Documentación de Cloud Manager y Cloud Volumes ONTAP

Cloud Manager 3.7

NetApp
March 25, 2024

Tabla de contenidos

Documentación de Cloud Manager y Cloud Volumes ONTAP

Cloud Manager le permite poner en marcha y gestionar Cloud Volumes ONTAP de NetApp, una solución de gestión de datos que ofrece protección, visibilidad y control para sus cargas de trabajo basadas en cloud.

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

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

Manos a la obra

- "Empiece a usar AWS"
- "Empiece a usar Azure"
- "Comience a usar Google Cloud Platform"
- "Busque las configuraciones compatibles para Cloud Volumes ONTAP"
- "Revise los requisitos de red para Cloud Manager"
- "Revise los requisitos de red para Cloud Volumes ONTAP para AWS"
- "Revise los requisitos de red para Cloud Volumes ONTAP para Azure"
- "Revise los requisitos de red para Cloud Volumes ONTAP para GCP"
- "Planifique la configuración de Cloud Volumes ONTAP"

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 3.7

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

¿Busca una versión anterior?"Novedades en 3.6"
"Novedades en 3.5"
"Novedades en 3.4"

Actualización de Cloud Manager 3.7.5 (16 de diciembre de 2019)

Esta actualización incluye las siguientes mejoras:

- Cloud Volumes ONTAP 9.7
- Cumplimiento de normativas cloud para Cloud Volumes ONTAP

Cloud Volumes ONTAP 9.7

Cloud Volumes ONTAP 9.7 ya está disponible en AWS, Azure y Google Cloud Platform.

"Vea las novedades de Cloud Volumes ONTAP 9.7".

Cumplimiento de normativas cloud para Cloud Volumes ONTAP

Cloud Compliance es un servicio de privacidad y cumplimiento de normativas de datos para Cloud Volumes ONTAP en AWS y Azure. Mediante la tecnología basada en la inteligencia artificial (IA), Cloud Compliance ayuda a las organizaciones a comprender el contexto de los datos e identificar los datos confidenciales en los sistemas de Cloud Volumes ONTAP.

Cloud Compliance está actualmente disponible como versión de disponibilidad controlada.

"Más información sobre Cloud Compliance".

Cloud Manager 3.7.5 (3 de diciembre de 2019)

Cloud Manager 3.7.5 incluye las siguientes mejoras.

- Alta velocidad de escritura para Cloud Volumes ONTAP en GCP
- Clústeres de ONTAP en las instalaciones como almacenamiento persistente para Kubernetes
- Última versión de Trident para Kubernetes
- Compatibilidad con cuentas de almacenamiento de Azure de uso general v2
- Prefijos de los nombres de cuentas de almacenamiento de Azure mediante API

Alta velocidad de escritura para Cloud Volumes ONTAP en GCP

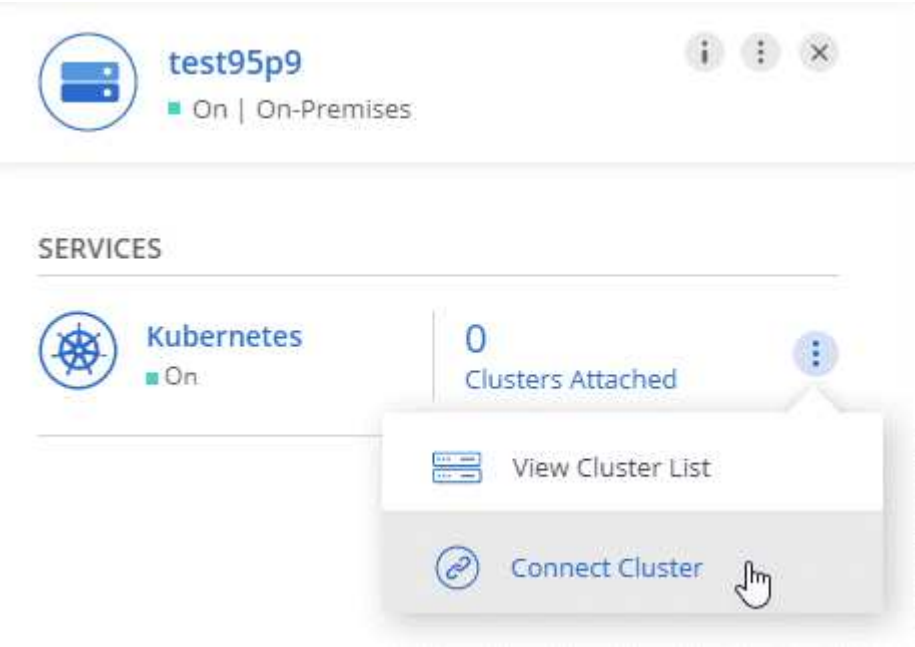
Ahora puede habilitar una alta velocidad de escritura en sistemas de Cloud Volumes ONTAP nuevos y existentes en Google Cloud Platform. La alta velocidad de escritura es una buena opción si se requiere rendimiento de escritura rápido para su carga de trabajo.

- "Aprenda a elegir una velocidad de escritura"
- "Aprenda a cambiar la velocidad de escritura en sistemas existentes"

Clústeres de ONTAP en las instalaciones como almacenamiento persistente para Kubernetes

Cloud Manager ahora le permite usar clústeres ONTAP locales como almacenamiento persistente para contenedores. Al igual que Cloud Volumes ONTAP, Cloud Manager automatiza la puesta en marcha de Trident de NetApp y conecta ONTAP con los clústeres de Kubernetes.

Después de añadir un clúster de Kubernetes a Cloud Manager, puede conectarlo a los clústeres de ONTAP en las instalaciones desde la página entornos de trabajo:



"Aprenda cómo empezar".

Última versión de Trident para Kubernetes

Cloud Manager ahora instala una versión más reciente de Trident (versión 19.07.1) cuando se conecta un entorno de trabajo a un clúster de Kubernetes.

Compatibilidad con cuentas de almacenamiento de Azure de uso general v2

A la hora de implementar nuevos sistemas Cloud Volumes ONTAP en Azure, las cuentas de almacenamiento que Cloud Manager crea para diagnósticos y organización en niveles de datos ahora son cuentas de almacenamiento de v2 de uso general.

Prefijos de los nombres de cuentas de almacenamiento de Azure mediante API

Ahora puede añadir un prefijo para los nombres de las cuentas de almacenamiento de Azure que crea Cloud Manager para Cloud Volumes ONTAP. Solo tiene que usar el parámetro *storageAccountPrefix* cuando

implementa un nuevo sistema Cloud Volumes ONTAP en Azure.

"Consulte la Guía para desarrolladores de API para obtener más detalles sobre el uso de API".

Cloud Manager 3.7.4 (6 de octubre de 2019)

Cloud Manager 3.7.4 incluye las siguientes mejoras.

- Compatibilidad con Azure NetApp Files
- Mejoras de Cloud Volumes ONTAP para GCP
- Mejora de backup en S3
- Cifrado de discos de arranque y raíz en AWS
- Compatibilidad con la región de AWS Bahréin
- Compatibilidad con la región norte de Azure Emiratos Árabes Unidos

Compatibilidad con Azure NetApp Files

Ahora puede ver y crear NFS Volumes para Azure NetApp Files directamente desde Cloud Manager. Esta mejora continúa con nuestro objetivo de ayudarle a gestionar su almacenamiento en cloud desde una única interfaz.

"Aprenda cómo empezar".

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

```
"Microsoft.NetApp/netAppAccounts/read",
"Microsoft.NetApp/netAppAccounts/capacityPools/read",
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete"
```

Mejoras de Cloud Volumes ONTAP para GCP

Cloud Manager 3.7.4 ofrece las siguientes mejoras en Cloud Volumes ONTAP para Google Cloud Platform:

Suscripciones de pago por uso en GCP Marketplace

Ahora puede pagar por Cloud Volumes ONTAP cuando lo usa suscribiéndose a Cloud Volumes ONTAP en el mercado de Google Cloud Platform.

"Mercado de Google Cloud Platform: Cloud Manager para Cloud Volumes ONTAP"

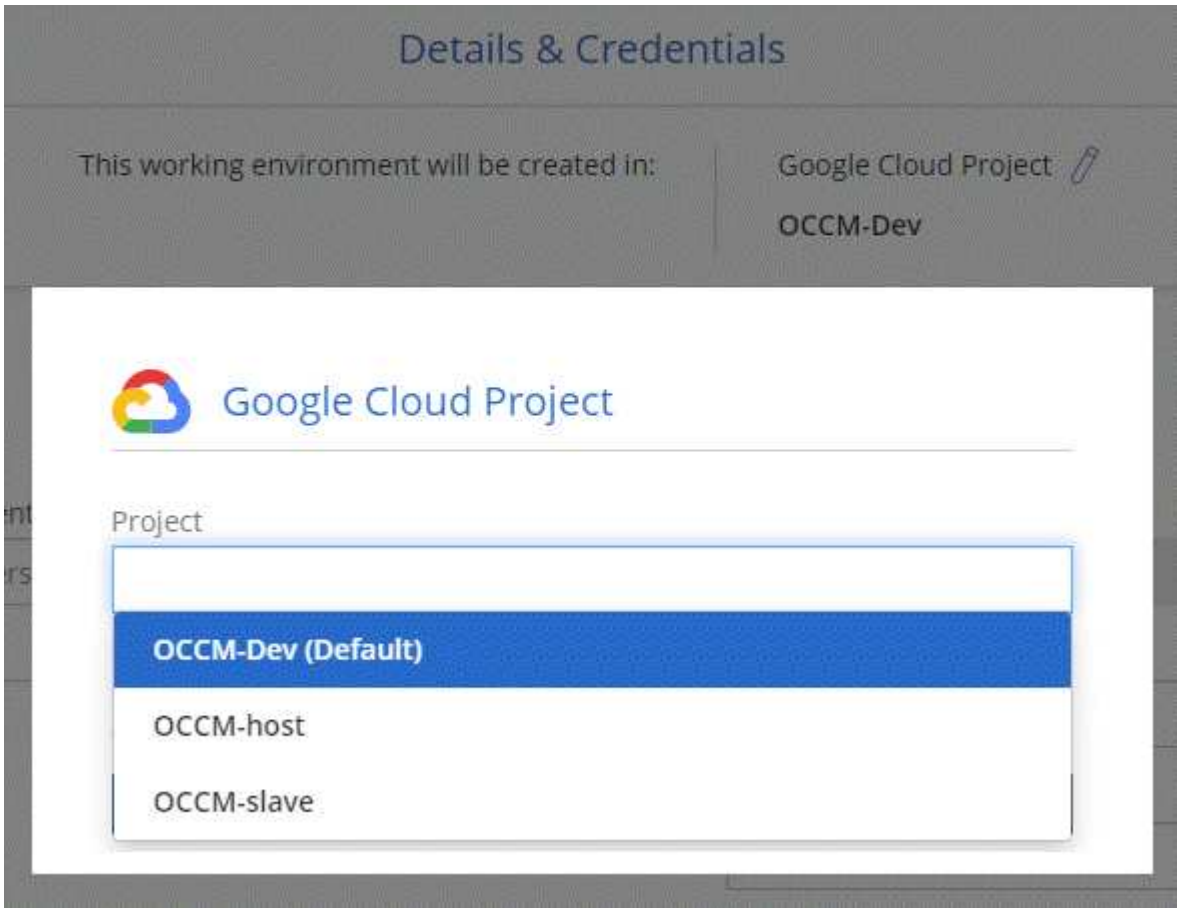
VPC compartido

Cloud Manager y Cloud Volumes ONTAP ahora son compatibles con un VPC compartido de Google Cloud Platform.

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 Cloud Manager y Cloud Volumes ONTAP en un *proyecto de servicio*. "Documentación de Google Cloud: Información general sobre VPC compartido".

Varios proyectos de Google Cloud

Cloud Volumes ONTAP ya no tiene por qué estar en el mismo proyecto que Cloud Manager. Añada la cuenta de servicio y el rol de Cloud Manager a otros proyectos y podrá elegir entre aquellos proyectos que ponga en marcha Cloud Volumes ONTAP.



