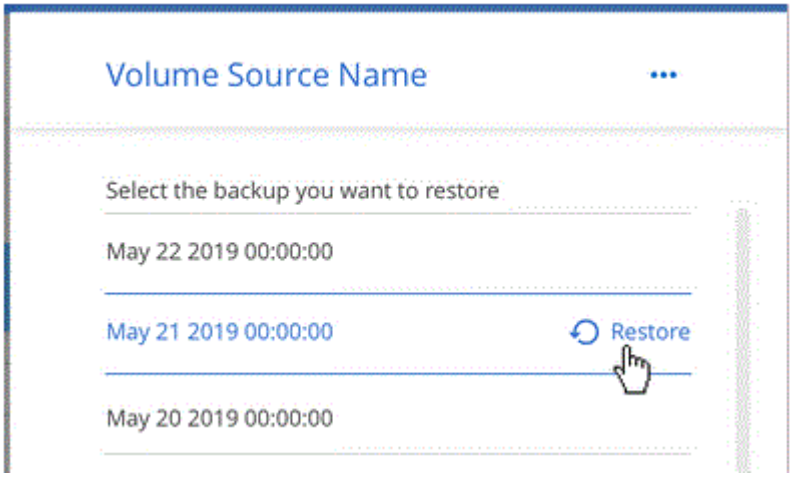
Pasos

1. Seleccione el entorno de trabajo.
2. Haga clic en Y seleccione **Ver copias de seguridad**.

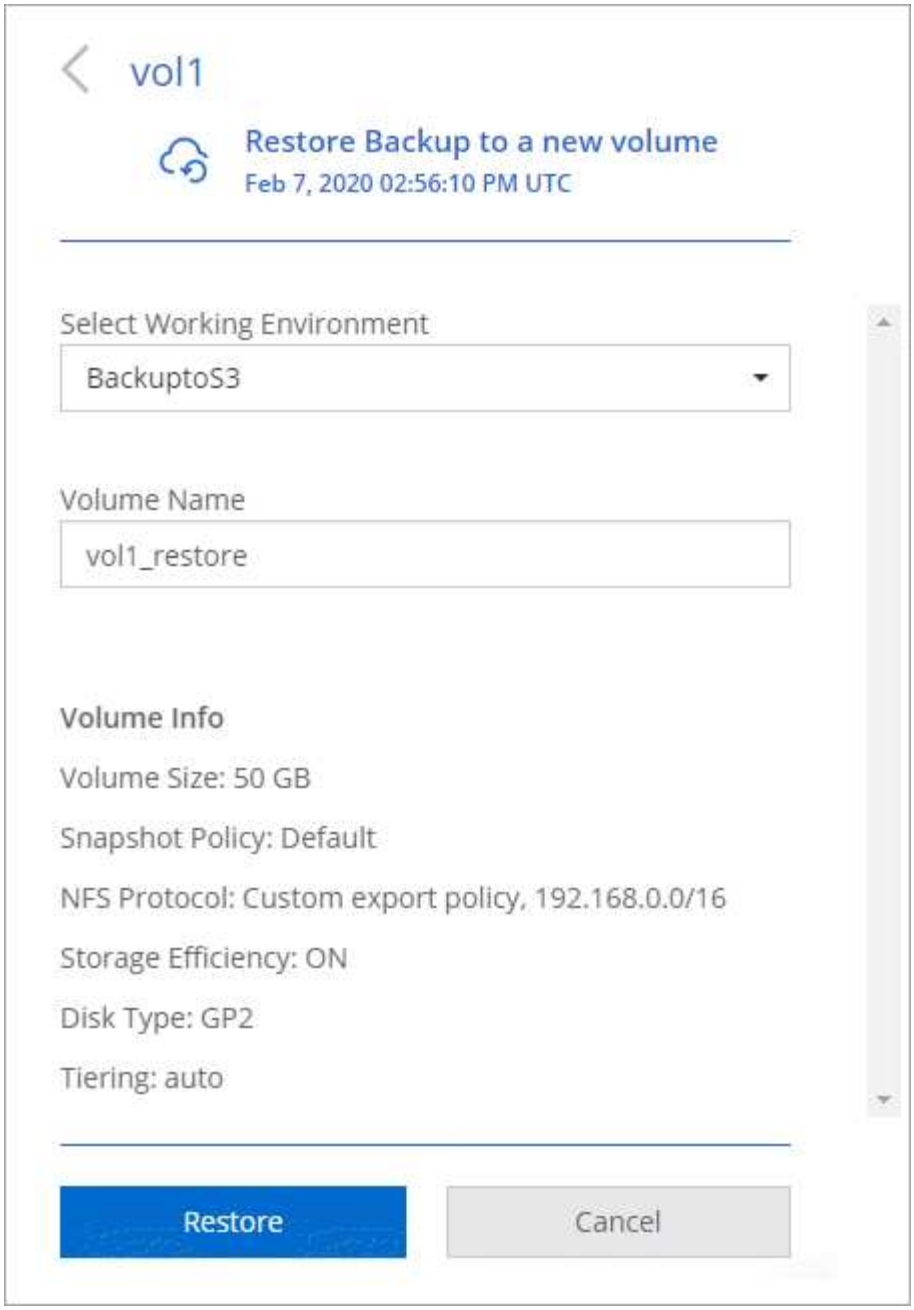
3. Seleccione la fila del volumen que desea restaurar y haga clic en **Ver lista de copias de seguridad**.



4. Busque la copia de seguridad que desea restaurar y haga clic en el icono **Restaurar**.



5. Rellene la página *Restore Backup to new volume*:
   a. Seleccione el entorno de trabajo al que desea restaurar el volumen.
   b. Escriba un nombre para el volumen.
   c. Haga clic en **Restaurar**.



Resultado

Cloud Manager crea un nuevo volumen según el backup seleccionado. Puede hacerlo "gestione este nuevo volumen" según sea necesario.

Eliminar backups

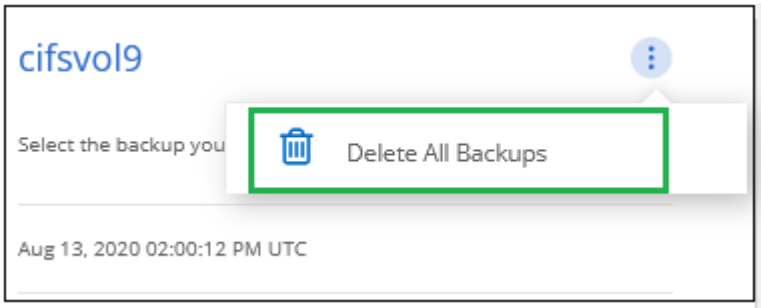
Backup to Cloud le permite eliminar *All* copias de seguridad de un volumen específico. No puede eliminar copias de seguridad *individual*.

Es posible hacerlo si ya no necesita los backups o si se eliminó el volumen de origen y desea quitar todos los backups.

Si piensa eliminar un sistema Cloud Volumes ONTAP o ONTAP en las instalaciones que tiene copias de seguridad, debe eliminar las copias de seguridad **antes de** eliminar el sistema. Copia de seguridad en la nube no elimina automáticamente las copias de seguridad cuando elimina un sistema, y no hay compatibilidad actual en la interfaz de usuario para eliminar las copias de seguridad después de que el sistema haya sido eliminado.

Pasos

1. En la parte superior de Cloud Manager, haga clic en **copia de seguridad**.
2. En la lista de volúmenes, busque el volumen y haga clic en **Ver lista de copias de seguridad**.
3. Haga clic en ••• Y seleccione **Eliminar todas las copias de seguridad**.



4. En el cuadro de diálogo de confirmación, haga clic en **Eliminar**.

Deshabilitación de Backup to Cloud

Al deshabilitar Backup en Cloud para un entorno de trabajo, se desactivan los backups de cada volumen en el sistema y también se deshabilita la capacidad para restaurar un volumen. No se eliminarán los backups existentes.

Tenga en cuenta que el proveedor de cloud seguirá facturando los costes de almacenamiento de objetos por la capacidad que utilicen sus backups a menos que elimine los backups.

Pasos

1. Seleccione el entorno de trabajo.
2. Haga clic en ⋮ Y seleccione **Configuración de copia de seguridad**.

3. En la página *Backup Settings*, haga clic en ••• Para el entorno de trabajo y seleccione **Desactivar copia de seguridad en la nube**.

4. En el cuadro de diálogo de confirmación, haga clic en **Desactivar**.

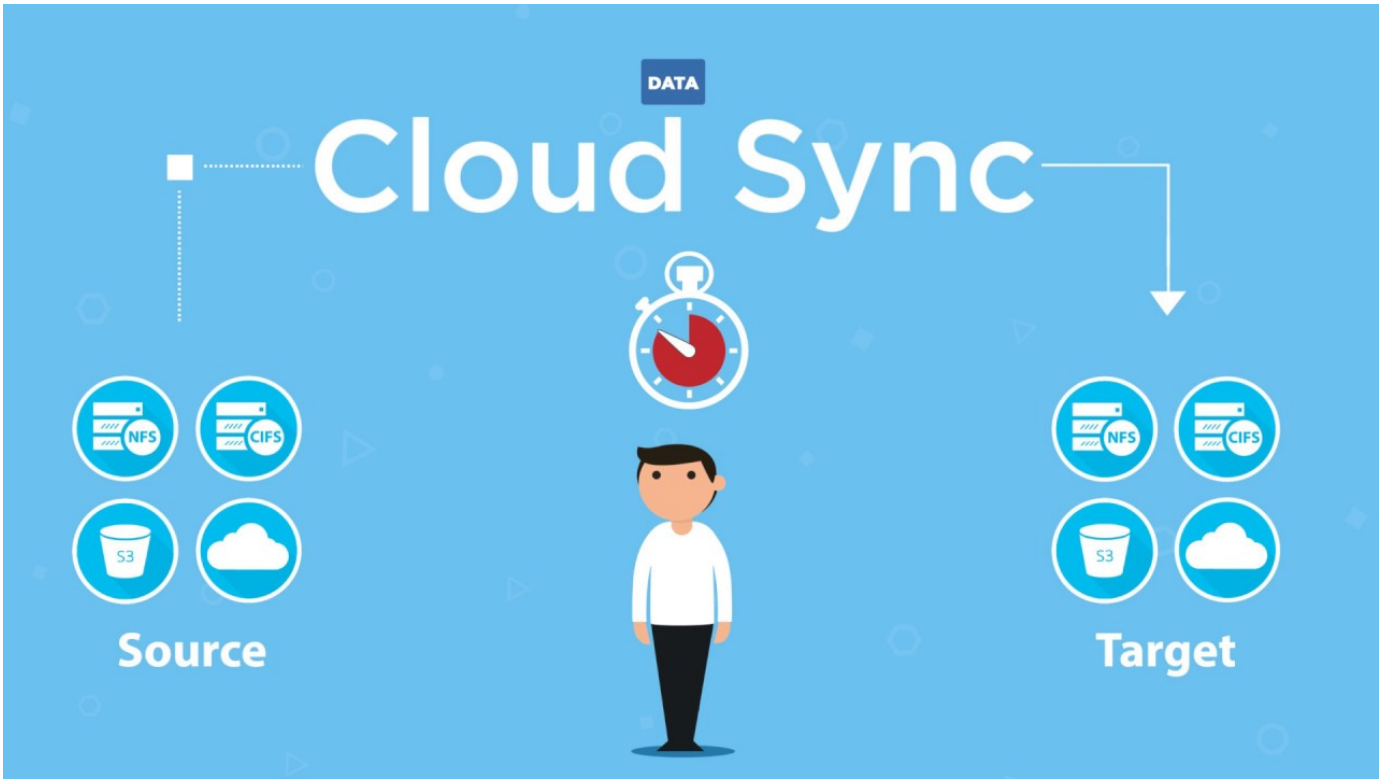
Copiar y sincronizar datos

Información general de Cloud Sync

El servicio Cloud Sync de NetApp ofrece una forma sencilla, segura y automatizada de migrar sus datos a cualquier destino, tanto en el cloud como en las instalaciones. Tanto si se trata de un conjunto de datos NAS basado en archivos (NFS o SMB), un formato de objeto Amazon simple Storage Service (S3), un dispositivo StorageGRID® de NetApp o cualquier otro almacén de objetos de proveedores de cloud, Cloud Sync puede convertirlo y moverlo por usted.

Funciones

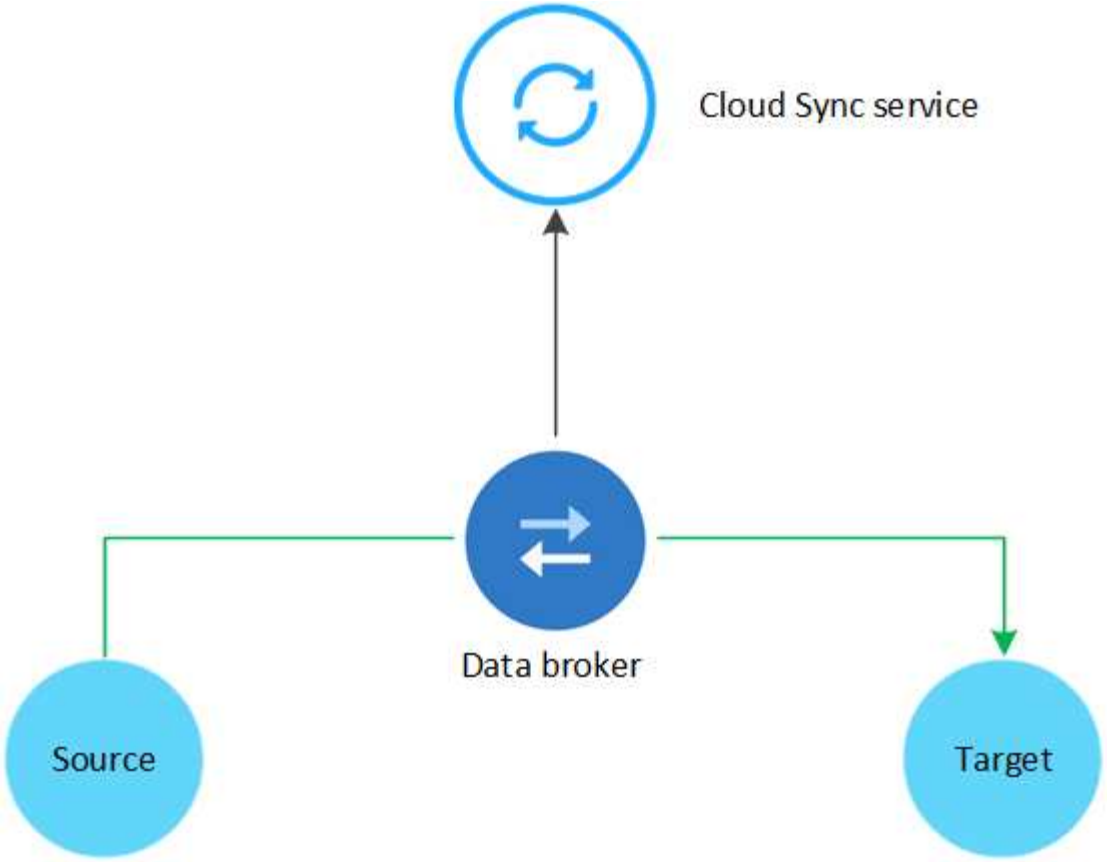
Vea el siguiente vídeo para obtener información general sobre Cloud Sync:



Cómo funciona Cloud Sync

Cloud Sync es una plataforma de software como servicio (SaaS) que consta de un agente de datos, una interfaz basada en cloud disponible a través de Cloud Manager y un origen y un destino.

En la siguiente imagen, se muestra la relación entre los componentes de Cloud Sync:



El software de agente de datos de NetApp sincroniza los datos de un origen con un destino (lo que se denomina *Sync Relationship*). Puede ejecutar el agente de datos en AWS, Azure, Google Cloud Platform o en sus instalaciones. El agente de datos necesita una conexión a Internet saliente a través del puerto 443 para que pueda comunicarse con el servicio Cloud Sync y ponerse en contacto con otros servicios y repositorios. "Consulte la lista de extremos".

Después de la copia inicial, el servicio sincroniza los datos modificados con la programación que se haya establecido.

Tipos de almacenamiento admitidos

Cloud Sync admite los siguientes tipos de almacenamiento:

- Cualquier servidor NFS
- Cualquier servidor SMB
- EFS DE AWS
- AWS S3
- Azure Blob
- Azure NetApp Files
- Cloud Volumes Service
- Cloud Volumes ONTAP
- Google Cloud Storage
- Almacenamiento de objetos en cloud de IBM

- Clúster de ONTAP en las instalaciones
- Almacenamiento ONTAP S3
- StorageGRID

"Revise las relaciones de sincronización compatibles".

Coste

Existen dos tipos de costes asociados con el uso de Cloud Sync: Cargos por recursos y cargos por servicios.

Cargos por recursos

Los cargos por recursos están relacionados con los costes de cómputo y almacenamiento para ejecutar el agente de datos en el cloud.

Cargos por servicio

Hay dos formas de pagar las relaciones de sincronización después de que termine su prueba gratuita de 14 días. La primera opción es suscribirse a AWS o Azure, lo que permite pagar por horas o anualmente. La segunda opción consiste en comprar licencias directamente a NetApp. Lea las secciones siguientes para obtener más información.

Suscripción a Marketplace

Al suscribirse al servicio de Cloud Sync de AWS o Azure, usted podrá pagar por horas o pagar anualmente. "Puede suscribirse a través de AWS o Azure", en función de dónde desee facturar.

Suscripciones por horas

Con una suscripción de pago por horas, el servicio Cloud Sync cobra por hora en función del número de relaciones de sincronización que cree.

- "Ver los precios en Azure"
- "Vea los precios de pago por uso en AWS"

Suscripciones anuales

Una suscripción anual proporciona una licencia para 20 relaciones de sincronización que usted paga por adelantado. Si va por encima de 20 relaciones de sincronización y se ha suscrito a Azure, pagará por las relaciones adicionales por horas.

"Ver precios anuales en AWS"

De NetApp

Otra forma de pagar por las relaciones de sincronización es mediante la compra de licencias directamente a NetApp. Cada licencia permite crear hasta 20 relaciones de sincronización.

Puede usar estas licencias con una suscripción a AWS o Azure. Por ejemplo, si tiene 25 relaciones de sincronización, puede pagar las primeras 20 relaciones de sincronización con una licencia y, a continuación, pagar por el uso desde AWS o Azure con las 5 relaciones de sincronización restantes.

"Aprenda a comprar licencias y a añadirlas a cloud Sincr".

Términos de licencia

Los clientes que adquieran una licencia propia (BYOL) para el servicio Cloud Sync deben conocer las limitaciones asociadas con el derecho de la licencia.

- Los clientes tienen derecho a aprovechar la licencia BYOL por un período que no supere un año a partir de la fecha de entrega.
- Los clientes tienen derecho a aprovechar la licencia BYOL para establecer y no superar un total de 20 conexiones individuales entre un origen y un destino (cada una de ellas una “relación de sincronización”).
- El derecho de un cliente expira al finalizar el plazo de un año para la licencia, independientemente de si el cliente ha alcanzado la limitación de relación de sincronización de 20.
- En el caso de que el Cliente decida renovar su licencia, las relaciones de sincronización no utilizadas asociadas a la concesión de licencia anterior NO se reviertan a la renovación de la licencia.

Privacidad de datos

NetApp no tiene acceso a ninguna credencial que proporcione mientras utiliza el servicio Cloud Sync. Las credenciales se almacenan directamente en el equipo de Data broker, que reside en la red.

Según la configuración seleccionada, Cloud Sync puede pedirle credenciales cuando cree una nueva relación. Por ejemplo, cuando se configura una relación que incluye un servidor SMB o cuando se implementa el agente de datos en AWS.

Estas credenciales siempre se guardan directamente en el propio agente de datos. El agente de datos reside en un equipo de su red, ya sea en las instalaciones o en su cuenta de cloud. NetApp nunca pone a disposición de estas credenciales.

Las credenciales se cifran localmente en la máquina de corredores de datos utilizando HashiCorp Vault.

Limitaciones

- Cloud Sync no es compatible con China.
- Además de China, el agente de datos de Cloud Sync no se ofrece en las siguientes regiones:
  - AWS GovCloud (EE. UU.)
  - Gobierno de Azure EE. UU
  - DoD de Azure US

Manos a la obra

Inicio rápido de Cloud Sync

Primeros pasos en el servicio Cloud Sync incluyen algunos pasos.

Prepare el origen y el destino

Compruebe que el origen y el destino son compatibles y están configurados. El requisito más importante es verificar la conectividad entre el agente de datos y las ubicaciones de origen y destino. "Leer más".

Prepare una ubicación para el agente de datos de NetApp

El software de agente de datos de NetApp sincroniza los datos de un origen con un destino (lo que se denomina *Sync Relationship*). Puede ejecutar el agente de datos en AWS, Azure, Google Cloud Platform o en sus instalaciones. El agente de datos necesita una conexión a Internet saliente a través del puerto 443 para que pueda comunicarse con el servicio Cloud Sync y ponerse en contacto con otros servicios y repositorios. "Consulte la lista de extremos".

Cloud Sync le guía por el proceso de instalación cuando crea una relación de sincronización, en cuyo momento puede implementar el agente de datos en el cloud o descargar un script de instalación para su propio host Linux.

- "Revise la instalación de AWS"
- "Revise la instalación de Azure"
- "Revise la instalación de GCP"
- "Revise la instalación del host Linux"

Cree su primera relación de sincronización

Inicie sesión en "Cloud Manager", haga clic en **Sincronizar** y, a continuación, arrastre y suelte las selecciones para el origen y el destino. Siga las indicaciones para completar la configuración. "Leer más".

Pague por sus relaciones de sincronización una vez que finalice su prueba gratuita

Suscríbase a AWS o Azure para pagar según el uso o anualmente. O adquiera licencias directamente a NetApp. Sólo tiene que ir a la página Configuración de licencia de Cloud Sync para configurarlo. "Leer más".

Preparación del origen y del destino

Prepárese para sincronizar los datos mediante la verificación de que el origen y el destino son compatibles y la configuración.

Relaciones de sincronización compatibles

Cloud Sync le permite sincronizar datos de un origen a un destino (esto se denomina *SYNC Relationship*). Debe comprender las relaciones admitidas antes de comenzar.

Ubicación de origen	Ubicaciones de destino compatibles
EFS DE AWS	• EFS DE AWS • AWS S3 • Azure Blob • Azure NetApp Files (NFS) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • Almacenamiento de objetos en cloud de IBM • Google Cloud Storage • Servidor NFS • Clúster de ONTAP en las instalaciones • StorageGRID
AWS S3	• EFS DE AWS • AWS S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Almacenamiento de objetos en cloud de IBM • Google Cloud Storage • Servidor NFS • Clúster de ONTAP en las instalaciones • Servidor SMB • StorageGRID

Ubicación de origen	Ubicaciones de destino compatibles
Azure Blob	• EFS DE AWS • AWS S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • Almacenamiento de objetos en cloud de IBM • Servidor NFS • Clúster de ONTAP en las instalaciones • Servidor SMB • StorageGRID
Azure NetApp Files (NFS)	• EFS DE AWS • AWS S3 • Azure Blob • Azure NetApp Files (NFS) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • Almacenamiento de objetos en cloud de IBM • Google Cloud Storage • Servidor NFS • Clúster de ONTAP en las instalaciones • StorageGRID
Azure NetApp Files (SMB)	• AWS S3 • Azure Blob • Azure NetApp Files (SMB) • Cloud Volumes ONTAP (SMB) • Cloud Volumes Service (SMB) • Google Cloud Storage • Almacenamiento de objetos en cloud de IBM • Clúster de ONTAP en las instalaciones • Servidor SMB • StorageGRID

Ubicación de origen	Ubicaciones de destino compatibles
Cloud Volumes ONTAP (NFS)	• EFS DE AWS • AWS S3 • Azure Blob • Azure NetApp Files (NFS) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • Almacenamiento de objetos en cloud de IBM • Google Cloud Storage • Servidor NFS • Clúster de ONTAP en las instalaciones • StorageGRID
Cloud Volumes ONTAP (SMB)	• AWS S3 • Azure Blob • Azure NetApp Files (SMB) • Cloud Volumes ONTAP (SMB) • Cloud Volumes Service (SMB) • Google Cloud Storage • Almacenamiento de objetos en cloud de IBM • Clúster de ONTAP en las instalaciones • Servidor SMB • StorageGRID
Cloud Volumes Service (NFS)	• EFS DE AWS • AWS S3 • Azure Blob • Azure NetApp Files (NFS) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • Almacenamiento de objetos en cloud de IBM • Google Cloud Storage • Servidor NFS • Clúster de ONTAP en las instalaciones • StorageGRID

Ubicación de origen	Ubicaciones de destino compatibles
Cloud Volumes Service (SMB)	• AWS S3 • Azure Blob • Azure NetApp Files (SMB) • Cloud Volumes ONTAP (SMB) • Cloud Volumes Service (SMB) • Google Cloud Storage • Almacenamiento de objetos en cloud de IBM • Clúster de ONTAP en las instalaciones • Servidor SMB • StorageGRID
Google Cloud Storage	• EFS DE AWS • AWS S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • Almacenamiento de objetos en cloud de IBM • Servidor NFS • Clúster de ONTAP en las instalaciones • Servidor SMB • StorageGRID
Almacenamiento de objetos en cloud de IBM	• EFS DE AWS • AWS S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • Almacenamiento de objetos en cloud de IBM • Servidor NFS • Clúster de ONTAP en las instalaciones • Servidor SMB • StorageGRID

Ubicación de origen	Ubicaciones de destino compatibles
Servidor NFS	• EFS DE AWS • AWS S3 • Azure Blob • Azure NetApp Files (NFS) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • Almacenamiento de objetos en cloud de IBM • Google Cloud Storage • Servidor NFS • Clúster de ONTAP en las instalaciones • StorageGRID
Clúster de ONTAP en las instalaciones (NFS)	• EFS DE AWS • AWS S3 • Azure Blob • Azure NetApp Files (NFS) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • Almacenamiento de objetos en cloud de IBM • Google Cloud Storage • Servidor NFS • Clúster de ONTAP en las instalaciones • StorageGRID
Clúster de ONTAP en las instalaciones (SMB)	• AWS S3 • Azure Blob • Azure NetApp Files (SMB) • Cloud Volumes ONTAP (SMB) • Cloud Volumes Service (SMB) • Google Cloud Storage • Almacenamiento de objetos en cloud de IBM • Clúster de ONTAP en las instalaciones • Servidor SMB • StorageGRID
Almacenamiento ONTAP S3	• StorageGRID

Ubicación de origen	Ubicaciones de destino compatibles
Servidor SMB	• AWS S3 • Azure Blob • Azure NetApp Files (SMB) • Cloud Volumes ONTAP (NFS) • Cloud Volumes Service (NFS) • Almacenamiento de objetos en cloud de IBM • Google Cloud Storage • Clúster de ONTAP en las instalaciones • Servidor SMB • StorageGRID
StorageGRID	• EFS DE AWS • AWS S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Almacenamiento de objetos en cloud de IBM • Google Cloud Storage • Servidor NFS • Clúster de ONTAP en las instalaciones • Almacenamiento ONTAP S3 • Servidor SMB • StorageGRID

Notas:

1. Puede elegir un nivel de almacenamiento específico de Azure Blob cuando un contenedor Blob es el destino:
    - Almacenamiento en caliente
    - Almacenamiento en frío
2. puede elegir un tipo de almacenamiento S3 específico cuando AWS S3 es el destino:
    - Estándar (esta es la clase predeterminada)
    - Organización en niveles inteligente
    - Acceso Estándar-poco frecuente
    - Una Zona de acceso poco frecuente
    - Glaciar

- Glacier Deep Archive

Redes para el origen y el destino

- El origen y el destino deben tener una conexión de red con el agente de datos.

  Por ejemplo, si un servidor NFS se encuentra en su centro de datos y el agente de datos se encuentra en AWS, necesitará una conexión de red (VPN o Direct Connect) desde su red hasta el VPC.

- NetApp recomienda configurar el origen, el destino y el intermediario de datos para utilizar un servicio de protocolo de tiempo de redes (NTP). La diferencia de tiempo entre los tres componentes no debe superar los 5 minutos.

Requisitos de origen y objetivo

Compruebe que el origen y los objetivos cumplen los siguientes requisitos.

requisitos de bloque de AWS S3

Asegúrese de que su bloque de AWS S3 cumpla con los siguientes requisitos.

Ubicaciones de agentes de datos compatibles para AWS S3

Las relaciones de sincronización que incluyen el almacenamiento S3 requieren un agente de datos implementado en AWS o en sus instalaciones. En cualquier caso, Cloud Sync le solicita que asocie el agente de datos con una cuenta de AWS durante la instalación.

- "Descubra cómo implementar el agente de datos de AWS"
- "Descubra cómo instalar el agente de datos en un Linux host"

Regiones admitidas de AWS

Todas las regiones están soportadas excepto las regiones China y GovCloud (EE.UU.).

Permisos necesarios para bloques de S3 en otras cuentas de AWS

Al configurar una relación de sincronización, puede especificar un bloque de S3 que resida en una cuenta de AWS que no esté asociado al agente de datos.

"Los permisos incluidos en este archivo JSON" Debe aplicarse a ese bloque de S3 para que el agente de datos pueda acceder a él. Estos permisos permiten al agente de datos copiar datos desde y hacia el bloque y enumerar los objetos del bloque.

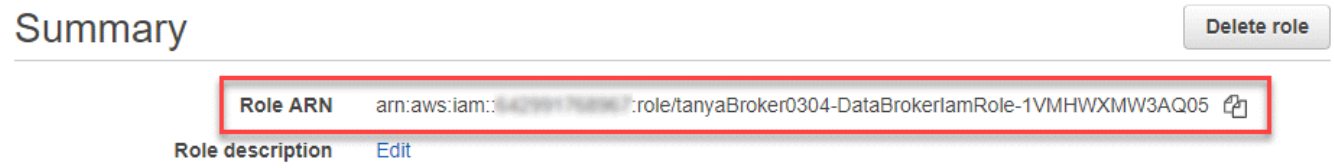
Tenga en cuenta lo siguiente acerca de los permisos incluidos en el archivo JSON:

1. *<BucketName>* es el nombre del bloque que reside en la cuenta de AWS que no está asociada con el agente de datos.
2. *<RoleARN>* debe sustituirse por uno de los siguientes:

   - Si el agente de datos se instaló manualmente en un host Linux, *RoleARN* debería ser el ARN del usuario de AWS para el que ha proporcionado credenciales de AWS al implementar el agente de datos.
   - Si el agente de datos se implementó en AWS mediante la plantilla CloudFormation, *RoleARN* debería

ser el ARN de la función IAM creada por la plantilla.

Para encontrar el rol ARN, vaya a la consola EC2, seleccione la instancia de Data broker y haga clic en el rol IAM en la pestaña Descripción. A continuación, debería ver la página Resumen de la consola del IAM que contiene el rol ARN.



requisitos de almacenamiento de Azure Blob

Asegúrese de que su almacenamiento de Azure Blob cumpla los siguientes requisitos.

Ubicaciones de agentes de datos compatibles para Azure Blob

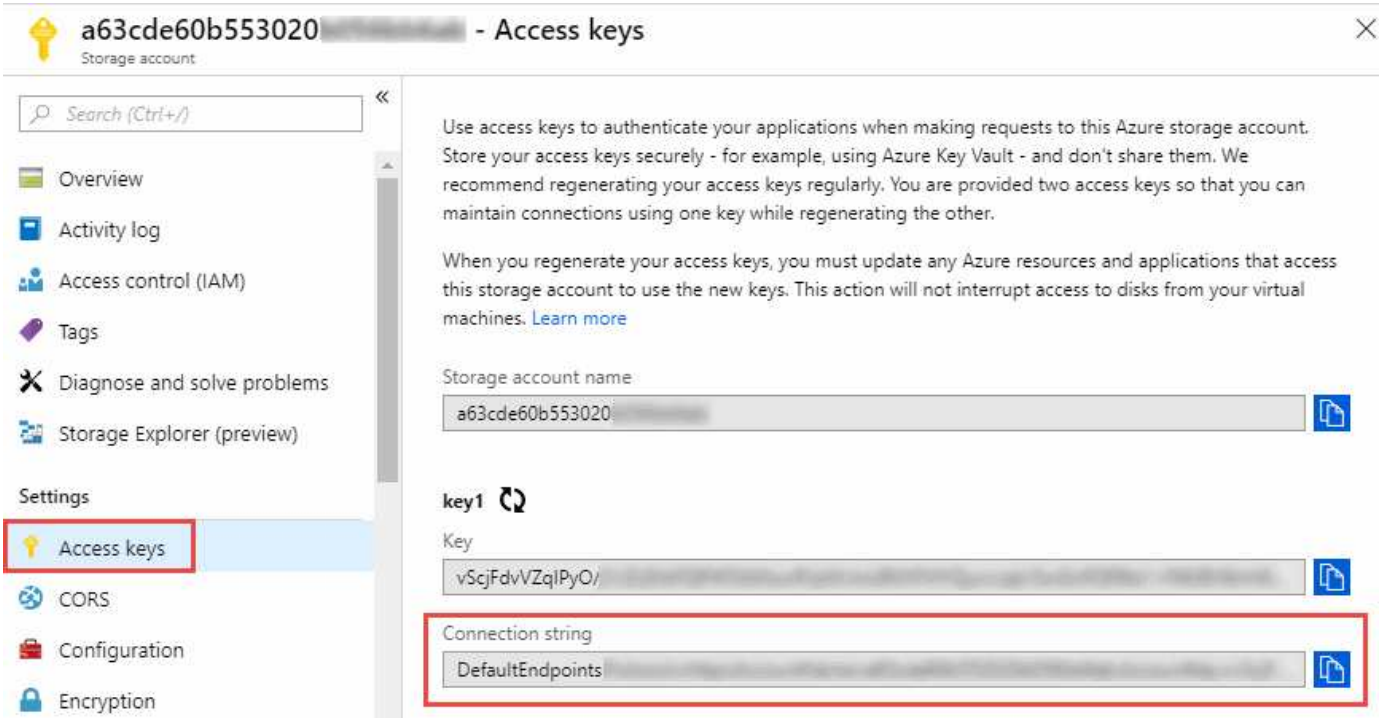
El agente de datos puede residir en cualquier ubicación cuando una relación de sincronización incluye el almacenamiento de Azure Blob.

Regiones de Azure compatibles

Todas las regiones cuentan con el apoyo de las regiones de China, la gobernadora de los Estados Unidos y el Departamento de Defensa de los Estados Unidos.

Se requiere una cadena de conexión para relaciones que incluyen Azure Blob y. NFS/SMB

A la hora de crear una relación de sincronización entre un contenedor de Azure Blob y un servidor NFS o SMB, debe proporcionar a Cloud Sync la cadena de conexión de la cuenta de almacenamiento:

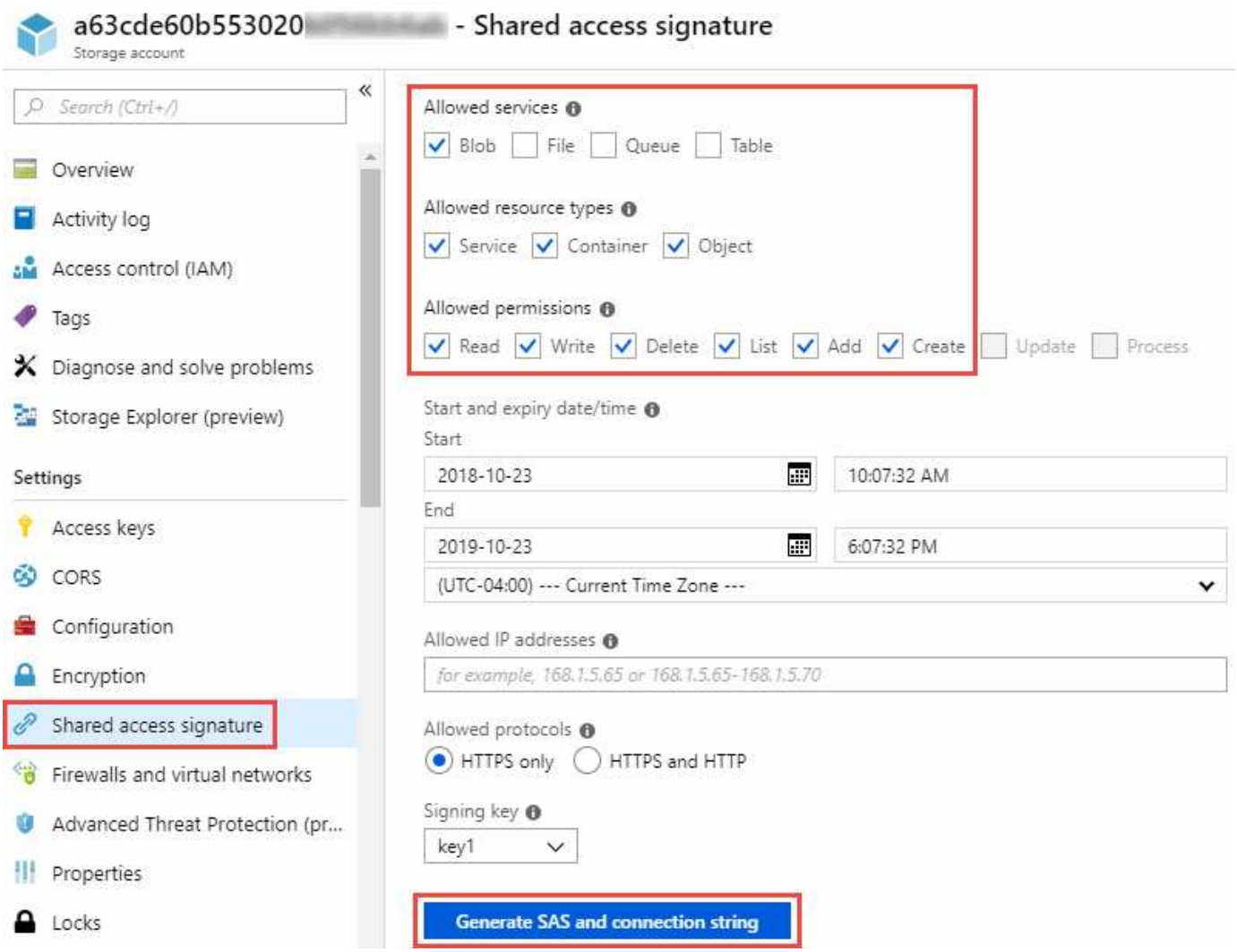


Si desea sincronizar datos entre dos contenedores de Azure Blob, la cadena de conexión debe incluir un

"firma de acceso compartido" (SAS). También tiene la opción de utilizar un SAS al sincronizar entre un contenedor Blob y un servidor NFS o SMB.

El SAS debe permitir el acceso al servicio Blob y todos los tipos de recursos (Servicio, contenedor y objeto). El SAS también debe incluir los siguientes permisos:

- Para el contenedor de fuente Blob: Leer y enumerar
- Para el contenedor de blob de destino: Leer, escribir, Lista, Agregar y Crear



Requisito de Azure NetApp Files

Utilice el nivel de servicio Premium o Ultra cuando sincronice datos con o desde Azure NetApp Files. Es posible que experimente errores y problemas de rendimiento si el nivel de servicio del disco es estándar.

Consulte a un arquitecto de soluciones si necesita ayuda para determinar el nivel de servicio adecuado. El tamaño del volumen y el nivel de volumen determinan el rendimiento que se puede obtener.

"Obtenga más información acerca de los niveles de servicio y el rendimiento de Azure NetApp Files".

Requisitos de bucket de Google Cloud Storage

Asegúrese de que su bloque de Google Cloud Storage cumpla con los siguientes requisitos.

Ubicaciones de agentes de datos compatibles para Google Cloud Storage

Las relaciones de sincronización que incluyen Google Cloud Storage requieren que un agente de datos se ponga en marcha en GCP o en sus instalaciones. Cloud Sync le guía por el proceso de instalación de Data broker cuando crea una relación de sincronización.

- "Descubra cómo implementar el agente de datos para GCP"
- "Descubra cómo instalar el agente de datos en un Linux host"

Regiones compatibles de GCP

Se admiten todas las regiones.

Requisitos del servidor NFS

- El servidor NFS puede ser un sistema de NetApp o un sistema que no sea de NetApp.
- El servidor de archivos debe permitir que el host de Data broker acceda a las exportaciones.
- Se admiten las versiones 3, 4.0, 4.1 y 4.2 de NFS.

  La versión deseada debe estar activada en el servidor.

- Si desea sincronizar datos NFS desde un sistema ONTAP, asegúrese de que el acceso a la lista de exportación NFS de una SVM esté habilitado (vserver nfs modify -vserver *svm_name* -showmount habilitado).

  La configuración predeterminada para showmount es *Enabled* a partir de ONTAP 9.2.

Requisitos de almacenamiento de S3 de ONTAP

ONTAP 9.7 admite Amazon simple Storage Service (Amazon S3) como vista previa pública. "Obtenga más información sobre la compatibilidad de ONTAP para Amazon S3".

Al configurar una relación de sincronización que incluya el almacenamiento de ONTAP S3, tendrá que proporcionar lo siguiente:

- La dirección IP de la LIF conectada a ONTAP S3
- La clave de acceso y la clave secreta configurada por ONTAP para usar

Requisitos del servidor SMB

- El servidor SMB puede ser un sistema de NetApp o un sistema distinto de NetApp.
- El servidor de archivos debe permitir que el host de Data broker acceda a las exportaciones.
- Se admiten las versiones 1.0, 2.0, 2.1, 3.0 y 3.11 de SMB.
- Conceda el grupo "Administradores" con permisos "Control total" a las carpetas de origen y destino.

  Si no otorga este permiso, es posible que el agente de datos no tenga permisos suficientes para obtener las ACL en un archivo o directorio. Si esto ocurre, recibirá el siguiente error: "Getxattr error 95"

Limitación de SMB para directorios y archivos ocultos

Una limitación de SMB afecta a directorios y archivos ocultos al sincronizar datos entre servidores SMB. Si alguno de los directorios o archivos del servidor SMB de origen se ocultó a través de Windows, el atributo oculto no se copiará al servidor SMB de destino.

Comportamiento de sincronización de SMB por limitación de falta de sensibilidad en caso

El protocolo SMB no distingue mayúsculas y minúsculas, lo que significa que las letras mayúsculas y minúsculas se tratan como las mismas. Este comportamiento puede provocar errores de copia de directorio y archivos sobrescritos si una relación de sincronización incluye un servidor SMB y los datos ya existen en el destino.

Por ejemplo, digamos que hay un archivo llamado "a" en el origen y un archivo llamado "A" en el destino. Cuando Cloud Sync copia el archivo denominado "a" en el destino, el archivo "A" se sobrescribe con el archivo "a" del origen.

En el caso de los directorios, digamos que hay un directorio llamado "b" en el origen y un directorio llamado "B" en el destino. Cuando Cloud Sync intenta copiar el directorio llamado "b" en el destino, Cloud Sync recibe un error que dice que el directorio ya existe. Como resultado, Cloud Sync siempre falla al copiar el directorio llamado “b.”.

La mejor manera de evitar esta limitación es asegurarse de que sincroniza los datos con un directorio vacío.

Permisos para un destino de SnapMirror

Si el origen de una relación de sincronización es un destino de SnapMirror (que es de solo lectura), los permisos de "lectura/lista" son suficientes para sincronizar los datos del origen en un destino.

Información general sobre redes para Cloud Sync

La conexión de red para Cloud Sync incluye la conectividad entre el agente de datos y las ubicaciones de origen y destino, y una conexión de Internet saliente desde el agente de datos a través del puerto 443.

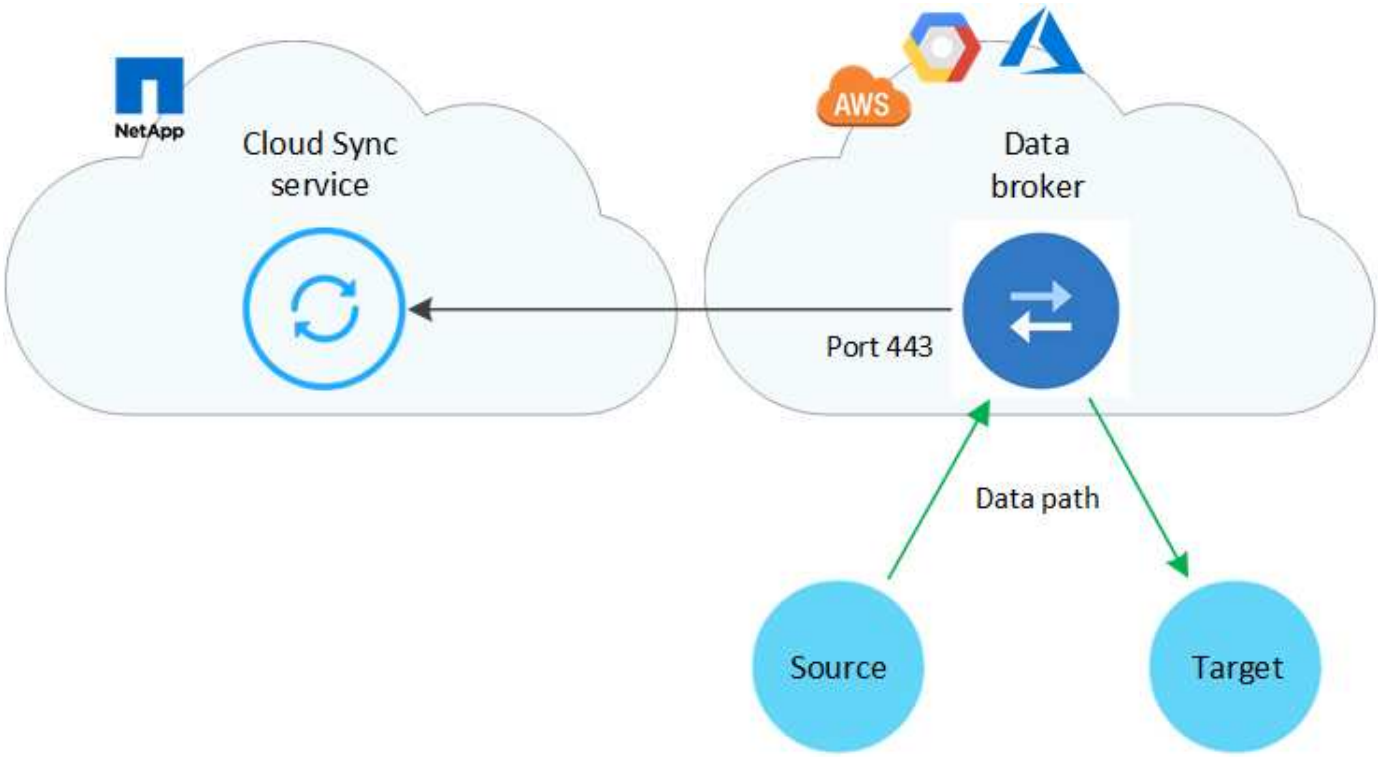
Ubicación de agente de datos

Puede instalar el agente de datos en el cloud o en sus instalaciones.

Agente de datos en el cloud

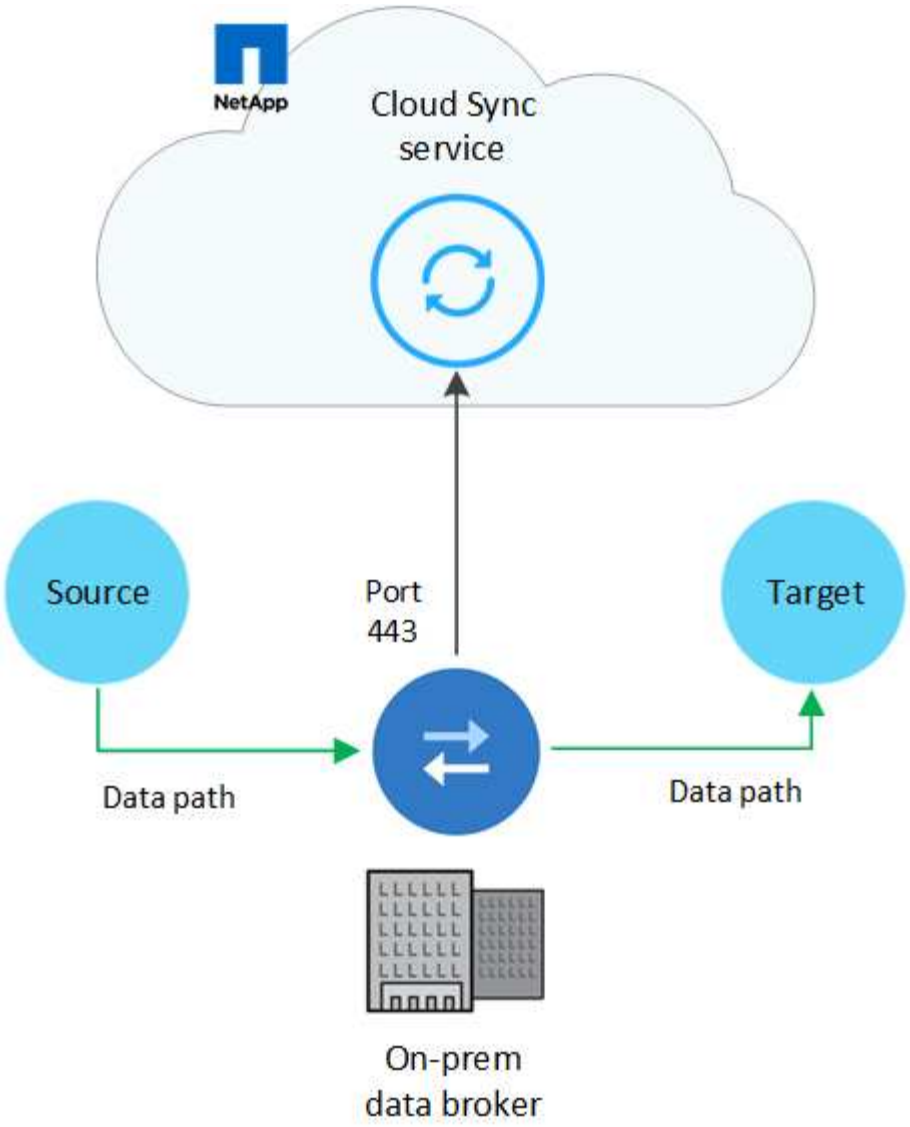
La siguiente imagen muestra el agente de datos que se ejecuta en el cloud, ya sea en AWS, GCP o Azure. El origen y el destino pueden encontrarse en cualquier ubicación, siempre que haya una conexión con el agente de datos. Por ejemplo, es posible que tenga una conexión VPN desde su centro de datos hacia su proveedor de cloud.

Cuando Cloud Sync implementa el agente de datos en AWS, Azure o GCP, crea un grupo de seguridad que permite las comunicaciones salientes necesarias.



Agente de datos en sus instalaciones

La siguiente imagen muestra el agente de datos que se ejecuta en las instalaciones, en un centro de datos. De nuevo, el origen y el destino pueden encontrarse en cualquier ubicación, siempre que haya una conexión con el agente de datos.



Requisitos de red

- El origen y el destino deben tener una conexión de red con el agente de datos.

  Por ejemplo, si un servidor NFS se encuentra en su centro de datos y el agente de datos se encuentra en AWS, necesitará una conexión de red (VPN o Direct Connect) desde su red hasta el VPC.

- El agente de datos necesita una conexión saliente a Internet para que pueda sondear el servicio Cloud Sync para las tareas a través del puerto 443.
- NetApp recomienda configurar el origen, el destino y el intermediario de datos para utilizar un servicio de protocolo de tiempo de redes (NTP). La diferencia de tiempo entre los tres componentes no debe superar los 5 minutos.

Extremos de red

El agente de datos de NetApp requiere acceso saliente a Internet a través del puerto 443 para comunicarse con el servicio Cloud Sync y ponerse en contacto con algunos otros servicios y repositorios. El explorador web local también requiere acceder a extremos para determinadas acciones. Si necesita limitar la conectividad saliente, consulte la siguiente lista de puntos finales al configurar el firewall para el tráfico saliente.

Extremos de Data broker

El agente de datos se pone en contacto con los siguientes extremos:

Puntos finales	Específico
olcentgbl.trafficmanager.net:443	Para ponerse en contacto con un repositorio para actualizar paquetes CentOS para el host de Data broker. Solo se puede contactar con este extremo si instala manualmente el agente de datos en un host CentOS.
rpm.nodesource.com:443 registry.npmjs.org:443 nodejs.org:443	Para ponerse en contacto con repositorios para actualizar los paquetes Node.js, npm y otros paquetes de terceros utilizados en desarrollo.
tgz.pm2.io:443	Para acceder a un repositorio para la actualización de Pm2, que es un paquete de terceros que se utiliza para supervisar Cloud Sync.
sqs.us-east-1.amazonaws.com:443 kinesis.us-east-1.amazonaws.com:443	Para ponerse en contacto con los servicios de AWS que Cloud Sync utiliza en las operaciones (poner en cola archivos, registrar acciones y entregar actualizaciones al agente de datos).
s3.*region*.amazonaws.com:443 por ejemplo: s3.us-east-2.amazonaws.com:443https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region["Consulte la documentación de AWS para obtener una lista de extremos de S3"^]	Para ponerse en contacto con Amazon S3 cuando una relación de sincronización incluya un bloque de S3.
cf.cloudsync.netapp.com:443 repo.cloudsync.netapp.com:443	Para ponerse en contacto con el servicio Cloud Sync.
support.netapp.com:443	Para ponerse en contacto con el soporte de NetApp cuando use una licencia BYOL para relaciones de sincronización.
fedoraproject.org:443	Para instalar 7z en la máquina virtual Data Broker durante la instalación y las actualizaciones. Es necesario enviar mensajes de AutoSupport al soporte técnico de NetApp.

Extremos del navegador web

El explorador web necesita acceder al siguiente extremo para descargar los registros con fines de solución de problemas:

logs.cloudsync.netapp.com:443

Cómo instalar un agente de datos

Instalar el agente de datos en AWS

Al crear una relación de sincronización, elija la opción AWS Data Broker para implementar el software de agente de datos en una nueva instancia de EC2 en un VPC. Cloud Sync le guía durante el proceso de instalación, pero en esta página se repiten los requisitos y los pasos que le ayudarán a preparar la instalación.

También tiene la opción de instalar el agente de datos en un host Linux existente en el cloud o en sus

instalaciones. "Leer más".

Regiones admitidas de AWS

Todas las regiones están soportadas excepto las regiones China y GovCloud (EE.UU.).

Requisitos de red

- El agente de datos necesita una conexión saliente a Internet para que pueda sondear el servicio Cloud Sync para las tareas a través del puerto 443.

  Cuando Cloud Sync implementa el agente de datos en AWS, crea un grupo de seguridad que permite la comunicación saliente necesaria. Tenga en cuenta que puede configurar el agente de datos para que utilice un servidor proxy durante el proceso de instalación.

  Si necesita limitar la conectividad saliente, consulte "lista de puntos finales con los que se contacta el data broker".

- NetApp recomienda configurar el origen, el destino y el intermediario de datos para utilizar un servicio de protocolo de tiempo de redes (NTP). La diferencia de tiempo entre los tres componentes no debe superar los 5 minutos.

Permisos necesarios para implementar el agente de datos en AWS

La cuenta de usuario de AWS que utiliza para implementar el el agente de datos debe tener los permisos incluidos en "Esta política proporcionada por NetApp".

requisitos para utilizar su propia función de IAM con el agente de datos de AWS

Cuando Cloud Sync implementa el Data broker, crea una función IAM para la instancia de Data broker. Si lo prefiere, puede implementar el agente de datos con su propio rol de IAM. Puede usar esta opción si su organización tiene políticas de seguridad estrictas.

El rol del IAM debe cumplir los siguientes requisitos:

- Se debe permitir al servicio EC2 asumir el rol IAM como entidad de confianza.
- "Los permisos definidos en este archivo JSON" Se debe adjuntar a la función IAM para que el intermediario de datos pueda funcionar correctamente.

Siga los pasos que se indican a continuación para especificar la función de IAM al implementar el agente de datos.

Instalación del Data broker

Puede instalar un agente de datos en AWS al crear una relación de sincronización.

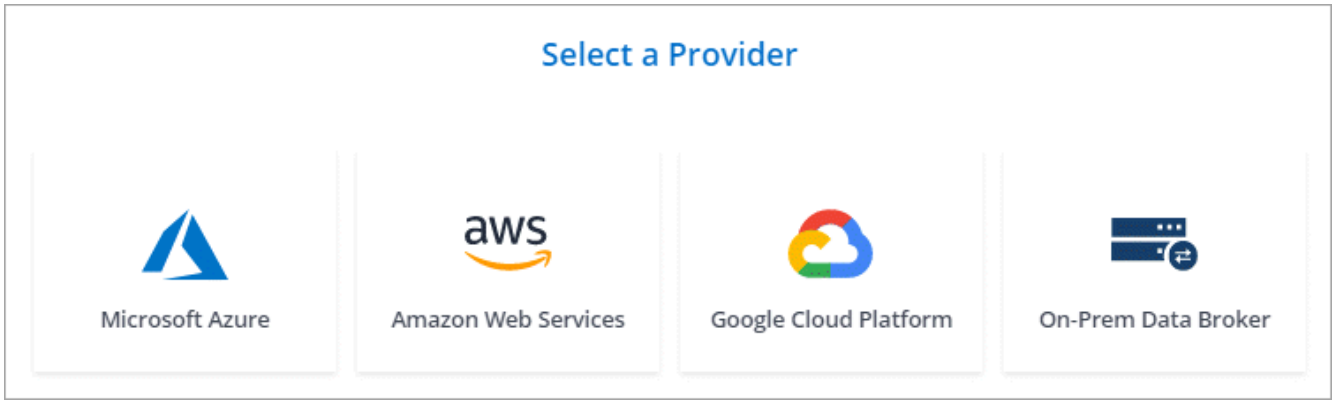
Pasos

1. Haga clic en **Crear nueva sincronización**.
2. En la página **definir relación de sincronización**, elija un origen y un destino y haga clic en **continuar**.

   Complete los pasos hasta llegar a la página **Data Broker**.

3. En la página **Data Broker**, haga clic en **Crear Data Broker** y, a continuación, seleccione **Amazon Web Services**.

Si ya tiene un agente de datos, tendrá que hacer clic en el + icono primero.



4. Introduzca un nombre para el Data broker y haga clic en **continuar**.
5. Introduzca una clave de acceso de AWS para que Cloud Sync pueda crear el agente de datos en AWS en su nombre.

   Las teclas no se guardan ni utilizan para ningún otro propósito.

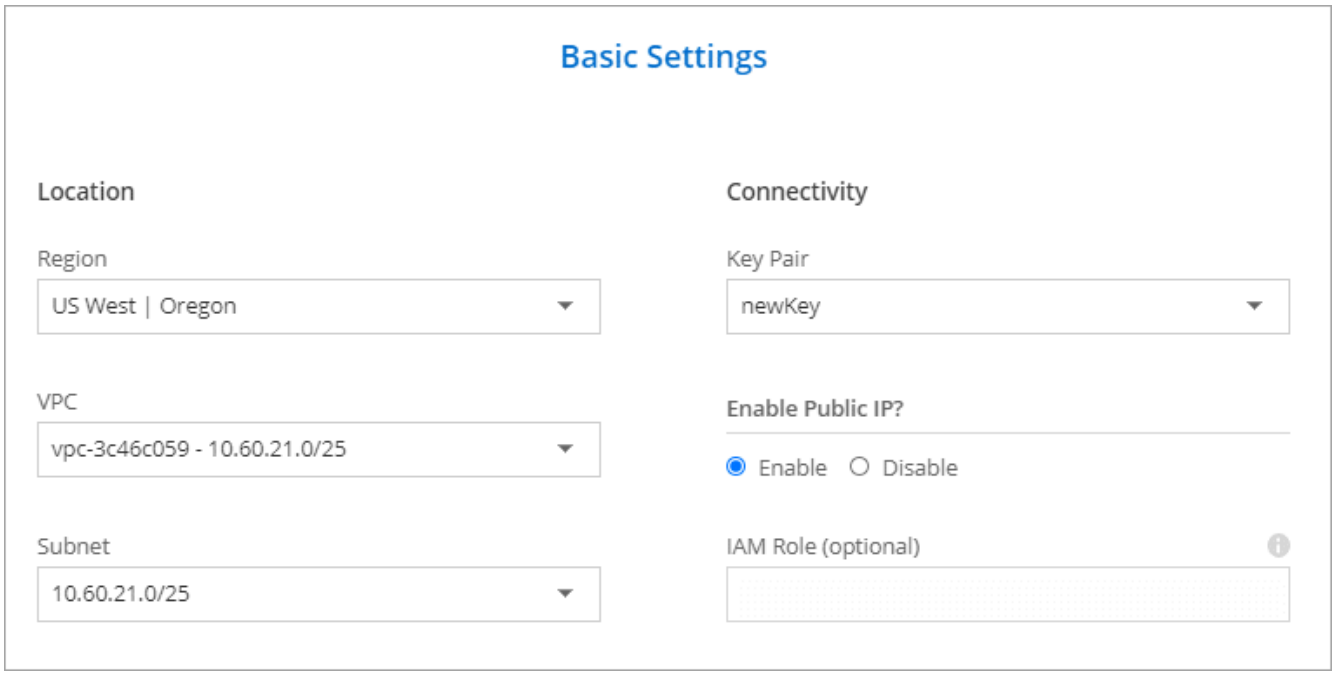
   Si prefiere no proporcionar claves de acceso, haga clic en el vínculo situado en la parte inferior de la página para utilizar una plantilla CloudFormation en su lugar. Cuando usa esta opción, no necesita proporcionar credenciales, ya que inicia sesión directamente en AWS.

   en el siguiente vídeo se muestra cómo iniciar la instancia de Data broker mediante una plantilla CloudFormation:

   ► https://docs.netapp.com/es-es/occm38//media/video_cloud_sync.mp4 *(video)*

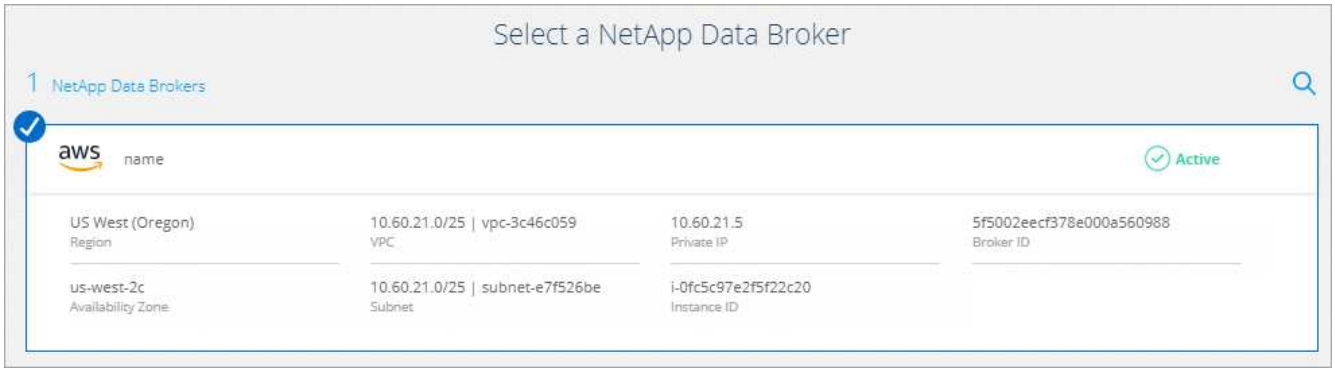
6. Si introdujo una clave de acceso de AWS, seleccione una ubicación para la instancia, seleccione un par de claves, elija si desea habilitar una dirección IP pública y, a continuación, seleccione un rol de IAM existente o deje el campo en blanco para que Cloud Sync cree el rol para usted.

   Si elige su propio rol de IAM, deberá proporcionar los permisos necesarios.



7. Después de que el Data broker esté disponible, haga clic en **continuar** en Cloud Sync.

   En la siguiente imagen se muestra una instancia implementada correctamente en AWS:



8. Complete las páginas del asistente para crear la nueva relación de sincronización.

Resultado

Ha implementado un agente de datos en AWS y creado una nueva relación de sincronización. Puede utilizar este Data broker con relaciones de sincronización adicionales.

Instalar el agente de datos en Azure

Al crear una relación de sincronización, elija la opción de Azure Data Broker para implementar el software de agente de datos en una nueva máquina virtual en un vnet. Cloud Sync le guía durante el proceso de instalación, pero en esta página se repiten los requisitos y los pasos que le ayudarán a preparar la instalación.

También tiene la opción de instalar el agente de datos en un host Linux existente en el cloud o en sus instalaciones. "Leer más".

Regiones de Azure compatibles

Todas las regiones cuentan con el apoyo de las regiones de China, la gobernadora de los Estados Unidos y el Departamento de Defensa de los Estados Unidos.

Requisitos de red

- El agente de datos necesita una conexión saliente a Internet para que pueda sondear el servicio Cloud Sync para las tareas a través del puerto 443.

  Cuando Cloud Sync implementa el agente de datos en Azure, crea un grupo de seguridad que permite la comunicación saliente necesaria.

  Si necesita limitar la conectividad saliente, consulte "lista de puntos finales con los que se contacta el data broker".

- NetApp recomienda configurar el origen, el destino y el intermediario de datos para utilizar un servicio de protocolo de tiempo de redes (NTP). La diferencia de tiempo entre los tres componentes no debe superar los 5 minutos.

Método de autenticación

Al implementar el agente de datos, tendrá que elegir un método de autenticación: Una contraseña o un par de claves público-privadas SSH.

Para obtener ayuda sobre la creación de un par de claves, consulte "Documentación de Azure: Cree y utilice una pareja de claves SSH público-privada para máquinas virtuales de Linux en Azure".

Instalación del Data broker

Puede instalar un agente de datos en Azure al crear una relación de sincronización.

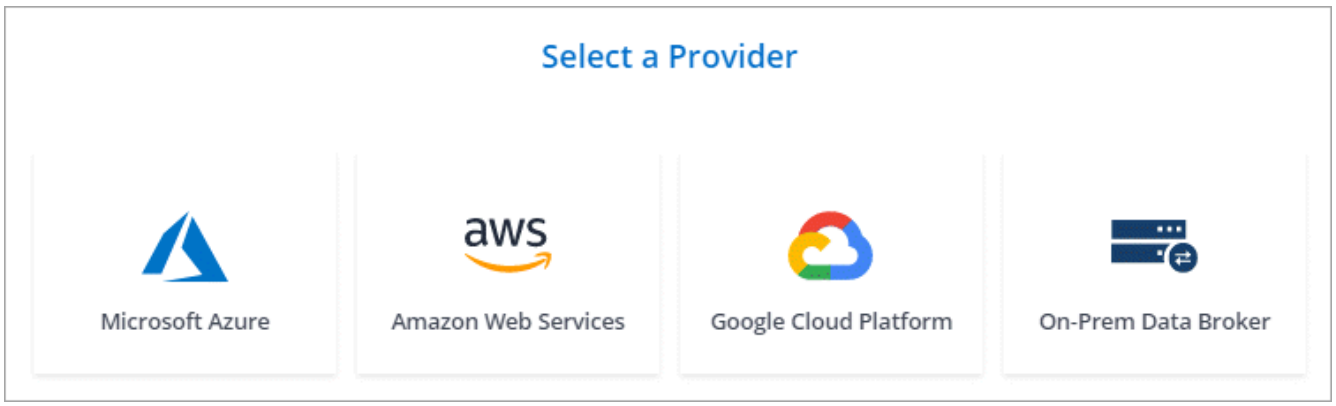
Pasos

1. Haga clic en **Crear nueva sincronización**.
2. En la página **definir relación de sincronización**, elija un origen y un destino y haga clic en **continuar**.

   Rellene las páginas hasta que llegue a la página **Data Broker**.

3. En la página **Data Broker**, haga clic en **Crear Data Broker** y, a continuación, seleccione **Microsoft Azure**.

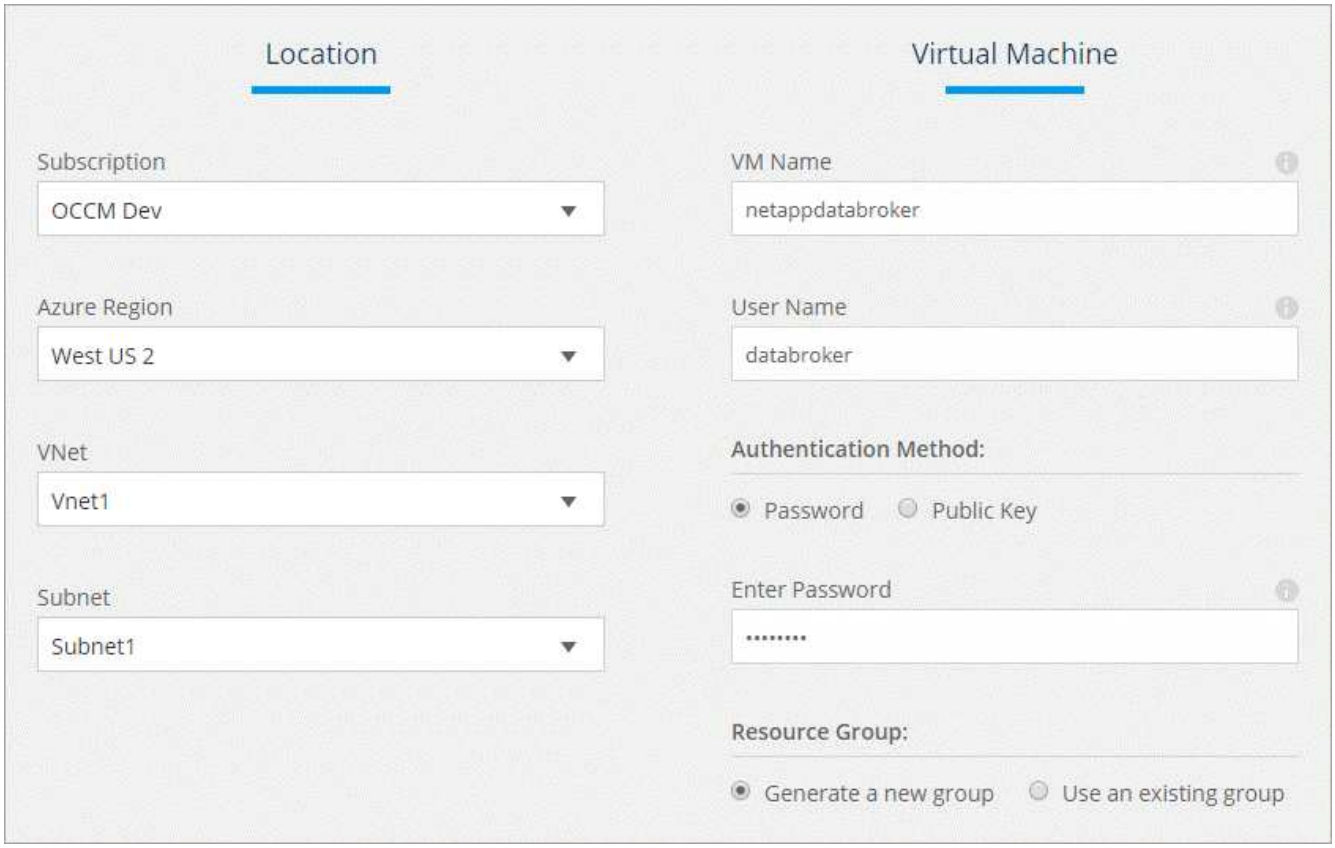
   Si ya tiene un agente de datos, tendrá que hacer clic en el + icono primero.



4. Introduzca un nombre para el Data broker y haga clic en **continuar**.
5. Si se le solicita, inicie sesión en su cuenta de Microsoft. Si no se le solicita, haga clic en **Iniciar sesión en Azure**.

   El formulario es propiedad de Microsoft y está alojado en él. Sus credenciales no se proporcionan a NetApp.

6. Elija una ubicación para el agente de datos e introduzca detalles básicos sobre la máquina virtual.



7. Haga clic en **continuar** y mantenga la página abierta hasta que finalice la implementación.

   El proceso puede tardar hasta 7 minutos.

8. En Cloud Sync, haga clic en **continuar** una vez que el Data broker esté disponible.
9. Complete las páginas del asistente para crear la nueva relación de sincronización.

Resultado

Ha puesto en marcha un agente de datos en Azure y creado una nueva relación de sincronización. Puede utilizar este Data broker con relaciones de sincronización adicionales.

¿obtiene un mensaje acerca de cómo se necesita el consentimiento de administrador?

Si Microsoft le notifica que se requiere la aprobación del administrador porque Cloud Sync necesita permiso para acceder a los recursos de la organización en su nombre, dispone de dos opciones:

1. Pida a su administrador de AD que le proporcione los siguientes permisos:

   En Azure, vaya a **Centros de administración > Azure AD > usuarios y grupos > Configuración de usuario** y active **los usuarios pueden dar su consentimiento a las aplicaciones que acceden a los datos de la empresa en su nombre**.

2. Pida a su administrador de AD que consiente en su nombre **CloudSync-AzureDataBrokerCreator** utilizando la siguiente URL (éste es el punto final del consentimiento de administración):

   https://login.microsoftonline.com/{FILL AQUÍ su ID DE INQUILINO}/v2.0/adminconsent?client_id=8ee4ca3a-bafa-4831-97cc-5a38923cab85&redirect_uri=https://cloudsync.netapp.com&scope=https://management.azure.com/user_impersonationhttps://graph.microsoft.com/User.Read

   Como se muestra en la URL, nuestra URL de aplicación es https://cloudsync.netapp.com y el ID de cliente de aplicación es 8ee4ca3a-bafa-4831-97cc-5a38923cab85.

Instalación del agente de datos en Google Cloud Platform

Al crear una relación de sincronización, elija la opción GCP Data Broker para implementar el software de broker de datos en una nueva instancia de máquina virtual en un VPC. Cloud Sync le guía durante el proceso de instalación, pero en esta página se repiten los requisitos y los pasos que le ayudarán a preparar la instalación.

También tiene la opción de instalar el agente de datos en un host Linux existente en el cloud o en sus instalaciones. "Leer más".

Regiones compatibles de GCP

Se admiten todas las regiones.

Requisitos de red

- El agente de datos necesita una conexión saliente a Internet para que pueda sondear el servicio Cloud Sync para las tareas a través del puerto 443.

  Cuando Cloud Sync implementa el intermediario de datos en GCP, crea un grupo de seguridad que habilita la comunicación saliente necesaria.

  Si necesita limitar la conectividad saliente, consulte "lista de puntos finales con los que se contacta el data broker".

- NetApp recomienda configurar el origen, el destino y el intermediario de datos para utilizar un servicio de protocolo de tiempo de redes (NTP). La diferencia de tiempo entre los tres componentes no debe superar los 5 minutos.

Permisos necesarios para desplegar el agente de datos en GCP

Asegúrese de que el usuario de GCP que despliega el intermediario de datos tiene los siguientes permisos:

```
- compute.networks.list
- compute.regions.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.operations.get
- iam.serviceAccounts.list
```

Permisos necesarios para la cuenta de servicio

Al implementar el agente de datos, debe seleccionar una cuenta de servicio que tenga los siguientes permisos:

```
- logging.logEntries.create
- resourcemanager.projects.get
- storage.buckets.get
- storage.buckets.list
- storage.objects.*
```

Instalación del Data broker

Puede instalar un intermediario de datos en GCP cuando cree una relación de sincronización.

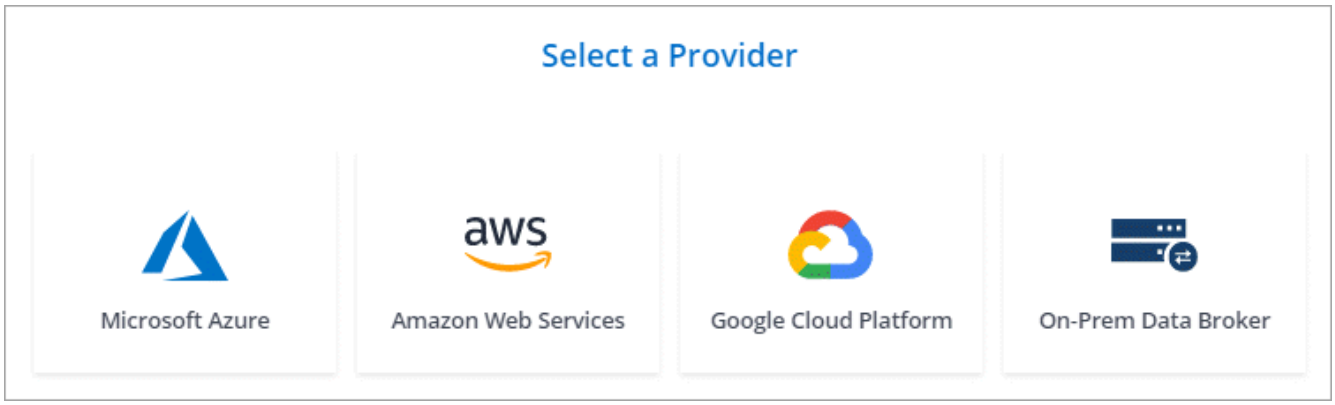
Pasos

1. Haga clic en **Crear nueva sincronización**.
2. En la página **definir relación de sincronización**, elija un origen y un destino y haga clic en **continuar**.

   Complete los pasos hasta llegar a la página **Data Broker**.

3. En la página **Data Broker**, haga clic en **Crear Data Broker** y seleccione **Google Cloud Platform**.

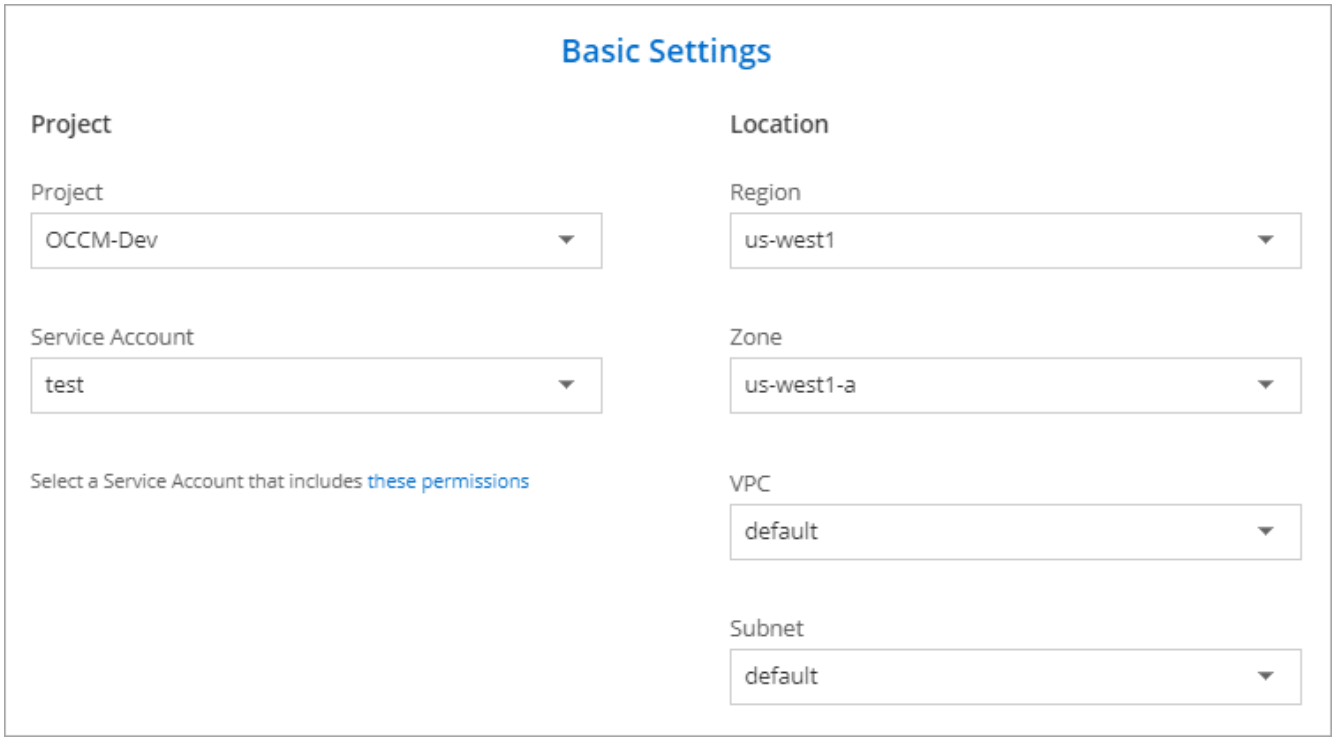
   Si ya tiene un agente de datos, tendrá que hacer clic en el + icono primero.



4. Introduzca un nombre para el Data broker y haga clic en **continuar**.
5. Si se le solicita, inicie sesión con su cuenta de Google.

   El formulario es propiedad de Google y está alojado en él. Sus credenciales no se proporcionan a NetApp.

6. Seleccione un proyecto y una cuenta de servicio y, a continuación, elija una ubicación para el agente de datos.



7. Una vez que el Data broker esté disponible, haga clic en **continuar** en Cloud Sync.

   La puesta en marcha de la instancia tarda entre 5 y 10 minutos, aproximadamente. Puede supervisar el progreso desde el servicio Cloud Sync, que se actualiza automáticamente cuando la instancia está disponible.

8. Complete las páginas del asistente para crear la nueva relación de sincronización.

Resultado

Ha implementado un agente de datos en GCP y creado una nueva relación de sincronización. Puede utilizar este Data broker con relaciones de sincronización adicionales.

Instalar el agente de datos en un host Linux

Al crear una relación de sincronización, elija la opción de Data Broker en las instalaciones para instalar el software de agente de datos en un host Linux local o en un host Linux existente en el cloud. Cloud Sync le guía durante el proceso de instalación, pero en esta página se repiten los requisitos y los pasos que le ayudarán a preparar la instalación.

Requisitos del host Linux

- **sistema operativo**:
  - CentOS 7.0, 7.7 y 8.0
  - Red Hat Enterprise Linux 7.7 y 8.0
  - Sistema operativo Ubuntu Server 18.04 LTS
  - SUSE Linux Enterprise Server 15 SP1

    El comando `yum update all` debe ejecutarse en el host antes de instalar el agente de datos.

  Debe registrarse un sistema Red Hat Enterprise Linux con Red Hat Subscription Management. Si no está registrado, el sistema no puede acceder a los repositorios para actualizar el software necesario de terceros durante la instalación.

- **RAM**: 16 GB
- **CPU**: 4 núcleos
- **espacio libre en disco**: 10 GB
- **SELinux**: Le recomendamos que desactive la función "SELinux" en el host.

  SELinux aplica una política que bloquea las actualizaciones de software de Data broker y puede bloquear el intermediario de datos de los extremos de contacto necesarios para un funcionamiento normal.

- **OpenSSL**: Debe estar instalado en el host Linux.

Requisitos de red

- El host Linux debe tener una conexión con el origen y el destino.
- El servidor de archivos debe permitir que el host Linux acceda a las exportaciones.
- El puerto 443 debe estar abierto en el host Linux para el tráfico saliente a AWS (el agente de datos se comunica constantemente con el servicio Amazon SQS).
- NetApp recomienda configurar el origen, el destino y el intermediario de datos para utilizar un servicio de protocolo de tiempo de redes (NTP). La diferencia de tiempo entre los tres componentes no debe superar los 5 minutos.

Habilitar el acceso a AWS

Si planea utilizar el agente de datos con una relación de sincronización que incluya un bloque de S3, debe preparar el host Linux para el acceso a AWS. Cuando instale el agente de datos, necesitará proporcionar claves AWS para un usuario de AWS que tenga acceso al mismo mediante programación y permisos específicos.

Pasos

1. Cree una política de IAM mediante "Esta política proporcionada por NetApp". "Consulte las instrucciones de AWS".
2. Cree un usuario IAM con acceso mediante programación. "Consulte las instrucciones de AWS".

   Asegúrese de copiar las claves de AWS porque debe especificarlas al instalar el software de Data broker.

Habilitar el acceso a Google Cloud

Si tiene pensado utilizar el agente de datos con una relación de sincronización que incluya un bucket de Google Cloud Storage, debería preparar el host Linux para acceso a GCP. Al instalar el Data Broker, deberá proporcionar una clave para una cuenta de servicio que tenga permisos específicos.

Pasos

1. Cree una cuenta de servicio de GCP que tenga permisos de administrador de almacenamiento, si aún no tiene una.
2. Cree una clave de cuenta de servicio guardada en formato JSON. "Vea las instrucciones de GCP".

   El archivo debe contener al menos las siguientes propiedades: "Project_id", "private_key" y "client_email"

   Al crear una clave, el archivo se genera y descarga en el equipo.

3. Guarde el archivo JSON en el host Linux.

Habilitar el acceso a Microsoft Azure

El acceso a Azure se define por relación proporcionando una cuenta de almacenamiento y una cadena de conexión en el asistente de relaciones de sincronización.

Instalación del Data broker

Puede instalar un agente de datos en un host Linux al crear una relación de sincronización.

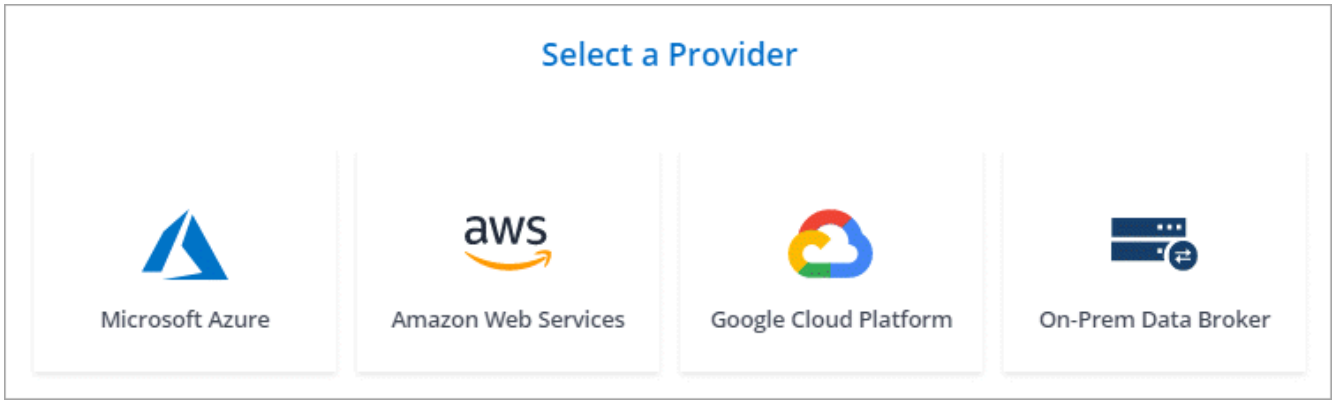
Pasos

1. Haga clic en **Crear nueva sincronización**.
2. En la página **definir relación de sincronización**, elija un origen y un destino y haga clic en **continuar**.

   Complete los pasos hasta llegar a la página **Data Broker**.

3. En la página **Data Broker**, haga clic en **Crear Data Broker** y, a continuación, seleccione **On-Prem Data Broker**.

   Si ya tiene un agente de datos, tendrá que hacer clic en el + icono primero.



Aunque la opción se etiqueta ***on-Prem*** **Data Broker**, se aplica a un host Linux en sus instalaciones o en la nube.

4. Introduzca un nombre para el Data broker y haga clic en **continuar**.

   La página de instrucciones se carga en breve. Tendrá que seguir estas instrucciones; incluyen un enlace único para descargar el instalador.

5. En la página de instrucciones:
   a. Seleccione si desea activar el acceso a **AWS**, **Google Cloud** o ambos.
   b. Seleccione una opción de instalación: **sin proxy**, **usar servidor proxy** o **usar servidor proxy con autenticación**.
   c. Utilice los comandos para descargar e instalar el Data broker.

      En los siguientes pasos se ofrecen detalles sobre cada posible opción de instalación. Siga la página de instrucciones para obtener el comando exacto según la opción de instalación.

   d. Descargue el instalador:
      - Sin proxy:

        ```
        curl <URI> -o data_broker_installer.sh
        ```

      - Usar servidor proxy:

        ```
        curl <URI> -o data_broker_installer.sh -x <proxy_host>:<proxy_port>
        ```

      - Utilice el servidor proxy con autenticación:

        ```
        curl <URI> -o data_broker_installer.sh -x
        <proxy_username>:<proxy_password>@<proxy_host>:<proxy_port>
        ```

        URI

        Cloud Sync muestra el URI del archivo de instalación en la página de instrucciones, que se carga cuando sigue los mensajes para implementar el agente de datos en las instalaciones. Ese URI no se repite aquí porque el enlace se genera dinámicamente y sólo se puede usar una vez. Siga estos pasos para obtener el URI de Cloud Sync.

   e. Cambie a superusuario, haga ejecutable el instalador e instale el software:

      > Cada uno de los comandos enumerados a continuación incluye parámetros para acceso a AWS y acceso a GCP. Siga la página de instrucciones para obtener el comando exacto según la opción de instalación.

      - Sin configuración de proxy:

        ```
        sudo -s
        chmod +x data_broker_installer.sh
        ./data_broker_installer.sh -a <aws_access_key> -s <aws_secret_key> -g
        <absolute_path_to_the_json_file>
        ```

      - Configuración de proxy:

        ```
        sudo -s
        chmod +x data_broker_installer.sh
        ./data_broker_installer.sh -a <aws_access_key> -s <aws_secret_key> -g
        ```

```
<absolute_path_to_the_json_file> -h <proxy_host> -p <proxy_port>
```

- Configuración del proxy con autenticación:

```
sudo -s
chmod +x data_broker_installer.sh
./data_broker_installer.sh -a <aws_access_key> -s <aws_secret_key> -g
<absolute_path_to_the_json_file> -h <proxy_host> -p <proxy_port> -u
<proxy_username> -w <proxy_password>
```

Claves de AWS

Estas son las claves para el usuario que debería se prepararon siga estos pasos. Las claves de AWS se almacenan en el agente de datos, que se ejecuta en la red local o en el cloud. NetApp no utiliza las claves fuera del agente de datos.

Archivo JSON

Este es el archivo JSON que contiene una cuenta de servicio clave que usted debe haber preparado siga estos pasos.

6. Una vez que el Data broker esté disponible, haga clic en **continuar** en Cloud Sync.
7. Complete las páginas del asistente para crear la nueva relación de sincronización.

Creación de una relación de sincronización

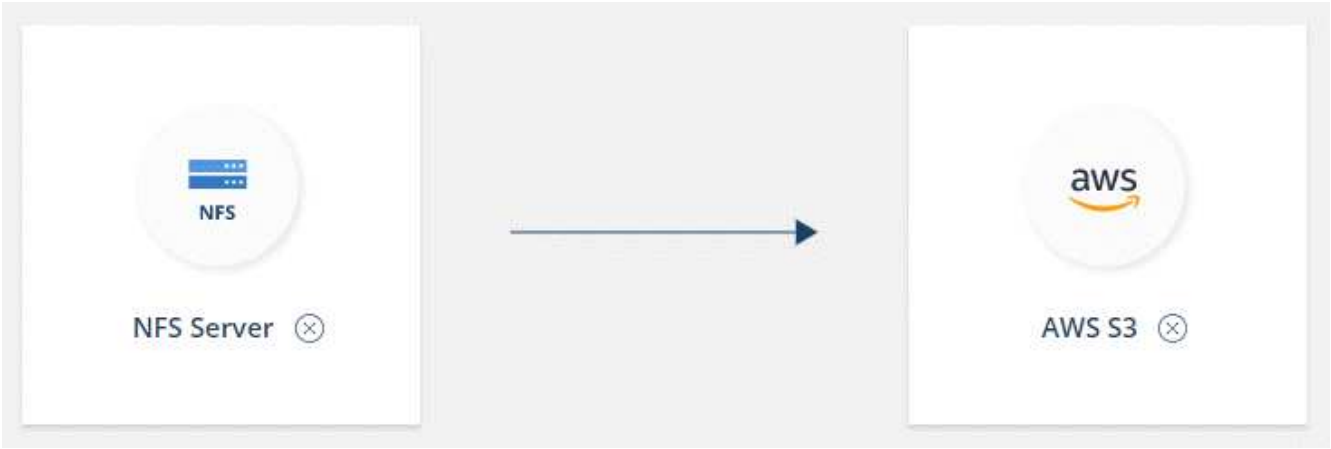
Al crear una relación de sincronización, el servicio Cloud Sync copia los archivos del origen al destino. Después de la copia inicial, el servicio sincroniza los datos modificados cada 24 horas.

Los siguientes pasos proporcionan un ejemplo que muestra cómo configurar una relación de sincronización desde un servidor NFS a un bloque de S3.

Pasos

1. En Cloud Manager, haga clic en **sincronización**.
2. En la página **definir relación de sincronización**, elija un origen y un destino.

   En los siguientes pasos se proporciona un ejemplo de cómo crear una relación de sincronización desde un servidor NFS hasta un bloque de S3.

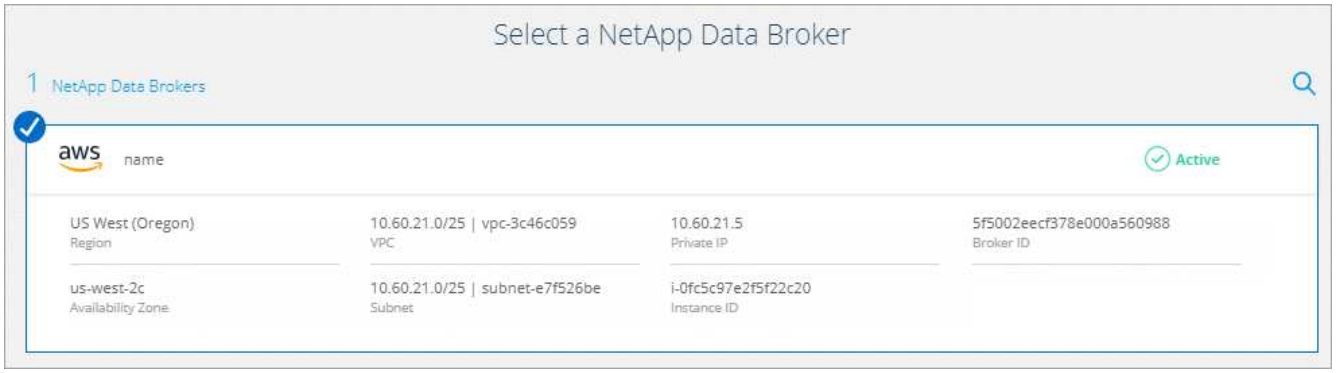


3. En la página **servidor NFS**, introduzca la dirección IP o el nombre de dominio completo del servidor NFS que desea sincronizar con AWS.
4. En la página **Data Broker**, siga las indicaciones para crear una máquina virtual de Data Broker en AWS, Azure o Google Cloud Platform, o para instalar el software de Data broker en un host Linux existente.

   Para obtener más información, consulte las siguientes páginas:

   - "Instalar el agente de datos en AWS"
   - "Instalar el agente de datos en Azure"
   - "Instalación del agente de datos en GCP"
   - "Instalar el agente de datos en un host Linux"
5. Después de instalar el Data broker, haga clic en **continuar**.

   La siguiente imagen muestra un agente de datos implementado correctamente en AWS:

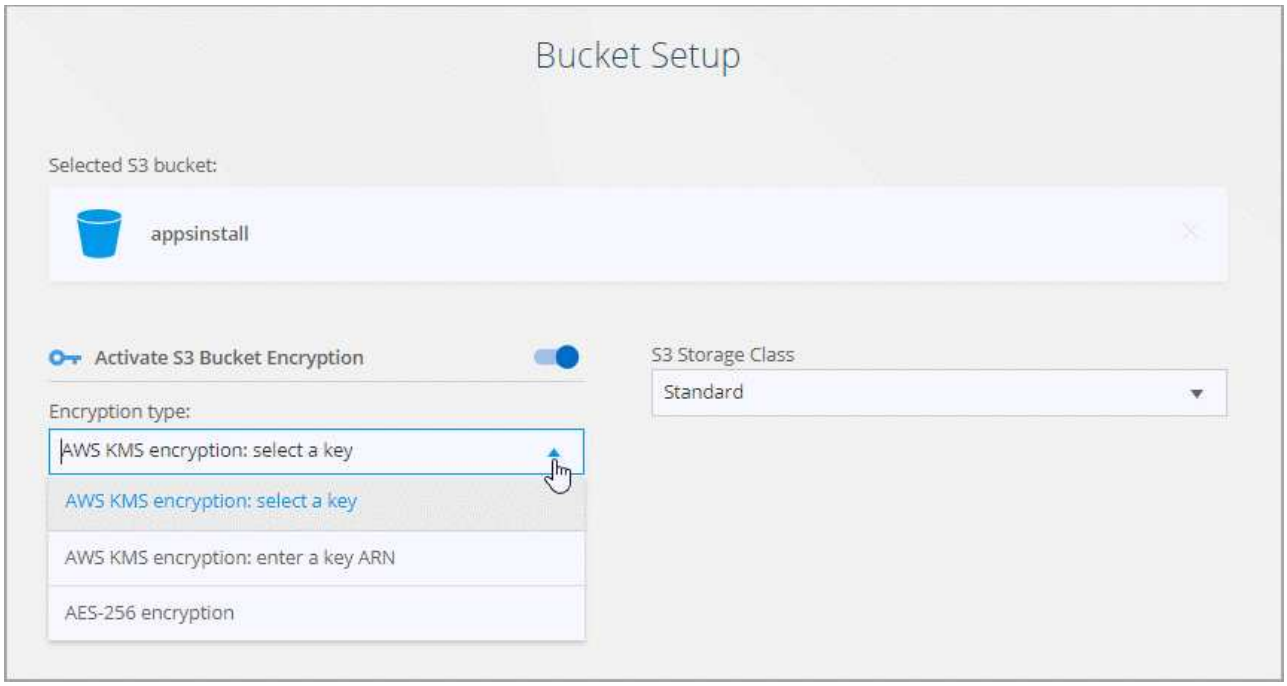


6. en la página **directorios**, seleccione un directorio o subdirectorio de nivel superior.

   Si Cloud Sync no puede recuperar las exportaciones, haga clic en **Agregar exportación manualmente** e introduzca el nombre de una exportación NFS.

   > Si desea sincronizar más de un directorio en el servidor NFS, debe crear relaciones de sincronización adicionales una vez haya terminado.

7. En la página **AWS S3 Bucket**, seleccione un bloque:
   - Examine para seleccionar una carpeta existente dentro del bloque o para seleccionar una carpeta nueva que cree dentro del bloque.
   - Haga clic en **Agregar a la lista** para seleccionar un bloque de S3 que no esté asociado a su cuenta de AWS. "Los permisos específicos se deben aplicar al bloque de S3".
8. En la página **Configuración de bloque**, configure el cucharón:
   - Elija si desea habilitar el cifrado de bloque de S3 y, a continuación, seleccione una clave de AWS KMS, introduzca el ARN de una clave de KMS o seleccione el cifrado AES-256.
   - Seleccione una clase de almacenamiento S3. "Consulte las clases de almacenamiento compatibles".



9. En la página **Configuración**, defina cómo se sincronizan y mantienen los archivos y carpetas de origen en la ubicación de destino:

Programación

Elija una programación recurrente para sincronizar en el futuro o desactive la programación de sincronización. Puede programar una relación para que se sincronice datos con una frecuencia de hasta cada 1 minuto.

Reintentos

Defina el número de veces que Cloud Sync debe volver a intentar sincronizar un archivo antes de omitirlo.

Archivos modificados recientemente

Elija excluir los archivos que se modificaron recientemente antes de la sincronización programada.

Eliminar archivos en el origen

Elija eliminar archivos de la ubicación de origen después de que Cloud Sync copie los archivos en la ubicación de destino. Esta opción incluye el riesgo de pérdida de datos porque los archivos de origen se eliminan una vez copiados.

Si habilita esta opción, también debe cambiar un parámetro en el archivo local.json del agente de datos. Abra el archivo y cambie el parámetro denominado *workers.transferrer.delete-on-source* a **TRUE**.

Eliminar archivos en destino

Elija eliminar archivos de la ubicación de destino, si se eliminaron del origen. El valor predeterminado es no eliminar nunca los archivos de la ubicación de destino.

Etiquetado de objetos

Cuando AWS S3 es el destino de una relación de sincronización, Cloud Sync etiqueta objetos de S3 con metadatos relevantes para la operación de sincronización. Puede deshabilitar el etiquetado de objetos S3 si no se desea en el entorno. Cloud Sync no afecta si deshabilita el etiquetado: Cloud Sync solo almacena los metadatos de sincronización de una manera diferente.

Tipos de archivo

Defina los tipos de archivo que se van a incluir en cada sincronización: Archivos, directorios y enlaces simbólicos.

Excluir extensiones de archivo

Especifique las extensiones de archivo que desea excluir de la sincronización escribiendo la extensión de archivo y pulsando **Intro**. Por ejemplo, escriba *log* o *.log* para excluir archivos *.log. No es necesario un separador para varias extensiones. El siguiente vídeo proporciona una breve demostración:

► https://docs.netapp.com/es-es/occm38//media/video_file_extensions.mp4 *(video)*

Tamaño de archivo

Elija sincronizar todos los archivos independientemente de su tamaño o sólo los archivos que se encuentren en un rango de tamaño específico.

Fecha de modificación

Elija todos los archivos independientemente de su fecha de última modificación, los archivos modificados después de una fecha específica, antes de una fecha específica o entre un intervalo de tiempo.

10. En la página **etiquetas de relación**, introduzca hasta 9 etiquetas de relación y, a continuación, haga clic en **continuar**.

    El servicio Cloud Sync asigna las etiquetas a cada objeto que se sincroniza con el bloque de S3.

11. Revise los detalles de la relación de sincronización y haga clic en **Crear relación**.

resultado

Cloud Sync inicia la sincronización de datos entre el origen y el destino.

Pago de las relaciones de sincronización después de que finalice su prueba gratuita

Hay dos formas de pagar las relaciones de sincronización después de que termine su prueba gratuita de 14 días. La primera opción es suscribirse a AWS o Azure para pagar por uso o anualmente. La segunda opción consiste en comprar licencias directamente a NetApp.

Puede usar licencias de NetApp con una suscripción a AWS o Azure. Por ejemplo, si tiene 25 relaciones de sincronización, puede pagar las primeras 20 relaciones de sincronización con una licencia y, a continuación, pagar por el uso desde AWS o Azure con las 5 relaciones de sincronización restantes.

"Obtenga más información sobre cómo funcionan las licencias".

¿Qué pasa si no 8217 pago inmediatamente después de que finalice mi prueba gratuita?

No podrá crear relaciones adicionales. Las relaciones existentes no se eliminan, pero no puede realizar ningún cambio hasta que se suscriba o introduzca una licencia.

Suscribirse a AWS

AWS le permite pagar anualmente.

De pago por uso

1. Haga clic en **Sincronizar > licencias**.
2. Seleccione **AWS**
3. Haga clic en **Suscribirse** y, a continuación, en **continuar**.
4. Suscríbase desde el mercado de AWS y, a continuación, vuelva a iniciar sesión en el servicio Cloud Sync para completar el registro.

   El siguiente vídeo muestra el proceso:

   ► https://docs.netapp.com/es-es/occm38//media/video_cloud_sync_registering.mp4 *(video)*

Pasos a pagar anualmente

1. "Vaya a la página AWS Marketplace".
2. Haga clic en **continuar para suscribirse**.
3. Seleccione sus opciones de contrato y haga clic en **Crear contrato**.

suscribirse de Azure

Azure le permite pagar por uso o anualmente.

Lo que necesitará

Cuenta de usuario de Azure con permisos de colaborador o propietario en la suscripción correspondiente.

Pasos

1. Haga clic en **Sincronizar > licencias**.
2. Seleccione **Azure**.
3. Haga clic en **Suscribirse** y, a continuación, en **continuar**.
4. En el portal de Azure, haga clic en **Crear**, seleccione sus opciones y haga clic en **Suscribirse**.

   Seleccione **Mensual** para pagar por hora, o **Anual** para pagar por un año antes de la fecha.

5. Una vez completada la implementación, haga clic en el nombre del recurso SaaS en la ventana emergente de notificaciones.
6. Haga clic en **Configurar cuenta** para volver a Cloud Sync.

   El siguiente vídeo muestra el proceso:

   ► https://docs.netapp.com/es-es/occm38//media/video_cloud_sync_registering_azure.mp4 *(video)*

Compra de licencias de NetApp y añadirlas a Cloud Sync

Para pagar por adelantado sus relaciones de sincronización, debe adquirir una o más licencias y añadirlas al servicio de Cloud Sync.

Pasos

1. Adquiera una licencia por correo electrónico:ng-cloudsync-contact@netapp.com?Subject=Cloud%20Sync%20Service%20-%20BYOL%20Licencia%20Compra%20Solicite[Contacto con NetApp].
2. En Cloud Manager, haga clic en **sincronización > licencias**.
3. Haga clic en **Agregar licencia** y agregue la licencia.

Tutoriales

Copiar ACL entre recursos compartidos de SMB

Cloud Sync puede copiar listas de control de acceso (ACL) entre un recurso compartido de SMB de origen y un recurso compartido de SMB de destino. Si es necesario, puede conservar manualmente las ACL usted mismo mediante robocopy.

Opciones

- Configure Cloud Sync para que copie automáticamente las ACL
- Copie manualmente las ACL usted mismo

Configurar Cloud Sync para copiar ACL entre servidores SMB

Copiar ACL entre servidores de SMB habilitando una configuración cuando se crea una relación o después de crear una relación.

Tenga en cuenta que esta función está disponible para las nuevas relaciones de sincronización creadas después de la versión 23 de febrero de 2020. Si desea utilizar esta característica con relaciones existentes creadas antes de esa fecha, deberá volver a crear la relación.

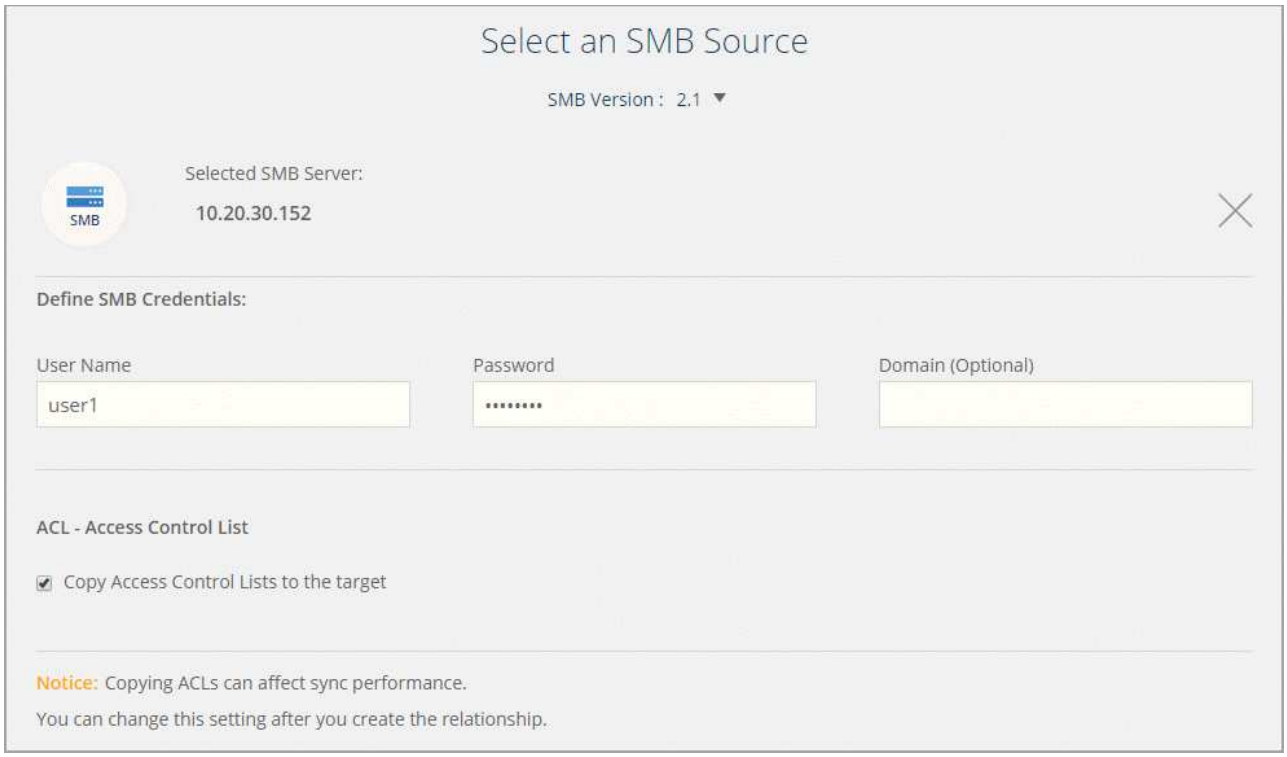
Lo que necesitará

- Una nueva relación de sincronización o una relación de sincronización existente creada después de la versión del 23 de febrero de 2020.
- Cualquier tipo de agente de datos.

  Esta función funciona con *any* type de agente de datos: AWS, Azure, Google Cloud Platform o agente de datos en las instalaciones. Se puede ejecutar el agente de datos en las instalaciones "cualquier sistema operativo compatible".

Pasos para una nueva relación

1. En Cloud Sync, haga clic en **Crear nueva sincronización**.
2. Arrastre y suelte **SMB Server** al origen y al destino y haga clic en **continuar**.
3. En la página **SMB Server**:
   a. Introduzca un nuevo servidor SMB o seleccione un servidor existente y haga clic en **continuar**.
   b. Introduzca credenciales para el servidor SMB.
   c. Seleccione **Copiar listas de control de acceso al destino** y haga clic en **continuar**.



4. Siga el resto de las indicaciones para crear la relación de sincronización.

Pasos para una relación existente

1. Pase el ratón por la relación de sincronización y haga clic en el menú de acción.
2. Haga clic en **Configuración**.
3. Seleccione **Copiar listas de control de acceso al destino**.
4. Haga clic en **Guardar configuración**.

Resultado

Al sincronizar datos, Cloud Sync conserva las ACL entre los recursos compartidos de SMB de origen y de destino.

Copia manual de ACL

Se pueden conservar manualmente las ACL entre recursos compartidos de SMB mediante el comando Windows robocopy.

Pasos

1. Identifique un host Windows con acceso completo a ambos recursos compartidos SMB.
2. Si alguno de los extremos requiere autenticación, utilice el comando **net use** para conectarse a los extremos desde el host de Windows.

   Debe realizar este paso antes de utilizar robocopy.

3. En Cloud Sync, cree una nueva relación entre los recursos compartidos de SMB de origen y de destino, o sincronice una relación existente.
4. Una vez finalizada la sincronización de datos, ejecute el siguiente comando desde el host de Windows para sincronizar las ACL y la propiedad:

```
robocopy /E /COPY:SOU /secfix [source] [target] /w:0 /r:0 /XD ~snapshots
/UNILOG:”[logfilepath]
```

Se deben especificar tanto *source* como *target* con el formato UNC. Por ejemplo: \\<servidor>\<recurso compartido>\<ruta>

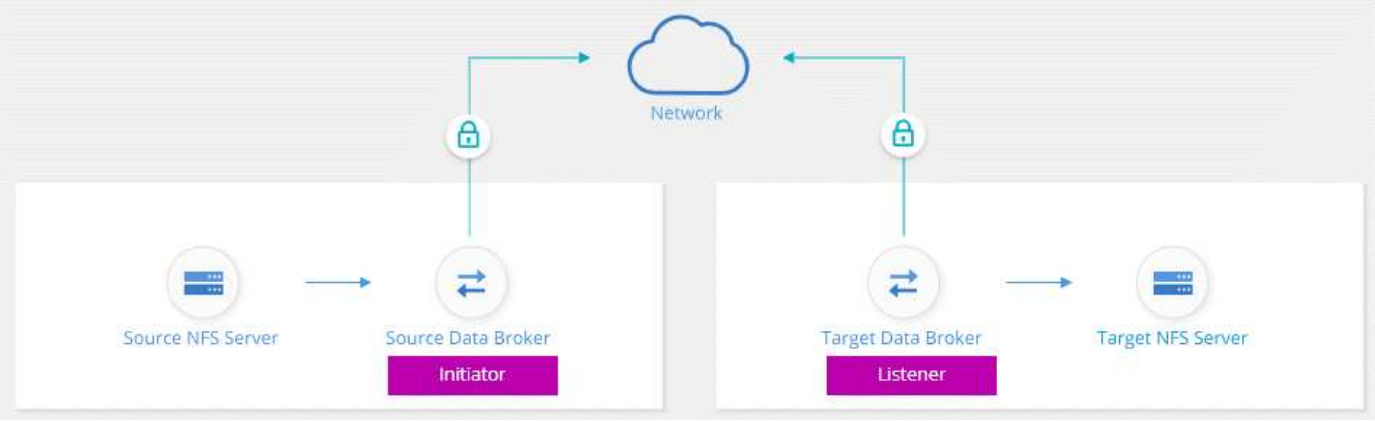
Sincronizando los datos NFS mediante el cifrado de datos en tránsito

Si su negocio tiene políticas de seguridad estrictas, puede sincronizar datos NFS mediante el cifrado de datos en tránsito. Esta función es compatible desde un servidor NFS a otro servidor NFS y de Azure NetApp Files a Azure NetApp Files.

Por ejemplo, se recomienda sincronizar datos entre dos servidores NFS que se encuentran en redes diferentes. O puede que necesite transferir datos de Azure NetApp Files de manera segura en subredes o regiones.

Cómo funciona el cifrado de datos en tiempo real

El cifrado en tiempo real de los datos cifra los datos NFS cuando se envían a través de la red entre dos gestores de datos. La siguiente imagen muestra una relación entre dos servidores NFS y dos agentes de datos:



Un agente de datos funciona como el *initiator*. Cuando es hora de sincronizar datos, envía una solicitud de conexión al otro intermediario de datos, que es el *listener*. Ese agente de datos escucha las solicitudes en el puerto 443. Puede utilizar un puerto diferente, si es necesario, pero asegúrese de comprobar que el puerto no está en uso por otro servicio.

Por ejemplo, si sincroniza datos de un servidor NFS local con un servidor NFS basado en cloud, puede elegir el agente de datos que escucha las solicitudes de conexión y que las envía.

Así es como funciona el cifrado en tránsito:

1. Después de crear la relación de sincronización, el iniciador inicia una conexión cifrada con el otro agente de datos.
2. El agente de datos de origen cifra los datos del origen mediante TLS 1.3.
3. A continuación, envía los datos a través de la red al agente de datos de destino.
4. El agente de datos de destino descifra los datos antes de enviarlos al destino.

5. Después de la copia inicial, el servicio sincroniza los datos modificados cada 24 horas. Si hay datos que sincronizar, el proceso comienza con el iniciador abriendo una conexión cifrada con el otro agente de datos.

   Si prefiere sincronizar datos con mayor frecuencia, "se puede cambiar la programación después de crear la relación".

Versiones NFS compatibles

- En los servidores NFS, el cifrado de datos en tránsito es compatible con las versiones 3, 4.0, 4.1 y 4.2 de NFS.
- En Azure NetApp Files, el cifrado de datos en tiempo real es compatible con las versiones 3 y 4.1 de NFS.

Lo que necesitará para comenzar

No olvide disponer de lo siguiente:

- Dos servidores NFS que cumplen "requisitos de origen y objetivo" O Azure NetApp Files en dos subredes o regiones.
- Las direcciones IP o los nombres de dominio completos de los servidores.
- Ubicaciones de red para dos agentes de datos.

  Puede seleccionar un agente de datos existente pero debe funcionar como iniciador. El agente de datos del listener debe ser un agente de datos *new*.

  Si aún no ha implementado un agente de datos, revise los requisitos de Data Broker. Debido a que tiene directivas de seguridad estrictas, asegúrese de revisar los requisitos de red, que incluyen tráfico saliente desde el puerto 443 y el "puntos finales de internet" que el agente de datos se pone en contacto con.

  - "Revise la instalación de AWS"
  - "Revise la instalación de Azure"
  - "Revise la instalación de GCP"
  - "Revise la instalación del host Linux"

Sincronizando los datos NFS mediante el cifrado de datos en tránsito

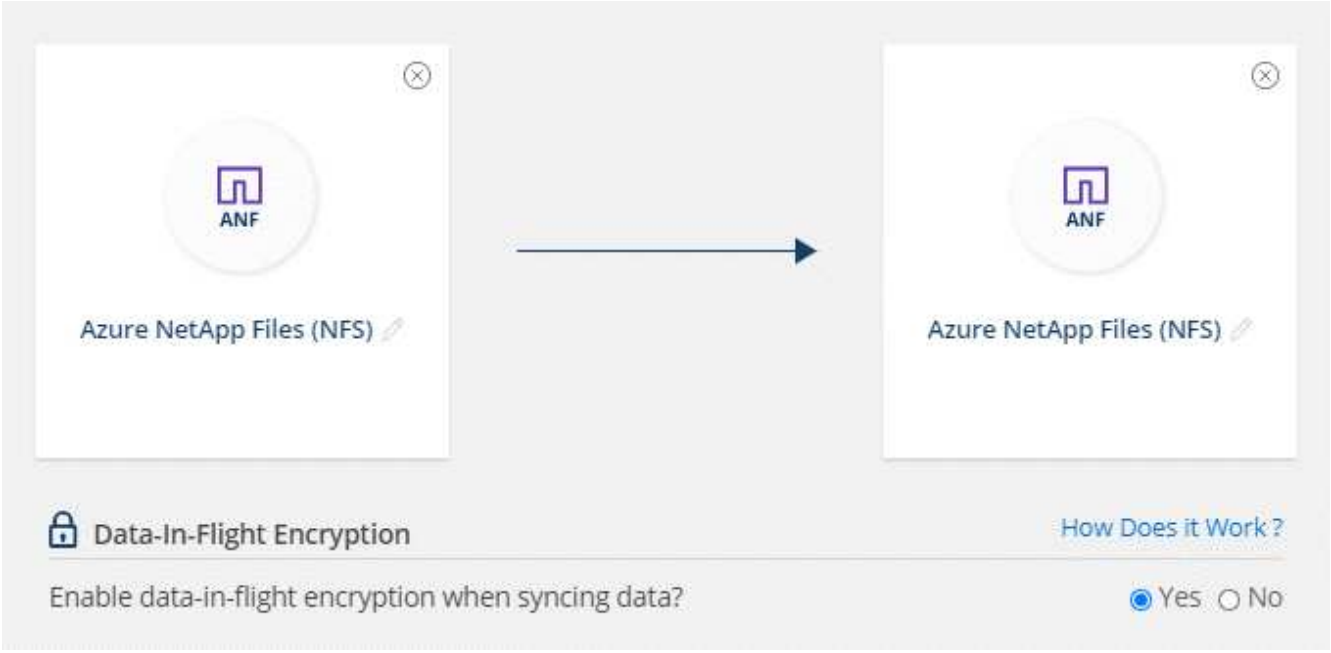
Cree una nueva relación de sincronización entre dos servidores NFS o entre Azure NetApp Files, habilite la opción de cifrado en curso y siga las indicaciones.

Pasos

1. Haga clic en **Crear nueva sincronización**.
2. Arrastre y suelte **servidor NFS** a las ubicaciones de origen y destino o **Azure NetApp Files** a las ubicaciones de origen y destino y seleccione **Sí** para activar el cifrado de datos en vuelo.

   En la siguiente imagen se muestra lo que seleccionaría para sincronizar datos entre dos servidores NFS:

La siguiente imagen muestra lo que seleccionaría para sincronizar datos entre Azure NetApp Files:



3. Siga las indicaciones para crear la relación:

   a. **NFS Server/Azure NetApp Files**: Elija la versión NFS y, a continuación, especifique un nuevo origen NFS o seleccione un servidor existente.

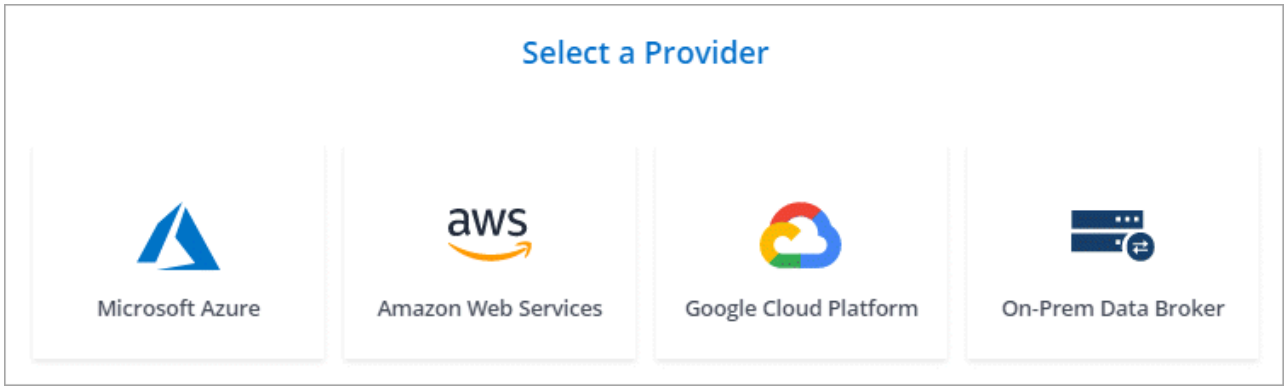
   b. **definir la funcionalidad de Data Broker**: Defina qué intermediario de datos *escucha* las solicitudes de conexión de un puerto y cuál *inicia* la conexión. Elija en función de sus requisitos de red.

   c. **Data Broker**: Siga las indicaciones para agregar un nuevo intermediario de datos de origen o seleccionar un intermediario de datos existente.

      Si el agente de datos de origen actúa como oyente, debe ser un nuevo agente de datos.

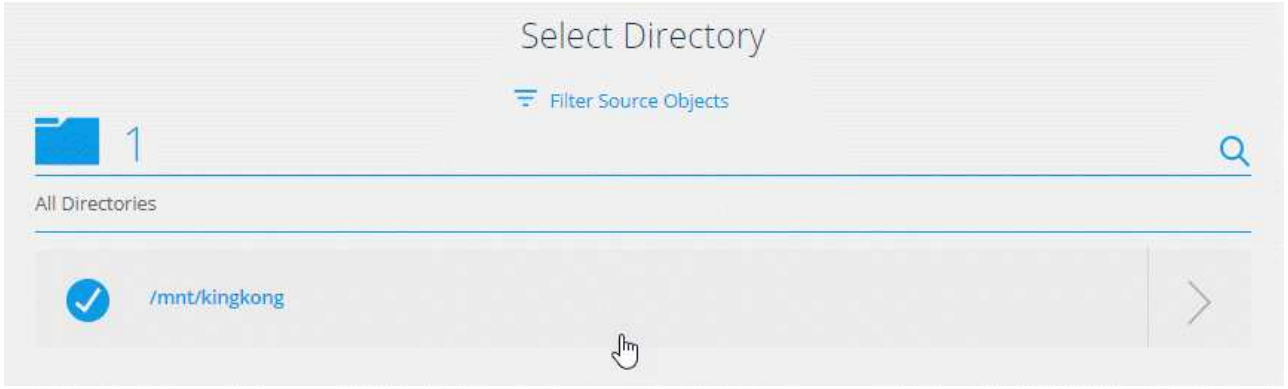
      Si necesita un nuevo agente de datos, Cloud Sync le pedirá las instrucciones de instalación. Puede

desplegar el agente de datos en el cloud o descargar un script de instalación para su propio host Linux.



d. **directorios**: Elija los directorios que desea sincronizar seleccionando todos los directorios, o taladrando y seleccionando un subdirectorio.

   Haga clic en **Filtrar objetos de origen** para modificar la configuración que define cómo se sincronizan y mantienen los archivos y carpetas de origen en la ubicación de destino.

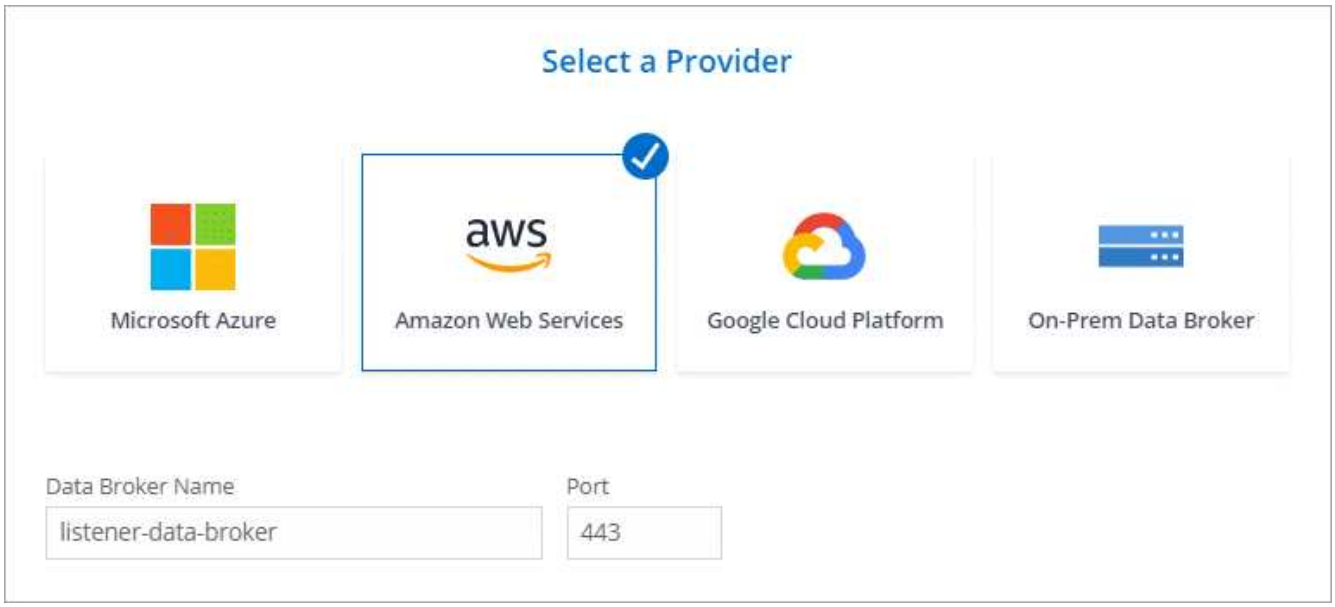


e. **servidor NFS de destino/Azure NetApp Files de destino**: Elija la versión NFS y, a continuación, introduzca un destino NFS nuevo o seleccione un servidor existente.

f. **Target Data Broker**: Siga las indicaciones para agregar un nuevo intermediario de datos de origen o seleccionar un intermediario de datos existente.

   Si el agente de datos de destino actúa como oyente, debe ser un nuevo agente de datos.

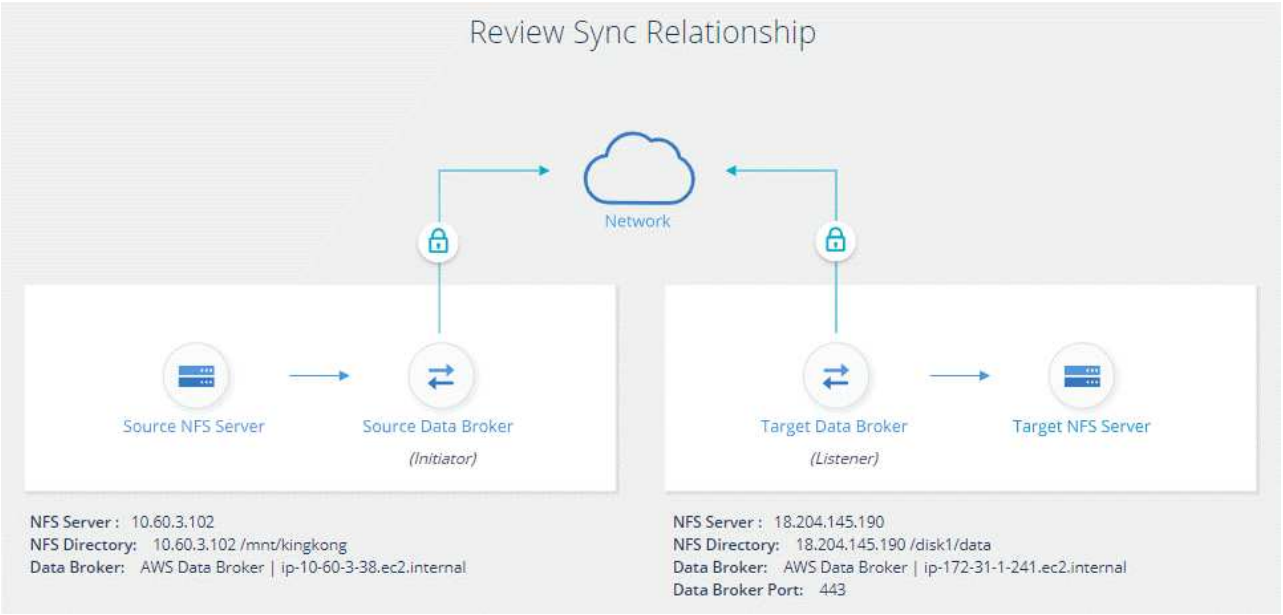
   A continuación se muestra un ejemplo del mensaje en el que el agente de datos de destino funciona como el listener. Observe la opción para especificar el puerto.



a. **directorios de destino**: Seleccione un directorio de nivel superior o examine para seleccionar un subdirectorio existente o crear una nueva carpeta dentro de una exportación.

b. **Configuración**: Defina cómo se sincronizan y mantienen los archivos y carpetas de origen en la ubicación de destino.

c. **Revisión**: Revise los detalles de la relación de sincronización y haga clic en **Crear relación**.



Resultado

Cloud Sync comienza a crear la nueva relación de sincronización. Cuando haya terminado, haga clic en **Ver en Panel** para ver detalles sobre la nueva relación.

Gestión de relaciones de sincronización

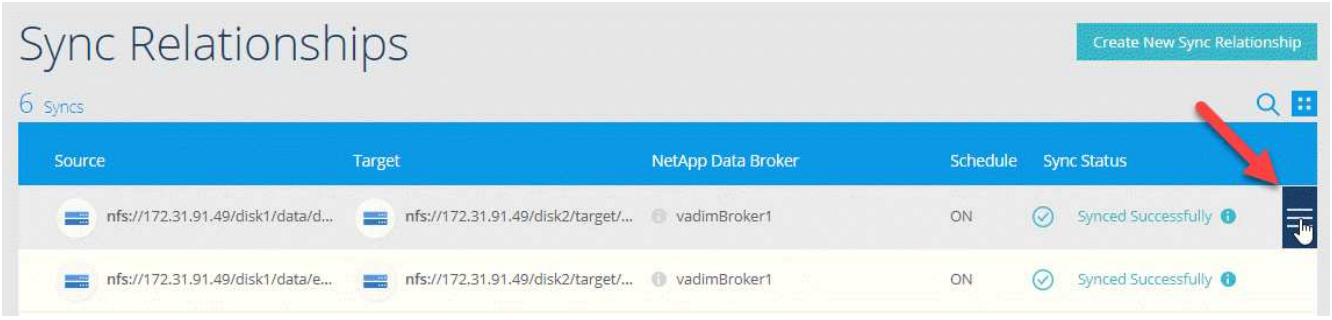
Puede gestionar las relaciones de sincronización en cualquier momento sincronizando de forma inmediata datos, cambiando programaciones y mucho más.

Realizar una sincronización inmediata de datos

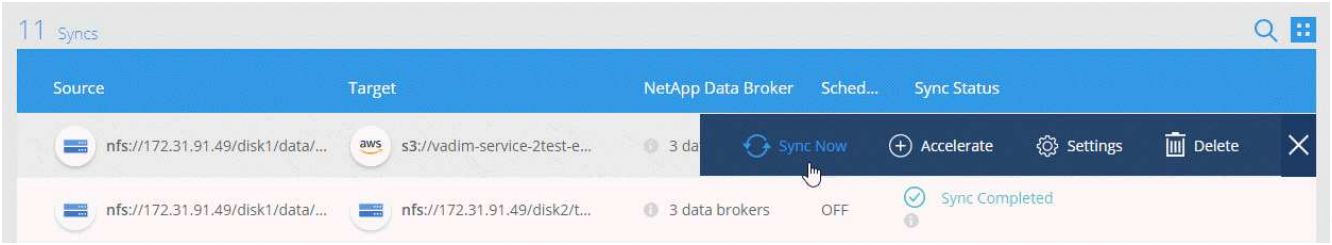
En lugar de esperar a la siguiente sincronización programada, puede pulsar un botón para sincronizar inmediatamente los datos entre la fuente y el destino.

Pasos

1. En **Consola de sincronización**, pase el ratón sobre la relación de sincronización y haga clic en el menú de acciones.



2. Haga clic en **Sincronizar ahora** y, a continuación, en **Sincronizar** para confirmar.



Resultado

Cloud Sync inicia el proceso de sincronización de datos para la relación.

Acelerando el rendimiento de la sincronización

Acelere el rendimiento de una relación de sincronización añadiendo un agente de datos adicional a la relación. El agente de datos adicional debe ser un intermediario de datos *new*.

Cómo funciona

Si los agentes de datos existentes en la relación se utilizan en otras relaciones de sincronización, Cloud Sync agrega automáticamente el nuevo agente de datos a dichas relaciones.

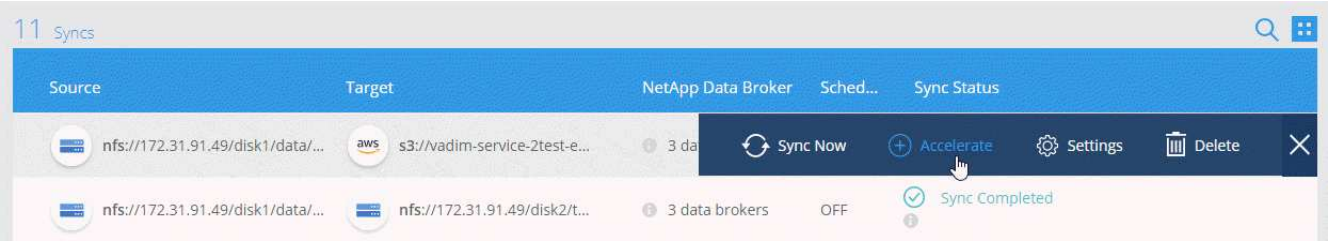
Por ejemplo, digamos que usted tiene tres relaciones:

- La relación 1 utiliza el agente DE datos A
- La relación 2 utiliza Data broker B
- La relación 3 utiliza Data broker A

Desea acelerar el rendimiento de la relación 1 para agregar un nuevo agente de datos a dicha relación (agente de datos C). Debido a que el agente DE datos A también se utiliza en la relación 3, el nuevo agente de datos también se agrega automáticamente a la relación 3.

Pasos

1. Asegúrese de que al menos uno de los agentes de datos existentes en la relación esté en línea.
2. Pase el ratón por la relación de sincronización y haga clic en el menú de acción.
3. Haga clic en **acelerar**.



4. Siga las indicaciones para crear un nuevo Data broker.

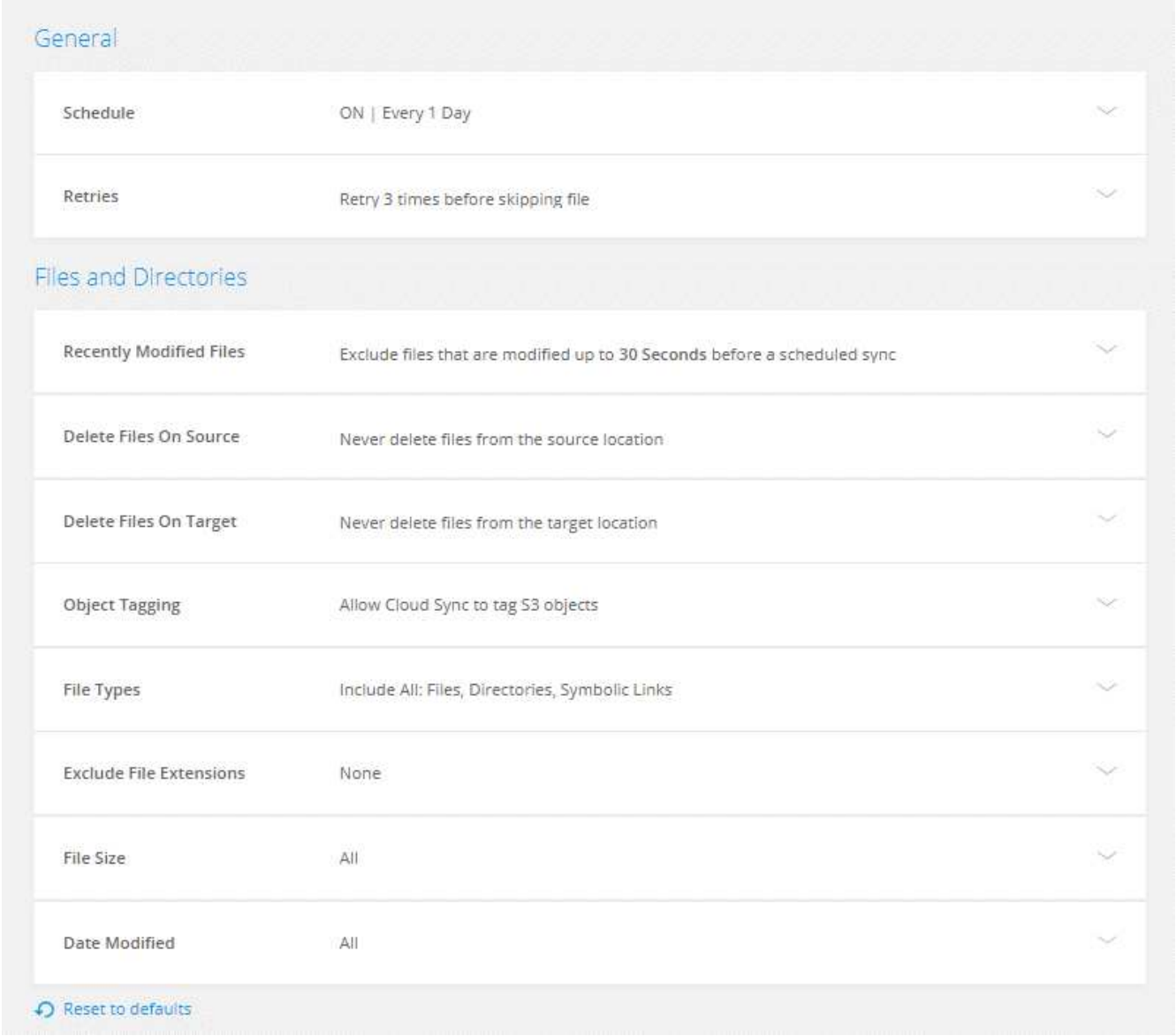
Resultado

Cloud Sync agrega el nuevo agente de datos a las relaciones de sincronización. Es necesario acelerar el rendimiento de la siguiente sincronización de datos.

Cambiar la configuración de una relación de sincronización

Modifique la configuración que define cómo se sincronizan y mantienen los archivos y carpetas de origen en la ubicación de destino.

1. Pase el ratón por la relación de sincronización y haga clic en el menú de acción.
2. Haga clic en **Configuración**.
3. Modifique cualquiera de los ajustes.



aquí hay una breve descripción de cada configuración:

Programación

Elija una programación recurrente para sincronizar en el futuro o desactive la programación de sincronización. Puede programar una relación para que se sincronice datos con una frecuencia de hasta cada 1 minuto.

Reintentos

Defina el número de veces que Cloud Sync debe volver a intentar sincronizar un archivo antes de omitirlo.

Archivos modificados recientemente

Elija excluir los archivos que se modificaron recientemente antes de la sincronización programada.

Eliminar archivos en el origen

Elija eliminar archivos de la ubicación de origen después de que Cloud Sync copie los archivos en la ubicación de destino. Esta opción incluye el riesgo de pérdida de datos porque los archivos de origen se eliminan una vez copiados.

Si habilita esta opción, también debe cambiar un parámetro en el archivo local.json del agente de datos. Abra el archivo y cambie el parámetro denominado *workers.transferrer.delete-on-source* a **TRUE**.

Eliminar archivos en destino

Elija eliminar archivos de la ubicación de destino, si se eliminaron del origen. El valor predeterminado es no eliminar nunca los archivos de la ubicación de destino.

Etiquetado de objetos

Cuando AWS S3 es el destino de una relación de sincronización, Cloud Sync etiqueta objetos de S3 con metadatos relevantes para la operación de sincronización. Puede deshabilitar el etiquetado de objetos S3 si no se desea en el entorno. Cloud Sync no afecta si deshabilita el etiquetado: Cloud Sync solo almacena los metadatos de sincronización de una manera diferente.

Tipos de archivo

Defina los tipos de archivo que se van a incluir en cada sincronización: Archivos, directorios y enlaces simbólicos.

Excluir extensiones de archivo

Especifique las extensiones de archivo que desea excluir de la sincronización escribiendo la extensión de archivo y pulsando **Intro**. Por ejemplo, escriba *log* o *.log* para excluir archivos *.log. No es necesario un separador para varias extensiones. El siguiente vídeo proporciona una breve demostración:

► https://docs.netapp.com/es-es/occm38//media/video_file_extensions.mp4 *(video)*

Tamaño de archivo

Elija sincronizar todos los archivos independientemente de su tamaño o sólo los archivos que se encuentren en un rango de tamaño específico.

Fecha de modificación

Elija todos los archivos independientemente de su fecha de última modificación, los archivos modificados después de una fecha específica, antes de una fecha específica o entre un intervalo de tiempo.

Copiar listas de control de acceso en el destino

Opción de copiar listas de control de acceso (ACL) entre los recursos compartidos de SMB de origen y los recursos compartidos de SMB de destino. Tenga en cuenta que esta opción solo está disponible para relaciones de sincronización creadas después de la versión 23 de febrero de 2020.

4. Haga clic en **Guardar configuración**.

Resultado

Cloud Sync modifica la relación de sincronización con las nuevas opciones de configuración.

Eliminar relaciones

Puede eliminar una relación de sincronización si ya no necesita sincronizar datos entre el origen y el destino. Esta acción no elimina la instancia de Data broker y no elimina los datos del destino.

Pasos

1. Pase el ratón por la relación de sincronización y haga clic en el menú de acción.
2. Haga clic en **Eliminar** y, a continuación, vuelva a hacer clic en **Eliminar** para confirmar.

Resultado

Cloud Sync elimina la relación de sincronización.

API de Cloud Sync

Las funcionalidades Cloud Sync que están disponibles en la interfaz de usuario web también están disponibles mediante API RESTful.

Primeros pasos

Para comenzar a usar las API de Cloud Sync, necesita obtener un token de usuario y su ID de cuenta de Cloud Central. Deberá agregar el token y el ID de cuenta al encabezado de autorización cuando realice llamadas a la API.

Pasos

1. Obtenga un token de usuario de Cloud Central de NetApp.

```
POST https://netapp-cloud-account.auth0.com/oauth/token
Header: Content-Type: application/json
Body:
{
                "username": "<user_email>",
                "scope": "profile",
                "audience": "https://api.cloud.netapp.com",
                "client_id": "UaVhOIXMWQs5i1WdDxauXe5Mqkb34NJQ",
                "grant_type": "password",
                "password": "<user_password>"
}
```

2. Obtenga su ID de cuenta de Cloud Central.

```
GET https://cloudsync.netapp.com/api/accounts
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
```

Esta API devolverá una respuesta como la siguiente:

```
[
  {
    "accountId": "account-JeL97Ry3",
    "name": "Test"
  }
]
```

3. Agregue el identificador de usuario y el ID de cuenta en el encabezado de autorización de cada llamada de API.

   ejemplo

   El siguiente ejemplo muestra una llamada de API para crear un agente de datos en Microsoft Azure. Simplemente debería reemplazar <user_token> y <accountId> por el token y el ID que ha obtenido en los pasos anteriores.

```
POST https://cloudsync.netapp.com/api/data-brokers
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
Body: { "name": "databroker1", "type": "AZURE" }
```

¿Qué debo hacer cuando caduca el token?

El token de usuario de NetApp Cloud Central tiene una fecha de vencimiento. Para actualizar el token, debe volver a llamar a la API desde el paso 1.

La respuesta de la API incluye un campo "expires_in" que indica cuándo caduca el token.

Referencia de API

Es posible acceder a la documentación para cada API de Cloud Sync en "Cloud Central de NetApp".

Uso de list API

Las API de la lista son API asíncronas, por lo que el resultado no devuelve de inmediato (por ejemplo: `GET /data-brokers/{id}/list-nfs-export-folders` y.. `GET /data-brokers/{id}/list-s3-buckets`). La única respuesta del servidor es el estado HTTP 202. Para obtener el resultado real, debe usar el `GET /messages/client` API.

Pasos

1. Llame a la API de lista que desea utilizar.
2. Utilice la `GET /messages/client` API para ver el resultado de la operación.
3. Utilice la misma API anexándola con el ID que acaba de recibir: `GET http://cloudsync.netapp.com/api/messages/client?last=<id_from_step_2>`

   Tenga en cuenta que el ID cambia cada vez que llama al `GET /messages/client` API.

ejemplo

Al llamar al `list-s3-buckets` API, los resultados no se devuelven inmediatamente:

```
GET http://cloudsync.netapp.com/api/data-brokers/<data-broker-id>/list-s3-buckets
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

El resultado es el código de estado HTTP 202, lo que significa que el mensaje fue aceptado, pero aún no se ha procesado.

Para obtener el resultado de la operación, debe usar la siguiente API:

```
GET http://cloudsync.netapp.com/api/messages/client
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

El resultado es una matriz con un objeto que incluye un campo ID. El campo Id. Representa el último mensaje enviado por el servidor. Por ejemplo:

```
[
    {
        "header": {
            "requestId": "init",
            "clientId": "init",
            "agentId": "init"
        },
        "payload": {
            "init": {}
        },
        "id": "5801"
    }
]
```

Ahora haría la siguiente llamada a la API mediante el ID que acaba de recibir:

```
GET http://cloudsync.netapp.com/api/messages/client?last=<id_from_step_2>
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

El resultado es un conjunto de mensajes. Dentro de cada mensaje hay un objeto de carga, que consiste en el nombre de la operación (como clave) y su resultado (como valor). Por ejemplo:

```
[
    {
        "payload": {
            "list-s3-buckets": [
                {
                    "tags": [
                        {
                            "Value": "100$",
                            "Key": "price"
                        }
                    ],
                    "region": {
                        "displayName": "US West (Oregon)",
                        "name": "us-west-2"
                    },
                    "name": "small"
                }
            ]
        },
        "header": {
            "requestId": "f687ac55-2f0c-40e3-9fa6-57fb8c4094a3",
            "clientId": "5beb032f548e6e35f4ed1ba9",
            "agentId": "5bed61f4489fb04e34a9aac6"
        },
        "id": "5802"
    }
]
```


Preguntas técnicas frecuentes sobre Cloud Sync

Estas preguntas frecuentes pueden ayudar si sólo está buscando una respuesta rápida a una pregunta.

Primeros pasos

Las siguientes preguntas tratan sobre los primeros pasos con Cloud Sync.

¿Cómo funciona Cloud Sync?

Cloud Sync utiliza el software de intermediarios de datos de NetApp para sincronizar los datos de un origen con un destino (esto se denomina *Sync Relationship*).

El agente de datos controla las relaciones de sincronización entre sus orígenes y destinos. Después de configurar una relación de sincronización, Cloud Sync analiza su sistema de origen y lo divide en varios flujos de replicación para enviar los datos de destino seleccionados.

Después de la copia inicial, el servicio sincroniza los datos modificados con la programación que se haya

establecido.

¿Cómo funciona la prueba gratuita de 14 días?

La prueba gratuita de 14 días se inicia cuando se inscriba en el servicio Cloud Sync. No está sujeto a los cargos por NetApp relacionados con las relaciones con Cloud Sync que cree durante 14 días. Sin embargo, sigue siendo aplicable todo coste por recursos que se cobren a los agentes de datos que se instalen.

¿Cuánto cuesta Cloud Sync?

Hay dos tipos de costos asociados con el uso de Cloud Sync: Cargos por servicios y cargos por recursos.

cargos por servicio

Para los precios de pago por uso, los cargos del servicio Cloud Sync se cobran por hora según el número de relaciones de sincronización que cree.

- "Vea los precios de pago por uso en AWS"
- "Ver precios anuales en AWS"
- "Ver los precios en Azure"

Las licencias de Cloud Sync también están disponibles a través de su representante de NetApp. Cada licencia activa 20 relaciones de sincronización durante 12 meses.

"Más información sobre las licencias".

gastos de recursos

Las cargas de recursos están relacionadas con los costes de informática y almacenamiento para ejecutar el agente de datos en el cloud.

¿Cómo se factura Cloud Sync?

Hay dos formas de pagar las relaciones de sincronización después de que termine su prueba gratuita de 14 días. La primera opción es suscribirse a AWS o Azure, lo que le permite pagar por uso o anualmente. La segunda opción consiste en comprar licencias directamente a NetApp.

¿Puedo usar Cloud Sync fuera del cloud?

Sí, puede usar Cloud Sync en una arquitectura que no sea de cloud. El origen y el destino pueden residir en las instalaciones, por lo que puede hacerlo el agente de datos.

Tenga en cuenta los siguientes puntos clave sobre el uso de Cloud Sync fuera del cloud:

- Para la sincronización en las instalaciones, hay un bloque de Amazon S3 privado disponible a través de StorageGRID de NetApp.
- El agente de datos necesita una conexión a Internet para comunicarse con el servicio Cloud Sync.
- Si no adquiere una licencia directamente a NetApp, necesitará una cuenta de AWS o Azure para la facturación del servicio de PAYGO Cloud Sync.

¿Cómo puedo acceder a Cloud Sync?

Cloud Sync está disponible en Cloud Manager en la ficha **sincronización**.

Orígenes y objetivos compatibles

Las siguientes preguntas relacionadas con el origen y los destinos que se admiten en una relación de sincronización.

¿Qué orígenes y destinos es compatible con Cloud Sync?

Cloud Sync admite muchos tipos distintos de relaciones de sincronización. "Vea toda la lista".

¿Qué versiones de NFS y SMB es compatible Cloud Sync?

Cloud Sync admite NFS versión 3 y posteriores, y SMB versión 1 y posteriores.

"Más información sobre los requisitos de sincronización".

Cuando Amazon S3 es el objetivo, ¿se pueden organizar los datos en niveles en un tipo de almacenamiento S3 específico?

Sí, puede elegir una clase de almacenamiento S3 específica cuando AWS S3 es el destino:

- Estándar (esta es la clase predeterminada)
- Organización en niveles inteligente
- Acceso Estándar-poco frecuente
- Una Zona de acceso poco frecuente
- Glaciar
- Glacier Deep Archive

¿Qué pasa con los niveles de almacenamiento para el almacenamiento de Azure Blob?

Puede elegir un nivel de almacenamiento específico de Azure Blob cuando un contenedor Blob es el destino:

- Almacenamiento en caliente
- Almacenamiento en frío

Redes

Las siguientes preguntas hacen referencia a los requisitos de red de Cloud Sync.

¿Cuáles son los requisitos de red de Cloud Sync?

El entorno de Cloud Sync requiere que el agente de datos esté conectado al origen y al destino a través del protocolo seleccionado (NFS, SMB, EFS) o de la API de almacenamiento de objetos (Amazon S3, Azure Blob, IBM Cloud Object Storage).

Además, el agente de datos necesita una conexión a Internet saliente a través del puerto 443 para que pueda comunicarse con el servicio Cloud Sync y ponerse en contacto con otros servicios y repositorios.

Si quiere más información, "revise los requisitos de red".

¿Existen limitaciones de red relacionadas con la conectividad de Data broker?

Los agentes de datos requieren acceso a Internet. No ofrecemos compatibilidad con un servidor proxy cuando implantamos el agente de datos en Azure o Google Cloud Platform.

Sincronización de datos

Las siguientes preguntas se refieren a cómo funciona la sincronización de datos.

¿con qué frecuencia se produce la sincronización?

La programación predeterminada se define para la sincronización diaria. Después de la sincronización inicial, puede:

- Modifique la programación de sincronización con el número de días, horas o minutos que desee
- Deshabilite la programación de sincronización
- Eliminar la programación de sincronización (no se perderán datos; solo se eliminará la relación de sincronización)

¿Cuál es el programa de sincronización mínimo?

Puede programar una relación para que se sincronice datos con una frecuencia de hasta cada 1 minuto.

¿vuelve a intentar el agente de datos cuando un archivo no se puede sincronizar? ¿o se agote el tiempo de espera?

El agente de datos no se agotó cuando un único archivo no se transfiere. En su lugar, el agente de datos reintenta 3 veces antes de omitir el archivo. El valor de reintento se puede configurar en la configuración de una relación de sincronización.

"Aprenda a cambiar la configuración de una relación de sincronización".

¿y si tengo un conjunto de datos muy grande?

Si un único directorio contiene 600,000 archivos o más, contact US para que le podamos ayudar a configurar el agente de datos para manejar la carga. Es posible que necesitemos agregar memoria adicional al equipo de Data broker.

Seguridad

Las siguientes preguntas están relacionadas con la seguridad.

¿es Cloud Sync seguro?

Sí. Toda la conectividad de redes del servicio Cloud Sync se realiza mediante "Amazon simple Queue Service (SQS)".

Toda la comunicación entre el agente de datos y Amazon S3, Azure Blob, Google Cloud Storage y IBM Cloud Object Storage se realiza mediante el protocolo HTTPS.

Si utiliza Cloud Sync con sistemas en las instalaciones (origen o destino), puede ver algunas opciones de conectividad recomendadas:

- Una conexión de AWS Direct Connect, Azure ExpressRoute o Google Cloud Interconnect, que no es enrutada por Internet (y solo puede comunicarse con las redes cloud que especifique).
- Una conexión VPN entre el dispositivo de puerta de enlace local y el redes cloud
- Para obtener una transferencia de datos más segura con bloques S3, almacenamiento de Azure Blob o Google Cloud Storage, se puede establecer un Amazon Private S3 Endpoint, extremos de servicio de red virtual de Azure o Google Private Access.

Cualquiera de estos métodos establece una conexión segura entre los servidores NAS locales y un agente de datos Cloud Sync.

¿los datos están cifrados por Cloud Sync?

- Cloud Sync admite el cifrado de datos en tiempo real entre los servidores NFS de origen y de destino. "Leer más".
- SMB no es compatible con el cifrado.
- Cuando un bloque de Amazon S3 es el destino de una relación de sincronización, puede elegir si habilitar el cifrado de datos mediante el cifrado AWS KMS o el cifrado AES-256.

Permisos

Las siguientes preguntas se refieren a los permisos de datos.

¿los permisos de datos del SMB se sincronizan con la ubicación de destino?

Es posible configurar Cloud Sync para que se conserven las listas de control de acceso (ACL) entre un recurso compartido de SMB de origen y un recurso compartido de SMB de destino. También puede copiar manualmente las ACL usted mismo. "Aprenda a copiar ACL entre recursos compartidos de SMB".

¿los permisos de datos NFS se sincronizan con la ubicación de destino?

Cloud Sync copia automáticamente los permisos de NFS entre servidores NFS de la siguiente forma:

- NFS versión 3: Cloud Sync copia los permisos y el propietario del grupo de usuarios.
- NFS versión 4: Cloud Sync copia las ACL.

Rendimiento

Las siguientes preguntas están relacionadas con el rendimiento de Cloud Sync.

¿Qué representa el indicador de progreso de una relación de sincronización?

La relación de sincronización muestra el rendimiento del adaptador de red del agente de datos. Si aceleró el rendimiento de sincronización mediante el uso de varios agentes de datos, el rendimiento será la suma de todo el tráfico. Este rendimiento se actualiza cada 20 segundos.

Estoy experimentando problemas de rendimiento. ¿podemos limitar el número de transferencias simultáneas?

El agente de datos puede sincronizar 4 archivos a la vez. Si tiene archivos muy grandes (varios TB cada uno), puede tardar mucho tiempo en completar el proceso de transferencia y el rendimiento puede verse afectado.

Limitar el número de transferencias simultáneas puede ser de ayuda. Mailto:ng-cloudsync-

support@netapp.com[Contacte con nosotros para obtener ayuda].

¿por qué estoy experimentando un bajo rendimiento con Azure NetApp Files?

Al sincronizar datos con o desde Azure NetApp Files, es posible que experimente errores y problemas de rendimiento si el nivel de servicio del disco es estándar.

Cambie el nivel de servicio a Premium o Ultra para mejorar el rendimiento de la sincronización.

"Obtenga más información acerca de los niveles de servicio y el rendimiento de Azure NetApp Files".

¿por qué estoy experimentando un bajo rendimiento con Cloud Volumes Service para AWS?

Al sincronizar datos con un volumen de cloud o desde este, es posible que experimente errores y problemas de rendimiento si el nivel de rendimiento del volumen de cloud es estándar.

Cambie el nivel de servicio a Premium o Extreme para mejorar el rendimiento de la sincronización.

¿Cuántos agentes de datos son necesarios?

Al crear una nueva relación, comienza con un único agente de datos (a menos que haya seleccionado un agente de datos existente que pertenezca a una relación de sincronización acelerada). En muchos casos, un único agente de datos puede satisfacer los requisitos de rendimiento de una relación de sincronización. Si no lo hace, puede acelerar el rendimiento de la sincronización añadiendo agentes de datos adicionales. Pero primero debe comprobar otros factores que pueden afectar al rendimiento de la sincronización.

El rendimiento de la transferencia de datos puede afectar múltiples factores. El rendimiento general de la sincronización puede verse afectado debido al ancho de banda de la red, la latencia y la topología de la red, así como las especificaciones del equipo virtual del agente de datos y el rendimiento del sistema de almacenamiento. Por ejemplo, un solo agente de datos en una relación de sincronización puede alcanzar los 100 MB/s, mientras que el rendimiento del disco en el destino sólo puede permitir 64 MB/s. Como resultado, el agente de datos sigue intentando copiar los datos, pero el objetivo no puede satisfacer el rendimiento del agente de datos.

Por lo tanto, asegúrese de comprobar el rendimiento de la red y del disco en el destino.

A continuación, puede plantearse acelerar el rendimiento de sincronización añadiendo un agente de datos adicional para compartir la carga de dicha relación. "Descubra cómo acelerar el rendimiento de la sincronización".

Eliminar cosas

Las siguientes preguntas tratan de eliminar relaciones de sincronización y datos de orígenes y destinos.

¿Qué sucede si elimino mi relación con Cloud Sync?

Al eliminar una relación se detienen todos los datos futuros y se termina el pago. Todos los datos que se sincronizaron con el destino siguen siendo tal cual.

¿Qué ocurre si se elimina algo de mi servidor de origen? ¿se ha eliminado del objetivo también?

De forma predeterminada, si tiene una relación de sincronización activa, el elemento eliminado en el servidor de origen no se eliminará del destino durante la siguiente sincronización. Pero hay una opción en la configuración de sincronización para cada relación, donde puede definir que Cloud Sync eliminará los archivos de la ubicación de destino si se eliminaron del origen.

"Aprenda a cambiar la configuración de una relación de sincronización".

¿Qué sucede si elimino algo de mi destino? ¿se ha eliminado de mi fuente también?

Si se elimina un elemento del destino, no se eliminará del origen. La relación es unidireccional, desde la fuente hasta el objetivo. En el siguiente ciclo de sincronización, Cloud Sync compara el origen con el destino, identifica que falta el elemento y Cloud Sync lo copia de nuevo del origen al destino.

Resolución de problemas

"Base de conocimientos de NetApp: Preguntas frecuentes de Cloud Sync: Soporte y solución de problemas"

Análisis en profundidad de los agentes de datos

La siguiente pregunta se refiere al agente de datos.

¿puede explicar la arquitectura del agente de datos?

Claro. Estos son los puntos más importantes:

- Data broker es una aplicación node.js que se ejecuta en un host Linux.
- Cloud Sync implementa el agente de datos de la siguiente manera:
  - AWS: Desde una plantilla AWS CloudFormation
  - Azure: Desde Azure Resource Manager
  - Google: De Google Cloud Deployment Manager
  - Si utiliza su propio host Linux, debe instalar manualmente el software
- El software Data broker se actualiza automáticamente a la última versión.
- El agente de datos utiliza AWS SQS como un canal de comunicación fiable y seguro, y para el control y la supervisión. SQS también proporciona una capa de persistencia.
- Puede agregar agentes de datos adicionales a una relación para aumentar la velocidad de transferencia y agregar alta disponibilidad. Hay resiliencia de servicios si un agente de datos falla.

Obtenga información sobre la privacidad de sus datos

Más información sobre Cloud Compliance

Cloud Compliance es un servicio de cumplimiento de normativas y privacidad de datos para Cloud Manager que analiza sus volúmenes, bloques de Amazon S3 y bases de datos para identificar los datos personales y confidenciales que se encuentran en esos archivos. Con la tecnología impulsada por la inteligencia artificial (IA), Cloud Compliance ayuda a las organizaciones a comprender el contexto de los datos e identificar los datos confidenciales.

"Obtenga información sobre los casos de uso de Cloud Compliance".

Funciones

Cloud Compliance proporciona varias herramientas que le ayudan en sus tareas de cumplimiento de normativas. Puede usar Cloud Compliance para:

- Identificación de la Información personal de identificación (PII).
- Identificar un amplio abanico de información confidencial que requieran las normativas de privacidad del RGPD, la CCPA, el PCI y la HIPAA
- Responder a solicitudes de acceso de sujetos de datos (DSAR)

Entornos de trabajo y fuentes de datos compatibles

Cloud Compliance puede analizar datos de los siguientes tipos de orígenes de datos:

- Cloud Volumes ONTAP en AWS
- Cloud Volumes ONTAP en Azure
- Azure NetApp Files
- Amazon S3
- Bases de datos que residen en cualquier ubicación (no hay ningún requisito de que la base de datos resida en un entorno de trabajo)

Nota: para Azure NetApp Files, Cloud Compliance puede analizar cualquier volumen que se encuentre en la misma región que Cloud Manager.

Coste

- El coste de utilizar Cloud Compliance depende de la cantidad de datos que se escanee. A partir del 7 de octubre de 2020, el primer TB de datos que analiza Cloud Compliance en un espacio de trabajo de Cloud Manager es gratuito. Esto incluye datos de Cloud Volumes ONTAP Volumes, Azure NetApp Files Volumes, bloques de Amazon S3 y esquemas de base de datos. Es necesario contar con una suscripción a AWS o Azure Marketplace para seguir analizando los datos después de ese punto. Consulte "precios" para obtener más detalles.

  "Aprenda a suscribirse".

- La instalación de Cloud Compliance requiere la puesta en marcha de una instancia de cloud, que resulta en cobros al proveedor de cloud en el que se ha puesto en marcha. Consulte el tipo de instancia que se pone en marcha en cada cloud proveedor
- Cloud Compliance requiere que haya implementado un conector. En muchos casos ya tiene un conector debido a otro almacenamiento y servicios que utiliza en Cloud Manager. La instancia de Connector representa cargos del proveedor de cloud en el que se ha puesto en marcha. Consulte "tipo de instancia que se pone en marcha para cada proveedor de cloud".

Costes de transferencia de datos

Los costes de la transferencia de datos dependen de su configuración. Si la instancia y el origen de datos de Cloud Compliance se encuentran en la misma zona de disponibilidad y región, no habrá costes de transferencia de datos. Pero si el origen de los datos, como un clúster de Cloud Volumes ONTAP o un bloque de S3, está en una zona o región *diferente*, su proveedor de cloud le cobrará los costes de transferencia de datos. Consulte estos enlaces para obtener más información:

- "AWS: Precios de Amazon EC2"
- "Microsoft Azure: Detalles de precios del ancho de banda"

Cómo funciona Cloud Compliance

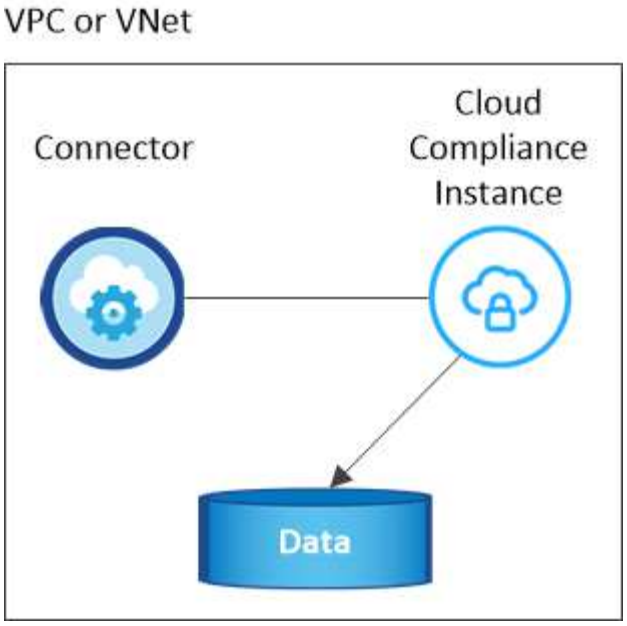
En un nivel superior, Cloud Compliance funciona como esta:

1. Se implementa una instancia de Cloud Compliance en Cloud Manager.
2. Se habilita en uno o más entornos de trabajo o bases de datos.
3. Cloud Compliance analiza los datos mediante un proceso de aprendizaje de IA.
4. En Cloud Manager, haga clic en **conformidad** y utilice el panel y las herramientas de informes proporcionados para ayudarle en sus esfuerzos de cumplimiento.

La instancia de Cloud Compliance

Al habilitar Cloud Compliance, Cloud Manager implementa una instancia de Cloud Compliance en la misma subred que Connector. "Más información sobre conectores."

Si el conector está instalado en las instalaciones, pone en marcha la instancia de Cloud Compliance en el mismo VPC o vnet que el primer sistema Cloud Volumes ONTAP de la solicitud.



Tenga en cuenta lo siguiente acerca de la instancia:

- En Azure, Cloud Compliance se ejecuta en una máquina virtual Standard_D16s_v3 con un disco de 512 GB.
- En AWS, Cloud Compliance se ejecuta en una instancia de 5,4 x grande con un disco GP2 de 500 GB.

  En regiones donde no hay m5.4xLarge disponible, Cloud Compliance se ejecuta en lugar de una instancia m4.4xLarge.

  No se admite el cambio o cambio de tamaño del tipo de máquina virtual/instancia. Debe utilizar el tamaño que se proporciona.

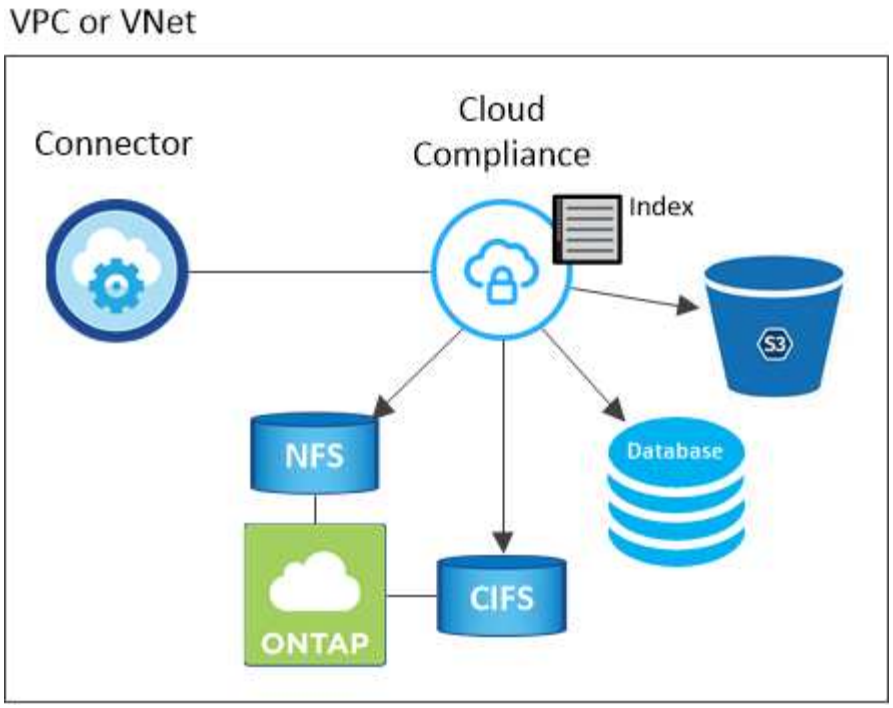
- La instancia se denomina *CloudCompliance* con un hash generado (UUID) concatenado. Por ejemplo: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*
- Solo se implementa una instancia de Cloud Compliance por conector.
- Las actualizaciones del software de Cloud Compliance se automatizan, ya que no tiene que preocuparse por ello.

La instancia debe permanecer en ejecución en todo momento debido a que Cloud Compliance analiza los datos de forma continua.

Cómo funcionan las exploraciones

Después de habilitar Cloud Compliance y seleccionar los esquemas de volúmenes, bloques o bases de datos que desea analizar, comienza de inmediato a analizar los datos para identificar datos personales y confidenciales. Asigna los datos de la organización, categoriza cada archivo e identifica y extrae entidades y patrones predefinidos en los datos. El resultado de la exploración es un índice de información personal, información personal confidencial y categorías de datos.

Cloud Compliance se conecta a los datos como cualquier otro cliente al montar volúmenes NFS y CIFS. Se accede automáticamente a los volúmenes NFS como de solo lectura, mientras que se necesitan proporcionar credenciales de Active Directory para analizar volúmenes CIFS.



Después del análisis inicial, Cloud Compliance analiza continuamente cada volumen para detectar cambios incrementales (por eso es importante mantener la instancia en ejecución).

Puede activar y desactivar los análisis en el "nivel de volumen", en la "nivel de cucharón", y en el "nivel de esquema de base de datos".

Información que indexa Cloud Compliance

Cloud Compliance recopila, indexa y asigna categorías a datos no estructurados (archivos). Los datos que indexa Cloud Compliance incluyen los siguientes:

Metadatos estándar

Cloud Compliance recopila metadatos estándar sobre los archivos: El tipo de archivo, su tamaño, fechas de creación y modificación, etc.

Datos personales

Información de identificación personal, como direcciones de correo electrónico, números de identificación o números de tarjetas de crédito. "Más información sobre datos personales".

Datos personales confidenciales

Tipos especiales de información confidencial, como datos sanitarios, origen étnico o opiniones políticas, según lo define el RGPD y otras regulaciones de privacidad. "Más información sobre datos personales confidenciales".

Categorías

Cloud Compliance toma los datos que ha analizado y los divide en diferentes tipos de categorías. Las categorías son temas basados en el análisis de IA del contenido y los metadatos de cada archivo. "Más información sobre categorías".

Reconocimiento de entidad de nombre

Cloud Compliance utiliza la IA para extraer los nombres de las personas naturales de los documentos. "Obtenga información sobre cómo responder a las solicitudes de acceso a sujetos de datos".

Información general sobre redes

Cloud Manager implementa la instancia de Cloud Compliance con un grupo de seguridad que permite conexiones HTTP entrantes desde la instancia de Connector.

Cuando se utiliza Cloud Manager en modo SaaS, la conexión a Cloud Manager se ofrece mediante HTTPS y los datos privados enviados entre el explorador y la instancia de Cloud Compliance se protegen con cifrado integral, lo que significa que NetApp y terceros no pueden leerlo.

Si necesita utilizar la interfaz de usuario local en lugar de la interfaz de usuario SaaS por cualquier motivo, puede seguir siendo así "Acceda a la interfaz de usuario local".

Las reglas salientes están completamente abiertas. Se necesita acceso a Internet para instalar y actualizar el software Cloud Compliance y enviar mediciones de uso.

Si tiene requisitos estrictos de red, "Obtenga información sobre los extremos con los que se contacta Cloud Compliance".

Acceso de los usuarios a la información de cumplimiento

La función a la que se ha asignado cada usuario proporciona distintas funcionalidades dentro de Cloud Manager y dentro de Cloud Compliance:

- **los administradores de cuentas** pueden administrar la configuración de cumplimiento y ver la información de cumplimiento de todos los entornos de trabajo.
- **los administradores de espacio de trabajo** pueden administrar la configuración de cumplimiento y ver la información de cumplimiento sólo para los sistemas a los que tienen permisos de acceso. Si un administrador de área de trabajo no puede tener acceso a un entorno de trabajo en Cloud Manager, no podrá ver ninguna información de cumplimiento para el entorno de trabajo en la ficha cumplimiento.
- Los usuarios con la función **Cloud Compliance Viewer** sólo pueden ver información de cumplimiento y generar informes para los sistemas a los que tienen permiso de acceso. Estos usuarios no pueden habilitar o deshabilitar el análisis de volúmenes, bloques o esquemas de base de datos.

"Más información acerca de los roles de Cloud Manager" y cómo "añadir usuarios con roles específicos".

Manos a la obra

Ponga en marcha el cumplimiento normativo del cloud

Complete algunos pasos para implementar la instancia de Cloud Compliance en el espacio de trabajo de Cloud Manager.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

Cree un conector

Si aún no tiene un conector, cree un conector en Azure o AWS. Consulte "Creación de un conector en AWS" o. "Creación de un conector en Azure".

Revise los requisitos previos

Asegúrese de que su entorno de nube pueda cumplir con los requisitos previos, que incluyen 16 vCPU para la instancia de Cloud Compliance, acceso saliente a Internet para la instancia, conectividad entre el conector y Cloud Compliance a través del puerto 80, etc. Vea la lista completa.

Ponga en marcha el cumplimiento normativo del cloud

Inicie el asistente de instalación para implementar la instancia de Cloud Compliance en Cloud Manager.

Suscríbase al servicio Cloud Compliance

Los primeros 1 TB de datos que analiza Cloud Compliance en Cloud Manager son gratuitos. Es necesario contar con una suscripción a AWS o Azure Marketplace para seguir analizando los datos después de ese punto.

Creación de un conector

Si aún no tiene un conector, cree un conector en Azure o AWS. Consulte "Creación de un conector en AWS" o. "Creación de un conector en Azure". En la mayoría de los casos probablemente tendrá un juego de conectores Realice el primero antes de intentar activar Cloud Compliance porque la mayoría "Las funciones de Cloud Manager requieren un conector", pero hay casos en los que necesita configurar uno ahora.

Hay algunas situaciones en las que debe utilizar un conector en AWS o Azure para Cloud Compliance.

- Cuando se escanea datos en Cloud Volumes ONTAP en AWS o en bloques de AWS S3, se utiliza un conector en AWS.
- Al analizar datos en Cloud Volumes ONTAP en Azure o en Azure NetApp Files, utiliza un conector en Azure.
- Las bases de datos se pueden escanear con cualquiera de los conectores.

Como puede ver, puede que haya algunas situaciones en las que necesite utilizar "Múltiples conectores".

Si está planeando el análisis de Azure NetApp Files, debe asegurarse de que está implementando en la misma región que los volúmenes que desea analizar.

Revisión de requisitos previos

Revise los siguientes requisitos previos para asegurarse de tener una configuración compatible antes de implementar Cloud Compliance.

Habilite el acceso saliente a Internet

Cloud Compliance requiere acceso a Internet de salida. Si la red virtual utiliza un servidor proxy para el acceso a Internet, asegúrese de que la instancia de Cloud Compliance tiene acceso saliente a Internet para ponerse en contacto con los siguientes extremos. Tenga en cuenta que Cloud Manager implementa la instancia de Cloud Compliance en la misma subred que Connector.

Puntos finales	Específico
https://cloudmanager.cloud.netapp.com	Comunicación con el servicio Cloud Manager, que incluye cuentas de Cloud Central.
https://netapp-cloud-account.auth0.com https://auth0.com	Comunicación con Cloud Central de NetApp para la autenticación de usuario centralizada.
https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Proporciona acceso a imágenes, manifiestos y plantillas de software.
https://kinesis.us-east-1.amazonaws.com	Permite a NetApp transmitir datos desde registros de auditoría.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com	Permite a Cloud Compliance acceder y descargar manifiestos y plantillas, así como enviar registros y métricas.

Compruebe que Cloud Manager tenga los permisos necesarios

Asegúrese de que Cloud Manager tiene permisos para implementar recursos y crear grupos de seguridad para la instancia de Cloud Compliance. Puede encontrar los permisos más recientes de Cloud Manager en "Las políticas proporcionadas por NetApp".

Compruebe sus límites de vCPU

Compruebe que el límite de vCPU de su proveedor de cloud permita poner en marcha una instancia con 16 núcleos. Deberá comprobar el límite de vCPU para la familia de instancias relevante en la región donde se ejecuta Cloud Manager.

En AWS, la familia de instancias es *On-Demand Standard Instances*. En Azure, la familia de instancias es *Standard DSv3 Family*.

Para obtener más información sobre los límites de vCPU, consulte lo siguiente:

- "Documentación de AWS: Límites del servicio de Amazon EC2"
- "Documentación de Azure: Cuotas de vCPU de máquina virtual"

Compruebe que Cloud Manager pueda acceder a Cloud Compliance

Garantice la conectividad entre el conector y la instancia de Cloud Compliance. El grupo de seguridad del conector debe permitir el tráfico entrante y saliente a través del puerto 80 hacia y desde la instancia de Cloud Compliance.

Esta conexión permite la implementación de la instancia de Cloud Compliance y permite ver información en la ficha cumplimiento.

Configurar el descubrimiento de Azure NetApp Files

Antes de poder analizar volúmenes para Azure NetApp Files, "Cloud Manager debe configurarse para detectar la configuración".

Asegúrese de poder mantener Cloud Compliance en funcionamiento

La instancia de Cloud Compliance debe permanecer activa para analizar sus datos de forma continua.

Asegúrese de que la conectividad del navegador web es compatible con Cloud Compliance

Después de habilitar Cloud Compliance, asegúrese de que los usuarios acceden a la interfaz de Cloud Manager desde un host que tiene una conexión con la instancia de Cloud Compliance.

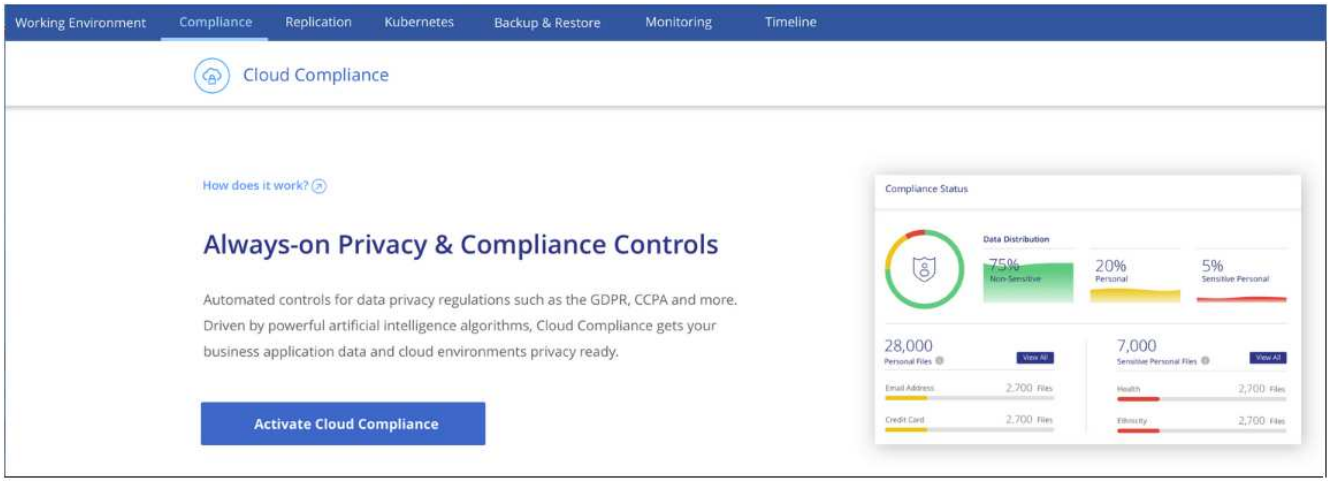
La instancia de Cloud Compliance utiliza una dirección IP privada para garantizar que no se pueda acceder a Internet a los datos indexados. Como resultado, el explorador web que utiliza para acceder a Cloud Manager debe tener una conexión con esa dirección IP privada. Esta conexión puede provenir de una conexión directa a AWS o Azure (por ejemplo, una VPN) o de un host que está dentro de la misma red que la instancia de Cloud Compliance.

Implementación de la instancia de Cloud Compliance

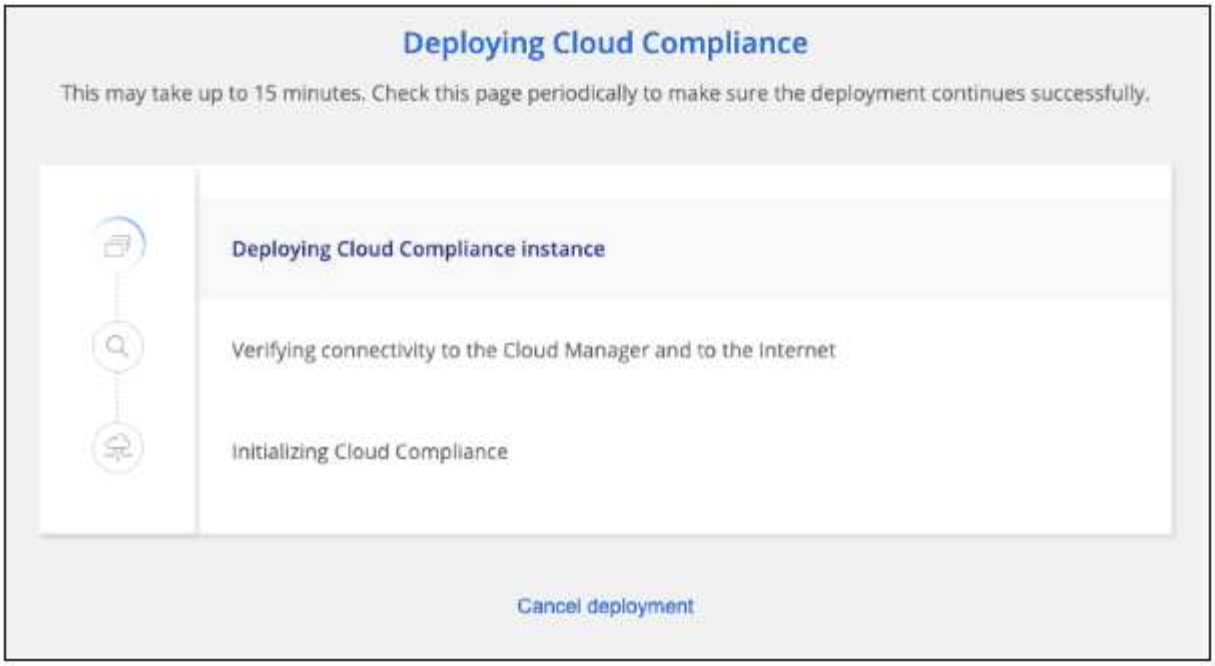
Se implementa una instancia de Cloud Compliance para cada instancia de Cloud Manager.

Pasos

1. En Cloud Manager, haga clic en **Cloud Compliance**.
2. Haga clic en **Activar Cloud Compliance** para iniciar el asistente de implementación.



3. El asistente muestra el progreso a medida que avanza por los pasos de implementación. Se detendrá y pedirá información si se presenta algún problema.



4. Cuando se despliegue la instancia, haga clic en **continuar con la configuración** para ir a la página *Scan Configuration*.

Resultado

Cloud Manager pone en marcha la instancia de Cloud Compliance en su proveedor de cloud.

El futuro

En la página Scan Configuration (Configuración de exploración), puede seleccionar los entornos de trabajo, los volúmenes y los bloques que desea analizar para el cumplimiento normativo. También puede conectarse a un servidor de base de datos para analizar esquemas de base de datos específicos. Active Cloud Compliance en cualquiera de estos orígenes de datos.

Suscripción al servicio Cloud Compliance

Los primeros 1 TB de datos que analiza Cloud Compliance en un espacio de trabajo de Cloud Manager son gratuitos. Es necesario contar con una suscripción a AWS o Azure Marketplace para seguir analizando los datos después de ese punto.

Puede suscribirse en cualquier momento y no se le cobrará hasta que la cantidad de datos supere 1 TB. Siempre puede ver la cantidad total de datos que se analizan en la consola de cumplimiento de normativas del cloud. Y el botón *Subscribe Now* facilita la suscripción cuando esté listo.

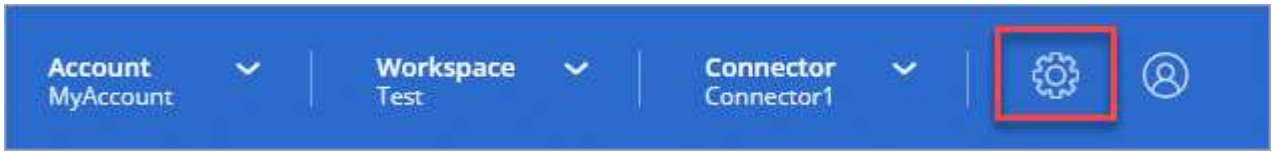
Nota: Si se le solicita la suscripción a Cloud Compliance, pero ya tiene una suscripción a Azure, probablemente utilice la antigua suscripción **Cloud Manager** y tendrá que cambiar a la nueva suscripción **NetApp Cloud Manager**. ConsulteCambiar al nuevo plan Cloud Manager de NetApp en Azure para obtener

más detalles.

Pasos

Un usuario que tenga la función *Account Admin* debe completar estos pasos.

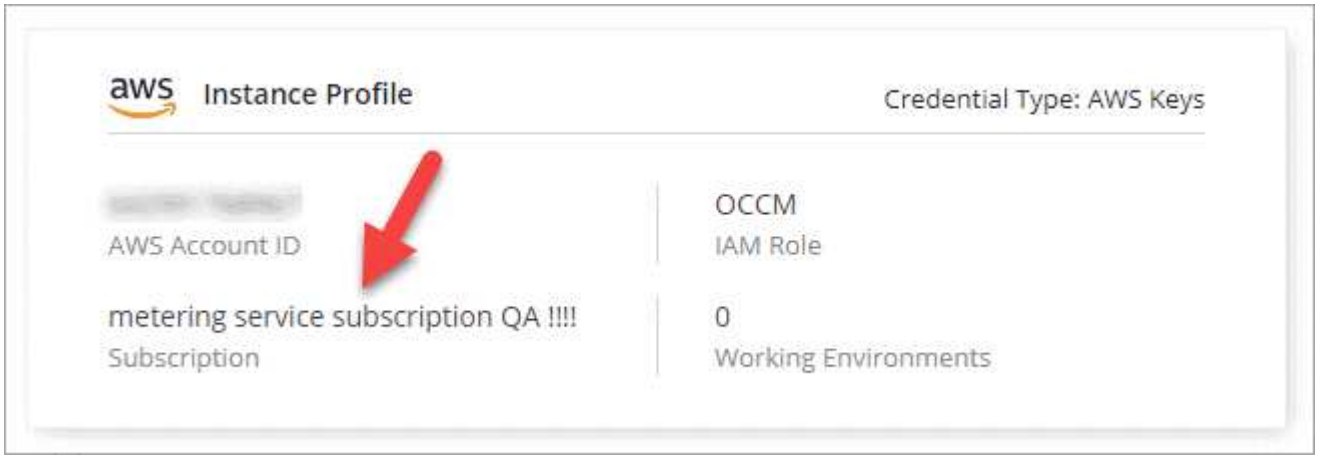
1. En la esquina superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **credenciales**.



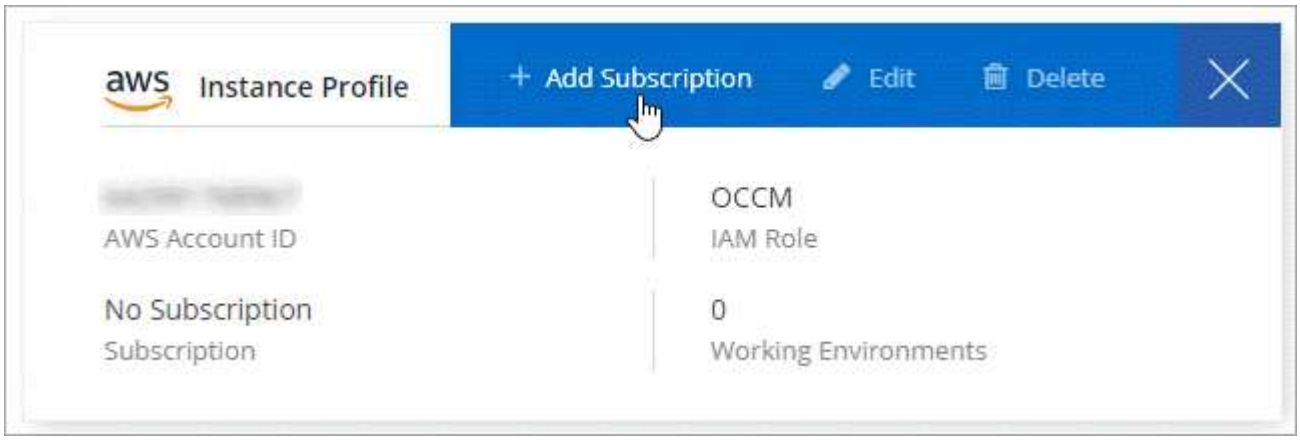
2. Busque las credenciales para el perfil de instancia de AWS o la identidad del servicio gestionado de Azure.

   La suscripción debe agregarse al perfil de instancia o a la identidad del servicio gestionado. La carga no funcionará de otro modo.

   Si ya tienes una suscripción, entonces estás todo establecido, no hay nada más que hacer.



3. Si todavía no tiene una suscripción, pase el cursor sobre las credenciales y haga clic en el menú de acciones.
4. Haga clic en **Agregar suscripción**.



5. Haga clic en **Agregar suscripción**, haga clic en **continuar** y siga los pasos.

En el siguiente vídeo se muestra cómo asociar una suscripción de Marketplace a una suscripción de AWS:

► https://docs.netapp.com/es-es/occm38//media/video_subscribing_aws.mp4 *(video)*

En el siguiente vídeo se muestra cómo asociar una suscripción de Marketplace a una suscripción de Azure:

► https://docs.netapp.com/es-es/occm38//media/video_subscribing_azure.mp4 *(video)*

Cambie al nuevo plan de Cloud Manager en Azure

Cloud Compliance se ha añadido a la suscripción a Azure Marketplace llamada * NetApp Cloud Manager* a partir del 7 de octubre de 2020. Si ya tiene la suscripción original de Azure **Cloud Manager**, no le permitirá utilizar Cloud Compliance.

Debe seguir estos pasos, seleccionar la nueva suscripción **NetApp Cloud Manager** y, a continuación, eliminar la antigua suscripción **Cloud Manager**.

> Si su suscripción existente se emitió con una oferta especial privada, debe ponerse en contacto con NetApp para que podamos emitir una nueva oferta especial privada con el cumplimiento incluido.

Pasos

Estos pasos son similares a añadir una nueva suscripción como se describe anteriormente, pero varían en algunos lugares.

1. En la esquina superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **credenciales**.
2. Busque las credenciales de la identidad de servicio gestionado de Azure para las que desea cambiar la suscripción y pase el ratón sobre las credenciales y haga clic en **Suscripción asociada**.

   Se muestran los detalles de su suscripción de Marketplace actual.

3. Haga clic en **Agregar suscripción**, haga clic en **continuar** y siga los pasos. Se le redirigirá al portal de Azure para crear la nueva suscripción.
4. Asegúrese de seleccionar el plan **NetApp Cloud Manager** que proporciona acceso a Cloud Compliance y no a Cloud Manager*.
5. Siga los pasos del vídeo para asociar una suscripción de Marketplace a una suscripción de Azure:

   ► https://docs.netapp.com/es-es/occm38//media/video_subscribing_azure.mp4 *(video)*

6. Vuelva a Cloud Manager, seleccione la nueva suscripción y haga clic en **asociado**.
7. Para verificar que ha cambiado su suscripción, pase el cursor sobre la suscripción “i” anterior en la tarjeta Credentials.

   Ahora puede cancelar la suscripción antigua en el portal de Azure.

8. En el portal de Azure, vaya a Software como servicio (SaaS), seleccione la suscripción y haga clic en **Anular la suscripción**.

Active el análisis en sus orígenes de datos

Primeros pasos con el cumplimiento de normativas cloud para Cloud Volumes ONTAP y Azure NetApp Files

Complete unos pasos para comenzar a utilizar el cumplimiento de normativas cloud para Cloud Volumes ONTAP o Azure NetApp Files.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

Implemente la instancia de Cloud Compliance

"Ponga en marcha Cloud Compliance en Cloud Manager" si aún no hay una instancia implementada.

Habilite el cumplimiento de normativas del cloud en sus entornos de trabajo

Haga clic en **Cloud Compliance**, seleccione la ficha **Configuración** y active los análisis de cumplimiento para entornos de trabajo específicos.

Garantice el acceso a los volúmenes

Ahora que Cloud Compliance está habilitado, asegúrese de que pueda acceder a los volúmenes.

- La instancia de Cloud Compliance necesita una conexión de red para cada subred de Cloud Volumes ONTAP o subred de Azure NetApp Files.
- Los grupos de seguridad para Cloud Volumes ONTAP deben permitir conexiones entrantes desde la instancia de Cloud Compliance.
- Las políticas de exportación de volúmenes de NFS deben permitir el acceso desde la instancia de Cloud Compliance.
- Cloud Compliance necesita credenciales de Active Directory para analizar volúmenes CIFS.

  Haga clic en **Cloud Compliance** > **Scan Configuration** > **Edit CIFS Credentials** y proporcione las credenciales. Las credenciales pueden ser de sólo lectura, pero al proporcionar credenciales de administrador se garantiza que Cloud Compliance pueda leer datos que requieran permisos elevados.

Configure los volúmenes que desea analizar

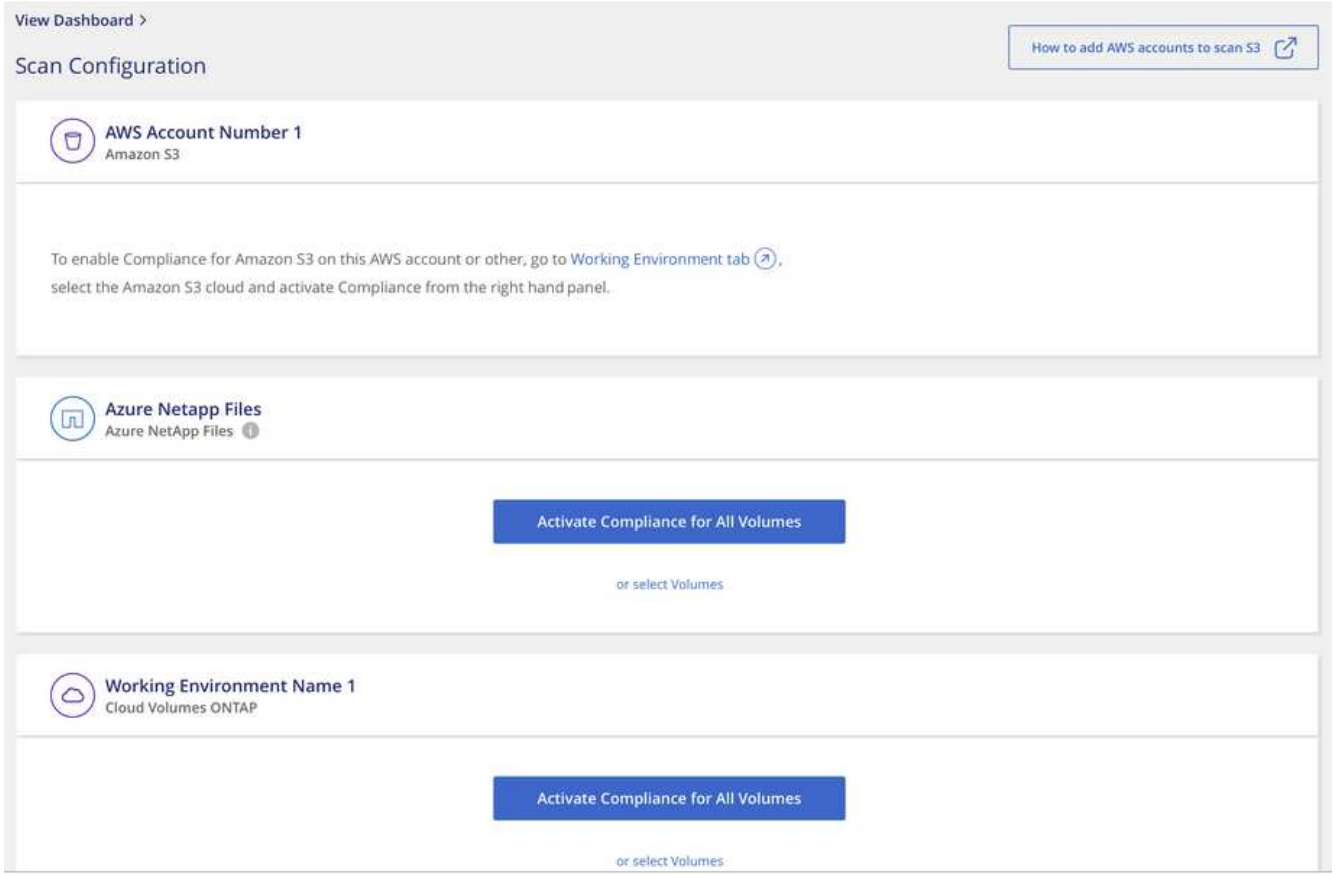
Seleccione los volúmenes que desea analizar y Cloud Compliance empezará a analizarlos.

Implementación de la instancia de Cloud Compliance

"Ponga en marcha Cloud Compliance en Cloud Manager" si aún no hay una instancia implementada.

Habilitar Cloud Compliance en sus entornos de trabajo

1. En la parte superior de Cloud Manager, haga clic en **cumplimiento de la nube** y, a continuación, seleccione la ficha **Configuración**.



2. Para analizar todos los volúmenes de un entorno de trabajo, haga clic en **Activar conformidad para todos los volúmenes**.

   Para analizar sólo ciertos volúmenes en un entorno de trabajo, haga clic en **o seleccione volúmenes** y, a continuación, elija los volúmenes que desea analizar.

Consulte Habilitar y deshabilitar los análisis de cumplimiento de normativas en los volúmenes para obtener más detalles.

Resultado

Cloud Compliance comienza a analizar los datos en cada entorno de trabajo. Los resultados estarán disponibles en la consola de cumplimiento tan pronto como Cloud Compliance termine los análisis iniciales. El tiempo que se tarda en depende de la cantidad de datos; puede que sea unos minutos u horas.

Comprobación de que Cloud Compliance tiene acceso a los volúmenes

Para asegurarse de que Cloud Compliance pueda acceder a los volúmenes, compruebe su red, los grupos de seguridad y las políticas de exportación. Necesitará proporcionar cumplimiento normativo del cloud con credenciales CIFS para poder acceder a volúmenes CIFS.

Pasos

1. Asegúrese de que haya una conexión de red entre la instancia de Cloud Compliance y cada red que incluya los volúmenes para Cloud Volumes ONTAP o Azure NetApp Files.

Para Azure NetApp Files, Cloud Compliance solo puede analizar volúmenes que se encuentren en la misma región que Cloud Manager.

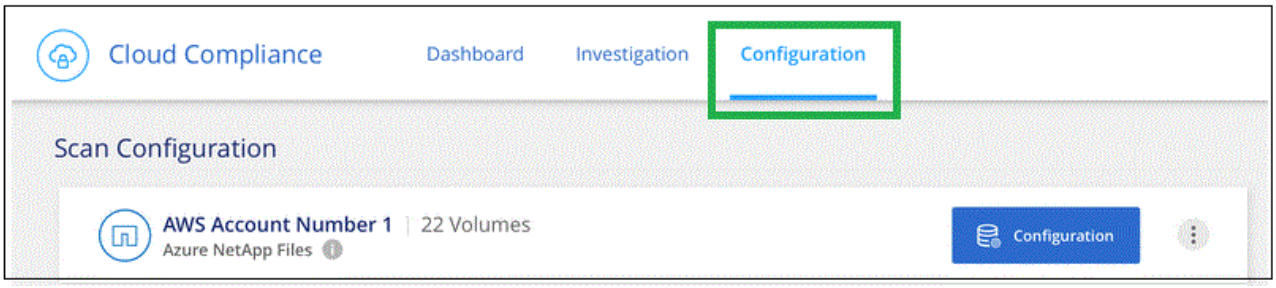
2. Asegúrese de que el grupo de seguridad para Cloud Volumes ONTAP permite el tráfico entrante desde la instancia de Cloud Compliance.

   Puede abrir el grupo de seguridad para el tráfico desde la dirección IP de la instancia de Cloud Compliance, o bien puede abrir el grupo de seguridad para todo el tráfico desde dentro de la red virtual.

3. Compruebe que las políticas de exportación de volúmenes NFS incluyan la dirección IP de la instancia de Cloud Compliance para poder acceder a los datos de cada volumen.
4. Si utiliza CIFS, proporcione Cloud Compliance con credenciales de Active Directory para que pueda analizar volúmenes CIFS.

   a. En la parte superior de Cloud Manager, haga clic en **Cloud Compliance**.

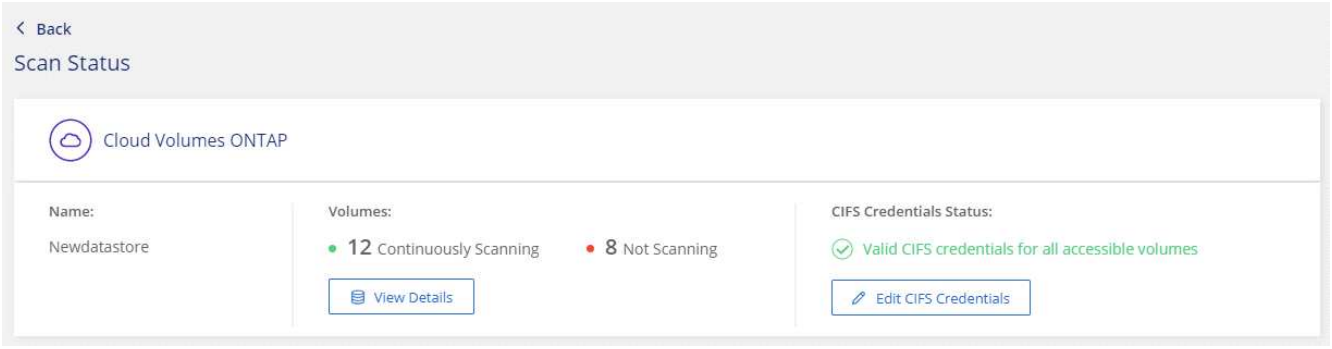
   b. Haga clic en la ficha **Configuración**.



   c. Para cada entorno de trabajo, haga clic en **Editar credenciales CIFS** e introduzca el nombre de usuario y la contraseña que Cloud Compliance necesita para acceder a los volúmenes CIFS en el sistema.

      Las credenciales pueden ser de sólo lectura, pero al proporcionar credenciales de administrador se garantiza que Cloud Compliance pueda leer cualquier dato que requiera permisos elevados. Las credenciales se almacenan en la instancia de Cloud Compliance.

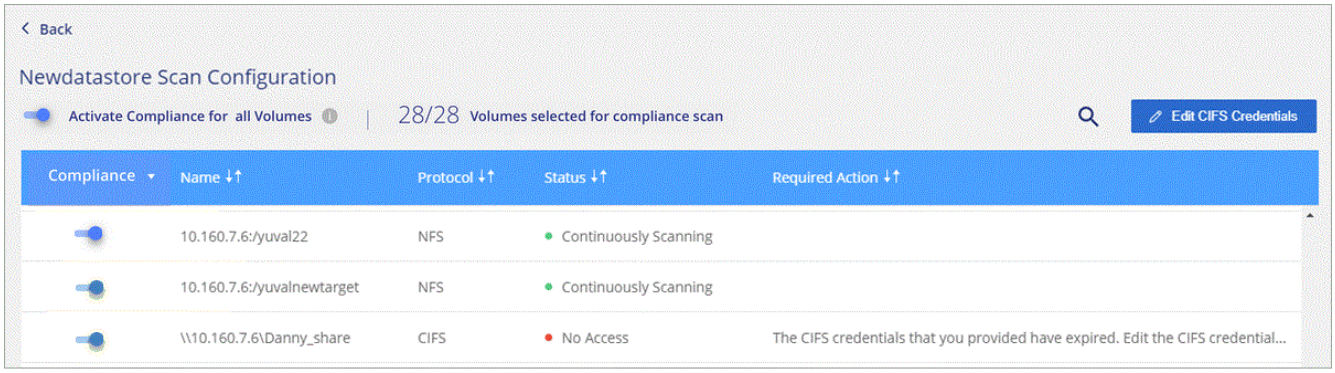
      Después de introducir las credenciales, debe ver un mensaje que indica que todos los volúmenes CIFS se autenticaron correctamente.



5. En la página *Scan Configuration*, haga clic en **View Details** para revisar el estado de cada volumen CIFS y NFS y corregir los errores.

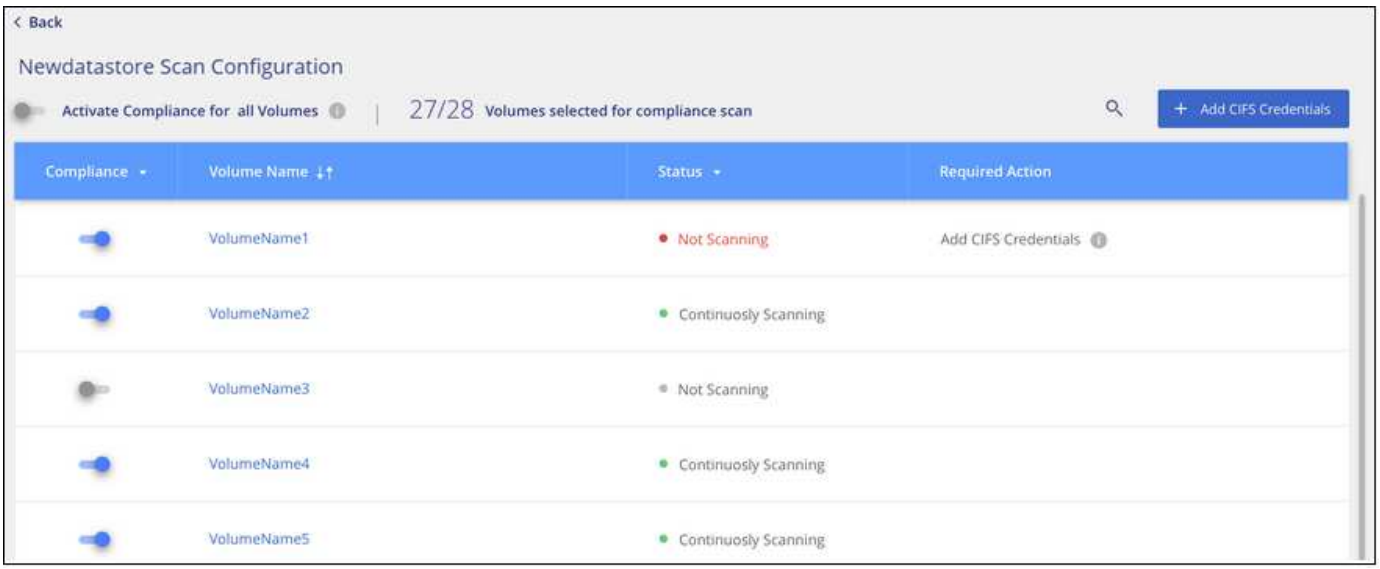
   Por ejemplo, la siguiente imagen muestra tres volúmenes; uno de los cuales no puede analizar Cloud Compliance debido a problemas de conectividad de red entre la instancia de Cloud Compliance y el

volumen.



Habilitar y deshabilitar los análisis de cumplimiento de normativas en los volúmenes

Puede detener o iniciar el análisis de volúmenes en un entorno de trabajo en cualquier momento desde la página Configuración de análisis. Le recomendamos que analice todos los volúmenes.



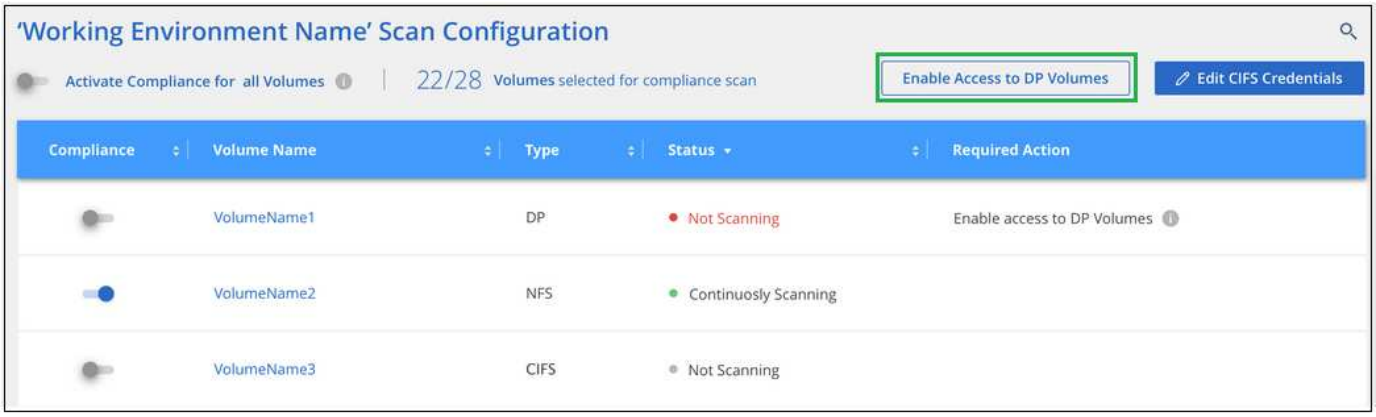
Para:	Haga lo siguiente:
Desactivar el análisis de un volumen	Mueva el control deslizante de volumen hacia la izquierda
Desactive el análisis en todos los volúmenes	Mueva el control deslizante **Activar cumplimiento para todos los volúmenes** a la izquierda
Active la búsqueda de un volumen	Mueva el control deslizante de volumen a la derecha
Active el análisis de todos los volúmenes	Mueva el control deslizante **Activar cumplimiento para todos los volúmenes** a la cierto

Los nuevos volúmenes agregados al entorno de trabajo se analizan automáticamente sólo cuando está activada la opción **Activar cumplimiento para todos los volúmenes**. Cuando este ajuste está desactivado, deberá activar el análisis en cada volumen nuevo que cree en el entorno de trabajo.

Análisis de volúmenes de protección de datos

De manera predeterminada, los volúmenes de protección de datos (DP) no se analizan porque no se exponen externamente y que Cloud Compliance no puede acceder a ellos. Estos volúmenes suelen ser los volúmenes de destino de las operaciones de SnapMirror de un clúster ONTAP en las instalaciones.

Inicialmente, la lista de volúmenes de Cloud Compliance identifica estos volúmenes como *Type* **DP** con el *Status* **no Scanning** y el *Required Action* **Enable Access to DP Volumes**.



Pasos

Si desea analizar estos volúmenes de protección de datos:

1. Haga clic en el botón **Activar acceso a volúmenes DP** situado en la parte superior de la página.
2. Active cada volumen DP que desee analizar o utilice el control **Activar cumplimiento para todos los volúmenes** para activar todos los volúmenes, incluidos todos los volúmenes DP.

Una vez habilitada, Cloud Compliance crea un recurso compartido NFS de cada volumen DP que se activó para la opción de cumplimiento de normativas de manera que se pueda analizar. Las políticas de exportación compartidas solo permiten el acceso desde la instancia de Cloud Compliance.

Solo se muestran en la lista de volúmenes los volúmenes que se crearon inicialmente como volúmenes NFS en el sistema ONTAP de origen. Los volúmenes de origen creados inicialmente como CIFS no aparecen actualmente en Cloud Compliance.

Introducción a Cloud Compliance para Amazon S3

Cloud Compliance puede analizar sus buckets de Amazon S3 para identificar los datos personales y confidenciales que se encuentran en el almacenamiento de objetos S3. Cloud Compliance puede analizar cualquier bloque de la cuenta, independientemente de si se ha creado para una solución de NetApp.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

Configure los requisitos de S3 en su entorno de cloud

Asegúrese de que su entorno cloud pueda cumplir los requisitos de Cloud Compliance, incluida la preparación de un rol IAM y la configuración de conectividad de Cloud Compliance a S3. Vea la lista completa.

Implemente la instancia de Cloud Compliance

"Ponga en marcha Cloud Compliance en Cloud Manager" si aún no hay una instancia implementada.

Active Compliance en su entorno de trabajo de S3

Seleccione el entorno de trabajo de Amazon S3, haga clic en **Activar cumplimiento** y seleccione una función de IAM que incluya los permisos necesarios.

Seleccione los cucharones que desea escanear

Seleccione los cubos que desea analizar y Cloud Compliance empezará a analizarlos.

Revisión de los requisitos previos de S3

Los siguientes requisitos son específicos para el análisis de bloques de S3.

Configurar un rol de IAM para la instancia de Cloud Compliance

Cloud Compliance necesita permisos para conectarse a los bloques de S3 de su cuenta y para analizarlos. Configure un rol de IAM que incluya los permisos que se indican a continuación. Cloud Manager le solicita que seleccione un rol de IAM cuando se habilita Cloud Compliance en el entorno de trabajo de Amazon S3.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "s3:Get*",
              "s3:List*",
              "s3:HeadBucket"
          ],
          "Resource": "*"
      },
      {
          "Effect": "Allow",
          "Action": [
              "iam:GetPolicyVersion",
              "iam:GetPolicy",
              "iam:ListAttachedRolePolicies"
          ],
          "Resource": [
              "arn:aws:iam::*:policy/*",
              "arn:aws:iam::*:role/*"
          ]
      }
  ]
}
```