Si quiere más información sobre cómo configurar la cuenta de servicio de Cloud Manager, "consulte el paso 4b en esta página".

Claves de cifrado gestionadas por los clientes al usar las API de Cloud Manager

Mientras Google Cloud Storage siempre cifra sus datos antes de escribirlos en el disco, puede usar las API de Cloud Manager para crear un nuevo 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.

Consulte la "Guía para desarrolladores de API" Para obtener más información sobre el uso de los parámetros "GcpEncryption".

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

```
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
```

Mejora de backup en S3

Ahora es posible eliminar los backups de los volúmenes existentes. Antes, solo se podían eliminar los backups de los volúmenes que se habían eliminado.

"Más información acerca de Backup en S3".

Cifrado de discos de arranque y raíz en AWS

Cuando habilita el cifrado de datos con el Servicio de administración de claves de AWS (KMS), los discos de arranque y raíz para Cloud Volumes ONTAP ahora 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.

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.

Compatibilidad con la región de AWS Bahréin

Cloud Manager y Cloud Volumes ONTAP ahora son compatibles con la región de AWS Oriente Medio (Bahrein).

Compatibilidad con la región norte de Azure Emiratos Árabes Unidos

Cloud Manager y Cloud Volumes ONTAP ahora son compatibles con Azure Emiratos Árabes Unidos al Norte.

"Ver todas las regiones admitidas".

Actualización de Cloud Manager 3.7.3 (15 de septiembre de 2019)

Cloud Manager ahora le permite realizar backups de datos desde Cloud Volumes ONTAP en Amazon S3.

Backup en S3

Backup a S3 es un servicio complementario para Cloud Volumes ONTAP que ofrece funcionalidades de backup y restauración totalmente gestionadas para la protección y un archivado a largo plazo de sus datos en el cloud. Los backups se almacenan en el almacenamiento de objetos de S3, independientemente de las copias Snapshot de volúmenes que se utilicen para la recuperación o el clonado a corto plazo.

"Aprenda cómo empezar".

Esta función requiere una actualización de "Política de Cloud Manager". Ahora se requieren los siguientes permisos de extremo VPC:

```
"ec2:DescribeVpcEndpoints",
"ec2:CreateVpcEndpoint",
"ec2:ModifyVpcEndpoint",
"ec2:DeleteVpcEndpoints"
```

Cloud Manager 3.7.3 (11 de septiembre de 2019)

Cloud Manager 3.7.3 incluye las siguientes mejoras.

- Identificación y administración de Cloud Volumes Service para AWS
- Es necesaria una nueva suscripción en AWS Marketplace
- Soporte para AWS GovCloud (EE. UU.-este)

Identificación y administración de Cloud Volumes Service para AWS

Cloud Manager ahora le permite descubrir los volúmenes de cloud del "Cloud Volumes Service para AWS" suscripción. Después de la detección, puede añadir volúmenes de cloud adicionales directamente desde Cloud Manager. Esta mejora ofrece un único panel desde el que puede gestionar su almacenamiento en cloud de NetApp.

"Aprenda cómo empezar".

Es necesaria una nueva suscripción en AWS Marketplace

"Existe una nueva suscripción disponible en AWS Marketplace". Esta suscripción única es necesaria para desplegar Cloud Volumes ONTAP 9.6 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 de Cloud Volumes ONTAP PAYGO que cree y cada función complementaria que habilite.

A partir de la versión 9.6, este nuevo método de suscripción sustituye las dos suscripciones existentes de AWS Marketplace para Cloud Volumes ONTAP PAYGO a las que se ha suscrito previamente. Sigue necesitando suscripciones a través de la "Páginas existentes de AWS Marketplace cuando se pone en marcha el modelo BYOL de Cloud Volumes ONTAP".

"Obtenga más información sobre cada página de AWS Marketplace".

Soporte para AWS GovCloud (EE. UU.-este)

Cloud Manager y Cloud Volumes ONTAP ahora son compatibles con la región AWS GovCloud (EE. UU.-este)

Disponibilidad general de Cloud Volumes ONTAP en GCP (3 de septiembre de 2019)

Cloud Volumes ONTAP ya está disponible de forma general en Google Cloud Platform (GCP) al llevar su propia licencia (BYOL). También está disponible una promoción de pago por uso. La promoción ofrece licencias gratuitas para un número ilimitado de sistemas y caducará a finales de septiembre de 2019.

- "Aprenda a empezar en GCP"
- "Ver las configuraciones admitidas"

Cloud Manager 3.7.2 (5 de agosto de 2019)

- Licencias FlexCache
- Clases de almacenamiento Kubernetes para iSCSI
- Gestión de inodos
- Soporte para la región de Hong Kong en AWS
- Soporte para las regiones de Australia Central en Azure

Licencias FlexCache

Cloud Manager genera ahora una licencia de FlexCache para todos los nuevos sistemas 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.

Clases de almacenamiento Kubernetes para iSCSI

Cuando se conecta Cloud Volumes ONTAP a un clúster de Kubernetes, Cloud Manager ahora crea dos clases de almacenamiento Kubernetes adicionales que se pueden usar con volúmenes persistentes iSCSI:

- **netapp-File-san**: Para vincular volúmenes persistentes iSCSI a sistemas Cloud Volumes ONTAP de un solo nodo
- **netapp-File-redundante-san**: Para vincular volúmenes persistentes iSCSI a pares de alta disponibilidad Cloud Volumes ONTAP

Gestión de inodos

Cloud Manager ahora 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.

Cloud Manager supervisa el uso de nodos de información solo cuando el modo de gestión de capacidad se configura en automático (esta es la configuración predeterminada).

Soporte para la región de Hong Kong en AWS

Cloud Manager y Cloud Volumes ONTAP ahora son compatibles con la región Asia-Pacífico (Hong Kong) en AWS.

Soporte para las regiones de Australia Central en Azure

Cloud Manager y Cloud Volumes ONTAP ahora son compatibles con las siguientes regiones de Azure:

- Australia Central
- Australia Central 2

"Consulte la lista completa de las regiones compatibles".

Actualización sobre copia de seguridad y restauración (15 de julio de 2019)

A partir de la versión 3.7.1, Cloud Manager ya no admite la descarga de un backup y lo utiliza para restaurar la configuración de Cloud Manager. "Debe seguir estos pasos para restaurar Cloud Manager".

Cloud Manager 3.7.1 (1 de julio de 2019)

- Esta versión incluye principalmente correcciones de errores.
- Incluye una mejora: Cloud Manager ahora instala una licencia de cifrado de volúmenes de NetApp (NVE) en cada sistema Cloud Volumes ONTAP registrado en el soporte de NetApp (sistemas nuevos y existentes).
  - "Adición de cuentas del sitio de soporte de NetApp a Cloud Manager"

- "Registro de sistemas de pago por uso"
- "Configurar el cifrado de volúmenes de NetApp"

> Cloud Manager no instala la licencia NVE en sistemas que residen en la región China.

Actualización de Cloud Manager 3.7 (16 de junio de 2019)

Cloud Volumes ONTAP 9.6 ya está disponible en AWS, Azure y Google Cloud Platform como versión preliminar privada. Para unirse a la previsualización privada, envíe una solicitud a ng-Cloud-Volume-ONTAP-preview@netapp.com.

"Vea las novedades de Cloud Volumes ONTAP 9.6"

Cloud Manager 3.7 (5 de junio de 2019)

- Soporte para la próxima versión de Cloud Volumes ONTAP 9.6
- Cuentas de Cloud Central de NetApp
- Backup y restauración con Cloud Backup Service

Soporte para la próxima versión de Cloud Volumes ONTAP 9.6

Cloud Manager 3.7 incluye soporte para la próxima versión de Cloud Volumes ONTAP 9.6. El lanzamiento de 9.6 incluye una versión preliminar privada de Cloud Volumes ONTAP en Google Cloud Platform. Actualizaremos las notas de la versión cuando esté disponible la versión 9.6.

Cuentas de Cloud Central de NetApp

Hemos mejorado la forma de gestionar los recursos de cloud. Cada sistema de Cloud Manager se asociará con una cuenta *de Cloud Central de NetApp*. La cuenta permite la multi-tenancy y está prevista para otros servicios de datos en el cloud de NetApp en el futuro.

En Cloud Manager, una cuenta de Cloud Central es un contenedor para sus sistemas de Cloud Manager y los *espacios de trabajo* en los que los usuarios implementan Cloud Volumes ONTAP.

"Conozca cómo las cuentas de Cloud Central permiten el multi-tenancy".

> Cloud Manager necesita acceder a *https://cloudmanager.cloud.netapp.com* para conectarse al servicio de cuenta de Cloud Central. Abra esta URL en el firewall para asegurarse de que Cloud Manager pueda ponerse en contacto con el servicio.

Integración del sistema con las cuentas de Cloud Central

En algún momento después de actualizar a Cloud Manager 3.7, NetApp elegirá sistemas específicos de Cloud Manager para integrarse con cuentas de Cloud Central. Durante este proceso, NetApp crea una cuenta, asigna nuevas funciones a cada usuario, crea espacios de trabajo y coloca los entornos de trabajo existentes en esos espacios de trabajo. No se produce ninguna interrupción en sus sistemas Cloud Volumes ONTAP.

"Si tiene alguna pregunta, consulte esta sección de preguntas frecuentes".

Backup y restauración con Cloud Backup Service

Cloud Backup Service de NetApp para Cloud Volumes ONTAP ofrece funcionalidades de backup y restauración totalmente gestionadas para la protección y el archivado a largo plazo de sus datos en el cloud. Puede integrar Cloud Backup Service con Cloud Volumes ONTAP para AWS. Los backups que crea el servicio se almacenan en el almacenamiento de objetos AWS S3.

"Obtenga más información acerca de Cloud Backup Service".

Para comenzar, instale y configure el agente de copia de seguridad y, a continuación, inicie las operaciones de copia de seguridad y restauración. Si necesita ayuda, le animamos a que se ponga en contacto con nosotros a través del icono de chat de Cloud Manager.

Este proceso manual ya no es compatible. La función Backup to S3 se integró en Cloud Manager en la versión 3.7.3.

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.

Cloud Manager debe seguir ejecutándose en todo momento

Cloud Manager es un componente clave en el estado y la facturación de Cloud Volumes ONTAP. Si Cloud Manager se apaga, los sistemas Cloud Volumes ONTAP se apagarán tras perder la comunicación con Cloud Manager durante más de 4 días.

No se admiten los hosts Linux compartidos

Cloud Manager no es compatible con un host que se comparte 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.

De forma predeterminada, Active Directory no es compatible con las nuevas instalaciones de Cloud Manager

A partir de la versión 3.4, las nuevas instalaciones de Cloud Manager no admiten el uso de la autenticación de Active Directory de su empresa para la gestión de usuarios. Si es necesario, NetApp puede ayudarle a configurar Active Directory con Cloud Manager. Haga clic en el icono de chat de la parte inferior derecha de Cloud Manager para obtener ayuda.

Limitaciones en la región de AWS GovCloud (EE. UU.

- Cloud Manager debe ponerse en marcha en la región de AWS GovCloud (EE. UU.) si desea iniciar instancias de Cloud Volumes ONTAP en la región de AWS GovCloud (EE. UU.)
- Cuando se implementa en la región de AWS GovCloud (EE. UU.), Cloud Manager no puede detectar clústeres de ONTAP en una configuración de almacenamiento privado de NetApp para Microsoft Azure ni una configuración de almacenamiento privado de NetApp para SoftLayer.

Cloud Manager no configura volúmenes iSCSI

Cuando se crea un volumen en Cloud Manager con la vista del sistema de almacenamiento, puede seleccionar el protocolo NFS o CIFS. Se debe usar System Manager de OnCommand para crear un volumen para iSCSI.

Limitación de máquinas virtuales de almacenamiento (SVM)

Cloud Volumes ONTAP admite un SVM que sirva datos y uno o varios SVM que se utilizan para la recuperación ante desastres. La una SVM que sirve datos abarca todo el sistema Cloud Volumes ONTAP (par de alta disponibilidad o nodo único).