Proporcione conectividad desde Cloud Compliance a Amazon S3

Cloud Compliance necesita una conexión con Amazon S3. La mejor forma de proporcionar esa conexión es mediante un extremo VPC con el servicio S3. Para ver instrucciones, consulte "Documentación de AWS: Crear un extremo de puerta de enlace".

Al crear el extremo VPC, asegúrese de seleccionar la región, VPC y tabla de rutas que correspondan a la instancia de Cloud Compliance. También debe modificar el grupo de seguridad para añadir una regla de HTTPS de salida que habilite el tráfico hacia el extremo de S3. De lo contrario, Cloud Compliance no se puede conectar con el servicio S3.

Si experimenta algún problema, consulte "Centro de conocimientos de soporte de AWS: ¿por qué no puedo conectarme a un bloque de S3 mediante un extremo de VPC de puerta de enlace?"

Una alternativa es proporcionar la conexión utilizando una puerta de enlace NAT.

No se puede usar un proxy para acceder a S3 a través de Internet.

Implementación de la instancia de Cloud Compliance

"Ponga en marcha Cloud Compliance en Cloud Manager" si aún no hay una instancia implementada.

Debe implementar la instancia en un conector de AWS para que Cloud Manager detecte automáticamente los bloques S3 en esta cuenta de AWS y los muestre en un entorno de trabajo Amazon S3.

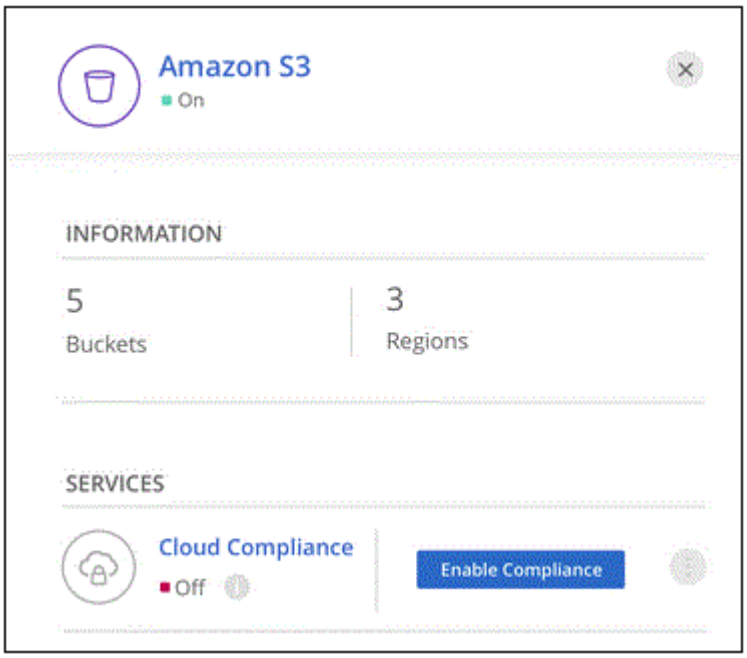
Activar el cumplimiento de normativas en el entorno de trabajo de S3

Habilite Cloud Compliance en Amazon S3 después de comprobar los requisitos previos.

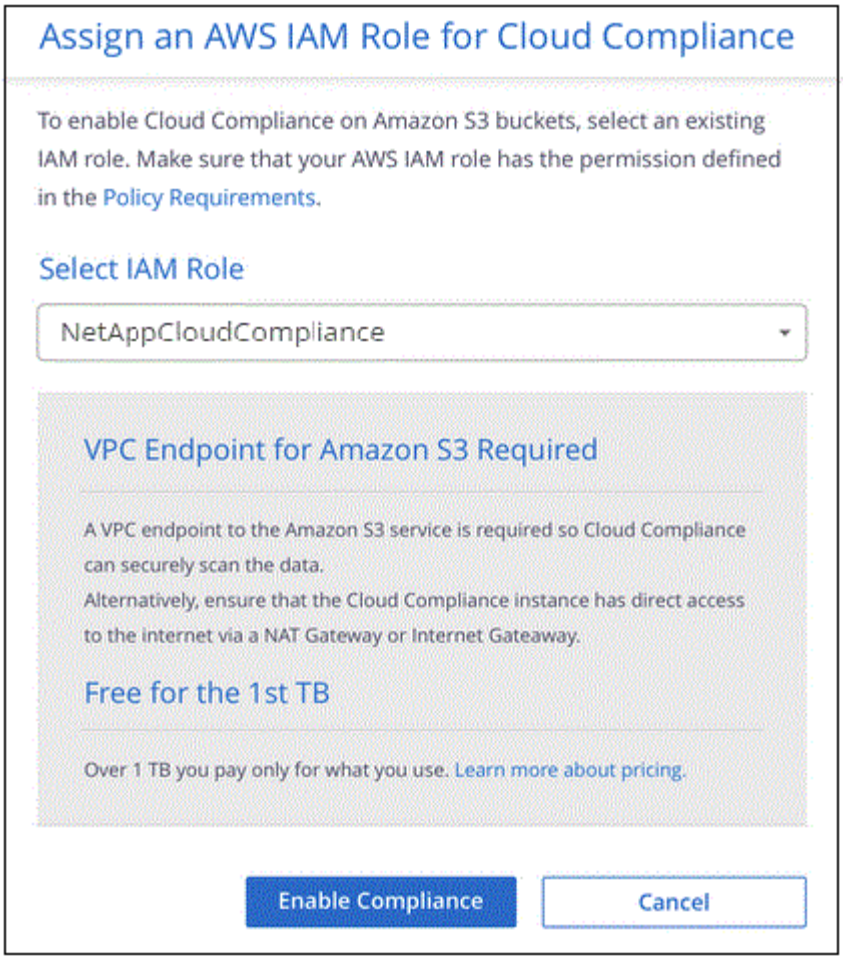
Pasos

1. En la parte superior de Cloud Manager, haga clic en **entornos de trabajo**.
2. Seleccione el entorno de trabajo de Amazon S3.

3. En el panel de la derecha, haga clic en **Activar cumplimiento**.



4. Cuando se le solicite, asigne una función IAM a la instancia de Cloud Compliance que tiene los permisos necesarios.



5. Haga clic en **Activar cumplimiento**.

También puede habilitar análisis de cumplimiento para un entorno de trabajo En la página Scan Configuration (Configuración de exploración), haga clic en Y seleccione **Activar cumplimiento**.

Resultado

Cloud Manager asigna el rol IAM a la instancia.

Habilitar y deshabilitar los análisis de cumplimiento de normativas en bloques S3

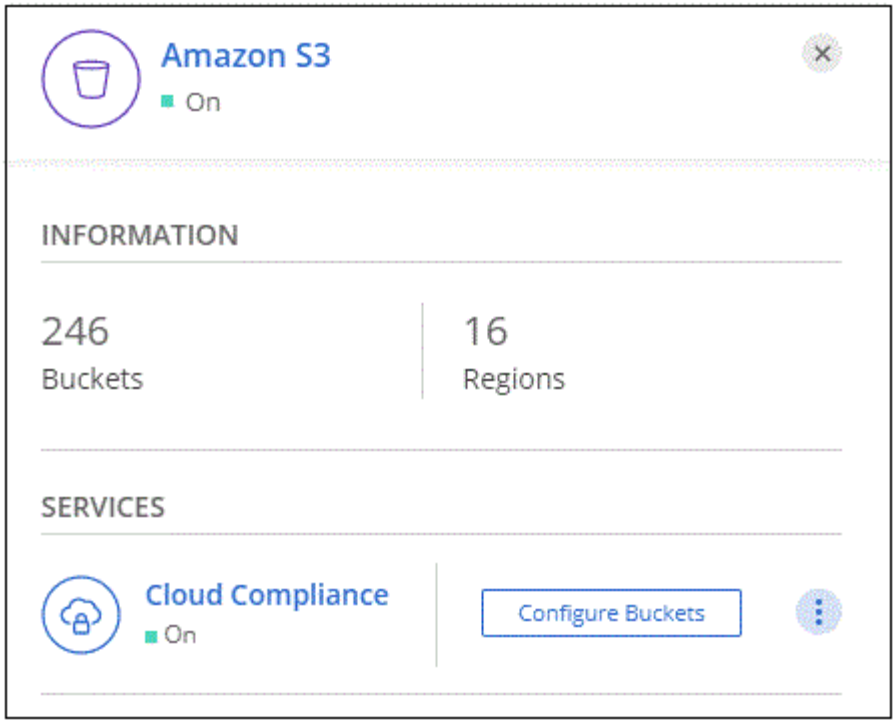
Después de que Cloud Manager habilita Cloud Compliance en Amazon S3, el paso siguiente es configurar los bloques que desea analizar.

Cuando Cloud Manager se ejecuta en la cuenta de AWS que tiene los bloques de S3 que desea analizar, detecta esos bloques y los muestra en un entorno de trabajo de Amazon S3.

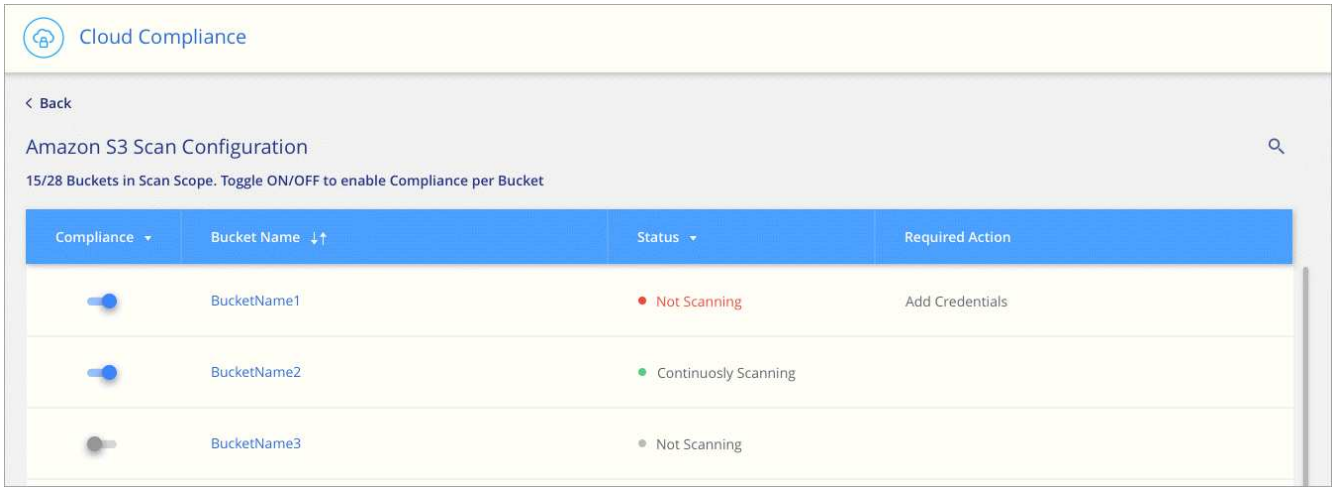
Cloud Compliance también puede Escanee bloques de S3 que se encuentran en diferentes cuentas de AWS.

Pasos

1. Seleccione el entorno de trabajo de Amazon S3.
2. En el panel de la derecha, haga clic en **Configurar cucharones**.



3. Habilite el cumplimiento de normativas en los cucharones que desee analizar.



Resultado

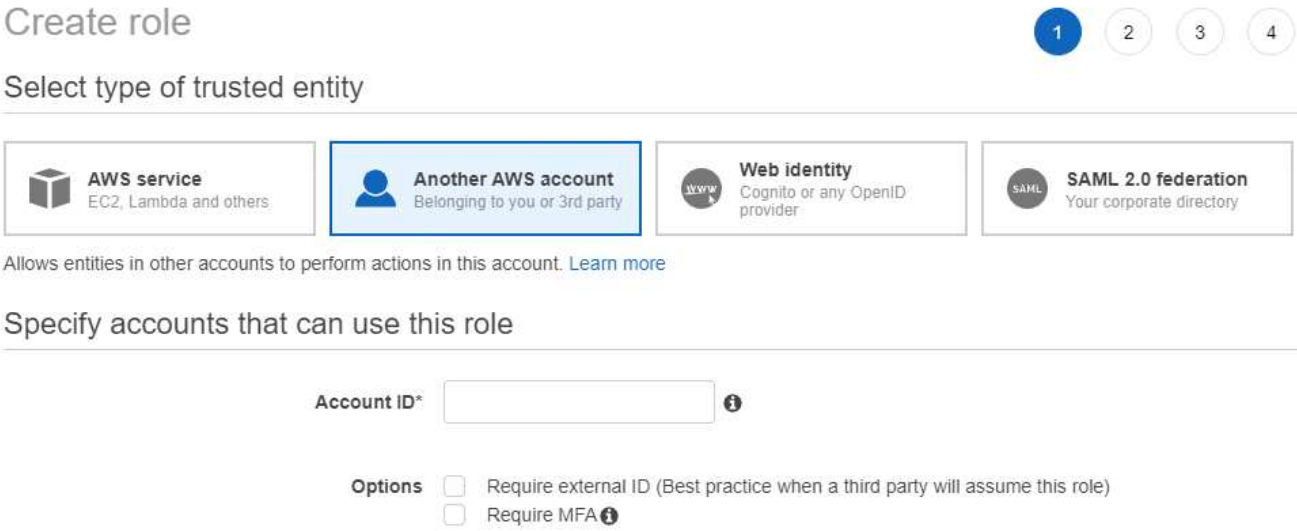
Cloud Compliance comienza a analizar los bloques de S3 que ha habilitado. Si hay algún error, aparecerán en la columna Estado, junto con la acción necesaria para corregir el error.

Escaneando bloques de cuentas de AWS adicionales

Puede analizar bloques de S3 que se encuentran en una cuenta de AWS diferente asignando un rol de esa cuenta para poder acceder a la instancia existente de Cloud Compliance.

Pasos

1. Vaya a la cuenta AWS de destino donde desee explorar bloques S3 y crear un rol IAM seleccionando **otra cuenta de AWS**.



No olvide hacer lo siguiente:

- Introduzca el ID de la cuenta en la que reside la instancia de Cloud Compliance.
- Cambie la duración máxima de la sesión de **CLI/API** de 1 hora a 12 horas y guarde dicho cambio.
- Asociar la política de IAM de cumplimiento de normativas de cloud. Asegúrese de que tiene los permisos necesarios.

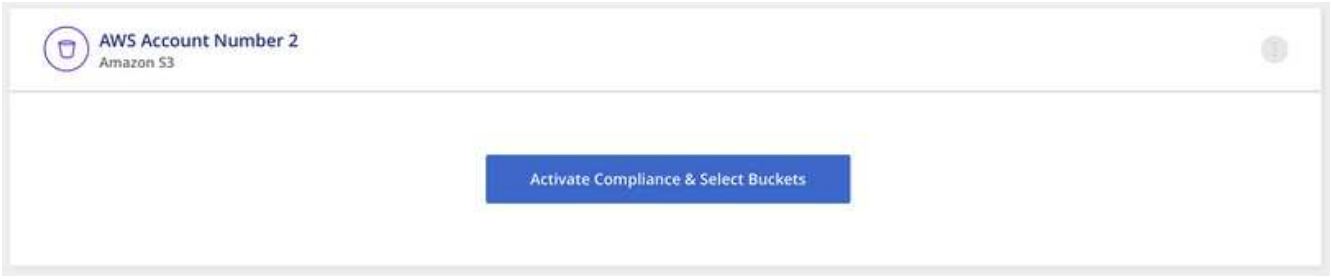
```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "s3:Get*",
              "s3:List*",
              "s3:HeadBucket"
          ],
          "Resource": "*"
      },
  ]
}
```