Cloud Manager no ofrece ninguna compatibilidad de configuración ni orquestación para la recuperación ante desastres de SVM. Tampoco admite tareas relacionadas con el almacenamiento en ninguna SVM adicional. Debe usar System Manager o la CLI para la recuperación ante desastres de SVM.

Conceptos

Información general sobre Cloud Manager y Cloud Volumes ONTAP

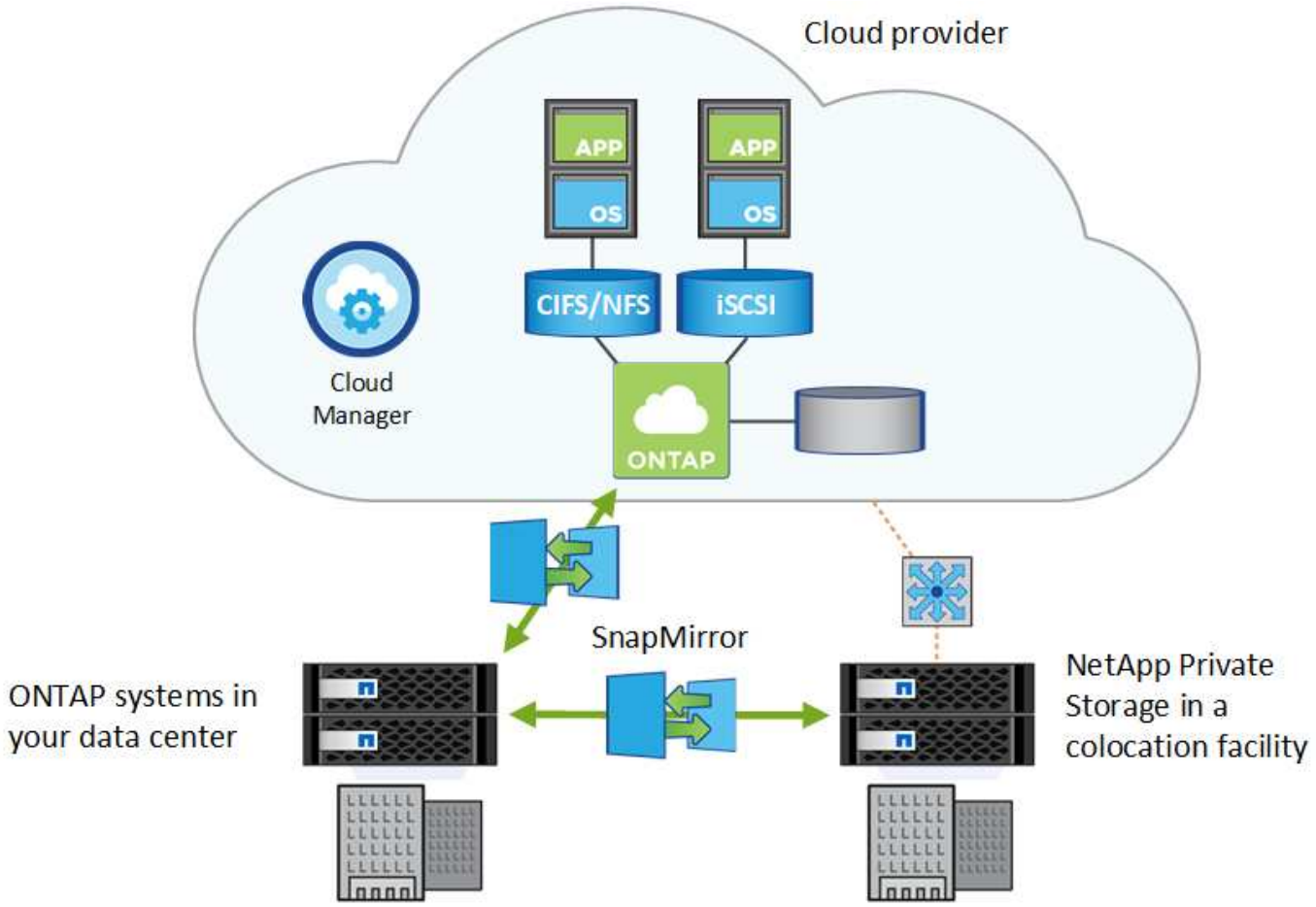
Cloud Manager le permite poner en marcha Cloud Volumes ONTAP, que proporciona funciones para la gran empresa para su almacenamiento en cloud y replicar datos fácilmente en clouds híbridos basados en NetApp.

Cloud Manager

Cloud Manager se creó pensando en la simplicidad. Le guía por la configuración de Cloud Volumes ONTAP en unos pocos pasos, facilita la gestión de datos al ofrecer un aprovisionamiento de almacenamiento simplificado y una gestión de la capacidad automatizada, permite la replicación de datos mediante arrastrar y soltar en un cloud híbrido, etc.

Es necesario Cloud Manager para poner en marcha y gestionar Cloud Volumes ONTAP, pero también puede detectar y aprovisionar almacenamiento para clústeres de ONTAP en las instalaciones. Esto proporciona un punto centralizado de control para su infraestructura de almacenamiento en el cloud y en las instalaciones.

Puede ejecutar Cloud Manager en la nube o en su red, solo necesita una conexión con las redes en las que desea implementar Cloud Volumes ONTAP. La siguiente imagen muestra la ejecución de Cloud Manager y Cloud Volumes ONTAP en un proveedor de cloud. También muestra replicación de datos en un cloud híbrido.



"Obtenga más información sobre Cloud Manager"

Cloud Volumes ONTAP

Cloud Volumes ONTAP es un dispositivo de almacenamiento exclusivamente de software que ejecuta el software para la gestión de datos ONTAP en el cloud. Puede utilizar Cloud Volumes ONTAP para cargas de trabajo de producción, recuperación ante desastres, DevOps, recursos compartidos de archivos y gestión de bases de datos.

Cloud Volumes ONTAP amplía el almacenamiento empresarial al cloud con las siguientes funciones clave:

- Eficiencias de almacenamiento aprovechan las tecnologías integradas de deduplicación de datos, compresión de datos, thin provisioning y clonado para minimizar los costes de almacenamiento.
- La alta disponibilidad garantiza la fiabilidad de su empresa y la continuidad de las operaciones en caso de fallos en su entorno cloud.
- Replicación de datos Cloud Volumes ONTAP aprovecha SnapMirror, la tecnología de replicación líder del sector de NetApp, para replicar datos en las instalaciones al cloud, de modo que es fácil disponer de copias secundarias para varios casos de uso.
- Organización en niveles de datos cambie entre pools de almacenamiento de alto y bajo rendimiento bajo demanda sin desconectar las aplicaciones.
- La consistencia de aplicaciones garantiza la consistencia de las copias Snapshot de NetApp mediante SnapCenter de NetApp.

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

"Consulte las configuraciones de Cloud Volumes ONTAP admitidas"

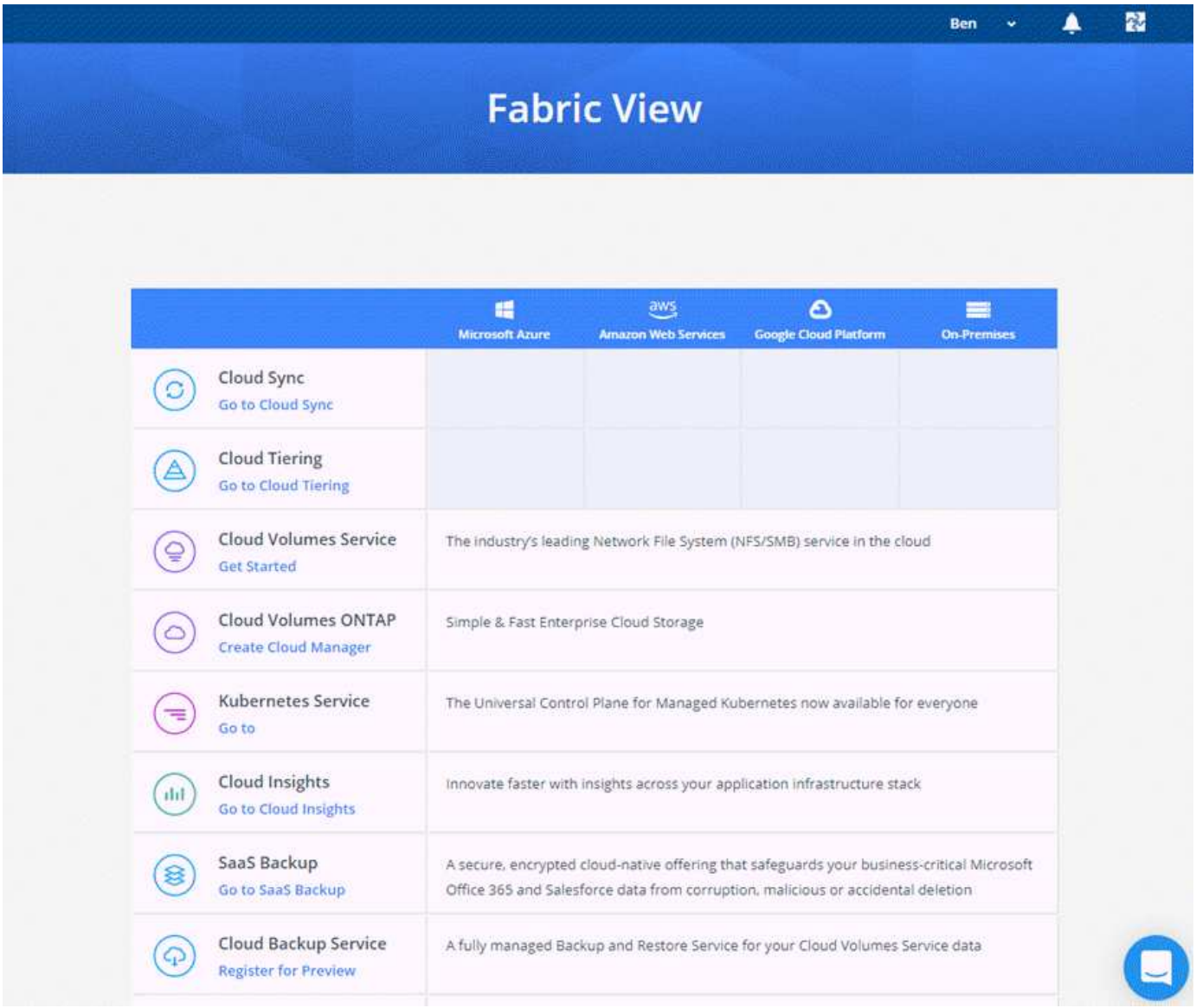
"Obtenga más información acerca de Cloud Volumes ONTAP"

Cloud Central de NetApp

"Cloud Central de NetApp" Ofrece una ubicación centralizada para acceder a los servicios de datos en el cloud de NetApp y gestionarlos. Estos servicios le permiten ejecutar aplicaciones críticas en el cloud, crear sitios de recuperación ante desastres automatizados, realizar backups de sus datos SaaS y migrar y controlar datos de forma efectiva entre varios clouds.

La integración de Cloud Manager con Cloud Central de NetApp ofrece varias ventajas, como una experiencia de implementación simplificada, una única ubicación para ver y gestionar varios sistemas de Cloud Manager y una autenticación de usuario centralizada.

Con la autenticación de usuarios centralizada, puede usar el mismo conjunto de credenciales en los sistemas de Cloud Manager y entre Cloud Manager y otros servicios de datos, como Cloud Sync. También es fácil restablecer la contraseña si la has olvidado.



Cuentas de Cloud Central

Cada sistema de Cloud Manager está asociado con una cuenta *de Cloud Central de NetApp*. Una cuenta de Cloud Central proporciona multi-tenancy y permite organizar usuarios y recursos en espacios de trabajo aislados.

Una cuenta de Cloud Central permite multi-tenancy:

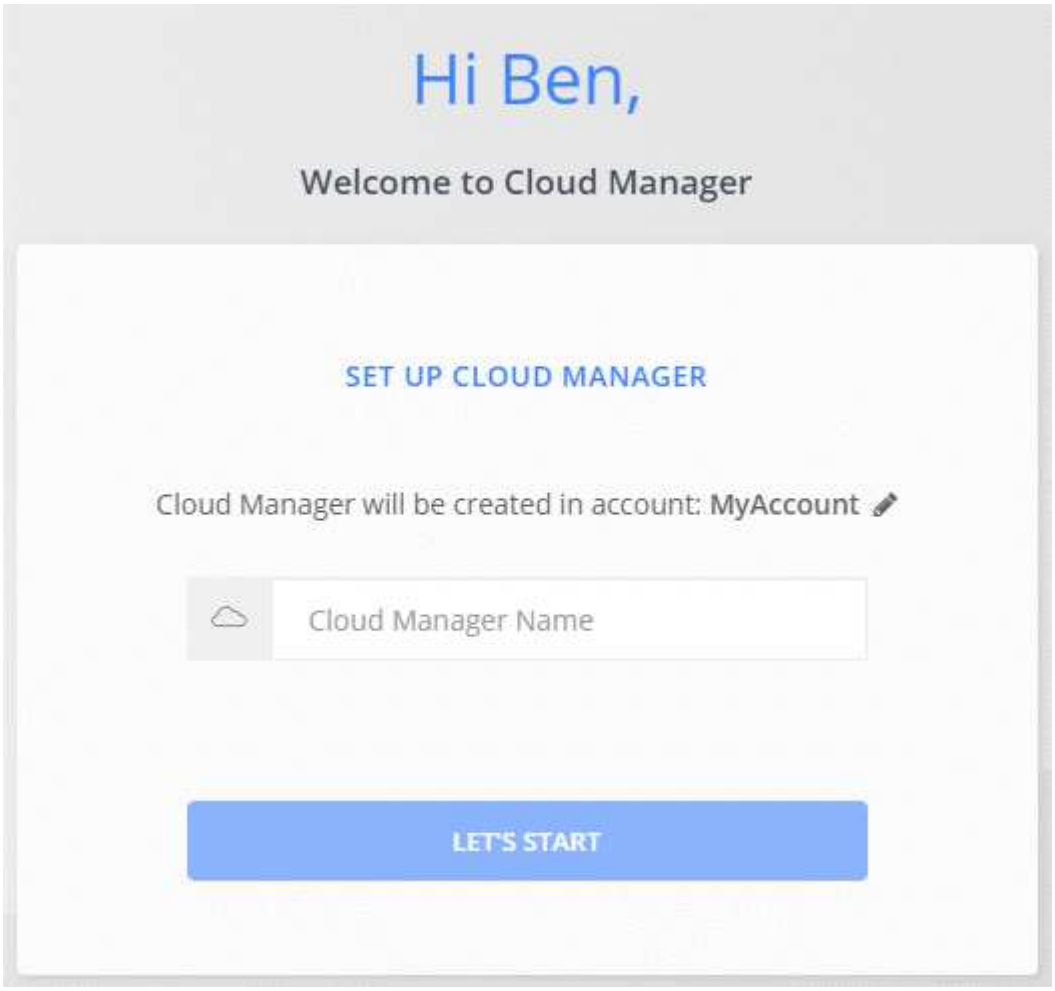
- Una única cuenta de Cloud Central puede incluir varios sistemas de Cloud Manager que satisfacen diferentes necesidades empresariales.

  Dado que los usuarios están asociados a la cuenta de Cloud Central, no es necesario configurar usuarios para cada sistema de Cloud Manager individual.

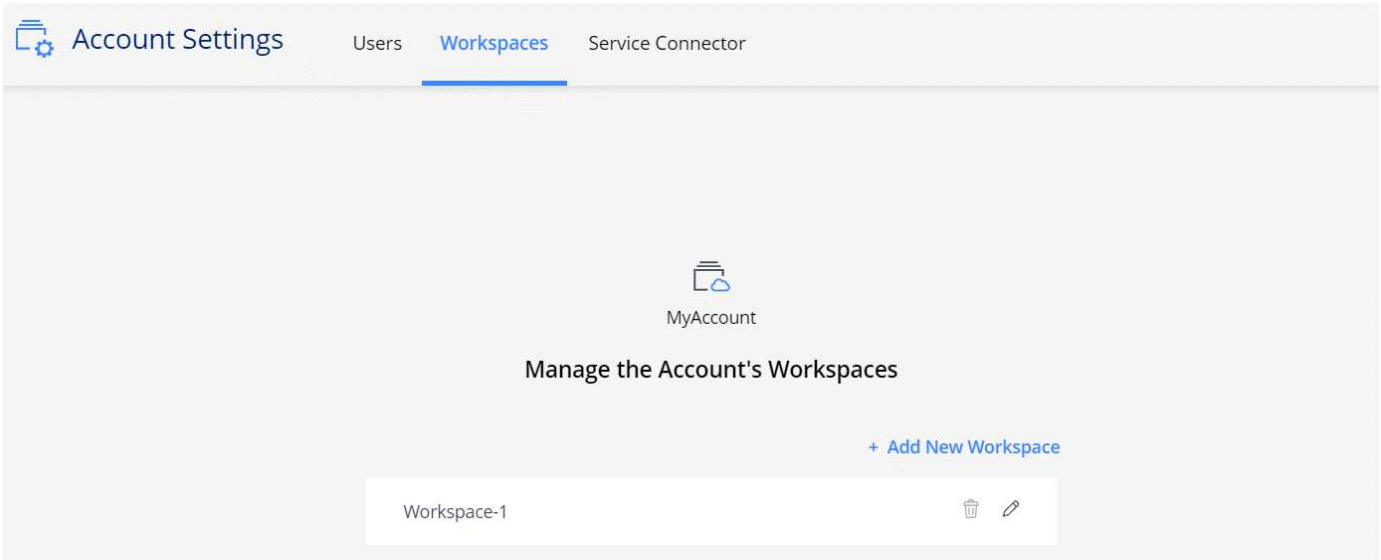
- En cada sistema de Cloud Manager, varios usuarios pueden poner en marcha y gestionar sistemas de Cloud Volumes ONTAP en entornos aislados denominados espacios de trabajo.

  Estos espacios de trabajo son invisibles para otros usuarios, a menos que se compartan.

Al implementar Cloud Manager, seleccione la cuenta de Cloud Central para asociarla con el sistema:



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



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

Cloud Manager necesita acceder a *https://cloudmanager.cloud.netapp.com* para conectarse al servicio de cuenta de Cloud Central. Abra esta URL en el firewall para asegurarse de que Cloud Manager pueda ponerse en contacto con el servicio.

Usuarios, espacios de trabajo y conectores de servicio

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 y conectores de servicio asociados a la cuenta.

Usuarios

Se trata de usuarios de Cloud Central de NetApp que está asociado con su 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.

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 de servicio

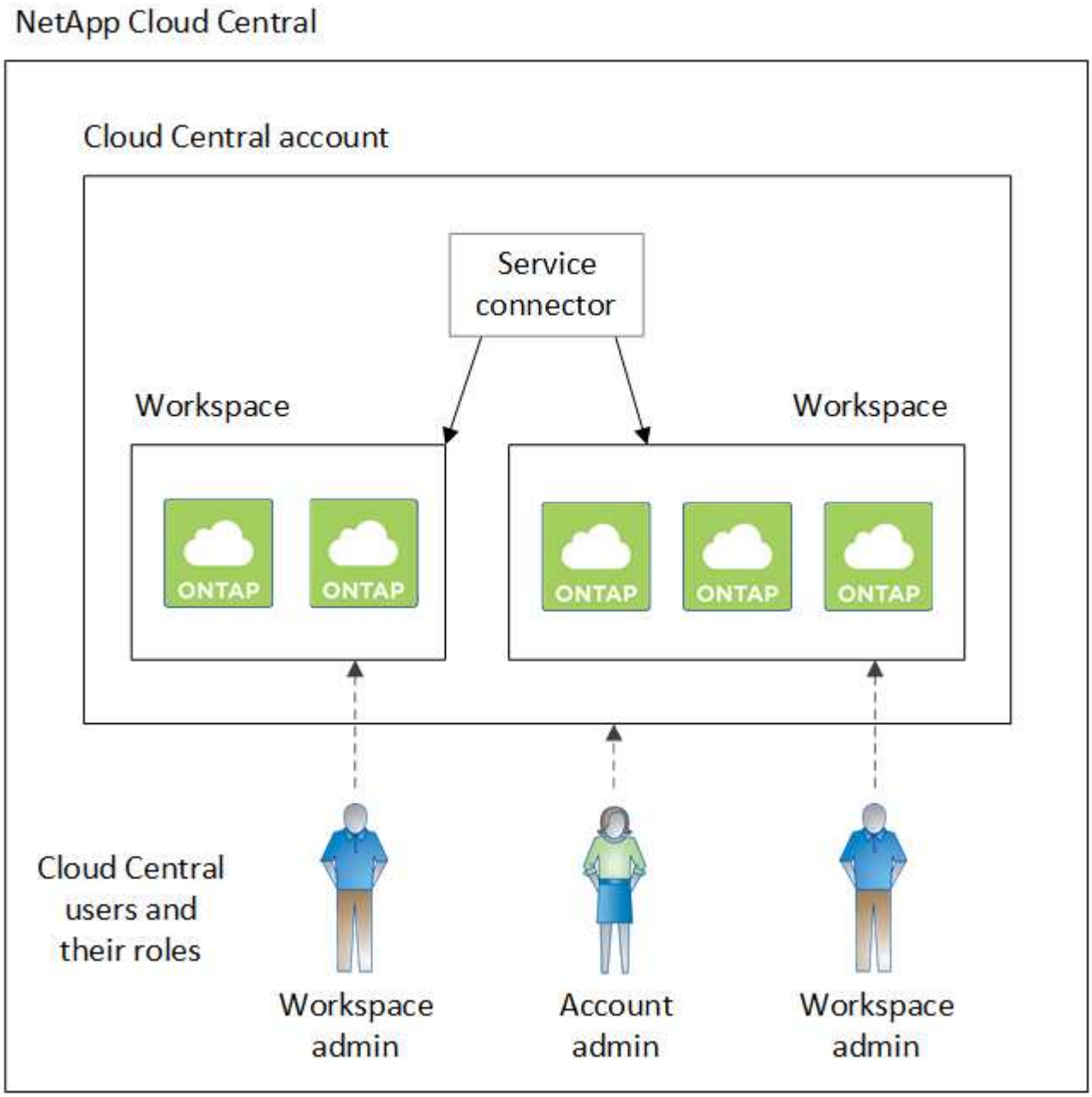
Un conector de servicio forma parte de Cloud Manager. Ejecuta gran parte del software de Cloud Manager (como la interfaz de usuario), excepto algunos servicios de Cloud Central a los que se conecta (cuentas auth0 y Cloud Central). El conector del servicio se ejecuta en la instancia de máquina virtual que se implementó en su proveedor de cloud o en un host en las instalaciones que configuró.

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

Ejemplos

En el ejemplo siguiente se muestra una cuenta que utiliza dos espacios de trabajo para crear entornos aislados para los sistemas Cloud Volumes ONTAP. Por ejemplo, un espacio de trabajo puede ser para un entorno de almacenamiento provisional, mientras que el otro para un entorno de producción.