2. Vaya a la cuenta de AWS de origen donde reside la instancia de Cloud Compliance y seleccione la función IAM que se adjunta a la instancia.
   a. Cambie la duración máxima de la sesión de **CLI/API** de 1 hora a 12 horas y guarde dicho cambio.
   b. Haga clic en **Adjuntar directivas** y, a continuación, en **Crear directiva**.
   c. Cree una directiva que incluya la acción "sts:AssumeRole" y el ARN del rol que creó en la cuenta de destino.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::<ADDITIONAL-ACCOUNT-
ID>:role/<ADDITIONAL_ROLE_NAME>"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedRolePolicies"
            ],
            "Resource": [
                "arn:aws:iam::*:policy/*",
                "arn:aws:iam::*:role/*"
            ]
        }
    ]
}
```

La cuenta del perfil de instancia de Cloud Compliance ahora tiene acceso a la cuenta de AWS adicional.

3. Vaya a la página **Configuración de análisis de Amazon S3** y aparecerá la nueva cuenta de AWS. Tenga en cuenta que Cloud Compliance puede tardar unos minutos en sincronizar el entorno de trabajo de la nueva cuenta y mostrar esta información.



4. Haga clic en **Activar cumplimiento y Seleccionar cucharones** y seleccione los cucharones que desea escanear.

Resultado

Cloud Compliance comienza a analizar los nuevos bloques de S3 que ha habilitado.

Analizando esquemas de base de datos

Realice algunos pasos para empezar a analizar sus esquemas de base de datos con Cloud Compliance.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

Revisar los requisitos previos de la base de datos

Asegúrese de que la base de datos es compatible y de que dispone de la información necesaria para conectarse a la base de datos.

Implemente la instancia de Cloud Compliance

"Ponga en marcha Cloud Compliance en Cloud Manager" si aún no hay una instancia implementada.

Agregue el servidor de la base de datos

Agregue el servidor de base de datos al que desea acceder.

Seleccione los esquemas

Seleccione los esquemas que desea analizar.

Revisión de requisitos previos

Revise los siguientes requisitos previos para asegurarse de tener una configuración compatible antes de habilitar Cloud Compliance.

Bases de datos compatibles

Cloud Compliance puede analizar esquemas de las siguientes bases de datos:

- MongoDB
- Oracle
- PostgreSQL
- SAP HANA
- Servidor SQL (MSSQL)

La característica de recopilación de estadísticas **debe estar activada** en la base de datos.

Requisitos de base de datos

Es posible analizar cualquier base de datos con conectividad a la instancia de Cloud Compliance, independientemente de dónde se encuentre. Sólo necesita la siguiente información para conectarse a la base de datos:

- Dirección IP o nombre de host
- Puerto
- Nombre del servicio (sólo para acceder a bases de datos Oracle)
- Credenciales que permiten el acceso de lectura a los esquemas

  Al elegir un nombre de usuario y contraseña, es importante elegir uno que tenga permisos de lectura completos para todos los esquemas y tablas que desee analizar. Le recomendamos que cree un usuario dedicado para el sistema Cloud Compliance con todos los permisos necesarios.

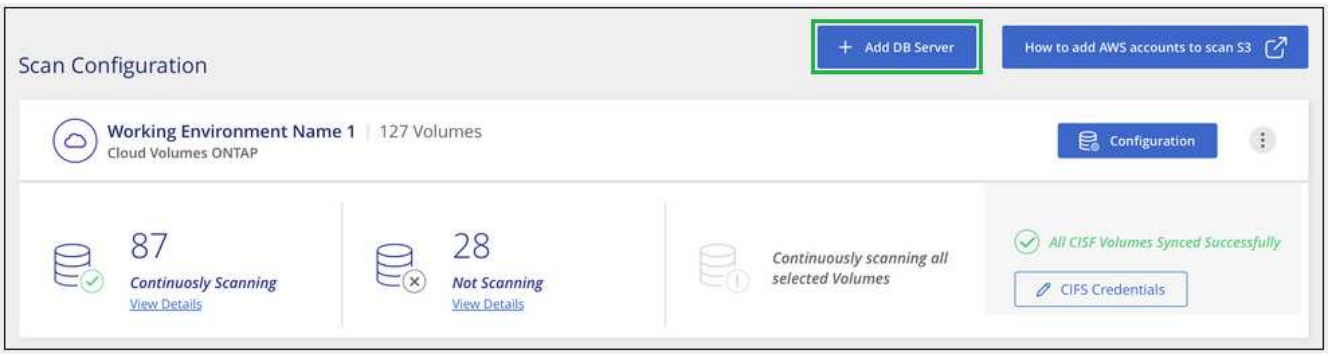
Nota: para MongoDB, se requiere una función de administrador de sólo lectura.

Agregando el servidor de la base de datos

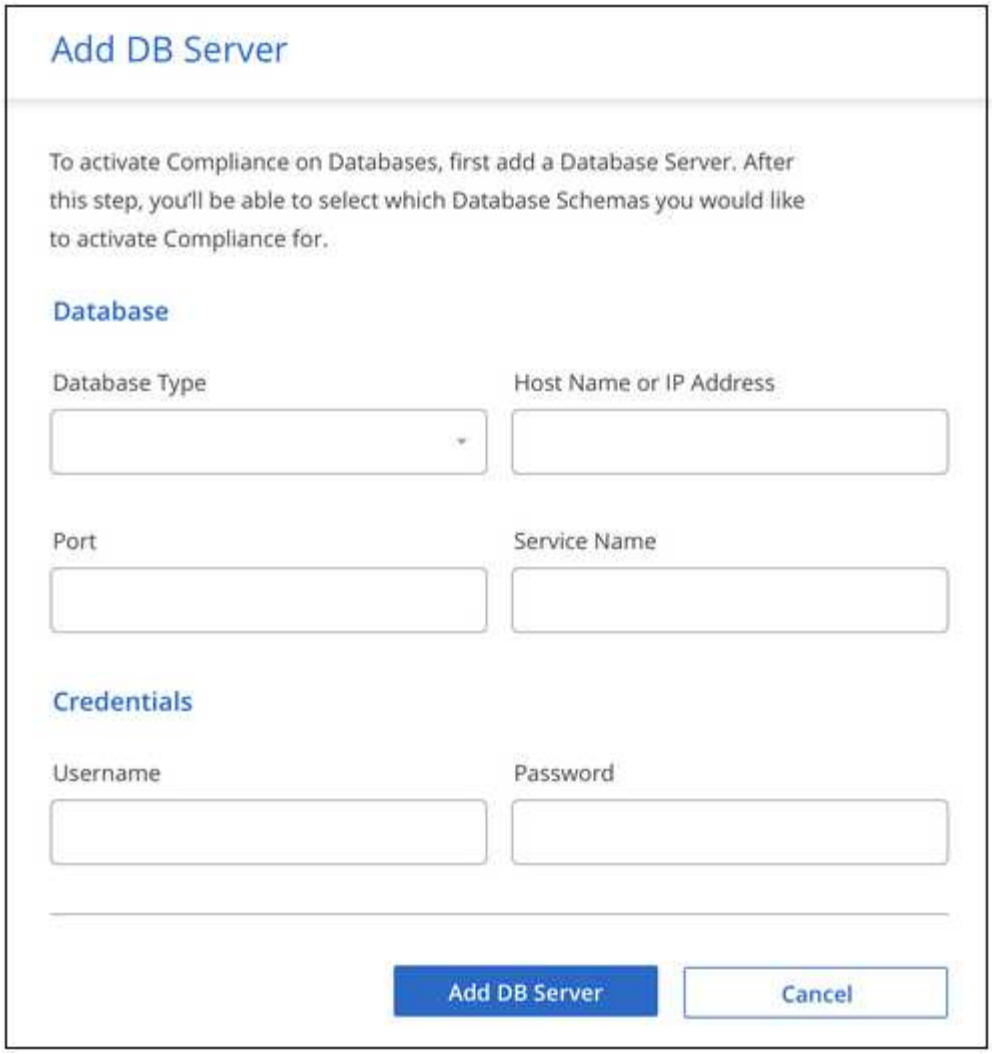
Debe tener "Ya se puso en marcha una instancia de Cloud Compliance en Cloud Manager".

Agregue el servidor de base de datos donde residen los esquemas.

1. En la página *Scan Configuration*, haga clic en el botón **Add DB Server**.



2. Introduzca la información necesaria para identificar el servidor de bases de datos.
   a. Seleccione el tipo de base de datos.
   b. Introduzca el puerto y el nombre de host o la dirección IP para conectarse a la base de datos.
   c. Para las bases de datos de Oracle, introduzca el nombre del servicio.
   d. Introduzca las credenciales para que Cloud Compliance pueda acceder al servidor.
   e. Haga clic en **Agregar servidor de base de datos**.



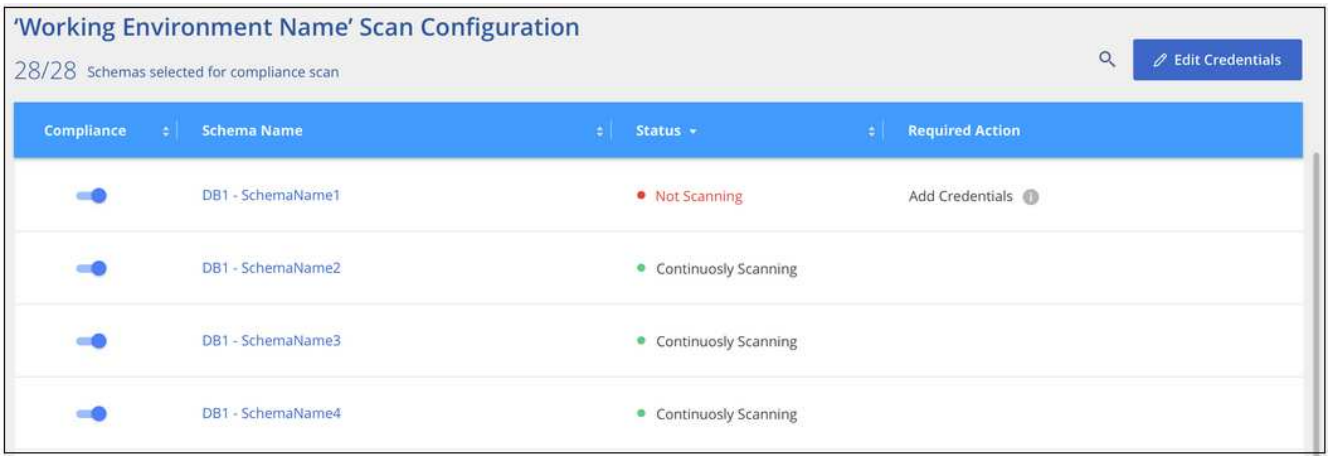
La base de datos se agrega a la lista de directorios de trabajo.

Habilitar y deshabilitar los análisis de cumplimiento de normativas en esquemas de base de datos

Puede detener o iniciar esquemas de análisis en cualquier momento.

1. En la página *Scan Configuration*, haga clic en el botón **Configuración** de la base de datos que desee configurar.

2. Seleccione los esquemas que desea analizar moviendo el control deslizante hacia la derecha.



Resultado

Cloud Compliance comienza a analizar los esquemas de base de datos que ha habilitado. Si hay algún error, aparecerán en la columna Estado, junto con la acción necesaria para corregir el error.

Quitar una base de datos de Cloud Manager

Si ya no desea analizar una determinada base de datos, puede eliminarla de la interfaz de Cloud Manager y detener todos los análisis.

En la página *Scan Configuration*, haga clic en En la fila de la base de datos y, a continuación, haga clic en **Quitar servidor de base de datos**.

Análisis de datos de ONTAP en las instalaciones con Cloud Compliance mediante SnapMirror

Puede analizar sus datos de ONTAP en las instalaciones con Cloud Compliance replicando los datos de NFS o CIFS en las instalaciones en un entorno de trabajo de Cloud Volumes ONTAP para después habilitar el cumplimiento de normativas. El análisis de los datos directamente desde un entorno de trabajo ONTAP en las instalaciones no es compatible.

Debe tener "Ya se puso en marcha una instancia de Cloud Compliance en Cloud Manager".

Pasos

1. En Cloud Manager, cree una relación de SnapMirror entre el clúster de ONTAP en las instalaciones y Cloud Volumes ONTAP.
   a. "Descubra el clúster en las instalaciones en Cloud Manager".

b. "Cree una replicación de SnapMirror entre el clúster de ONTAP en las instalaciones y. Cloud Volumes ONTAP de Cloud Manager".

2. Para los volúmenes DP creados a partir de volúmenes de origen SMB, desde la interfaz de línea de comandos de ONTAP, configure los volúmenes de destino SMB para el acceso a los datos. (Esto no es necesario en los volúmenes NFS porque el acceso a los datos se habilita de forma automática mediante Cloud Compliance).
   a. "Cree un recurso compartido de SMB en el volumen de destino".
   b. "Aplique las ACL adecuadas para el recurso compartido de SMB en el volumen de destino".
3. En Cloud Manager, active Cloud Compliance en el entorno de trabajo de Cloud Volumes ONTAP que contiene los datos de SnapMirror:
   a. Haga clic en **entornos de trabajo**.
   b. Seleccione el entorno de trabajo que contiene los datos de SnapMirror y haga clic en **Activar cumplimiento**.

      "Haga clic aquí si necesita ayuda para habilitar Cloud Compliance En un sistema Cloud Volumes ONTAP".

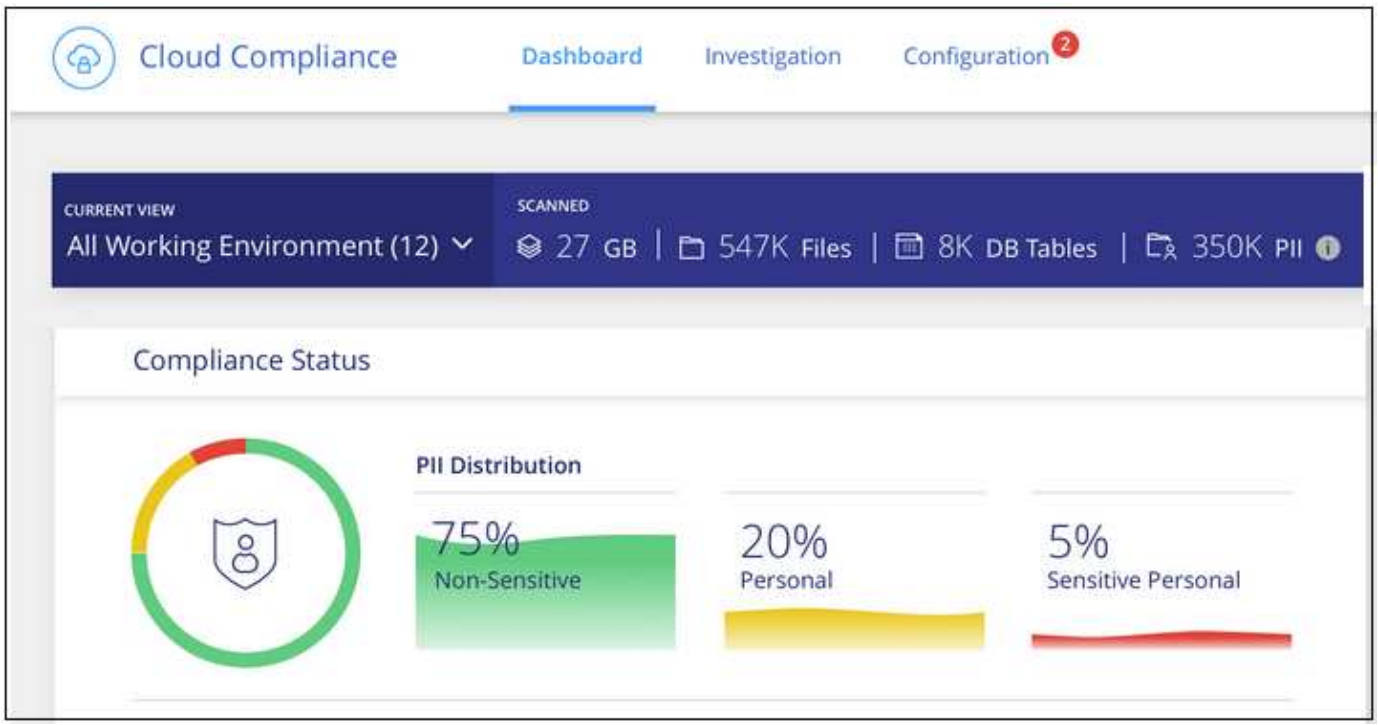
   c. Haga clic en el botón **Activar acceso a volúmenes DP** situado en la parte superior de la página *Scan Configuration*.
   d. Active cada volumen DP que desee analizar o utilice el control **Activar cumplimiento para todos los volúmenes** para activar todos los volúmenes, incluidos todos los volúmenes DP.

Consulte "Análisis de volúmenes de protección de datos" Para obtener más información sobre el análisis de volúmenes DP.

Obtener visibilidad y control de los datos privados

Controle sus datos privados al ver los detalles sobre los datos personales y los datos personales confidenciales de su empresa. También puede ver las categorías y los tipos de archivos que cumple con las normativas del cloud de los datos.

De forma predeterminada, la consola de Cloud Compliance muestra los datos de cumplimiento de normativas de todas las bases de datos y entornos de trabajo.



Si sólo desea ver datos para algunos de los entornos de trabajo, seleccione esos entornos de trabajo.

Datos personales

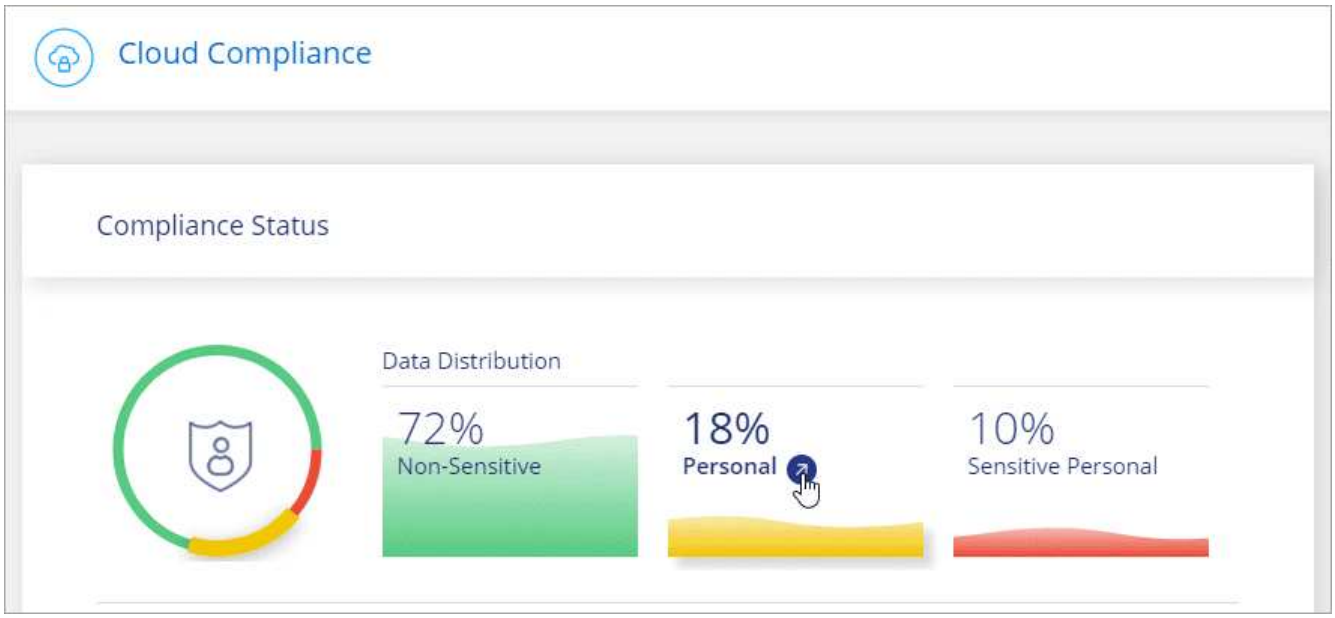
Cloud Compliance identifica automáticamente palabras, cadenas y patrones específicos (Regex) dentro de los datos. Por ejemplo, Información de identificación personal (PII), números de tarjeta de crédito, números de seguridad social, números de cuenta bancaria y mucho más. Consulte la lista completa.

Para algunos tipos de datos personales, Cloud Compliance utiliza *proximity validation* para validar sus hallazgos. La validación se produce buscando una o más palabras clave predefinidas cerca de los datos personales encontrados. Por ejemplo, Cloud Compliance identifica una normativa estadounidense Número de seguridad social (SSN) como un SSN si ve una palabra de proximidad junto a ella (por ejemplo, *SSN* o *seguridad social*). La siguiente lista Muestra cuándo Cloud Compliance utiliza la validación de proximidad.

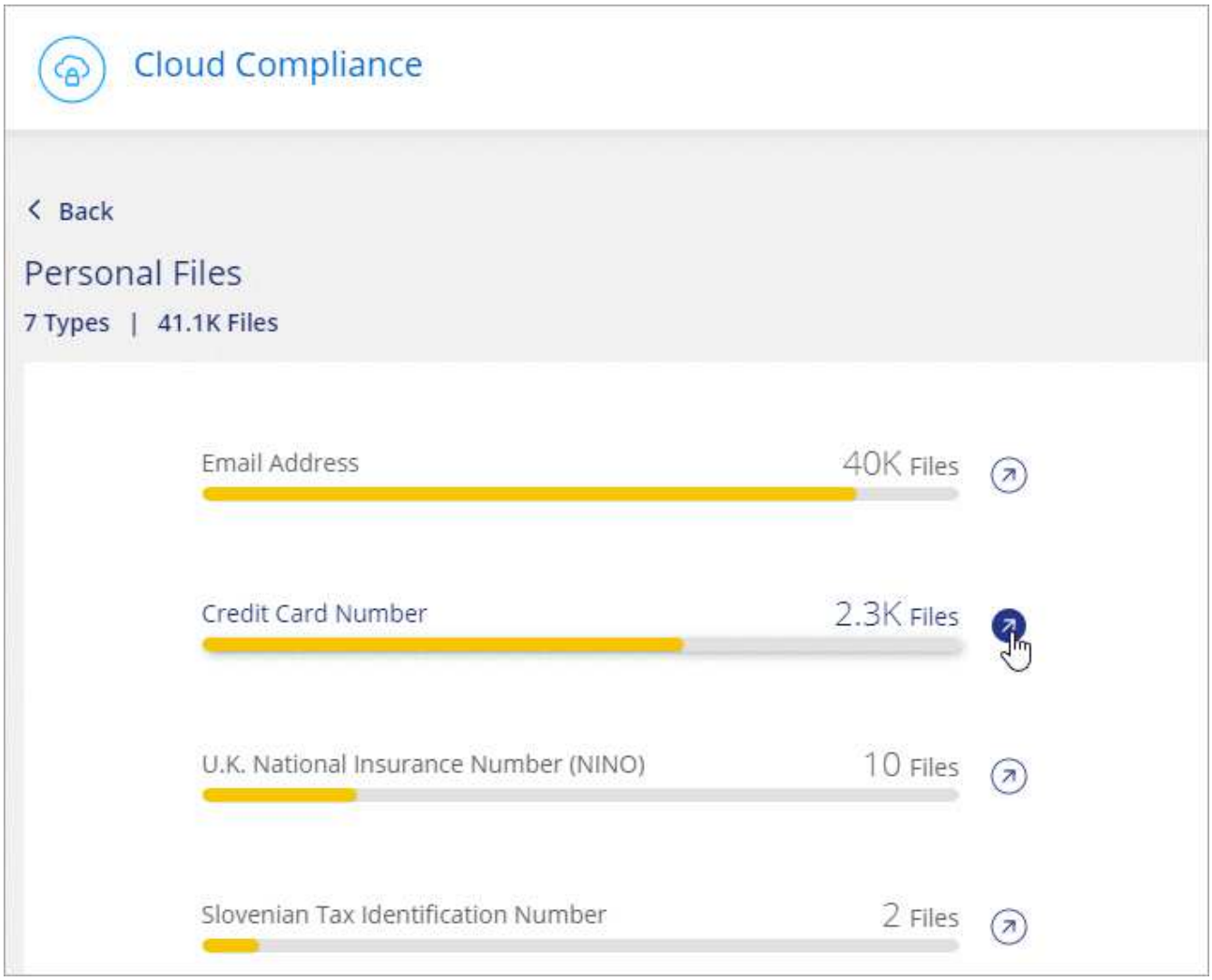
Visualización de archivos que contienen datos personales

Pasos

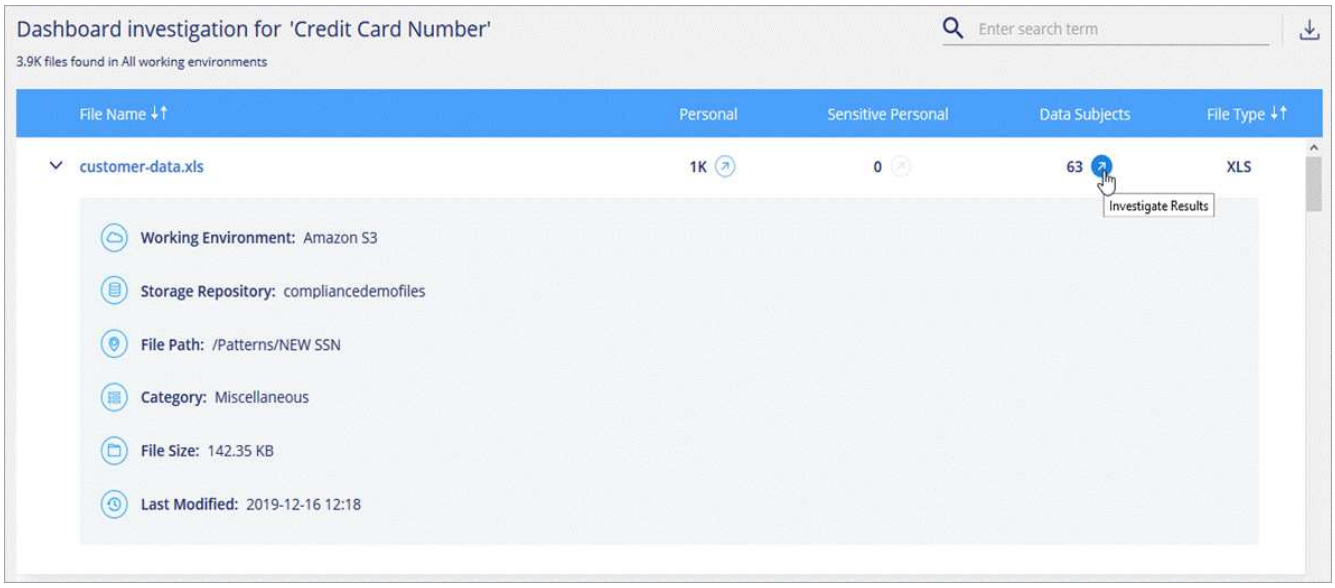
1. En la parte superior de Cloud Manager, haga clic en **cumplimiento de la nube** y haga clic en la ficha **Panel**.
2. Para investigar los detalles de todos los datos personales, haga clic en el icono situado junto al porcentaje de datos personales.



3. Para investigar los detalles de un tipo específico de datos personales, haga clic en **Ver todos** y, a continuación, haga clic en el icono **investigar resultados** para obtener un tipo específico de datos personales.

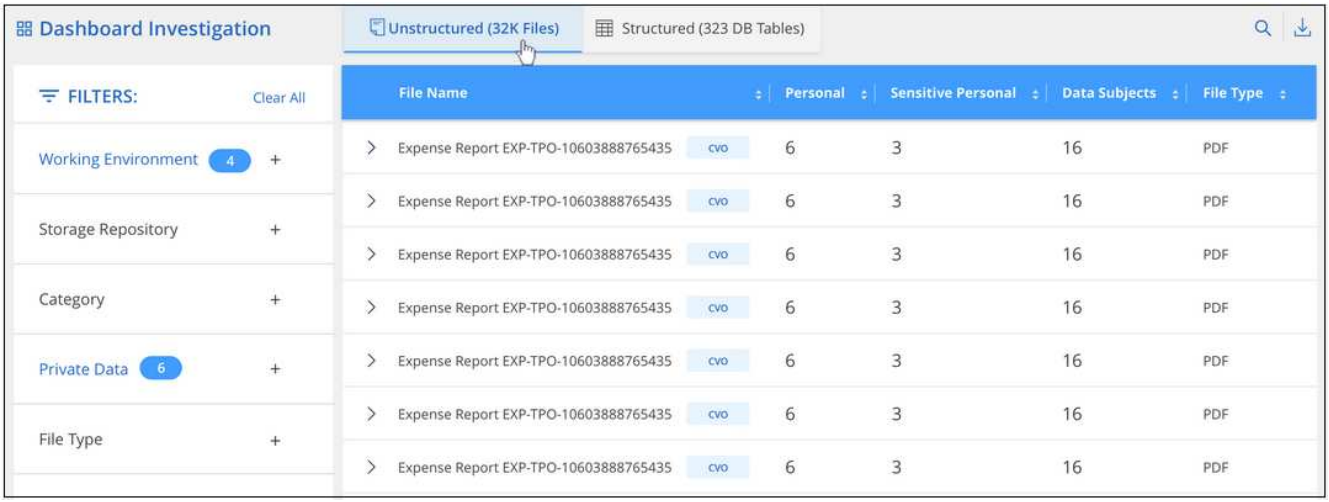


4. Investigue los datos buscando, ordenando, ampliando los detalles de un archivo específico, haciendo clic en **investigar resultados** para ver la información enmascarada o descargando la lista de archivos.



5. También puede filtrar el contenido de la página Investigación para que muestre solo los resultados que desea ver. Las pestañas de nivel superior le permiten ver datos de archivos (datos no estructurados) o de bases de datos (datos estructurados).

   A continuación, dispone de filtros para entorno de trabajo, repositorio de almacenamiento, categoría, datos privados, tipo de archivo, Fecha de la última modificación, y si los permisos del objeto S3 están abiertos al acceso público.



Tipos de datos personales

Los datos personales encontrados en los archivos pueden ser datos personales generales o identificadores nacionales. La tercera columna identifica si Cloud Compliance utiliza validación de proximidad validar los resultados del identificador.

Tipo	Identificador	¿validación de proximidad?
Generales	Dirección de correo electrónico	No
	Número de tarjeta de crédito	No
	Número de iban (número de cuenta bancaria internacional)	No

Tipo	Identificador	¿validación de proximidad?
Identificadores nacionales	ID belga (Numero Nacional)	Sí
	ID brasileño (CPF)	Sí
	ID búlgaro (UCN)	Sí
	Licencia de conducir de California	Sí
	Croata ID (OIB)	Sí
	Número de identificación fiscal de Chipre (TIC)	Sí
	ID checo/eslovaco	Sí
	ID danés (CPR)	Sí
	Dutch ID (BSN)	Sí
	Identificación Estonia	Sí
	Finlandés ID (HETU)	Sí
	Número de identificación fiscal francés (SPI)	Sí
	Número de identificación fiscal alemán (Steuerliche Identifikationsnummer)	Sí
	ID griego	Sí
	Número de identificación fiscal húngaro	Sí
	Irish ID (PPS)	Sí
	Documento de identidad israelí	Sí
	Número de identificación fiscal italiana	Sí
	ID letón	Sí
	ID lituano	Sí
	ID de Luxemburgo	Sí
	Identificación maltesa	Sí
	Identificación polaca (PESEL)	Sí
	Número de identificación fiscal (NIF) en portugués	Sí
	Rumano ID (CNP)	Sí
	ID esloveno (EMSO)	Sí
	ID sudafricano	Sí
	Número de identificación fiscal en español	Sí
	ID sueco	Sí
	REINO UNIDO ID (NINO)	Sí
	Número de Seguro Social de Estados Unidos (SSN)	Sí

Datos personales confidenciales

Cloud Compliance identifica automáticamente los tipos especiales de información personal confidencial, tal como se definen en normativas de privacidad como "Artículos 9 y 10 del RGPD". Por ejemplo, información sobre la salud, origen étnico o orientación sexual de una persona. Consulte la lista completa.

Cloud Compliance utiliza la inteligencia artificial (IA), el procesamiento de lenguaje natural (NLP), el aprendizaje automático (ML) y la computación cognitiva (CC) para comprender el significado del contenido que analiza con el fin de extraer entidades y categorizar según sea necesario.

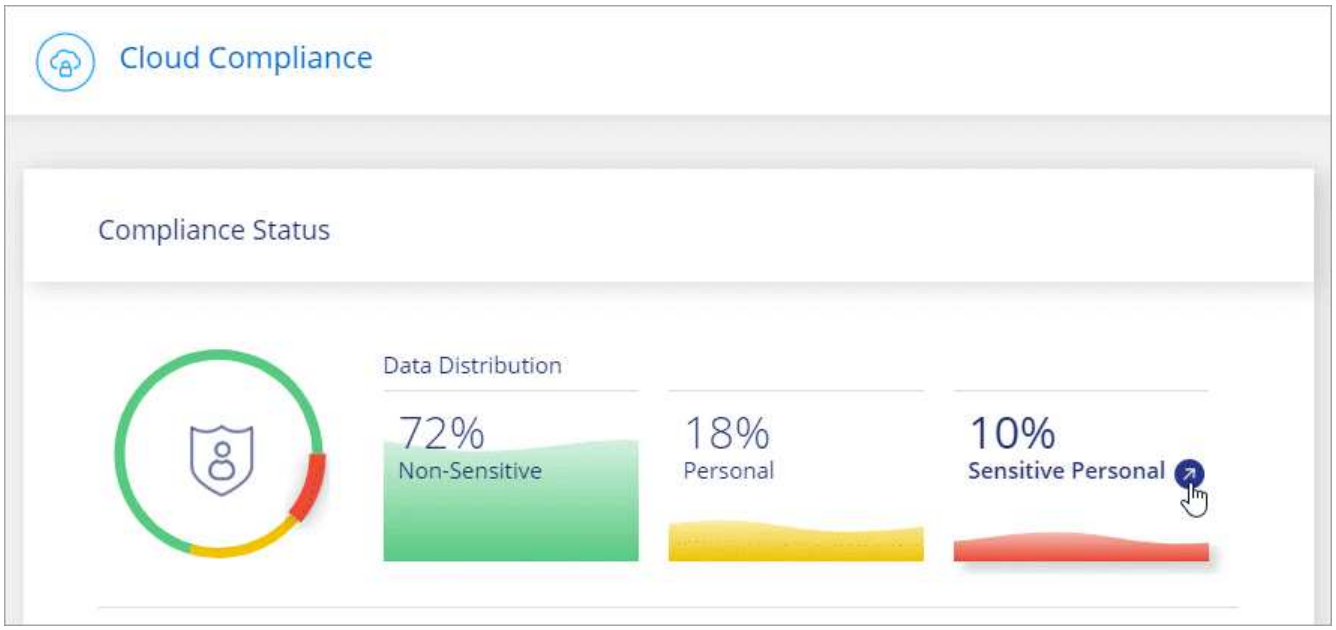
Por ejemplo, una categoría de datos confidenciales sobre el GDPR es su origen étnico. Debido a sus habilidades para NLP, Cloud Compliance puede distinguir la diferencia entre una frase que dice "George es mexicano" (que indica datos confidenciales como se especifica en el artículo 9 del RGPD), frente a "George está comiendo comida mexicana".

Sólo se admite inglés cuando se escanea datos personales confidenciales. Más adelante se añadirá compatibilidad con más idiomas.

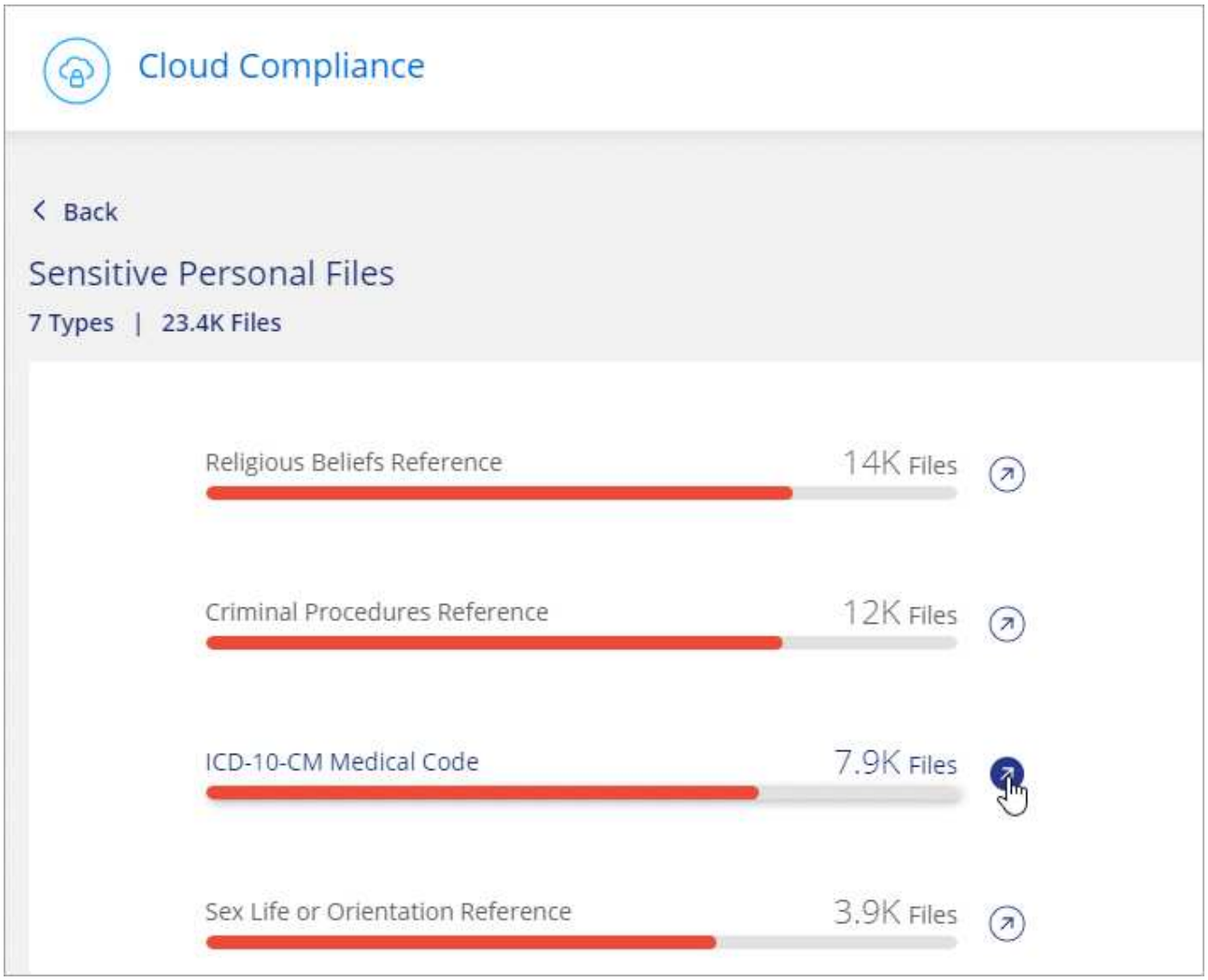
Visualización de archivos que contienen datos personales confidenciales

Pasos

1. En la parte superior de Cloud Manager, haga clic en **Cloud Compliance**.
2. Para investigar los detalles de todos los datos personales confidenciales, haga clic en el icono situado junto al porcentaje de datos personales confidenciales.



3. Para investigar los detalles de un tipo específico de datos personales confidenciales, haga clic en **Ver todo** y, a continuación, haga clic en el icono **investigar resultados** para obtener un tipo específico de datos personales confidenciales.



4. Investigue los datos buscando, ordenando, ampliando los detalles de un archivo específico, haciendo clic en **investigar resultados** para ver la información enmascarada o descargando la lista de archivos.

Tipos de datos personales confidenciales

Los datos personales confidenciales que Cloud Compliance puede encontrar en los archivos incluyen los siguientes:

Procedimientos penales referencia
Datos relativos a las condenas y delitos penales de una persona natural.

Referencia étnica
Datos relativos al origen racial o étnico de una persona natural.

Referencia de Salud
Datos relativos a la salud de una persona física.

Códigos médicos ICD-9-cm
Códigos utilizados en la industria médica y de la salud.

Códigos médicos ICD-10-cm

Códigos utilizados en la industria médica y de la salud.

Creencias filosóficas referencia

Datos relativos a las creencias filosóficas de una persona natural.

Referencia de creencias religiosas

Datos relativos a las creencias religiosas de una persona natural.

Referencia de vida sexual o orientación

Datos relativos a la vida sexual o la orientación sexual de una persona natural.

Categorías

Cloud Compliance toma los datos que ha analizado y los divide en diferentes tipos de categorías. Las categorías son temas basados en el análisis de IA del contenido y los metadatos de cada archivo. Vea la lista de categorías.

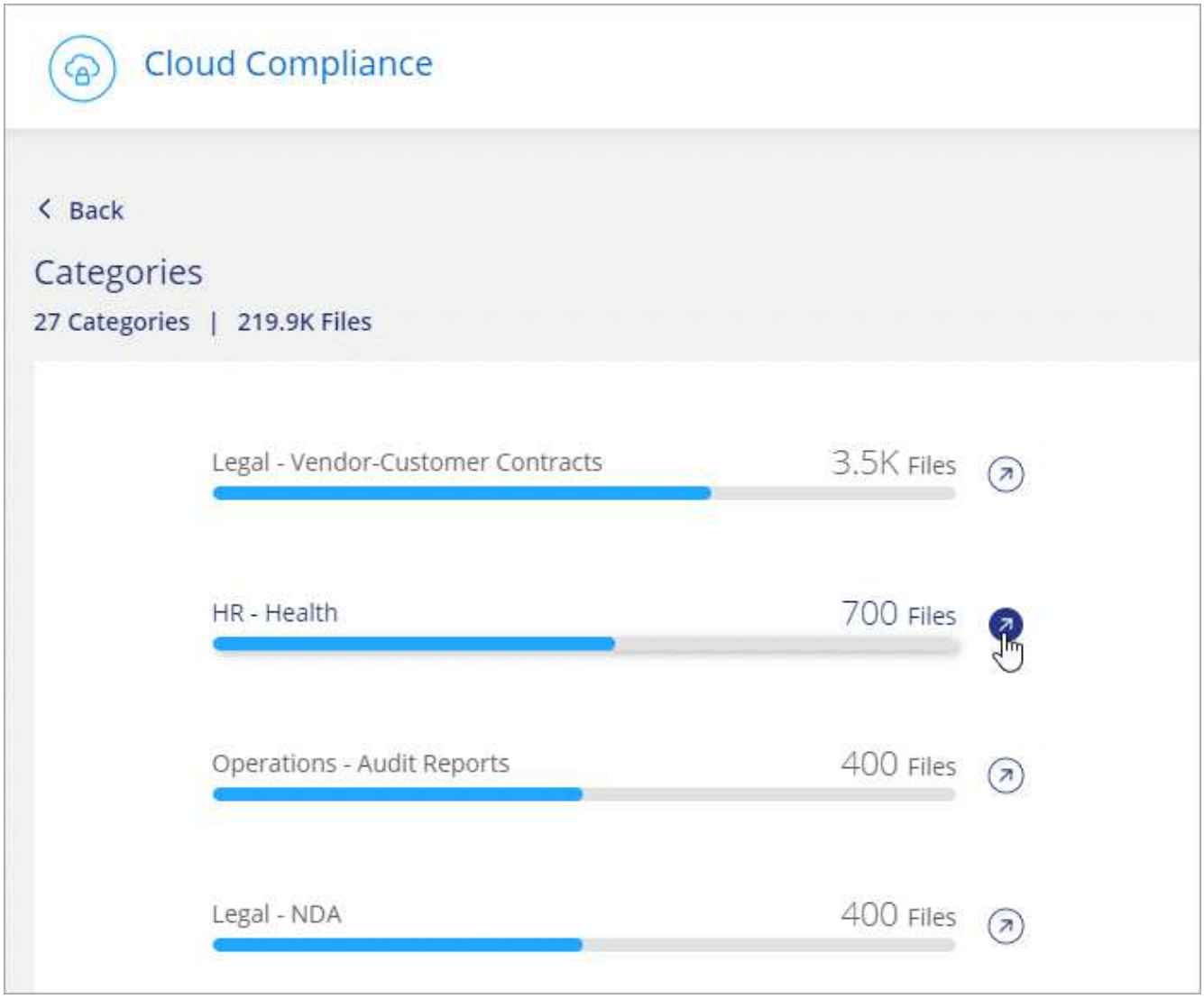
Las categorías pueden ayudarle a entender lo que está pasando con sus datos mostrándole los tipos de información que tiene. Por ejemplo, una categoría como currículos o contratos de empleados puede incluir datos confidenciales. Cuando investiga los resultados, puede que encuentre que los contratos de empleados están almacenados en una ubicación insegura. Entonces puede corregir ese problema.

Solo se admite inglés para categorías. Más adelante se añadirá compatibilidad con más idiomas.

Ver archivos por categorías

Pasos

1. En la parte superior de Cloud Manager, haga clic en **Cloud Compliance**.
2. Haga clic en el icono **investigar resultados** de una de las 4 categorías principales directamente desde la pantalla principal, o haga clic en **Ver todos** y luego haga clic en el icono de cualquiera de las categorías.



3. Investigue los datos buscando, ordenando, ampliando los detalles de un archivo específico, haciendo clic en **investigar resultados** para ver la información enmascarada o descargando la lista de archivos.

Tipos de categorías

Cloud Compliance categoriza sus datos de la siguiente manera:

Finanzas

- Hojas de balance
- Órdenes de compra
- Facturas
- Informes trimestrales

RR. HH

- Comprobaciones de fondo
- Planes de compensación
- Contratos de empleados
- Revisiones de empleados

- Salud
- Se reanudará

Legal
- NDAS
- Contratos con el proveedor y el cliente

Marketing
- Campañas
- Conferencias

Operaciones
- Informes de auditoría

Ventas
- Pedidos de ventas

Servicios
- RFI
- RFP
- CERDA
- Entrenamiento

Soporte técnico
- Quejas y boletos

Categorías de metadatos
- Datos de aplicaciones
- Archivos de archivo
- Audio
- Datos de aplicaciones de negocio
- Archivos CAD
- Codificación
- Archivos de base de datos e índice
- Archivos de diseño
- Datos de aplicación de correo electrónico
- Ejecutables
- Datos de aplicaciones financieras
- Datos de aplicación de salud
- Imágenes
- Registros
- Documentos varios
- Presentaciones diversas

- Hojas de cálculo varias
- Vídeos

Tipos de archivo

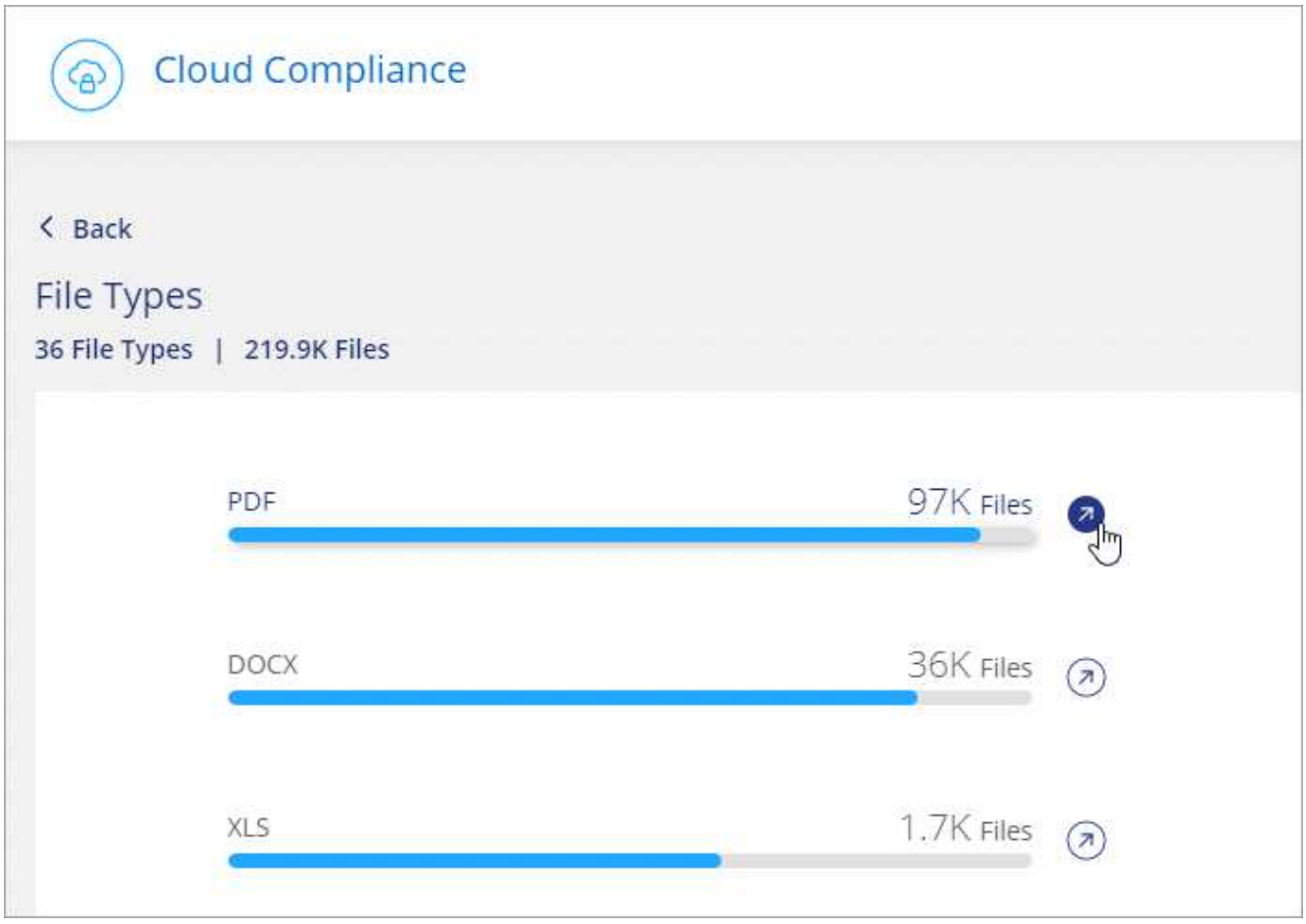
Cloud Compliance toma los datos que ha analizado y los divide por tipo de archivo. La revisión de los tipos de archivo puede ayudarle a controlar los datos confidenciales porque puede encontrar que determinados tipos de archivo no se almacenan correctamente. Consulte la lista de tipos de archivo.

Por ejemplo, puede almacenar archivos CAD que incluyan información muy confidencial sobre su organización. Si no está seguro, puede tomar el control de los datos confidenciales restringiendo permisos o moviendo los archivos a otra ubicación.

Visualización de tipos de archivo

Pasos

1. En la parte superior de Cloud Manager, haga clic en **Cloud Compliance**.
2. Haga clic en el icono **investigar resultados** de uno de los 4 tipos de archivo principales directamente desde la pantalla principal, o haga clic en **Ver todos** y, a continuación, haga clic en el icono de cualquiera de los tipos de archivo.



3. Investigue los datos buscando, ordenando, ampliando los detalles de un archivo específico, haciendo clic en **investigar resultados** para ver la información enmascarada o descargando la lista de archivos.

Tipos de archivos

Cloud Compliance analiza todos los archivos para obtener información sobre categorías y metadatos y muestra todos los tipos de archivos en la sección tipos de archivos de la consola.

Pero cuando Cloud Compliance detecta la información personal identificable (PII) o cuando realiza una búsqueda DSAR, sólo se admiten los siguientes formatos de archivo: .PDF, .DOCX, .DOC, .PPTX, .XLS, .CSV, .TXT, .RTF y .JSON.

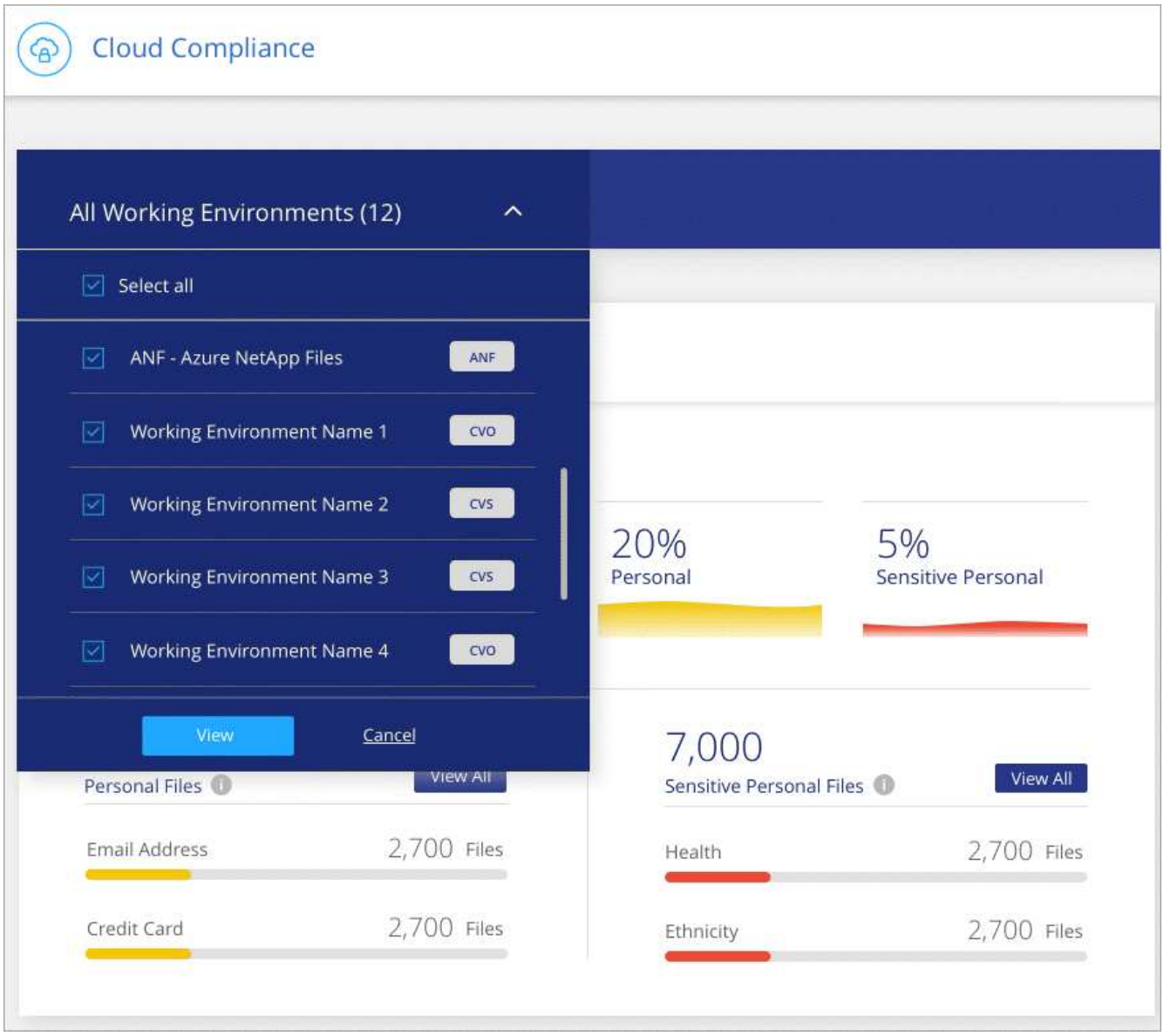
Visualización de datos de entornos de trabajo específicos

Puede filtrar el contenido del panel de Cloud Compliance para ver los datos de cumplimiento de normativas de todos los entornos de trabajo y bases de datos, o solo en entornos de trabajo específicos.

Al filtrar la consola, Cloud Compliance determina los datos de cumplimiento de normativas e informa solo a los entornos de trabajo que haya seleccionado.

Pasos

1. Haga clic en el menú desplegable filtro, seleccione los entornos de trabajo para los que desea ver datos y haga clic en **Ver**.



Precisión de la información encontrada

NetApp no puede garantizar una precisión del 100 % de los datos personales y datos personales confidenciales que identifica Cloud Compliance. Siempre debe validar la información revisando los datos.

La siguiente tabla, basada en nuestras pruebas, muestra la precisión de la información que encuentra Cloud Compliance. La dividiremos por *precision* y *RECALL*:

Precisión

La probabilidad de que lo que encontró el cumplimiento de cloud se haya identificado correctamente. Por ejemplo, una tasa de precisión del 90% para los datos personales significa que 9 de cada 10 archivos identificados como que contienen información personal contienen realmente información personal. 1 de cada 10 archivos sería un falso positivo.

Recuperar

La probabilidad de que el cumplimiento de normativas en el cloud encuentre lo que debería. Por ejemplo, una tasa de recuperación del 70 % para los datos personales significa que Cloud Compliance puede identificar 7 de cada 10 archivos que contienen información personal en su organización. Cloud

Compliance faltaría el 30 % de los datos y no aparecerá en el panel.

Cloud Compliance se encuentra en un lanzamiento de disponibilidad controlado y constantemente mejoramos la precisión de los resultados. Dichas mejoras estarán disponibles automáticamente en los próximos lanzamientos de Cloud Compliance.

Tipo	Precisión	Recuperar
Datos personales - General	90%-95%	60%-80%
Datos personales: Identificadores de país	30%-60%	40%-60%
Datos personales confidenciales	80%-95%	20%-30%
Categorías	90%-97%	60%-80%

Qué se incluye en cada informe de lista de archivos (archivo CSV)

Desde cada página de investigación puede descargar listas de archivos (en formato CSV) que incluyen detalles sobre los archivos identificados. Si hay más de 10,000 resultados, sólo los 10,000 primeros aparecen en la lista.

Cada lista de archivos incluye la siguiente información:

- Nombre de archivo
- Tipo de ubicación
- Entorno de trabajo
- Repositorio de almacenamiento
- Protocolo
- Ruta del archivo
- Tipo de archivo
- Categoría
- Información personal
- Información personal confidencial
- Fecha de detección de eliminación

  Una fecha de detección de eliminación identifica la fecha en la que se eliminó o movió el archivo. Esto le permite identificar cuándo se han movido los archivos confidenciales. Los archivos eliminados no forman parte del recuento de números de archivo que aparece en el panel o en la página Investigación. Los archivos solo aparecen en los informes CSV.

Ver informes de cumplimiento

Cloud Compliance proporciona informes que puede usar para comprender mejor el estado del programa de privacidad de datos de su organización.

De forma predeterminada, la consola de Cloud Compliance muestra los datos de cumplimiento de normativas de todas las bases de datos y entornos de trabajo. Si desea ver informes que contengan datos sólo para algunos de los entornos de trabajo, seleccione esos entornos de trabajo.

NetApp no puede garantizar una precisión del 100 % de los datos personales y datos personales confidenciales que identifica Cloud Compliance. Siempre debe validar la información revisando los datos.

Informe de evaluación del riesgo de privacidad

El informe de evaluación de riesgos de privacidad proporciona una descripción general del estado de riesgo de privacidad de su organización, tal y como lo exigen las normativas de privacidad como RGPD y CCPA. El informe incluye la siguiente información:

Estado de cumplimiento

A. puntuación de gravedad y la distribución de los datos, ya sean personales, confidenciales o no confidenciales.

Descripción general de la evaluación

Desglose de los tipos de datos personales encontrados, así como de las categorías de datos.

Datos sujetos en esta evaluación

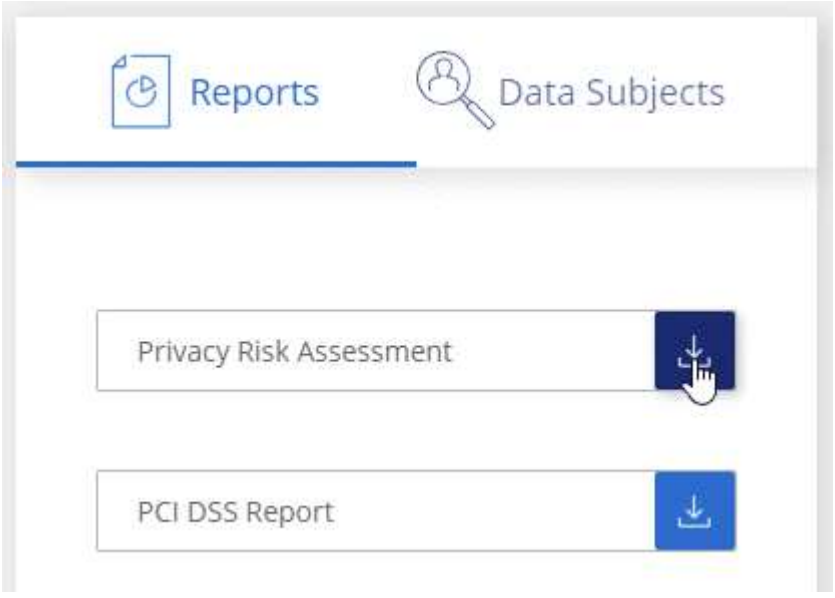
El número de personas, por ubicación, para las cuales se encontraron identificadores nacionales.

Generación del Informe de Evaluación de riesgo de Privacidad

Vaya a la ficha cumplimiento para generar el informe.

Pasos

1. En la parte superior de Cloud Manager, haga clic en **Cloud Compliance**.
2. En **Informes**, haga clic en el icono de descarga situado junto a **Evaluación de riesgo de privacidad**.



Resultado

Cloud Compliance genera un informe en PDF que puede revisar y enviar a otros grupos según sea necesario.

Puntuación de gravedad

Cloud Compliance calcula la puntuación de gravedad del informe de evaluación del riesgo de privacidad sobre la base de tres variables:

- El porcentaje de datos personales de todos los datos.
- El porcentaje de datos personales confidenciales de todos los datos.
- El porcentaje de archivos que incluyen temas de datos, determinado por identificadores nacionales como ID nacionales, números de Seguro Social y números de identificación fiscal.

La lógica utilizada para determinar la puntuación es la siguiente:

Puntuación de gravedad	Lógica
0	Las tres variables son exactamente 0 %
1	Una de las variables es mayor que 0 %
2	Una de las variables es mayor que el 3 %
3	Dos de las variables son mayores que el 3%
4	Tres de las variables son mayores que el 3%
5	Una de las variables es mayor que el 6 %
6	Dos de las variables son mayores que el 6%
7	Tres de las variables son mayores que el 6%
8	Una de las variables es mayor que el 15 %
9	Dos de las variables son mayores que el 15%
10	Tres de las variables son mayores que el 15%

Informe PCI DSS

El Informe de estándares de seguridad de datos del sector de la tarjeta de pago (PCI DSS) puede ayudarle a identificar la distribución de información de la tarjeta de crédito a través de sus archivos. El informe incluye la siguiente información:

Descripción general
: Cuántos archivos contienen información de tarjeta de crédito y en qué entornos de trabajo.

Cifrado
: Porcentaje de archivos que contienen información de la tarjeta de crédito en entornos de trabajo cifrados o no cifrados. Esta información es específica de Cloud Volumes ONTAP.

Protección contra ransomware
: Porcentaje de archivos que contienen información de tarjetas de crédito en entornos de trabajo que tienen o no la protección contra ransomware habilitada. Esta información es específica de Cloud Volumes ONTAP.

Retención
: El periodo de tiempo en el que se modificaron por última vez los archivos. Esto es útil porque no debe mantener la información de la tarjeta de crédito por más tiempo de lo que necesita para procesarla.

Distribución de la información de la tarjeta de crédito

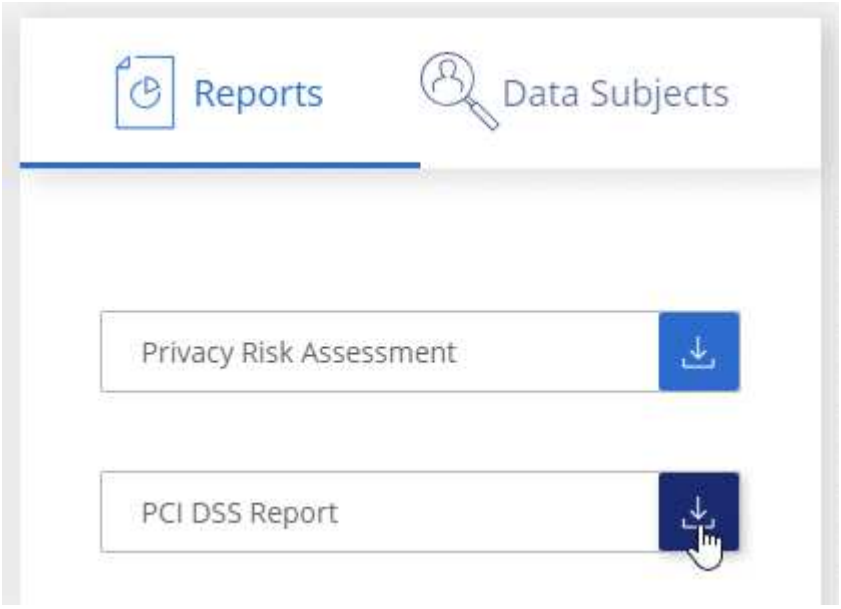
Entornos en los que se encontró la información de la tarjeta de crédito y si la protección mediante cifrado y ransomware están habilitadas.

Generación del informe PCI DSS

Vaya a la ficha cumplimiento para generar el informe.

Pasos

1. En la parte superior de Cloud Manager, haga clic en **Cloud Compliance**.
2. En **Informes**, haga clic en el icono de descarga situado junto a **PCI DSS Report**.



Resultado

Cloud Compliance genera un informe en PDF que puede revisar y enviar a otros grupos según sea necesario.

Informe HIPAA

El Informe de la Ley de Portabilidad y responsabilidad de los Seguros médicos (HIPAA) puede ayudarle a identificar archivos que contengan información médica. Está diseñado para ayudar en el requisito de su organización de cumplir con las leyes de privacidad de datos HIPAA. El Cloud Compliance de información incluye:

- Patrón de referencia de salud
- Código médico ICD-10-cm
- Código médico ICD-9-cm
- HR – Categoría de salud
- Datos de aplicación de Salud

El informe incluye la siguiente información:

Descripción general

Cuántos archivos contienen información médica y en qué entornos de trabajo.

Cifrado

Porcentaje de archivos que contienen información médica en entornos de trabajo cifrados o no cifrados. Esta información es específica de Cloud Volumes ONTAP.

Protección contra ransomware

Porcentaje de archivos que contienen información médica en entornos de trabajo que tienen o no la protección contra ransomware activada. Esta información es específica de Cloud Volumes ONTAP.

Retención

El periodo de tiempo en el que se modificaron por última vez los archivos. Esto es útil porque no debe mantener la información de salud por más tiempo de lo que necesita para procesarla.

Distribución de la información de salud

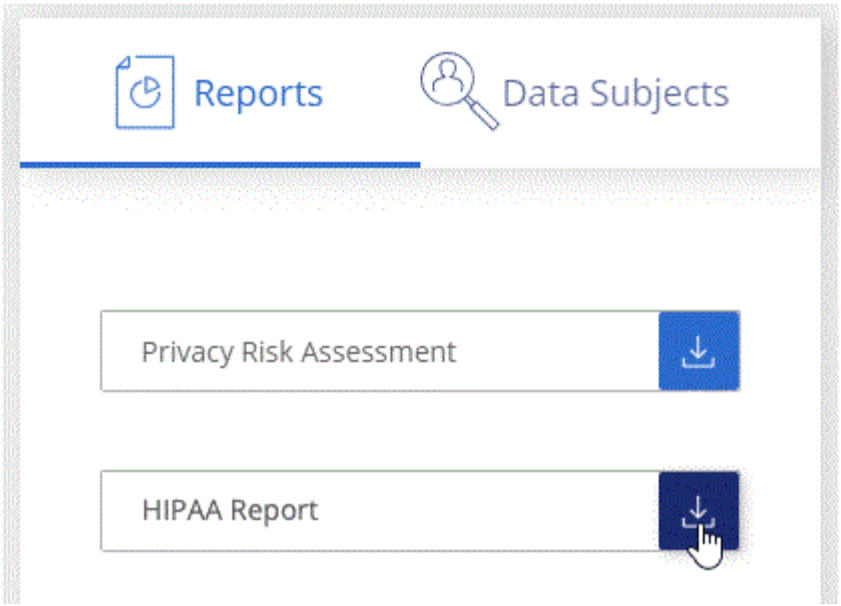
Entornos en los que se encontró la información médica y si está habilitada el cifrado y la protección contra ransomware.

Generación del informe HIPAA

Vaya a la ficha cumplimiento para generar el informe.

Pasos

1. En la parte superior de Cloud Manager, haga clic en **Cloud Compliance**.
2. En **Informes**, haga clic en el icono de descarga situado junto a **Informe HIPAA**.



Resultado

Cloud Compliance genera un informe en PDF que puede revisar y enviar a otros grupos según sea necesario.

Selección de los entornos de trabajo para los informes

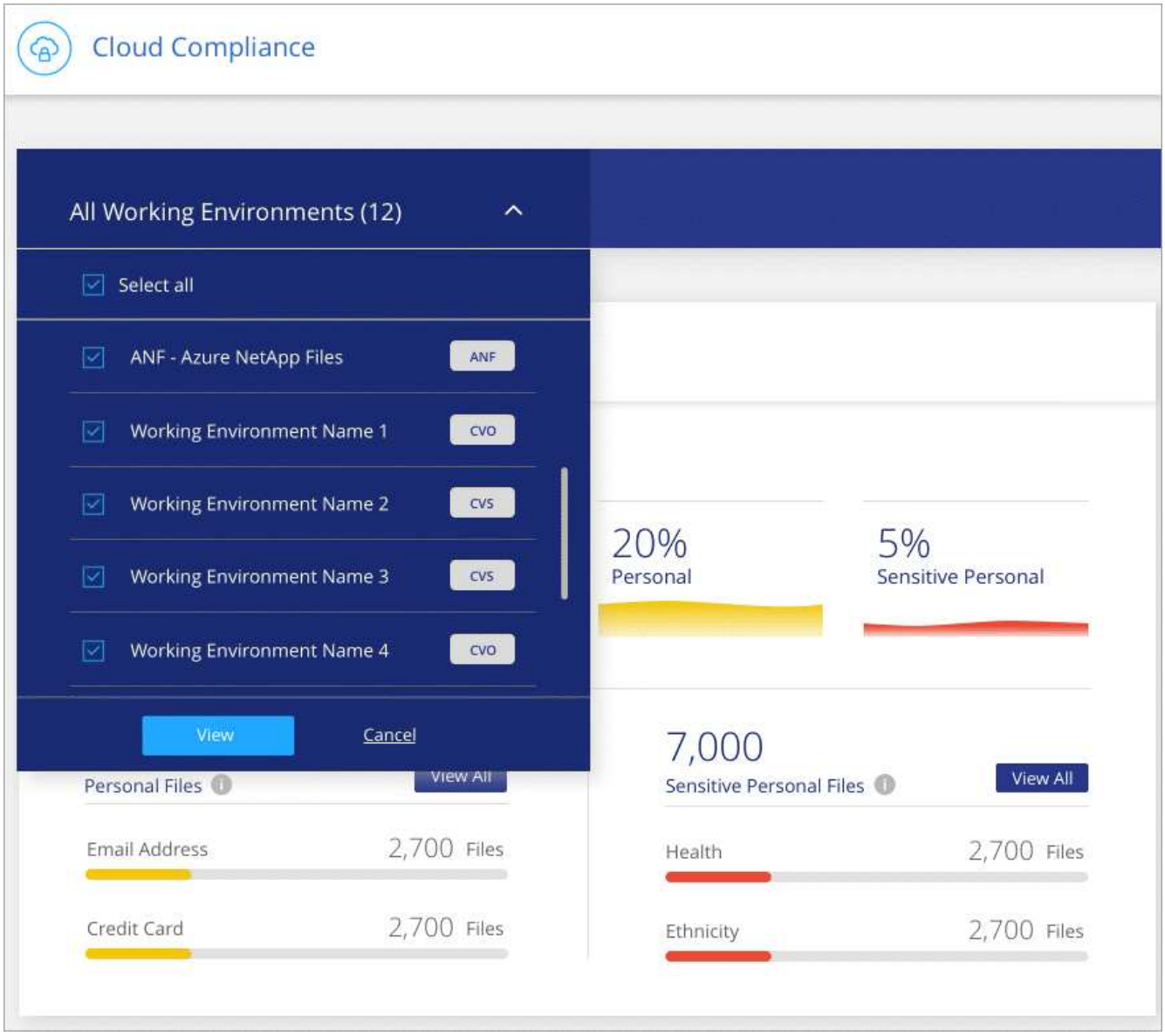
Puede filtrar el contenido del panel de Cloud Compliance para ver los datos de cumplimiento de normativas de

todos los entornos de trabajo y bases de datos, o solo en entornos de trabajo específicos.

Al filtrar la consola, Cloud Compliance determina los datos de cumplimiento de normativas e informa solo a los entornos de trabajo que haya seleccionado.

Pasos

1. Haga clic en el menú desplegable filtro, seleccione los entornos de trabajo para los que desea ver datos y haga clic en **Ver**.



Respuesta a una solicitud de acceso de un sujeto de datos

Responda a una solicitud de acceso a un sujeto de datos (DSAR) buscando el nombre completo o el identificador conocido de un sujeto (como una dirección de correo electrónico) y, a continuación, descargando un informe. El informe está diseñado para ayudar en el requisito de su organización a cumplir con el RGPD o con leyes de privacidad de datos similares.

NetApp no puede garantizar una precisión del 100 % de los datos personales y datos personales confidenciales que identifica Cloud Compliance. Siempre debe validar la información revisando los datos.

¿Qué es una solicitud de acceso de asunto de datos?

Las normas de privacidad, como el GDPR europeo, otorgan a sujetos de datos (como clientes o empleados) el derecho a acceder a sus datos personales. Cuando un sujeto de datos solicita esta información, se le conoce como DSAR (solicitud de acceso a sujetos de datos). Las organizaciones deben responder a estas solicitudes "sin demora indebida" y, a más tardar, en el plazo de un mes a partir de su recepción.

¿Cómo puede ayudarle Cloud Compliance a responder a un DSAR?

Cuando realiza una búsqueda de asunto de datos, Cloud Compliance encuentra todos los archivos que contienen el nombre o identificador de esa persona. Cloud Compliance comprueba si existen los datos preindexados más recientes en cuanto a nombre o identificador. No inicia una nueva exploración.

Una vez finalizada la búsqueda, puede descargar la lista de archivos para un informe de solicitud de acceso a un sujeto de datos. El informe agrega información procedente de los datos y los coloca en términos legales de los que se puede enviar a la persona.

Búsqueda de sujetos de datos y descarga de informes

Busque el nombre completo o el identificador conocido del sujeto de datos y, a continuación, descargue un informe de la lista de archivos o un informe DSAR. Puede buscar por "cualquier tipo de información personal".

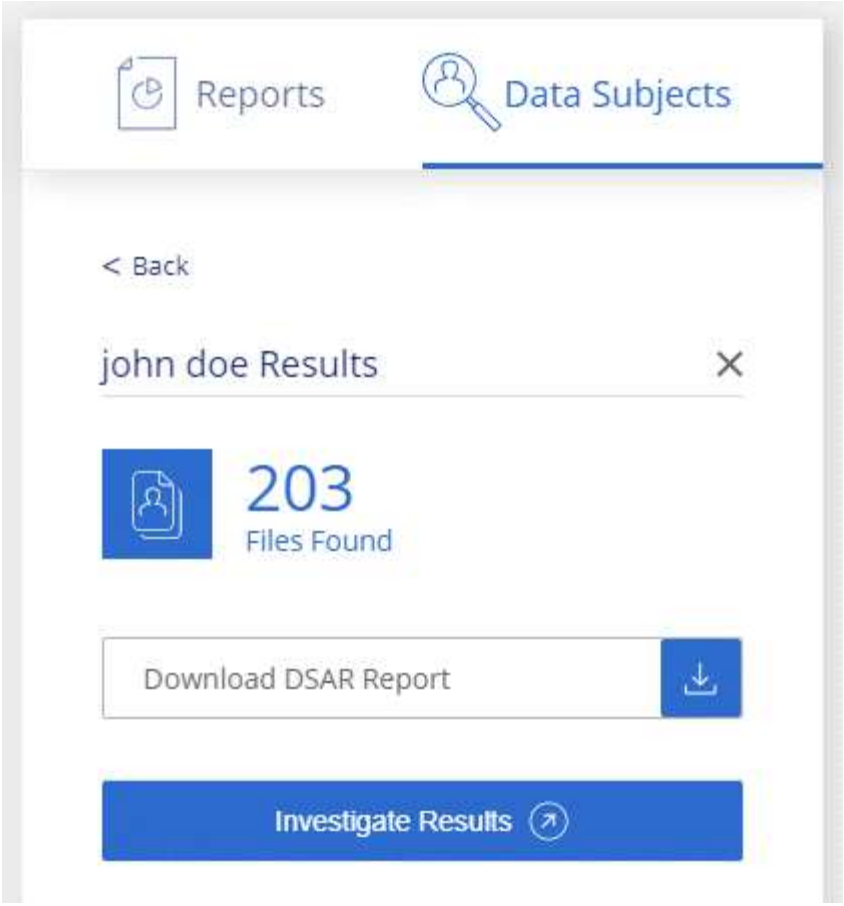
Sólo se admite inglés al buscar los nombres de los sujetos de datos. Más adelante se añadirá compatibilidad con más idiomas.

La búsqueda de sujetos de datos no es compatible en las bases de datos en este momento.

Pasos

1. En la parte superior de Cloud Manager, haga clic en **Cloud Compliance**.
2. Haga clic en **Temas de datos**.
3. Busque el nombre completo o el identificador conocido del sujeto de datos.

   A continuación se muestra un ejemplo que muestra una búsqueda del nombre *john doe*:



4. Elija una de las opciones disponibles:
   - **Descargar informe DSAR**: Respuesta formal a la solicitud de acceso que se puede enviar al sujeto de datos. Este informe contiene información generada automáticamente en función de los datos de que Cloud Compliance se encuentra en el asunto de los datos y se ha diseñado para su uso como plantilla. Debe completar el formulario y revisarlo internamente antes de enviarlo al sujeto de datos.
   - **investigar resultados**: Página que permite investigar los datos mediante la búsqueda, clasificación, ampliación de los detalles de un archivo específico y descarga de la lista de archivos.

     Si hay más de 10,000 resultados, sólo los 10,000 primeros aparecen en la lista de archivos.

Desactivación de Cloud Compliance

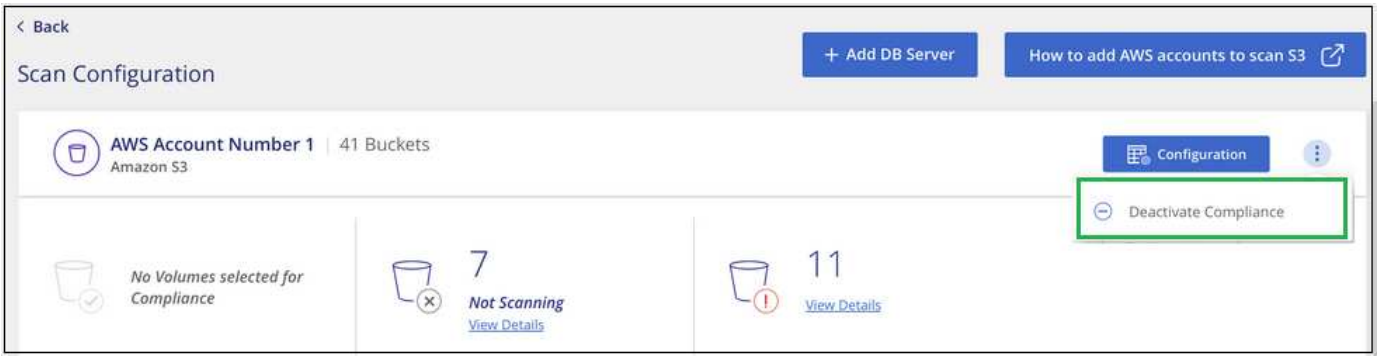
Si lo necesita, puede detener Cloud Compliance de analizar uno o más entornos de trabajo o bases de datos. También puede eliminar la instancia de Cloud Compliance si ya no desea utilizar Cloud Compliance con sus entornos de trabajo.

Desactivar los análisis de cumplimiento de normativas en un entorno de trabajo

Al desactivar los análisis, Cloud Compliance ya no analiza los datos del sistema y elimina la información de cumplimiento indexada de la instancia de Cloud Compliance (los datos del entorno de trabajo o de la base de datos en sí no se eliminan).

Pasos

En la página *Scan Configuration*, haga clic en En la fila del entorno de trabajo y, a continuación, haga clic en **Desactivar conformidad**.



También puede desactivar los análisis de cumplimiento de un entorno de trabajo desde el panel Servicios cuando seleccione el entorno de trabajo.

Eliminación de la instancia de Cloud Compliance

Puede eliminar la instancia de Cloud Compliance si ya no desea utilizar Cloud Compliance. Al eliminar la instancia también se eliminan los discos asociados en los que residen los datos indexados.

Paso

1. Vaya a la consola de su proveedor de cloud y elimine la instancia de Cloud Compliance.

   La instancia se denomina *CloudCompliance* con un hash generado (UUID) concatenado. Por ejemplo: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*

Preguntas frecuentes sobre Cloud Compliance

Estas preguntas frecuentes pueden ayudar si sólo está buscando una respuesta rápida a una pregunta.

¿Qué es el cumplimiento de normativas en el cloud?

Cloud Compliance es una oferta de cloud que utiliza la tecnología impulsada por inteligencia artificial (IA) para ayudar a las organizaciones a comprender el contexto de los datos e identificar datos confidenciales en sus configuraciones de Azure NetApp Files, sistemas Cloud Volumes ONTAP alojados en AWS o Azure, bloques de Amazon S3 y bases de datos.

Cloud Compliance ofrece parámetros predefinidos (como tipos y categorías de información confidencial) para hacer frente a nuevas normativas de cumplimiento de normativas de datos para privacidad y sensibilidad de los datos, como RGPD, CCPA, HIPAA, etc.

¿por qué debo usar Cloud Compliance?

El cumplimiento normativo del cloud puede poner a su disposición todos los datos que le ayudarán a:

- Cumpla con las normativas sobre privacidad y cumplimiento de normativas de datos.
- Cumpla con las políticas de retención de datos.

- Localice con facilidad y cree informes sobre datos específicos en respuesta a sujetos de datos, según lo requiera el RGPD, la CCPA, la HIPAA y otras normativas de privacidad de los datos.

¿Cuáles son los casos de uso comunes de Cloud Compliance?

- Identificación de la Información personal de identificación (PII).
- Identificar un amplio abanico de información confidencial que requieran las normativas de privacidad del RGPD y de la CCPA.
- Cumpla con las normativas de privacidad de datos nuevas y futuras.

"Obtenga más información sobre los casos de uso de cumplimiento de normativas para el cloud".

¿Qué tipos de datos se pueden analizar con Cloud Compliance?

Cloud Compliance admite el análisis de datos no estructurados sobre protocolos NFS y CIFS gestionados por Cloud Volumes ONTAP y Azure NetApp Files. Cloud Compliance también puede analizar datos almacenados en bloques de Amazon S3.

Además, Cloud Compliance puede analizar las bases de datos que se encuentran en cualquier lugar; no es necesario que Cloud Manager las gestione.

"Descubra cómo funcionan las exploraciones".

¿Qué proveedores de cloud son compatibles?

Cloud Compliance funciona como parte de Cloud Manager y actualmente admite AWS y Azure. Esto proporciona a su organización una visibilidad de privacidad unificada a través de distintos proveedores de cloud. Pronto se añadirá la compatibilidad con Google Cloud Platform (GCP).

¿Cómo puedo acceder a Cloud Compliance?

Cloud Compliance se opera y gestiona a través de Cloud Manager. Puede acceder a las funciones de Cloud Compliance desde la ficha **cumplimiento** de Cloud Manager.

¿Cómo funciona Cloud Compliance?

Cloud Compliance pone en marcha otra capa de inteligencia artificial junto con su sistema Cloud Manager y sus sistemas de almacenamiento. A continuación, analiza los datos en volúmenes, bloques y bases de datos e indexa la información que se encuentra.

"Más información sobre el funcionamiento de Cloud Compliance".

¿Cuánto cuesta el cumplimiento de las normativas cloud?

El coste de utilizar Cloud Compliance depende de la cantidad de datos que se escanee. Los primeros 1 TB de datos que analiza Cloud Compliance en un espacio de trabajo de Cloud Manager son gratuitos. Es necesario contar con una suscripción a AWS o Azure Marketplace para seguir analizando los datos después de ese punto. Consulte "precios" para obtener más detalles.

¿con qué frecuencia el Cloud Compliance analiza mis datos?

Los datos cambian con frecuencia, por lo que Cloud Compliance analiza los datos de forma continua y sin

impacto en los datos. Aunque el análisis inicial de los datos puede tardar más tiempo, los análisis posteriores sólo analizan los cambios incrementales, lo que reduce los tiempos de análisis del sistema.

"Descubra cómo funcionan las exploraciones".

¿ofrece informes Cloud Compliance?

Sí. La información que ofrece Cloud Compliance puede ser relevante para otras partes interesadas de sus organizaciones. De esta forma, le permitimos generar informes para compartir la información.

Los siguientes informes están disponibles para Cloud Compliance:

Informe de evaluación de riesgos de privacidad

Proporciona información sobre la privacidad de sus datos y una puntuación de riesgo para la privacidad. "Leer más".

Informe de solicitud de acceso de asunto de datos

Permite extraer un informe de todos los archivos que contienen información sobre el nombre específico o el identificador personal de un sujeto de datos. "Leer más".

Informe PCI DSS

Le ayuda a identificar la distribución de la información de la tarjeta de crédito a través de sus archivos. "Leer más".

Informe HIPAA

Le ayuda a identificar la distribución de información médica a través de sus archivos. "Leer más".

Informa sobre un tipo de información específico

Hay informes disponibles que incluyen detalles sobre los archivos identificados que contienen datos personales y datos personales confidenciales. También puede ver los archivos desglosados por categoría y tipo de archivo. "Leer más".

¿Qué tipo de instancia o máquina virtual se requiere para Cloud Compliance?

- En Azure, Cloud Compliance se ejecuta en una máquina virtual Standard_D16s_v3 con un disco de 512 GB.
- En AWS, Cloud Compliance se ejecuta en una instancia de 5,4 x grande con un disco GP2 de 500 GB.

  En regiones donde no hay m5.4xLarge disponible, Cloud Compliance se ejecuta en lugar de una instancia m4.4xLarge.

No se admite el cambio o cambio de tamaño del tipo de máquina virtual/instancia. Debe utilizar el tamaño predeterminado que se proporciona.

"Más información sobre el funcionamiento de Cloud Compliance".

¿el rendimiento del análisis varía?

El rendimiento de análisis puede variar en función del ancho de banda de la red y del tamaño medio de los archivos del entorno de cloud.

¿Qué tipos de archivo son compatibles?

Cloud Compliance analiza todos los archivos para obtener información sobre categorías y metadatos y muestra todos los tipos de archivos en la sección tipos de archivos de la consola.

Cuando Cloud Compliance detecta información personal identificable (PII) o cuando realiza una búsqueda DSAR, sólo se admiten los siguientes formatos de archivo: .PDF, .DOCX, .DOC, .PPTX, .XLS, .XLSX, .CSV, .TXT, .RTF y .JSON.

¿Cómo hago posible el cumplimiento de normativas para el cloud?

En primer lugar, tiene que implementar una instancia de Cloud Compliance en Cloud Manager. Una vez que la instancia se esté ejecutando, puede habilitarla en entornos de trabajo y bases de datos existentes desde la ficha **cumplimiento** o seleccionando un entorno de trabajo específico.

"Aprenda cómo empezar".

> La activación de Cloud Compliance da como resultado un análisis inicial inmediato. Los resultados de cumplimiento se muestran poco después.

¿Cómo se deshabilita Cloud Compliance?

Puede deshabilitar Cloud Compliance desde la página entornos de trabajo después de seleccionar un entorno de trabajo individual.

"Leer más".

> Para eliminar por completo la instancia de Cloud Compliance, puede eliminar manualmente la instancia de Cloud Compliance del portal de su proveedor de cloud.

¿Qué sucede si la organización en niveles de datos está habilitada en Cloud Volumes ONTAP?

Es posible que desee habilitar Cloud Compliance en un sistema Cloud Volumes ONTAP que organiza los datos inactivos en almacenamiento de objetos. Si la organización en niveles de los datos está habilitada, Cloud Compliance analiza todos los datos, ya sea en discos o datos inactivos organizados en niveles para el almacenamiento de objetos.

El análisis de cumplimiento de normativas no calienta los datos inactivos: Permanece frío y organizado en niveles en el almacenamiento de objetos.

¿Puedo utilizar Cloud Compliance para analizar almacenamiento ONTAP en las instalaciones?

No se admite el análisis de los datos directamente desde un entorno de trabajo local de ONTAP. Pero puede analizar sus datos de ONTAP en las instalaciones replicando los datos NFS o CIFS en las instalaciones en un entorno de trabajo de Cloud Volumes ONTAP para después activar el cumplimiento de normativas en dichos volúmenes. Tenemos pensado admitir el cumplimiento de normativas cloud con ofertas de cloud adicionales como Cloud Volumes Service.

"Leer más".

¿Cloud Compliance puede enviar notificaciones a mi organización?

No, pero puede descargar informes de estado que puede compartir internamente en su organización.

¿Puedo personalizar el servicio según las necesidades de mi organización?

Cloud Compliance proporciona información inmediata para sus datos. Estos conocimientos se pueden extraer y utilizar para las necesidades de su organización.

¿Puedo limitar la información de Cloud Compliance a usuarios específicos?

Sí, Cloud Compliance se integra totalmente con Cloud Manager. Los usuarios de Cloud Manager solo pueden ver información de los entornos de trabajo que pueden ver de acuerdo con los privilegios de su espacio de trabajo.

Además, si desea permitir a determinados usuarios ver los resultados del análisis de Cloud Compliance sin tener la capacidad de administrar la configuración de Cloud Compliance, puede asignar a esos usuarios la función *Cloud Compliance Viewer*.

"Leer más".

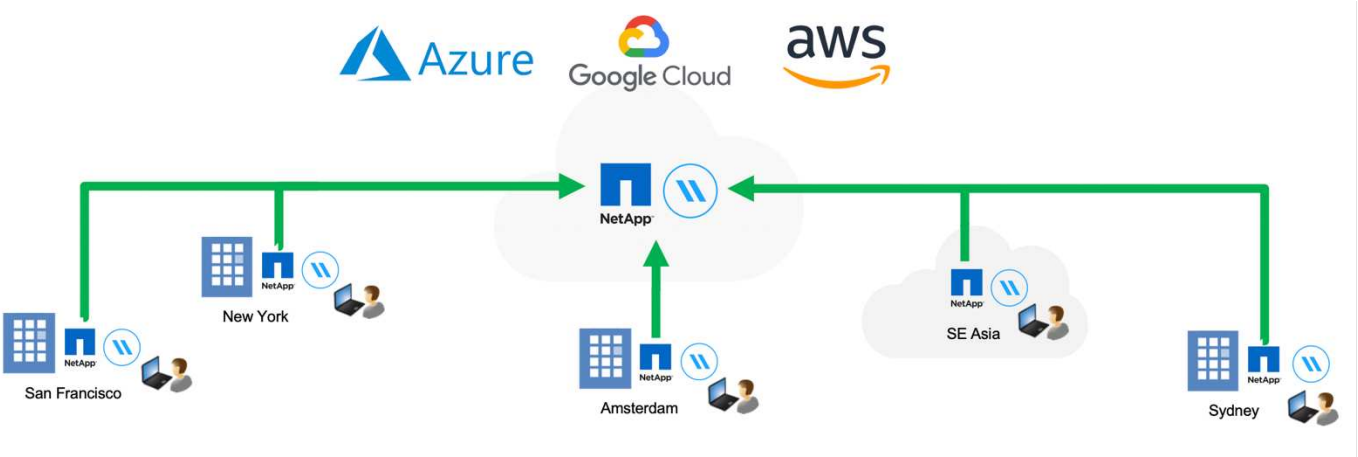
Habilitación del uso compartido de archivos global en tiempo real

Obtenga más información sobre la caché global de archivos

NetApp Global File Cache le permite consolidar silos de servidores de archivos distribuidos en un espacio de almacenamiento global cohesivo en el cloud público. Esto crea un sistema de archivos con acceso global en la nube que todas las ubicaciones remotas pueden usar como si fueran locales.

Descripción general

La implementación de Global File Cache da como resultado un único espacio de almacenamiento centralizado, frente a una arquitectura de almacenamiento distribuido que requiere gestión de datos local, backup, gestión de la seguridad, almacenamiento e infraestructura en cada ubicación.



Funciones

La caché global de archivos habilita las siguientes características:

- Consolide y centralice sus datos en el cloud público y en las aplicaciones aproveche la escalabilidad y el rendimiento de las soluciones de almacenamiento de clase empresarial
- Crear un único conjunto de datos para usuarios de todo el mundo y aprovechar el almacenamiento en caché inteligente de archivos para mejorar el rendimiento, la colaboración y el acceso a los datos
- Confíe en una caché autosostenible y de gestión automática, y elimine los backups y las copias de datos completas. Utilice el almacenamiento en caché de archivos locales para los datos activos y reduzca el almacenamiento externa
- Acceso transparente desde sucursales a través de un espacio de nombre global con bloqueo central de archivos en tiempo real

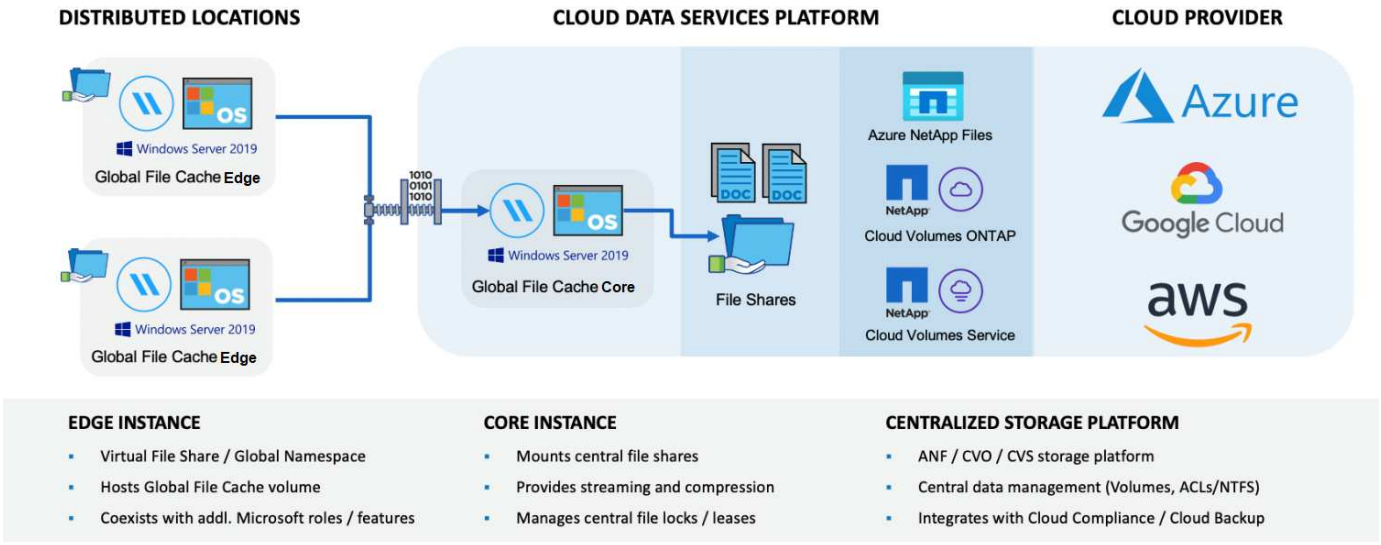
Consulte más información sobre las funciones y los casos de uso de la caché global de archivos "aquí".

Componentes de caché de archivos global

La caché global de archivos consta de los siguientes componentes:

- Servidor de gestión de caché de archivos global
- Núcleo de caché de archivos global
- Global File Cache Edge (puesta en marcha en ubicaciones remotas)

La instancia de almacenamiento central en caché de archivos global se monta en los recursos compartidos de archivos de su empresa alojados en la plataforma de almacenamiento de back-end elegida (como Cloud Volumes ONTAP, Cloud Volumes Service, Y Azure NetApp Files), que crean la estructura de caché de archivos global que permite centralizar y consolidar los datos no estructurados en un único conjunto de datos, ya residan en una o varias plataformas de almacenamiento en el cloud público.



Plataformas de almacenamiento compatibles

Las plataformas de almacenamiento compatibles con Global File Cache varían en función de la opción de implementación seleccionada.

Opciones de puesta en marcha automatizadas

La memoria caché de archivos global es compatible con los siguientes tipos de entornos de trabajo al implementar Cloud Manager:

- Cloud Volumes ONTAP en Azure
- Cloud Volumes ONTAP en AWS

Esta configuración le permite implementar y administrar toda la implementación del lado del servidor de caché de archivos global, incluido Global File Cache Management Server y Global File Cache Core, desde Cloud Manager.

Opciones de puesta en marcha manual

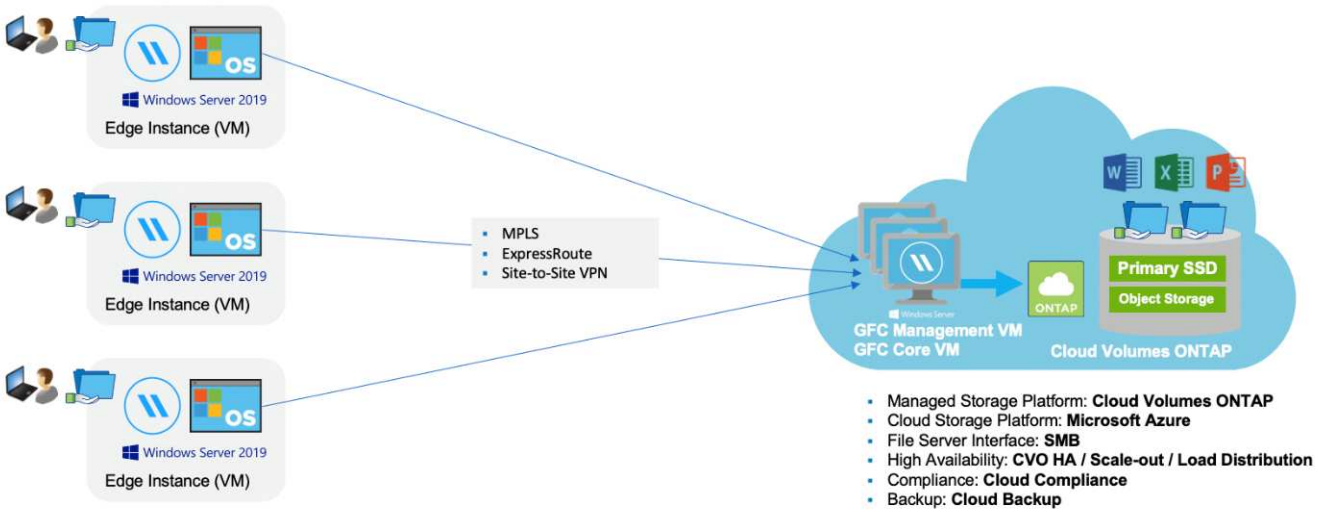
Las configuraciones de caché de archivos global también son compatibles con Cloud Volumes ONTAP, Cloud Volumes Service o Azure NetApp Files instaladas en infraestructuras de almacenamiento en cloud público de

Microsoft Azure, Google Cloud Platform o Amazon Web Services. Las soluciones en las instalaciones también están disponibles en las plataformas AFF y FAS de NetApp. En estas instalaciones, los componentes del servidor de caché de archivos global deben configurarse e implementarse manualmente, no mediante Cloud Manager.

Consulte "Guía del usuario de caché global de archivos de NetApp" para obtener más detalles.

Funcionamiento de la caché global de archivos

Global File Cache crea una estructura de software que almacena en caché los conjuntos de datos activos en oficinas remotas globalmente. Como resultado, se garantiza a los usuarios empresariales un acceso transparente a los datos y un rendimiento óptimo a escala global.



La topología a la que se hace referencia en este ejemplo es un modelo de concentrador y radio, en el que la red de oficinas remotas/ubicaciones está accediendo a un conjunto común de datos en la nube. Los puntos clave de este ejemplo son:

- Almacenamiento de datos centralizado:
  - Plataforma de almacenamiento en cloud público empresarial, como Cloud Volumes ONTAP
- Estructura de caché de archivos global:
  - Extensión del almacén de datos central a las ubicaciones remotas
  - Instancia central de caché de archivos global, montaje en recursos compartidos de archivos corporativos (SMB).
  - Instancias de Global File Cache Edge que se ejecutan en cada ubicación remota.
  - Presenta un recurso compartido de archivos virtual en cada ubicación remota que proporciona acceso a los datos centrales.
  - Aloja la caché de archivos inteligente en un volumen NTFS de tamaño personalizado (`D:\`).
- Configuración de red:
  - Conectividad de conmutación de etiquetas multiprotocolo (MPLS), ExpressRoute o VPN
- Integración con los servicios de dominio de Active Directory del cliente.
- Espacio de nombres DFS para el uso de un espacio de nombres global (recomendado).

Coste

El coste de uso de la caché de archivos global depende del tipo de instalación que haya elegido.

- Todas las instalaciones requieren que usted ponga en marcha uno o más volúmenes en el cloud (Cloud Volumes ONTAP, Cloud Volumes Service o Azure NetApp Files). Esto resulta en cargos del proveedor de cloud seleccionado.
- Todas las instalaciones también requieren la puesta en marcha de dos o más máquinas virtuales (VM) en el cloud. Esto resulta en cargos del proveedor de cloud seleccionado.
    - Servidor de gestión global de caché de archivos:

      En Azure, se ejecuta en una máquina virtual D2S_V3 o equivalente (2 vCPU/8 GB de RAM) con SSD premium de 127 GB

      En AWS, se ejecuta en una instancia m4.Large o equivalente (2 vCPU/8 GB de RAM) con SSD de 127 GB de uso general

    - Núcleo de caché de archivos global:

      En Azure, se ejecuta en una máquina virtual d4s_V3 o equivalente (4 vCPU/16 GB RAM) con 127 GB SSD premium

    En AWS, se ejecuta en una instancia m4.xlarge o equivalente (4 vCPU/16 GB de RAM) con 127 GB de SSD de uso general

- Cuando se instala con Cloud Volumes ONTAP en Azure o AWS (las configuraciones admitidas completamente implementadas a través de Cloud Manager), se cobra 3,000 USD por sitio (por cada instancia de Global File Cache Edge), al año.
- Cuando se instala con las opciones de implementación manual, el precio es diferente. Para ver una estimación de costes de alto nivel, consulte "Calcule cuánto puede ahorrar" También puede consultar al ingeniero de soluciones de caché global de archivos si desea obtener más información sobre las mejores opciones para la implementación de su empresa.

Licencia

Global File Cache incluye un servidor de gestión de licencias (LMS) basado en software, que permite consolidar la gestión de licencias e implantar licencias en todas las instancias de Core y Edge mediante un mecanismo automatizado.

Al implementar la primera instancia de Core en el centro de datos o en la nube, puede elegir designar dicha instancia como la LMS para su organización. Esta instancia LMS se configura una vez, se conecta al servicio de suscripción (a través de HTTPS) y valida su suscripción utilizando el ID de cliente proporcionado por nuestro departamento de soporte/operaciones al habilitar la suscripción. Después de realizar esta designación, asocie las instancias de Edge con el LMS proporcionando el ID de cliente y la dirección IP de la instancia de LMS.

Al adquirir licencias Edge adicionales o renovar su suscripción, nuestro departamento de soporte/operaciones actualiza los detalles de la licencia, por ejemplo, el número de sitios o la fecha de finalización de la suscripción. Una vez que LMS consulta al servicio de suscripción, los detalles de la licencia se actualizan automáticamente en la instancia de LMS y se aplican a las instancias de GFC Core y Edge.

Consulte "Guía del usuario de caché global de archivos de NetApp" para obtener más información sobre las licencias.

Limitaciones

- La versión de Global File Cache compatible con Cloud Manager requiere que la plataforma de almacenamiento de back-end utilizada como el almacenamiento central debe ser un entorno de trabajo donde se haya implementado un único nodo de Cloud Volumes ONTAP o un par de alta disponibilidad en Azure o AWS.

  Actualmente, otras plataformas de almacenamiento y otros proveedores de cloud no son compatibles con Cloud Manager, pero se pueden poner en marcha mediante procedimientos de puesta en marcha anteriores.

Estas otras configuraciones, por ejemplo, de caché de archivos global con Cloud Volumes ONTAP, Cloud Volumes Service y Azure NetApp Files en Microsoft Azure, Google Cloud y AWS, siguen siendo compatibles con los procedimientos anteriores. Consulte "Incorporación e información general sobre la caché de archivos global" para obtener más detalles.

Antes de comenzar a implementar la caché de archivos global

Hay muchos requisitos que debe tener en cuenta antes de comenzar a implementar la caché de archivos global en el cloud y en sus oficinas remotas.

Consideraciones de diseño del núcleo de caché de archivos global

En función de sus necesidades, es posible que deba implementar una o varias instancias de Global File Cache Core para crear la estructura Global File Cache. La instancia de Core está diseñada para actuar como un cop de tráfico entre las instancias distribuidas de Global File Cache Edge y los recursos del servidor de archivos del centro de datos, por ejemplo, recursos compartidos de archivos, carpetas y archivos.

Al diseñar su implementación de caché de archivos global, necesita determinar cuál es el más adecuado para su entorno en términos de escala, disponibilidad de recursos y redundancia. Global File Cache Core se puede implementar de las siguientes maneras:

- Instancia independiente de GFC Core
- Diseño distribuido de carga central GFC (en espera en frío)

Consulte Directrices de tamaño Para comprender el número máximo de instancias de Edge y el total de usuarios que cada configuración admite:

Consulte a un ingeniero de soluciones globales de caché de archivos si desea conocer las mejores opciones para la implementación de su empresa.

Directrices de tamaño

Hay algunas pautas de tamaño que debe tener en cuenta a la hora de configurar el sistema inicial. Debe volver a revisar estas relaciones una vez acumulado algún historial de uso para asegurarse de que está utilizando el sistema de forma óptima. Entre ellos se incluyen:

- Proporción de bordes de caché de archivos global/núcleo
- Proporción de usuarios distribuidos/Global File Cache Edge
- Proporción de usuarios distribuidos/núcleo de caché global de archivos

Número de instancias de Edge por instancia de Core

Nuestras directrices recomiendan hasta 10 instancias Edge por instancia de Core de caché de archivos global, con un máximo de 20 bordes por instancia de Core de caché de archivos global. Depende en gran medida del tipo y el tamaño medio de los archivos de la carga de trabajo más común. En algunos casos, con cargas de trabajo más comunes, puede añadir más instancias de Edge por Core, pero, en estos casos, debe ponerse en contacto con el servicio de soporte de NetApp para ajustar correctamente el tamaño de las instancias de Edge y Core, en función de los tipos y tamaños de los conjuntos de archivos.

Puede aprovechar múltiples instancias de Global File Cache Edge y Core simultáneamente para escalar horizontalmente su infraestructura en función de los requisitos.

Número de usuarios simultáneos por instancia de Edge

Global File Cache Edge gestiona el trabajo pesado en términos de algoritmos de almacenamiento en caché y diferenciación a nivel de archivo. Una única instancia de Global File Cache Edge puede servir hasta 400 usuarios por instancia física Edge dedicada y hasta 200 usuarios para puestas en marcha virtuales dedicadas. Depende en gran medida del tipo y el tamaño medio de los archivos de la carga de trabajo más común. Para tipos de archivos de colaboración más grandes, guiar hacia el 50% del límite inferior máximo de usuarios por límite inferior de Global File Cache Edge (en función de la implementación física o virtual). Para elementos de Office más comunes con un tamaño medio de archivo <1 MB, guía hacia el 100% de usuarios por límite superior de borde de caché de archivos global (dependiendo de la implementación física o virtual).

Global File Cache Edge detecta si se está ejecutando en una instancia virtual o física y limitará el número de conexiones SMB al recurso compartido local de archivos virtuales al máximo de 200 o 400 conexiones simultáneas.

Número de usuarios simultáneos por instancia de Core

La instancia de Global File Cache Core es extremadamente escalable, con un número recomendado de usuarios simultáneos de 3,000 usuarios por Core. Depende en gran medida del tipo y el tamaño medio de los archivos de la carga de trabajo más común.

Consulte a un ingeniero de soluciones globales de caché de archivos si desea conocer las mejores opciones para la implementación de su empresa.

Requisitos previos

Los requisitos previos descritos en esta sección son para los componentes instalados en la nube: El servidor de administración de caché global de archivos y el núcleo de caché global de archivos.

Se describen los requisitos previos de Global File Cache Edge "aquí".

Instancia de Cloud Manager

Cuando utilice Cloud Volumes ONTAP para Azure como plataforma de almacenamiento, asegúrese de que Cloud Manager tenga los permisos que se muestran en la información más reciente "Política de Cloud Manager para Azure".

Las instancias recién creadas tendrán todos los permisos necesarios de forma predeterminada. Si implementó su instancia antes de la versión 3.8.7 (3 de agosto de 2020), tendrá que añadir estos elementos.