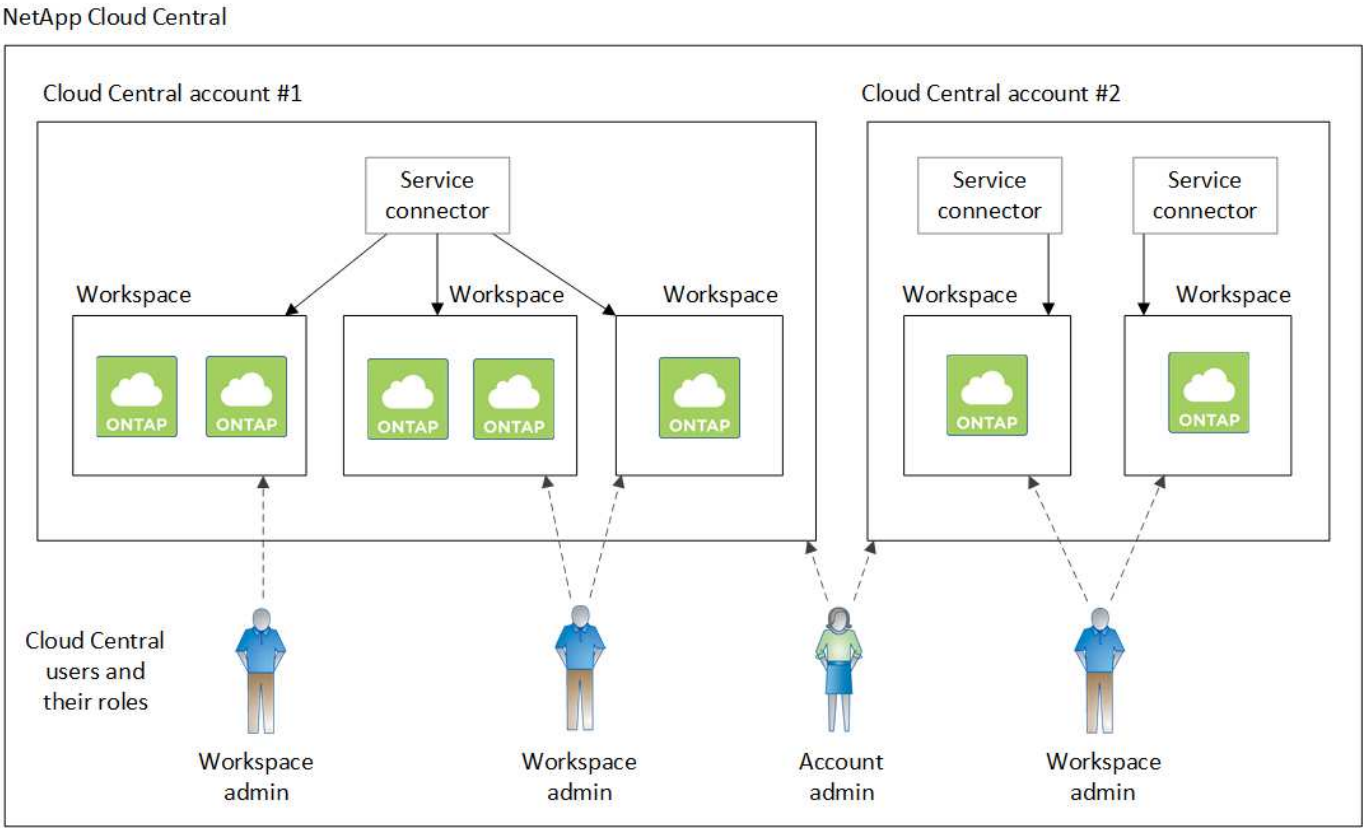
Cloud Manager y los sistemas de Cloud Volumes ONTAP no residen en la cuenta de Cloud Central de NetApp, que se ejecutan en un proveedor de cloud. Ésta es una representación conceptual de la relación entre cada componente.



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 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.

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

De nuevo, Cloud Manager y los sistemas Cloud Volumes ONTAP no residen *en* la cuenta de Cloud Central de NetApp, sino que se ejecutan en un proveedor de cloud. Ésta es una representación conceptual de la relación entre cada componente.



Preguntas frecuentes sobre la integración con cuentas de Cloud Central

En algún momento después de actualizar a Cloud Manager 3.7, NetApp elegirá sistemas específicos de Cloud Manager para integrarse con cuentas de Cloud Central. Estas preguntas frecuentes pueden responder a las preguntas que pueda tener sobre el proceso.

¿Cuánto tiempo tarda el proceso?

Sólo unos minutos.

¿Cloud Manager no estará disponible?

No, todavía puede acceder a su sistema Cloud Manager.

¿y Cloud Volumes ONTAP?

No se produce ninguna interrupción en sus sistemas Cloud Volumes ONTAP.

¿Qué sucede durante este proceso?

NetApp lleva a cabo lo siguiente durante el proceso de integración:

1. Crea una nueva cuenta de Cloud Central y la asocia con el sistema Cloud Manager.
2. Asigna roles nuevos a cada usuario existente:
   - Los administradores de Cloud Manager se convierten en administradores de cuentas
   - Los administradores de inquilinos y los administradores del entorno de trabajo se convierten en administradores de espacio de trabajo

3. Crea espacios de trabajo que reemplazan a los arrendatarios existentes.
4. Coloca sus entornos de trabajo en esos espacios de trabajo.
5. Asocia el conector de servicio a todas las áreas de trabajo.

¿Importa dónde he instalado mi sistema Cloud Manager?

No NetApp integrará sistemas con cuentas de Cloud Central sin importar dónde residan, ya sea en AWS, Azure o en sus instalaciones.

Cuentas de proveedores de cloud

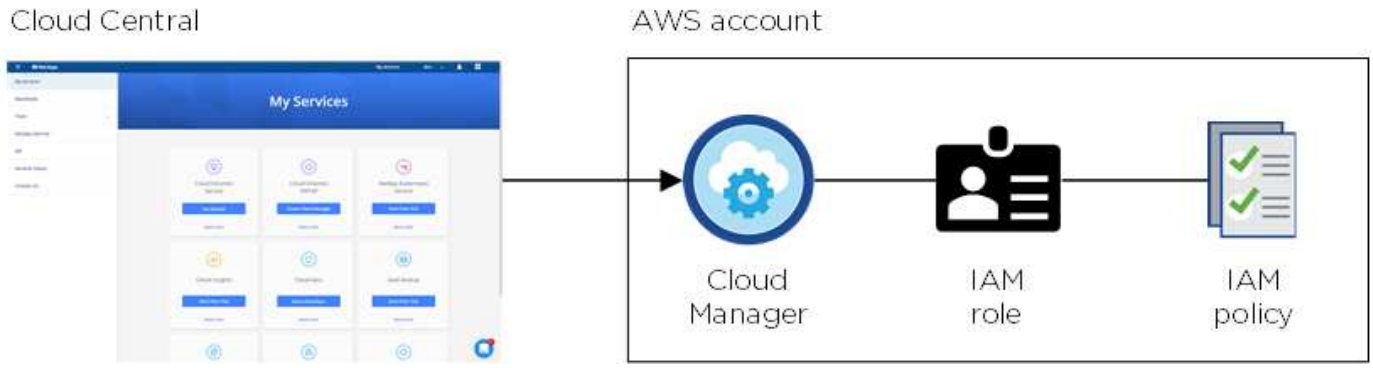
Cuentas y permisos de AWS

Cloud Manager permite elegir la cuenta de AWS en la que desea implementar un sistema Cloud Volumes ONTAP. Puede poner en marcha todos los sistemas Cloud Volumes ONTAP en la cuenta inicial de AWS o configurar cuentas adicionales.

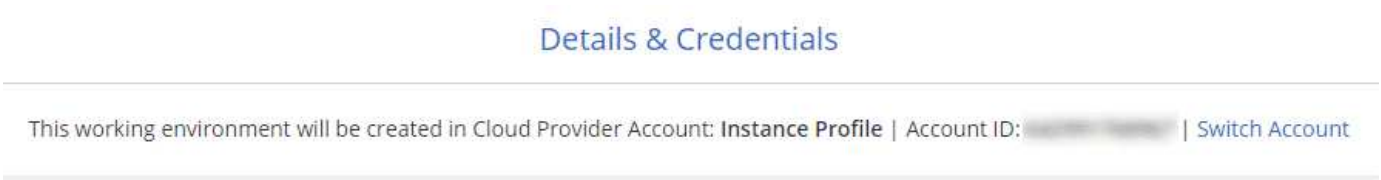
La cuenta inicial de AWS

Al implementar Cloud Manager desde NetApp Cloud Central, necesita utilizar una cuenta de AWS que tenga permisos para iniciar la instancia de Cloud Manager. Los permisos necesarios se enumeran en la "Política central de Cloud de NetApp para AWS".

Cuando Cloud Central inicia la instancia de Cloud Manager en AWS, crea un rol IAM y un perfil de instancia para la instancia. También une una política que ofrece permisos para implementar y gestionar Cloud Volumes ONTAP en esa cuenta de AWS. "Revise cómo Cloud Manager utiliza los permisos".



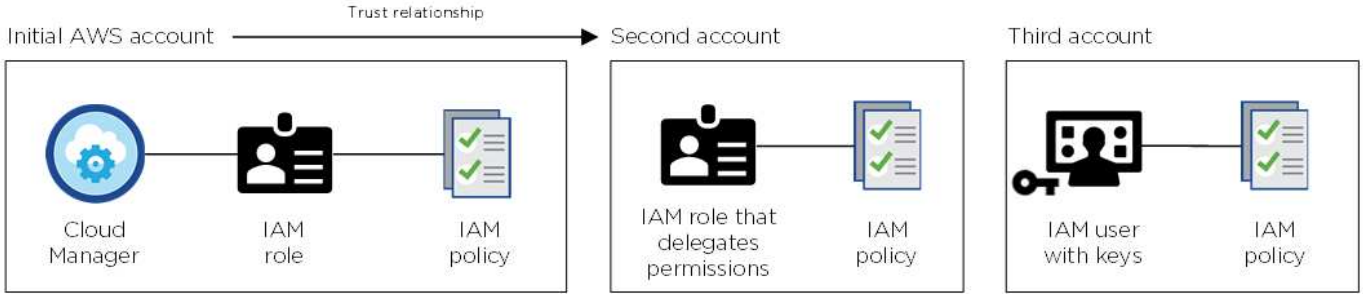
Cloud Manager selecciona esta cuenta de proveedor de cloud de forma predeterminada al crear un nuevo entorno de trabajo:



Otras cuentas de AWS

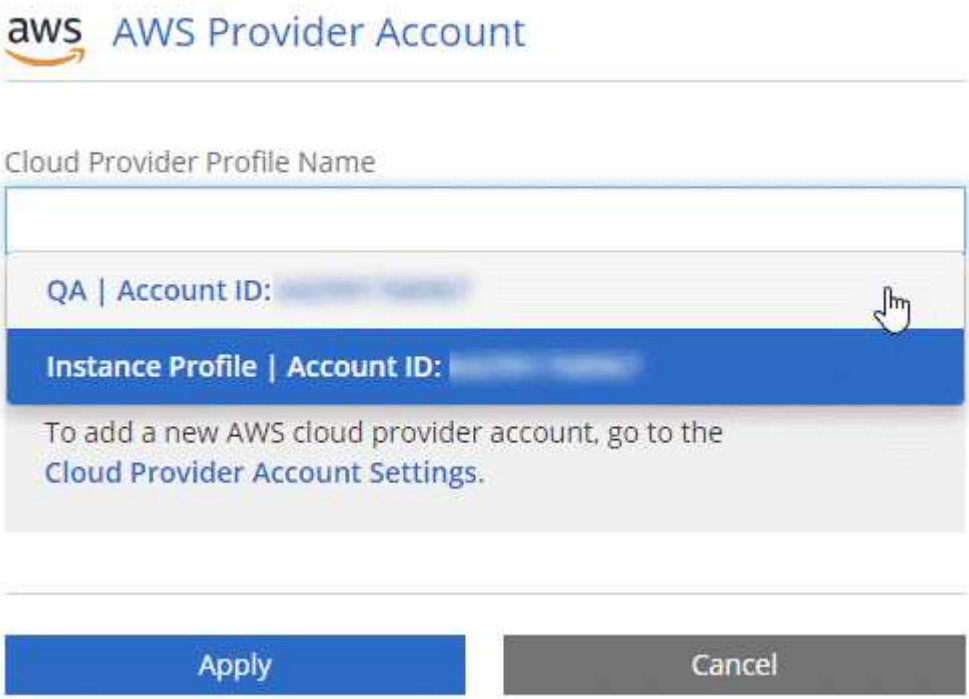
Si desea ejecutar Cloud Volumes ONTAP en diferentes cuentas de AWS, puede hacerlo también "Proporcione

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 cuentas de proveedor de cloud 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 agregar otra cuenta, puede cambiar a ella 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 de NetApp Cloud Central. También puede implementar Cloud Manager en AWS desde el "Mercado AWS" y usted puede "Instale Cloud Manager 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.