```
"Microsoft.Resources/deployments/operationStatuses/read",
"Microsoft.Insights/Metrics/Read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/extensions/delete",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
```

Plataforma de almacenamiento (volúmenes)

La plataforma de almacenamiento del entorno de administración, en este caso, la instancia de Cloud Volumes ONTAP implementada, debería presentar recursos compartidos de archivos SMB. Todos los recursos compartidos que se expongan a través de la caché global de archivos deben permitir al grupo Everyone Control total en el nivel de recurso compartido, restringiendo al mismo tiempo los permisos a través de los permisos NTFS.

Si no ha configurado al menos un recurso compartido de archivos SMB en la instancia de Cloud Volumes ONTAP, debe tener lista la siguiente información para poder configurar esta información durante la instalación:

- Nombre de dominio de Active Directory, dirección IP del servidor de nombres y credenciales de administración de Active Directory.
- El nombre y el tamaño del volumen que se desea crear, el nombre del agregado en el que se creará el volumen y el nombre del recurso compartido.

Recomendamos que el volumen sea lo suficientemente grande como para alojar el conjunto de datos total para la aplicación junto con la capacidad de escalar en función de lo que crezca el conjunto de datos. Si tiene varios agregados en el entorno de trabajo, consulte "Gestión de los agregados existentes" para determinar qué agregado tiene el espacio más disponible para el nuevo volumen.

Servidor de gestión de caché de archivos global

Este servidor de gestión global de caché de archivos requiere acceso externo a través de HTTPS (puerto TCP 443) para conectarse al servicio de suscripción del proveedor de cloud y acceder a estas direcciones URL:

- "https://talonazuremicroservices.azurewebsites.net"
- "https://talonlicensing.table.core.windows.net"

Este puerto debe excluirse de cualquier dispositivo de optimización WAN o políticas de restricción de firewall para que el software de caché de archivos global funcione correctamente.

El servidor de administración de caché de archivos global también requiere un nombre NetBIOS único (geográfico) para la instancia (como GFC-MS1).

Un servidor de administración puede admitir varias instancias de Global File Cache Core implementadas en diferentes entornos de trabajo. Cuando se pone en marcha desde Cloud Manager, cada entorno de trabajo tiene su propio almacenamiento back-end independiente y no contendría los mismos datos.

Núcleo de caché de archivos global

Este núcleo de caché de archivos global escucha el intervalo de puertos TCP 6618-6630. En función de su firewall o de la configuración del grupo de seguridad de red (NSG), es posible que tenga que permitir explícitamente el acceso a estos puertos mediante reglas de puerto entrantes. Además, estos puertos deben excluirse de cualquier dispositivo de optimización WAN o directivas de restricción de firewall para que el software de caché de archivos global funcione correctamente.

Los requisitos principales de la caché global de archivos son:

- Nombre NetBIOS exclusivo (geográfico) para la instancia (Como GFC-CORE1)
- Nombre de dominio de Active Directory
  - Las instancias de caché de archivos global deben unirse al dominio de Active Directory.
  - Las instancias de caché de archivos global deben gestionarse en una unidad organizativa específica (OU) de caché de archivos global y excluirse de los GPO de la empresa heredados.
- Cuenta de servicio. Los servicios de este núcleo de caché global de archivos se ejecutan como una cuenta de usuario de dominio específica. Esta cuenta, también conocida como cuenta de servicio, debe tener los siguientes privilegios en cada uno de los servidores SMB que se asociarán a la instancia de núcleo de caché de archivos global:
  - La cuenta de servicio aprovisionada debe ser un usuario de dominio.

Dependiendo del nivel de restricciones y GPO del entorno de red, esta cuenta podría requerir privilegios de administrador de dominio.

- Debe tener privilegios de "Ejecutar como servicio".
- La contraseña se debe establecer en "no caducar nunca".
- La opción de cuenta "el usuario debe cambiar la contraseña en el siguiente inicio de sesión" debe ESTAR DESACTIVADA (sin marcar).
- Debe ser miembro del grupo operadores de copia de seguridad integrados del servidor de archivos back-end (esto se habilita automáticamente cuando se implementa a través de Cloud Manager).

Servidor de gestión de licencias

- El servidor de gestión de licencias de caché global de archivos (LMS) debe configurarse en una edición de Microsoft Windows Server 2016 Standard o Datacenter o Windows Server 2019 Standard o Datacenter, preferiblemente en la instancia de núcleo de caché global de archivos en el centro de datos o en la nube.
- Si necesita una instancia LMS de caché global de archivos independiente, debe instalar el paquete de instalación más reciente del software de caché global de archivos en una instancia prístina de Microsoft Windows Server.
- La instancia de LMS debe poder conectarse al servicio de suscripción (servicios Azure / Internet pública) mediante HTTPS (puerto TCP 443).
- Las instancias Core y Edge deben conectarse a la instancia LMS mediante HTTPS (puerto TCP 443).

Redes

- Firewall: Se deben permitir los puertos TCP entre las instancias Global File Cache Edge y Core.
- Puertos TCP de caché de archivos global: 443 (HTTPS), 6618–6630.
- Los dispositivos de optimización de red (como Riverbed Steelhead) deben configurarse para pasar por los puertos específicos de la caché global de archivos (TCP 6618-6630).

Primeros pasos

Utilice Cloud Manager para implementar el servidor de administración de caché de archivos global y el software Global File Cache Core en el entorno de trabajo.

Habilite la caché de archivos global mediante Cloud Manager

En esta configuración, implementará el servidor de administración de caché de archivos global y el núcleo de caché de archivos global en el mismo entorno de trabajo en el que creó el sistema Cloud Volumes ONTAP mediante Cloud Manager.

Ver "este vídeo" para ver los pasos de principio a fin.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles:

Ponga en marcha Cloud Volumes ONTAP

Ponga en marcha Cloud Volumes ONTAP en Azure o AWS y configure los recursos compartidos de archivos de SMB. Para obtener más información, consulte "Inicio de Cloud Volumes ONTAP en Azure" o. "Inicio de Cloud Volumes ONTAP en AWS".

Implemente el servidor de gestión global de caché de archivos

Implemente una instancia del servidor de administración de caché de archivos global en el mismo entorno de trabajo que la instancia de Cloud Volumes ONTAP.

Implemente el núcleo de caché global de archivos

Implementar una instancia, o varias instancias, del núcleo de caché de archivos global en el mismo entorno de trabajo que la instancia de Cloud Volumes ONTAP y unirlo al dominio de Active Directory.

Memoria caché de archivos global de licencias

Configure el servicio de servidor de gestión de licencias (LMS) de caché global de archivos en una instancia de núcleo de caché global de archivos. Necesitará sus credenciales de NSS o un ID de cliente que proporcione NetApp para activar su suscripción.

Implemente las instancias de Global File Cache Edge

Consulte "Implementación de instancias globales de File Cache Edge" Para implementar las instancias de Global File Cache Edge en cada ubicación remota. Este paso no se realiza mediante Cloud Manager.

Ponga en marcha Cloud Volumes ONTAP como su plataforma de almacenamiento

En la versión actual, la caché de archivos global es compatible con Cloud Volumes ONTAP implementado en Azure o AWS. Para obtener detalles sobre los requisitos previos, los requisitos y las instrucciones de puesta en marcha, consulte "Inicio de Cloud Volumes ONTAP en Azure" o. "Inicio de Cloud Volumes ONTAP en AWS".

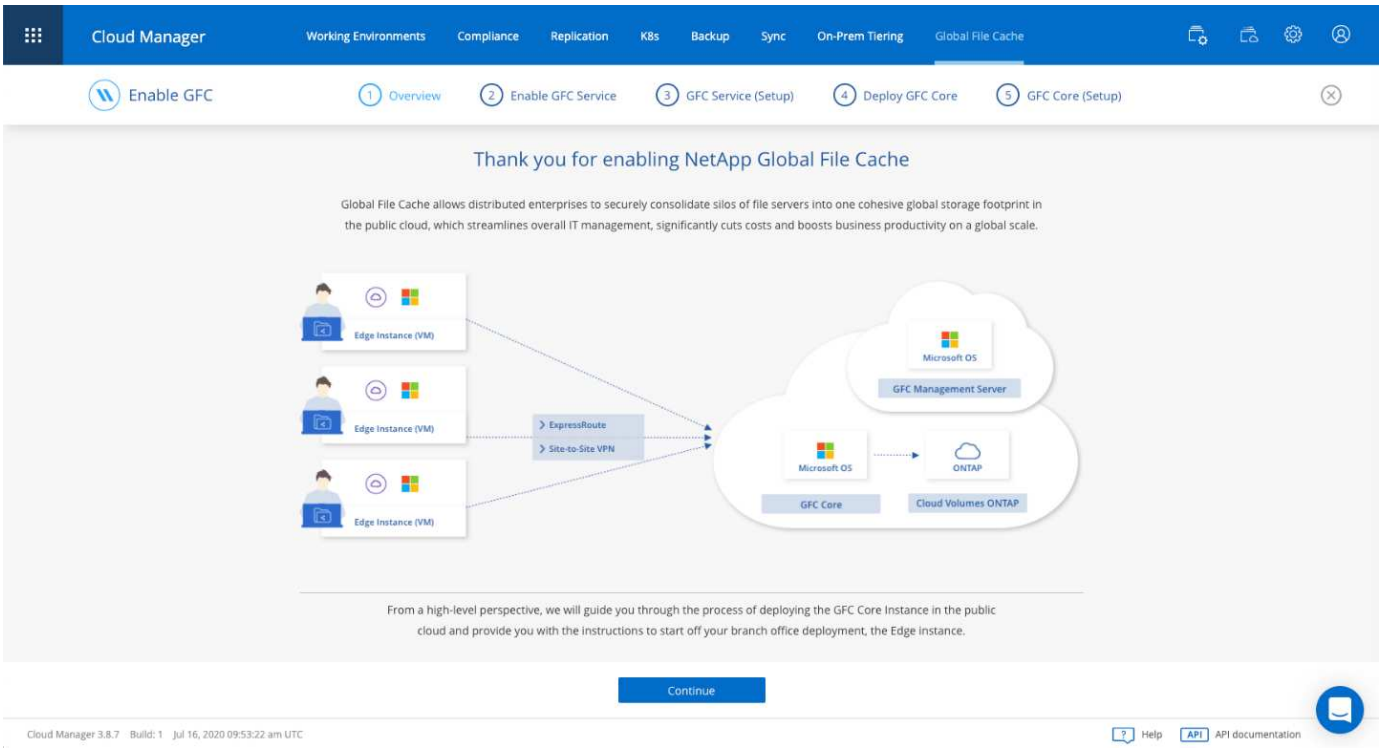
Tenga en cuenta los siguientes requisitos adicionales de caché global de archivos:

- Debe configurar los recursos compartidos de archivos SMB en la instancia de Cloud Volumes ONTAP.

  Si no hay recursos compartidos de archivos SMB configurados en la instancia, se le pedirá que configure los recursos compartidos SMB durante la instalación de los componentes de Global File Cache.

Habilite la caché global de archivos en el entorno de trabajo

El asistente de caché global de archivos le guía por los pasos para implementar la instancia de servidor de gestión global de caché de archivos y la instancia de núcleo de caché global de archivos, como se indica a continuación.



Pasos

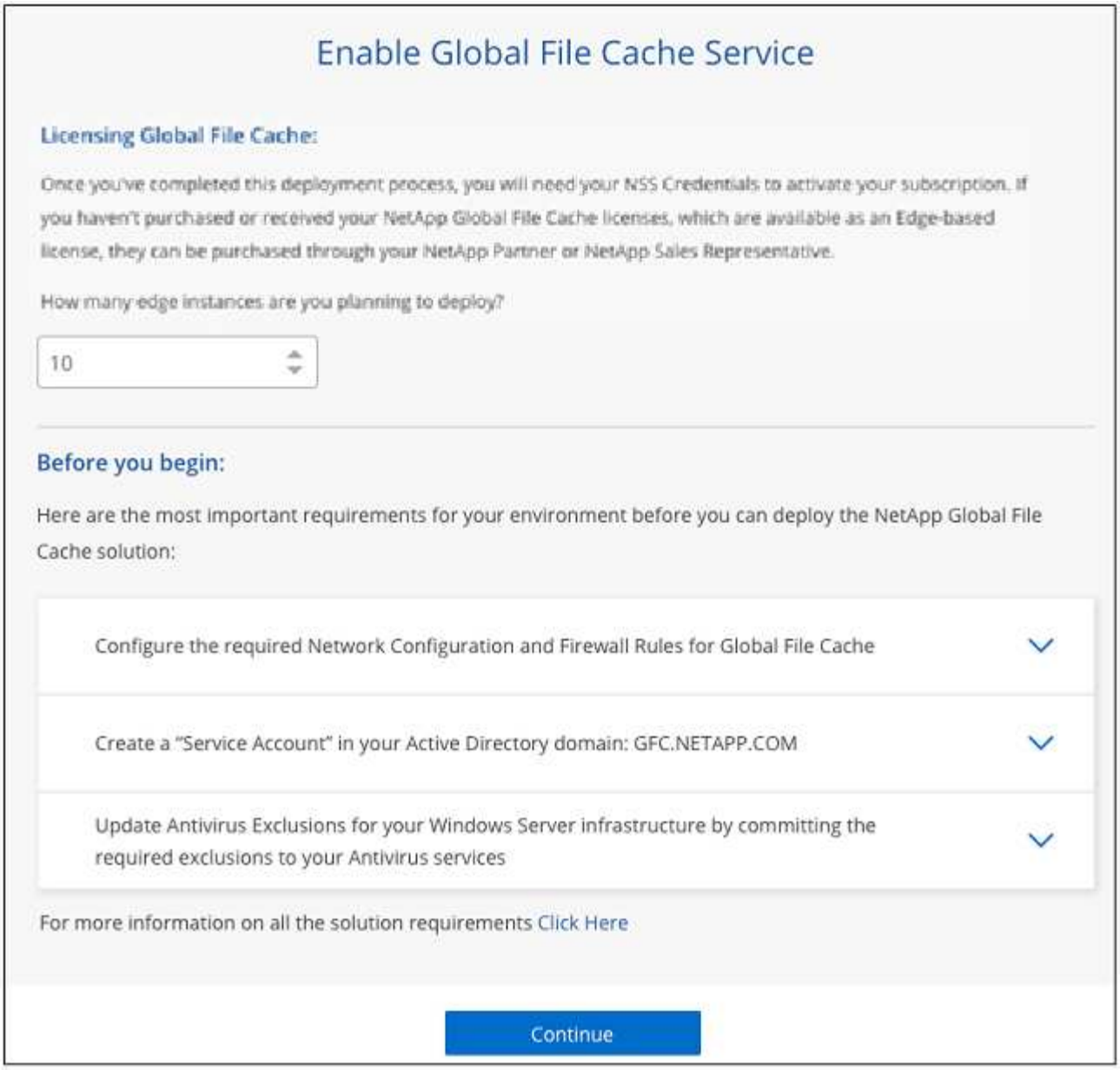
1. Seleccione el entorno de trabajo en el que ha implementado Cloud Volumes ONTAP.
2. En el panel Servicios, haga clic en **Activar GFC**.

3. Lea la página Descripción general y haga clic en **continuar**.

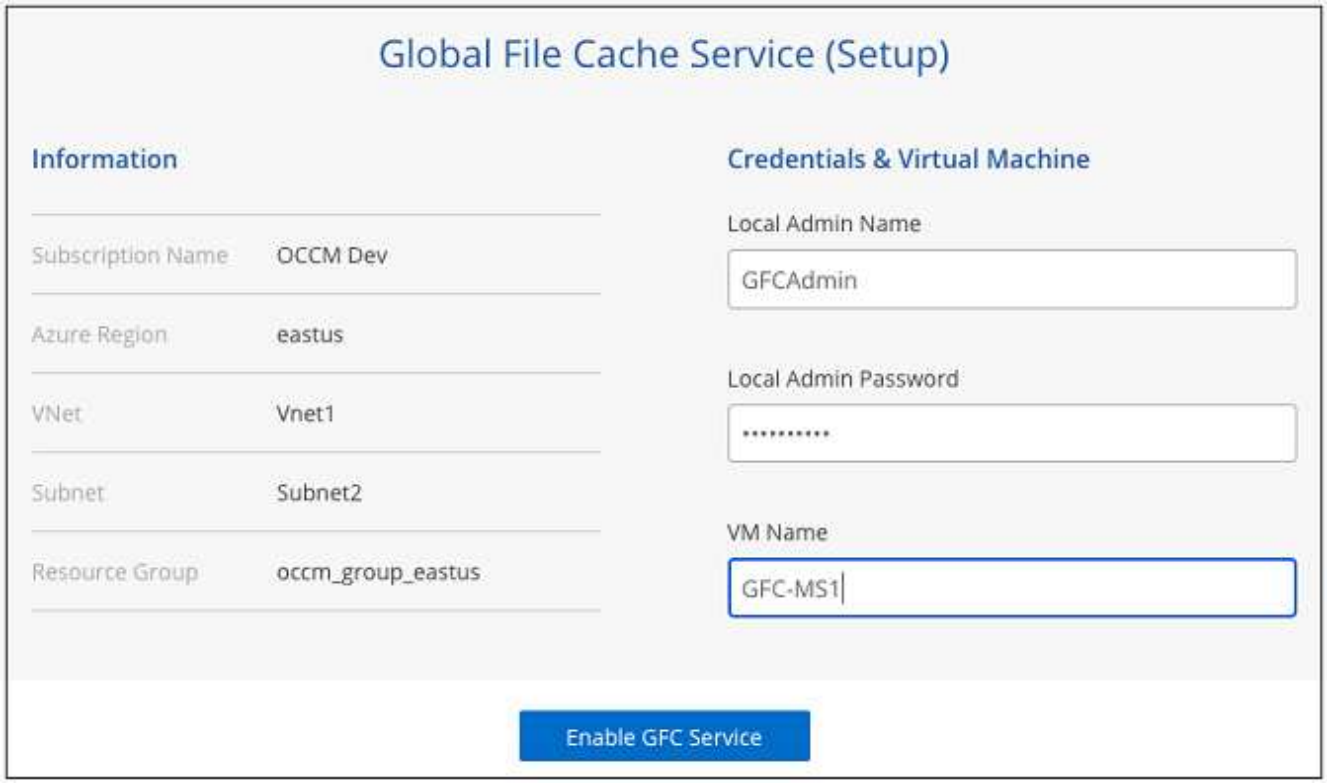
4. Si no hay recursos compartidos de SMB disponibles en la instancia de Cloud Volumes ONTAP, se le pedirá que introduzca los detalles de SMB Server y SMB Share para crear el recurso compartido ahora. Para obtener más detalles sobre la configuración SMB, consulte "Plataforma de almacenamiento dinámica".

   Cuando termine, haga clic en **continuar** para crear el recurso compartido SMB.

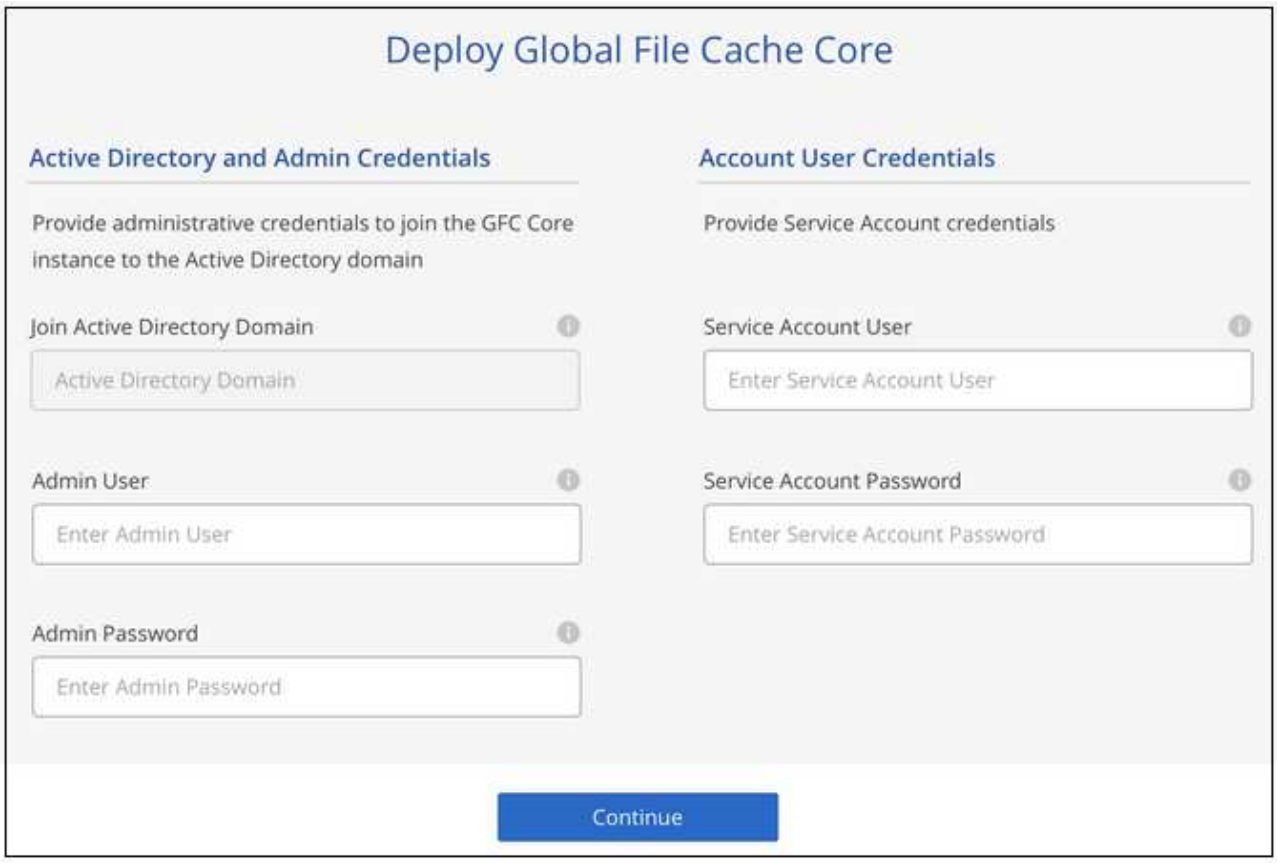
5. En la página Global File Cache Service, introduzca el número de instancias de Global File Cache Edge que tiene previsto implementar y, a continuación, asegúrese de que el sistema cumple los requisitos de las reglas de configuración de red y firewall, la configuración de Active Directory y las exclusiones de antivirus. Consulte "Requisitos previos" para obtener más detalles.



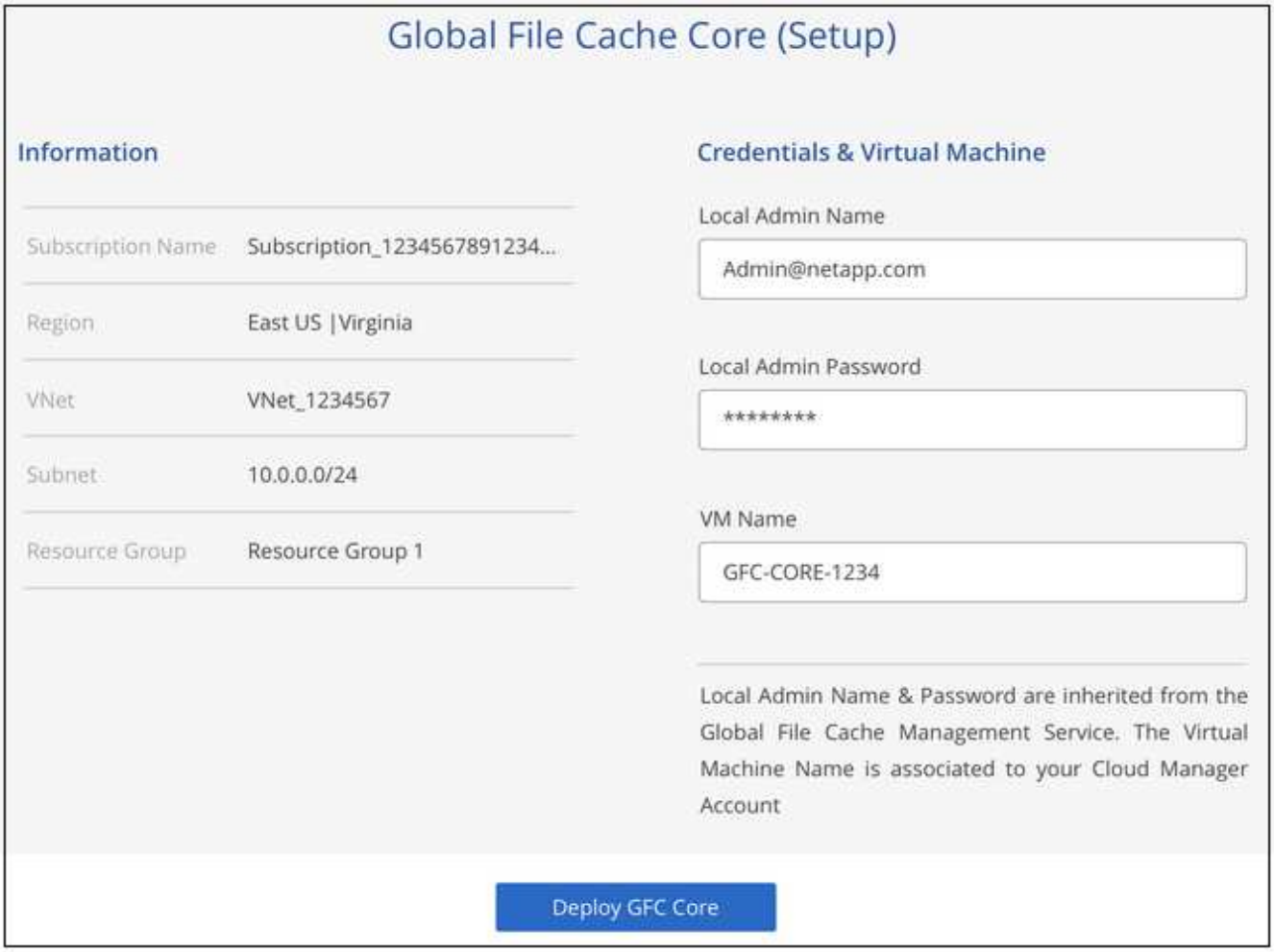
6. Después de verificar que se han cumplido los requisitos o que tiene la información necesaria para cumplir estos requisitos, haga clic en **continuar**.
7. Introduzca las credenciales de administrador que utilizará para acceder a la VM del servidor de gestión de caché de archivos global y haga clic en **Activar GFC Service**. Para Azure, debe introducir las credenciales como nombre de usuario y contraseña; para AWS, seleccione la pareja de claves adecuada. Es posible cambiar el nombre de la máquina virtual/instancia si se desea.



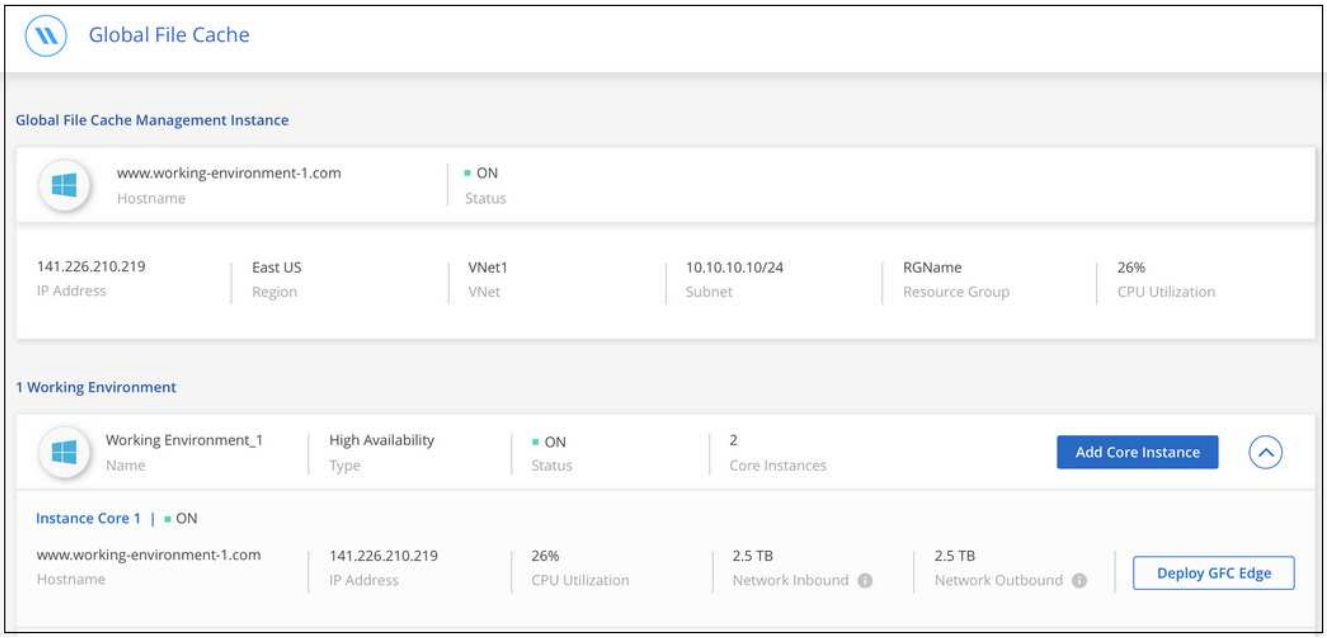
8. Después de implementar correctamente el servicio de administración de caché de archivos global, haga clic en **continuar**.
9. Para Global File Cache Core, introduzca las credenciales de usuario admin para unirse al dominio de Active Directory y las credenciales de usuario de la cuenta de servicio. A continuación, haga clic en **continuar**.
   - La instancia núcleo de caché de archivos global debe implementarse en el mismo dominio de Active Directory que la instancia de Cloud Volumes ONTAP.
   - La cuenta de servicio es un usuario de dominio y forma parte del grupo BUILTIN\operadores de copia de seguridad de la instancia de Cloud Volumes ONTAP.



10. Introduzca las credenciales de administración que utilizará para acceder a la VM principal de caché de archivos global y haga clic en **implementar GFC Core**. Para Azure, debe introducir las credenciales como nombre de usuario y contraseña; para AWS, seleccione la pareja de claves adecuada. Es posible cambiar el nombre de la máquina virtual/instancia si se desea.



11. Una vez que el núcleo de caché de archivos global se haya implementado correctamente, haga clic en **vaya a Dashboard**.



El Panel muestra que la instancia de Management Server y la instancia de Core son **on** y están funcionando.

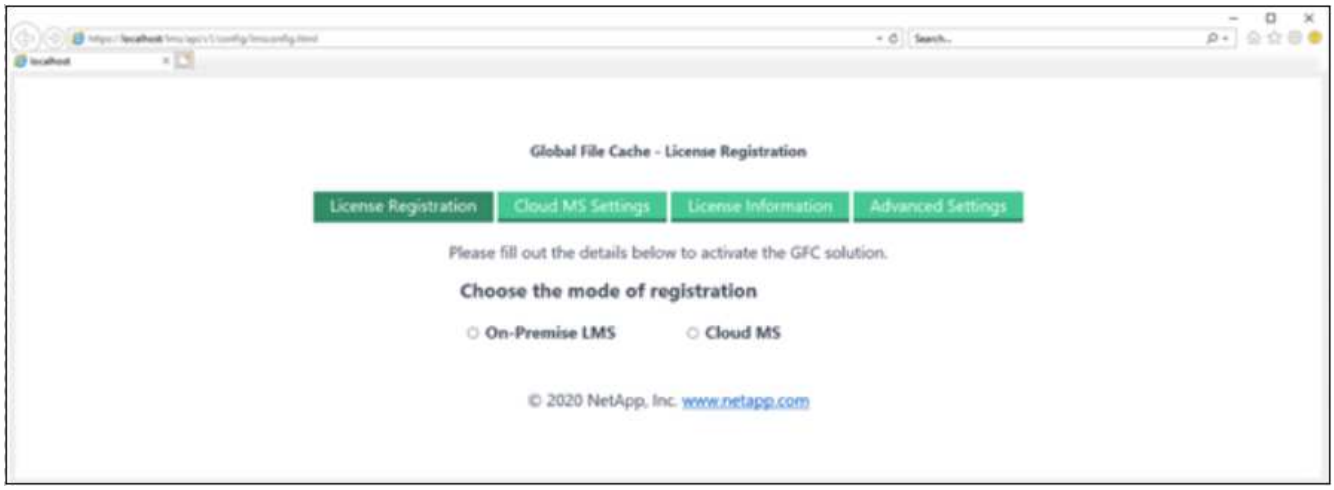
Licencia de la instalación de Global File Cache

Para poder utilizar Global File Cache, debe configurar el servicio Global File Cache License Management Server (LMS) en una instancia de Global File Cache Core. Necesitará sus credenciales de NSS o un ID de cliente proporcionado por NetApp para activar su suscripción.

En este ejemplo, configuraremos el servicio LMS en una instancia Core que acaba de poner en marcha en la nube pública. Este es un proceso único que configura el servicio LMS.

Pasos

1. Abra la página Registro de licencias de la caché global de archivos en el núcleo de la caché global de archivos (el núcleo que está designando como servicio LMS) mediante la siguiente URL. Sustituya *<dirección_ip>* por la dirección IP de Global File Cache Core:https://<ip_address>/lms/api/v1/config/lmsconfig.html[]
2. Haga clic en “continuar a este sitio web (no recomendado)” para continuar. Se muestra una página que permite configurar el LMS o comprobar la información de licencia existente.



3. Elija el modo de registro seleccionando “LMS en las instalaciones” o “Cloud MS”.
   - Se utiliza «LMS in situ» para clientes existentes o de prueba que han recibido un ID de cliente a través del servicio de soporte de NetApp.
   - «Cloud MS» se utiliza para los clientes que han adquirido licencias de NetApp Global File Cache Edge en NetApp o de sus partners certificados y tienen sus credenciales de NetApp.
4. Para Cloud MS, haga clic en **Cloud MS**, introduzca sus credenciales de NSS y haga clic en **Enviar**.

5. Para LMS en las instalaciones, haga clic en **LMS en las instalaciones**, introduzca su ID de cliente y haga clic en **Registrar LMS**.

¿Cuál es el futuro?

Si ha determinado que necesita implementar varios núcleos de caché global de archivos para admitir su configuración, haga clic en **Agregar instancia principal** en el Panel de control y siga el asistente de implementación.

Una vez finalizada la implementación básica, debe hacerlo "Implemente las instancias de Global File Cache Edge" en cada una de sus oficinas remotas.

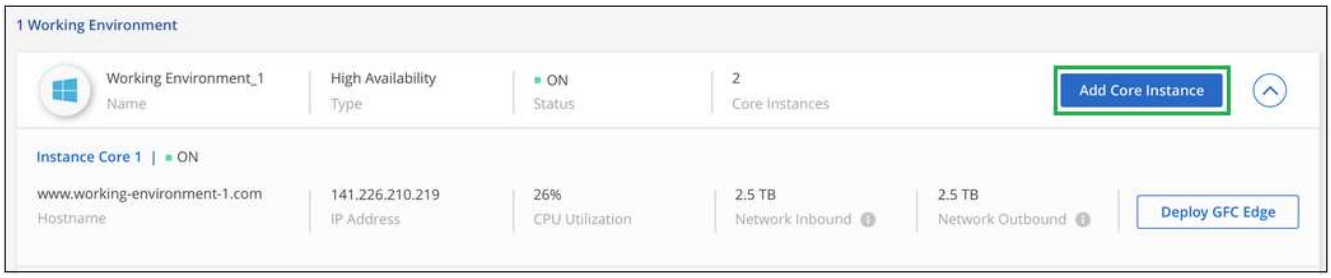
Puesta en marcha de instancias de Core adicionales

Si su configuración requiere que se instale más de un núcleo de caché de archivos global debido a un gran número de instancias de Edge, puede agregar otro núcleo al entorno de trabajo.

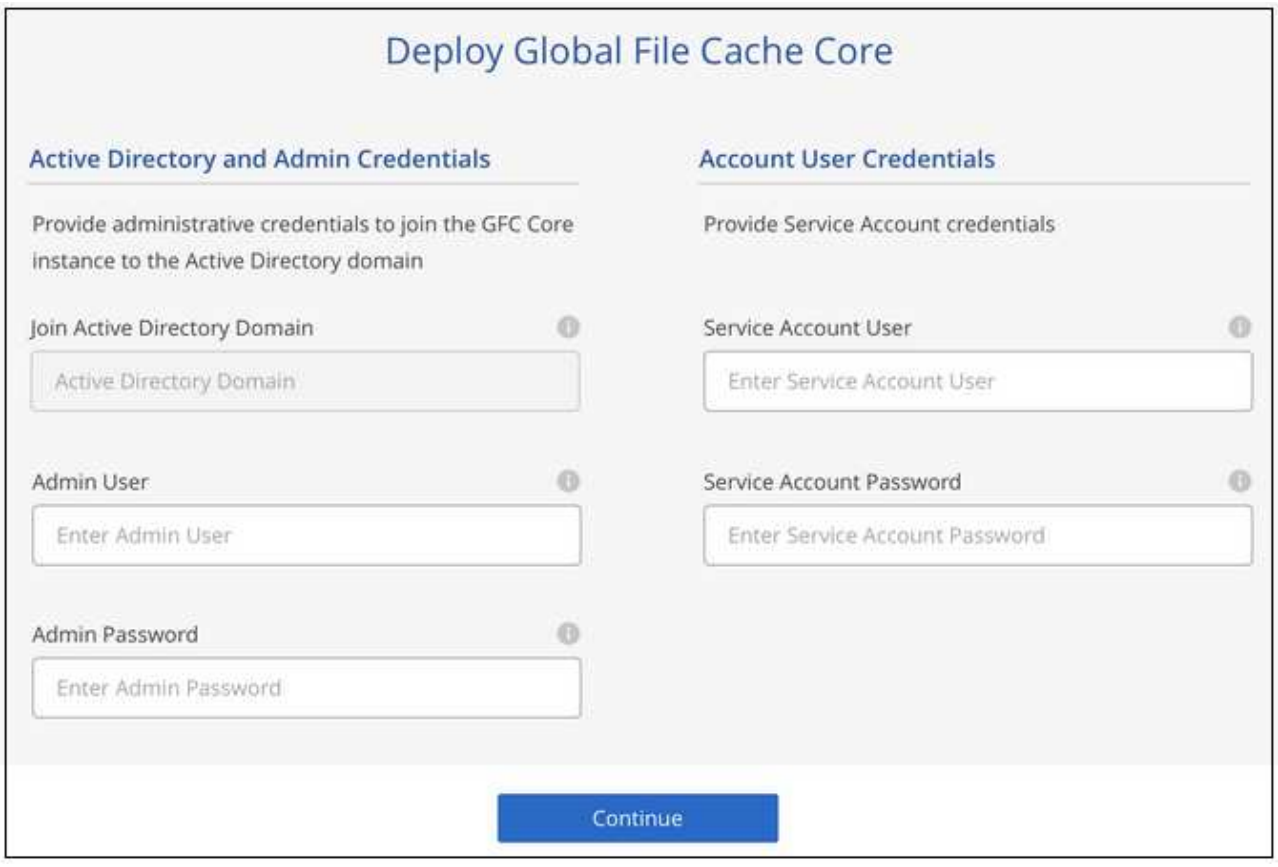
Al implementar instancias de Edge, configurará algunos para que se conecten al primer núcleo y otros al segundo núcleo. Las dos instancias principales acceden al mismo almacenamiento de back-end (su instancia

de Cloud Volumes ONTAP) del entorno de trabajo.

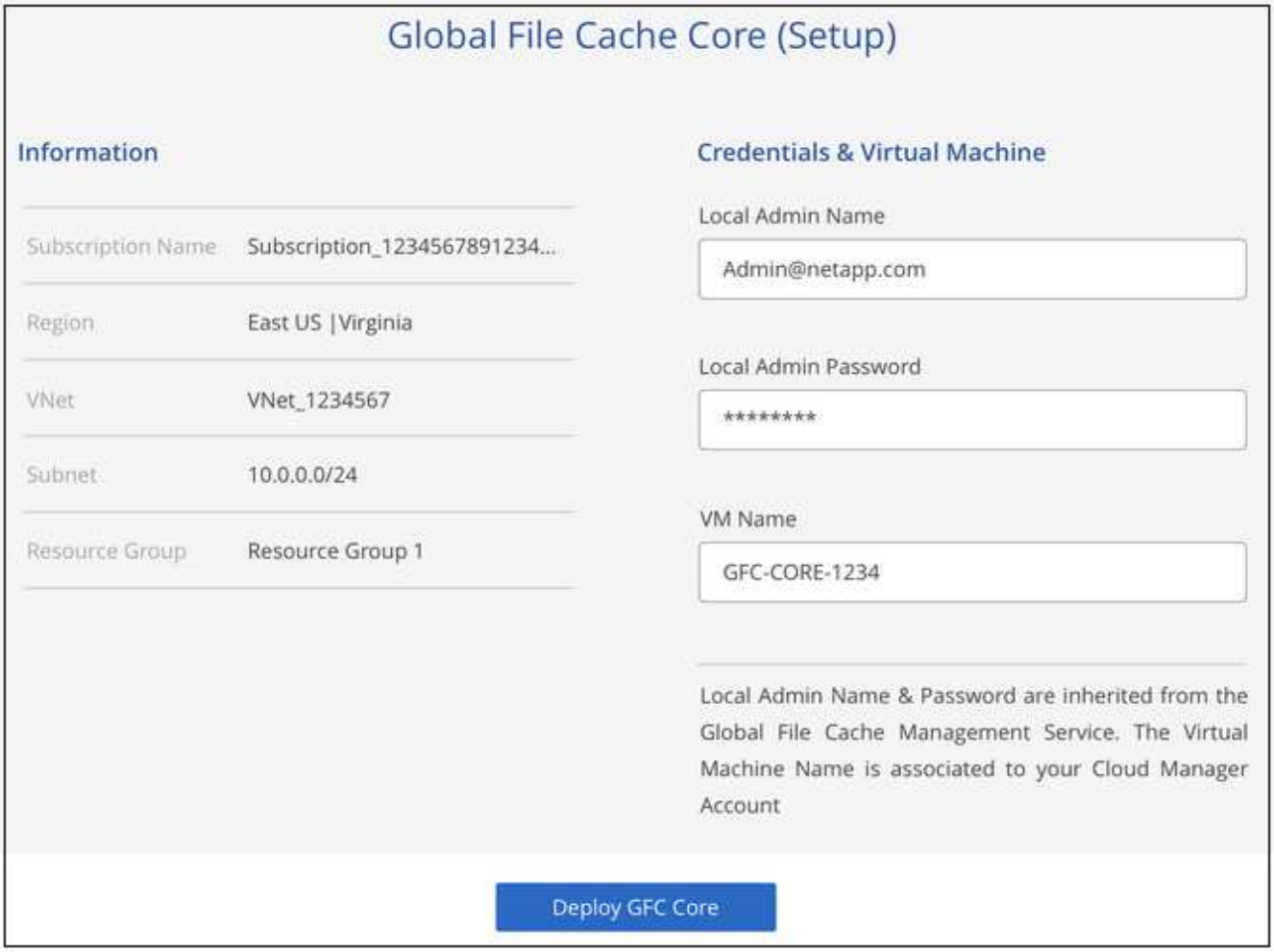
1. En el Panel de caché global de archivos, haga clic en **Agregar instancia principal**.



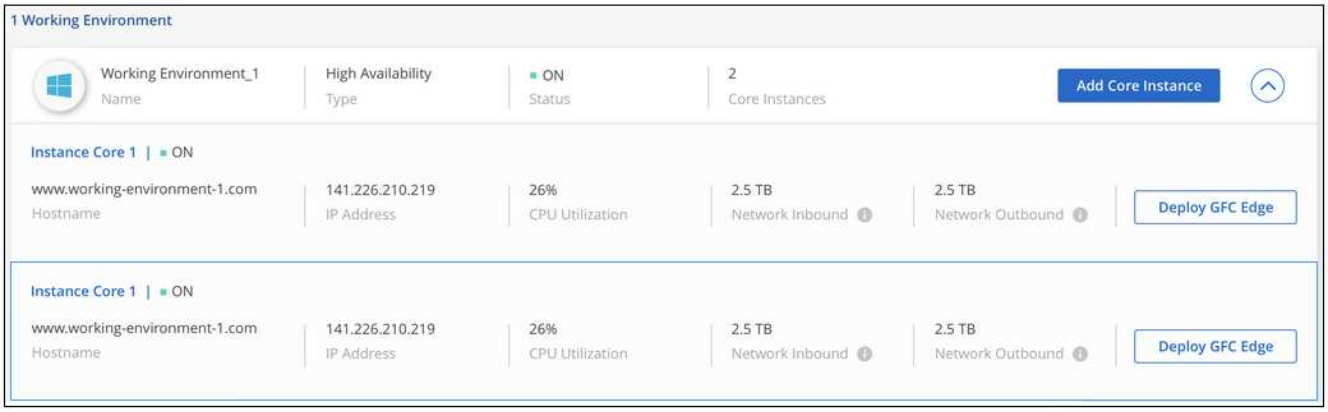
2. Introduzca las credenciales de usuario administrador para unirse al dominio de Active Directory y las credenciales de usuario de la cuenta de servicio. A continuación, haga clic en **continuar**.
   - La instancia núcleo de caché de archivos global debe estar en el mismo dominio de Active Directory que la instancia de Cloud Volumes ONTAP.
   - La cuenta de servicio es un usuario de dominio y forma parte del grupo BUILTIN\operadores de copia de seguridad de la instancia de Cloud Volumes ONTAP.



3. Introduzca las credenciales de administración que utilizará para acceder a la VM principal de caché de archivos global y haga clic en **implementar GFC Core**. Para Azure, debe introducir las credenciales como nombre de usuario y contraseña; para AWS, seleccione la pareja de claves adecuada. Puede cambiar el nombre de la máquina virtual si desea.



4. Una vez que el núcleo de caché de archivos global se haya implementado correctamente, haga clic en **vaya a Dashboard**.



El panel de control refleja la segunda instancia de Core para el entorno de trabajo.

Antes de empezar a implementar instancias de Global File Cache Edge

Hay muchos requisitos que debe tener en cuenta antes de empezar a instalar el software Global File Cache Edge en sus oficinas remotas.

Descargue los recursos necesarios

Descargue las plantillas virtuales de caché global de archivos que tiene previsto utilizar en sus sucursales, el paquete de instalación de software y la documentación de referencia adicional:

- Plantilla virtual de Windows Server 2016:

  "Windows Server 2016 .OVA, incluido GFC de NetApp (VMware vSphere 6.5+)"
  "Windows Server 2016 .VHDX, incluido NetApp GFC (Microsoft Hyper-v)"

- Plantilla virtual de Windows Server 2019:

  "Windows Server 2019 .OVA, incluido GFC de NetApp (VMware vSphere 6.5+)"
  "Windows Server 2019 .VHDX, incluido NetApp GFC (Microsoft Hyper-v)"

- Software Global File Cache Edge:

  "Software GFC de NetApp (.EXE)"

- Documentación de Global File Cache:

  "Guía del usuario de caché global de archivos de NetApp"

Diseño e implementación de Global File Cache Edge

En función de sus requisitos, es posible que deba implementar una o varias instancias de Global File Cache Edge en función de las sesiones de usuario simultáneas en una sucursal. La instancia de Edge presenta el recurso compartido de archivos virtual a los usuarios finales de la sucursal, que se ha ampliado de forma transparente desde la instancia de Global File Cache Core asociada. El borde de caché global de archivos debe contener un `D:\` Volumen NTFS, que contiene los archivos almacenados en caché dentro de la sucursal.

Para Global File Cache Edge, es importante comprender "directrices de tamaño". Esto le ayudará a realizar el diseño correcto para su implementación de la caché global de archivos. También tendría que determinar cuál es el más adecuado para su entorno en términos de escala, disponibilidad de recursos y redundancia.

Instancia de Global File Cache Edge

Al implementar una instancia de Global File Cache Edge, necesita aprovisionar un único equipo virtual mediante la implementación de Windows Server 2016 Standard o Datacenter Edition, Windows Server 2019 Standard o Datacenter Edition, o bien mediante la caché de archivos global `.OVA` o. `.VHD` Plantilla, que incluye el sistema operativo Windows Server elegido y el software Global File Cache.

Pasos rápidos

1. Implemente la plantilla virtual de caché de archivos global, o Windows Server 2016 VM, o Windows Server 2019 Standard o Datacenter Edition.
2. Asegúrese de que la máquina virtual está conectada a la red, unida al dominio y accesible a través de RDP.
3. Instale el software Global File Cache Edge más reciente.
4. Identifique el servidor de gestión de caché de archivos global y la instancia principal.

5. Configure la instancia de Edge de caché de archivos global.

Requisitos de Global File Cache Edge

Global File Cache Edge se ha diseñado para funcionar en todas las plataformas compatibles con Windows Server 2016 y 2019, lo que simplifica LA TECNOLOGÍA a las oficinas remotas corporativas y mucho más. Lo más importante es que Global File Cache se puede poner en marcha en su infraestructura de hardware existente, virtualización o entornos de cloud híbrido/público en casi todos los casos si se cumplen unos pocos requisitos básicos.

Global File Cache Edge requiere que los siguientes recursos de hardware y software funcionen de forma óptima. Para obtener más información acerca de las directrices de tamaño generales, consulte "Directrices de tamaño".

Dispositivo servidor reforzado

El paquete de instalación Global File Cache crea un dispositivo de software reforzado en cualquier instancia de Microsoft Windows Server. *no desinstalar* el paquete de caché global de archivos. La desinstalación de la caché global de archivos afectará a la funcionalidad de la instancia del servidor y podría requerir una reconstrucción completa de la instancia del servidor.

Requisitos físicos de hardware

- 4 núcleos de CPU como mínimo
- 16 GB de RAM como mínimo
- NIC dedicado único o redundante de 1 Gbps
- SSD o HDD SAS de 10 000 rpm (opción preferida)
- Controladora RAID con la funcionalidad de almacenamiento en caché de escritura simultánea habilitada

Requisitos de implementación virtual

Se sabe que las plataformas de hipervisores están sujetas a la degradación del rendimiento desde la perspectiva de un subsistema de almacenamiento (por ejemplo, latencia). Para obtener un rendimiento óptimo con la caché global de archivos, se recomienda una instancia de servidor físico con SSD.

Para obtener el mejor rendimiento en entornos virtuales, además de los requisitos físicos del host, se deben cumplir los siguientes requisitos y reservas de recursos:

Microsoft Hyper-V 2012 R2 y posterior:

- Procesador (CPU): Las CPU deben establecerse como **estático**: Mínimo: 4 núcleos vCPU.
- Memoria (RAM): Mínimo: 16 GB establecido como **estático**.
- Aprovisionamiento de discos duros: Los discos duros deben configurarse como **disco fijo**.

VMware vSphere 6.x y posteriores:

- Procesador (CPU): Se debe establecer la reserva de los ciclos de la CPU. Mínimo: 4 núcleos vCPU a 10000 MHz.
- Memoria (RAM): Mínimo: Reserva de 16 GB.
- Provisionamiento de discos duros:

    - El aprovisionamiento de disco debe definirse como **Thick provisioned eager zeroed**.
    - Los recursos compartidos de disco duro deben configurarse en **Alta**.
    - Devices.hotplug debe configurarse como **False** mediante vSphere Client para evitar que Microsoft Windows presente las unidades de caché de archivos global como extraíbles.
- Conexión en red: La interfaz de red se debe establecer en **VMXNEL3** (requiere herramientas de VM).

El caché global de archivos se ejecuta en Windows Server 2016 y 2019, por lo que la plataforma de virtualización debe admitir el sistema operativo, así como la integración con utilidades que mejoran el rendimiento del sistema operativo invitado de la máquina virtual y la administración de la máquina virtual, como VM Tools.

Requisitos de tamaño de particiones

- C:\ - mínimo 250 GB (volumen de sistema/arranque)
- D:\ - mínimo 1 TB (Volumen de datos independiente para caché de archivos inteligente Global File Cache*)

*el tamaño mínimo es el doble del conjunto de datos activo. El volumen de caché (D:\) puede ampliarse y sólo está restringido por las limitaciones del sistema de archivos NTFS de Microsoft Windows.

Requisitos del disco de caché inteligente de archivos de Global File Cache

La latencia de disco en el disco de caché de archivos inteligente (D:\) de Global File Cache debería ofrecer una latencia de disco de I/o media de < 0,5 ms y un rendimiento de 1 MB por usuario simultáneo.

Para obtener más información, consulte "Guía del usuario de caché global de archivos de NetApp".

Redes

- Firewall: Se deben permitir los puertos TCP entre las instancias de Global File Cache Edge y Management Server y Core.

  Puertos TCP de caché de archivos global: 443 (HTTPS - LMS), 6618 – 6630.

- Los dispositivos de optimización de red (como Riverbed Steelhead) deben configurarse para pasar por los puertos específicos de la caché global de archivos (TCP 6618-6630).

Estación de trabajo cliente y prácticas recomendadas de la aplicación

La caché global de archivos se integra de forma transparente en los entornos del cliente, permitiendo a los usuarios acceder a datos centralizados mediante sus estaciones de trabajo cliente, ejecutando aplicaciones empresariales. Mediante la caché global de archivos, se accede a los datos a través de una asignación directa de unidades o a través de un espacio de nombres DFS. Si quiere más información sobre la estructura de caché global de archivos, el almacenamiento en caché inteligente de archivos y aspectos clave del software, consulte la "Antes de comenzar a implementar la caché de archivos global" sección.

Para garantizar una experiencia y un rendimiento óptimos, es importante cumplir con los requisitos y las prácticas recomendadas del cliente de Microsoft Windows, tal y como se describe en la Guía del usuario de la caché global de archivos. Esto se aplica a todas las versiones de Microsoft Windows.

Para obtener más información, consulte "Guía del usuario de caché global de archivos de NetApp".

Mejores prácticas de firewall y antivirus

Aunque Global File Cache hace un esfuerzo razonable para validar que los paquetes de aplicaciones antivirus más comunes son compatibles con Global File Cache, NetApp no puede garantizar y no es responsable de ninguna incompatibilidad o problemas de rendimiento causados por estos programas, ni de sus actualizaciones, paquetes de servicio ni modificaciones asociados.

La caché global de archivos no recomienda la instalación ni la aplicación de soluciones de supervisión o antivirus en ninguna instancia habilitada de Global File Cache (Core o Edge). Si la solución se instalara, por elección o por política, deberán aplicarse las siguientes prácticas recomendadas y recomendaciones. Si desea conocer los paquetes antivirus habituales, consulte el Apéndice A de la "Guía del usuario de caché global de archivos de NetApp".

Configuración del firewall

- Firewall de Microsoft:
  - Conserve la configuración del firewall de forma predeterminada.
  - Recomendación: Deje LA configuración y los servicios del firewall de Microsoft EN LA configuración predeterminada DE OFF y no se inicie para las instancias estándar de Global File Cache Edge.
  - Recomendación: Deje LA configuración y los servicios del firewall de Microsoft en LA configuración predeterminada DE ACTIVADO y comience para las instancias de Edge que también ejecuten la función controlador de dominio.
- Firewall de la empresa:
  - La instancia de Global File Cache Core escucha en los puertos TCP 6618-6630, asegúrese de que las instancias de Global File Cache Edge se pueden conectar a estos puertos TCP.
  - Las instancias de caché de archivos global requieren comunicaciones con el servidor de administración de caché de archivos global en el puerto TCP 443 (HTTPS).
- Las soluciones/dispositivos de optimización de red deben configurarse para pasar por los puertos específicos de la caché global de archivos.

Mejores prácticas de antivirus

Esta sección le ayuda a comprender los requisitos cuando ejecuta software antivirus en una instancia de Windows Server que ejecuta la caché de archivos global. Global File Cache ha probado los productos antivirus más utilizados, como Cylance, McAfee, Symantec, Sophos, Trend Micro, Kaspersky y Windows Defender, para su uso en combinación con Global File Cache.

> Añadir antivirus a un dispositivo Edge puede tener un impacto del 10 al 20% en el rendimiento del usuario.

Para obtener más información, consulte "Guía del usuario de caché global de archivos de NetApp".

Configurar exclusiones

El software antivirus u otras utilidades de indexación o análisis de terceros nunca deben analizar la unidad D:\ en la instancia de Edge. Estos análisis de la unidad de servidor Edge D:\ darán como resultado numerosas solicitudes de apertura de archivos para todo el espacio de nombres de caché. Esto provocará que se optimicen en el centro de datos las búsquedas de archivos en la WAN de todos los servidores de archivos. Se producirán inundaciones en la conexión WAN y cargas innecesarias en la instancia de Edge, lo que provocaría una degradación del rendimiento.

Además de la unidad D:\, generalmente se deben excluir de todas las aplicaciones antivirus los siguientes directorios y procesos de la caché global de archivos:

- `C:\Program Files\TalonFAST\`
- `C:\Program Files\TalonFAST\Bin\LMClientService.exe`
- `C:\Program Files\TalonFAST\Bin\LMServerService.exe`
- `C:\Program Files\TalonFAST\Bin\Optimus.exe`
- `C:\Program Files\TalonFAST\Bin\tafsexport.exe`
- `C:\Program Files\TalonFAST\Bin\tafsutils.exe`
- `C:\Program Files\TalonFAST\Bin\tapp.exe`
- `C:\Program Files\TalonFAST\Bin\tfs.exe`
- `C:\Program Files\TalonFAST\Bin\TService.exe`
- `C:\Program Files\TalonFAST\Bin\tum.exe`
- `C:\Program Files\TalonFAST\FastDebugLogs\`
- `C:\Windows\System32\drivers\tfast.sys`
- `\\?\TafsMtPt:\ or \\?\TafsMtPt*`
- `\Device\TalonCacheFS\`
- `\\?\GLOBALROOT\Device\TalonCacheFS\`
- `\\?\GLOBALROOT\Device\TalonCacheFS\*`

Política de soporte de NetApp

Las instancias de caché de archivos global se han diseñado específicamente para la caché de archivos global como aplicación principal que se ejecuta en una plataforma Windows Server 2016 y 2019. La caché global de archivos requiere acceso prioritario a los recursos de la plataforma, por ejemplo, disco, memoria, interfaces de red y puede suponer una gran demanda de estos recursos. Las puestas en marcha virtuales requieren reservas de memoria/CPU y discos de alto rendimiento.

- Para las implementaciones de sucursales de Global File Cache, los servicios y aplicaciones compatibles en el servidor que ejecuta Global File Cache están limitados a:
  - DNS/DHCP
  - Controlador de dominio de Active Directory (La caché de archivos global debe estar en un volumen independiente)
  - Servicios de impresión
  - System Center Configuration Manager (SCCM) de Microsoft
  - Agentes del sistema de cliente aprobados por Global File Cache y aplicaciones antivirus
- El soporte y el mantenimiento de NetApp se aplican solo a la caché de archivos global.
- No se admite el software de productividad de la línea de negocio, que suele requerir muchos recursos, por ejemplo, servidores de bases de datos, servidores de correo, etc.
- El cliente es responsable de cualquier software no Global File Cache que pueda instalarse en el servidor que ejecute Global File Cache:

    - Si un paquete de software de terceros provoca conflictos de software o recursos con la caché global de archivos o el rendimiento se ve comprometido, la organización de asistencia de Global File Cache podría requerir al cliente que desactive o elimine el software del servidor que ejecuta la caché global de archivos.
    - Es responsabilidad del cliente por toda la instalación, integración, asistencia técnica y actualización de cualquier software agregado al servidor que ejecute la aplicación Global File Cache.
- Las utilidades/agentes de administración de sistemas, como las herramientas antivirus y los agentes de licencia, pueden coexistir. Sin embargo, excepto en el caso de los servicios y aplicaciones compatibles que se enumeran anteriormente, estas aplicaciones no son compatibles con la caché global de archivos y deben seguir las mismas directrices que se han indicado anteriormente:
    - Es responsabilidad del cliente por toda la instalación, integración, asistencia técnica y actualización de cualquier software agregado.
    - Si un cliente instala un paquete de software de terceros que cause o sospecha que esté causando conflictos de software o recursos con la caché global de archivos o el rendimiento se ve comprometido, puede que la organización de soporte de Global File Cache tenga que desactivar o eliminar el software.

Ponga en marcha instancias globales de File Cache Edge

Una vez que haya comprobado que su entorno cumple con todos los requisitos, instale el software Global File Cache Edge en cada oficina remota.

Antes de empezar

Para completar las tareas de configuración de Global File Cache Edge, necesita la siguiente información:

- Direcciones IP estáticas para cada instancia de Global File Cache
- Máscara de subred
- Dirección IP de la pasarela
- El FQDN que desea asignar a cada archivo global Servidor de caché
- El sufijo DNS (opcional)
- Nombre de usuario y contraseña de un usuario administrativo en el dominio
- La dirección FQDN y/o IP de los servidores principales asociados
- Un volumen que se usará como caché de archivos inteligente. Se recomienda que tenga al menos el doble de tamaño que el conjunto de datos activo. Debe tener formato NTFS y asignarse como `D:\`.

Puertos TCP utilizados habitualmente

Los servicios de caché global de archivos utilizan varios puertos TCP. Es obligatorio que los dispositivos se puedan comunicar en estos puertos y se excluyan de cualquier dispositivo de optimización WAN o directivas de restricción de firewall:

- Puerto TCP de licencias de caché de archivos global: 443
- Puertos TCP de caché de archivos global: 6618-6630

Despliegue la plantilla virtual de caché global de archivos

La plantilla virtual `.OVA` y.. `.VHD`) Las imágenes contienen la última versión del software Global File Cache. Si va a implementar la caché global de archivos mediante `.OVA` o. `.VHD` Plantilla de máquina virtual (VM), siga los pasos descritos en esta sección. Se asume que comprende cómo implementar el `.OVA` o. `.VHD` plantilla en la plataforma de hipervisor designada.

Asegúrese de que las preferencias de los equipos virtuales, incluidas las reservas de recursos, se ajustan a los requisitos de la forma descrita en la "Requisitos de implementación virtual".

Pasos

1. Extraiga el paquete de la plantilla que ha descargado.
2. Despliegue la plantilla virtual. Consulte los siguientes vídeos antes de iniciar la implementación:
   - "Poner en funcionamiento la plantilla virtual en VMware"
   - "Puesta en marcha de la plantilla virtual en Hyper-V"
3. Después de implementar la plantilla virtual y de configurar la configuración del equipo virtual, inicie la máquina virtual.
4. Durante el inicio inicial, cuando el sistema operativo Windows Server 2016 ó 2019 se esté preparando para su primer uso, complete la experiencia inmediata instalando los controladores correctos e instalando los componentes necesarios para el hardware correspondiente.
5. Una vez completada la instalación básica de la instancia de Global File Cache Edge, el sistema operativo Windows Server 2016 ó 2019 le guiará a través de un asistente de configuración inicial para configurar los detalles del sistema operativo, como la localización y la clave del producto.
6. Una vez completado el asistente de configuración inicial, inicie sesión localmente en el sistema operativo Windows Server 2016 o 2019 con las siguientes credenciales:
   - Nombre de usuario: **FASTAdmin**
   - Contraseña: **Tal0nFAST!**
7. Configure el equipo virtual de Windows Server, únase al dominio de Active Directory de la organización y continúe con la sección de configuración de borde de caché de archivos global.

Configure la instancia de Edge de caché de archivos global

La instancia de Global File Cache Edge se conecta a un núcleo de caché de archivos global para proporcionar a los usuarios de la sucursal acceso a los recursos del servidor de archivos del centro de datos.

> La instancia de Edge debe tener una licencia como parte de la puesta en marcha de Cloud Volumes ONTAP antes de iniciar la configuración. Consulte "Licencia" para obtener más información acerca de las licencias.

Si su configuración requiere que se instale más de un núcleo de caché de archivos global debido a un gran número de instancias de Edge, configurará algunas instancias de Edge para conectarse al primer núcleo y otras instancias para conectarse al segundo Core. Asegúrese de que tiene el FQDN o la dirección IP y otra información necesaria para la instancia de Core correcta.

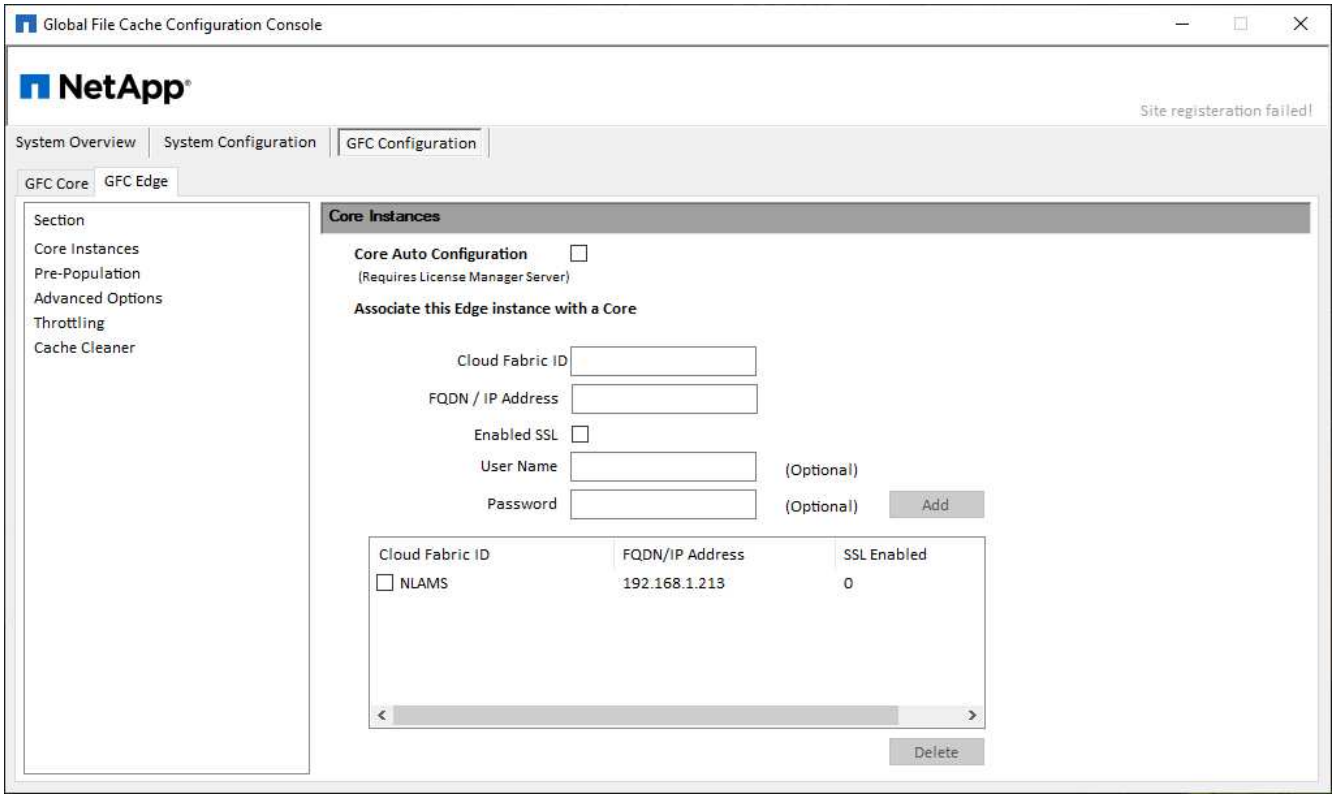
Para configurar la instancia de Edge, lleve a cabo los siguientes pasos:

Pasos

1. Haga clic en **ejecutar** junto al paso no seleccionado Configuración de núcleo que aparece en la sección "pasos de configuración de borde" del asistente de configuración inicial. Esto abre una nueva pestaña,

GFC Edge, y muestra la sección *Core Instances*.

2. Proporcione el **ID de Cloud Fabric** del servidor principal de caché de archivos global. El ID de Cloud Fabric suele ser el nombre NetBIOS o la ubicación geográfica del servidor de archivos back-end.
3. Proporcione **FQDN/dirección IP** del servidor principal de caché de archivos global:
   a. (Opcional) Active la casilla **SSL** para activar la compatibilidad SSL con cifrado mejorado desde Edge hasta Core.
   b. Introduzca el nombre de usuario y la contraseña, que son las credenciales de la cuenta de servicio utilizada en el núcleo.
4. Haga clic en **Agregar** para confirmar la adición del dispositivo Global File Cache Core. Aparecerá un cuadro de confirmación. Haga clic en **Aceptar** para descartarlo.



Actualice el software Global File Cache Edge

Con frecuencia, Global File Cache actualiza el software, ya sea con parches, mejoras o nuevas funciones/funcionalidades. Aunque la plantilla virtual (`.OVA` y.. `.VHD`) Las imágenes contienen la versión más reciente del software Global File Cache; es posible que haya una versión más reciente disponible en el portal de descarga de soporte de NetApp.

Asegúrese de que las instancias de Global File Cache estén actualizadas con la última versión.

> Este paquete de software también se puede utilizar para instalaciones prístinas en Microsoft Windows Server 2016 Standard o Datacenter Edition, Windows Server 2019 Standard o Datacenter Edition, o bien como parte de su estrategia de actualización.

A continuación encontrará los pasos necesarios para actualizar el paquete de instalación de caché de archivos global:

Pasos

1. Después de guardar el paquete de instalación más reciente en la instancia de Windows Server deseada, haga doble clic en él para ejecutar el ejecutable de instalación.
2. Haga clic en **Siguiente** para continuar con el proceso.
3. Haga clic en **Siguiente** para continuar.
4. Acepte el Contrato de licencia y haga clic en **Siguiente**.
5. Seleccione la ubicación de destino de instalación que desee.

   NetApp recomienda utilizar la ubicación de la instalación predeterminada.

6. Haga clic en **Siguiente** para continuar.
7. Seleccione la carpeta del menú Inicio.
8. Haga clic en **Siguiente** para continuar.
9. Verifique los parámetros de instalación deseados y haga clic en **instalar** para comenzar la instalación.

   Se ejecutará el proceso de instalación.

10. Una vez finalizada la instalación, reinicie el servidor cuando se le solicite.

El futuro

Para obtener más información acerca de la configuración avanzada de Global File Cache Edge, consulte "Guía del usuario de caché global de archivos de NetApp".

Formación para el usuario final

Usted querrá formar a sus usuarios en las prácticas recomendadas para acceder a los archivos compartidos a través de la caché global de archivos.

Esta es la fase final de la implementación de la caché global de archivos, la fase de implementación del usuario final.

Para preparar y agilizar el proceso de integración del usuario final, utilice la siguiente plantilla de correo electrónico que le ayudará a informar a los usuarios finales sobre lo que significa trabajar en un entorno de "datos centrales". Esto ayudará a sus usuarios a aprovechar todas las ventajas de la solución Global File Cache. También hemos publicado un vídeo que se puede compartir con los usuarios "de formación" cuando sea necesario.

Personalice y reenvíe los siguientes recursos a los usuarios finales para prepararlos para la implementación:

- Vídeo de formación de usuarios"Vídeo de formación para usuarios finales"
- Plantilla de correo electrónico"Plantilla de correo electrónico para Mac (.emltpl)"

  "Plantilla de correo electrónico de Windows (.msg)"

- Comunicaciones de incorporación"Documento de Word (.docx)"

Consulte el capítulo 12 de la "Guía del usuario de caché global de archivos de NetApp" para material adicional.

Información adicional

Utilice los siguientes enlaces para obtener más información acerca de Global File Cache y otros productos de NetApp:

- Preguntas más frecuentes sobre la caché global de archivos
  - Vea una lista de preguntas y respuestas más frecuentes "aquí"
- "Guía del usuario de caché global de archivos de NetApp"
- Documentación de productos de NetApp
  - Consulte documentación adicional para los productos cloud de NetApp "aquí"
  - Consulte la documentación adicional para todos los productos de NetApp "aquí"
- El soporte al cliente para usuarios de la caché global de archivos con Cloud Volumes ONTAP está disponible a través de los siguientes canales:
  - Proceso guiado de resolución de problemas, gestión de casos, base de conocimientos, descargas, herramientas y mucho más, vaya "aquí"
  - Inicie sesión en el soporte de NetApp en https://mysupport.netapp.com Con sus credenciales de NSS
  - Para obtener asistencia inmediata para un problema P1, llame al +1 856.481.3990 (opción 2)
- El soporte al cliente para usuarios de caché global de archivos que utilizan Cloud Volumes Services y Azure NetApp Files está disponible a través de un soporte estándar de su proveedor. Póngase en contacto con el Servicio de atención al cliente de Google o con el Servicio de atención al cliente de Microsoft,

Optimice los costes de cloud computing

Obtenga más información sobre el servicio de computación

Aprovechando "Servicio spot's Cloud Analyzer", Cloud Manager puede proporcionar un análisis de costes de alto nivel de su gasto en informática en la nube e identificar ahorros potenciales.

Cloud Analyzer es una solución de gestión de infraestructura de cloud que utiliza análisis avanzados para ofrecer visibilidad e información acerca de los costes del cloud. Le muestra dónde puede optimizar esos costos y le permite implementar esa optimización con la cartera de productos de optimización continua de Spot en tan solo unos clics.

Funciones

- Un análisis de costes que muestra el coste actual del mes, los costes mensuales proyectados y los ahorros perdidos
- Vista de la eficiencia del gasto por cuenta, incluido el ahorro adicional estimado
- Un enlace a Spot's Cloud Analyzer para obtener más detalles sobre el gasto en todas las cuentas

Proveedores de cloud compatibles

Este servicio es compatible con AWS.

Coste

Sin coste para usar este servicio a través de Cloud Manager.

Funcionamiento de Cloud Analyzer con Cloud Manager

En un nivel superior, la integración de Cloud Analyzer con Cloud Manager funciona como el siguiente:

1. Haga clic en **calcular** y conecte su cuenta de pagador principal de AWS.
2. NetApp configura su entorno de la siguiente manera:
   a. Crea una organización en la plataforma Spot.
   b. Envía un correo electrónico de bienvenida a Spot.

      Puede iniciar sesión en el servicio Spot con las mismas credenciales de inicio de sesión único que utiliza con Cloud Central y Cloud Manager.

   c. Cloud Analyzer comienza a procesar los datos de sus cuentas de AWS.
3. En Cloud Manager, la página Compute se actualiza y utiliza la información para obtener información sobre los costes del cloud pasado, actual y futuro.
4. Haga clic en **obtener análisis completo** en cualquier momento para ir a Spot's Cloud Analyzer, que ofrece un análisis completo de su gasto en nube y oportunidades de ahorro.

Seguridad de datos

Los datos de Cloud Analyzer están cifrados en reposo y no se almacenan credenciales para ninguna cuenta.

Empiece a optimizar sus costes de cloud computing

Conecte su cuenta de AWS y, a continuación, vea el análisis para empezar a optimizar sus costes de tecnología cloud.

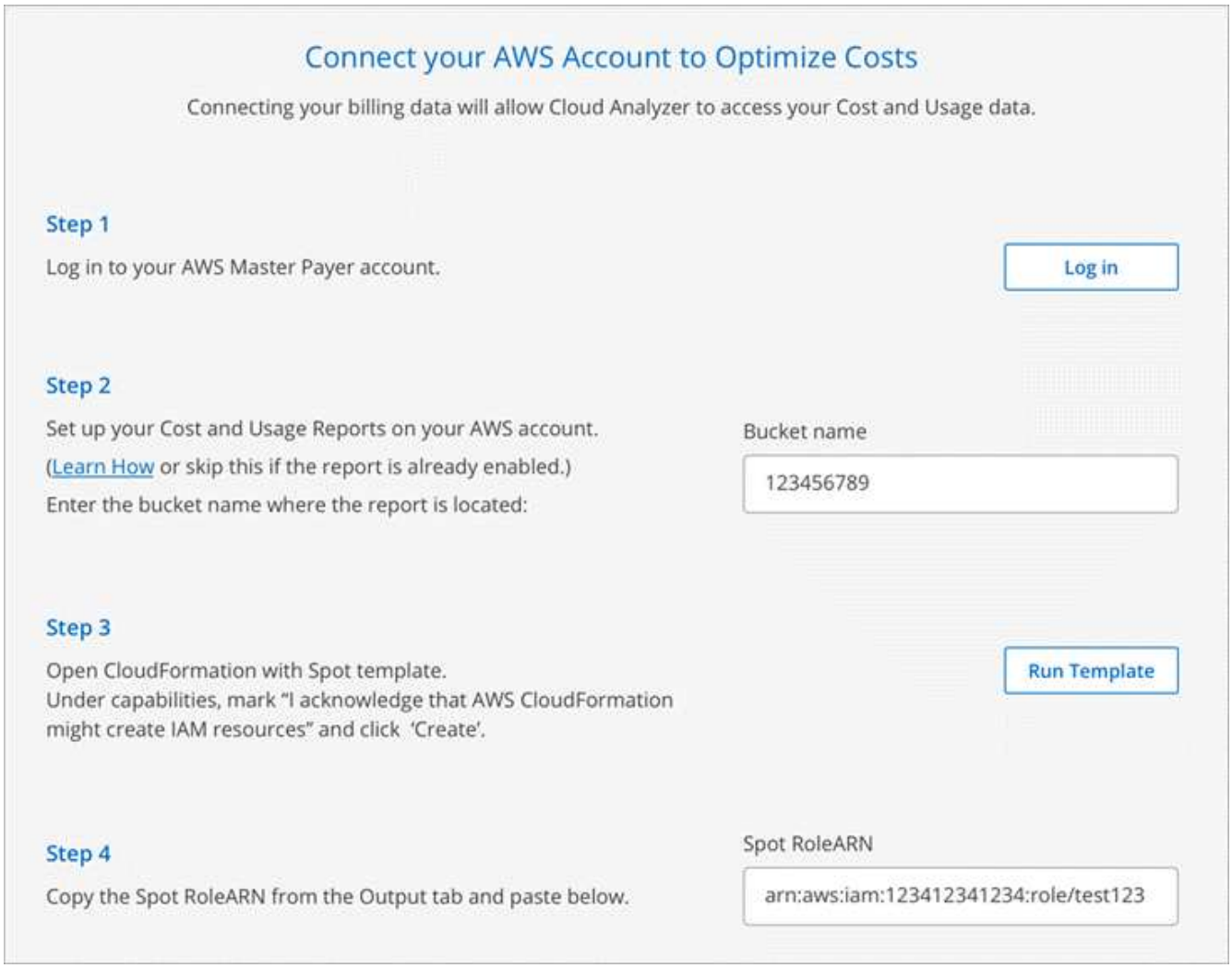
Conecte Cloud Analyzer a su cuenta de AWS

Haga clic en **calcular** y conecte su cuenta de pagador de AWS.

Pasos

1. Haga clic en **calcular**.
2. Haga clic en **Agregar credenciales de AWS a Inicio**.
3. Siga los pasos que aparecen en la página para conectar su cuenta de AWS:
    a. Inicie sesión en su cuenta de pagador maestro de AWS.
    b. Configure informes de costes y uso en la cuenta de AWS.
    c. Ejecute la plantilla CloudFormation.
    d. Pegue el RoleARN del punto.

    "Vea más detalles sobre estos pasos".

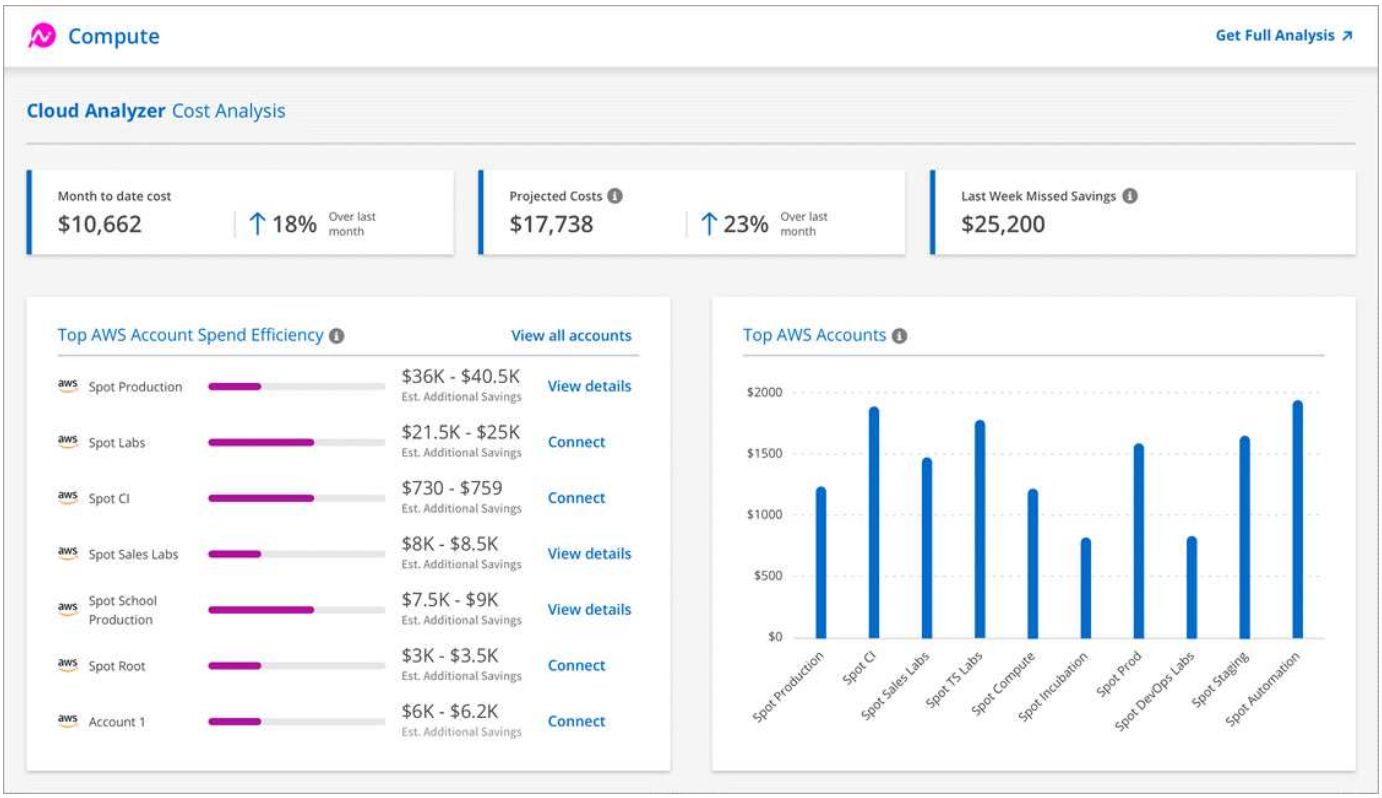


Resultado

Cloud Analyzer comienza a procesar los datos de sus cuentas de AWS. Si tiene varias cuentas, Cloud Analyzer comienza con capacidades de sólo lectura para todas las cuentas vinculadas de la cuenta de pagador principal. Si desea obtener más información sobre el ahorro potencial de esas cuentas, tendrá que conectarlos también. Puede encontrar más información sobre ese proceso en la sección siguiente.

Analice sus costes informáticos

Después de que Cloud Analyzer procese sus datos de cuenta, la pestaña Compute muestra información sobre los costes del cloud pasados, actuales y futuros.



Coste del mes hasta la fecha

El coste total de las cargas de trabajo desde el principio del mes actual hasta la actualidad.

Costos proyectados

El coste previsto al final del mes basado en el análisis de su patrón de uso.

Ahorros que faltó la semana pasada

Ahorros que podrían haberse logrado en los siete días anteriores gracias a la optimización de instancias puntuales y reservas.

Principales niveles de eficiencia del gasto en cuentas de AWS

Las 10 cuentas principales según la mayor cantidad de ahorro adicional estimado.

A cada cuenta se le asigna una puntuación de eficiencia en función del ahorro potencial actual y adicional. El ahorro adicional estimado indica cuánto se puede ahorrar aún más aprovechando el uso de instancias puntuales y reservadas.

Puede realizar las siguientes acciones para optimizar aún más sus cuentas:

- **Ver detalles**: Vea sus oportunidades de optimización de costos en Spot's Cloud Analyzer.
- **Connect**: Conecte una cuenta que aún no se haya administrado. Se le dirigirá al asistente que conecta la cuenta.

Principales cuentas de AWS

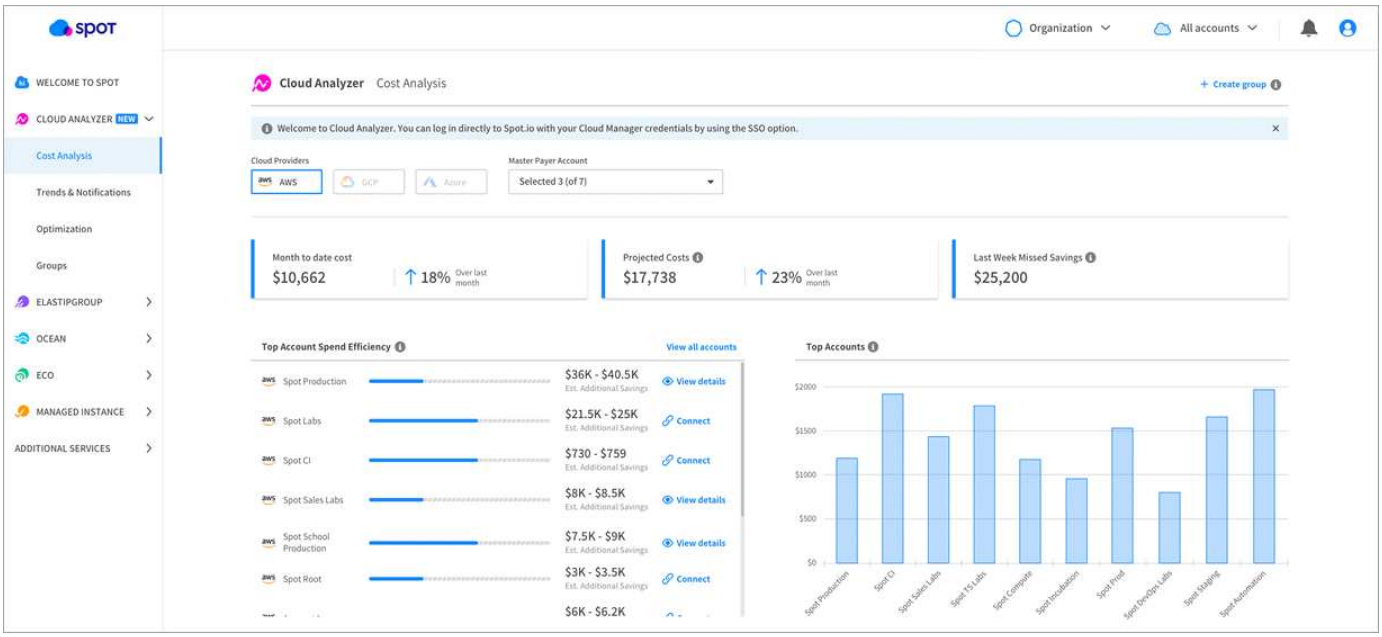
Este es un gráfico de barras que muestra sus diez cuentas principales por coste. El gráfico se basa en los últimos 30 días de actividad de gasto.

"Obtenga más información acerca de la página Análisis de costes disponible en Spot's Cloud Analyzer".

Visite Cloud Analyzer para obtener más análisis y recomendaciones

Haga clic en **obtener análisis completo** en cualquier momento para acceder a más gráficos y análisis, recomendaciones en profundidad, un desglose de optimización de casos de uso (contenedores, aplicaciones elástica y reservas) y mucho más.

He aquí un ejemplo de lo que verá en Cloud Analyzer:



- "Vea la página de Cloud Analyzer para obtener más información acerca de sus funcionalidades".
- "Consulte la documentación de Spot para obtener ayuda sobre el uso de Cloud Analizador".

Organice los datos en niveles en el cloud

Más información acerca de Cloud Tiering

El servicio Cloud Tiering de NetApp amplía su centro de datos al cloud organizando en niveles los datos inactivos de los clústeres ONTAP en las instalaciones al almacenamiento de objetos. Esto libera un valioso espacio en el clúster para más cargas de trabajo sin tener que realizar cambios en la capa de la aplicación. La organización en niveles del cloud puede reducir los costes en su centro de datos y permite cambiar de un modelo de gastos de capital a uno operativo.

El servicio Cloud Tiering aprovecha las funcionalidades de *FabricPool*. FabricPool es una tecnología Data Fabric de NetApp que permite la organización en niveles automatizada de los datos en un almacenamiento de objetos de bajo coste. Los datos activos permanecen en unidades SSD de alto rendimiento, mientras que los datos inactivos se organizan en niveles en almacenamiento de objetos de bajo coste a la vez que se mantienen las eficiencias de datos de ONTAP.

Funciones

La organización en niveles del cloud ofrece automatización, supervisión, informes y una interfaz de gestión común:

- Gracias a la automatización, resulta más sencillo configurar y gestionar los datos Organización en niveles desde clústeres de ONTAP en las instalaciones al cloud
- Un único panel elimina la necesidad de disponer de forma independiente Gestione FabricPool en varios clústeres
- Los informes muestran la cantidad de datos activos e inactivos en cada clúster
- El estado de una organización en niveles le ayuda a identificar y corregir problemas a medida que ocurren
- Si tiene sistemas Cloud Volumes ONTAP, los encontrará en la consola de clústeres para que obtenga una visión completa de la organización en niveles de los datos en su infraestructura de cloud híbrido

Los sistemas Cloud Volumes ONTAP son de solo lectura de la organización en niveles del cloud. "Debe configurar la organización en niveles para Cloud Volumes ONTAP en el Entorno de trabajo en Cloud Manager".

Para obtener más información sobre el valor que ofrece Cloud Tiering, "Visite la página Cloud Tiering en NetApp Cloud Central".

Mientras que Cloud Tiering puede reducir significativamente el espacio de almacenamiento, no es una solución de backup.

Proveedores de almacenamiento de objetos admitidos

Puede organizar en niveles los datos inactivos de un clúster de ONTAP en Amazon S3, almacenamiento de Microsoft Azure Blob, Google Cloud Storage o StorageGRID (cloud privado).

Precios y licencias

Pague por niveles en el cloud mediante una suscripción de pago por uso, una licencia de organización en niveles de ONTAP llamada *FabricPool* o una combinación de ambos. Hay disponible una prueba gratuita de 30 días para su primer grupo si no tiene una licencia.

Al organizar los datos en niveles en StorageGRID, no hay ningún coste. No se requiere ni una licencia BYOL ni registro de PAYGO.

"Ver detalles de precios".

prueba gratuita de 30 días

Si no tiene una licencia de FabricPool, se inicia una prueba gratuita de 30 días de Cloud Tiering al configurar la organización en niveles en su primer clúster. Después de que finalice la prueba gratuita de 30 días, deberá pagar por Cloud Tiering mediante una suscripción de pago por uso, una licencia de FabricPool o una combinación de ambas opciones.

Si su prueba gratuita finaliza y no se ha suscrito o agregado una licencia, ONTAP ya no organiza los datos inactivos en niveles para el almacenamiento de objetos, pero los datos existentes aún están disponibles para su acceso.

Suscripción de pago por uso

Cloud Tiering ofrece licencias basadas en consumo en un modelo de pago por uso. Después de suscribirse a través del mercado de su proveedor de la nube, usted paga por GB por los datos organizados en niveles --no hay pago por adelantado. Su proveedor de cloud se le factura con cargo mensual.

Debe suscribirse aunque tenga una prueba gratuita o si lleva su propia licencia (BYOL):

- La suscripción garantiza que no se produzcan interrupciones en el servicio una vez que finalice la prueba gratuita.

  Cuando finalice la prueba, se le cobrará cada hora según la cantidad de datos que organice.

- Si establece un nivel de más datos del permitido por su licencia de FabricPool, la organización en niveles de datos continúa a través de la suscripción de pago por uso.

  Por ejemplo, si tiene una licencia de 10 TB, toda la capacidad que supere los 10 TB se cobrará a través de la suscripción de pago por uso.

No se le cobrará la suscripción de pago por uso durante la prueba gratuita o si no ha superado la licencia de FabricPool.

"Aprenda a configurar una suscripción de pago por uso".

Con su propia licencia

Con su propia licencia adquiere una licencia de ONTAP FabricPool de NetApp. Puede adquirir licencias perpetuas o basadas en plazos.

Después de comprar una licencia de FabricPool, tendrá que añadirla al clúster, "Que puede hacer directamente desde el cloud por niveles".

Después de activar la licencia a través de Cloud Tiering, si adquiere capacidad adicional más adelante, la

licencia del clúster se actualiza automáticamente con la nueva capacidad. No es necesario aplicar un nuevo archivo de licencia de NetApp (NLF) al clúster.

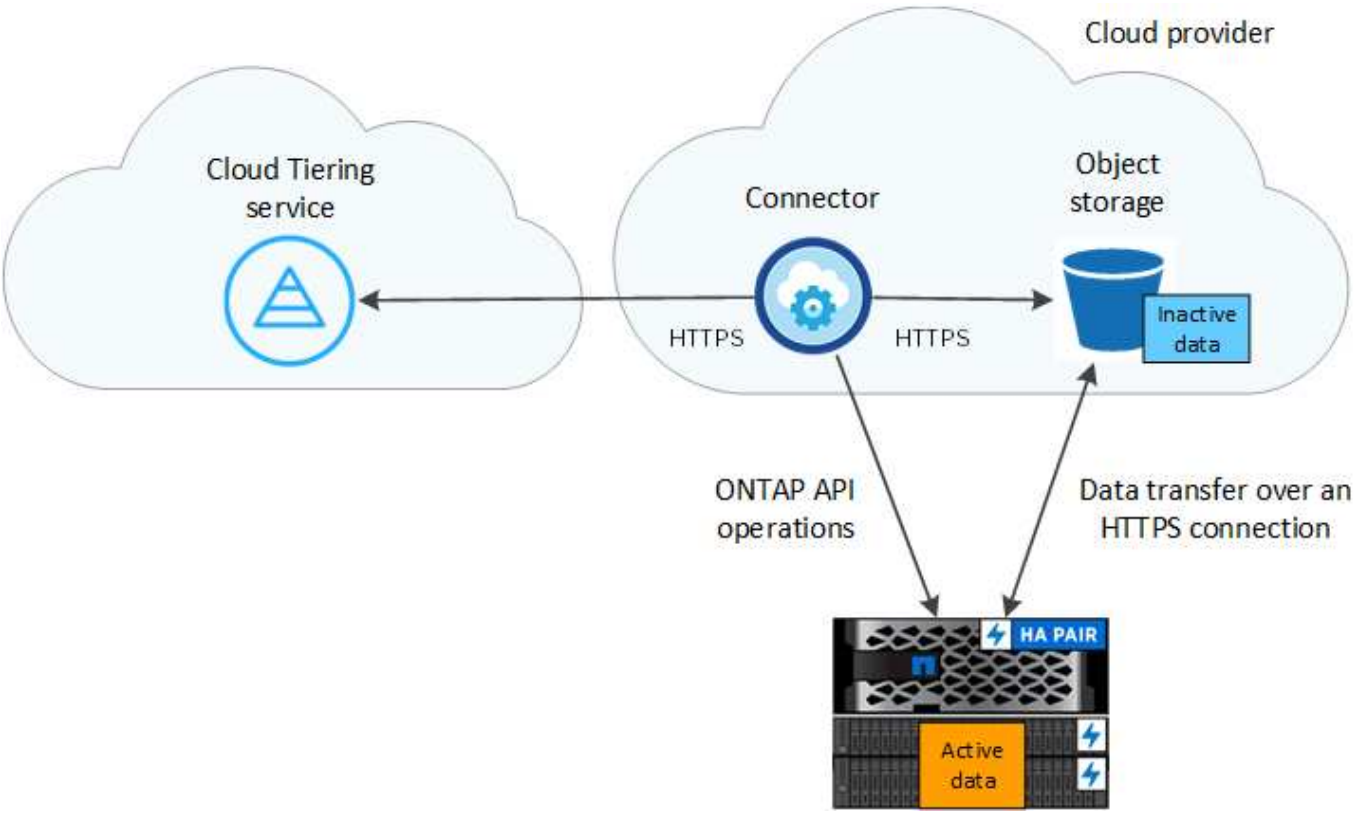
Como se ha indicado anteriormente, le recomendamos que establezca una suscripción de pago por uso, incluso si su clúster tiene una licencia BYOL.

Mailto:ng-cloud-tiering@netapp.com?Subject=Licensing[Póngase en contacto con nosotros para adquirir una licencia].

Funcionamiento de Cloud Tiering

Cloud Tiering es un servicio gestionado por NetApp que utiliza tecnología de FabricPool para organizar automáticamente en niveles los datos inactivos (inactivos) de sus clústeres de ONTAP en las instalaciones en almacenamiento de objetos en su cloud público o en su cloud privado. Las conexiones a ONTAP se realizan desde un conector.

La siguiente imagen muestra la relación entre cada componente:



En un nivel general, Cloud Tiering funciona como este:

1. Descubre su clúster en las instalaciones desde Cloud Manager.
2. Para configurar la organización en niveles, debe proporcionar detalles sobre su almacenamiento de objetos, como el contenedor/bloque y una clase de almacenamiento o nivel de acceso.
3. Cloud Manager configura ONTAP para utilizar el proveedor de almacenamiento de objetos y determina la cantidad de datos activos e inactivos en el clúster.
4. La política de organización en niveles y los volúmenes se aplican a esos volúmenes.
5. ONTAP inicia la organización en niveles de los datos inactivos en el almacén de objetos, tan pronto como estos hayan alcanzado los umbrales que se deben considerar inactivos (consulte Políticas de organización

en niveles del volumen).

Almacenamiento de objetos

Cada clúster de ONTAP organiza los datos inactivos en un único almacén de objetos. Cuando configura la organización en niveles de datos, tiene la opción de añadir un nuevo bloque/contenedor o seleccionar un bloque/contenedor existente, junto con una clase de almacenamiento o nivel de acceso.

- "Obtenga información sobre las clases de almacenamiento S3 admitidas"
- "Obtenga más información sobre los niveles de acceso de Azure Blob admitidos"
- "Obtenga información sobre las clases de almacenamiento de Google Cloud admitidas"

Políticas de organización en niveles del volumen

Cuando selecciona los volúmenes que desea organizar en niveles, elige una *volume Tiering policy* que se aplicará a cada volumen. Una política de organización en niveles determina cuándo y si los bloques de datos de usuario de un volumen se mueven al cloud.

Sin política de organización en niveles

Mantiene los datos en un volumen en el nivel de rendimiento, lo que evita que se muevan al cloud.

Snapshots frías (solo Snapshot)

ONTAP organiza los bloques de instantáneas inactivos en el volumen que no se comparten con el sistema de archivos activo al almacenamiento de objetos. Si se leen, los bloques de datos inactivos del nivel de cloud se activan y se mueven al nivel de rendimiento.

Los datos se organizan en niveles solo después de que un agregado alcance el 50 % de la capacidad y cuando los datos hayan alcanzado el periodo de refrigeración. El número predeterminado de días de enfriamiento es 2, pero puede ajustar el número de días.

> Las escrituras del nivel de cloud al nivel de rendimiento se deshabilitan si la capacidad del nivel de rendimiento es superior al 70 %. Si esto sucede, se accede a los bloques directamente desde el nivel de cloud.

Datos de usuario fríos (automático)

ONTAP organiza todos los bloques de datos fríos en el volumen (sin metadatos incluidos) en niveles para el almacenamiento de objetos. Los datos inactivos incluyen no solo copias snapshot, sino también datos de usuarios inactivos del sistema de archivos activo.

Si las lecturas se leen al azar, los bloques de datos inactivos del nivel de cloud se activan y se mueven al nivel de rendimiento. Si las lecturas secuenciales, como las asociadas con análisis de índices y antivirus, los bloques de datos inactivos del nivel de cloud permanecen inactivos y no se escriben en el nivel de rendimiento.

Los datos se organizan en niveles solo después de que un agregado alcance el 50 % de la capacidad y cuando los datos hayan alcanzado el periodo de refrigeración. El período de refrigeración es el tiempo en el que los datos de usuario de un volumen deben permanecer inactivos para que los datos se puedan considerar "inactivos" y moverse al almacén de objetos. El número predeterminado de días de enfriamiento es 31, pero puede ajustar el número de días.

Las escrituras del nivel de cloud al nivel de rendimiento se deshabilitan si la capacidad del nivel de rendimiento es superior al 70 %. Si esto sucede, se accede a los bloques directamente desde el nivel de cloud.

Todos los datos de usuario (todos)

Todos los datos (no incluidos los metadatos) se marcan inmediatamente como fríos y por niveles en el almacenamiento de objetos lo antes posible. No es necesario esperar 48 horas hasta que se enfrían los bloques nuevos en un volumen. Tenga en cuenta que los bloques ubicados en el volumen antes de ajustar la normativa de todo requieren 48 horas de frío.

Si se leen, los bloques de datos inactivos del nivel de cloud permanecen activos y no se vuelven a escribir en el nivel de rendimiento. Esta política está disponible a partir de ONTAP 9.6.

Tenga en cuenta lo siguiente antes de elegir esta política de organización en niveles:

- La organización en niveles de los datos reduce inmediatamente las eficiencias del almacenamiento (solo en línea).
- Debe usar esta política solo si confía en que los datos en frío del volumen no cambiarán.
- El almacenamiento de objetos no es transaccional y provocará una fragmentación significativa si se somete a cambios.
- Tenga en cuenta el impacto de las transferencias de SnapMirror antes de asignar la política de organización en niveles de todos a los volúmenes de origen en las relaciones de protección de datos.

  Dado que los datos se organizan en niveles de inmediato, SnapMirror lee los datos del nivel de cloud en lugar del nivel de rendimiento. Como resultado, las operaciones de SnapMirror serán más lentas, posiblemente ralentizarán otras operaciones de SnapMirror más adelante en la cola, aunque utilicen diferentes políticas de organización en niveles.

Todos los datos de usuario de DP (respaldo)

Todos los datos de un volumen de protección de datos (sin incluir los metadatos) se mueven inmediatamente al nivel de cloud. Si se leen, los bloques de datos inactivos del nivel de cloud permanecen inactivos y no se vuelven a escribir en el nivel de rendimiento (a partir de ONTAP 9.4).

Esta política está disponible para ONTAP 9.5 o anterior. Se reemplazó por la política de organización en niveles **todo** a partir de ONTAP 9.6.

Manos a la obra

Organización en niveles de los datos de los clústeres ONTAP en las instalaciones a Amazon S3

Libere espacio en sus clústeres de ONTAP en las instalaciones organizando en niveles los datos en Amazon S3. La organización en niveles de los datos utiliza el servicio Cloud Tiering de NetApp.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

Prepárese para organizar los datos en niveles en Amazon S3

Necesita lo siguiente:

- Un sistema AFF o FAS con agregados íntegramente de SSD que ejecutan ONTAP 9.2 o una versión posterior y que tiene una conexión HTTPS con Amazon S3.
- Una cuenta de AWS que tiene una clave de acceso y. los permisos necesarios De este modo, el clúster de ONTAP puede organizar en niveles los datos inactivos en S3 y salen de ella.
- Un conector instalado en un VPC o en las instalaciones de AWS.
- Redes para el conector que permite una conexión HTTPS de salida al clúster de ONTAP, al almacenamiento S3 y al servicio Cloud Tiering.

Configure la organización en niveles

En Cloud Manager, seleccione un entorno de trabajo en las instalaciones, haga clic en **Configurar organización en niveles** y siga las indicaciones para organizar los datos en niveles en Amazon S3.

Configurar la licencia

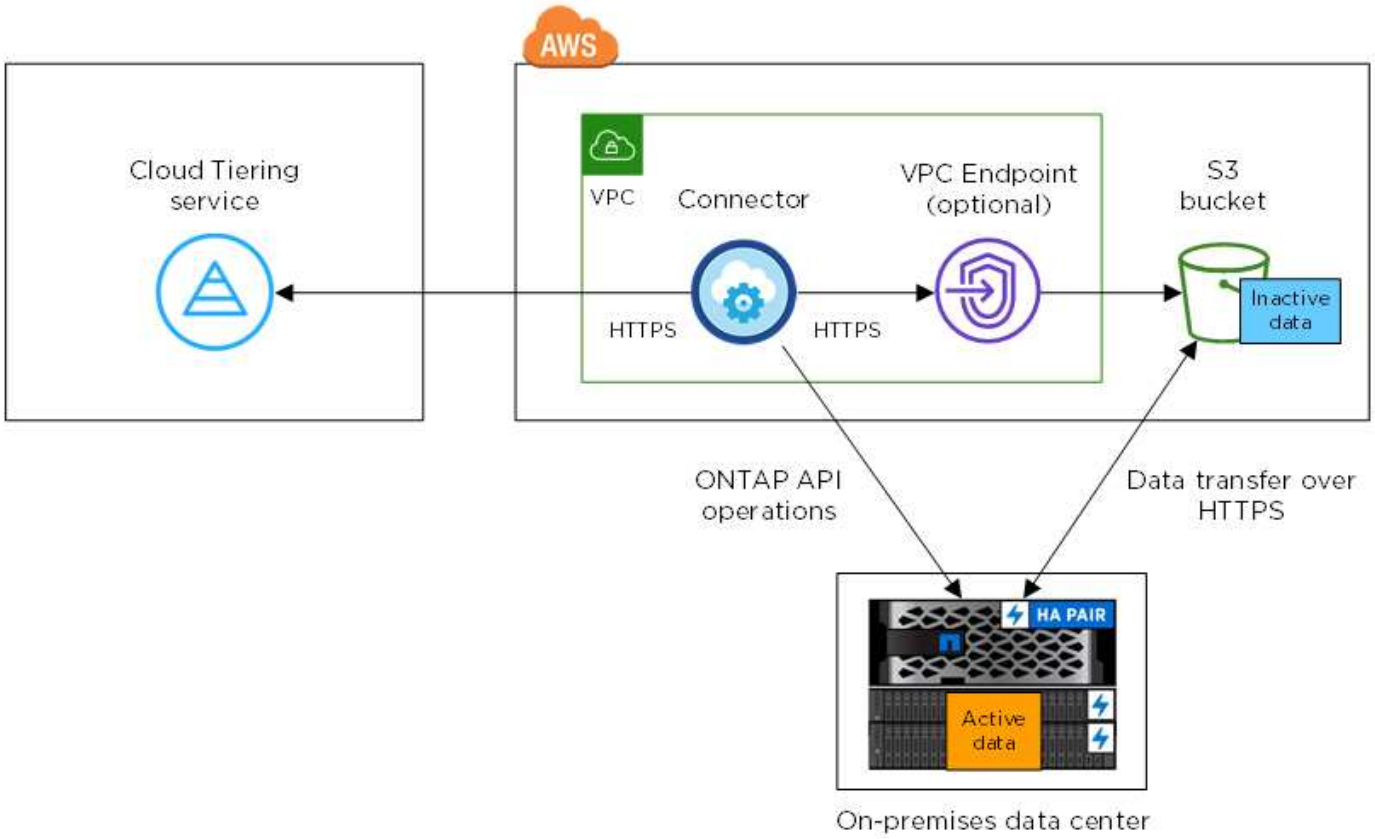
Cuando finalice la prueba gratuita, pague por Cloud Tiering mediante una suscripción de pago por uso, una licencia de organización en niveles de ONTAP o una combinación de ambas:

- Para suscribirse desde AWS Marketplace, haga clic en **segmentación > Licencia**, haga clic en **Suscribirse** y siga las indicaciones.
- Para pagar usando una licencia de organización en niveles, contactarnos si necesita comprar una y luego "Añádalo a su clúster desde la organización en niveles del cloud".

Requisitos

Verifique la compatibilidad con su clúster de ONTAP, configure las redes y prepare el almacenamiento de objetos.

La siguiente imagen muestra cada componente y las conexiones que necesita preparar entre ellos:



La comunicación entre un conector y S3 es únicamente para la configuración del almacenamiento de objetos. El conector puede residir en sus instalaciones, en lugar de en la nube.

Preparar los clústeres de ONTAP

Los clústeres de ONTAP deben cumplir los siguientes requisitos cuando organizando los datos en niveles en Amazon S3.

Plataformas ONTAP compatibles

Cloud Tiering admite sistemas AFF y agregados íntegramente de SSD en sistemas FAS.

Versión de ONTAP compatible

ONTAP 9.2 o posterior

Requisitos para la red de clúster

- El clúster de ONTAP inicia una conexión HTTPS a través del puerto 443 a Amazon S3.

  ONTAP lee y escribe datos en y desde el almacenamiento de objetos. El almacenamiento de objetos nunca se inicia, solo responde.

  Aunque la conexión directa de AWS ofrece un mejor rendimiento y menores cargas de transferencia de datos, no es necesario entre el clúster ONTAP y S3. Debido a que el rendimiento mejora significativamente cuando se usa AWS Direct Connect, es la mejor práctica recomendada.

- Se requiere una conexión entrante desde el conector, que puede residir en un VPC de AWS o en sus instalaciones.

No se necesita una conexión entre el clúster y el servicio Cloud Tiering.

- Se requiere una LIF de interconexión de clústeres en cada nodo ONTAP que aloje volúmenes por niveles. La LIF debe estar asociada al *IPspace* que ONTAP debería utilizar para conectarse al almacenamiento de objetos.

  Los espacios IP permiten la segregación del tráfico de red, lo que permite separar el tráfico de clientes para garantizar la privacidad y la seguridad. "Obtenga más información acerca de los espacios IP".

  Cuando configura la organización en niveles de datos, Cloud Tiering le solicita que utilice el espacio IP. Debe elegir el espacio IP al que está asociada cada LIF. Puede ser el espacio IP «predeterminado» o un espacio IP personalizado que haya creado.

Volúmenes y agregados compatibles

El número total de volúmenes que puede organizar en niveles en Cloud puede ser menor que el número de volúmenes en su sistema ONTAP. Esto se debe a que los volúmenes no pueden estar organizados en niveles desde algunos agregados. Por ejemplo, no se pueden organizar los datos por niveles desde SnapLock Volumes o desde configuraciones MetroCluster. Consulte la documentación de ONTAP para "Funcionalidad o funciones no compatibles con FabricPool".

Cloud Tiering admite FlexGroup Volumes, a partir de ONTAP 9.5. El programa de instalación funciona igual que cualquier otro volumen.

Creación o conmutación de conectores

Se requiere un conector para organizar los datos en niveles en el cloud. Al organizar en niveles los datos en AWS S3, puede usar un conector que esté en un VPC de AWS o en las instalaciones. Tendrá que crear un conector nuevo o asegurarse de que el conector seleccionado actualmente reside en AWS o en las instalaciones.

- "Más información sobre conectores"
- "Creación de un conector en AWS"
- "Requisitos del host del conector"
- "Instalar el conector en un host Linux existente"
- "Cambio entre conectores"

Preparación de la conexión a redes para el conector

Asegúrese de que el conector tiene las conexiones de red necesarias. Se puede instalar un conector en las instalaciones o en AWS.

Pasos

1. Asegúrese de que la red en la que está instalado el conector habilita las siguientes conexiones:
   - Una conexión de Internet saliente al servicio Cloud Tiering Puerto 443 (HTTPS)
   - Una conexión HTTPS a través del puerto 443 a S3
   - Una conexión HTTPS a través del puerto 443 en los clústeres de ONTAP
2. Si es necesario, habilite un extremo de VPC a S3.

   Se recomienda un extremo de VPC a S3 si tiene una conexión de Conexión directa o VPN del clúster de ONTAP al VPC y desea que la comunicación entre el conector y S3 permanezca en la red interna de AWS.

Preparación de Amazon S3

Cuando se configura la organización en niveles de datos en un nuevo clúster, se le pedirá que cree un bloque de S3 o que seleccione un bloque de S3 existente en la cuenta de AWS donde se haya configurado el conector.

La cuenta de AWS debe tener permisos y una clave de acceso que se puede introducir en Cloud Tiering. El clúster de ONTAP utiliza la clave de acceso para colocar los datos en niveles dentro y fuera de S3.

Pasos

1. Proporcione los siguientes permisos al usuario de IAM:

   ```
   "s3:ListAllMyBuckets",
   "s3:ListBucket",
   "s3:GetBucketLocation",
   "s3:GetObject",
   "s3:PutObject",
   "s3:DeleteObject"
   ```

   "Documentación de AWS: Crear un rol para delegar permisos en un usuario de IAM"

2. Cree o busque una clave de acceso.

   La organización en niveles de cloud transfiere la clave de acceso al clúster ONTAP. Las credenciales no se almacenan en el servicio Cloud Tiering.

   "Documentación de AWS: Gestionar claves de acceso para usuarios de IAM"

Organización en niveles de los datos inactivos del primer clúster en Amazon S3

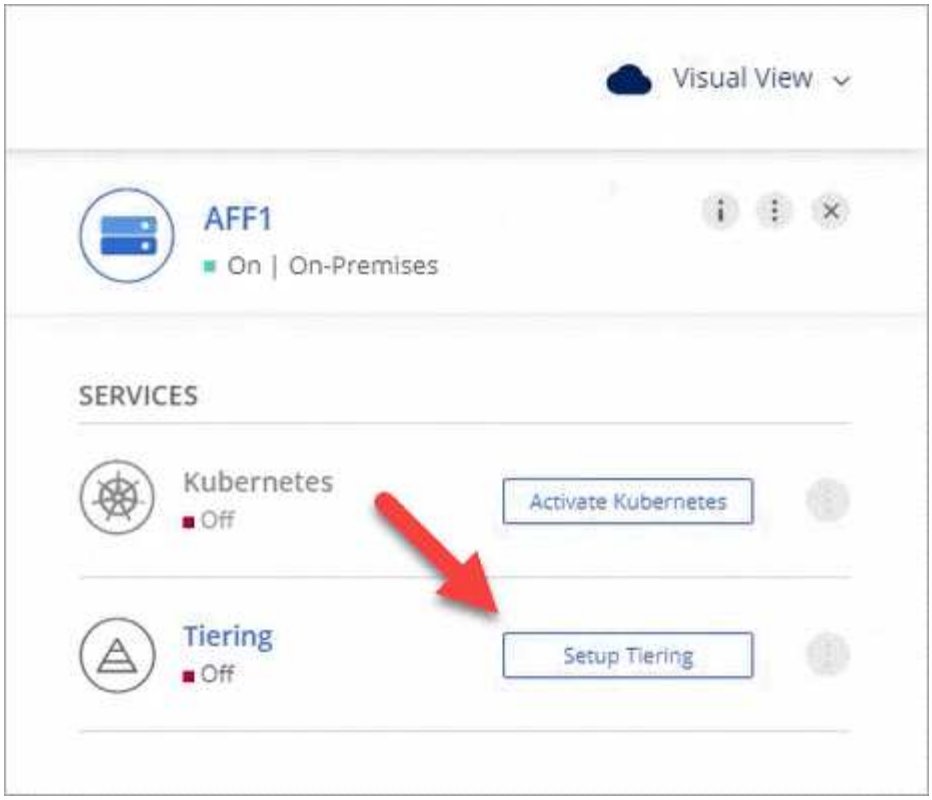
Después de preparar su entorno AWS, comience a organizar en niveles los datos inactivos del primer clúster.

Lo que necesitará

- "Un entorno de trabajo en las instalaciones".
- Una clave de acceso de AWS para un usuario de IAM que tiene los permisos de S3 necesarios.

Pasos

1. Seleccione un clúster en las instalaciones.
2. Haga clic en **Configurar organización en niveles**.



Ahora se encuentra en la consola de almacenamiento por niveles.

3. Haga clic en **Configurar organización en niveles** junto al clúster.
4. Complete los pasos en la página **Configuración de niveles**:

    a. **S3 Bucket**: Agregue un nuevo cubo S3 o seleccione un cubo S3 existente que comience con el prefijo *Fabric-pool* y haga clic en **Continue**.

    Se requiere el prefijo *Fabric-pool* porque la política IAM del conector permite a la instancia realizar acciones S3 en bloques denominados con ese prefijo exacto.

    Por ejemplo, se puede asignar el nombre S3 bucket Fabric-pool-AFF1, donde AFF1 es el nombre del clúster.

    a. **clase de almacenamiento**: Seleccione la clase de almacenamiento S3 a la que desea transferir los datos después de 30 días y haga clic en **continuar**.

    Si elige Estándar, los datos permanecen en esa clase de almacenamiento.

    b. **Credentials**: Introduzca el ID de clave de acceso y la clave secreta para un usuario IAM que tenga los permisos S3 necesarios.

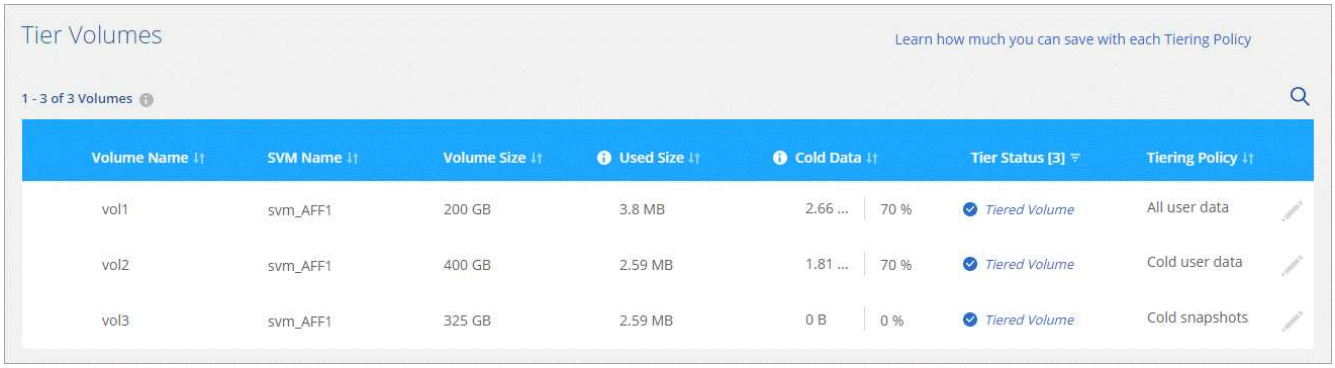
    El usuario IAM debe estar en la misma cuenta de AWS que el bloque que ha seleccionado o creado en la página **S3 Bucket**.

    c. **Red de clúster**: Seleccione el espacio IP que ONTAP debe utilizar para conectarse al almacenamiento de objetos y haga clic en **continuar**.

    Al seleccionar el espacio IP correcto, se garantiza que Cloud Tiering pueda configurar una conexión entre ONTAP y el almacenamiento de objetos de su proveedor de cloud.

5. Haga clic en **continuar** para seleccionar los volúmenes que desea organizar en niveles.
6. En la página **Tier Volumes**, configure la clasificación por niveles para cada volumen. Haga clic en la Seleccione una política de organización en niveles, ajuste opcionalmente los días de refrigeración y haga clic en **aplicar**.

   "Más información acerca de las políticas de organización en niveles de volúmenes".



Resultado

Ha configurado correctamente la organización en niveles de datos de los volúmenes del clúster en el almacenamiento de objetos S3.

El futuro

"Asegúrese de suscribirse al servicio de organización en niveles de cloud".

También puede añadir clústeres adicionales o revisar información sobre los datos activos e inactivos del clúster. Para obtener más información, consulte "Gestionar la organización en niveles de datos desde los clústeres".

Organización en niveles de los datos de los clústeres de ONTAP en las instalaciones al almacenamiento de Azure Blob

Libere espacio en sus clústeres de ONTAP en las instalaciones organizando en niveles los datos en el almacenamiento de Azure Blob. La organización en niveles de los datos utiliza el servicio Cloud Tiering de NetApp.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

1 Prepárese para organizar los datos en niveles en el almacenamiento de Azure Blob

Necesita lo siguiente:

- Un sistema AFF o FAS con agregados íntegramente de SSD que ejecutan ONTAP 9.4 o posterior y que tiene una conexión HTTPS con almacenamiento Azure Blob.
- Un conector instalado en un vnet de Azure.

- Conexión a redes para un conector que permite una conexión HTTPS de salida al clúster de ONTAP en su centro de datos, al almacenamiento de Azure Blob y al servicio Cloud Tiering.

Configure la organización en niveles

En Cloud Manager, seleccione un entorno de trabajo en las instalaciones, haga clic en **Setup Tiering** y siga las indicaciones para organizar los datos en niveles en el almacenamiento de Azure Blob.

Configurar la licencia

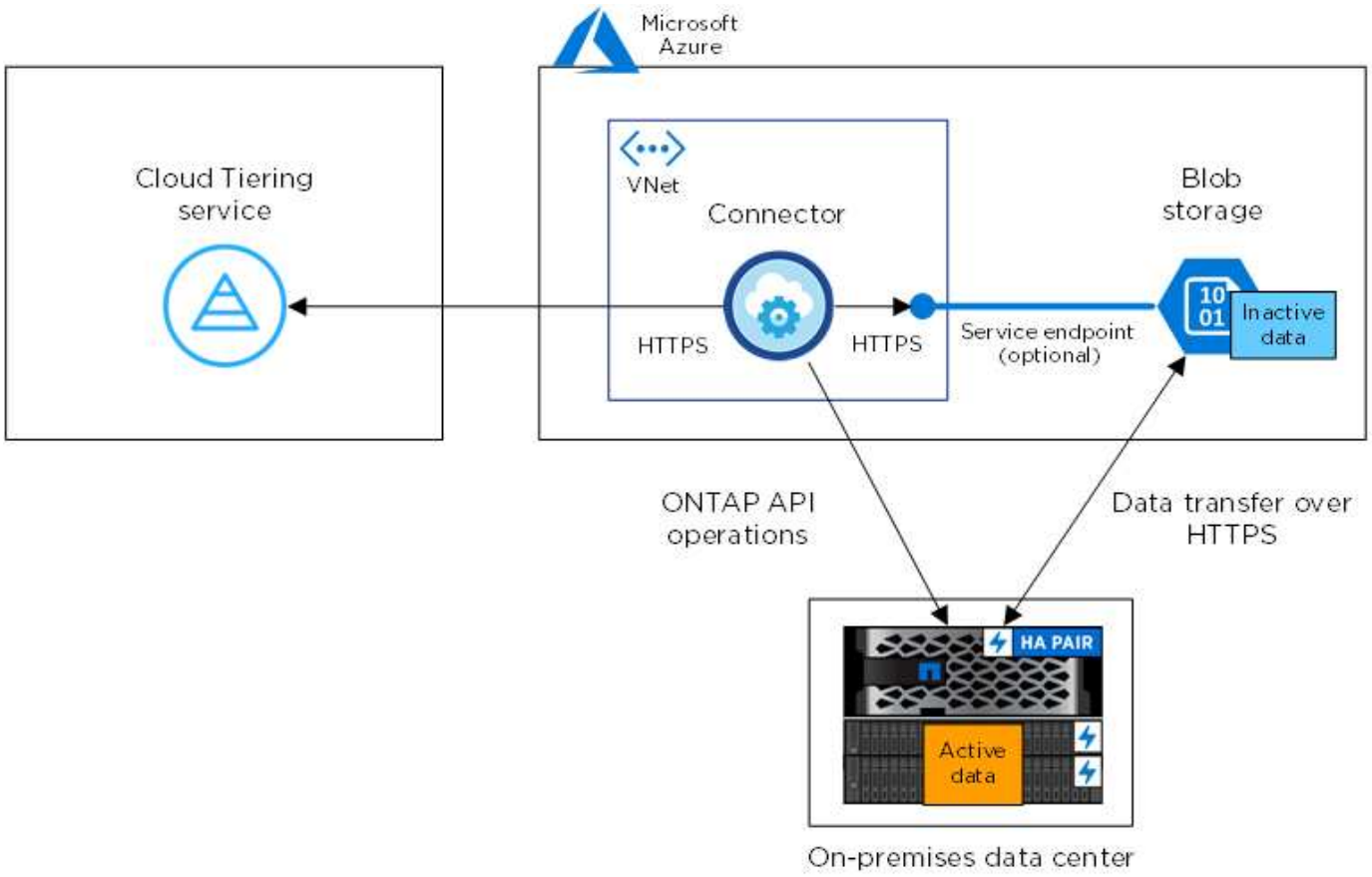
Cuando finalice la prueba gratuita, pague por Cloud Tiering mediante una suscripción de pago por uso, una licencia de organización en niveles de ONTAP o una combinación de ambas:

- Para suscribirse desde Azure Marketplace, haga clic en **segmentación > licencias**, haga clic en **Suscribirse** y siga las indicaciones.
- Para añadir una licencia de organización en niveles, contactarnos si necesita adquirirla y, a continuación, póngase en contacto con nosotros "Añádalo a su clúster desde la organización en niveles del cloud".

Requisitos

Verifique la compatibilidad con su clúster de ONTAP, configure las redes y prepare el almacenamiento de objetos.

La siguiente imagen muestra cada componente y las conexiones que necesita preparar entre ellos:



La comunicación entre el conector y el almacenamiento blob se utiliza únicamente para la configuración del almacenamiento de objetos.

Preparar los clústeres de ONTAP

Sus clústeres de ONTAP deben cumplir los siguientes requisitos cuando organizando los datos en niveles en el almacenamiento de Azure Blob.

Plataformas ONTAP compatibles

Cloud Tiering admite sistemas AFF y agregados íntegramente de SSD en sistemas FAS.

Versión de ONTAP compatible

ONTAP 9.4 o posterior

Requisitos para la red de clúster

- El clúster de ONTAP inicia una conexión HTTPS a través del puerto 443 a almacenamiento de Azure Blob.

  ONTAP lee y escribe datos en y desde el almacenamiento de objetos. El almacenamiento de objetos nunca se inicia, solo responde.

  Aunque ExpressRoute proporciona un mejor rendimiento y menores tasas de transferencia de datos, no es necesario entre el clúster ONTAP y el almacenamiento de Azure Blob. Debido a que el rendimiento mejora significativamente cuando se usa ExpressRoute, hacerlo es la mejor práctica recomendada.

- Se requiere una conexión entrante desde el Service Connector de NetApp, que reside en un vnet de Azure.

  No se necesita una conexión entre el clúster y el servicio Cloud Tiering.

- Se requiere una LIF de interconexión de clústeres en cada nodo ONTAP que aloje volúmenes por niveles. La LIF debe estar asociada al *IPspace* que ONTAP debería utilizar para conectarse al almacenamiento de objetos.

  Los espacios IP permiten la segregación del tráfico de red, lo que permite separar el tráfico de clientes para garantizar la privacidad y la seguridad. "Obtenga más información acerca de los espacios IP".

  Cuando configura la organización en niveles de datos, Cloud Tiering le solicita que utilice el espacio IP. Debe elegir el espacio IP al que está asociada cada LIF. Puede ser el espacio IP «predeterminado» o un espacio IP personalizado que haya creado.

Volúmenes y agregados compatibles

El número total de volúmenes que puede organizar en niveles en Cloud puede ser menor que el número de volúmenes en su sistema ONTAP. Esto se debe a que los volúmenes no pueden estar organizados en niveles desde algunos agregados. Por ejemplo, no se pueden organizar los datos por niveles desde SnapLock Volumes o desde configuraciones MetroCluster. Consulte la documentación de ONTAP para "Funcionalidad o funciones no compatibles con FabricPool".

Cloud Tiering admite FlexGroup Volumes, a partir de ONTAP 9.5. El programa de instalación funciona igual que cualquier otro volumen.

Creación o conmutación de conectores

Se requiere un conector para organizar los datos en niveles en el cloud. Cuando se Tiering los datos para almacenar en niveles en el almacenamiento de Azure Blob, debe haber un conector disponible en un vnet de Azure. Tendrá que crear un conector nuevo o asegurarse de que el conector seleccionado actualmente reside en Azure.

- "Más información sobre conectores"
- "Creación de un conector en Azure"
- "Cambio entre conectores"

Preparación de la conexión a redes para el conector

Asegúrese de que el conector tiene las conexiones de red necesarias.

Pasos

1. Asegúrese de que el vnet donde está instalado el conector habilita las siguientes conexiones:
    - Una conexión de Internet saliente al servicio Cloud Tiering Puerto 443 (HTTPS)
    - Una conexión HTTPS a través del puerto 443 al almacenamiento de Azure Blob
    - Una conexión HTTPS a través del puerto 443 en los clústeres de ONTAP
2. Si es necesario, habilite un extremo de servicio de vnet para el almacenamiento de Azure.

    Se recomienda un extremo de servicio vnet con el almacenamiento de Azure si tiene una conexión ExpressRoute o VPN de su clúster de ONTAP a vnet y desea que la comunicación entre el conector y el almacenamiento BLOB permanezca en su red privada virtual.

Organización en niveles de los datos inactivos del primer clúster en Azure Blob reducida

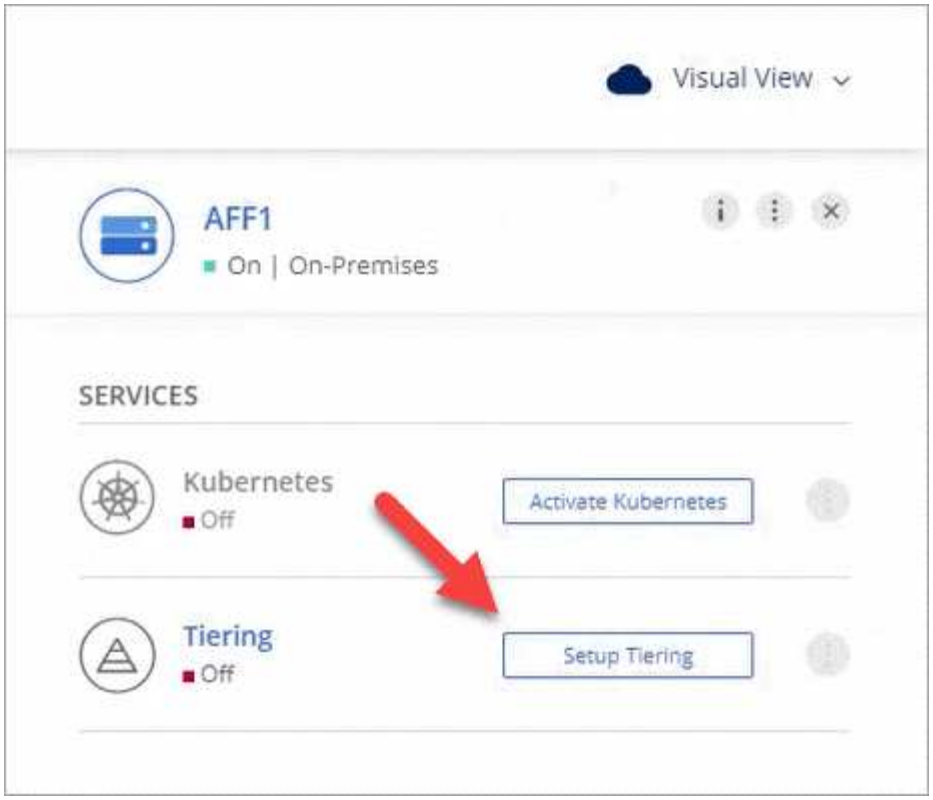
Después de preparar su entorno de Azure, comience a organizar en niveles los datos inactivos del primer clúster.

Lo que necesitará

"Un entorno de trabajo en las instalaciones".

Pasos

1. Seleccione un clúster en las instalaciones.
2. Haga clic en **Configurar organización en niveles**.



Ahora se encuentra en la consola de almacenamiento por niveles.

3. Haga clic en **Configurar organización en niveles** junto al clúster.
4. Complete los pasos en la página **Configuración de niveles**:
   a. **Grupo de recursos**: Seleccione un grupo de recursos en el que se administre un contenedor existente o donde desee crear un contenedor nuevo para datos organizados por niveles.
   b. **contenedor Azure**: Agregue un nuevo contenedor Blob a una cuenta de almacenamiento o seleccione un contenedor existente y haga clic en **continuar**.

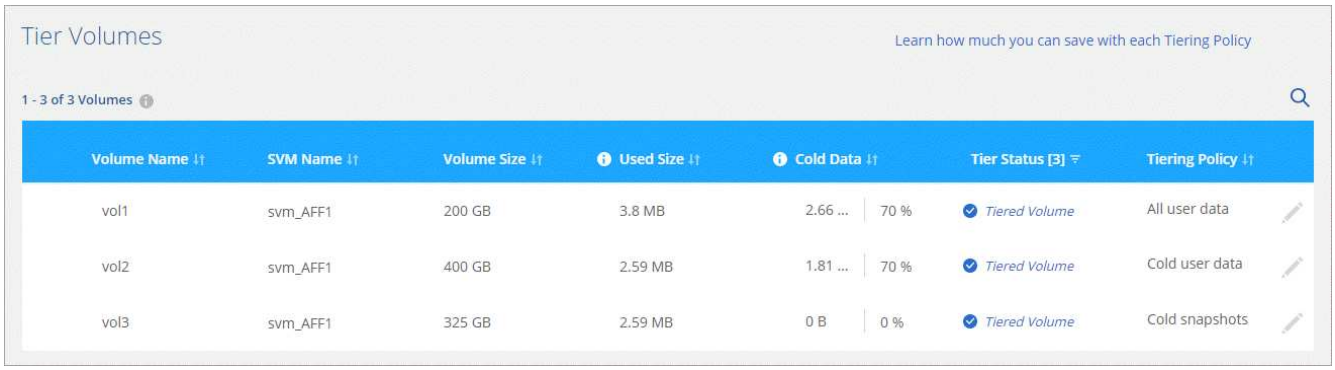
      La cuenta de almacenamiento y los contenedores que aparecen en este paso pertenecen al grupo de recursos seleccionado en el paso anterior.

   c. **nivel de acceso**: Seleccione el nivel de acceso que desea utilizar para los datos organizados por niveles y haga clic en **continuar**.
   d. **Red de clúster**: Seleccione el espacio IP que ONTAP debe utilizar para conectarse al almacenamiento de objetos y haga clic en **continuar**.

      Al seleccionar el espacio IP correcto, se garantiza que Cloud Tiering pueda configurar una conexión entre ONTAP y el almacenamiento de objetos de su proveedor de cloud.

5. Haga clic en **continuar** para seleccionar los volúmenes que desea organizar en niveles.
6. En la página **Tier Volumes**, configure la clasificación por niveles para cada volumen. Haga clic en la  Seleccione una política de organización en niveles, ajuste opcionalmente los días de refrigeración y haga clic en **aplicar**.

   "Más información acerca de las políticas de organización en niveles de volúmenes".



Resultado

Ha configurado correctamente la organización en niveles de datos de los volúmenes del clúster en el almacenamiento de objetos de Azure Blob.

El futuro

"Asegúrese de suscribirse al servicio de organización en niveles de cloud".

También puede añadir clústeres adicionales o revisar información sobre los datos activos e inactivos del clúster. Para obtener más información, consulte "Gestionar la organización en niveles de datos desde los clústeres".

Organización en niveles de los datos de los clústeres de ONTAP en las instalaciones a Google Cloud Storage

Espacio libre en sus clústeres ONTAP en las instalaciones mediante la organización en niveles de los datos en Google Cloud Storage. La organización en niveles de los datos utiliza el servicio Cloud Tiering de NetApp.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

1 Prepárese para organizar los datos en niveles en Google Cloud Storage

Necesita lo siguiente:

- Un sistema AFF o FAS con agregados íntegramente de SSD que ejecutan ONTAP 9.6 o posterior y que tiene una conexión HTTPS con Google Cloud Storage.
- Una cuenta de servicio con el rol de administrador de almacenamiento predefinido y las claves de acceso al almacenamiento.
- Un conector instalado en un VPC de Google Cloud Platform.
- Conexión a redes para el conector que permite una conexión HTTPS de salida al clúster de ONTAP en el centro de datos, a Google Cloud Storage y al servicio Cloud Tiering.

Configure la organización en niveles

En Cloud Manager, seleccione un entorno de trabajo en las instalaciones, haga clic en **Configurar organización en niveles** y siga las indicaciones para organizar los datos en niveles en Google Cloud Storage.

Configurar la licencia

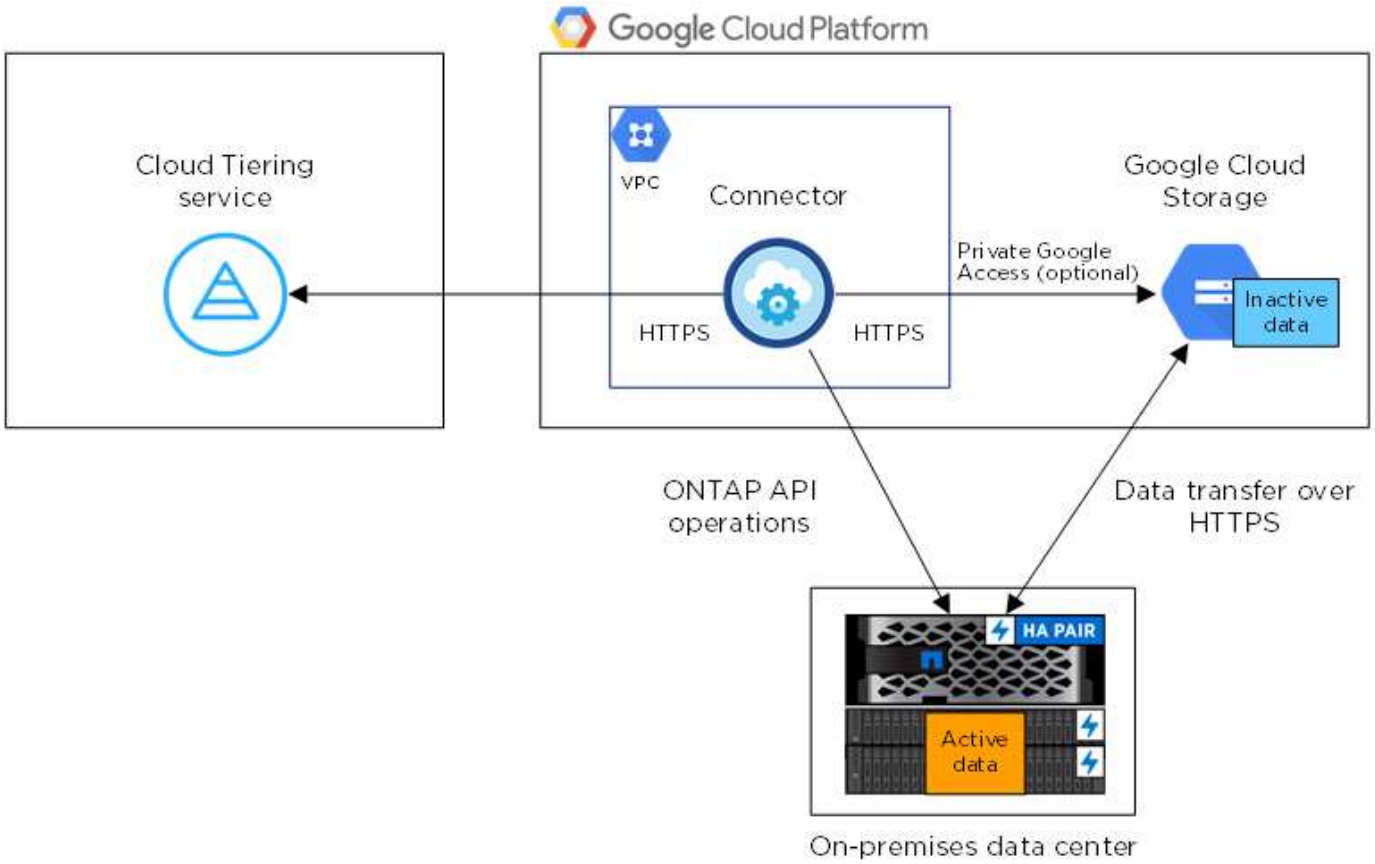
Cuando finalice la prueba gratuita, pague por Cloud Tiering mediante una suscripción de pago por uso, una licencia de organización en niveles de ONTAP o una combinación de ambas:

- Para suscribirse desde GCP Marketplace, haga clic en **segmentación > Licencia**, haga clic en **Suscribirse** y siga las indicaciones.
- Para añadir una licencia de organización en niveles, contactarnos si necesita adquirirla y, a continuación, póngase en contacto con nosotros "Añádalo a su clúster desde la organización en niveles del cloud".

Requisitos

Verifique la compatibilidad con su clúster de ONTAP, configure las redes y prepare el almacenamiento de objetos.

La siguiente imagen muestra cada componente y las conexiones que necesita preparar entre ellos:



La comunicación entre el conector y Google Cloud Storage se utiliza únicamente para la configuración del almacenamiento de objetos.

Preparar los clústeres de ONTAP

Sus clústeres de ONTAP deben cumplir los siguientes requisitos cuando organizando los datos en niveles en Google Cloud Storage.

Plataformas ONTAP compatibles

Cloud Tiering admite sistemas AFF y agregados íntegramente de SSD en sistemas FAS.

Versiones de ONTAP compatibles

ONTAP 9.6 o posterior

Requisitos para la red de clúster

- El clúster de ONTAP inicia una conexión HTTPS a través del puerto 443 a Google Cloud Storage.

  ONTAP lee y escribe datos en y desde el almacenamiento de objetos. El almacenamiento de objetos nunca se inicia, solo responde.

  A pesar de que Google Cloud Interconnect ofrece un mejor rendimiento y menores cargas de transferencia de datos, no es necesario entre el clúster ONTAP y Google Cloud Storage. Dado que el rendimiento es significativamente mejor cuando se usa Google Cloud Interconnect, se recomienda hacerlo.

- Se requiere una conexión entrante en el conector de servicios de NetApp, que reside en un VPC de Google Cloud Platform.

  No se necesita una conexión entre el clúster y el servicio Cloud Tiering.

- Se requiere una LIF de interconexión de clústeres en cada nodo ONTAP que aloje volúmenes por niveles. La LIF debe estar asociada al *IPspace* que ONTAP debería utilizar para conectarse al almacenamiento de objetos.

  Los espacios IP permiten la segregación del tráfico de red, lo que permite separar el tráfico de clientes para garantizar la privacidad y la seguridad. "Obtenga más información acerca de los espacios IP".

  Cuando configura la organización en niveles de datos, Cloud Tiering le solicita que utilice el espacio IP. Debe elegir el espacio IP al que está asociada cada LIF. Puede ser el espacio IP «predeterminado» o un espacio IP personalizado que haya creado.

Volúmenes y agregados compatibles

El número total de volúmenes que puede organizar en niveles en Cloud puede ser menor que el número de volúmenes en su sistema ONTAP. Esto se debe a que los volúmenes no pueden estar organizados en niveles desde algunos agregados. Por ejemplo, no se pueden organizar los datos por niveles desde SnapLock Volumes o desde configuraciones MetroCluster. Consulte la documentación de ONTAP para "Funcionalidad o funciones no compatibles con FabricPool".

Cloud Tiering admite FlexGroup Volumes. El programa de instalación funciona igual que cualquier otro volumen.

Creación o conmutación de conectores

Se requiere un conector para organizar los datos en niveles en el cloud. Al organizar los datos en niveles en Google Cloud Storage, debe haber un conector disponible en un VPC de Google Cloud Platform. Tendrá que crear un conector nuevo o asegurarse de que el conector seleccionado actualmente reside en GCP.

- "Más información sobre conectores"
- "Creación de un conector en GCP"
- "Cambio entre conectores"

Preparación de la conexión a redes para el conector

Asegúrese de que el conector tiene las conexiones de red necesarias.

Pasos

1. Asegúrese de que el VPC donde está instalado el conector habilita las siguientes conexiones:
   - Una conexión de Internet saliente al servicio Cloud Tiering Puerto 443 (HTTPS)
   - Una conexión HTTPS a través del puerto 443 a Google Cloud Storage
   - Una conexión HTTPS a través del puerto 443 en los clústeres de ONTAP
2. Opcional: Habilite Google Access privado en la subred en la que planea implementar Service Connector.

   "Acceso privado a Google" Es recomendable si tiene una conexión directa de su clúster de ONTAP al VPC y desea que la comunicación entre el conector y Google Cloud Storage permanezca en su red privada virtual. Tenga en cuenta que Private Google Access funciona con instancias de VM que sólo tienen direcciones IP internas (privadas) (sin direcciones IP externas).

Preparación de Google Cloud Storage para la organización de los datos en niveles

Cuando se configura una organización en niveles, debe proporcionar claves de acceso al almacenamiento para una cuenta de servicio con permisos de administrador de almacenamiento. Una cuenta de servicio permite que Cloud Tiering autentique y acceda a los bloques de almacenamiento en cloud que se utilizan para la organización en niveles de los datos. Las claves son necesarias para que Google Cloud Storage sepa quién está haciendo la solicitud.

Pasos

1. "Cree una cuenta de servicio con el Administrador de almacenamiento predefinido función".
2. Vaya a. "Configuración de almacenamiento para GCP" y crear claves de acceso para la cuenta de servicio:
   a. Seleccione un proyecto y haga clic en **interoperabilidad**. Si todavía no lo ha hecho, haga clic en **Activar acceso de interoperabilidad**.
   b. En **claves de acceso para cuentas de servicio**, haga clic en **Crear una clave para una cuenta de servicio**, seleccione la cuenta de servicio que acaba de crear y haga clic en **Crear clave**.

      Tendrá que hacerlo "Introduzca las claves en Cloud Tiering" más tarde al configurar la organización en niveles.

Organización en niveles de los datos inactivos del primer clúster en Google Cloud Reducida

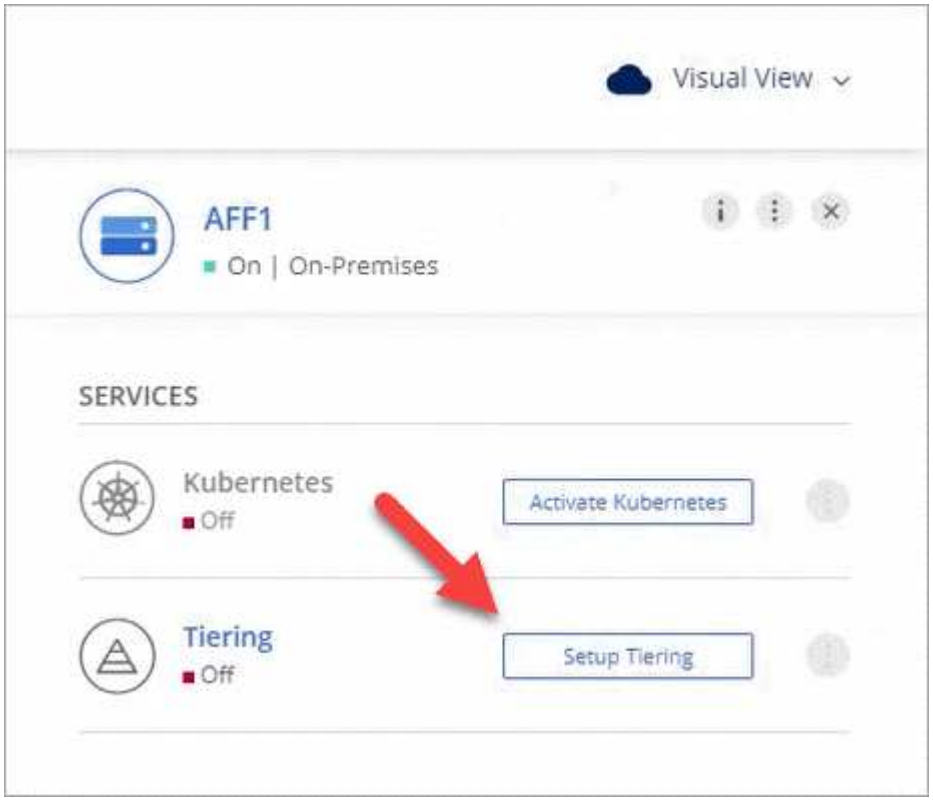
Después de preparar su entorno de Google Cloud, comience a organizar en niveles los datos inactivos del primer clúster.

Lo que necesitará

- "Un entorno de trabajo en las instalaciones".
- Claves de acceso al almacenamiento de una cuenta de servicio con el rol Storage Admin.

Pasos

1. Seleccione un clúster en las instalaciones.
2. Haga clic en **Configurar organización en niveles**.



   Ahora se encuentra en la consola de almacenamiento por niveles.

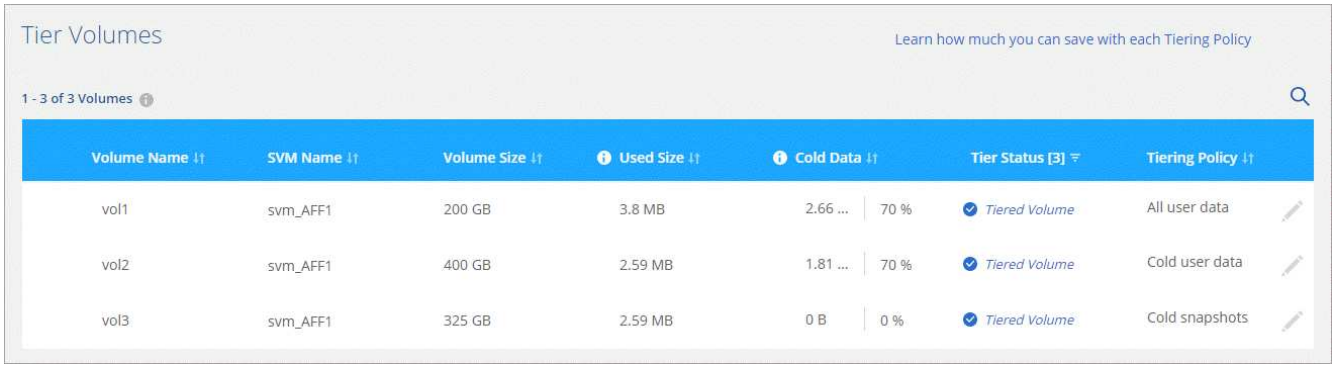
3. Haga clic en **Configurar organización en niveles** junto al clúster.
4. Complete los pasos en la página **Configuración de niveles**:
   a. **Bucket**: Añada un nuevo cubo de Google Cloud Storage o seleccione un bloque existente y haga clic en **continuar**.
   b. **clase de almacenamiento**: Seleccione la clase de almacenamiento que desea utilizar para los datos organizados por niveles y haga clic en **continuar**.
   c. **Credentials**: Introduzca la clave de acceso al almacenamiento y la clave secreta para una cuenta de servicio que tenga el rol Storage Admin.
   d. **Red de clúster**: Seleccione el espacio IP que ONTAP debe utilizar para conectarse al almacenamiento de objetos y haga clic en **continuar**.

      Al seleccionar el espacio IP correcto, se garantiza que Cloud Tiering pueda configurar una conexión entre ONTAP y el almacenamiento de objetos de su proveedor de cloud.

5. Haga clic en **continuar** para seleccionar los volúmenes que desea organizar en niveles.
6. En la página **Tier Volumes**, configure la clasificación por niveles para cada volumen. Haga clic en la

Seleccione una política de organización en niveles, ajuste opcionalmente los días de refrigeración y haga clic en **aplicar**.

"Más información acerca de las políticas de organización en niveles de volúmenes".



Resultado

Ha configurado correctamente la organización en niveles de datos de los volúmenes del clúster en el almacenamiento de objetos Google Cloud.

El futuro

"Asegúrese de suscribirse al servicio de organización en niveles de cloud".

También puede añadir clústeres adicionales o revisar información sobre los datos activos e inactivos del clúster. Para obtener más información, consulte "Gestionar la organización en niveles de datos desde los clústeres".

Organización en niveles de los datos de los clústeres de ONTAP en las instalaciones a StorageGRID

Libere espacio en sus clústeres de ONTAP en las instalaciones organizando en niveles los datos en StorageGRID. La organización en niveles de los datos utiliza el servicio Cloud Tiering de NetApp.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

Prepárese para organizar los datos en niveles en StorageGRID

Necesita lo siguiente:

- Un sistema AFF o FAS con agregados compuestos íntegramente de SSD que ejecutan ONTAP 9.4 o posterior, y una conexión a StorageGRID por un puerto especificado por el usuario.
- StorageGRID 10.3 o una versión posterior con claves de acceso de AWS que tienen permisos de S3.
- Un conector instalado en sus instalaciones.
- Redes para el conector que permite una conexión HTTPS de salida al clúster de ONTAP, a StorageGRID y al servicio de organización en niveles del cloud.

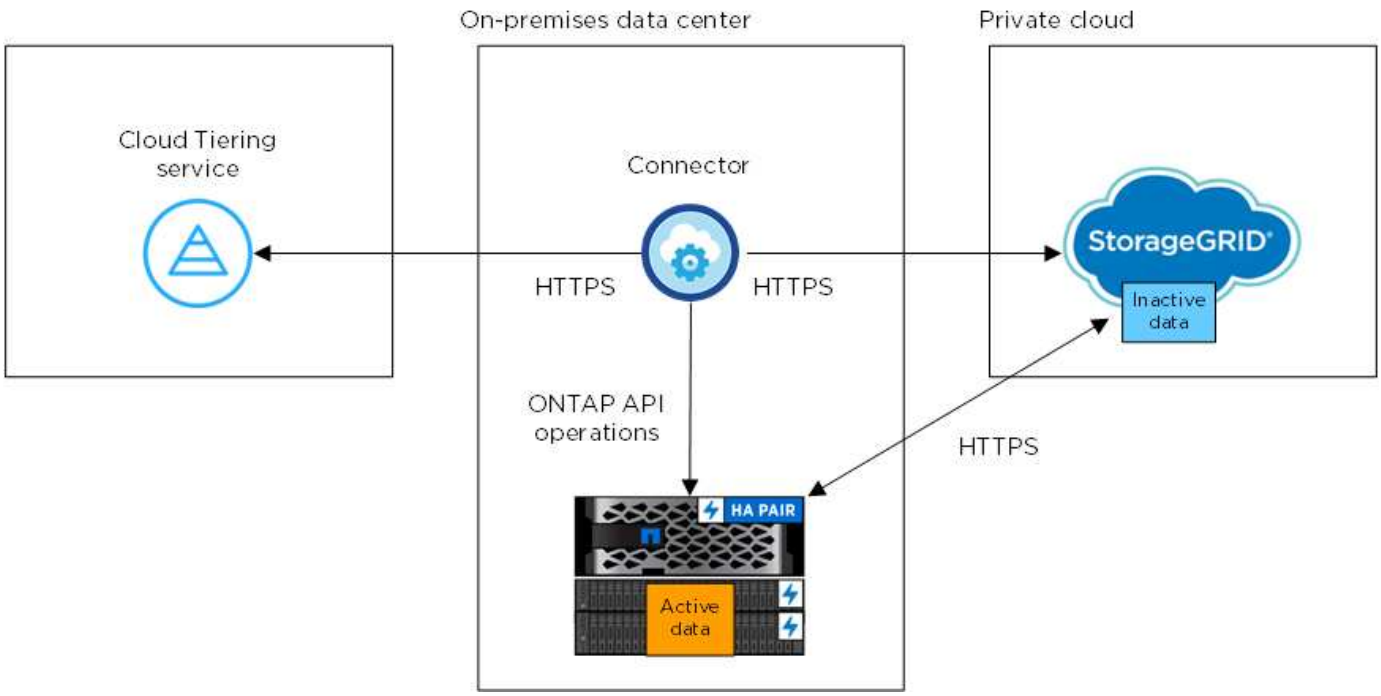
Configure la organización en niveles

Seleccione un entorno de trabajo en las instalaciones, haga clic en **Configurar organización en niveles** y siga las indicaciones para organizar los datos en niveles en StorageGRID.

Requisitos

Verifique la compatibilidad con su clúster de ONTAP, configure las redes y prepare el almacenamiento de objetos.

La siguiente imagen muestra cada componente y las conexiones que necesita preparar entre ellos:



La comunicación entre el conector y StorageGRID es únicamente para la configuración del almacenamiento de objetos.

Preparar los clústeres de ONTAP

Los clústeres de ONTAP deben cumplir los siguientes requisitos cuando organizando datos en niveles en StorageGRID.

Plataformas ONTAP compatibles

Cloud Tiering admite sistemas AFF y agregados íntegramente de SSD en sistemas FAS.

Versión de ONTAP compatible

ONTAP 9.4 o posterior

Licencia

No se necesita una licencia de FabricPool en el clúster de ONTAP cuando se Tiering los datos en StorageGRID.

Requisitos para la red de clúster

- El clúster de ONTAP inicia una conexión HTTPS a través de un puerto especificado por el usuario a StorageGRID (el puerto se puede configurar durante la configuración del almacenamiento por niveles).

  ONTAP lee y escribe datos en y desde el almacenamiento de objetos. El almacenamiento de objetos nunca se inicia, solo responde.

- Es necesaria una conexión de entrada desde el conector, que debe residir en sus instalaciones.

  No se necesita una conexión entre el clúster y el servicio Cloud Tiering.

- Se requiere una LIF de interconexión de clústeres en cada nodo ONTAP que aloje volúmenes por niveles. La LIF debe estar asociada al *IPspace* que ONTAP debería utilizar para conectarse al almacenamiento de objetos.

  Los espacios IP permiten la segregación del tráfico de red, lo que permite separar el tráfico de clientes para garantizar la privacidad y la seguridad. "Obtenga más información acerca de los espacios IP".

  Cuando configura la organización en niveles de datos, Cloud Tiering le solicita que utilice el espacio IP. Debe elegir el espacio IP al que está asociada cada LIF. Puede ser el espacio IP «predeterminado» o un espacio IP personalizado que haya creado.

Volúmenes y agregados compatibles

El número total de volúmenes que puede organizar en niveles en Cloud puede ser menor que el número de volúmenes en su sistema ONTAP. Esto se debe a que los volúmenes no pueden estar organizados en niveles desde algunos agregados. Por ejemplo, no se pueden organizar los datos por niveles desde SnapLock Volumes o desde configuraciones MetroCluster. Consulte la documentación de ONTAP para "Funcionalidad o funciones no compatibles con FabricPool".

Cloud Tiering admite FlexGroup Volumes, a partir de ONTAP 9.5. El programa de instalación funciona igual que cualquier otro volumen.

Preparando StorageGRID

StorageGRID debe cumplir con los siguientes requisitos.

Versiones de StorageGRID compatibles

Se admiten StorageGRID 10.3 y versiones posteriores.

Credenciales de S3

Cuando se configura una organización en niveles en StorageGRID, debe proporcionar la organización en niveles del cloud con una clave de acceso S3 y una clave secreta. Cloud Tiering utiliza las claves para acceder a sus bloques.

Estas claves de acceso deben estar asociadas a un usuario que tenga los siguientes permisos:

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject",
"s3:CreateBucket"
```