Cuentas y permisos de Azure

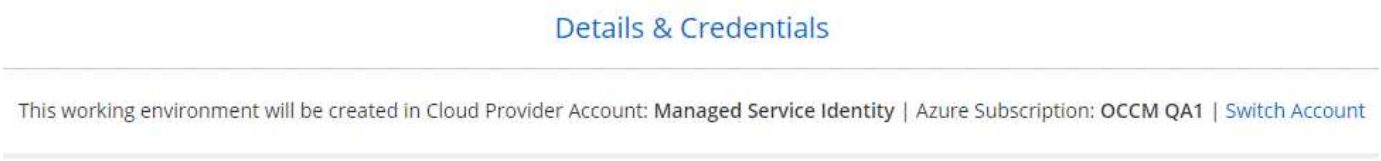
Cloud Manager permite elegir la cuenta de Azure en la que desea implementar un sistema Cloud Volumes ONTAP. Puede poner en marcha todos sus sistemas Cloud Volumes ONTAP en la cuenta de Azure inicial o configurar cuentas adicionales.

La cuenta inicial de Azure

Al poner en marcha Cloud Manager desde NetApp Cloud Central, necesita utilizar una cuenta de Azure con permisos para implementar la máquina virtual de Cloud Manager. Los permisos necesarios se enumeran en la "Política Cloud Central de NetApp para Azure".

Cuando Cloud Central pone en marcha la máquina virtual de Cloud Manager en Azure, habilita una "identidad administrada asignada por el sistema" En la máquina virtual de Cloud Manager, crea un rol personalizado y lo asigna a la máquina virtual. El rol proporciona permisos para implementar y gestionar Cloud Volumes ONTAP en esa suscripción de Azure. "Revise cómo Cloud Manager utiliza los permisos".

Cloud Manager selecciona esta cuenta de proveedor de cloud de forma predeterminada al crear un nuevo entorno de trabajo:

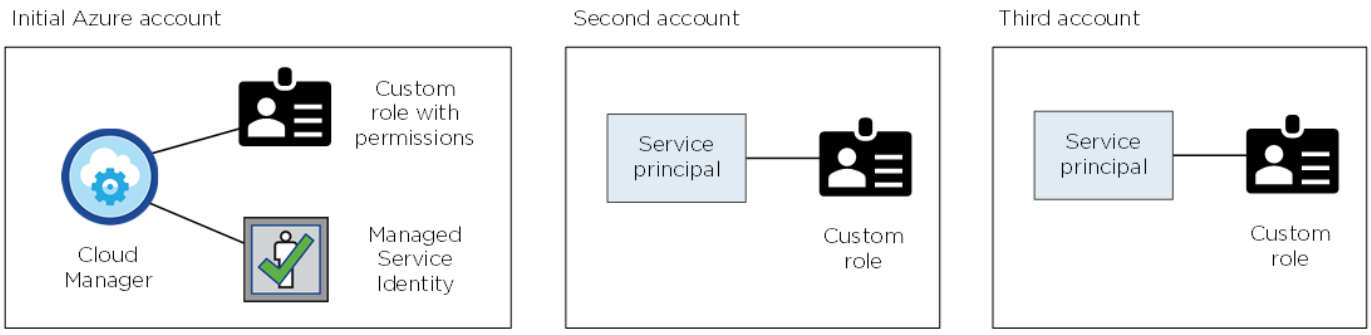


Suscripciones adicionales de Azure para la cuenta inicial

La identidad administrada está asociada a la suscripción en la que inició Cloud Manager. Si desea seleccionar una suscripción de Azure diferente, tendrá que hacerlo "asocie la identidad administrada a esas suscripciones".

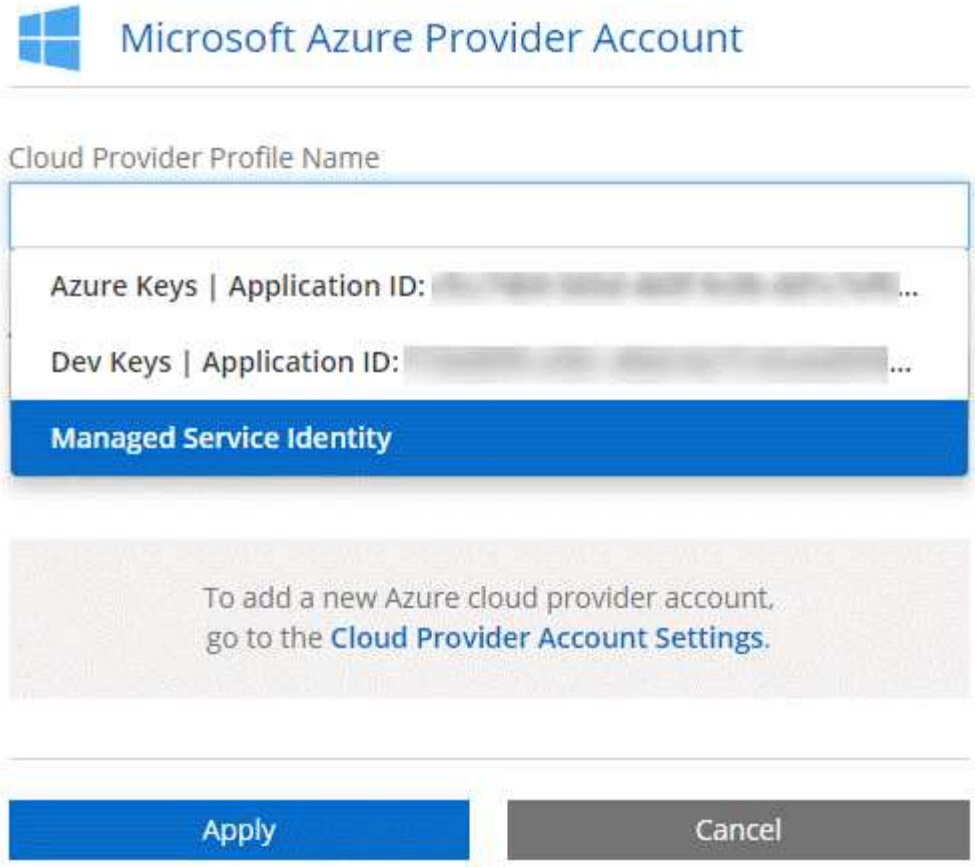
Otras cuentas de Azure

Si desea implementar Cloud Volumes ONTAP en diferentes cuentas 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 cuentas de proveedor de cloud a Cloud Manager" Proporcionando detalles acerca del director de servicio de AD.

Después de agregar otra cuenta, puede cambiar a ella 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 de NetApp Cloud Central. También puede implementar Cloud Manager en Azure desde el "Azure Marketplace", y usted puede "Instale Cloud Manager en las instalaciones".

Si utiliza el Marketplace, los permisos se proporcionan de la misma manera. Solo tiene que crear y configurar manualmente la identidad administrada para Cloud Manager y, a continuación, proporcionar permisos para cualquier cuenta adicional.

Para implementaciones en las instalaciones, no puede configurar una identidad administrada para el sistema Cloud Manager, pero puede proporcionar permisos como lo haría para cuentas adicionales.

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. Las cuentas de Google Cloud que añada a Cloud Manager utilizan para habilitar la organización en niveles de los datos.

Proyecto y permisos para Cloud Manager

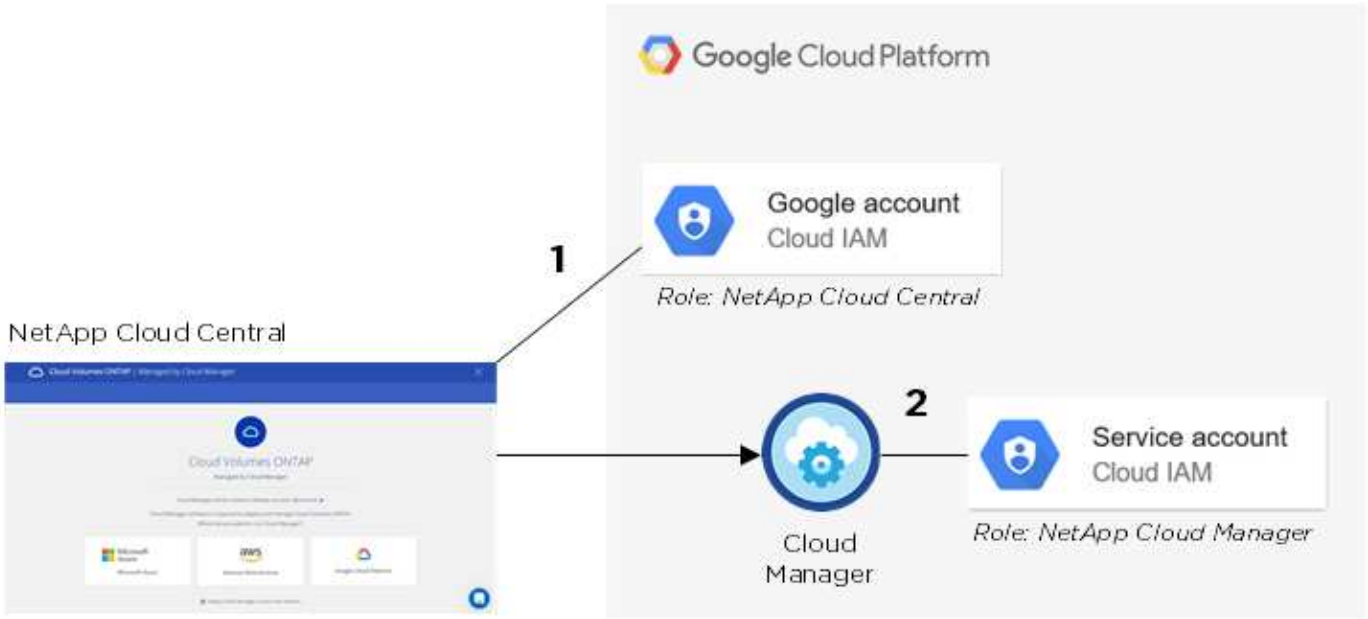
Antes de poder poner en marcha Cloud Volumes ONTAP en Google Cloud, es necesario poner en marcha Cloud Manager en un proyecto de Google Cloud. Cloud Manager no puede ejecutarse en sus instalaciones ni en un proveedor de cloud diferente.

Debe haber dos conjuntos de permisos antes de implementar Cloud Manager desde "Cloud Central de NetApp":

1. Necesita implementar Cloud Manager con una cuenta de Google que tenga permisos para iniciar la instancia de Cloud Manager VM desde Cloud Central.
2. Al implementar Cloud Manager, se le solicitará 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 Cloud Manager, o en un proyecto diferente. Para poner en marcha Cloud Volumes ONTAP en otro proyecto, primero tiene que añadir la cuenta de servicio y la función de Cloud Manager al proyecto.

- "Aprenda a configurar la cuenta de servicio de Cloud Manager (consulte el paso 4).".
- "Descubra cómo implementar Cloud Volumes ONTAP en GCP y seleccione un proyecto".

Responsables de la organización en niveles de los datos

Es necesario añadir una cuenta de Google Cloud a Cloud Manager para habilitar la organización en niveles de los datos en un sistema Cloud Volumes ONTAP. 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".