Control de versiones de objetos

No debe habilitar el control de versiones de objetos StorageGRID en el bloque de almacenamiento de objetos.

Creación o conmutación de conectores

Se requiere un conector para organizar los datos en niveles en el cloud. Al organizar los datos en niveles en StorageGRID, debe haber un conector disponible en las instalaciones. Tendrá que instalar un conector nuevo o asegurarse de que el conector seleccionado actualmente reside en las instalaciones.

- "Más información sobre conectores"
- "Requisitos del host del conector"
- "Instalar el conector en un host Linux existente"
- "Cambio entre conectores"

Preparación de la conexión a redes para el conector

Asegúrese de que el conector tiene las conexiones de red necesarias.

Pasos

1. Asegúrese de que la red en la que está instalado el conector habilita las siguientes conexiones:
   - Una conexión de Internet saliente al servicio Cloud Tiering Puerto 443 (HTTPS)
   - Una conexión HTTPS a través del puerto 443 a StorageGRID
   - Una conexión HTTPS a través del puerto 443 en los clústeres de ONTAP

Organización en niveles de los datos inactivos del primer clúster en StorageGRID

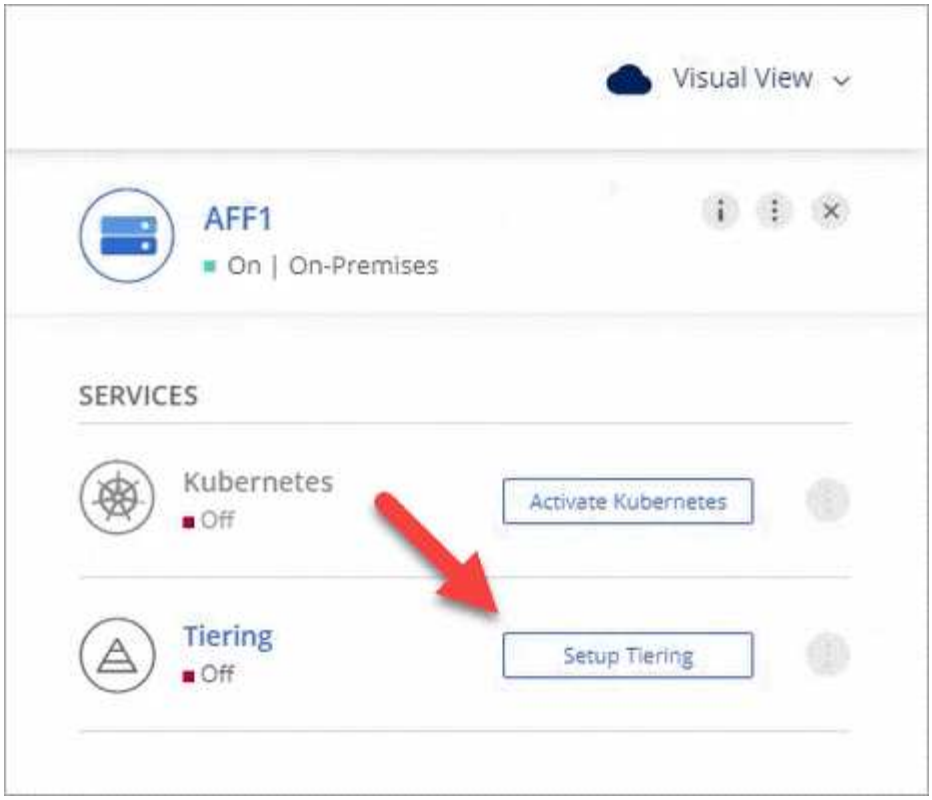
Después de preparar su entorno, comience a organizar en niveles los datos inactivos del primer clúster.

Lo que necesitará

- "Un entorno de trabajo en las instalaciones".
- Una clave de acceso de AWS que tiene los permisos de S3 requeridos.

Pasos

1. Seleccione un clúster en las instalaciones.
2. Haga clic en **Configurar organización en niveles**.

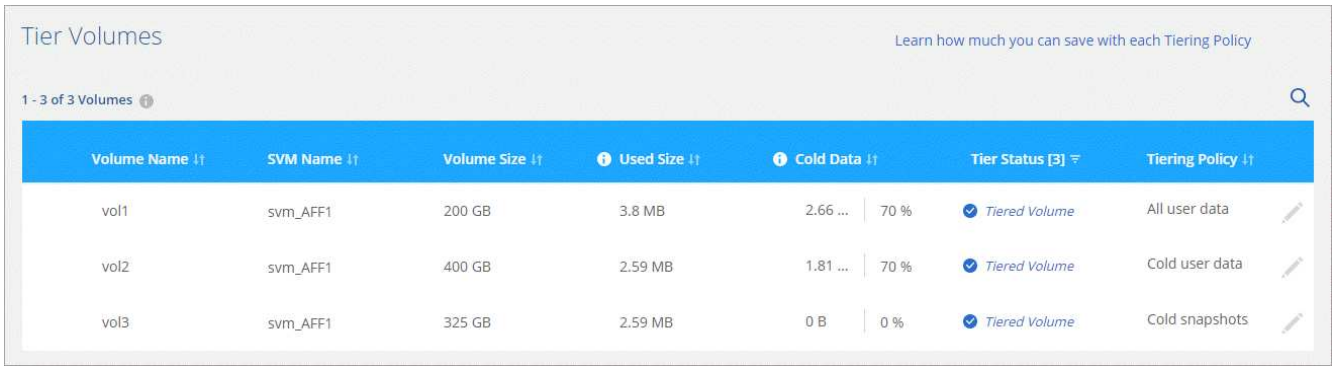


Ahora se encuentra en la consola de almacenamiento por niveles.

3. Haga clic en **Configurar organización en niveles** junto al clúster.
4. Complete los pasos en la página **Configuración de niveles**:
   a. **Elija su proveedor**: Seleccione StorageGRID.
   b. **servidor**: Introduzca el FQDN del servidor StorageGRID, introduzca el puerto que ONTAP debe utilizar para la comunicación HTTPS con StorageGRID e introduzca la clave de acceso y la clave secreta para una cuenta AWS que tenga los permisos S3 necesarios.
   c. **Bucket**: Agregue un nuevo cucharón o seleccione un cucharón existente para los datos organizados por niveles.
   d. **Red de clúster**: Seleccione el espacio IP que ONTAP debe utilizar para conectarse al almacenamiento de objetos y haga clic en **continuar**.

      Al seleccionar el espacio IP correcto, se garantiza que Cloud Tiering pueda configurar una conexión entre ONTAP y el almacenamiento de objetos de su proveedor de cloud.
5. Haga clic en **continuar** para seleccionar los volúmenes que desea organizar en niveles.
6. En la página **Tier Volumes**, configure la clasificación por niveles para cada volumen. Haga clic en la  Seleccione una política de organización en niveles, ajuste opcionalmente los días de refrigeración y haga clic en **aplicar**.

   "Más información acerca de las políticas de organización en niveles de volúmenes".



Resultado

Ha configurado correctamente la organización en niveles de datos de los volúmenes del clúster en StorageGRID.

El futuro

Puede añadir clústeres adicionales o revisar información sobre los datos activos e inactivos del clúster. Para obtener más información, consulte "Gestionar la organización en niveles de datos desde los clústeres".

Configure las licencias para Cloud Tiering

Pague por niveles en el cloud mediante una suscripción de pago por uso, una licencia de organización en niveles de ONTAP llamada *FabricPool* o una combinación de ambos. Si quiere pagar por uso, debe suscribirse al mercado del proveedor de cloud al que quiera organizar en niveles los datos inactivos. No es necesario suscribirse desde todos los mercados.

Antes de leer más:

- Si ya hay una licencia de FabricPool instalada en el clúster, estará configurado; no hay nada más que deba hacer.
- Si ya está suscrito a la suscripción de Cloud Manager en el mercado de su proveedor de cloud, también se suscribe automáticamente a Cloud Tiering. Verá una suscripción activa en la pestaña Cloud Tiering **Licensing**. No tendrá que volver a suscribirse.
- Al organizar los datos en niveles en StorageGRID, no hay ningún coste. No se requiere ni una licencia BYOL ni registro de PAYGO.

"Obtenga más información sobre cómo funciona la licencia para Cloud Tiering".

Suscribirse desde AWS Marketplace

Suscríbase a Cloud Tiering desde AWS Marketplace para configurar una suscripción de pago por uso para organizar los datos en niveles desde clústeres de ONTAP a AWS S3.

Pasos

1. En Cloud Manager, haga clic en **Tiering > Licensing**.
2. Haga clic en **Suscribirse** en AWS Marketplace y a continuación, haga clic en **continuar**.
3. Suscríbase desde el mercado de AWS y, a continuación, vuelva a iniciar sesión en Cloud Central para completar el registro.

El siguiente vídeo muestra el proceso:

► https://docs.netapp.com/es-es/occm38//media/video_subscribing_aws_tiering.mp4 *(video)*

Suscribirse desde Azure Marketplace

Suscríbase a Cloud Tiering desde Azure Marketplace para configurar una suscripción de pago por uso para organizar los datos en niveles desde clústeres de ONTAP al almacenamiento de Azure Blob.

Pasos

1. En Cloud Manager, haga clic en **Tiering > Licensing**.
2. Haga clic en **Suscribirse** en Azure Marketplace y a continuación, haga clic en **continuar**.
3. Suscríbase desde Azure Marketplace y vuelva a iniciar sesión en Cloud Central para completar el registro.

El siguiente vídeo muestra el proceso:

► https://docs.netapp.com/es-es/occm38//media/video_subscribing_azure_tiering.mp4 *(video)*

Suscribirse desde el mercado de GCP

Suscríbase a Cloud Tiering desde GCP Marketplace para establecer una suscripción de pago por uso para organizar los datos en niveles desde clústeres de ONTAP hasta el almacenamiento Google Cloud.

Pasos

1. En Cloud Manager, haga clic en **Tiering > Licensing**.
2. Haga clic en **Suscribirse** en GCP Marketplace y a continuación, haga clic en **continuar**.
3. Suscríbase desde el mercado de GCP y, a continuación, vuelva a iniciar sesión en Cloud Central para completar el registro.

el siguiente vídeo muestra el proceso:

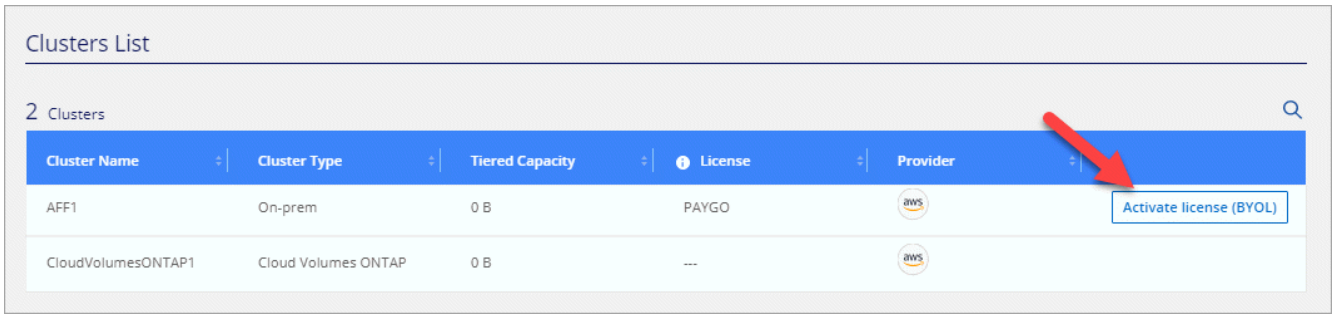
► https://docs.netapp.com/es-es/occm38//media/video_subscribing_gcp_tiering.mp4 *(video)*

Se añade una licencia de organización en niveles a ONTAP

Con su propia licencia adquiere una licencia de ONTAP FabricPool de NetApp.

Pasos

1. Si no tiene una licencia de FabricPool, contactarnos para comprar una.
2. En Cloud Manager, haga clic en **Tiering > Licensing**.
3. En la tabla Lista de clústeres, haga clic en **Activar licencia (BYOL)** para un clúster ONTAP en las instalaciones.



4. Introduzca el número de serie de la licencia y, a continuación, introduzca la cuenta del sitio de soporte de NetApp asociada con el número de serie.
5. Haga clic en **Activar licencia**.

Resultado

Cloud Tiering registra la licencia y la instala en el clúster.

Después de terminar

Si adquiere capacidad adicional adicional en otro momento, la licencia del clúster se actualiza automáticamente con la nueva capacidad. No es necesario aplicar un nuevo archivo de licencia de NetApp (NLF) al clúster.

Gestionar la organización en niveles de datos desde los clústeres

Ahora que ha configurado la organización en niveles de datos desde sus clústeres de ONTAP, puede organizar los datos en niveles desde volúmenes adicionales, cambiar la política de organización en niveles de un volumen y mucho más.

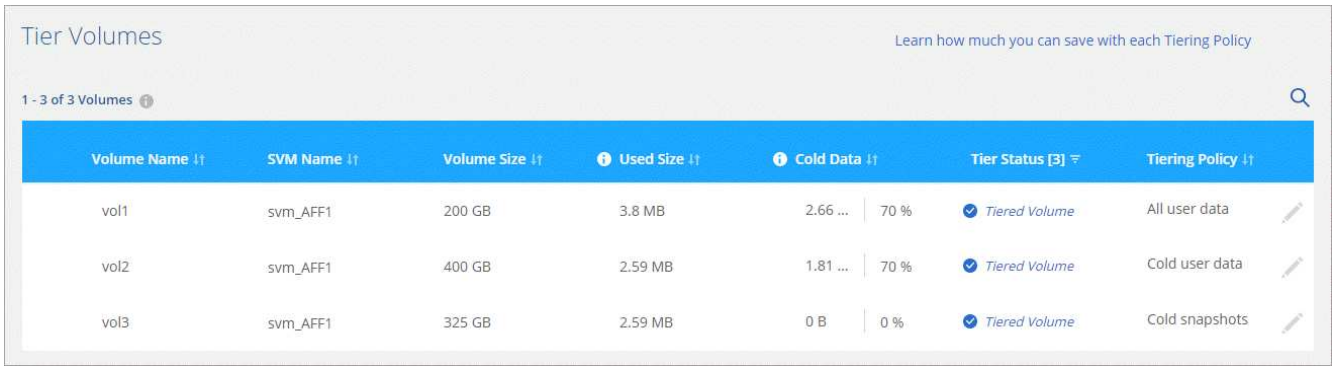
Organización en niveles de datos de volúmenes adicionales

Configure la organización en niveles de datos para volúmenes adicionales en cualquier momento, por ejemplo, después de crear un nuevo volumen.

Pasos

1. En la parte superior de Cloud Manager, haga clic en **segmentación**.
2. En **Cluster Dashboard**, haga clic en **Tier Volumes** para el clúster.
3. Para cada volumen, haga clic en la  Seleccione una política de organización en niveles, ajuste opcionalmente los días de refrigeración y haga clic en **aplicar**.

   "Más información acerca de las políticas de organización en niveles de volúmenes".



No es necesario configurar el almacenamiento de objetos porque ya se ha configurado al configurar inicialmente la organización en niveles para el clúster. ONTAP organiza en niveles los datos inactivos de estos volúmenes en el mismo almacén de objetos.

4. Cuando haya terminado, haga clic en **Cerrar**.

Cambio de la política de organización en niveles de un volumen

Cambiar la política de organización en niveles de un volumen cambia la forma en que ONTAP organiza los datos inactivos en almacenamiento de objetos. El cambio empieza desde el momento en que cambia la política: Solo cambia el comportamiento de organización en niveles posterior del volumen.

Pasos

1. En la parte superior de Cloud Manager, haga clic en **segmentación**.
2. En **Cluster Dashboard**, haga clic en **Tier Volumes** para el clúster.
3. Haga clic en la Seleccione una política de organización en niveles, ajuste opcionalmente los días de refrigeración y haga clic en **aplicar**.

   "Más información acerca de las políticas de organización en niveles de volúmenes".

Gestión de la configuración de organización en niveles en agregados

Cada agregado tiene dos configuraciones que puede ajustar: El umbral de ocupación de la organización en niveles y si la generación de informes de datos inactivos está habilitada.

Umbral de ocupación de la organización en niveles

Si se establece el umbral en un número menor, se reduce la cantidad de datos necesarios para almacenar en el nivel de rendimiento antes de que se lleve a cabo la organización en niveles. Esto puede ser útil para agregados de gran tamaño que contienen pocos datos activos.

Si se establece el umbral en un número mayor, se aumenta la cantidad de datos necesarios para almacenar en el nivel de rendimiento antes de que se lleve a cabo la organización en niveles. Esto puede resultar útil para soluciones diseñadas para realizar niveles solo cuando los agregados están cerca de la capacidad máxima.

Generación de informes de datos inactivos

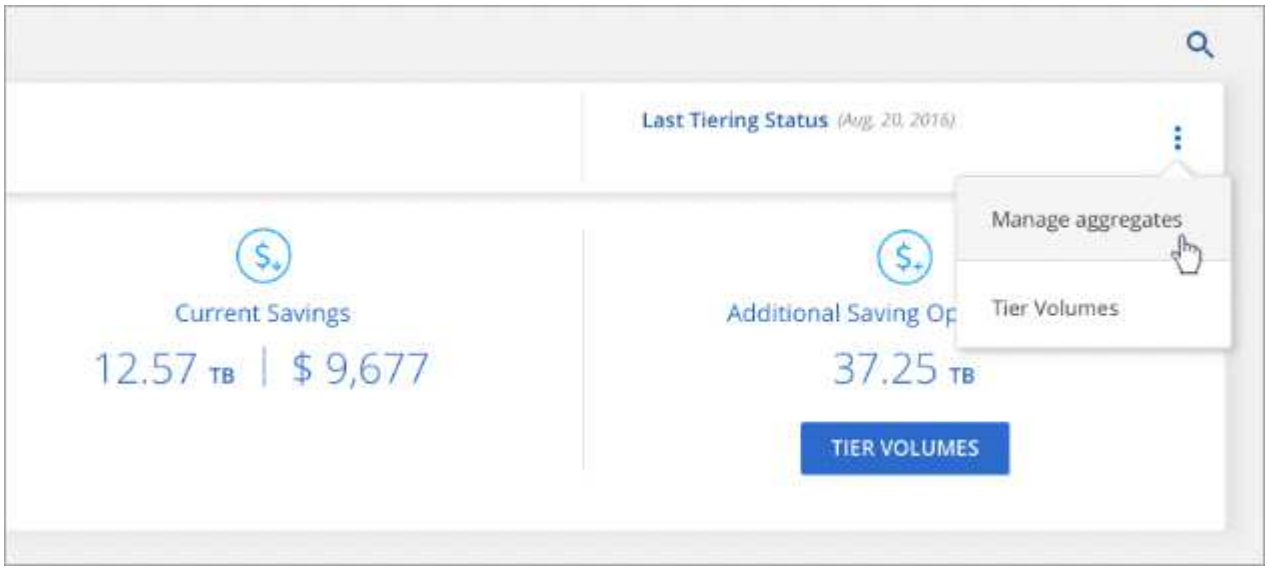
La generación de informes de datos inactivos (IDR) utiliza un periodo de enfriamiento de 31 días para determinar qué datos se consideran inactivos. La cantidad de datos inactivos organizados en niveles depende de las políticas de organización en niveles establecidas en volúmenes. Esta cantidad puede ser

diferente de la cantidad de datos fríos detectados por IDR utilizando un período de enfriamiento de 31 días.

Es mejor mantener activado IDR porque ayuda a identificar sus oportunidades de ahorro y datos inactivos. El IDR debe seguir activado si se habilitó la organización en niveles de datos en un agregado.

Pasos

1. En la parte superior de Cloud Manager, haga clic en **segmentación**.
2. En la página **Cloud Tiering**, haga clic en el icono de menú de un clúster y seleccione **gestionar agregados**.



3. En la página **Administrar agregados**, haga clic en icono de un agregado de la tabla.
4. Modifique el umbral de llenado y elija si desea habilitar o deshabilitar los informes de datos inactivos.

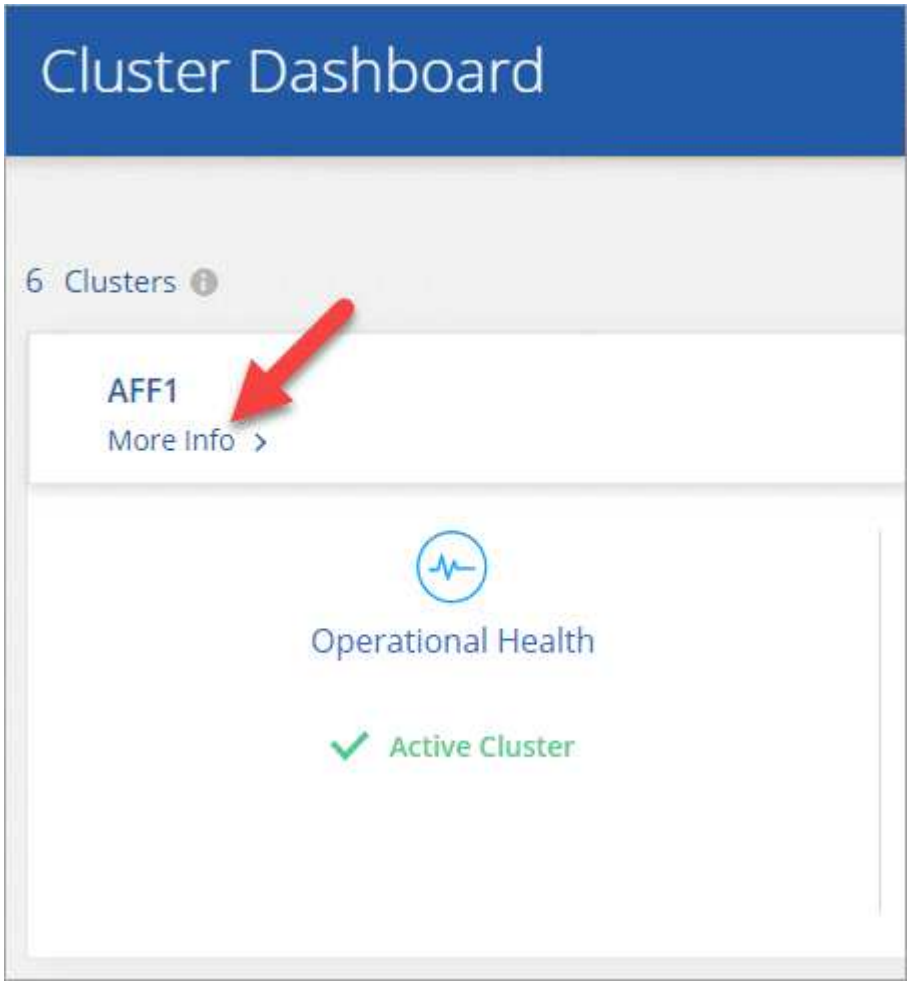
5. Haga clic en **aplicar**.

Revisión de la información de organización en niveles de un clúster

Puede que desee ver cuántos datos hay en el nivel de cloud y cuántos datos hay en los discos. O bien, puede que desee ver la cantidad de datos activos y inactivos en los discos del clúster. La organización en niveles de cloud proporciona esta información para cada clúster.

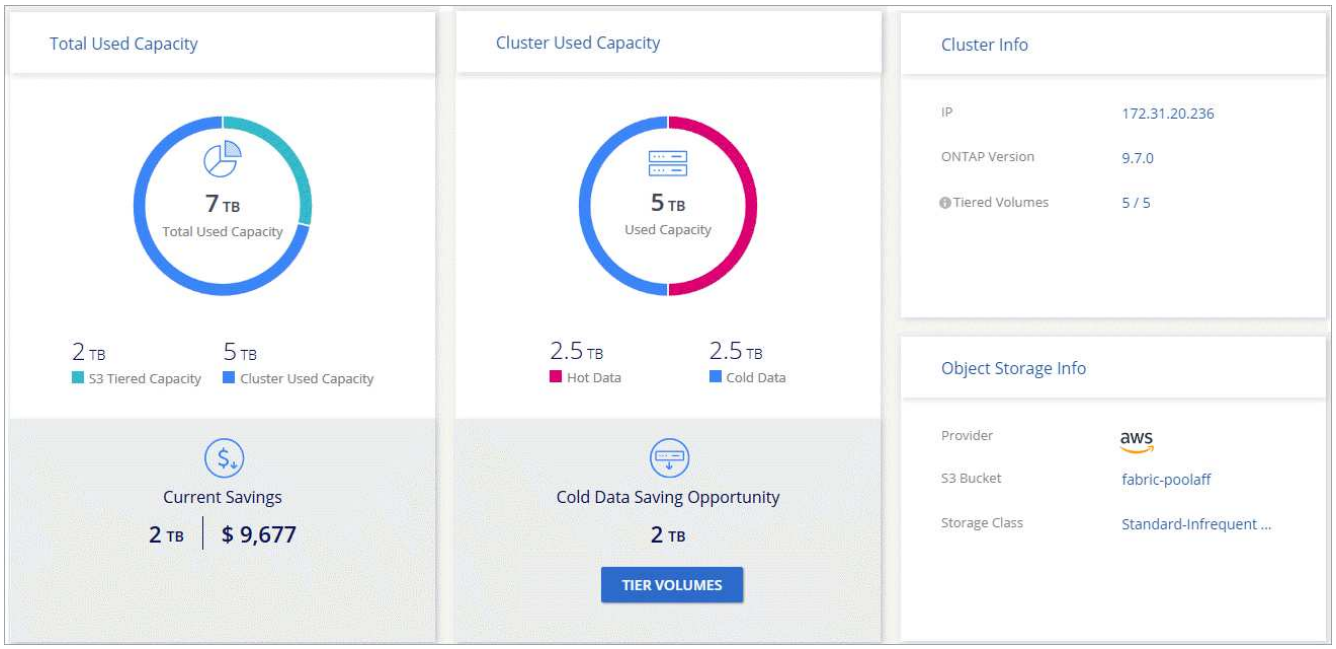
Pasos

1. En la parte superior de Cloud Manager, haga clic en **segmentación**.
2. En **Panel de clústeres**, haga clic en **más información** para un clúster.



3. Revise los detalles sobre el clúster.

   Veamos un ejemplo:

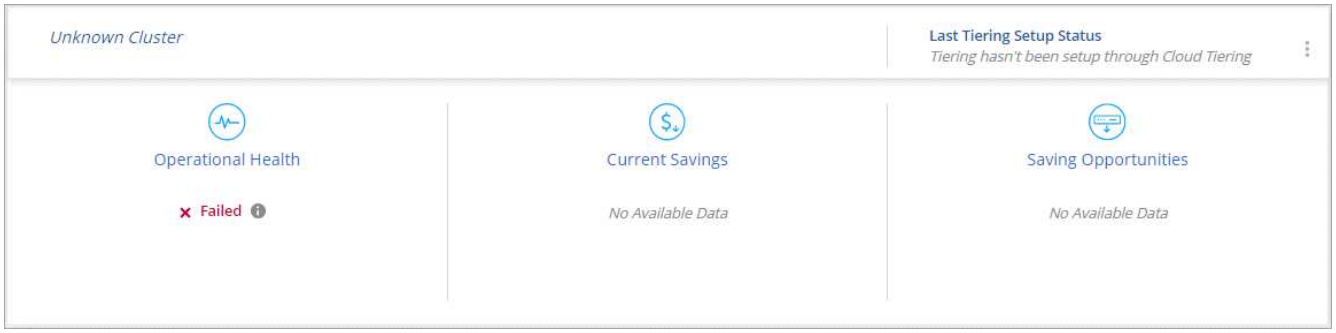


Reparación de la salud operativa

Los fallos pueden producirse. Cuando lo hacen, Cloud Tiering muestra un estado de estado operativo que no se ha podido completar en la consola del clúster. El estado refleja el estado del sistema ONTAP y de Cloud Manager.

Pasos

1. Identifique los clústeres con un estado operativo de "error".



2. Pase el ratón sobre para ver el motivo del fallo.
3. Corrija el problema:
   a. Compruebe que el clúster de ONTAP esté operativo y que tenga una conexión entrante y saliente con el proveedor de almacenamiento de objetos.
   b. Compruebe que Cloud Manager tiene conexiones salientes al servicio Cloud Tiering, al almacén de objetos y a los clústeres de ONTAP que detecta.

Preguntas técnicas frecuentes sobre la organización en niveles del cloud

Estas preguntas frecuentes pueden ser de ayuda si solo está buscando una respuesta

rápida a una pregunta.

ONTAP

Las siguientes preguntas hacen referencia a ONTAP.

¿Cuáles son los requisitos del clúster de ONTAP?

Depende del lugar en el que organice los datos inactivos. Consulte lo siguiente:

- "Organización en niveles de los datos de los clústeres ONTAP en las instalaciones a Amazon S3"
- "Organización en niveles de los datos de los clústeres de ONTAP en las instalaciones al almacenamiento de Azure Blob"
- "Organización en niveles de los datos de los clústeres de ONTAP en las instalaciones a Google Cloud Storage"
- "Organización en niveles de los datos de los clústeres de ONTAP en las instalaciones a StorageGRID"

¿la organización en niveles del cloud habilita los informes de datos inactivos?

Sí, Cloud Tiering permite la generación de informes de datos inactivos en cada agregado. Este ajuste nos permite identificar la cantidad de datos inactivos que se pueden organizar en niveles en almacenamiento de objetos de bajo coste.

¿Puedo organizar los datos en niveles desde volúmenes NAS y SAN?

Puede usar Cloud Tiering para organizar datos en niveles desde NAS Volumes en el cloud público y DE SAN Volumes en un cloud privado usando StorageGRID.

¿y Cloud Volumes ONTAP?

Si tiene sistemas Cloud Volumes ONTAP, los encontrará en la consola de clústeres para que observe una vista completa de la organización en niveles de los datos en su infraestructura de cloud híbrido.

En la consola del clúster, puede ver información de organización en niveles similar a un clúster ONTAP en las instalaciones: Estado operativo, ahorro actual, oportunidades de ahorro, detalles sobre volúmenes y agregados, etc.

Los sistemas Cloud Volumes ONTAP son de solo lectura de la organización en niveles del cloud. No se puede configurar la organización en niveles de datos en Cloud Volumes ONTAP desde la organización en niveles del cloud. De todas formas, configurará la organización en niveles de la misma forma: Desde el entorno de trabajo en Cloud Manager.

Almacenamiento de objetos

Las siguientes preguntas están relacionadas con el almacenamiento de objetos.

¿Qué proveedores de almacenamiento de objetos son compatibles?

Amazon S3, el almacenamiento de Azure Blob, Google Cloud Storage y StorageGRID utilizando el protocolo S3 son compatibles.

¿Puedo usar mi propio contenedor/cucharón?

Sí, puedes. Cuando configura la organización en niveles de datos, tiene la opción de añadir un nuevo bloque/contenedor o seleccionar un bloque/contenedor existente.

¿Qué regiones son compatibles?

- "Regiones admitidas de AWS"
- "Regiones de Azure compatibles"
- "Regiones compatibles de Google Cloud"

¿Qué clases de almacenamiento S3 son compatibles?

La organización en niveles del cloud admite la organización en niveles de los datos en la clase de almacenamiento *Standard*, *Standard-Infrecuente Access*, *One Zone-IA* o *Intelligent*. Consulte "Clases de almacenamiento S3 compatibles" para obtener más detalles.

¿Qué niveles de acceso de Azure Blob son compatibles?

La organización en niveles del cloud utiliza automáticamente el nivel de acceso *Hot* para los datos inactivos.

¿Qué clases de almacenamiento son compatibles con Google Cloud Storage?

Cloud Tiering utiliza la clase de almacenamiento *Standard* para los datos inactivos.

¿Cloud Tiering usa un almacén de objetos para todo el clúster o uno por agregado?

Un almacén de objetos para todo el clúster.

¿Puedo aplicar políticas en mi almacén de objetos para mover datos independientemente de la organización en niveles?

No, Cloud Tiering no admite reglas de gestión del ciclo de vida de objetos que mueven o eliminan datos de almacenes de objetos.

Conectores

Las siguientes preguntas se refieren a conectores.

¿Dónde se debe instalar el conector?

- Al organizar en niveles los datos en S3, un conector puede residir en un VPC de AWS o en las instalaciones.
- Al organizar los datos en niveles en un almacenamiento BLOB, un conector debe residir en una red virtual de Azure.
- Al organizar los datos en niveles en Google Cloud Storage, un conector debe residir en un VPC de Google Cloud Platform.
- Al organizar los datos en niveles en StorageGRID, un conector debe residir en un host Linux en las instalaciones.

Redes

Las siguientes preguntas hacen referencia a las redes.

¿Cuáles son los requisitos de red?

- El clúster de ONTAP inicia una conexión HTTPS a través del puerto 443 al proveedor de almacenamiento de objetos.

  ONTAP lee y escribe datos en y desde el almacenamiento de objetos. El almacenamiento de objetos nunca se inicia, solo responde.

- Para StorageGRID, el clúster ONTAP inicia una conexión HTTPS a través de un puerto especificado por el usuario a StorageGRID (el puerto se puede configurar durante la configuración del almacenamiento por niveles).
- Un conector necesita una conexión HTTPS de salida a través del puerto 443 a los clústeres de ONTAP, al almacén de objetos y al servicio Cloud Tiering.

Para obtener información detallada, consulte:

- "Organización en niveles de los datos de los clústeres ONTAP en las instalaciones a Amazon S3"
- "Organización en niveles de los datos de los clústeres de ONTAP en las instalaciones al almacenamiento de Azure Blob"
- "Organización en niveles de los datos de los clústeres de ONTAP en las instalaciones a Google Cloud Storage"
- "Organización en niveles de los datos de los clústeres de ONTAP en las instalaciones a StorageGRID"

Permisos

Las siguientes preguntas se refieren a los permisos.

¿Qué permisos se requieren en AWS?

Se requieren permisos "Para gestionar el bloque de S3".

¿Qué permisos se requieren en Azure?

No se necesitan permisos adicionales fuera de los permisos que necesite proporcionar a Cloud Manager.

¿Qué permisos se requieren en Google Cloud Platform?

Se necesitan permisos de administrador de almacenamiento para una cuenta de servicio que tenga claves de acceso de almacenamiento.

¿Qué permisos se requieren para StorageGRID?

"Se necesitan permisos de S3".

Referencia

Clases y regiones de almacenamiento S3 admitidas

Cloud Tiering admite varias clases de almacenamiento S3 y la mayoría de regiones.

Clases de almacenamiento S3 compatibles

La organización en niveles de cloud puede aplicar una regla de ciclo de vida para que los datos se transiciones desde la clase de almacenamiento *Standard* a otra clase de almacenamiento después de 30 días. Puede elegir entre las siguientes clases de almacenamiento:

- Acceso Estándar-poco frecuente
- Una Zona-IA
- Inteligente

Si elige Estándar, los datos permanecen en esa clase de almacenamiento.

"Obtenga información acerca de las clases de almacenamiento S3".

Regiones admitidas de AWS

Cloud Tiering admite las siguientes regiones de AWS.

Asia-Pacífico

- Bombay
- Seúl
- Singapur
- Sídney
- Tokio

Europa

- Frankfurt
- Irlanda
- Londres
- París
- Estocolmo

América del Norte

- Canada Central
- GovCloud (EE. UU.-oeste) – a partir de ONTAP 9.3
- Este DE EE. UU. (N. Virginia)
- Este DE EE. UU. (Ohio)
- Oeste DE EE. UU. (N. California)
- Oeste DE EE. UU. (Oregón)

Sudamérica

- São Paulo

Niveles de acceso de Azure Blob y regiones compatibles

Cloud Tiering admite el nivel de acceso *Hot* y la mayoría de las regiones.

Niveles de acceso de Azure Blob compatibles

Cuando configura la organización en niveles de datos en Azure, Cloud Tiering utiliza automáticamente el nivel de acceso *Hot* para los datos inactivos.

Regiones de Azure compatibles

Cloud Tiering admite las siguientes regiones de Azure.

África

- Sudáfrica Norte

Asia-Pacífico

- Australia Oriental
- Australia Sureste
- Asia Oriental
- Japón este
- Japón Oeste
- Corea Central
- Corea del Sur
- Sudeste asiático

Europa

- Francia Central
- Alemania Central
- Alemania Noreste
- Europa del Norte
- Reino Unido Sur
- Oeste del Reino Unido
- Europa Occidental

América del Norte

- Canada Central
- Canadá este
- Estados Unidos Central

- Este de Estados Unidos
- EE.UU. Oriental 2
- Centro Norte de Estados Unidos
- Centro Sur de EE. UU
- Oeste de EE. UU
- Oeste de EE.UU. 2
- Centro Oeste de Estados Unidos

Sudamérica

- Brasil Sur

Clases y regiones de almacenamiento compatibles con Google Cloud

Cloud Tiering admite la clase de almacenamiento estándar y la mayoría de las regiones de Google Cloud.

Niveles de acceso compatibles

Cloud Tiering usa el nivel de acceso *Standard* para sus datos inactivos.

Regiones compatibles de Google Cloud

Cloud Tiering admite las siguientes regiones.

América

- Iowa
- Los Ángeles
- Montreal
- N. Virginia
- Oregón
- Sao Paulo
- Carolina del Sur

Asia-Pacífico

- Hong Kong
- Bombay
- Osaka
- Singapur
- Sídney
- Taiwán
- Tokio

Europa

- Bélgica
- Finlandia
- Frankfurt
- Londres
- Países Bajos
- Zurich

Ver los bloques de Amazon S3

Después de instalar un conector en AWS, Cloud Manager puede detectar automáticamente información sobre los bloques de Amazon S3 que residen en la cuenta de AWS en la que está instalado.

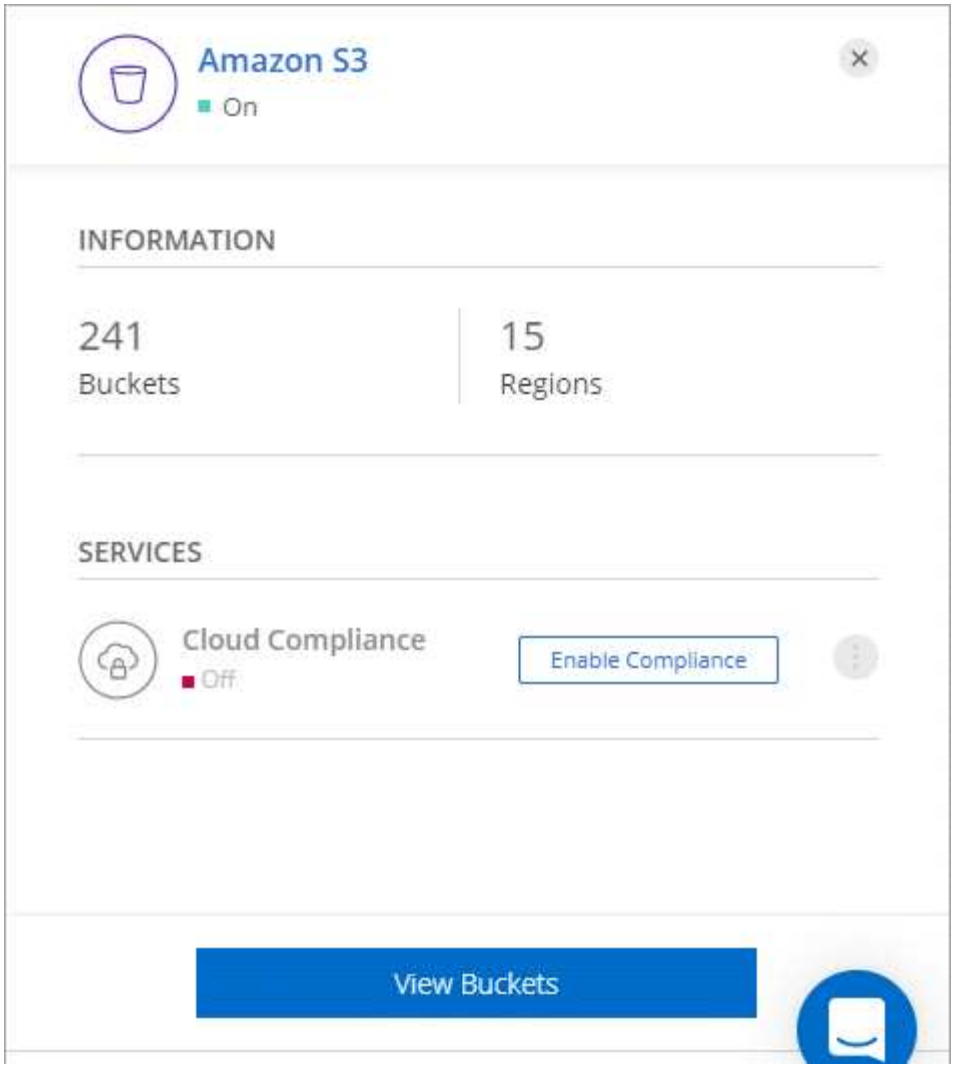
Puede ver detalles sobre sus bloques de S3, incluida la región, el nivel de acceso, la clase de almacenamiento y si el bloque se utiliza con Cloud Volumes ONTAP para backups o la organización en niveles de datos. Además, puede analizar los cubos de S3 con Cloud Compliance.

Pasos

1. "Instale un conector" En la cuenta de AWS, donde desea ver sus bloques de Amazon S3.

   Verá automáticamente un entorno de trabajo de Amazon S3 poco después.

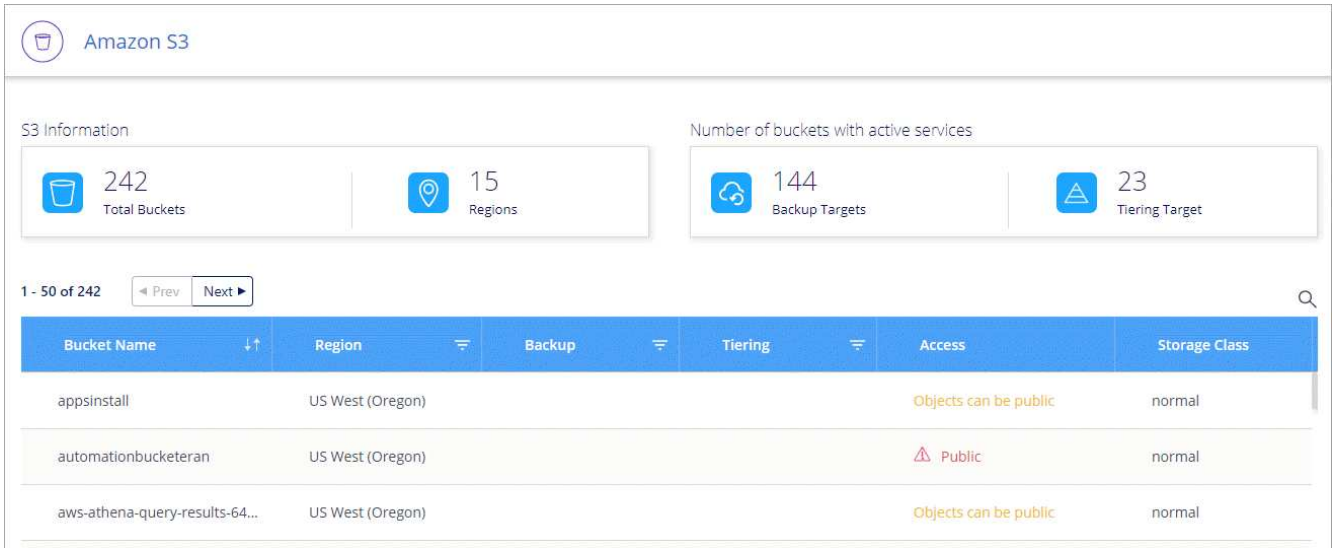
2. Haga clic en el entorno de trabajo y seleccione una acción en el panel derecho.



3. Haga clic en **Activar cumplimiento** para analizar los bloques S3 en busca de datos personales y confidenciales.

   Para obtener información detallada, consulte "Introducción a Cloud Compliance para Amazon S3".

4. Haga clic en **Ver cucharones** para ver detalles sobre los bloques S3 de su cuenta de AWS.



Administre Cloud Manager

Buscar el ID del sistema de Cloud Manager

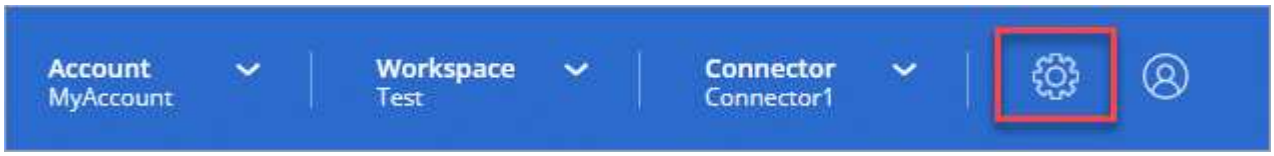
Para ayudarle a comenzar, su representante de NetApp puede pedirle el ID de sistema de Cloud Manager. El ID se utiliza normalmente para licencias y solución de problemas.

Lo que necesitará

Debe crear un conector antes de poder cambiar la configuración de Cloud Manager. "Vea cómo".

Pasos

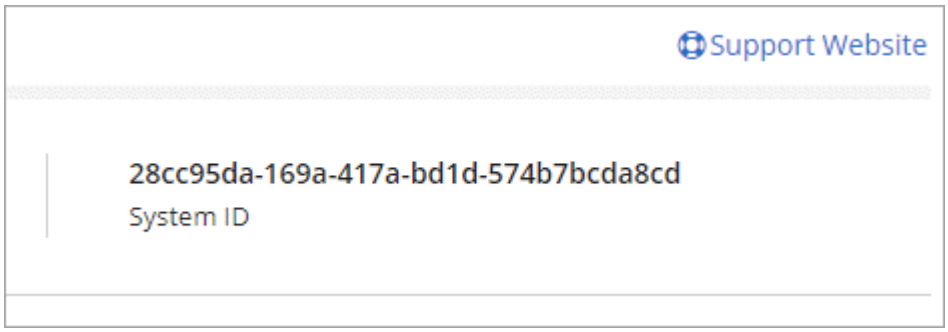
1. En la esquina superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración.



2. Haga clic en **Panel de soporte**.

   El ID del sistema aparece en la parte superior derecha.

   ejemplo



Gestionar conectores

Gestión de conectores existentes

Después de crear uno o más conectores, puede gestionarlos cambiando entre conectores, conectándose a la interfaz de usuario local que se ejecuta en un conector, entre otros.

Cambio entre conectores

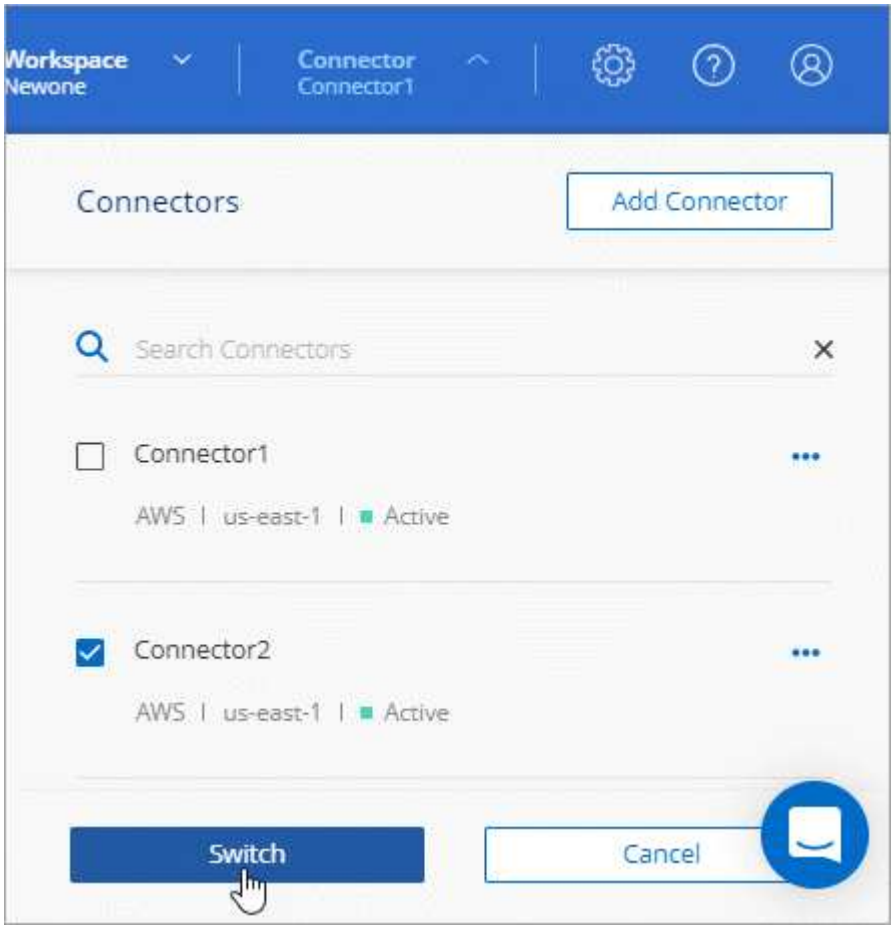
Si tiene varios conectores, puede alternar entre ellos para ver los entornos de trabajo asociados a un conector específico.

Por ejemplo, digamos que trabaja en un entorno multicloud. Es posible que tenga un conector en AWS y otro en Google Cloud. Tendría que cambiar entre estos conectores para gestionar los sistemas Cloud Volumes

ONTAP que se ejecutan en esas nubes.

Paso

1. Haga clic en el menú desplegable **conector**, seleccione otro conector y, a continuación, haga clic en **conmutador**.



Cloud Manager actualiza y muestra los entornos de trabajo asociados con el conector seleccionado.

Obtener acceso a la interfaz de usuario local

Aunque debe realizar casi todas las tareas desde la interfaz de usuario de SaaS, todavía hay disponible una interfaz de usuario local en el conector. Esta interfaz es necesaria para algunas tareas que se deben realizar desde el propio conector:

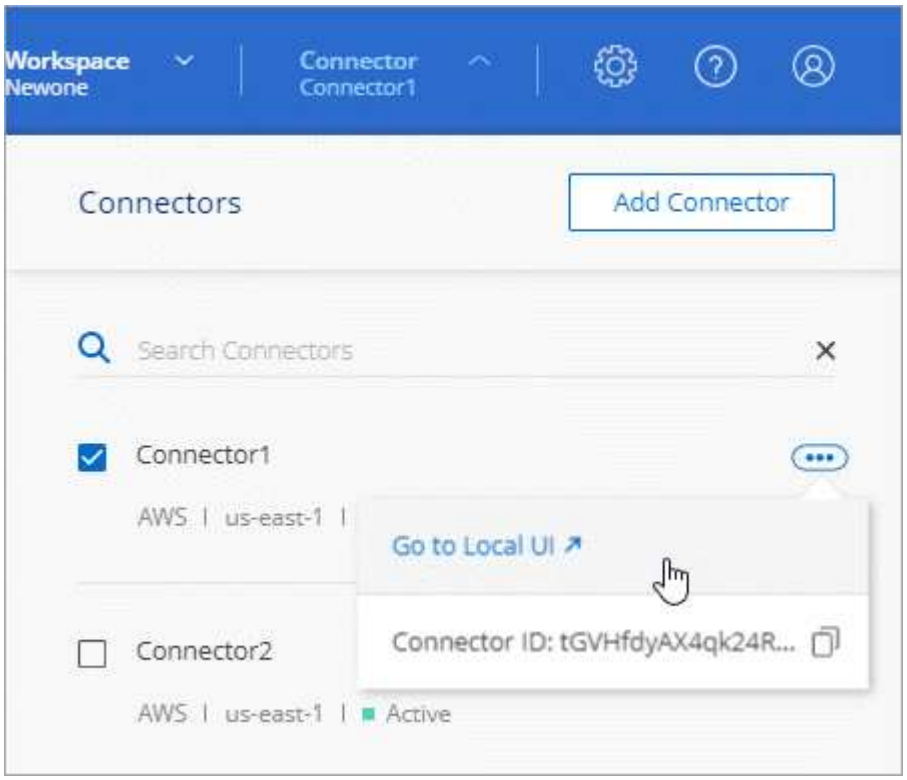
- "Establecimiento de un servidor proxy"
- Instalación de un parche (Normalmente, trabajará con el personal de NetApp para instalar un parche).
- Descargando mensajes de AutoSupport (Normalmente dirigido por el personal de NetApp cuando tiene problemas)

Pasos

1. "Inicie sesión en la interfaz del SaaS de Cloud Manager" Desde un equipo que tiene una conexión de red a la instancia de conector.

   Si el conector no tiene una dirección IP pública, necesitará una conexión VPN o deberá conectarse desde un host de salto que esté en la misma red que el conector.

2. Haga clic en el menú desplegable **conector**, haga clic en el menú de acción de un conector y, a continuación, haga clic en **Ir a interfaz de usuario local**.



La interfaz de Cloud Manager que se ejecuta en el conector se carga en una nueva pestaña del navegador.

Quitando conectores de Cloud Manager

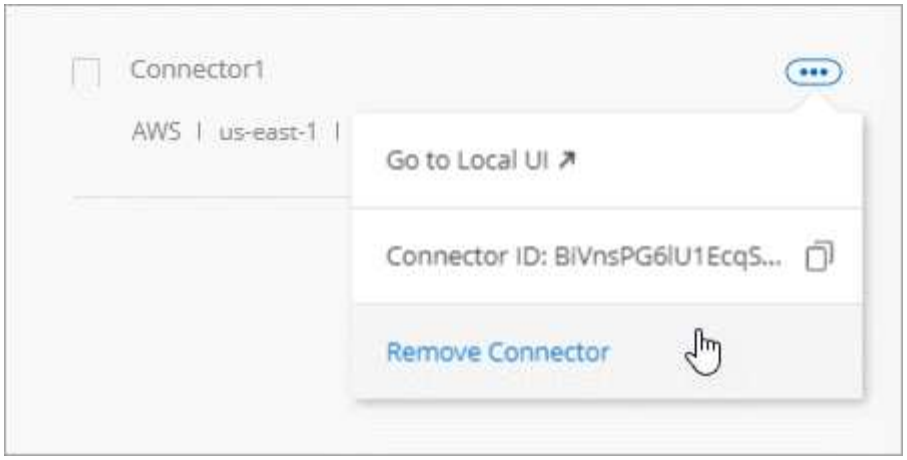
Si un conector está inactivo, puede quitarlo de la lista de conectores de Cloud Manager. Puede hacerlo si ha eliminado la máquina virtual conector o si ha desinstalado el software conector.

Tenga en cuenta lo siguiente sobre la extracción de un conector:

- Esta acción no elimina la máquina virtual.
- No se puede revertir esta acción. Una vez que se quita un conector de Cloud Manager, no se puede volver a añadir a Cloud Manager.

Pasos

1. Haga clic en el menú desplegable conector del encabezado Cloud Manager.
2. Haga clic en el menú de acción de un conector inactivo y haga clic en **Quitar conector**.



3. Introduzca el nombre del conector que desea confirmar y, a continuación, haga clic en Quitar.

Resultado

Cloud Manager quita el conector de sus registros.

Desinstalación del software del conector

El conector incluye una secuencia de comandos de desinstalación que puede utilizar para desinstalar el software para solucionar problemas o para quitar permanentemente el software del host.

Paso

1. Desde el host Linux, ejecute el script de desinstalación:

   /opt/application/netapp/cloudmanager/bin/uninstall.sh [silent]

   silent ejecuta la secuencia de comandos sin que se le solicite confirmación.

¿y las actualizaciones de software?

El conector actualiza automáticamente su software a la última versión, siempre que lo haya hecho "acceso a internet de salida" para obtener la actualización de software.

Más formas de crear conectores

Requisitos del host del conector

El software del conector debe ejecutarse en un host que cumpla con requisitos específicos del sistema operativo, requisitos de RAM, requisitos de puerto, etc.

Se requiere un host dedicado

El conector no es compatible con un host compartido con otras aplicaciones. El host debe ser un host dedicado.

CPU

4 núcleos o 4 vCPU

RAM

14 GB

Tipo de instancia de AWS EC2

Tipo de instancia que cumple los requisitos anteriores de CPU y RAM. Recomendamos t3.xlarge y el uso de ese tipo de instancia al implementar el conector directamente desde Cloud Manager.

Tamaño de la máquina virtual de Azure

Tipo de instancia que cumple los requisitos anteriores de CPU y RAM. Recomendamos DS3 v2 y utilizar ese tamaño de equipo virtual al implementar el conector directamente desde Cloud Manager.

Tipo de máquina GCP

Tipo de instancia que cumple los requisitos anteriores de CPU y RAM. Le recomendamos n1-standard-4 y utilizar ese tipo de máquina cuando ponga en marcha el conector directamente desde Cloud Manager.

Sistemas operativos compatibles

- CentOS 7.6
- CentOS 7.7
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7

  El sistema Red Hat Enterprise Linux debe estar registrado con Red Hat Subscription Management. Si no está registrado, el sistema no puede acceder a los repositorios para actualizar el software necesario de terceros durante la instalación del conector.