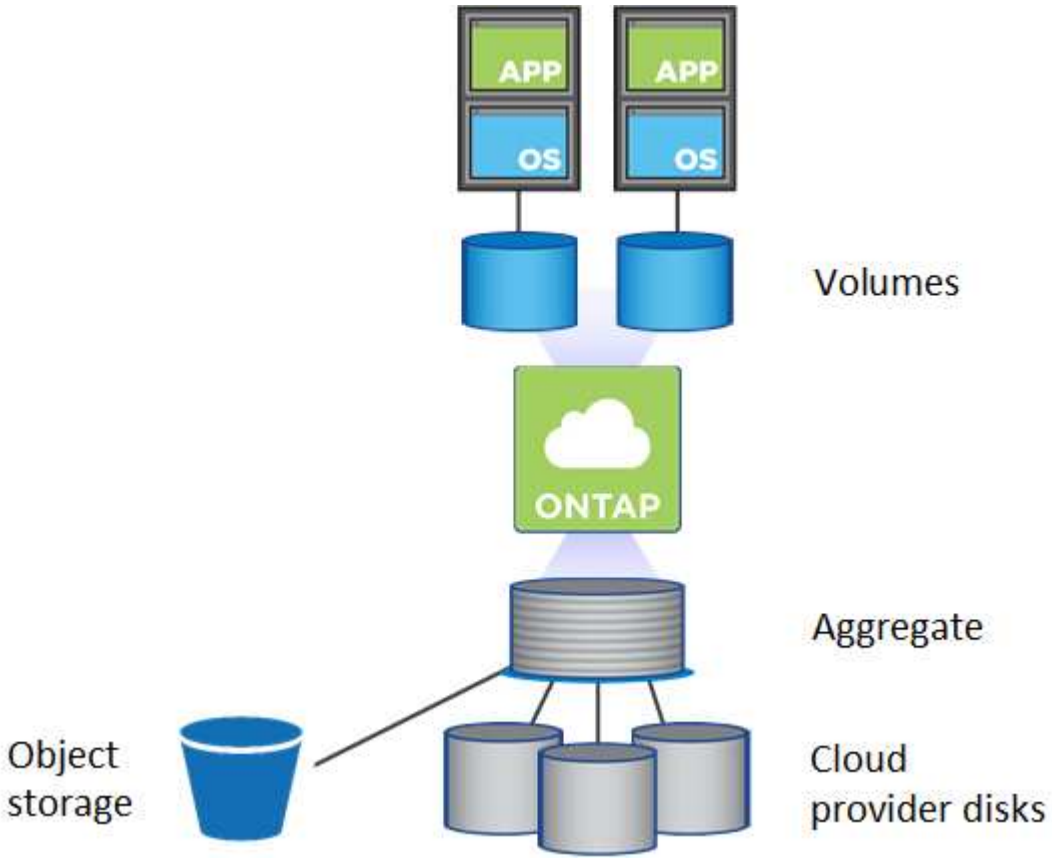
Reducida

Discos y agregados

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

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"

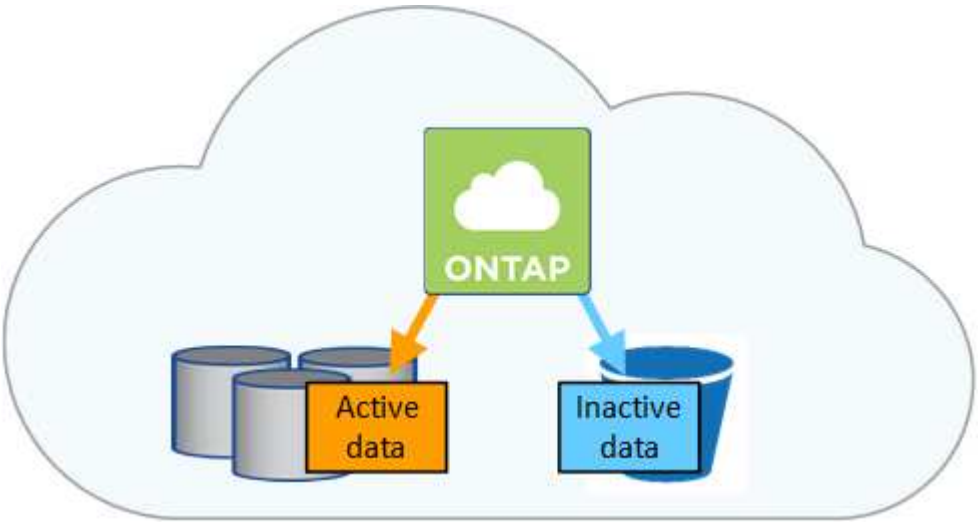
Tipo de RAID

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 función 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. Al cambiar el nivel de organización en niveles de un sistema, puede elegir otra clase de almacenamiento de S3.

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.

Niveles

Si no tiene previsto acceder a los datos inactivos, puede reducir los costes de almacenamiento cambiando el nivel de organización en niveles de un sistema a uno de los siguientes: *Intelligent Tiering*, *One-Zone Infrecuente Access* o *Standard-Infrecuente Access*. Cuando cambia el nivel de organización en niveles, los datos inactivos comienzan en la clase de almacenamiento estándar y se mueven a la clase de almacenamiento que seleccionó si no se accede a los datos transcurridos 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 organización en niveles. "Obtenga más información acerca de las clases de almacenamiento de Amazon S3".

Después de crear el sistema, es posible cambiar el nivel de organización en niveles. Para obtener más información, consulte "Organización en niveles de los datos inactivos en almacenamiento de objetos de bajo coste".

El nivel de organización en niveles es para todo el sistema, no es 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. Al cambiar el nivel de organización en niveles del sistema, puede elegir otro nivel de almacenamiento de Azure.

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

Si no tiene pensado acceder a los datos inactivos, puede reducir sus costes de almacenamiento cambiando el nivel de organización en niveles de un sistema al nivel de almacenamiento Azure *COOL*. Cuando cambia el nivel de organización en niveles, los datos inactivos comienzan en el nivel de almacenamiento activo y se mueven al nivel 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 organización en niveles. "Obtenga más información acerca de los niveles de acceso al almacenamiento de Azure Blob".

Después de crear el sistema, es posible cambiar el nivel de organización en niveles. Para obtener más información, consulte "Organización en niveles de los datos inactivos en almacenamiento de objetos de bajo coste".

El nivel de organización en niveles es para todo el sistema, no 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.

Niveles

Por el momento, no se admiten otras clases de almacenamiento de GCP.

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.

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. No se puede devolver el espacio a AWS o Azure en este escenario.

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

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.

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.

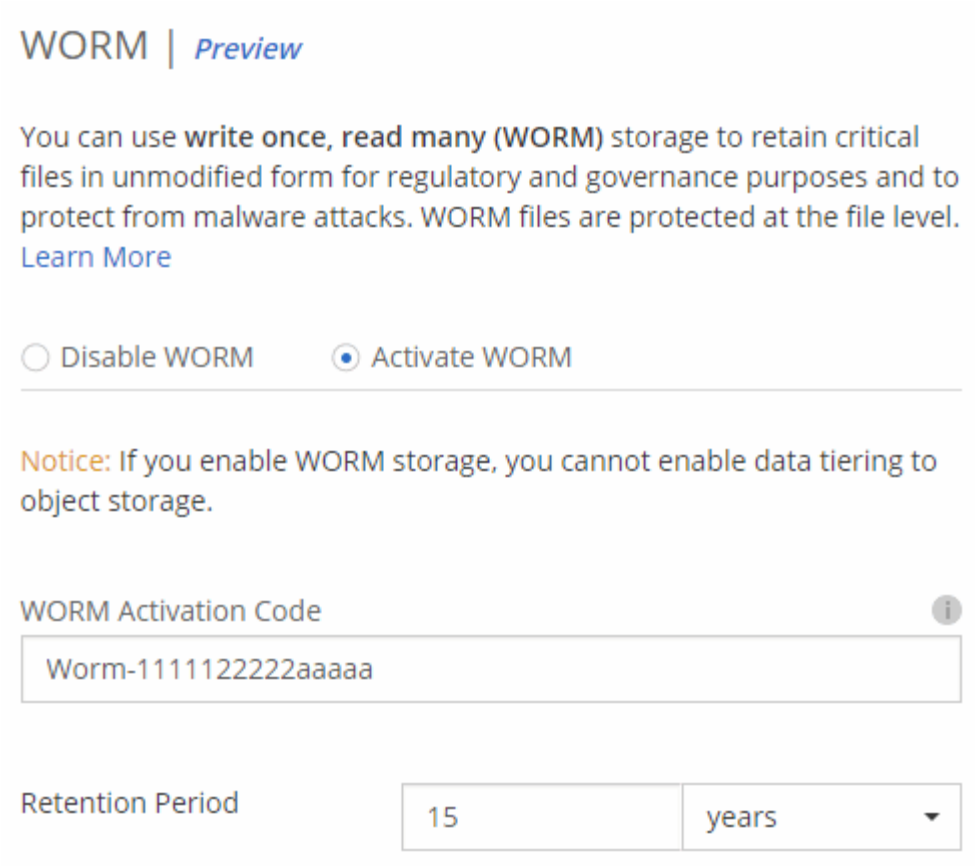
Una vez transcurrido el período de retención, es responsable de eliminar los archivos que ya no se necesiten.

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.

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.

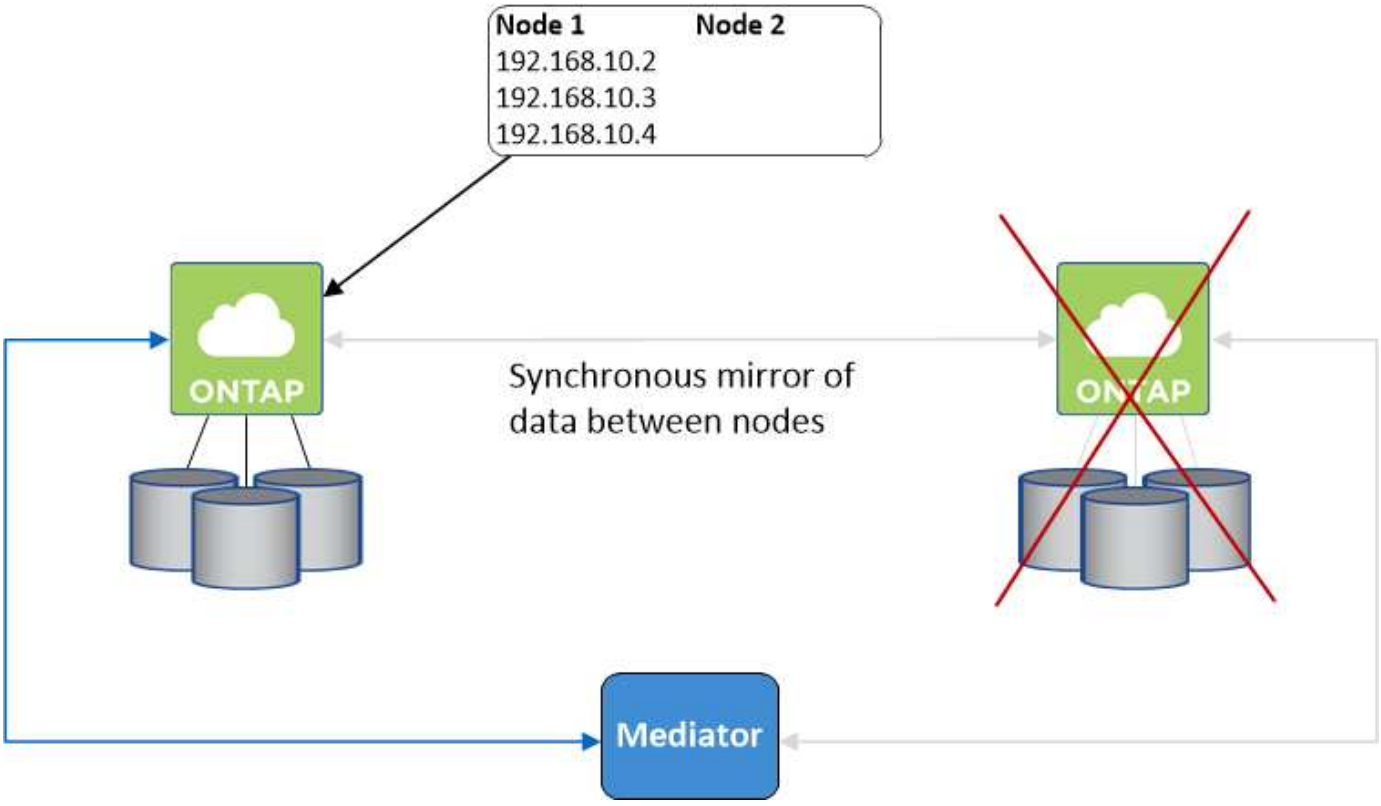
Toma de control y retorno del almacenamiento para iSCSI