  El conector es compatible con las versiones en inglés de estos sistemas operativos.

Hipervisor

Un hipervisor de configuración básica o alojado certificado Ejecute CentOS o Red Hat Enterprise Linuxhttps://access.redhat.com/certified-hypervisors["Red Hat Solution: ¿Qué hipervisores están certificados para ejecutar Red Hat Enterprise Linux?"^]

Espacio en disco en /opt

Debe haber 100 GB de espacio disponibles

Acceso a Internet de salida

Se requiere acceso saliente a Internet para instalar el conector y el conector para gestionar recursos y procesos dentro de su entorno de cloud público. Para ver una lista de extremos, consulte "Requisitos de red para el conector".

Creación de un conector desde AWS Marketplace

Es mejor crear un conector directamente desde Cloud Manager, pero puede iniciar un conector desde AWS Marketplace, si prefiere no especificar claves de acceso de AWS. Después de crear y configurar el conector, Cloud Manager lo utilizará automáticamente al crear nuevos entornos de trabajo.

Pasos

1. Crear una política de IAM y un rol para la instancia de EC2:

a. Descargue la política de IAM de Cloud Manager desde la siguiente ubicación:

   "NetApp Cloud Manager: Políticas de AWS, Azure y GCP"

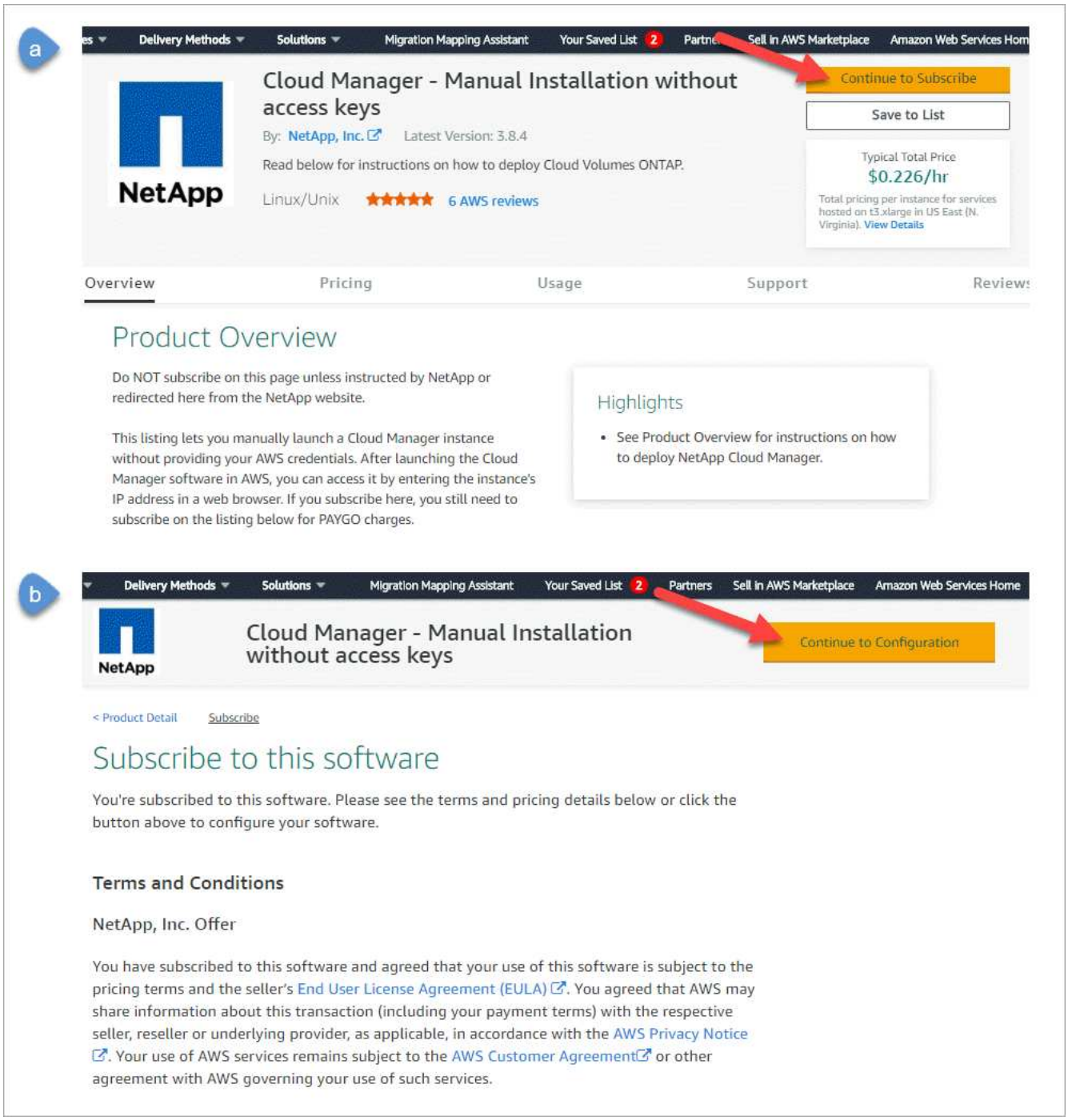
b. Desde la consola de IAM, cree su propia política copiando y pegando el texto de la política IAM de Cloud Manager.

c. Cree un rol IAM con el tipo de rol Amazon EC2 y asocie la política que ha creado en el paso anterior al rol.

2. Ahora vaya a la "Cloud Manager en el mercado de AWS" Para poner en marcha Cloud Manager desde una AMI.

   El usuario de IAM debe disponer de permisos de AWS Marketplace para suscribirse y cancelar la suscripción.

3. En la página Marketplace, haga clic en **continuar a Suscribirse** y luego haga clic en **continuar a Configuración**.



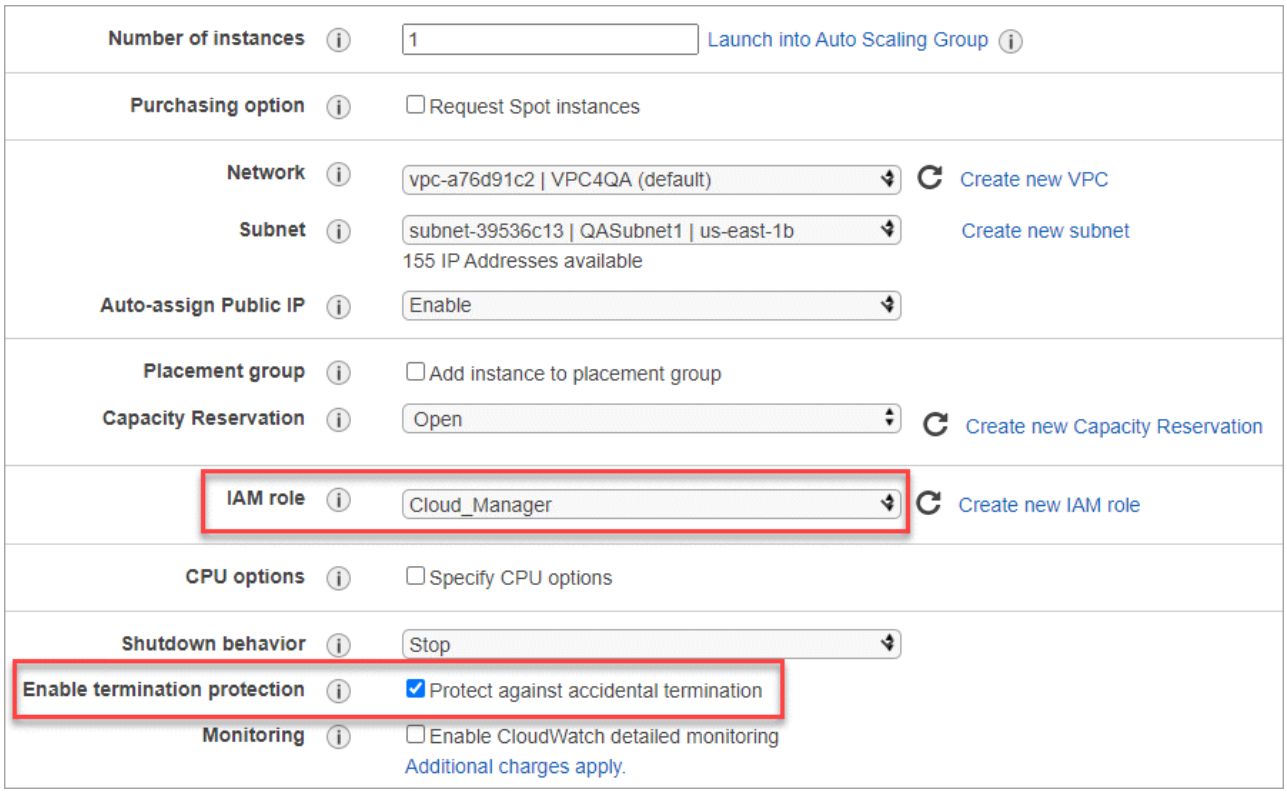
4. Cambie cualquiera de las opciones predeterminadas y haga clic en **continuar a Iniciar**.
5. En **elegir acción**, seleccione **Iniciar a través de EC2** y, a continuación, haga clic en **Iniciar**.

   Estos pasos describen cómo iniciar la instancia desde la consola EC2 porque la consola permite asociar un rol IAM a la instancia de Cloud Manager. Esto no es posible usando la acción **Iniciar desde el sitio web**.

6. Siga las instrucciones para configurar y desplegar la instancia:
   - **elegir tipo de instancia**: En función de la disponibilidad de la región, elija uno de los tipos de instancia admitidos (se recomienda t3.xlarge).

     "Revise los requisitos de la instancia".

- **Configurar instancia**: Seleccione un VPC y una subred, elija la función de IAM que creó en el paso 1, habilite la protección de terminación (recomendado) y elija cualquier otra opción de configuración que cumpla sus requisitos.



- **almacenamiento**: Mantenga las opciones de almacenamiento predeterminadas.
- **Agregar etiquetas**: Introduzca etiquetas para la instancia, si lo desea.
- **Configurar grupo de seguridad**: Especifique los métodos de conexión necesarios para la instancia de conector: SSH, HTTP y HTTPS.
- **Revisión**: Revise sus selecciones y haga clic en **Iniciar**.

  AWS inicia el software con la configuración especificada. La instancia y el software del conector deben estar funcionando en aproximadamente cinco minutos.

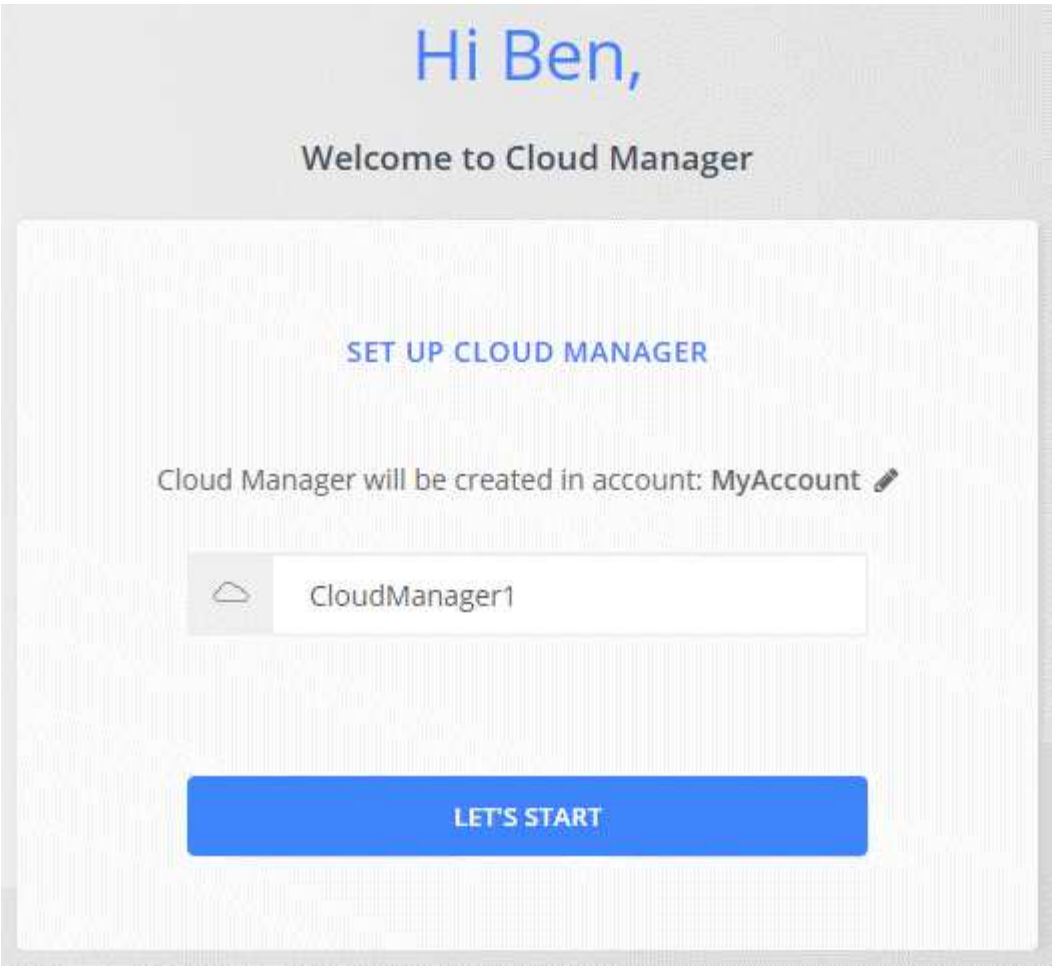
7. Abra un explorador Web desde un host que tenga una conexión con la instancia de Connector e introduzca la siguiente URL:

   http://ipaddress:80

8. Después de iniciar sesión, configure el conector:
   a. Especifique la cuenta de Cloud Central que desea asociar con el conector.

      "Obtenga más información acerca de las cuentas de Cloud Central".

   b. Escriba un nombre para el sistema.



Resultado

El conector ya está instalado y configurado con su cuenta de Cloud Central. Cloud Manager utilizará automáticamente este conector cuando cree nuevos entornos de trabajo. Pero si tiene más de un conector, necesitará "alterne entre ellos".

Creación de un conector desde Azure Marketplace

Es mejor crear un conector directamente desde Cloud Manager, pero si lo prefiere, puede iniciar un conector desde Azure Marketplace. Después de crear y configurar el conector, Cloud Manager lo utilizará automáticamente al crear nuevos entornos de trabajo.

Creación de un conector en Azure

Implemente el conector en Azure con la imagen en Azure Marketplace y luego inicie sesión en el conector para especificar su cuenta de Cloud Central.

Pasos

1. "Vaya a la página de Azure Marketplace para Cloud Manager".
2. Haga clic en **Get Now** y, a continuación, haga clic en **Continue**.
3. En el portal de Azure, haga clic en **Crear** y siga los pasos para configurar la máquina virtual.

   Tenga en cuenta lo siguiente al configurar la máquina virtual:

- Cloud Manager puede ofrecer un rendimiento óptimo tanto con discos HDD como SSD.
- Elija un tamaño de máquina virtual que cumpla los requisitos de CPU y RAM. Recomendamos DS3 v2.

  "Revise los requisitos de las máquinas virtuales".

- Para el grupo de seguridad de red, el conector requiere conexiones entrantes mediante SSH, HTTP y HTTPS.

  "Obtenga más información sobre las reglas de grupo de seguridad para el conector".

- En **Gestión**, active **identidad administrada asignada por el sistema** para el conector seleccionando **On**.

  Esta configuración es importante porque una identidad administrada permite que la máquina virtual Connector se identifique a sí misma en Azure Active Directory sin proporcionar credenciales. "Obtenga más información sobre las identidades gestionadas para recursos de Azure".

4. En la página **revisar + crear**, revise las selecciones y haga clic en **Crear** para iniciar la implementación.

   Azure implementa la máquina virtual con los ajustes especificados. El software de la máquina virtual y el conector debe estar funcionando en aproximadamente cinco minutos.

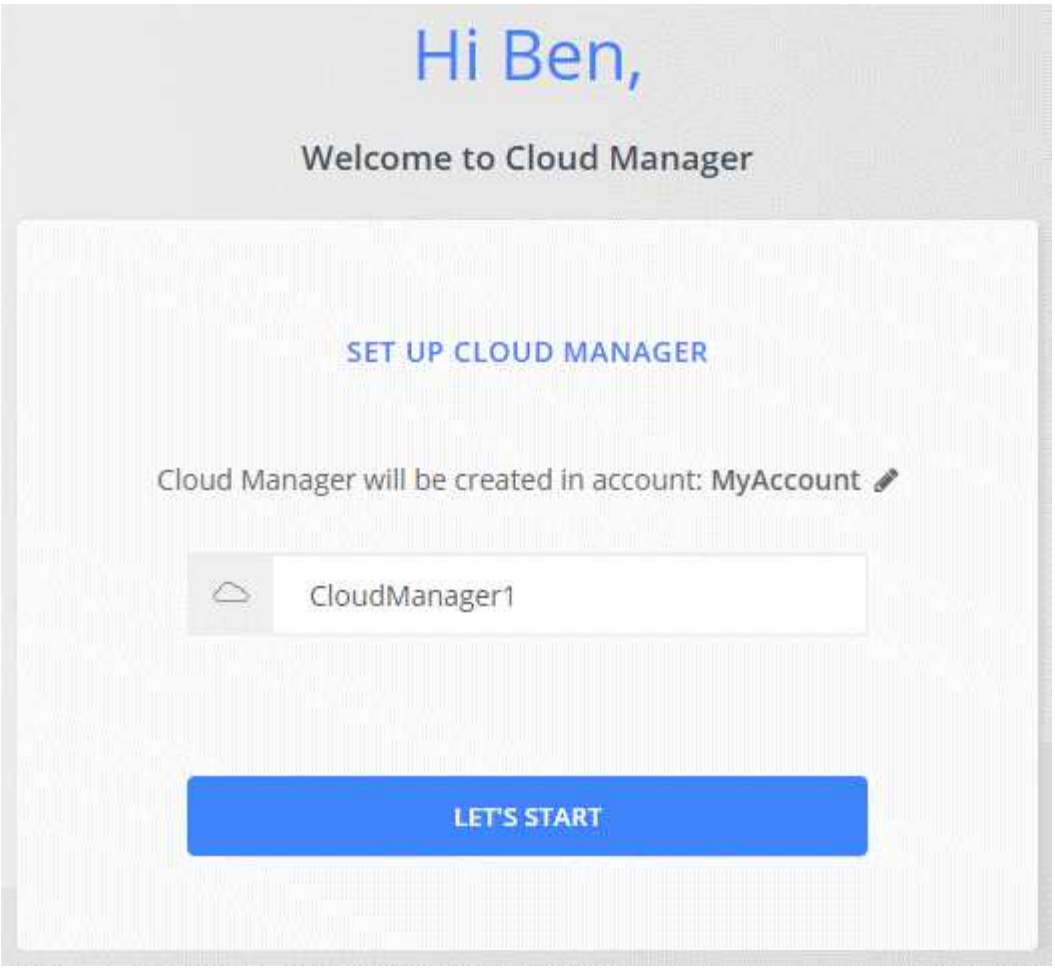
5. Abra un explorador Web desde un host que tenga una conexión con la máquina virtual Connector e introduzca la siguiente URL:

   http://ipaddress:80

6. Después de iniciar sesión, configure el conector:
   a. Especifique la cuenta de Cloud Central que desea asociar con el conector.

      "Obtenga más información acerca de las cuentas de Cloud Central".

   b. Escriba un nombre para el sistema.



Resultado

El conector ahora está instalado y configurado. Debe conceder permisos de Azure para que los usuarios puedan poner en marcha Cloud Volumes ONTAP en Azure.

Concesión de permisos de Azure

Cuando implementó Connector en Azure, debería haber habilitado un "identidad administrada asignada por el sistema". Ahora debe conceder los permisos de Azure necesarios creando una función personalizada y, a continuación, asignando la función a la máquina virtual Connector para una o más suscripciones.

Pasos

1. Cree un rol personalizado mediante la política de Cloud Manager:

   a. Descargue el "Política de Azure de Cloud Manager".

   b. Modifique el archivo JSON agregando ID de suscripción de Azure al ámbito asignable.

      Debe añadir el ID para cada suscripción de Azure desde la cual los usuarios crearán sistemas Cloud Volumes ONTAP.

      ejemplo

      "AssignableScopes": ["/subscripciones/d333af45-0d07-4154-943d-c25fbzzzzzzz", "/subscripciones/54b91999-b3e6-4599-908e-416e0zzzzzzz", "/subscripciones/398e471c-3bzb6b6b6b3b6bbb3bzb6b6b3b6b3bb6b3b6x-b6b6b3bb

c. Use el archivo JSON para crear una función personalizada en Azure.

   El ejemplo siguiente muestra cómo crear una función personalizada con la CLI de Azure 2.0:

   ```
   az role definition create --role-definition
   C:\Policy_for_cloud_Manager_Azure_3.8.7.json
   ```

Ahora debe tener un rol personalizado denominado operador de Cloud Manager que puede asignar a la máquina virtual conector.

2. Asigne el rol a la máquina virtual conector para una o más suscripciones:
   a. Abra el servicio **Suscripciones** y seleccione la suscripción en la que desea implementar sistemas Cloud Volumes ONTAP.
   b. Haga clic en **Control de acceso (IAM)**.
   c. Haga clic en **Agregar** > **Agregar asignación de rol** y, a continuación, agregue los permisos:
      - Seleccione el rol **operador de Cloud Manager**.

        Es el nombre predeterminado que se proporciona en la "Política de Cloud Manager". Si seleccionó otro nombre para el rol, seleccione ese nombre.

      - Asigne acceso a una **máquina virtual**.
      - Seleccione la suscripción en la que se creó la máquina virtual Connector.
      - Seleccione la máquina virtual conector.
      - Haga clic en **Guardar**.
   d. Si desea implementar Cloud Volumes ONTAP desde suscripciones adicionales, cambie a esa suscripción y repita estos pasos.

Resultado

Connector ahora tiene los permisos que necesita para gestionar recursos y procesos en su entorno de cloud público. Cloud Manager utilizará automáticamente este conector cuando cree nuevos entornos de trabajo. Pero si tiene más de un conector, necesitará "alterne entre ellos".

Instalar el software del conector en un host Linux existente

La forma más común de crear un conector es directamente desde Cloud Manager o desde el mercado de un proveedor de cloud. Pero tiene la opción de descargar e instalar el software Connector en un host Linux existente en su red o en la nube.

Si desea crear un sistema Cloud Volumes ONTAP en Google Cloud, también debe tener un conector en Google Cloud. No puede utilizar un conector que se ejecute en otra ubicación.

Requisitos

- El host debe encontrarse "Requisitos para el conector".
- Debe registrarse un sistema Red Hat Enterprise Linux con Red Hat Subscription Management. Si no está registrado, el sistema no puede acceder a los repositorios para actualizar el software necesario de terceros durante la instalación.
- El instalador del conector tiene acceso a varias direcciones URL durante el proceso de instalación. Debe asegurarse de que se permita el acceso saliente a Internet a estos puntos finales:

- http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm
- https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
- https://s3.amazonaws.com/aws-cli/awscli-bundle.zip

  Es posible que el host intente actualizar paquetes de sistema operativo durante la instalación. El host puede ponerse en contacto con diferentes sitios de duplicación para estos paquetes de SO.

Acerca de esta tarea

- No se requieren privilegios de usuario raíz para instalar el conector.
- La instalación instala las herramientas de línea de comandos de AWS (awscli) para habilitar los procedimientos de recuperación del soporte de NetApp.

  Si recibe un mensaje que ha fallado al instalar el awscli, puede ignorar el mensaje de forma segura. El conector puede funcionar correctamente sin las herramientas.

- El instalador disponible en el sitio de soporte de NetApp puede ser una versión anterior. Después de la instalación, el conector se actualiza automáticamente si hay una nueva versión disponible.

Pasos

1. Descargue el software Cloud Manager del "Sitio de soporte de NetApp"Y, a continuación, cópielo en el host Linux.

   Para obtener ayuda sobre la conexión y copia del archivo en una instancia de EC2 en AWS, consulte "Documentación de AWS: Conexión a la instancia de Linux mediante SSH".

2. Asigne permisos para ejecutar el script.

   ejemplo

   ```
    chmod +x OnCommandCloudManager-V3.8.4.sh
   . Ejecute el script de instalación:
   ```

   ```
   ./OnCommandCloudManager-V3.8.4.sh [silent] [proxy=ipaddress]
   [proxyport=port] [proxyuser=user_name] [proxypwd=password]
   ```

   silent ejecuta la instalación sin solicitar información.

   se requiere *proxy* si el host está detrás de un servidor proxy.

   proxyport es el puerto del servidor proxy.

   proxyuser es el nombre de usuario del servidor proxy, si se requiere autenticación básica.

   proxypwd es la contraseña del nombre de usuario que ha especificado.

3. A menos que haya especificado el parámetro silent, escriba **y** para continuar la secuencia de comandos y, a continuación, introduzca los puertos HTTP y HTTPS cuando se le solicite.

   Cloud Manager ya está instalado. Al finalizar la instalación, el servicio Cloud Manager (occm) se reinicia

dos veces si especificó un servidor proxy.

4. Abra un explorador web e introduzca la siguiente URL:

   https://ipaddress:port

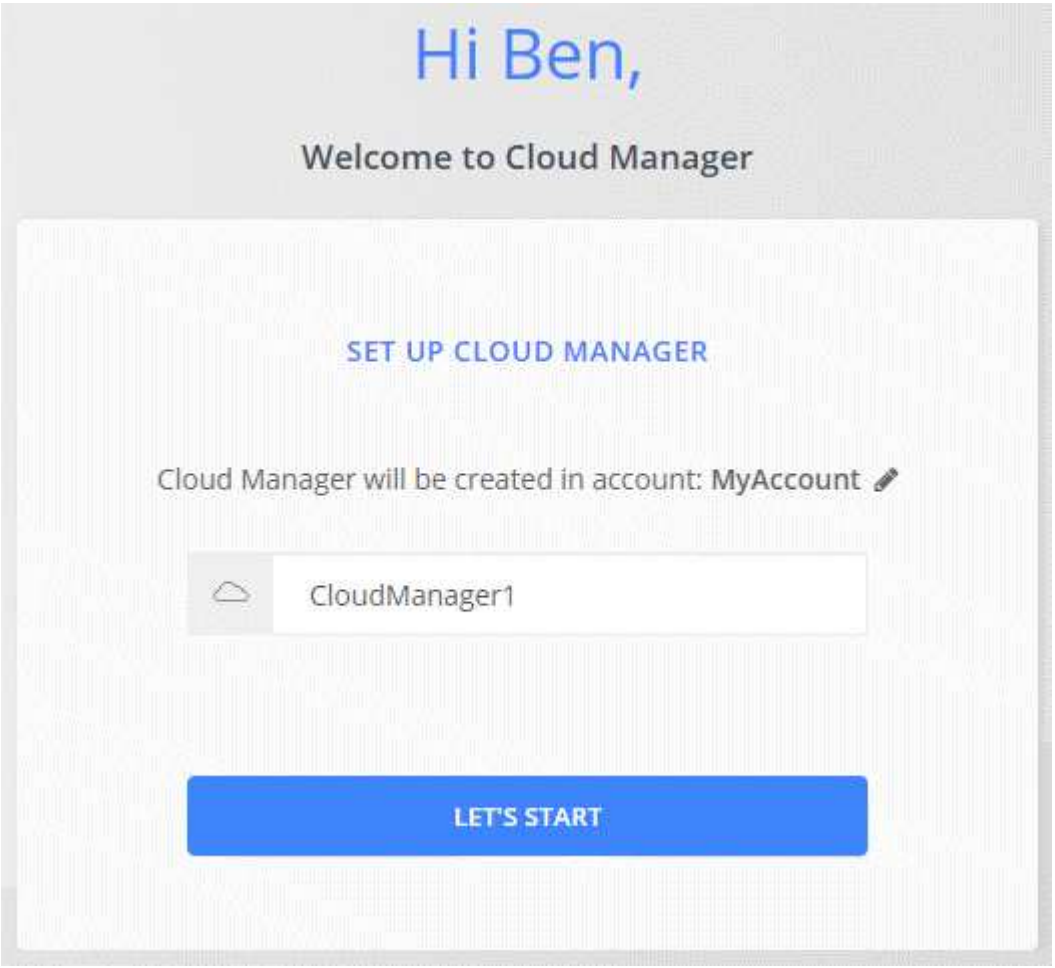
   ipaddress puede ser localhost, una dirección IP privada o una dirección IP pública, dependiendo de la configuración del host. Por ejemplo, si el conector está en la nube pública sin una dirección IP pública, debe introducir una dirección IP privada desde un host que tenga una conexión con el host del conector.

   Port es obligatorio si cambia los puertos HTTP (80) o HTTPS (443) predeterminados. Por ejemplo, si el puerto HTTPS se ha cambiado a 8443, debe introducir https://ipaddress:8443

5. Regístrese en NetApp Cloud Central o inicie sesión.
6. Después de iniciar sesión, configure Cloud Manager:
   a. Especifique la cuenta de Cloud Central que desea asociar con el conector.

      "Obtenga más información acerca de las cuentas de Cloud Central".

   b. Escriba un nombre para el sistema.



Resultado

El conector ya está instalado y configurado con su cuenta de Cloud Central. Cloud Manager utilizará automáticamente este conector cuando cree nuevos entornos de trabajo.

Después de terminar

Configure permisos para que Cloud Manager pueda gestionar recursos y procesos en su entorno de cloud público:

- AWS: "Configure una cuenta de AWS y, a continuación, añádela Cloud Manager".
- Azure: "Configure una cuenta de Azure y añada a. Cloud Manager".
- GCP: Configure una cuenta de servicio que tenga los permisos que Cloud Manager necesita para crear y gestionar sistemas Cloud Volumes ONTAP en proyectos.
  a. "Crear un rol en GCP" esto incluye los permisos definidos en la "Política de Cloud Manager para GCP".
  b. "Cree una cuenta de servicio de GCP y aplique el rol personalizado que acaba de crear".
  c. "Asocie esta cuenta de servicio a la máquina virtual del conector".
  d. Si desea poner en marcha Cloud Volumes ONTAP en otros proyectos, "Conceda el acceso añadiendo la cuenta de servicio con la nube La función de gerente de ese proyecto". Deberá repetir este paso con cada proyecto.

Configuración predeterminada del conector

Si necesita solucionar problemas del conector, puede ser útil entender cómo está configurado.

- Si puso en marcha el conector desde Cloud Manager (o directamente desde el mercado de un proveedor de cloud), tenga en cuenta lo siguiente:
  - En AWS, el nombre de usuario de la instancia de EC2 Linux es ec2-user.
  - El sistema operativo de la imagen es el siguiente:
    - AWS: Red Hat Enterprise Linux 7.5 (HVM)
    - Azure: Red Hat Enterprise Linux 7.6 (HVM)
    - GCP: CentOS 7.6

      El sistema operativo no incluye una GUI. Debe utilizar un terminal para acceder al sistema.
- La carpeta de instalación del conector se encuentra en la siguiente ubicación:

  /opt/aplicación/netapp/cloudmanager
- Los archivos de registro se encuentran en la siguiente carpeta:

  /opt/application/netapp/cloudmanager/log
- El servicio Cloud Manager se llama occm.
- El servicio occm depende del servicio MySQL.

  Si el servicio MySQL está inactivo, entonces el servicio occm también está inactivo.
- Cloud Manager instala los siguientes paquetes en el host Linux, si no están ya instalados:

- 7zip
- AWSCLI
- Docker
- Java
- Kubectl
- MySQL
- Tridentctl
- Tire
- Consiga

- El conector utiliza los siguientes puertos en el host Linux:
  - 80 para acceso HTTP
  - 443 para acceso HTTPS
  - 3306 para la base de datos de Cloud Manager
  - 8080 para el proxy de API de Cloud Manager
  - 8666 para la API de Service Manager
  - 8777 para la API de servicio de contenedores Health-Checker

Gestionar credenciales

AWS

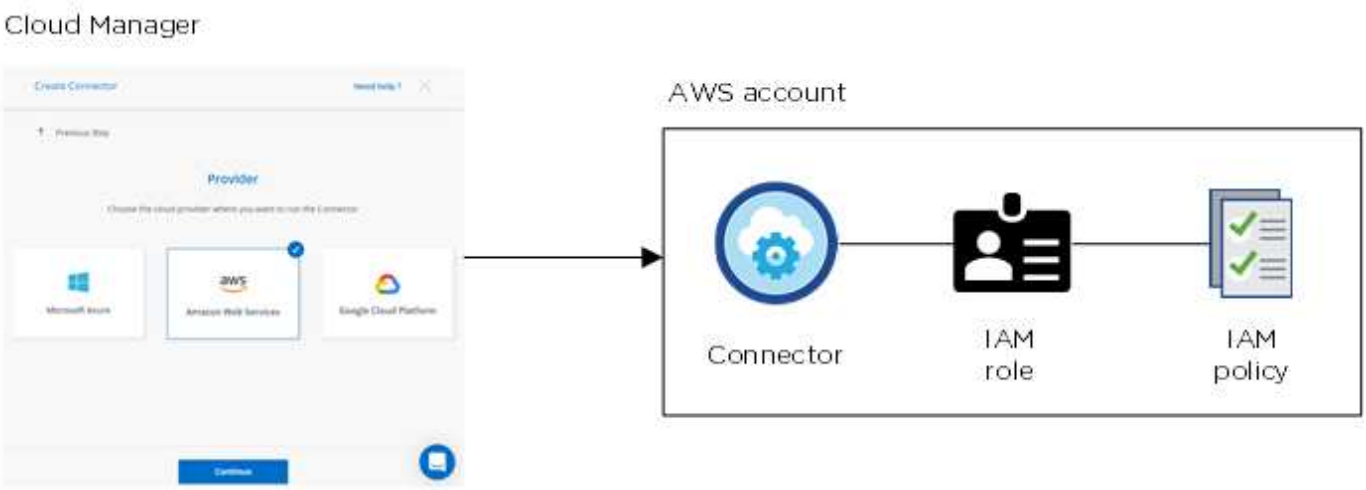
Credenciales y permisos de AWS

Cloud Manager le permite elegir las credenciales de AWS que desea utilizar al implementar Cloud Volumes ONTAP. Puede implementar todos sus sistemas Cloud Volumes ONTAP con las credenciales iniciales de AWS o bien añadir credenciales adicionales.

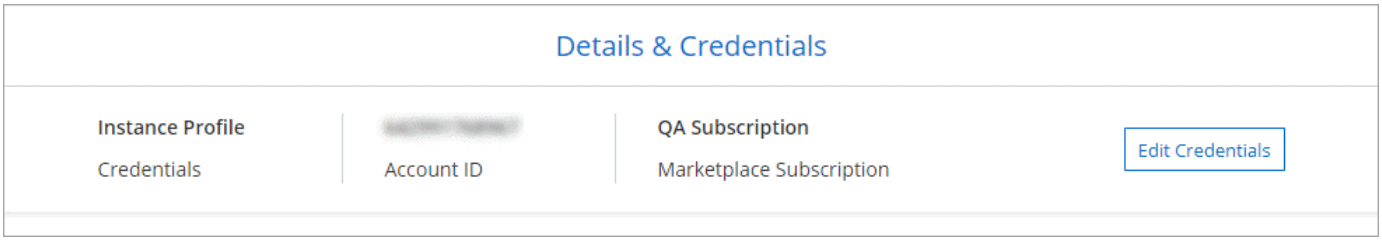
Credenciales iniciales de AWS

Al implementar un conector desde Cloud Manager, necesita utilizar una cuenta de AWS que tenga permisos para ejecutar la instancia de Connector. Los permisos necesarios se enumeran en la "La política de implementación de conectores para AWS".

Cuando Cloud Manager inicia la instancia de Connector en AWS, crea un rol IAM y un perfil de instancia para la instancia. También une una política que ofrece permisos para gestionar recursos y procesos dentro de esa cuenta de AWS. "Revise cómo Cloud Manager utiliza los permisos".

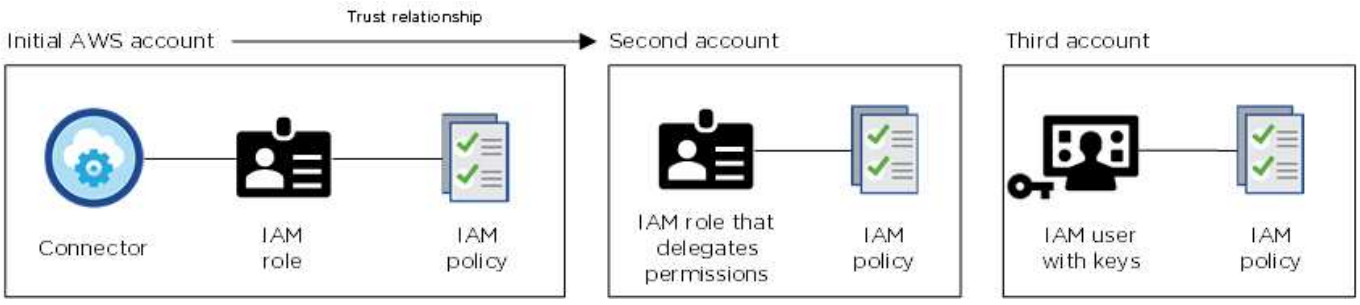


Cloud Manager selecciona estas credenciales de AWS de forma predeterminada al crear un entorno de trabajo nuevo para Cloud Volumes ONTAP:



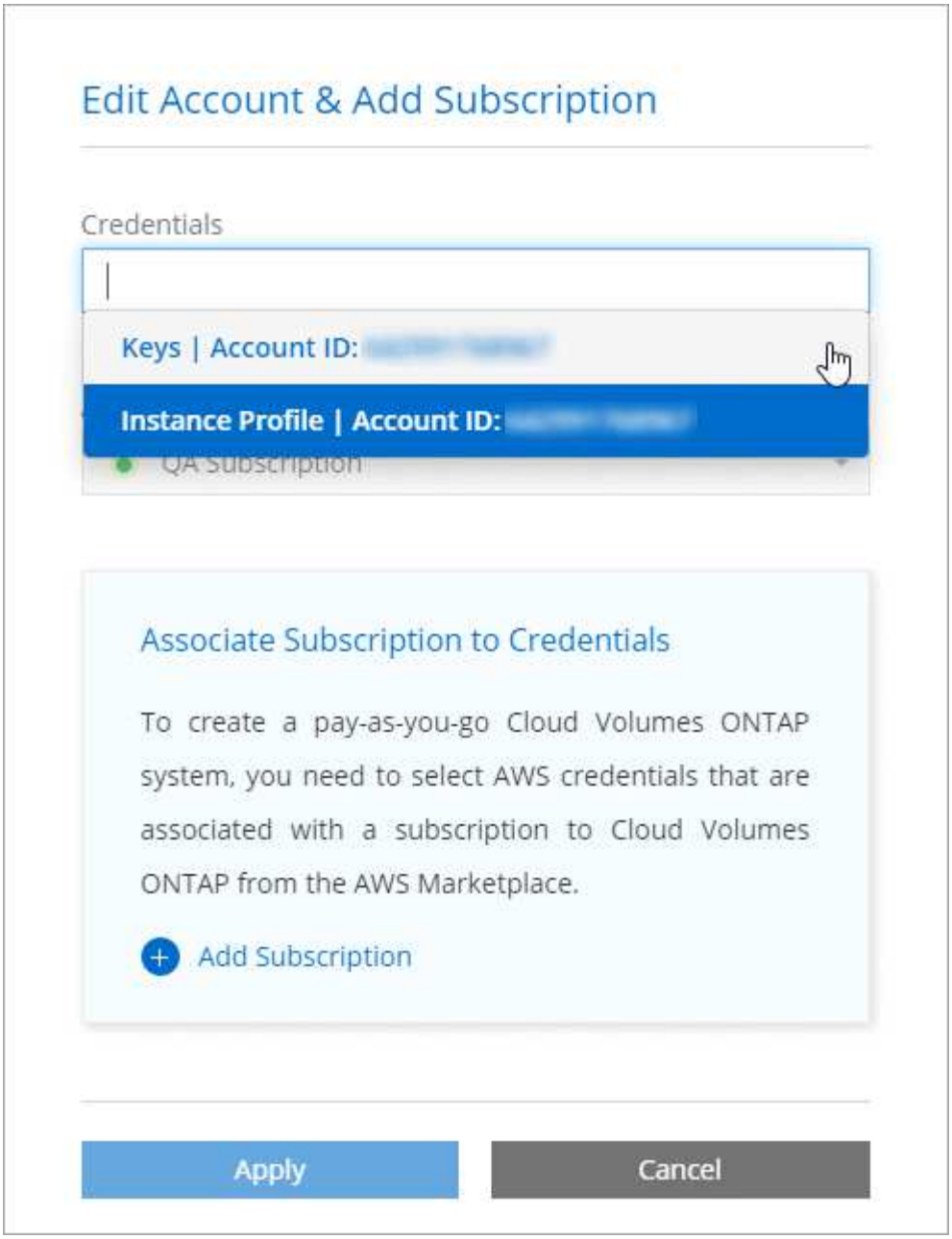
Credenciales adicionales de AWS

Si desea ejecutar Cloud Volumes ONTAP en diferentes cuentas de AWS, puede hacerlo también "Proporcione las claves AWS para un usuario de IAM o el ARN de un rol en una cuenta de confianza". En la siguiente imagen se muestran dos cuentas adicionales, una que proporciona permisos a través de una función IAM en una cuenta de confianza y otra a través de las claves AWS de un usuario de IAM:



Entonces lo haría "Añada las credenciales de la cuenta a Cloud Manager" Especificando el nombre de recurso de Amazon (ARN) del rol de IAM o las claves de AWS del usuario de IAM.

Después de añadir otro conjunto de credenciales, puede cambiar a ellas al crear un nuevo entorno de trabajo:



¿Qué pasa con las puestas en marcha de Marketplace y las puestas en marcha en las instalaciones?

En las secciones anteriores se describe el método de implementación recomendado para el conector, que es de Cloud Manager. También puede implementar un conector en AWS desde el "Mercado AWS" y usted puede "Instale el conector en las instalaciones".

Si utiliza el Marketplace, los permisos se proporcionan de la misma manera. Solo tiene que crear y configurar manualmente el rol IAM y, a continuación, proporcionar permisos para cualquier cuenta adicional.

En el caso de las implementaciones locales, no se puede configurar la función de IAM para el sistema Cloud Manager, pero se pueden proporcionar permisos del mismo modo que se busca para cuentas de AWS adicionales.

¿Cómo puedo rotar mis credenciales de AWS de forma segura?

Como se ha descrito anteriormente, Cloud Manager permite proporcionar credenciales de AWS de varias

maneras: Una función IAM asociada con la instancia de Connector, asumiendo un rol IAM en una cuenta de confianza o proporcionando claves de acceso de AWS.

Con las dos primeras opciones, Cloud Manager utiliza AWS Security Token Service para obtener credenciales temporales que giran constantemente. Este proceso es la mejor práctica, es automático y seguro.

Si proporciona claves de acceso a Cloud Manager para AWS, debe rotar las claves se actualizan en Cloud Manager a un intervalo regular. Este es un proceso completamente manual.

Gestión de las credenciales y suscripciones de AWS para Cloud Manager

Al crear un sistema de Cloud Volumes ONTAP, debe seleccionar las credenciales y la suscripción de AWS para utilizarlas con ese sistema. Si administra varias suscripciones de AWS, puede asignar cada una de ellas a diferentes credenciales de AWS desde la página Credentials.

Antes de añadir las credenciales de AWS a Cloud Manager, tiene que proporcionar los permisos necesarios para esa cuenta. Los permisos permiten que Cloud Manager gestione recursos y procesos dentro de esa cuenta de AWS. La forma en la que proporcione los permisos depende de si desea proporcionar a Cloud Manager claves de AWS o el ARN del rol en una cuenta de confianza.

Cuando implementó un conector desde Cloud Manager, Cloud Manager agregó automáticamente credenciales de AWS para la cuenta en la que implementó el conector. Esta cuenta inicial no se agrega si instaló manualmente el software Connector en un sistema existente. "Obtenga más información acerca de los permisos y credenciales de AWS".

opciones

- Concesión de permisos proporcionando claves AWS
- Otorgar permisos asumiendo roles de IAM en otras cuentas

¿Cómo puedo rotar mis credenciales de AWS de forma segura?

Cloud Manager le permite proporcionar credenciales de AWS de varias maneras: Una función IAM asociada con la instancia de Connector, asumiendo un rol IAM en una cuenta de confianza o proporcionando claves de acceso de AWS. "Obtenga más información acerca de las credenciales y permisos de AWS".

Con las dos primeras opciones, Cloud Manager utiliza AWS Security Token Service para obtener credenciales temporales que giran constantemente. Este proceso es la mejor práctica, es automático y seguro.

Si proporciona claves de acceso a Cloud Manager para AWS, debe rotar las claves se actualizan en Cloud Manager a un intervalo regular. Este es un proceso completamente manual.

Concesión de permisos proporcionando claves AWS

Si desea proporcionar a Cloud Manager claves AWS para un usuario IAM, debe conceder los permisos necesarios a ese usuario. La política de IAM de Cloud Manager define las acciones y los recursos de AWS que se permite el uso de Cloud Manager.

Pasos

1. Descargue la política de IAM de Cloud Manager desde el "Directivas de Cloud Manager".
2. Desde la consola de IAM, cree su propia política copiando y pegando el texto de la política IAM de Cloud Manager.

   "Documentación de AWS: Crear políticas de IAM"

3. Asocie la política a un rol de IAM o a un usuario de IAM.
   - "Documentación de AWS: Crear roles de IAM"
   - "Documentación de AWS: Adición y eliminación de políticas de IAM"

Resultado

La cuenta ahora tiene los permisos necesarios. Ahora puede añadirlo a Cloud Manager.

Otorgar permisos asumiendo roles de IAM en otras cuentas

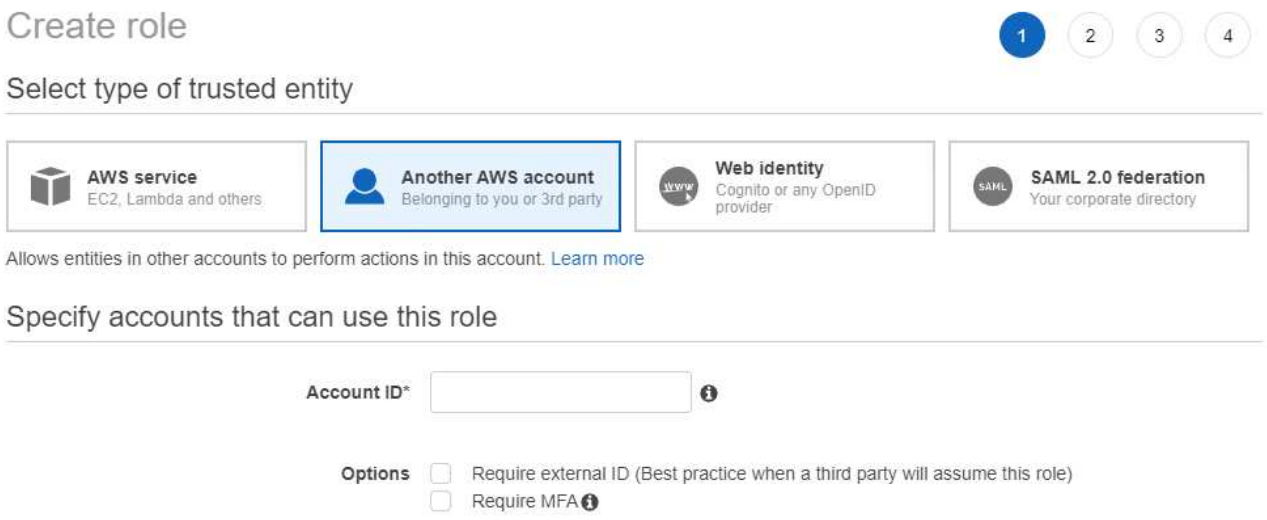
Puede configurar una relación de confianza entre la cuenta AWS de origen en la que ha implementado la instancia de Connector y otras cuentas de AWS mediante los roles IAM. A continuación, debe proporcionar a Cloud Manager el ARN de las funciones de IAM de las cuentas de confianza.

Pasos

1. Vaya a la cuenta de destino donde desea implementar Cloud Volumes ONTAP y cree una función IAM seleccionando **otra cuenta de AWS**.

   No olvide hacer lo siguiente:

   - Introduzca el código de la cuenta en la que reside la instancia de Connector.
   - Adjunte la política IAM de Cloud Manager, que está disponible en la "Directivas de Cloud Manager".



2. Vaya a la cuenta de origen en la que se encuentra la instancia de Connector y seleccione la función IAM asociada a la instancia.

   a. Haga clic en **Adjuntar directivas** y, a continuación, en **Crear directiva**.

   b. Cree una directiva que incluya la acción "sts:AssumeRole" y el ARN del rol que creó en la cuenta de destino.

ejemplo

```
{
 "Version": "2012-10-17",
 "Statement": {
   "Effect": "Allow",
   "Action": "sts:AssumeRole",
   "Resource": "arn:aws:iam::ACCOUNT-B-ID:role/ACCOUNT-B-ROLENAME"
}
}
```

Resultado

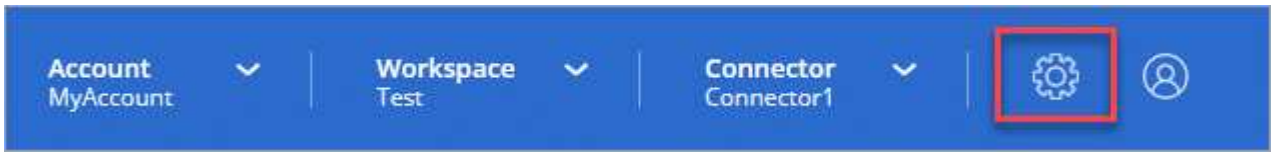
La cuenta ahora tiene los permisos necesarios. Ahora puede añadirlo a Cloud Manager.

Adición de credenciales de AWS a Cloud Manager

Después de proporcionar una cuenta de AWS con los permisos requeridos, puede añadir las credenciales para dicha cuenta a Cloud Manager. Esto le permite iniciar sistemas de Cloud Volumes ONTAP en esa cuenta.

Pasos

1. En la esquina superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **credenciales**.



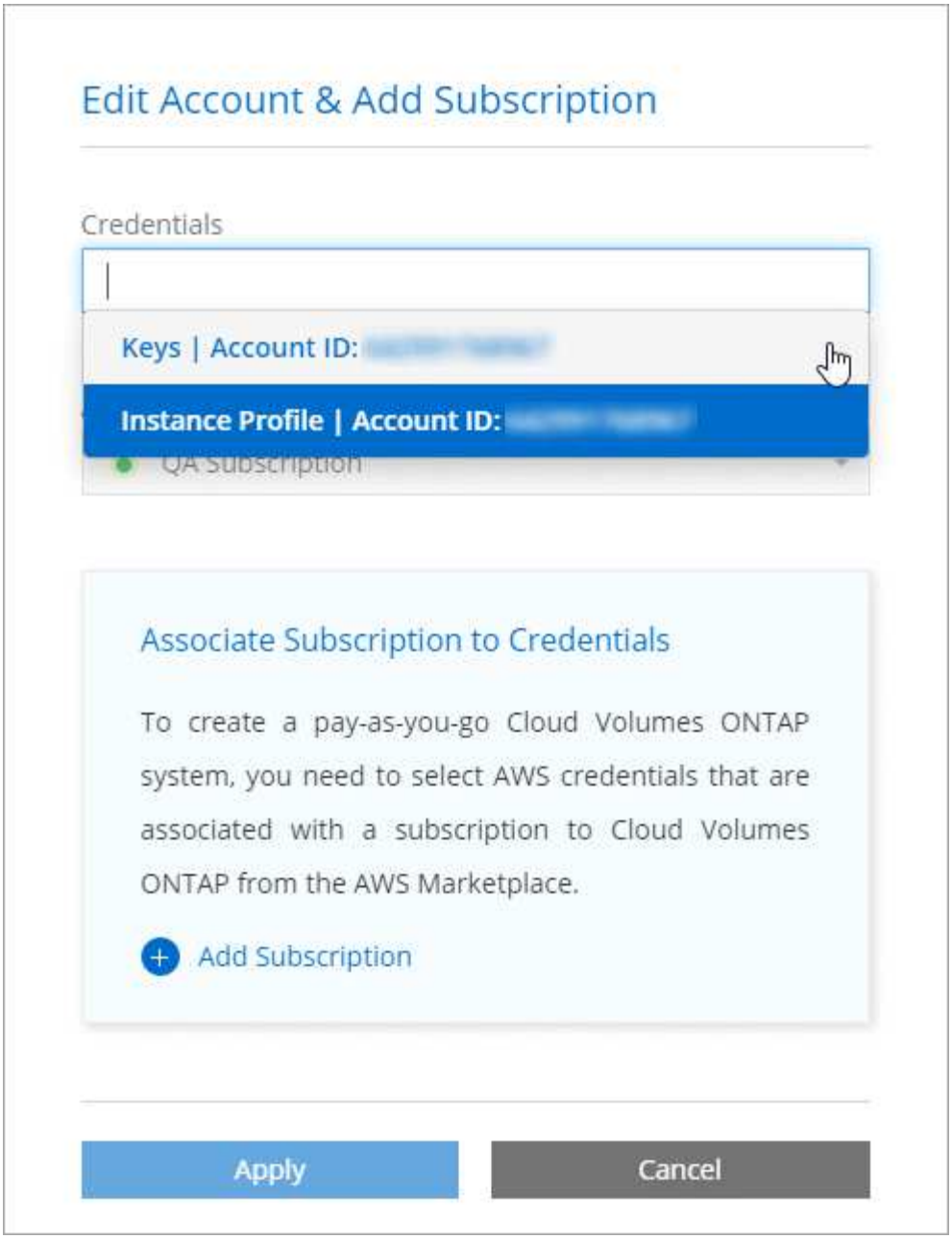
2. Haga clic en **Agregar credenciales** y seleccione **AWS**.
3. Proporcione las claves AWS o el ARN del rol de IAM de confianza.
4. Confirme que se han cumplido los requisitos de la directiva y haga clic en **continuar**.
5. Elija la suscripción de pago por uso que desee asociar con las credenciales o haga clic en **Agregar suscripción** si aún no tiene una.

   Para crear un sistema Cloud Volumes ONTAP de pago por uso, las credenciales de AWS deben estar asociadas con una suscripción a Cloud Volumes ONTAP desde AWS Marketplace.

6. Haga clic en **Agregar**.

Resultado

Ahora puede cambiar a un conjunto de credenciales diferente de la página Details y Credentials al crear un nuevo entorno de trabajo:



Asociación de una suscripción de AWS a credenciales

Después de añadir sus credenciales de AWS a Cloud Manager, puede asociar una suscripción a AWS Marketplace con estas credenciales. La suscripción le permite crear un sistema de pago por uso Cloud Volumes ONTAP y usar otros servicios cloud de NetApp.

Hay dos escenarios en los que puede asociar una suscripción a AWS Marketplace después de haber añadido las credenciales a Cloud Manager:

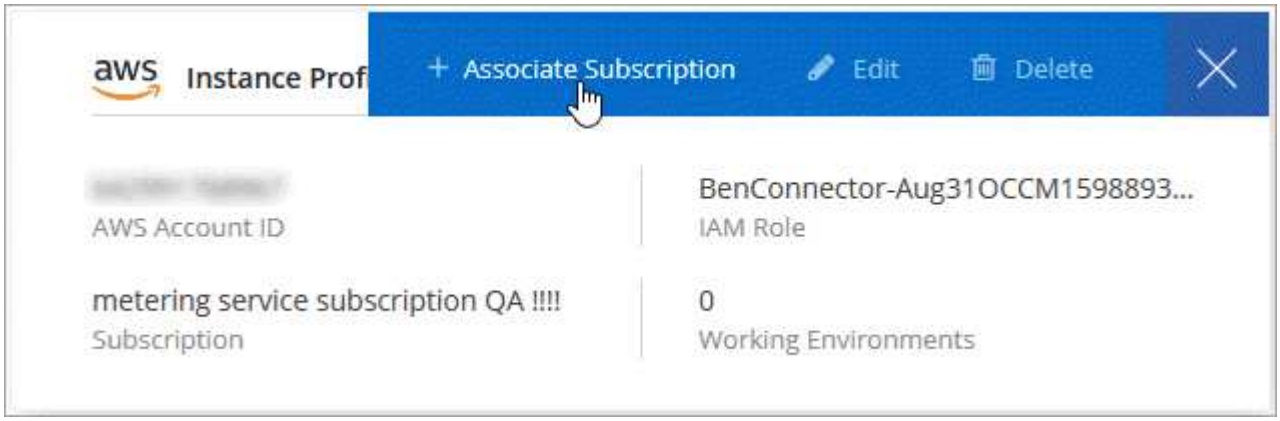
- No asoció una suscripción al agregar inicialmente las credenciales a Cloud Manager.
- Desea sustituir una suscripción existente de AWS Marketplace por una nueva suscripción.

Lo que necesitará

Debe crear un conector antes de poder cambiar la configuración de Cloud Manager. "Vea cómo".

Pasos

1. En la esquina superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **credenciales**.
2. Pase el ratón sobre un conjunto de credenciales y haga clic en el menú de acciones.
3. En el menú, haga clic en **Suscripción asociada**.



4. Seleccione una suscripción de la lista desplegable o haga clic en **Agregar suscripción** y siga los pasos para crear una nueva suscripción.

   ► https://docs.netapp.com/es-es/occm38//media/video_subscribing_aws.mp4 *(video)*

Azure

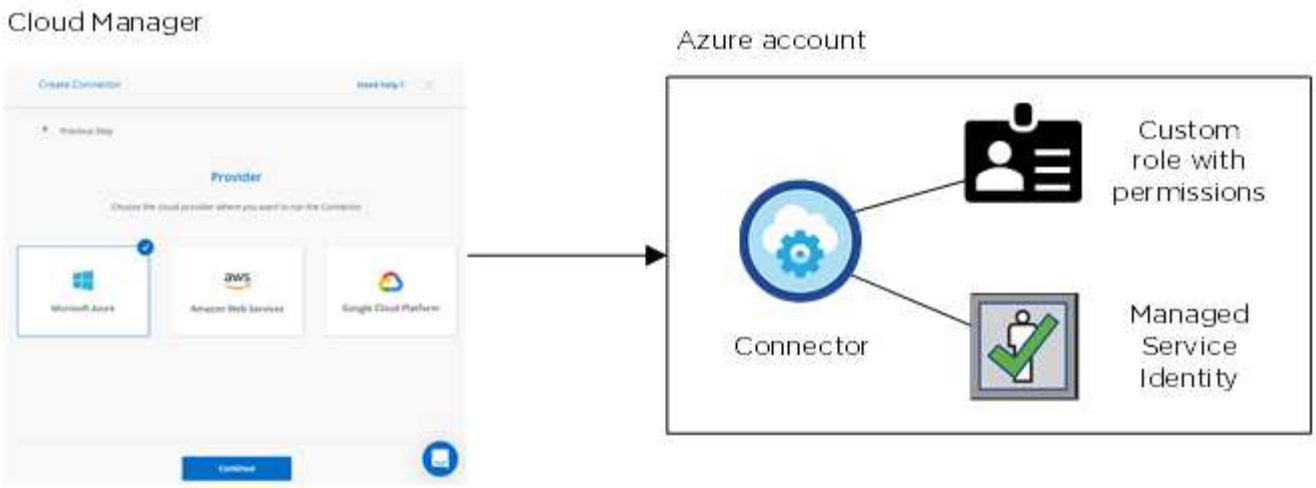
Credenciales y permisos de Azure

Cloud Manager permite elegir las credenciales de Azure que se utilizarán al implementar Cloud Volumes ONTAP. Puede poner en marcha todos los sistemas de Cloud Volumes ONTAP con las credenciales iniciales de Azure o bien añadir credenciales adicionales.

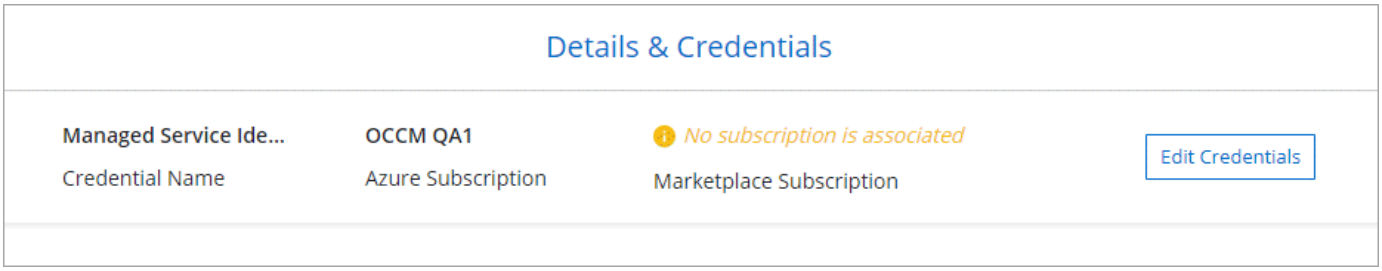
Credenciales iniciales de Azure

Al implementar un conector desde Cloud Manager, necesita utilizar una cuenta de Azure que tenga permisos para implementar la máquina virtual Connector. Los permisos necesarios se enumeran en la "Política de implementación de conectores para Azure".

Cuando Cloud Manager implementa la máquina virtual Connector en Azure, habilita una "identidad administrada asignada por el sistema" en una máquina virtual, crea un rol personalizado y lo asigna a la máquina virtual. El rol proporciona permisos a Cloud Manager para gestionar recursos y procesos dentro de esa suscripción de Azure. "Revise cómo Cloud Manager utiliza los permisos".



Cloud Manager selecciona estas credenciales de Azure de forma predeterminada cuando crea un entorno de trabajo nuevo para Cloud Volumes ONTAP:

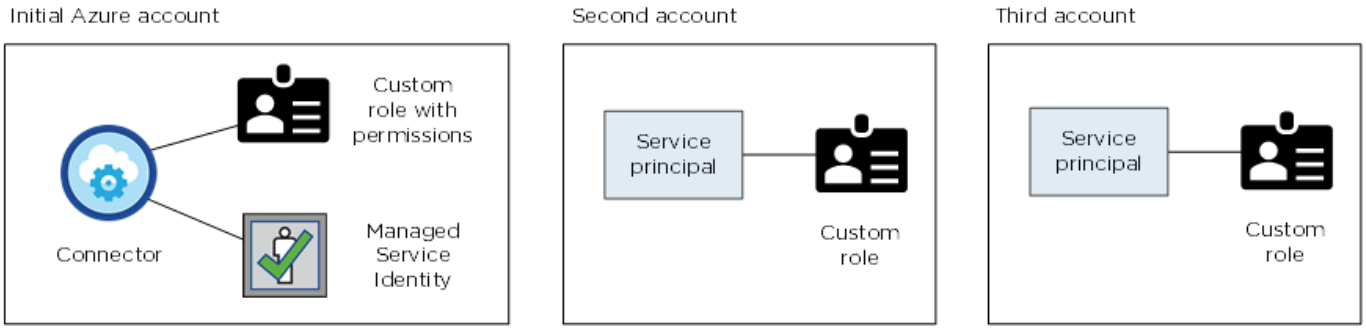


Suscripciones adicionales de Azure para una identidad gestionada

La identidad administrada está asociada a la suscripción en la que inició el conector. Si desea seleccionar una suscripción de Azure diferente, tendrá que hacerlo "asocie la identidad administrada a esas suscripciones".

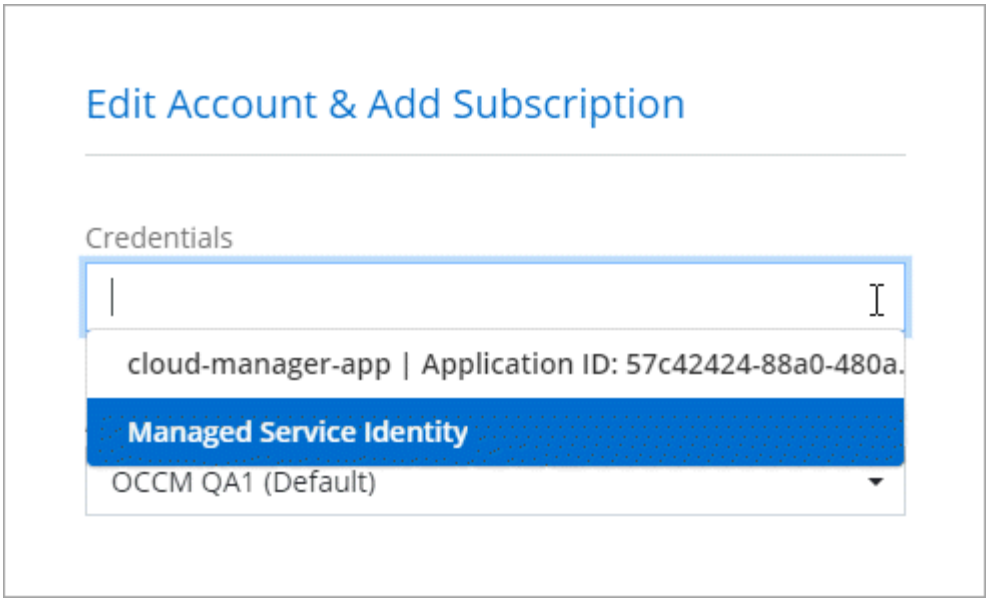
Credenciales adicionales de Azure

Si desea implementar Cloud Volumes ONTAP con diferentes credenciales de Azure, debe conceder los permisos necesarios mediante "Crear y configurar un servicio principal en Azure Active Directorio" Para cada cuenta de Azure. La siguiente imagen muestra dos cuentas adicionales, cada una configurada con una función personalizada y principal de servicio que proporciona permisos:



Entonces lo haría "Añada las credenciales de la cuenta a Cloud Manager" Proporcionando detalles acerca del director de servicio de AD.

Después de añadir otro conjunto de credenciales, puede cambiar a ellas al crear un nuevo entorno de trabajo:



¿Qué pasa con las puestas en marcha de Marketplace y las puestas en marcha en las instalaciones?

En las secciones anteriores se describe el método de puesta en marcha recomendado para el conector, que es de NetApp Cloud Central. También puede implementar un conector en Azure desde "Azure Marketplace", y usted puede "Instale el conector en las instalaciones".

Si utiliza el Marketplace, los permisos se proporcionan de la misma manera. Sólo tiene que crear y configurar manualmente la identidad administrada para el conector y, a continuación, proporcionar permisos para cualquier cuenta adicional.

Para implementaciones en las instalaciones, no puede configurar una identidad administrada para el conector, pero puede proporcionar permisos como lo haría para cuentas adicionales utilizando un director de servicio.

Administrar credenciales y suscripciones de Azure para Cloud Manager

Al crear un sistema Cloud Volumes ONTAP, necesita seleccionar las credenciales de Azure y la suscripción a Marketplace para utilizar con ese sistema. Si gestiona varias suscripciones a Azure Marketplace, puede asignar cada una de ellas a diferentes credenciales de Azure desde la página Credentials.

Existen dos formas de gestionar las credenciales de Azure en Cloud Manager. En primer lugar, si desea implementar Cloud Volumes ONTAP en diferentes cuentas de Azure, tendrá que proporcionar los permisos necesarios y añadir las credenciales a Cloud Manager. La segunda es asociar suscripciones adicionales a la identidad administrada de Azure.

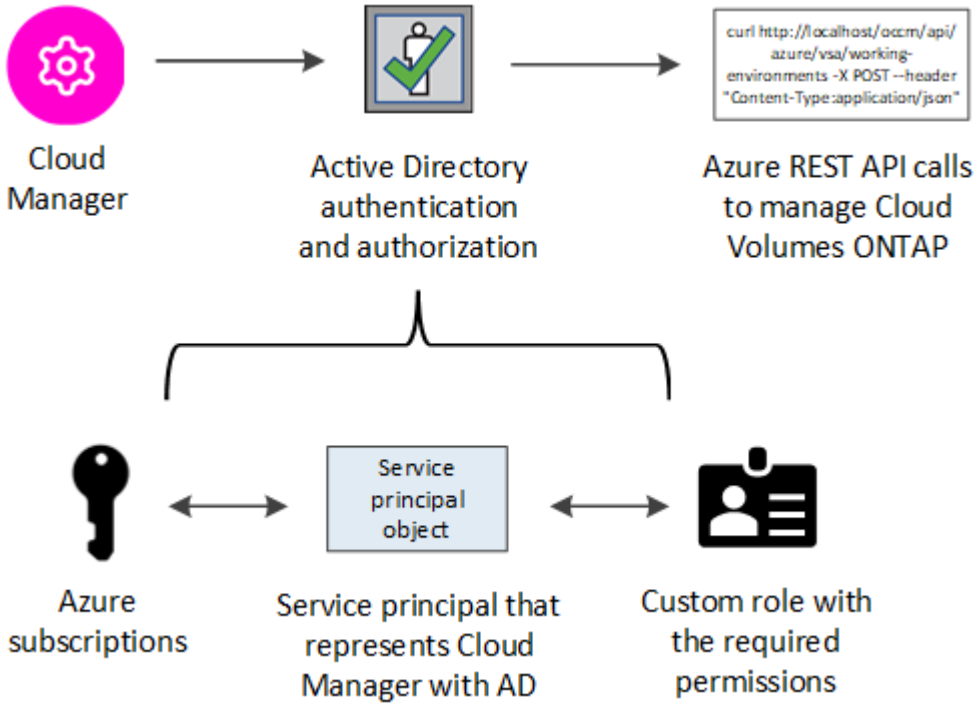
Cuando implementa un conector desde Cloud Manager, Cloud Manager agrega automáticamente la cuenta de Azure en la que implementó Connector. No se agrega una cuenta inicial si instaló manualmente el software Connector en un sistema existente. "Obtenga más información acerca de las cuentas y los permisos de Azure".

Concesión de permisos de Azure con un director de servicio

Cloud Manager necesita permisos para realizar acciones en Azure. Puede conceder los permisos requeridos a una cuenta de Azure creando y configurando un servicio principal en Azure Active Directory y obteniendo las credenciales de Azure que necesita Cloud Manager.

Acerca de esta tarea

La siguiente imagen muestra cómo Cloud Manager obtiene permisos para realizar operaciones en Azure. Un objeto principal de servicio, que está vinculado a una o varias suscripciones de Azure, representa Cloud Manager en Azure Active Directory y se asigna a una función personalizada que permite los permisos necesarios.



Pasos

1. Cree una aplicación de Azure Active Directory.
2. Asigne la aplicación a una función.
3. Añada permisos de API de administración de servicios de Windows Azure.
4. Obtener el ID de aplicación y el ID de directorio.
5. Cree un secreto de cliente.

Crear una aplicación de Azure Active Directory

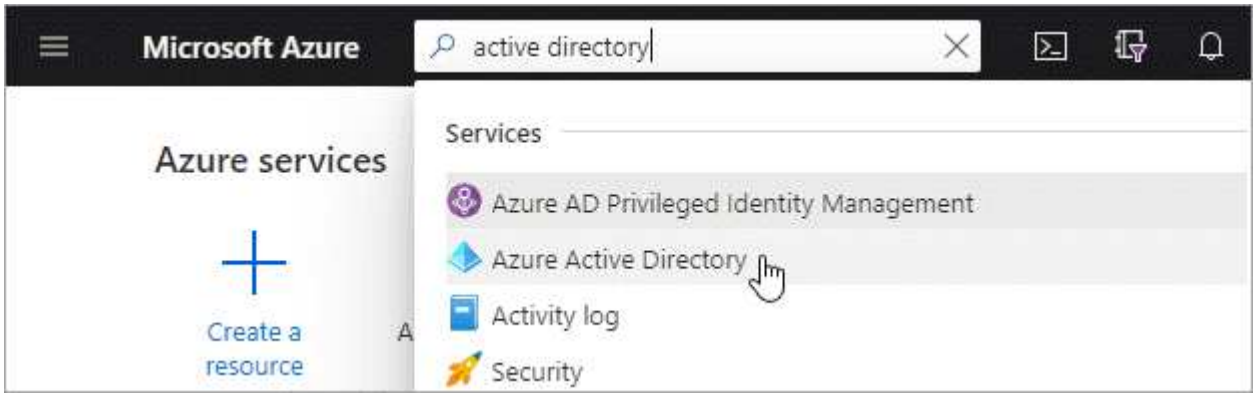
Cree una aplicación de Azure Active Directory (AD) y una entidad de servicio que Cloud Manager pueda usar para el control de acceso basado en roles.

Antes de empezar

Debe tener los permisos adecuados en Azure para crear una aplicación de Active Directory y asignar la aplicación a un rol. Para obtener más información, consulte "Documentación de Microsoft Azure: Permisos necesarios".

Pasos

1. Desde el portal de Azure, abra el servicio **Azure Active Directory**.



2. En el menú, haga clic en **App registrs**.
3. Haga clic en **Nuevo registro**.
4. Especificar detalles acerca de la aplicación:
   - **Nombre**: Introduzca un nombre para la aplicación.
   - **Tipo de cuenta**: Seleccione un tipo de cuenta (cualquiera funcionará con Cloud Manager).
   - **Redirigir URI**: Seleccione **Web** y, a continuación, escriba cualquier dirección URL; por ejemplo, https://url
5. Haga clic en **Registrar**.

Resultado

Ha creado la aplicación AD y el director de servicio.

Asignación de la aplicación a una función

Debe enlazar el principal del servicio a una o más suscripciones de Azure y asignarle el rol personalizado de operador de "OnCommand Cloud Manager" para que Cloud Manager tenga permisos en Azure.

Pasos

1. Crear un rol personalizado:

   a. Descargue el "Política de Azure de Cloud Manager".

   b. Modifique el archivo JSON agregando ID de suscripción de Azure al ámbito asignable.

   Debe añadir el ID para cada suscripción de Azure desde la cual los usuarios crearán sistemas Cloud Volumes ONTAP.

   ejemplo

```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
"/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

   c. Use el archivo JSON para crear una función personalizada en Azure.

El ejemplo siguiente muestra cómo crear una función personalizada con la CLI de Azure 2.0:

```
az role definition create --role-definition
C:\Policy_for_cloud_Manager_Azure_3.8.7.json
```

Ahora debe tener una función personalizada denominada *Cloud Manager Operator*.

2. Asigne la aplicación al rol:

   a. En el portal de Azure, abra el servicio **Suscripciones**.

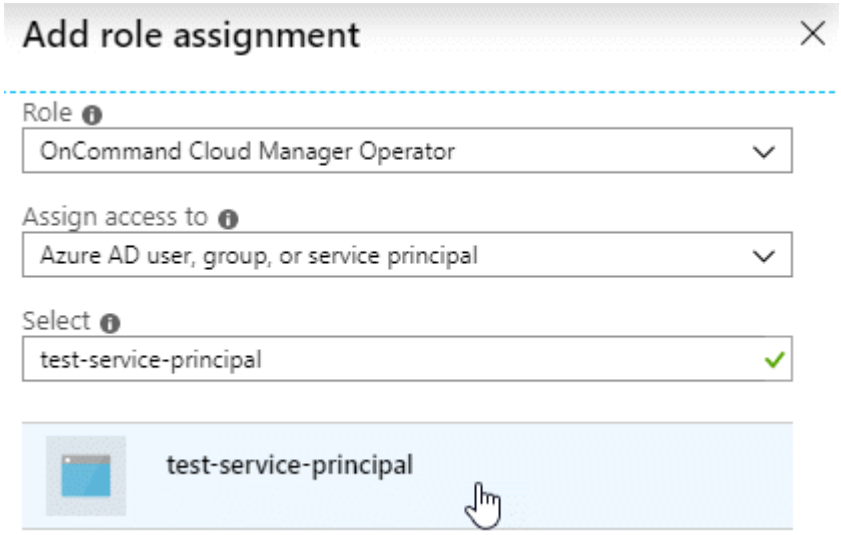
   b. Seleccione la suscripción.

   c. Haga clic en **Control de acceso (IAM) > Agregar > Agregar asignación de funciones**.

   d. Seleccione el rol **operador de Cloud Manager**.

   e. Mantener seleccionado **usuario, grupo o principal de servicio de Azure AD**.

   f. Busque el nombre de la aplicación (no puede encontrarlo en la lista desplazándose).



   g. Seleccione la aplicación y haga clic en **Guardar**.

   El director de servicio de Cloud Manager ahora tiene los permisos de Azure necesarios para esa suscripción.

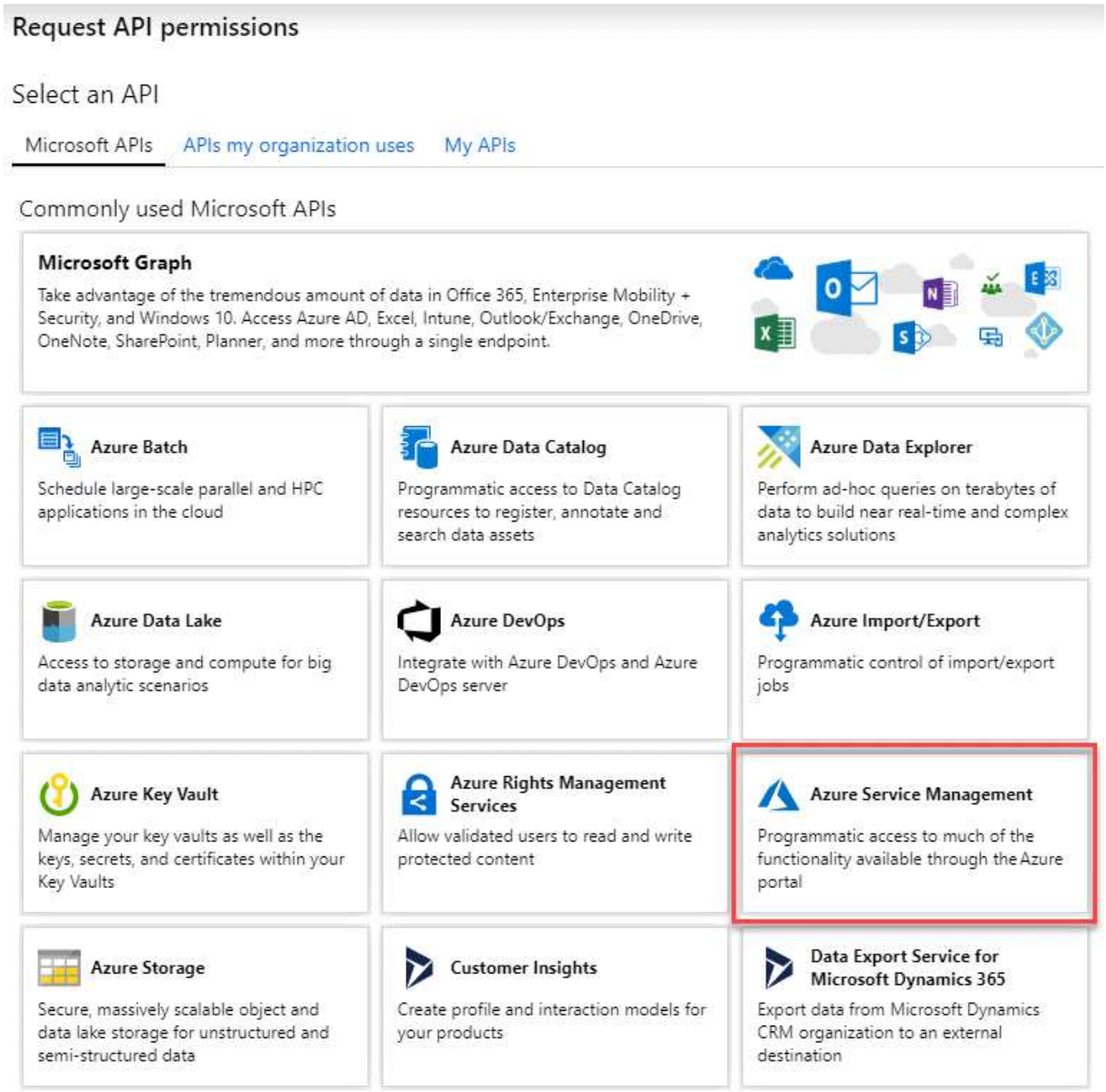
Si desea implementar Cloud Volumes ONTAP desde varias suscripciones a Azure, debe enlazar el principal del servicio con cada una de ellas. Cloud Manager le permite seleccionar la suscripción que desea utilizar al poner en marcha Cloud Volumes ONTAP.

Agregar permisos de API de administración de servicios de Windows Azure

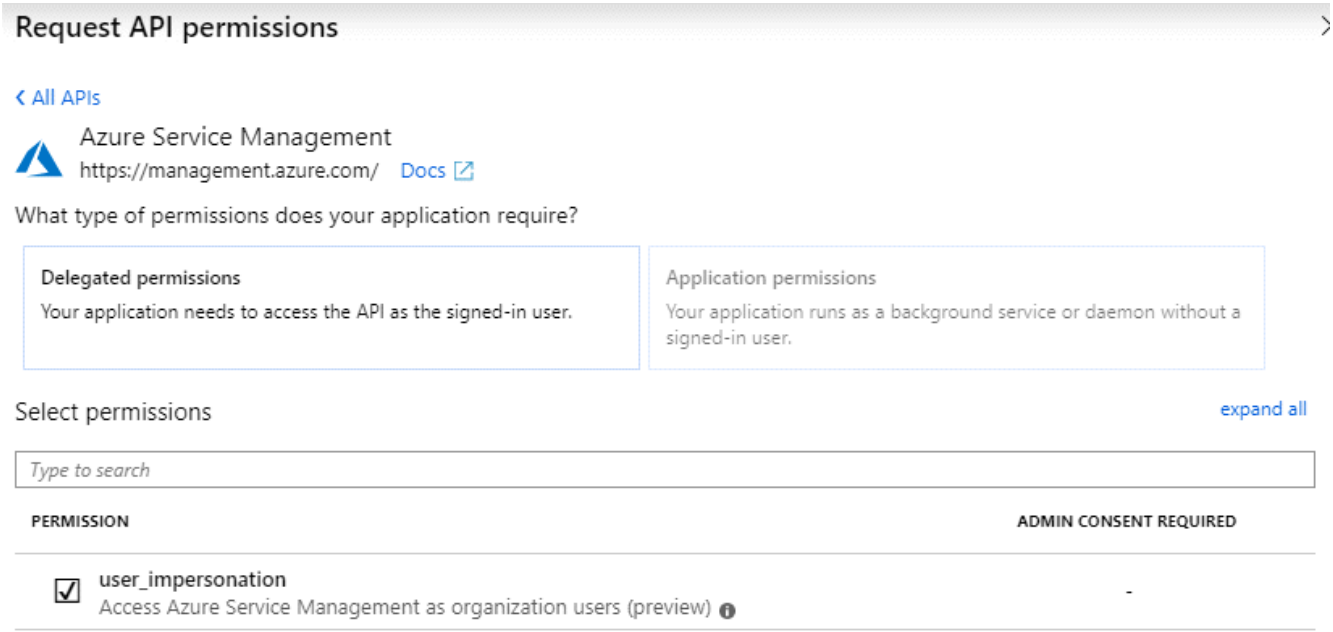
El principal de servicio debe tener permisos de "API de administración de servicios de Windows Azure".

Pasos

1. En el servicio **Azure Active Directory**, haga clic en **App registrs** y seleccione la aplicación.
2. Haga clic en **permisos de API > Agregar un permiso**.
3. En **API de Microsoft**, seleccione **Administración de servicios Azure**.



4. Haga clic en **Access Azure Service Management como usuarios de la organización** y, a continuación, haga clic en **Agregar permisos**.

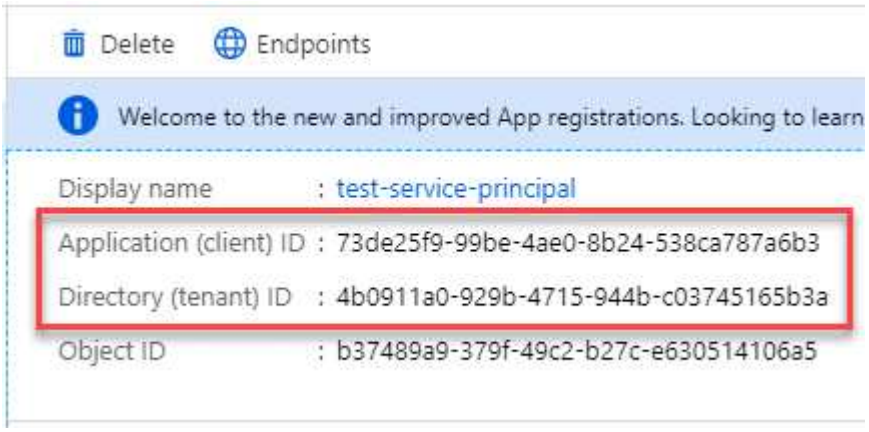


Obteniendo el ID de aplicación y el ID de directorio

Cuando agrega la cuenta de Azure a Cloud Manager, necesita proporcionar el ID de la aplicación (cliente) y el ID de directorio (inquilino) para la aplicación. Cloud Manager utiliza los ID para iniciar sesión mediante programación.

Pasos

1. En el servicio **Azure Active Directory**, haga clic en **App registrs** y seleccione la aplicación.
2. Copie el **ID de aplicación (cliente)** y el **ID de directorio (inquilino)**.



Crear un secreto de cliente

Debe crear un secreto de cliente y, a continuación, proporcionar a Cloud Manager el valor del secreto para que Cloud Manager pueda utilizarlo para autenticar con Azure AD.

Al agregar la cuenta a Cloud Manager, Cloud Manager hace referencia al secreto de cliente como la clave de aplicación.

Pasos

1. Abra el servicio **Azure Active Directory**.
2. Haga clic en **App registres** y seleccione su aplicación.
3. Haga clic en **certificados y secretos > Nuevo secreto de cliente**.
4. Proporcione una descripción del secreto y una duración.
5. Haga clic en **Agregar**.
6. Copie el valor del secreto de cliente.

Resultado

Su principal de servicio ahora está configurado y debe haber copiado el ID de aplicación (cliente), el ID de directorio (arrendatario) y el valor del secreto de cliente. Necesita introducir esta información en Cloud Manager al añadir una cuenta de Azure.

Añadir credenciales de Azure a Cloud Manager

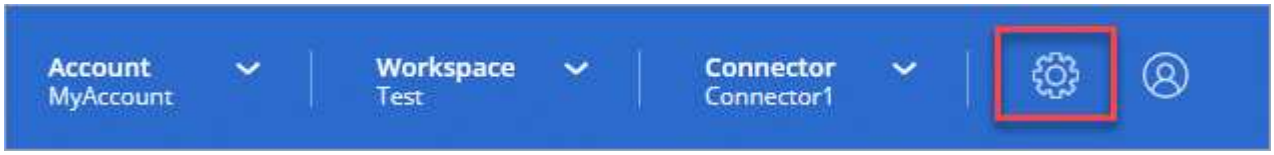
Después de proporcionar una cuenta de Azure con los permisos requeridos, puede añadir las credenciales para esa cuenta a Cloud Manager. Esto le permite iniciar sistemas de Cloud Volumes ONTAP en esa cuenta.

Lo que necesitará

Debe crear un conector antes de poder cambiar la configuración de Cloud Manager. "Vea cómo".

Pasos

1. En la esquina superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **credenciales**.



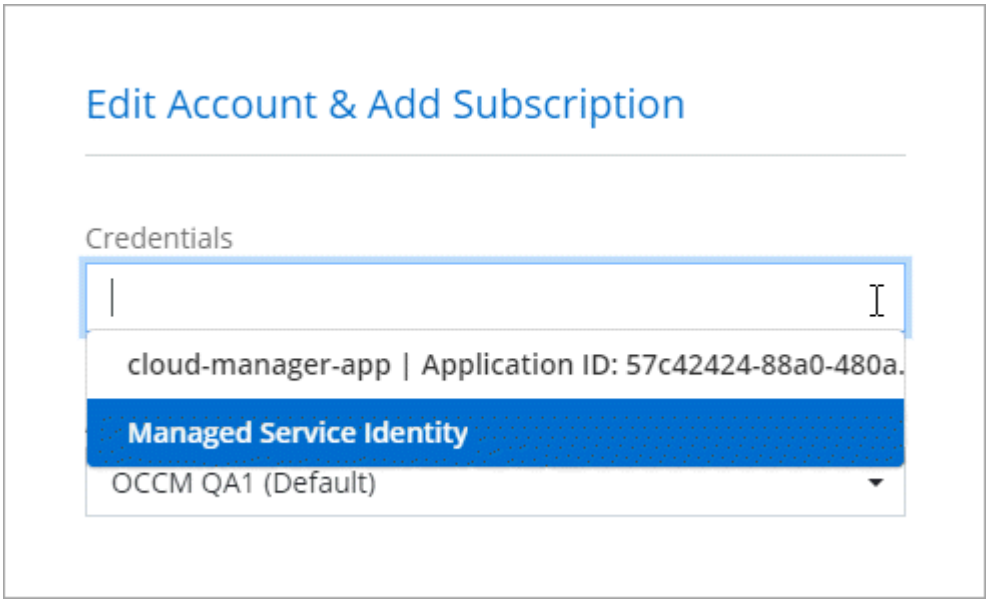
2. Haga clic en **Agregar credenciales** y seleccione **Microsoft Azure**.
3. Introduzca la información acerca del director del servicio de Azure Active Directory que otorga los permisos necesarios:
   - ID de aplicación (cliente): Consulte Obteniendo el ID de aplicación y el ID de directorio.
   - ID de directorio (arrendatario): Consulte Obteniendo el ID de aplicación y el ID de directorio.
   - Client Secret: Consulte Crear un secreto de cliente.
4. Confirme que se han cumplido los requisitos de la directiva y, a continuación, haga clic en **continuar**.
5. Elija la suscripción de pago por uso que desee asociar con las credenciales o haga clic en **Agregar suscripción** si aún no tiene una.

Para crear un sistema de Cloud Volumes ONTAP de pago por uso, las credenciales de Azure deben estar asociadas con una suscripción a Cloud Volumes ONTAP desde Azure Marketplace.

6. Haga clic en **Agregar**.

Resultado

Ahora puede cambiar a un conjunto diferente de credenciales La página Details y Credentials "al crear un nuevo entorno de trabajo":



Asociación de una suscripción de Azure Marketplace a credenciales

Después de añadir sus credenciales de Azure a Cloud Manager, puede asociar una suscripción de Azure Marketplace a esas credenciales. La suscripción le permite crear un sistema de pago por uso Cloud Volumes ONTAP y usar otros servicios cloud de NetApp.

Hay dos escenarios en los que puede asociar una suscripción a Azure Marketplace después de haber añadido las credenciales a Cloud Manager:

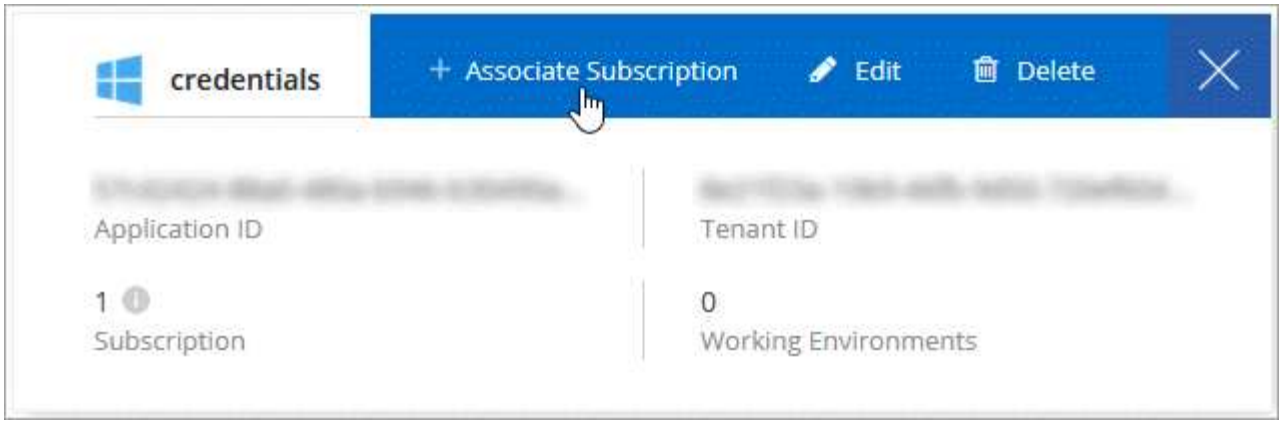
- No asoció una suscripción al agregar inicialmente las credenciales a Cloud Manager.
- Desea sustituir una suscripción existente de Azure Marketplace por una nueva suscripción.

Lo que necesitará

Debe crear un conector antes de poder cambiar la configuración de Cloud Manager. "Vea cómo".

Pasos

1. En la esquina superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **credenciales**.
2. Pase el ratón sobre un conjunto de credenciales y haga clic en el menú de acciones.
3. En el menú, haga clic en **Suscripción asociada**.



4. Seleccione una suscripción de la lista desplegable o haga clic en **Agregar suscripción** y siga los pasos para crear una nueva suscripción.

   El siguiente vídeo se inicia desde el contexto del asistente de entorno de trabajo, pero muestra el mismo flujo de trabajo después de hacer clic en **Agregar suscripción**:

   ► https://docs.netapp.com/es-es/occm38//media/video_subscribing_azure.mp4 *(video)*

Asociar suscripciones de Azure adicionales a una identidad administrada

Cloud Manager le permite elegir las credenciales de Azure y la suscripción a Azure en la que desea poner en marcha Cloud Volumes ONTAP. No puede seleccionar una suscripción de Azure diferente para la gestionada perfil de identidad a menos que asocie el "identidad administrada" con estas suscripciones.

Acerca de esta tarea

Una identidad administrada es "La cuenta inicial de Azure" Al implementar un conector desde Cloud Manager. Cuando implementó el conector, Cloud Manager creó el rol de operador de Cloud Manager y lo asignó a la máquina virtual Connector.

Pasos

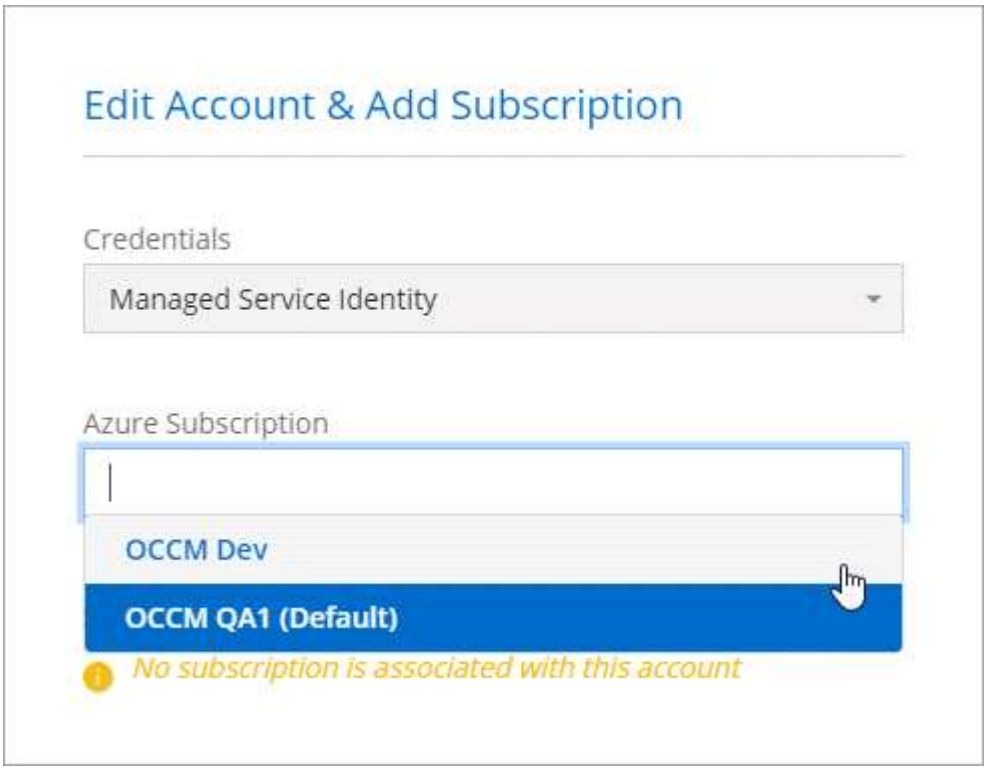
1. Inicie sesión en el portal de Azure.
2. Abra el servicio **Suscripciones** y seleccione la suscripción en la que desea implementar Cloud Volumes ONTAP.
3. Haga clic en **Control de acceso (IAM)**.
   a. Haga clic en **Agregar** > **Agregar asignación de rol** y, a continuación, agregue los permisos:
      - Seleccione el rol **operador de Cloud Manager**.

        Es el nombre predeterminado que se proporciona en la "Política de Cloud Manager". Si seleccionó otro nombre para el rol, seleccione ese nombre.

      - Asigne acceso a una **máquina virtual**.
      - Seleccione la suscripción en la que se creó la máquina virtual Connector.
      - Seleccione la máquina virtual conector.
      - Haga clic en **Guardar**.
4. Repita estos pasos para suscripciones adicionales.

Resultado

Al crear un nuevo entorno de trabajo, ahora debe tener la posibilidad de seleccionar varias suscripciones de Azure para el perfil de identidad administrada.



GCP

Proyectos, permisos y cuentas de Google Cloud

Una cuenta de servicio proporciona a Cloud Manager permisos para implementar y gestionar sistemas de Cloud Volumes ONTAP en el mismo proyecto que Cloud Manager o en diferentes proyectos.

Proyecto y permisos para Cloud Manager

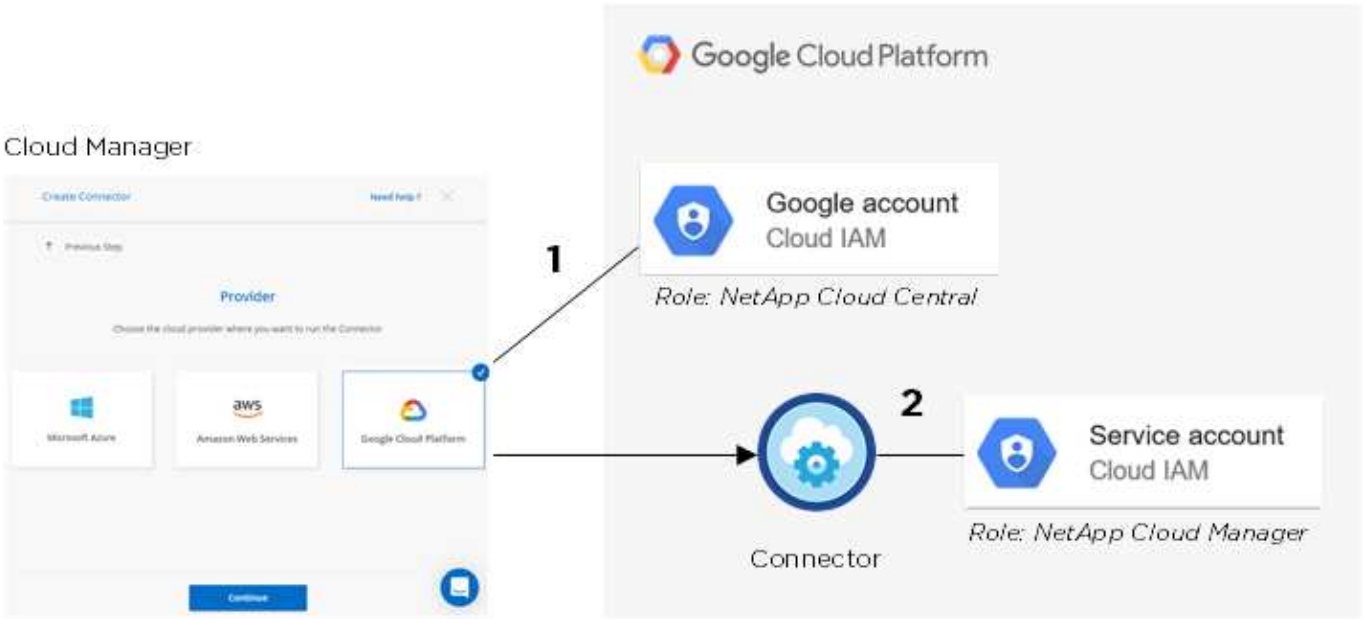
Antes de poder poner en marcha Cloud Volumes ONTAP en Google Cloud, primero debe poner en marcha un conector en un proyecto de Google Cloud. El conector no puede ejecutarse en sus instalaciones ni en un proveedor de cloud diferente.

Debe haber dos conjuntos de permisos antes de implementar un conector directamente desde Cloud Manager:

1. Necesita implementar un conector con una cuenta de Google que tenga permisos para iniciar la instancia de Connector VM desde Cloud Manager.
2. Al desplegar el conector, se le pedirá que seleccione un "cuenta de servicio" Para la instancia de máquina virtual. Cloud Manager obtiene permisos de la cuenta de servicio para crear y gestionar sistemas de Cloud Volumes ONTAP en su nombre. Los permisos se proporcionan asociando una función personalizada a la cuenta de servicio.

Hemos configurado dos archivos YAML que incluyen los permisos necesarios para el usuario y la cuenta de servicio. "Aprenda a usar los archivos YAML para configurar permisos".

La siguiente imagen muestra los requisitos de permisos descritos en los números 1 y 2 anteriores:



Proyecto para Cloud Volumes ONTAP

Cloud Volumes ONTAP puede residir en el mismo proyecto que el conector o en un proyecto diferente. Para implementar Cloud Volumes ONTAP en un proyecto diferente, primero debe agregar la cuenta de servicio del conector y la función a ese proyecto.

- "Aprenda a configurar una cuenta de servicio (consulte el paso 2).".
- "Descubra cómo implementar Cloud Volumes ONTAP en GCP y seleccione un proyecto".

Responsables de la organización en niveles de los datos

Cloud Manager requiere una cuenta de GCP para Cloud Volumes ONTAP 9.6, pero no para la versión 9.7 ni para las posteriores. Si desea utilizar la organización en niveles de datos con Cloud Volumes ONTAP 9.7, siga el paso 4 en "Introducción a Cloud Volumes ONTAP en Google Cloud Platform".

Es necesario añadir una cuenta de Google Cloud a Cloud Manager para habilitar la organización en niveles de datos en un sistema Cloud Volumes ONTAP 9.6. Organización en niveles de datos organiza automáticamente en niveles los datos fríos en un almacenamiento de objetos de bajo coste, lo que le permite recuperar espacio en el almacenamiento principal y reducir el almacenamiento secundario.

Al añadir la cuenta, necesita proporcionar a Cloud Manager una clave de acceso al almacenamiento para una cuenta de servicio con permisos de administrador de almacenamiento. Cloud Manager utiliza las claves de acceso para configurar y gestionar un bucket de Cloud Storage para la organización de datos en niveles.

Después de añadir una cuenta de Google Cloud, podrá habilitar la organización en niveles de los datos en volúmenes individuales al crearlos, modificarlos o replicarlos.

- "Aprenda a configurar y añadir cuentas de GCP a. Cloud Manager".
- "Aprenda a organizar en niveles los datos inactivos en almacenamiento de objetos de bajo coste".

Gestión de credenciales y suscripciones de GCP para Cloud Manager

Puede gestionar dos tipos de credenciales de Google Cloud Platform desde Cloud Manager: Las credenciales asociadas con la instancia de Connector VM y las claves de acceso al almacenamiento utilizadas con un sistema Cloud Volumes ONTAP 9.6 para "organización en niveles de los datos".

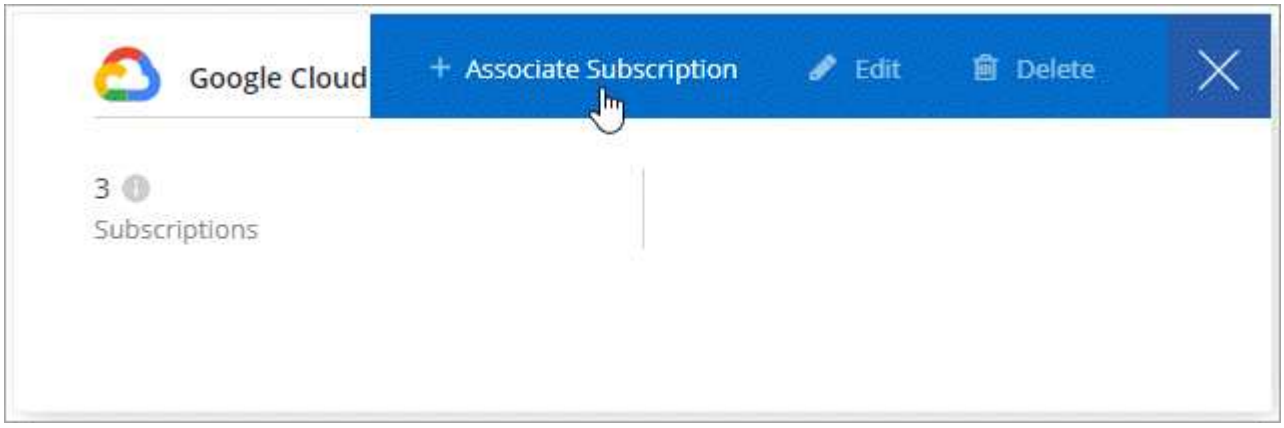
Asociación de una suscripción a Marketplace con credenciales de GCP

Al implementar un conector en GCP, Cloud Manager crea un conjunto predeterminado de credenciales asociadas con la instancia de Connector VM. Estas son las credenciales que utiliza Cloud Manager para poner en marcha Cloud Volumes ONTAP.

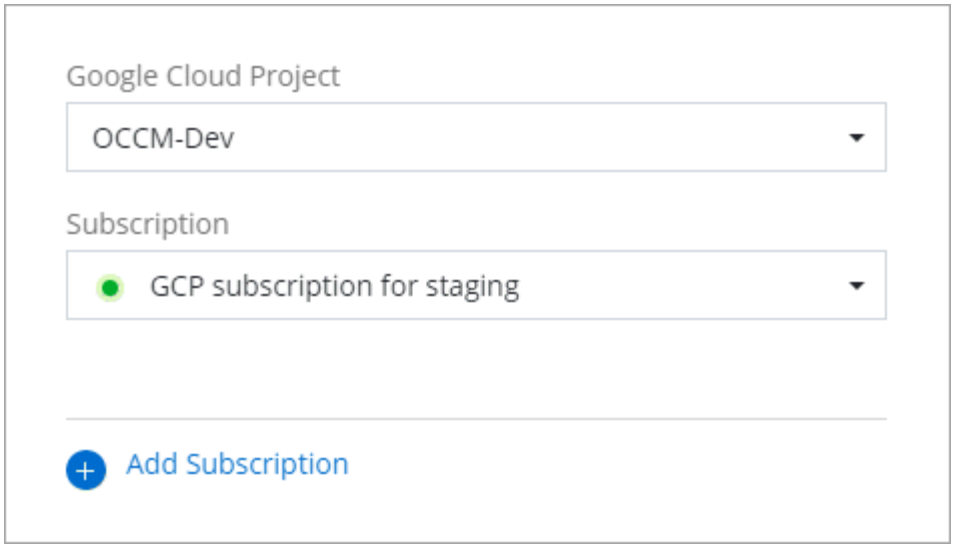
En cualquier momento, puede cambiar la suscripción de Marketplace asociada a estas credenciales. La suscripción le permite crear un sistema de pago por uso Cloud Volumes ONTAP y usar otros servicios cloud de NetApp.

Pasos

1. En la esquina superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **credenciales**.
2. Pase el ratón sobre un conjunto de credenciales y haga clic en el menú de acciones.
3. En el menú, haga clic en **Suscripción asociada**.



4. Seleccione un proyecto de Google Cloud y una suscripción en la lista desplegable o haga clic en **Agregar suscripción** y siga los pasos para crear una nueva suscripción.



5. Haga clic en **asociar**.

Configuración y adición de cuentas de GCP para la organización de datos en niveles con Cloud Volumes ONTAP 9.6

Si desea habilitar una instancia de Cloud Volumes ONTAP 9.6 sistema para "organización en niveles de los datos", debe proporcionar a Cloud Manager una clave de acceso a almacenamiento para una cuenta de servicio que tenga permisos de Administrador de almacenamiento. Cloud Manager utiliza las claves de acceso para configurar y gestionar un bucket de Cloud Storage para la organización de datos en niveles.

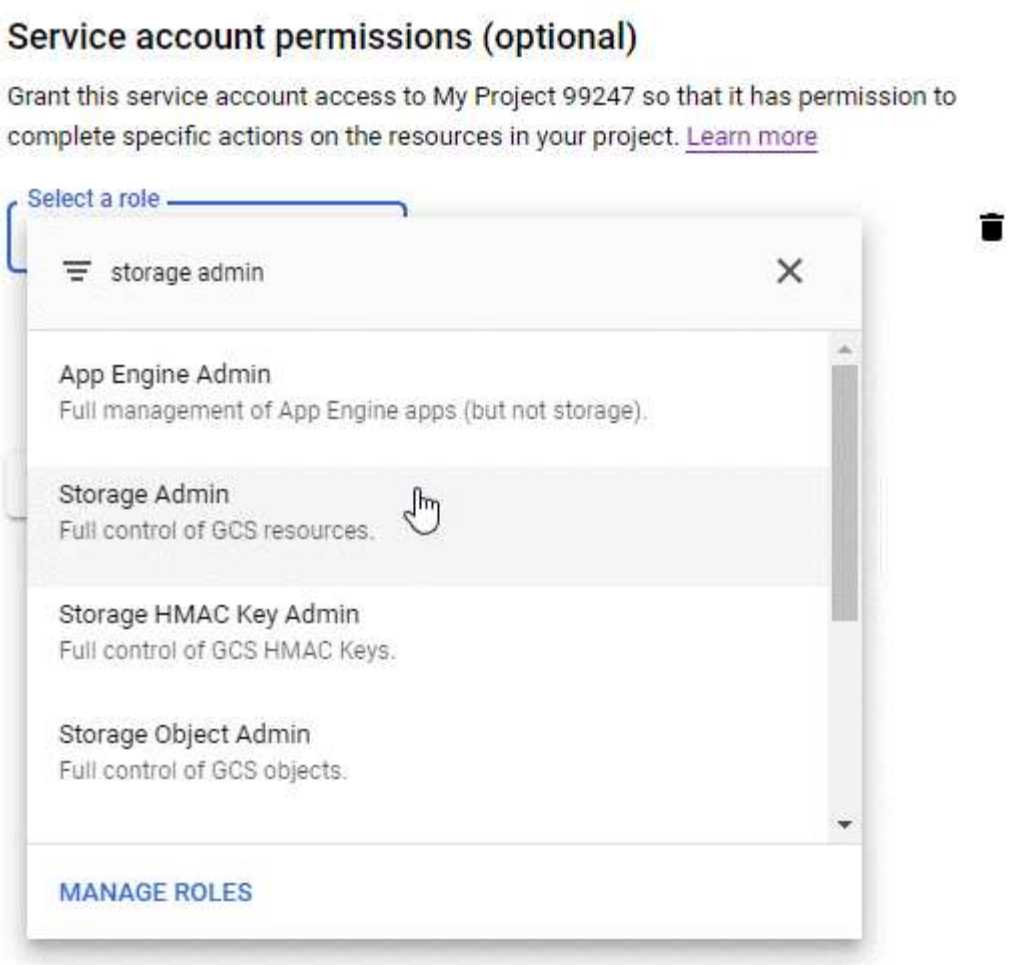
Si desea utilizar la organización en niveles de datos con Cloud Volumes ONTAP 9.7, siga el paso 4 en "Introducción a Cloud Volumes ONTAP en Google Cloud Platform".

Configuración de una cuenta de servicio y claves de acceso para Google Almacenamiento en cloud

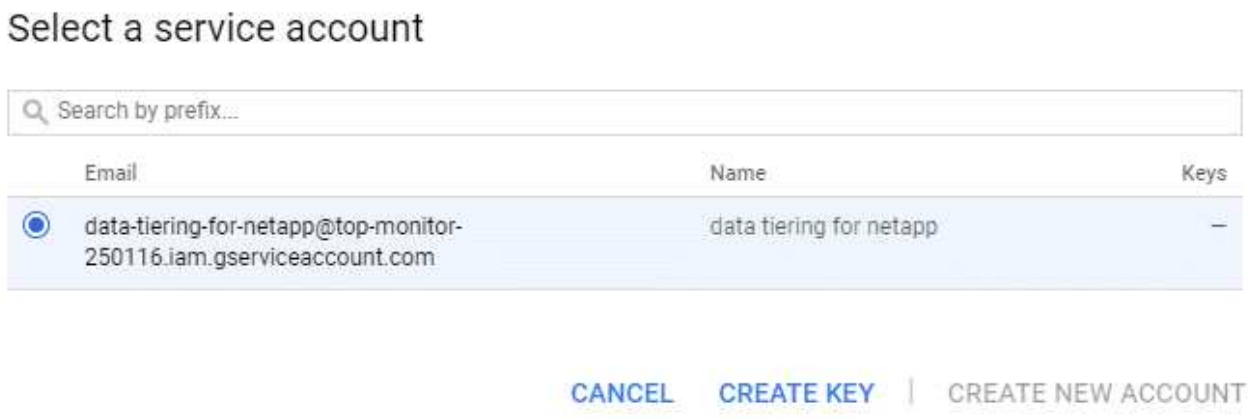
Una cuenta de servicio permite que Cloud Manager autentique y acceda a los bloques de almacenamiento en cloud que se utilizan para la organización en niveles de los datos. Las claves son necesarias para que Google Cloud Storage sepa quién está haciendo la solicitud.

Pasos

1. Abra la consola GCP IAM y. "Cree una cuenta de servicio con el rol Storage Admin".



2. Vaya a. "Configuración de almacenamiento para GCP".
3. Si se le solicita, seleccione un proyecto.
4. Haga clic en la pestaña **interoperabilidad**.
5. Si aún no lo ha hecho, haga clic en **Activar acceso de interoperabilidad**.
6. En **claves de acceso para cuentas de servicio**, haga clic en **Crear una clave para una cuenta de servicio**.
7. Seleccione la cuenta de servicio que ha creado en el paso 1.



8. Haga clic en **Crear clave**.
9. Copie la clave de acceso y el secreto.

   Tendrá que introducir esta información en Cloud Manager cuando añada la cuenta de GCP para la organización en niveles de los datos.

Añadir una cuenta de GCP a Cloud Manager

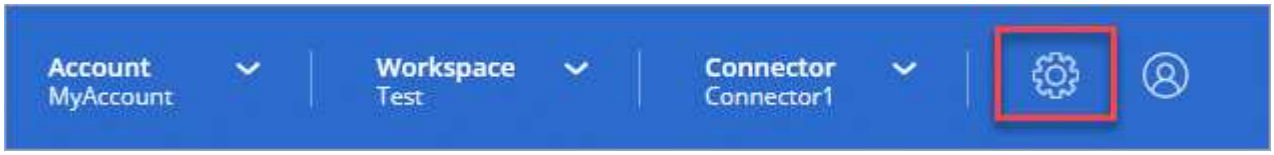
Ahora que tiene una clave de acceso para una cuenta de servicio, puede agregarla a Cloud Manager.

Lo que necesitará

Debe crear un conector antes de poder cambiar la configuración de Cloud Manager. "Vea cómo".

Pasos

1. En la esquina superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **credenciales**.



2. Haga clic en **Agregar credenciales** y seleccione **Google Cloud**.
3. Introduzca la clave de acceso y el secreto de la cuenta de servicio.

   Las claves permiten a Cloud Manager configurar un bucket de almacenamiento en cloud para la organización de datos en niveles.

4. Confirme que se han cumplido los requisitos de la directiva y, a continuación, haga clic en **Crear cuenta**.

El futuro

Ahora puede habilitar la organización en niveles de los datos en volúmenes individuales en un sistema Cloud Volumes ONTAP 9.6 cuando los crea, modifica o replica. Para obtener más información, consulte "Organización en niveles de los datos inactivos en almacenamiento de objetos de bajo coste".

Pero antes de hacerlo, asegúrese de que la subred en la que reside Cloud Volumes ONTAP esté configurada para acceso privado a Google. Para obtener instrucciones, consulte "Documentación de Google Cloud: Configuración de Private Google Access".

Adición de cuentas del sitio de soporte de NetApp a Cloud Manager

Para añadir su cuenta del sitio de soporte de NetApp a Cloud Manager debe poner en marcha un sistema BYOL. También es necesario registrar sistemas de pago por uso y actualizar el software de ONTAP.

Vea el siguiente vídeo para descubrir cómo añadir cuentas del sitio de soporte de NetApp a Cloud Manager. O desplácese hacia abajo para leer los pasos.

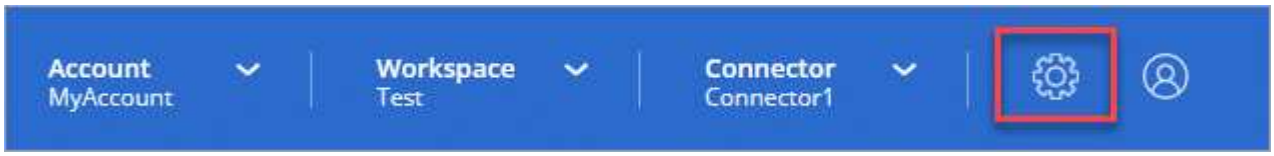
[] | *https://img.youtube.com/vi/V2fLTyztqYQ/maxresdefault.jpg*

Lo que necesitará

Debe crear un conector antes de poder cambiar la configuración de Cloud Manager. "Vea cómo".

Pasos

1. Si aún no dispone de una cuenta en la página de soporte de NetApp, "regístrese para uno".
2. En la esquina superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **credenciales**.



3. Haga clic en **Add Credentials** y seleccione **Sitio de soporte de NetApp**.
4. Escriba un nombre para la cuenta y, a continuación, escriba el nombre de usuario y la contraseña.
   - La cuenta debe ser una cuenta de nivel de cliente (no una cuenta de invitado o temporal).
   - Si tiene pensado poner en marcha sistemas BYOL:
     - La cuenta debe estar autorizada para acceder a los números de serie de los sistemas BYOL.
     - Si ha adquirido una suscripción BYOL segura, será necesaria una cuenta de NSS segura.
5. Haga clic en **Crear cuenta.**

El futuro

Ahora los usuarios pueden seleccionar la cuenta al crear nuevos sistemas de Cloud Volumes ONTAP y al registrar los sistemas existentes.

- "Inicio de Cloud Volumes ONTAP en AWS"
- "Inicio de Cloud Volumes ONTAP en Azure"
- "Registro de sistemas de pago por uso"
- "Descubra cómo Cloud Manager gestiona los archivos de licencia"

Gestión de usuarios, áreas de trabajo, conectores y suscripciones

"Después de realizar la configuración inicial", es posible que necesite administrar la configuración de su cuenta más adelante mediante la administración de usuarios, áreas de trabajo, conectores y suscripciones.

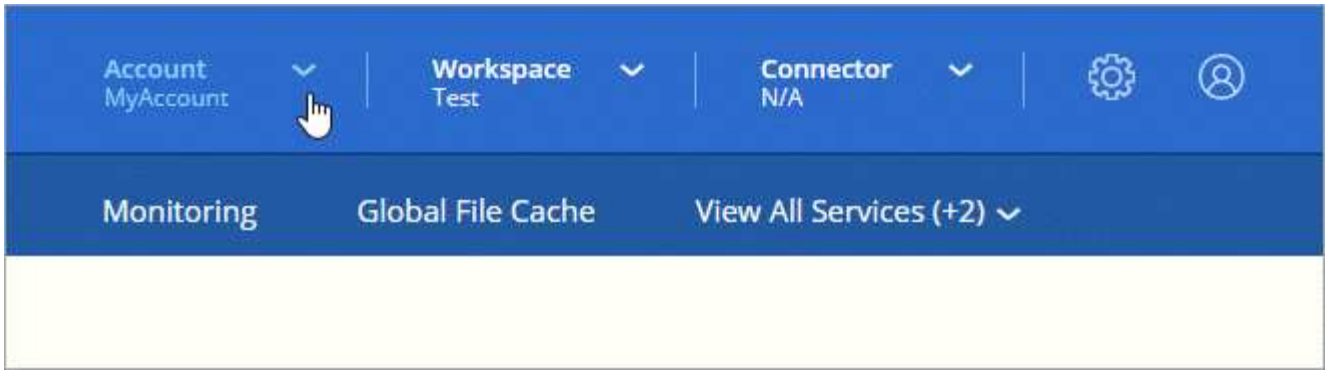
"Obtenga más información sobre cómo funcionan las cuentas de Cloud Central".

Adición de usuarios

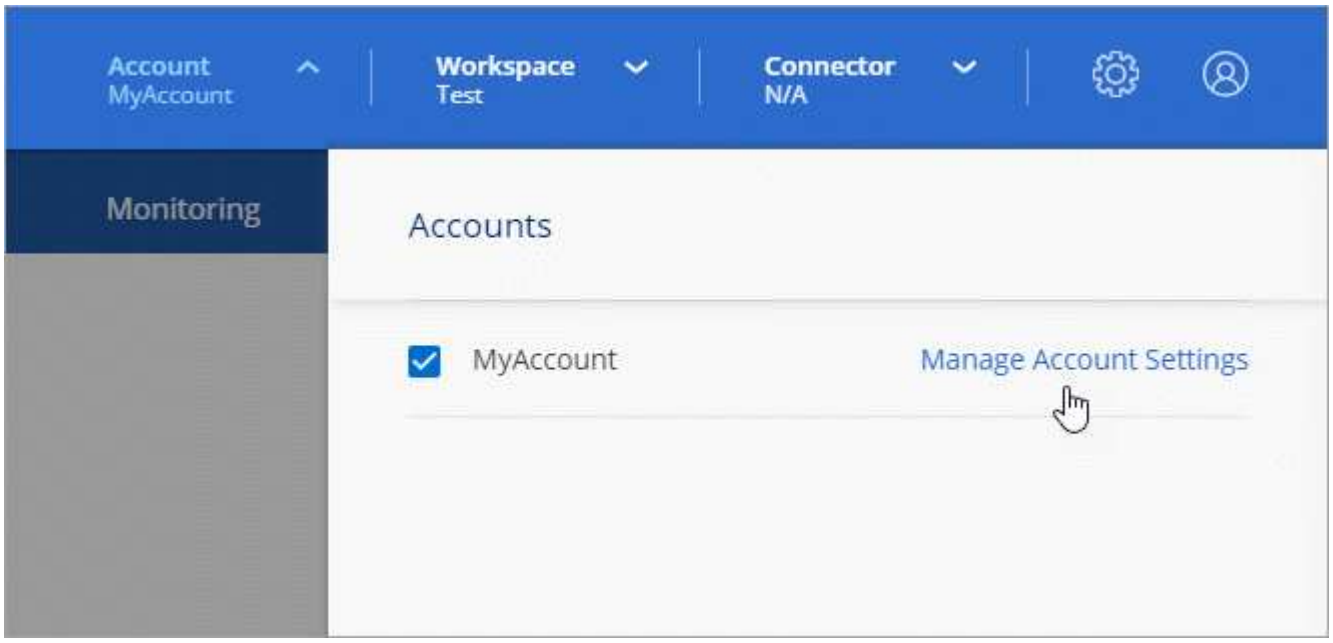
Asocie los usuarios de Cloud Central a la cuenta de Cloud Central para que esos usuarios puedan crear y gestionar entornos de trabajo en Cloud Manager.

Pasos

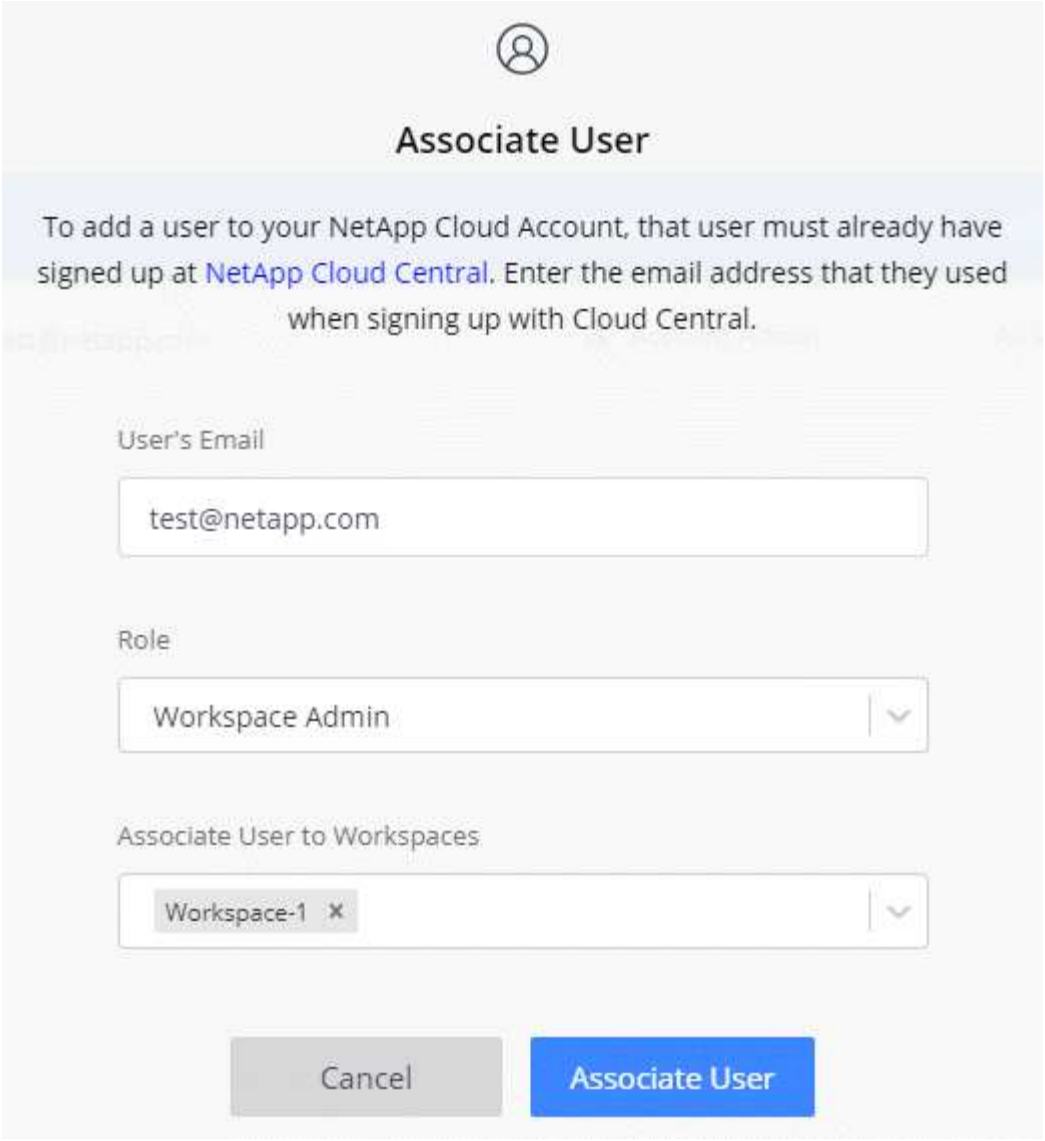
1. Si el usuario aún no lo ha hecho, pida al usuario que vaya a. "Cloud Central de NetApp" y regístrese.
2. En la parte superior de Cloud Manager, haga clic en el menú desplegable **cuenta**.



3. Haga clic en **Administrar cuenta** junto a la cuenta seleccionada actualmente.



4. En la ficha usuarios, haga clic en **Usuario asociado**.
5. Introduzca la dirección de correo electrónico del usuario y seleccione un rol para el usuario:
   - **Administrador de cuentas**: Puede realizar cualquier acción en Cloud Manager.
   - **Administración de área de trabajo**: Puede crear y administrar recursos en áreas de trabajo asignadas.
   - **Visor de cumplimiento**: Sólo puede ver información de cumplimiento y generar informes para áreas de trabajo a las que tienen permiso para acceder.
6. Si ha seleccionado Administrador de área de trabajo o Visor de cumplimiento, seleccione uno o varios espacios de trabajo para asociarlos con ese usuario.



7. Haga clic en **Usuario asociado**.

Resultado

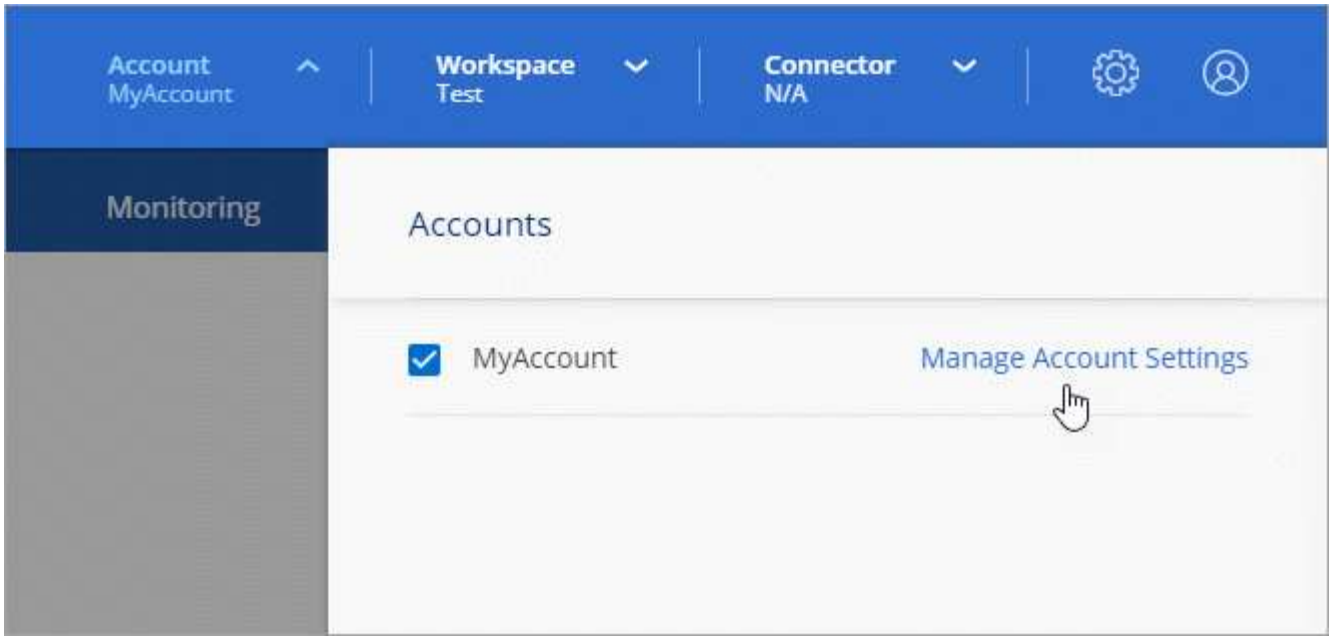
El usuario debe recibir un correo electrónico de Cloud Central de NetApp titulado "Account Association". El correo electrónico incluye la información necesaria para acceder a Cloud Manager.

Quitar usuarios

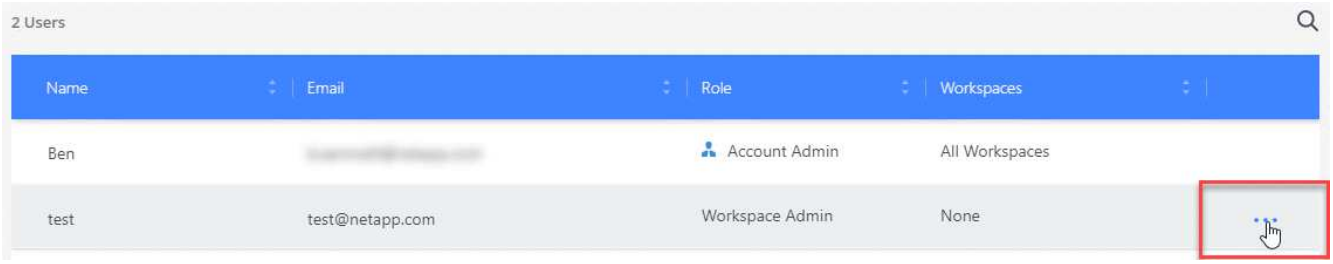
Al desasociar un usuario, éste lo hace para que no pueda acceder a los recursos de una cuenta de Cloud Central.

Pasos

1. En la parte superior de Cloud Manager, haga clic en el menú desplegable **cuenta** y haga clic en **gestionar cuenta**.



2. En la ficha usuarios , haga clic en el menú acción de la fila correspondiente al usuario.



3. Haga clic en **desasociar usuario** y haga clic en **desasociar** para confirmar.

Resultado

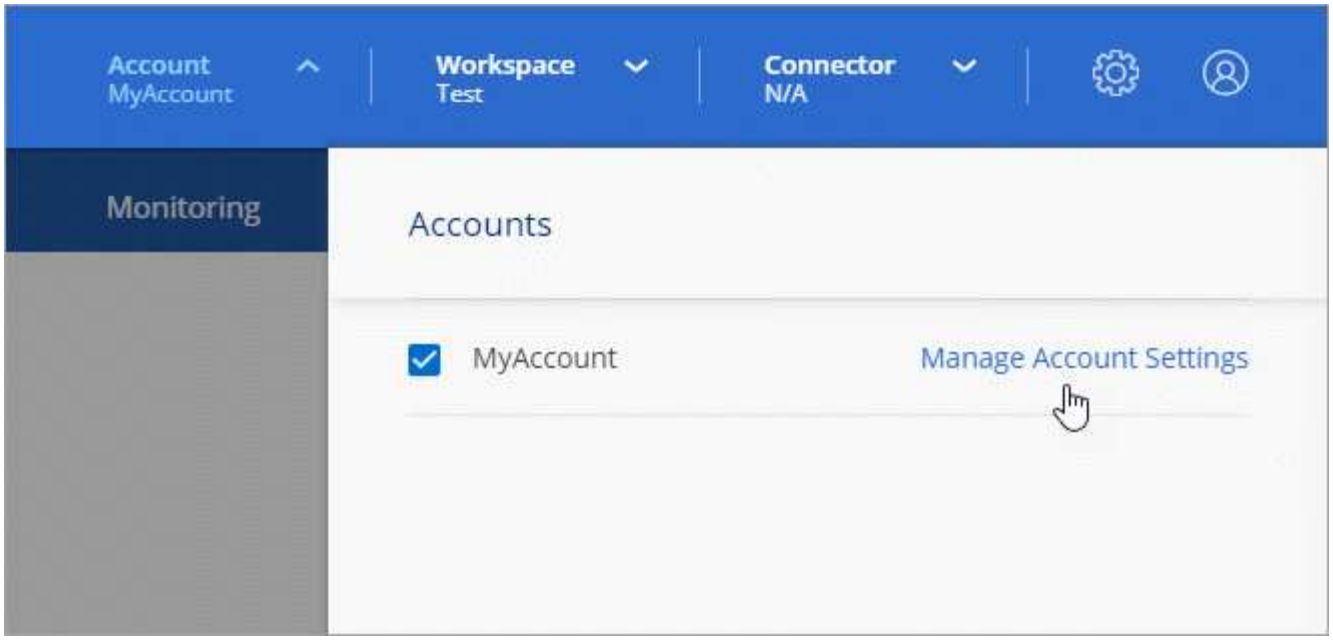
El usuario ya no puede acceder a los recursos de esta cuenta de Cloud Central.

Gestión de los espacios de trabajo de un administrador de área de trabajo

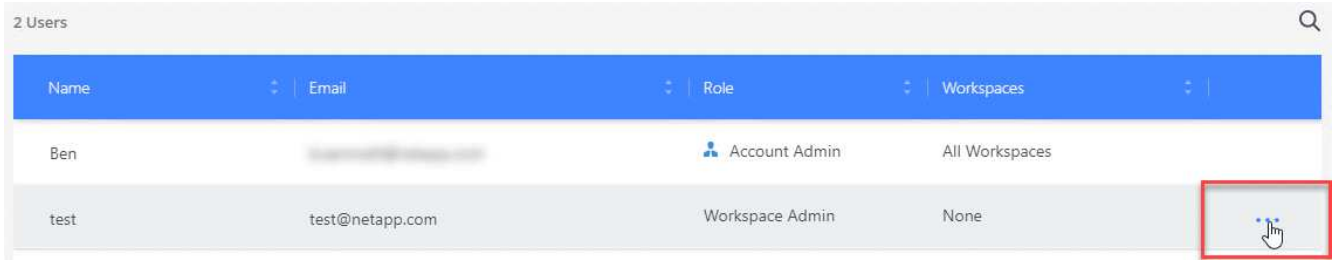
Puede asociar y desasociar administradores de área de trabajo con áreas de trabajo en cualquier momento. La asociación del usuario les permite crear y ver los entornos de trabajo en ese espacio de trabajo.

Pasos

1. En la parte superior de Cloud Manager, haga clic en el menú desplegable **cuenta** y haga clic en **gestionar cuenta**.



2. En la ficha usuarios , haga clic en el menú acción de la fila correspondiente al usuario.



3. Haga clic en **Administrar espacios de trabajo**.
4. Seleccione los espacios de trabajo que desea asociar con el usuario y haga clic en **aplicar**.

Resultado

Ahora el usuario puede acceder a esos espacios de trabajo desde Cloud Manager, siempre que el conector también esté asociado a los espacios de trabajo.

Gestión de espacios de trabajo

Gestione sus espacios de trabajo creando, cambiando el nombre y borrándolos. Tenga en cuenta que no puede eliminar un área de trabajo si contiene recursos. Debe estar vacío.

Pasos

1. En la parte superior de Cloud Manager, haga clic en el menú desplegable **cuenta** y haga clic en **gestionar cuenta**.
2. Haga clic en **espacios de trabajo**.
3. Seleccione una de las siguientes opciones:
   - Haga clic en **Agregar nuevo espacio de trabajo** para crear un nuevo espacio de trabajo.
   - Haga clic en **Cambiar nombre** para cambiar el nombre del espacio de trabajo.
   - Haga clic en **Eliminar** para eliminar el área de trabajo.

Gestión de los espacios de trabajo de un conector

Debe asociar el conector a espacios de trabajo para que los administradores de área de trabajo puedan acceder a estos espacios de trabajo desde Cloud Manager.

Si sólo tiene Administradores de cuentas, no es necesario asociar el conector a áreas de trabajo. Los administradores de cuentas tienen la posibilidad de acceder a todos los espacios de trabajo de Cloud Manager de forma predeterminada.

"Obtenga más información sobre usuarios, áreas de trabajo y conectores".

Pasos

1. En la parte superior de Cloud Manager, haga clic en el menú desplegable **cuenta** y haga clic en **gestionar cuenta**.
2. Haga clic en **conector**.
3. Haga clic en **Administrar áreas de trabajo** para el conector que desea asociar.
4. Seleccione las áreas de trabajo que desea asociar con el conector y haga clic en **aplicar**.

Gestión de suscripciones

Después de suscribirse desde el mercado de un proveedor de cloud, cada suscripción estará disponible en el widget Account Settings. Puede cambiar el nombre de una suscripción y desasociar la suscripción de una o más cuentas.

Por ejemplo, digamos que tiene dos cuentas y cada una se factura mediante suscripciones independientes. Puede desasociar una suscripción de una de las cuentas para que los usuarios de esa cuenta no elijan accidentalmente la suscripción incorrecta al crear un entorno de trabajo de Cloud Volume ONTAP.

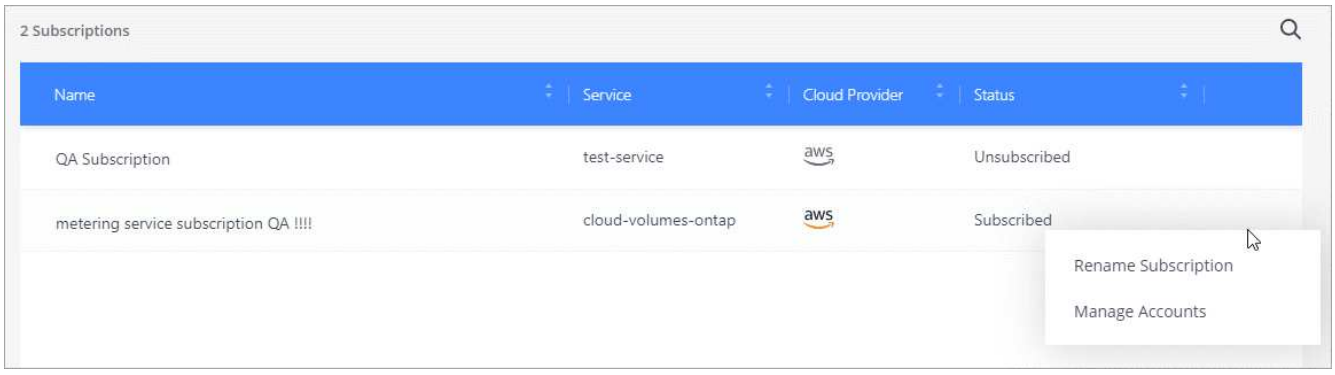
"Más información sobre suscripciones".

Pasos

1. En la parte superior de Cloud Manager, haga clic en el menú desplegable **cuenta** y haga clic en **gestionar cuenta**.
2. Haga clic en **Suscripciones**.

   Solo verá las suscripciones asociadas a la cuenta que está viendo actualmente.

3. Haga clic en el menú de acciones de la fila correspondiente a la suscripción que desea administrar.



4. Elija cambiar el nombre de la suscripción o administrar las cuentas asociadas a la suscripción.

Cambiando el nombre de la cuenta

Cambie el nombre de su cuenta en cualquier momento para cambiarlo a algo significativo para usted.

Pasos

1. En la parte superior de Cloud Manager, haga clic en el menú desplegable **cuenta** y haga clic en **gestionar cuenta**.
2. En la ficha **Descripción general**, haga clic en el icono de edición situado junto al nombre de la cuenta.
3. Escriba un nuevo nombre de cuenta y haga clic en **Guardar**.

Activación o desactivación de la plataforma SaaS

No recomendamos desactivar la plataforma SaaS a menos que necesite para cumplir con las políticas de seguridad de su empresa. Al deshabilitar la plataforma SaaS, se limita su capacidad para usar los servicios de cloud integrados de NetApp.

Los siguientes servicios no están disponibles en Cloud Manager si deshabilita la plataforma SaaS:

- Cumplimiento de normativas en el cloud
- Kubernetes
- Organización en niveles del cloud
- Caché de archivos global
- Supervisión (Cloud Insights)

Pasos

1. En la parte superior de Cloud Manager, haga clic en el menú desplegable **cuenta** y haga clic en **gestionar cuenta**.
2. En la ficha **Descripción general**, seleccione la opción para activar el uso de la plataforma SaaS.

Gestión de un certificado HTTPS para un acceso seguro

De forma predeterminada, Cloud Manager utiliza un certificado autofirmado para el acceso HTTPS a la consola web. Puede instalar un certificado firmado por una CA, que proporciona una mejor protección de seguridad que un certificado autofirmado.

Antes de empezar

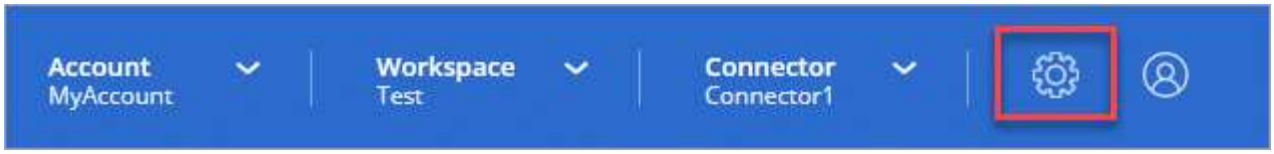
Debe crear un conector antes de poder cambiar la configuración de Cloud Manager. "Vea cómo".

Instalar un certificado HTTPS

Instale un certificado firmado por una CA para obtener acceso seguro.

Pasos

1. En la parte superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **Configuración HTTPS**.

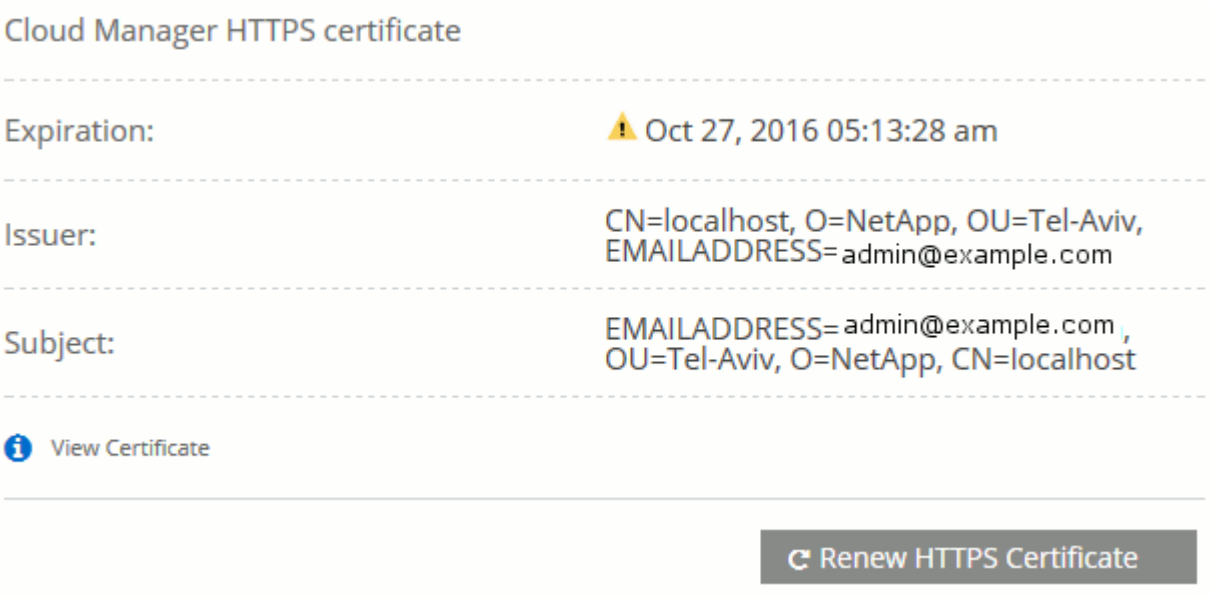


2. En la página HTTPS Setup, instale un certificado generando una solicitud de firma de certificación (CSR) o instalando su propio certificado firmado por una CA:

Opción	Descripción
Genere una CSR	a. Introduzca el nombre de host o DNS del host del conector (su nombre común) y, a continuación, haga clic en **generar CSR**. Cloud Manager muestra una solicitud de firma de certificación. b. Utilice la CSR para enviar una solicitud de certificado SSL a una CA. El certificado debe utilizar el formato X.509 codificado con Privacy Enhanced Mail (PEM) base-64. c. Copie el contenido del certificado firmado, péguelo en el campo Certificado y, a continuación, haga clic en **instalar**.
Instale su propio certificado firmado por CA	a. Seleccione **instalar certificado firmado por CA**. b. Cargue el archivo de certificado y la clave privada y, a continuación, haga clic en **instalar**. El certificado debe utilizar el formato X.509 codificado con Privacy Enhanced Mail (PEM) base-64.

Resultado

Cloud Manager ahora utiliza el certificado firmado por CA para proporcionar acceso HTTPS seguro. En la siguiente imagen se muestra un sistema Cloud Manager configurado para el acceso seguro:



Renovando el certificado HTTPS de Cloud Manager

Debe renovar el certificado HTTPS de Cloud Manager antes de que caduque para garantizar el acceso seguro a la consola web de Cloud Manager. Si no renueva el certificado antes de que caduque, aparece una advertencia cuando los usuarios acceden a la consola Web mediante HTTPS.

Pasos

1. En la parte superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **Configuración HTTPS**.

   Se muestran detalles sobre el certificado de Cloud Manager, incluida la fecha de vencimiento.

2. Haga clic en **renovar certificado HTTPS** y siga los pasos para generar una CSR o instalar su propio certificado firmado por CA.

Resultado

Cloud Manager usa el nuevo certificado firmado por la CA para proporcionar acceso HTTPS seguro.

Eliminación de entornos de trabajo de Cloud Volumes ONTAP

El administrador de cuentas puede eliminar un entorno de trabajo de Cloud Volumes ONTAP para moverlo a otro sistema o solucionar problemas de detección.

Acerca de esta tarea

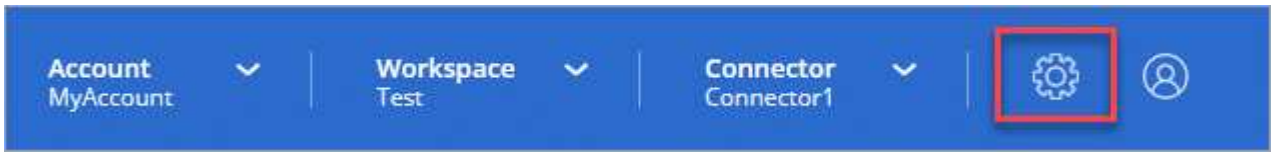
Quitar un entorno de trabajo de Cloud Volumes ONTAP lo elimina de Cloud Manager. No elimina el sistema Cloud Volumes ONTAP. Más tarde podrá volver a descubrir el entorno de trabajo.

La eliminación de un entorno de trabajo de Cloud Manager le permite hacer lo siguiente:

- Redescubrirlo en otro espacio de trabajo
- Redescúbralo en otro sistema Cloud Manager
- Redescubra si tuvo problemas durante el descubrimiento inicial

Pasos

1. En la parte superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **Herramientas**.



2. En la página Herramientas, haga clic en **Iniciar**.
3. Seleccione el entorno de trabajo Cloud Volumes ONTAP que desea quitar.
4. En la página revisar y aprobar, haga clic en **Ir**.

Resultado

Cloud Manager elimina el entorno de trabajo. Los usuarios pueden volver a descubrir este entorno de trabajo desde la página entornos de trabajo en cualquier momento.

Configuración de un conector para utilizar un servidor proxy

Si las directivas de la empresa dictan que utiliza un servidor proxy para todas las comunicaciones HTTP a Internet, debe configurar los conectores para que utilicen ese servidor proxy. El servidor proxy puede estar en la nube o en la red.

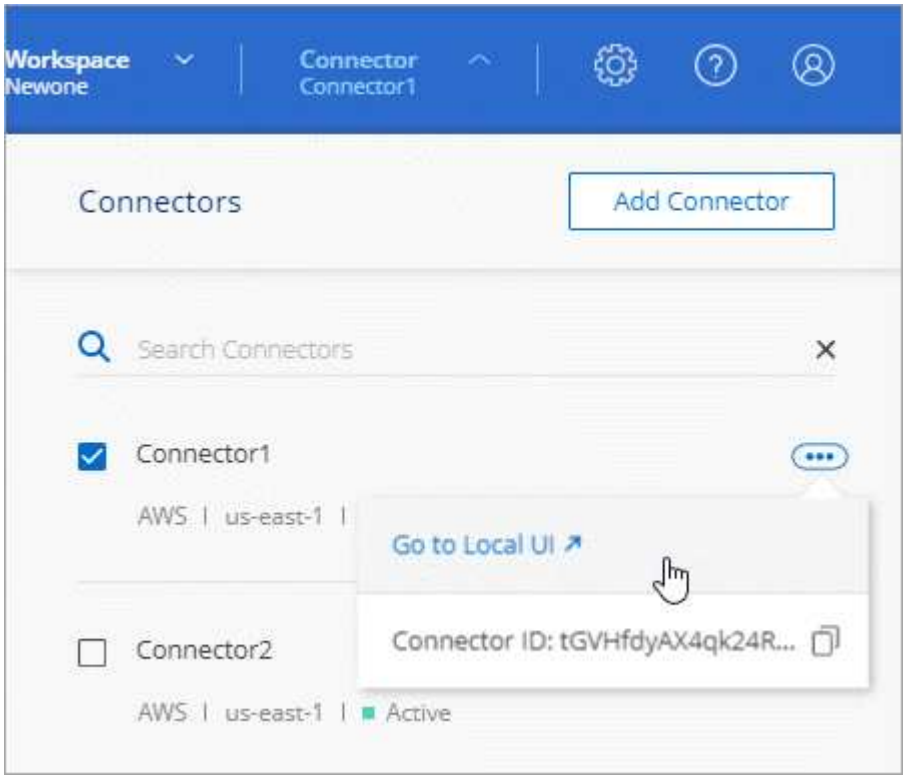
Cuando configura un conector para utilizar un servidor proxy, ese conector y los sistemas Cloud Volumes ONTAP que administra (incluidos los mediadores ha), todos utilizan el servidor proxy.

Pasos

1. "Inicie sesión en la interfaz del SaaS de Cloud Manager" Desde un equipo que tiene una conexión de red a la instancia de conector.

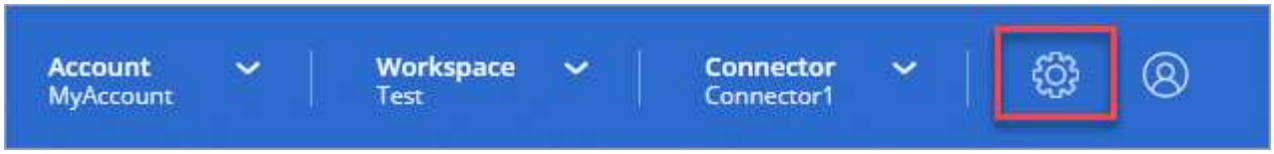
   Si el conector no tiene una dirección IP pública, necesitará una conexión VPN o deberá conectarse desde un host de salto que esté en la misma red que el conector.

2. Haga clic en el menú desplegable **conector** y, a continuación, haga clic en **Ir a la interfaz de usuario local** para ver un conector específico.



   La interfaz de Cloud Manager que se ejecuta en el conector se carga en una nueva pestaña del navegador.

3. En la parte superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **Configuración de Cloud Manager**.



4. En HTTP Proxy, introduzca el servidor con la sintaxis http://address:port, especifique un nombre de usuario y una contraseña si se requiere autenticación básica para el servidor y, a continuación, haga clic en Guardar.

Cloud Manager no admite contraseñas con el carácter @.

Resultado

Después de especificar el servidor proxy, los nuevos sistemas Cloud Volumes ONTAP se configuran automáticamente para utilizar el servidor proxy al enviar mensajes de AutoSupport. Si no especificó el servidor proxy antes de que los usuarios crearan sistemas Cloud Volumes ONTAP, deben usar System Manager para establecer manualmente el servidor proxy en las opciones de AutoSupport para cada sistema.

Anulación de los bloqueos de CIFS para la alta disponibilidad de Cloud Volumes ONTAP en Azure

El administrador de cuentas puede habilitar un ajuste en Cloud Manager para evitar problemas con la conmutación por error del almacenamiento de Cloud Volumes ONTAP durante eventos de mantenimiento de Azure. Cuando se habilita este ajuste, Cloud Volumes ONTAP veta CIFS locks y restablece las sesiones CIFS activas.

Acerca de esta tarea

Microsoft Azure programa eventos de mantenimiento periódicos en sus máquinas virtuales. Cuando se produce un evento de mantenimiento en un nodo de un par de alta disponibilidad de Cloud Volumes ONTAP, el par de alta disponibilidad inicia la toma de control del almacenamiento. Si hay sesiones CIFS activas durante este evento de mantenimiento, los bloqueos de archivos CIFS pueden evitar la conmutación por error del almacenamiento.

Si se habilita esta configuración, Cloud Volumes ONTAP vetará los bloqueos y restablecerá las sesiones CIFS activas. Como resultado, la pareja de alta disponibilidad puede completar los procesos de conmutación por error del almacenamiento durante estos eventos de mantenimiento.

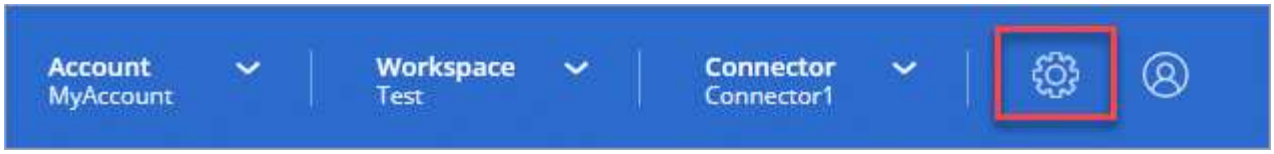
Este proceso puede provocar interrupciones en los clientes CIFS. Se pueden perder los datos que no están comprometidos con los clientes CIFS.

Lo que necesitará

Debe crear un conector antes de poder cambiar la configuración de Cloud Manager. "Vea cómo".

Pasos

1. En la parte superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **Configuración de Cloud Manager**.



2. En **bloqueos CIFS ha**, seleccione la casilla de verificación y haga clic en **Guardar**.

Referencia

Funciones

Las funciones Administrador de cuentas, Administrador de área de trabajo y Visor de cumplimiento de la nube proporcionan permisos específicos a los usuarios.

Tarea	Administrador de cuentas	Administrador de área de trabajo	Visor de cumplimiento de normativas cloud
Gestionar entornos de trabajo	Sí	Sí	No
Activar servicios en entornos de trabajo	Sí	Sí	No
Ver el estado de replicación de datos	Sí	Sí	No
Visualice la línea de tiempo	Sí	Sí	No
Cambiar entre espacios de trabajo	Sí	Sí	Sí
Ver resultados de análisis de cumplimiento	Sí	Sí	Sí
Eliminar entornos de trabajo	Sí	No	No
Conecte los clústeres de Kubernetes a entornos de trabajo	Sí	No	No
Reciba el informe de Cloud Volumes ONTAP	Sí	No	No
Crear conectores	Sí	No	No
Administrar cuentas de Cloud Central	Sí	No	No
Gestionar credenciales	Sí	No	No
Modifique la configuración de Cloud Manager	Sí	No	No
Consulte y gestione la consola de soporte	Sí	No	No
Elimine entornos de trabajo de Cloud Manager	Sí	No	No
Instale un certificado HTTPS	Sí	No	No

Enlaces relacionados

- "Configuración de espacios de trabajo y usuarios en la cuenta de Cloud Central"
- "Gestión de espacios de trabajo y usuarios en la cuenta de Cloud Central"

Cómo Cloud Manager utiliza los permisos de proveedores de cloud

Cloud Manager requiere permisos para realizar acciones en su proveedor de cloud. Estos permisos se incluyen en "Las políticas proporcionadas por NetApp". Tal vez desee entender qué hace Cloud Manager con estos permisos.

Qué hace Cloud Manager con los permisos de AWS

Cloud Manager utiliza una cuenta de AWS para realizar llamadas API a varios servicios de AWS, incluidos EC2, S3, CloudFormation, IAM, Security Token Service (STS) y el servicio de gestión de claves (KMS).

Acciones	Específico
"ec2:StartInstances", "ec2:StopInstances", "ec2:DescribeInstances", "ec2:DescribeInstanceStatus", "ec2:RunInstances", "ec2:TerminateInstances", "ec2:ModificyAttribute",	Inicia una instancia de Cloud Volumes ONTAP y detiene, inicia y supervisa la instancia.
"ec2:DescribeInstanceAttribute",	Verifica que las redes mejoradas están habilitadas para los tipos de instancia admitidos.
"ec2:DescribeRouteTables", "ec2:DescribeImages",	Inicia una configuración de alta disponibilidad de Cloud Volumes ONTAP.
"ec2:CreateTags",	Etiqueta todos los recursos que Cloud Manager crea con las etiquetas "WorkingEnvironment" y "WorkingEnvironmentId". Cloud Manager utiliza estas etiquetas para tareas de mantenimiento y asignación de costes.
"ec2:CreateVolume", "ec2:DescribeVolumes", "ec2:ModifyVolumeAttribute", "ec2:AttachVolume", "ec2:DeleteVolume", "ec2:DetachVolume",	Gestiona los volúmenes de EBS que Cloud Volumes ONTAP utiliza como almacenamiento back-end.
"ec2:CreateSecurityGroup", "ec2:DeleteSecurityGroup", "ec2:DescribeSecurityGroups", "ec2:RevokeSecurityGroupEgress", "ec2:AuthorizeSecurityGroupEgress", "ec2:AuthorizeGroupSecurityGroupIngress", "ec2:RevokeSecurityGroupIngress",	Crea grupos de seguridad predefinidos para Cloud Volumes ONTAP.
"ec2:CreateNetworkInterface", "ec2:DescribeNetworkInterface", "ec2:DeleteNetworkInterface", "ec2:ModifyNetworkInterfaceAttribute",	Crea y administra interfaces de red para Cloud Volumes ONTAP en la subred de destino.
"ec2:DescribeSubnets", "ec2:DescribeVpcs",	Obtiene la lista de subredes de destino y grupos de seguridad, que se necesita al crear un nuevo entorno de trabajo para Cloud Volumes ONTAP.

Acciones	Específico
"ec2:DescribDhcpOptions",	Determina los servidores DNS y el nombre de dominio predeterminado al iniciar instancias de Cloud Volumes ONTAP.
"ec2:CreateSnapshot", "ec2:DeleteSnapshot", "ec2:DescribeSnapshots",	Toma snapshots de volúmenes de EBS durante la configuración inicial y cada vez que se detiene una instancia de Cloud Volumes ONTAP.
"ec2:GetConsoleOutput",	Captura la consola de Cloud Volumes ONTAP, que está conectada a mensajes de AutoSupport.
"ec2:DescribeKeyPairs",	Obtiene la lista de pares de claves disponibles al iniciar instancias.
"ec2:regiones describidas",	Obtiene una lista de las regiones disponibles de AWS.
"ec2:DeleteTags", "ec2:DescribeTags",	Gestiona etiquetas de los recursos asociados a instancias de Cloud Volumes ONTAP.
"Cloudformation:CreateStack", "cloudformation:DeleteStack", "cloudformation:Describestacks", "cloudformation:DescribeStackEvents", "cloudformation:ValidateTemplate",	Inicia instancias de Cloud Volumes ONTAP.
"iam:PassRole", "iam:CreateRole", "iam:DeleteRole", "iam:PutRolePolicy", "iam:CreateInstanceProfile", "iam:DeleteRololePolicy", "iam:AddRoleToInstanceProfile", "iam:RemoveRoleFromInstanceProfile", "DeleteInstanceProfile"	Inicia una configuración de alta disponibilidad de Cloud Volumes ONTAP.
"iam:ListInstanceProfiles", "sts:DecodeAuthorizationMessage", "ec2:AssociateIamInstanceProfile", "ec2:DescribeIamInstanceProfileAssociations", "ec2:DisasociateIamanceProfile",	Administra perfiles de instancia para instancias de Cloud Volumes ONTAP.
"s3:GetBucketTagging", "s3:GetBucketLocation", "s3:ListAllMyBuckets", "s3:ListBucket"	Obtiene información sobre cubos de AWS S3 para que Cloud Manager pueda integrarse con el servicio Data Fabric Cloud Sync de NetApp.
"s3:CreateBucket", "s3:DeleteBucket", "s3:GetLifecycleConfiguration", "s3:PutLifecycleConfiguration", "s3:PutBucketTagging", "s3:ListBucketVersions", "bucs3:GetBucketPolicyStatus", "s3:GetBucketAccessBlock", "PublicGetS3:GetPutketPolicy", "buckets3", "buckets3:AccessPolicy"	Gestiona el bloque de S3 que un sistema Cloud Volumes ONTAP utiliza como nivel de capacidad para la organización de datos en niveles.
"Kms:List*", "kms:Recifrar*", "kms:describir*", "kms:CreateGrant",	Habilita el cifrado de datos de Cloud Volumes ONTAP mediante el Servicio de gestión de claves (KMS) de AWS.

Acciones	Específico
"ce:GetReservationUtilization", "CE:GetDimensionValues", "CE:GetCostAndUsage", "CE:getTags"	Obtiene los datos de costes de AWS para Cloud Volumes ONTAP.
"ec2:CreatePlacementGroup", "ec2:DeletePlacementGroup"	Al poner en marcha una configuración de alta disponibilidad en una única zona de disponibilidad de AWS, Cloud Manager lanza los dos nodos de alta disponibilidad y el mediador en un grupo de colocación extendido de AWS.
"ec2:DescribeReservedInstancesOfferings"	Cloud Manager utiliza el permiso como parte de la implementación de Cloud Compliance para elegir el tipo de instancia que desea utilizar.
"s3:DeleteBucket", "s3:GetLifecycleConfiguration", "s3:PutLifecycleConfiguration", "s3:PutketPolicyTaging", "s3:ListBucketVersions", "s3:BucketBucketBucket", "s3:ListAccessAllAccessMyBuckets", "s3:GetBucketPolicyPolicy", "getbuckets3", "BucketS3:GetBucketBucketBucketBucketBlock", "BucketS3", "BucketS3:GetBucketS3", "BucketBucketS3", "GetBucketBucketBucketBucketBucketBucketBucketBucketBucketBlock",", "	Cloud Manager utiliza estos permisos cuando se habilita el servicio Backup en S3.

Qué hace Cloud Manager con permisos de Azure

La política de Cloud Manager para Azure incluye los permisos que necesita Cloud Manager para implementar y gestionar Cloud Volumes ONTAP en Azure.

Acciones	Específico
"Microsoft.Compute/locations/operations/read", "Microsoft.Compute/locations/vmSizes/read", "Microsoft.Compute/operations/read", "Microsoft.Compute/virtualMachines/instanceView/read", "Microsoft.Compute/virtualMachines/powerOff/action", "Microsoft.Compute/virtualMachines/read", "Microsoft.Compute/virtualMachines/restart/action", "Microsoft.Compute/virtualMachines/start/action", "Microsoft.Compute/virtualMachines/deallocate/action", "Microsoft.Compute/virtualMachines/vmSizes/read", "Microsoft.Compute/virtualMachines/write",	Crea Cloud Volumes ONTAP y detiene, inicia, elimina y obtiene el estado del sistema.
"Microsoft.Compute/images/write", "Microsoft.Compute/images/read",	Permite la puesta en marcha de Cloud Volumes ONTAP desde un disco duro virtual.

Acciones	Específico
"Microsoft.Compute/disks/delete", "Microsoft.Compute/disks/read", "Microsoft.Compute/disks/write", "Microsoft.Storage/checknameAvailability/read", "Microsoft.Storage/opers/read", "Microsoft.Storage/storageAccounts/listkeys/action", "Microsoft.Storage/Accounts/read", "Microsoft.Storage/storageAccounts/regeneratekey/action", "Microsoft.Storage/Storage Accounts/write", "Storage.files/Storage/Storage/Storage Accounts", "	Gestiona cuentas de almacenamiento y discos de Azure y conecta los discos a Cloud Volumes ONTAP.
"Microsoft.Network/networkInterfaces/read", "Microsoft.Network/networkInterfaces/write", "Microsoft.Network/networkInterfaces/join/action",	Crea y administra interfaces de red para Cloud Volumes ONTAP en la subred de destino.
"Microsoft.Network/networkSecurityGroups/read", "Microsoft.Network/networkSecurityGroups/write", "Microsoft.Network/networkSecurityGroups/join/action",	Crea grupos de seguridad de red predefinidos para Cloud Volumes ONTAP.
"Microsoft.Resources/subscripciones/ubicaciones/lecturas", "Microsoft.Network/locations/operationResults/read", "Microsoft.Network/locations/operations/read", "Microsoft.Network/virtualNetworks/read", "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read", "Microsoft.Network/virtualNetworks/subnets/read", "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read", "Microsoft.Network/virtualNetworks/virtualMachines/read", "Microsoft.Network/virtualNetworks/subnets/join/action",	Obtiene información de red acerca de las regiones, la red virtual de destino y la subred, y agrega Cloud Volumes ONTAP a las redes virtuales.
"Microsoft.Network/virtualNetworks/subnets/write", "Microsoft.Network/routeTables/join/action",	Habilita extremos de servicio vnet para organizar los datos en niveles.
"Microsoft.Resources/despliegues/operaciones/lectura", "Microsoft.Resources/despliegues/read", "Microsoft.Resources/despliegues/write",	Implementa Cloud Volumes ONTAP a partir de una plantilla.

Acciones	Específico
"Microsoft.Resources/despliegues/operacions/read", "Microsoft.Resources/despliegues/read", "Microsoft.Resources/despliegues/write", "Microsoft.Resources/resources/read", "Microsoft.Resources/Resources/operationResults/read", "Microsoft.Resources/subscripciones/ResourceGroups/delete", "Microsoft.Resources/subscripciones/Groups/read/resources", "ResourceGroups/subscripciones"/resources/Microsoft.Resources/subscriptions/Microsoft","/resources/subscripciones"/resources/Microsoft.Microsoft/resources/resources/Microsoft.read/subscriptions/resources	Crea y gestiona grupos de recursos para Cloud Volumes ONTAP.
"Microsoft.Compute/snapshots/write", "Microsoft.Compute/snapshots/read", "Microsoft.Compute/disks/beginGetAccess/action"	Crea y gestiona copias Snapshot gestionadas de Azure.
"Microsoft.Compute/availabilitySets/write", "Microsoft.Compute/availabilitySets/read",	Crea y administra conjuntos de disponibilidad para Cloud Volumes ONTAP.
"Microsoft.MarketPlaceorders/offertypes/editoriales/Ofertas/planes/acuerdos/leídos", "Microsoft.MarketPlaceoring/offertypes/editoriales/Ofertas/planes/acuerdos/escribir"	Permite puestas en marcha mediante programación desde Azure Marketplace.
"Microsoft.Network/loadBalancers/read", "Microsoft.Network/loadBalancers/write", "Microsoft.Network/loadBalancers/delete", "Microsoft.Network/loadBalancers/backendAddressPools/read", "Microsoft.Network/loadBalancers/backendAddressPools/join/action", "Microsoft.Network/loadBalancers/frontendIPConfigurations/read", "Microsoft.Network/loadBalancers/loadBalancingRules/read", "Microsoft.Network/loadBalancers/probes/read", "Microsoft.Network/loadBalancers/probes/join/action",	Gestiona un equilibrador de carga de Azure para pares de alta disponibilidad.
"Microsoft.Autorizaciones/bloqueos/*"	Permite la gestión de bloqueos en discos de Azure.
"Microsoft.Authorization/roleDefinitions/write", "Microsoft.Authorization/roleAssignments/write", "Microsoft.Web/sites/*"	Gestiona la conmutación por error para pares de alta disponibilidad.

Acciones	Específico
"Microsoft.Network/privateEndpoints/write", "Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action", "Microsoft.Storage/storageAccounts/privateEndpointConnections/read", "Microsoft.Network/privateEndpoints/read", "Microsoft.Network/privateDnsZones/write", "Microsoft.Network/privateDnsZones/virtualNetworkLinks/write", "Microsoft.Network/virtualNetworks/join/action", "Microsoft.Network/privateDnsZones/A/write", "Microsoft.Network/privateDnsZones/read", "Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",	Permite la gestión de extremos privados. Los extremos privados se utilizan cuando no se proporciona conectividad fuera de la subred. Cloud Manager crea la cuenta de almacenamiento para alta disponibilidad con solo conectividad interna en la subred.
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",	Permite a Cloud Manager eliminar volúmenes para Azure NetApp Files.
"Microsoft.Resources/despliegues/operationStatuses/Read"	Azure requiere este permiso para algunas implementaciones de máquinas virtuales (depende del hardware físico subyacente que se haya utilizado durante la implementación).
"Microsoft.Resources/despliegues/operationStatuses/read", "Microsoft.Insights/Metrics/Read", "Microsoft.Compute/virtualMachines/extensions/write", "Microsoft.Compute/virtualMachines/extensions/read", "Microsoft.Compute/virtualMachines/extensions/delete", "Microsoft.Compute/virtualMachines/delete", "Microsoft.Network/networkInterfaces/delete", "Microsoft.Network/networkSecurityGroups/delete", "Microsoft.Resources/despliegues/delete",	Permite usar la caché de archivos global.
"Microsoft.Compute/diskEncryptionSets/read"	Permite a Cloud Manager cifrar discos gestionados de Azure en sistemas Cloud Volumes ONTAP de un solo nodo mediante claves externas de otra cuenta. Esta función es compatible con el uso de API.

Qué hace Cloud Manager con los permisos de GCP

La política de Cloud Manager para GCP incluye los permisos que Cloud Manager necesita para implementar y gestionar Cloud Volumes ONTAP.

Acciones	Específico
- Compute.disks.create - compute.disks.createSnapshot - compute.disks.delete - compute.disks.get - compute.disks.list - compute.disks.setLabels - compute.disks.use	Para crear y gestionar discos para Cloud Volumes ONTAP.
- computar.firewalls.create - compute.firewalls.delete - computar.firewalls.get - computar.firewalls.list	Para crear reglas de firewall para Cloud Volumes ONTAP.
- Compute.globalOperations.get	Para obtener el estado de las operaciones.

Acciones	Específico
- compute.images.get - compute.images.getFromFamily - compute.images.list - compute.images.useReadOnly	Para obtener imágenes para instancias de equipos virtuales.
- compute.instances.attachDisk - compute.instances.detachDisk	Para conectar y desconectar discos en Cloud Volumes ONTAP.
- compute.instances.create - compute.instances.delete	Para crear y eliminar instancias de Cloud Volumes ONTAP VM.
- compute.instances.get	Para mostrar instancias de máquina virtual.
- compute.instances.getSerialPortOutput	Para obtener los registros de la consola.
- compute.instances.list	Para recuperar la lista de instancias de una zona.
- compute.instances.setDeletionProtection	Para establecer la protección de eliminación en la instancia.
- compute.instances.setLabels	Para agregar etiquetas.
- compute.instances.setMachineType	Para cambiar el tipo de máquina para Cloud Volumes ONTAP.
- compute.instances.setMetadata	Para añadir metadatos.
- compute.instances.setTags	Para agregar etiquetas para reglas de firewall.
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	Para iniciar y detener Cloud Volumes ONTAP.
- computar.machineTypes.get	Para obtener el número de núcleos para comprobar qoutras.
- compute.projects.get	Para dar soporte a proyectos múltiples.
- Compute.snapshots.create - compute.snapshots.delete - compute.snapshots.get - compute.snapshots.list - compute.snapshots.setLabels	Para crear y gestionar instantáneas de disco persistentes.
- compute.networks.get - compute.networks.list - compute.regions.get - compute.regises.list - compute.subnetworks.get - Compute.subNetworks.list - Compute.zoneOperations.get - Compute.zones.get - Compute.zones.list	Para obtener la información de red necesaria para crear una nueva instancia de máquina virtual de Cloud Volumes ONTAP.

Acciones	Específico
- deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list - deploymentmanager.manifests.get - deploymentmanager.manifest.list - deploymentmanager.opers.get - deploymentmanager.opers.list - deploymentmanager.resources.get - deploymentmanager.resources.list - deploymentmanager.typeProviders.get - deploymentmanager.typeProviders.list - deploymentmanager.Types.get - deploymentmanager.types.list	Para poner en marcha la instancia de máquina virtual de Cloud Volumes ONTAP mediante Google Cloud Deployment Manager.
- logEntries.list - logging.privateLogEntries.list	Para obtener unidades de registro de pila.
- resourcemanager.projects.get	Para dar soporte a proyectos múltiples.
- storage.buckets.create - storage.buckets.delete - storage.buckets.get - storage.buckets.list - storage.buckets.update	Para crear y gestionar un bucket de Google Cloud Storage para la organización de datos en niveles.
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudKMS.cryptoKeys.get - cloudKMS.cryptoKeys.list - cloudKMS.Keyring.list	Para utilizar claves de cifrado gestionadas por el cliente desde el Servicio de gestión de claves cloud con Cloud Volumes ONTAP.
- compute.instances.setServiceAccount - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list	Para establecer una cuenta de servicio en la instancia de Cloud Volumes ONTAP. Esta cuenta de servicio proporciona permisos para organizar los datos en niveles en un bloque de Google Cloud Storage.

Páginas de AWS Marketplace para Cloud Manager y Cloud Volumes ONTAP

Existen varias ofertas disponibles en el mercado de AWS para Cloud Manager y Cloud Volumes ONTAP. Si necesita ayuda para entender el propósito de cada página, lea las descripciones a continuación.

En todos los casos, recuerde que no puede iniciar Cloud Volumes ONTAP en AWS desde AWS Marketplace. Es necesario iniciar directamente desde Cloud Manager.

Objetivo	Página AWS Marketplace para utilizar	Más información
Habilite el uso de Cloud Volumes ONTAP PAYGO, Cloud Tiering, Cloud Compliance y otros servicios adicionales	"Cloud Manager: Ponga en marcha y gestione los servicios de datos en el cloud de NetApp"	Esta suscripción permite cobrar la versión de PAYGO de Cloud Volumes ONTAP 9.6 y posterior. También permite cobrar los niveles del cloud, Cloud Compliance y otros servicios adicionales. Deberá suscribirse a esta oferta cuando Cloud Manager le solicite y le redireccione a la página. Cloud Manager le solicita en el asistente de entorno de trabajo o cuando agrega nuevas credenciales en Configuración. Esta página no le permite iniciar Cloud Manager en AWS. Eso se debe hacer desde "Cloud Central de NetApp"O bien, utilizando el AMI que se indica en la fila 3 de esta tabla.
Habilite el uso de Cloud Volumes ONTAP PAYGO, Cloud Tiering, Cloud Compliance y otros servicios adicionales *usando un contrato anual*	"Cloud Manager (contratos): Implemente gestione los servicios de datos en el cloud de NetApp"	Esta suscripción es una alternativa a la suscripción en la primera fila. Le permite obtener un pago inicial anual para los listings. En la mayoría de los casos está destinada a partners de NetApp.
Ponga en marcha Cloud Manager desde AWS Marketplace mediante un AMI	"Cloud Manager: Instalación manual sin claves de acceso"	Le recomendamos que ejecute Cloud Manager en AWS desde "Cloud Central de NetApp", pero puede iniciarlo desde esta página de AWS Marketplace, si lo prefiere.
Permitir la puesta en marcha de Cloud Volumes ONTAP PAYGO (9.5 o anterior)	• "Cloud Volumes ONTAP para AWS" • "Cloud Volumes ONTAP para AWS: Alta disponibilidad"	Estas páginas de AWS Marketplace le permiten suscribirse a las versiones de nodo único o ha de Cloud Volumes ONTAP PAYGO para las versiones 9.5 y anteriores. A partir de la versión 9.6, tiene que suscribirse a la página de AWS Marketplace que se encuentra en la fila 1 de esta tabla para las puestas en marcha de PAYGO.

Utilice API y automatización

Recursos de automatización para la infraestructura como código

Utilice los recursos de esta página para obtener ayuda para la integración Cloud Manager y Cloud Volumes ONTAP con su "infraestructura como código".

Los equipos de DevOps utilizan diversas herramientas para automatizar la configuración de nuevos entornos, lo que les permite tratar la infraestructura como código. Una de esas herramientas es Terraform. Hemos desarrollado un proveedor de Terraform que los equipos de DevOps pueden utilizar con Cloud Manager para automatizar e integrar Cloud Volumes ONTAP con la infraestructura como código.

"Consulte el proveedor de cloud-mManager de netapp".

Enlaces relacionados

- "Blog de cloud de NetApp: Uso de API DE REST de Cloud Manager con acceso federado"
- "Blog sobre cloud de NetApp: Automatización cloud con Cloud Volumes ONTAP Y REST"
- "Blog sobre cloud de NetApp: Clonado de datos automatizado para pruebas de aplicaciones de software basadas en cloud"
- "Blog de NetApp: Infrastructure-as-Code (IAC) Accelerated with Ansible + NetApp"
- "ThePub de NetApp: Gestión de configuraciones y automatización con Ansible"
- "ThePub de NetApp: Roles para el uso de Ansible ONTAP"

Dónde encontrar ayuda y más información

Puede obtener ayuda y encontrar más información sobre Cloud Manager y Cloud Volumes ONTAP a través de diversos recursos, como vídeos, foros y soporte.

- "Soporte Cloud Volumes ONTAP de NetApp"

  Acceda a recursos de soporte para obtener ayuda y solucionar problemas con Cloud Volumes ONTAP.

- "Vídeos para Cloud Manager y Cloud Volumes ONTAP"

  Vea vídeos que le muestran cómo poner en marcha y gestionar Cloud Volumes ONTAP, así como cómo replicar datos en su cloud híbrido.

- "Políticas para Cloud Manager"

  Descargue los archivos JSON que incluyen los permisos que Cloud Manager necesita para realizar acciones en un proveedor de cloud.

- "Guía para desarrolladores de API de Cloud Manager"

  Lea una descripción general de las API, ejemplos de cómo utilizarlas y una referencia de API.

- Formación para Cloud Volumes ONTAP
  - "Principios básicos de Cloud Volumes ONTAP"
  - "Implementación y gestión de Cloud Volumes ONTAP para Azure"
  - "Implementación y gestión de Cloud Volumes ONTAP para AWS"
- Informes técnicos
  - "Informe técnico de NetApp 4383: Caracterización del rendimiento de Cloud Volumes ONTAP en Amazon Web Services con cargas de trabajo de las aplicaciones"
  - "Informe técnico de NetApp 4671: Caracterización del rendimiento de Cloud Volumes ONTAP en Azure con cargas de trabajo de aplicaciones"
  - "Informe técnico de NetApp 4816: Caracterización del rendimiento de Cloud Volumes ONTAP para Google Cloud"
- Recuperación ante desastres de SVM

  La recuperación ante desastres de SVM es el mirroring asíncrono de los datos de SVM y la configuración de una SVM de origen a una SVM de destino. Puede activar rápidamente una SVM de destino para el acceso a los datos si la SVM de origen ya no está disponible.

  - "Guía exprés de preparación para la recuperación de desastres de SVM de Cloud Volumes ONTAP 9"

    Describe cómo configurar rápidamente una SVM de destino con el fin de prepararse para la recuperación de desastres.

  - "Guía exprés de recuperación de desastres de SVM de Cloud Volumes ONTAP 9"

    Describe cómo activar rápidamente una SVM de destino después de un desastre y, a continuación, reactivar la SVM de origen.

- "Guía completa de volúmenes de FlexCache para un acceso más rápido a los datos"

  Describe cómo crear y gestionar volúmenes de FlexCache en el mismo clúster o en un clúster diferente como volumen de origen para acelerar el acceso a los datos.

- "Notificaciones de seguridad"

  Identifique las vulnerabilidades conocidas (CVE) para los productos de NetApp, incluido ONTAP. Tenga en cuenta que puede subsanar las vulnerabilidades de seguridad de Cloud Volumes ONTAP mediante la siguiente documentación de ONTAP.

- "Centro de documentación de ONTAP 9"

  Acceda a documentación de productos para ONTAP, que puede ayudarle cuando utilice Cloud Volumes ONTAP.

- "Comunidad de NetApp: Servicios de datos en el cloud"

  Conéctese con colegas, realice preguntas, intercambie ideas, encuentre recursos y comparta prácticas recomendadas.

- "Cloud Central de NetApp"

  Encuentre información sobre otros productos y soluciones de NetApp para el cloud.

- "Documentación de productos de NetApp"

  Busque en la documentación de productos de NetApp instrucciones, recursos y respuestas.

Versiones anteriores de la documentación de Cloud Manager

La documentación de versiones anteriores de Cloud Manager está disponible en caso de que no esté ejecutando la versión más reciente.

- "Cloud Manager 3.7"
- "Cloud Manager 3.6"

Avisos legales

Los avisos legales proporcionan acceso a las declaraciones de copyright, marcas comerciales, patentes y mucho más.

Derechos de autor

http://www.netapp.com/us/legal/copyright.aspx

Marcas comerciales

NETAPP, el logotipo de NETAPP y las marcas enumeradas en la página de marcas comerciales de NetApp son marcas comerciales de NetApp, Inc. Los demás nombres de empresas y productos son marcas comerciales de sus respectivos propietarios.

http://www.netapp.com/us/legal/netapptmlist.aspx

Estadounidenses

Puede encontrar una lista actual de las patentes propiedad de NetApp en:

https://www.netapp.com/us/media/patents-page.pdf

Política de privacidad

https://www.netapp.com/us/legal/privacypolicy/index.aspx

Código abierto

Los archivos de notificación proporcionan información sobre los derechos de autor y las licencias de terceros que se utilizan en software de NetApp.

- "Aviso para Cloud Manager 3.8.7"
- "Aviso para Cloud Manager 3.8.6"
- "Aviso para Cloud Manager 3.8.5"
- "Aviso para Cloud Manager 3.8.4"
- "Aviso para Cloud Manager 3.8.3"
- "Aviso para Cloud Manager 3.8.2"
- "Aviso para Cloud Manager 3.8.1"
- "Aviso para Cloud Manager 3.8"
- "Aviso para el Cloud Backup Service"
- "Aviso de caché de archivos global"
- "Aviso de cumplimiento de normativas cloud"