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

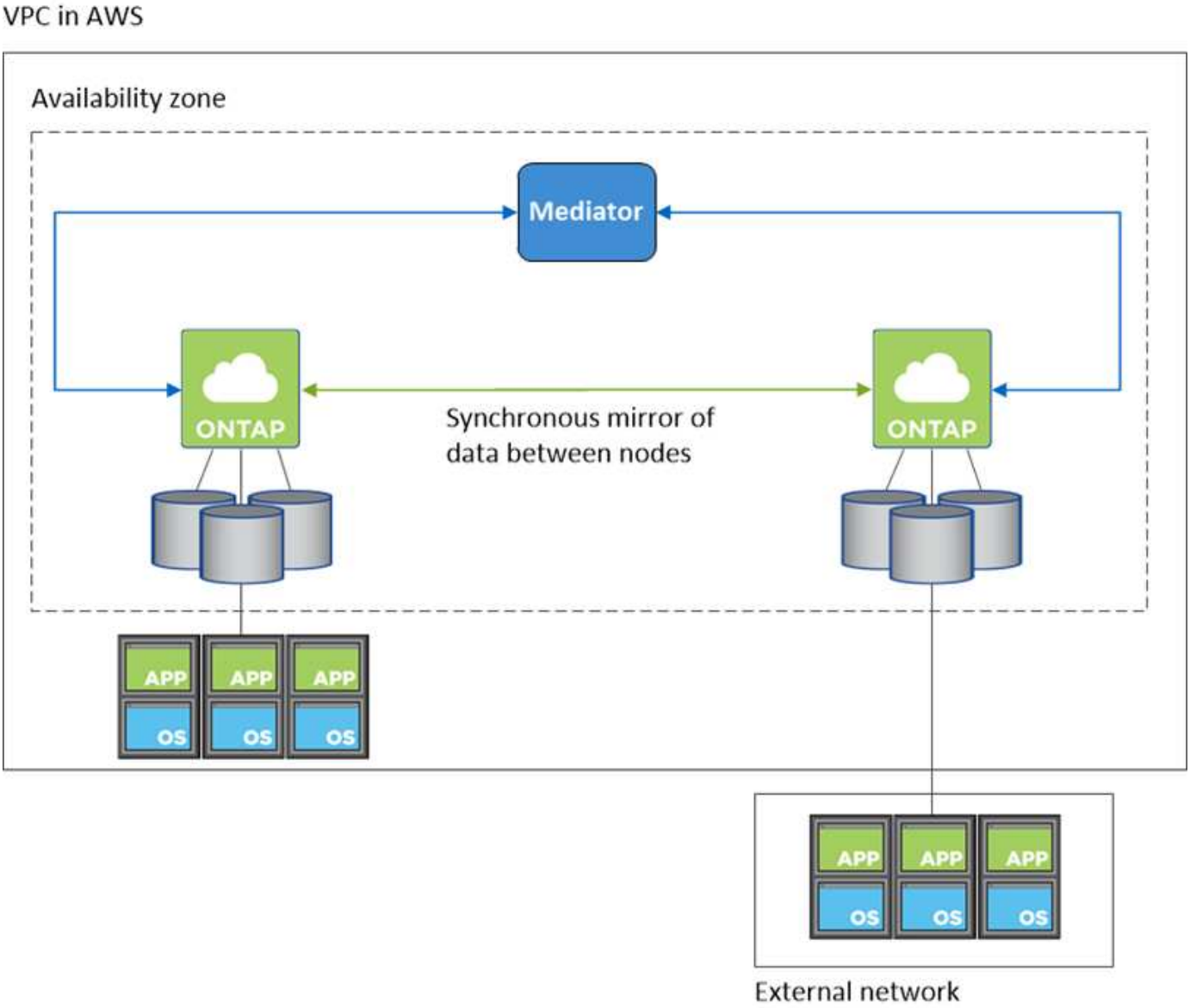
La implementación de una configuración de alta disponibilidad en una única zona de disponibilidad (AZ) puede garantizar una alta disponibilidad de los datos en caso de que falle una instancia que ejecute un nodo de Cloud Volumes ONTAP. Fuera del VPC, se puede acceder a todos los datos de forma nativa.

> 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.

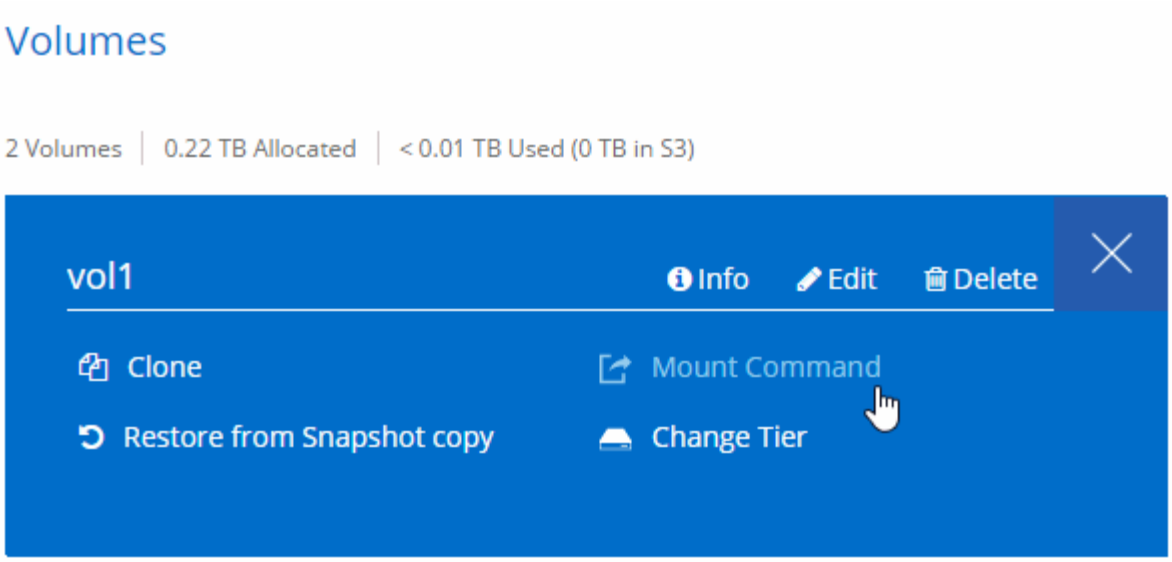
Para obtener más información sobre el rendimiento de Cloud Volumes ONTAP, consulte "Rendimiento".

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:

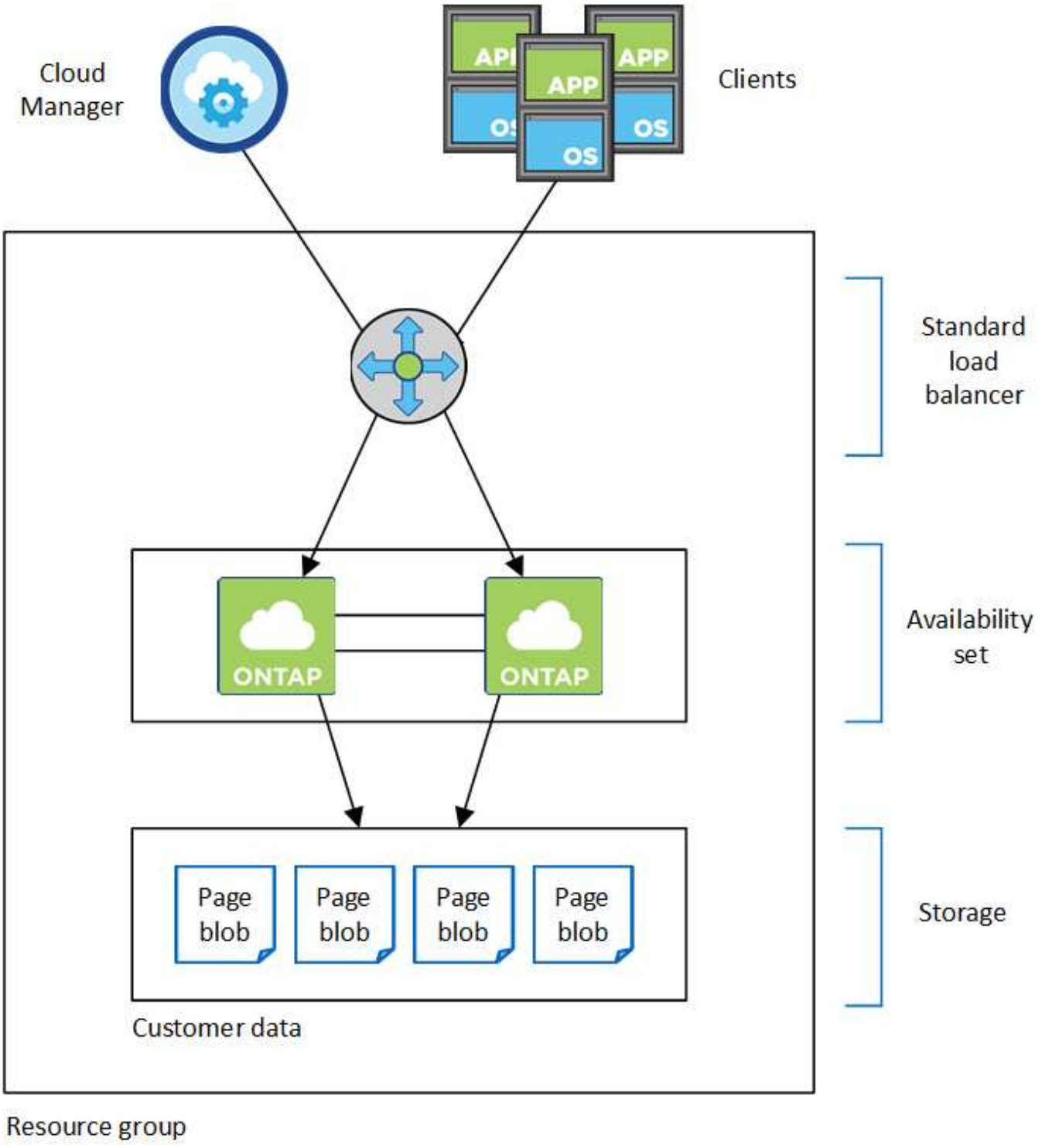


Pares de alta disponibilidad en Azure

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 de arranque, raíz y principales:

- Dos discos SSD Premium de 90 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 128 GB para ahorrar núcleos (uno por nodo)

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.

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.

Es posible acceder a una prueba gratuita de 30 días desde la que se encuentra disponible un sistema Cloud Volumes ONTAP de un único nodo "Cloud Central de NetApp". No se cobran costes de software por hora, pero siguen siendo aplicables los costes de infraestructura. Una prueba gratuita se convierte automáticamente en una suscripción por hora de pago cuando expira.

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.

Licencia

Cada sistema BYOL de Cloud Volumes ONTAP debe tener una licencia instalada con una suscripción activa. Si no se instala una licencia activa, el sistema Cloud Volumes ONTAP se apaga después de 30 días. Cloud Manager simplifica el proceso al gestionar las licencias para usted y notificar antes de que caduquen.

Gestión de licencias para un nuevo sistema

Cuando crea un sistema BYOL, Cloud Manager le solicita una 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 una conexión a Internet segura, puede obtener el archivo usted mismo y, a continuación, cargarlo manualmente en Cloud Manager. Para ver instrucciones, consulte "Instalación de archivos de licencia en sistemas BYOL de Cloud Volumes ONTAP".

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 una conexión a Internet segura, puede obtener el archivo usted mismo y, a continuación, cargarlo manualmente en Cloud Manager. Para ver instrucciones, consulte "Instalación de archivos de licencia en sistemas BYOL de Cloud Volumes ONTAP".

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:

- Cifrado de volúmenes de NetApp (a partir de Cloud Volumes ONTAP 9.5)
- Servicio de gestión de claves de AWS
- Cifrado del servicio de almacenamiento de Azure
- Cifrado predeterminado de la plataforma Google Cloud

Puede usar el cifrado de volúmenes de NetApp con el cifrado nativo AWS, Azure o GCP, que cifra los datos a nivel de hipervisor.

Cifrado de volúmenes de NetApp

El cifrado de volúmenes de NetApp (NVE) es una tecnología basada en software para cifrar datos en reposo un volumen por vez. Se cifran datos, copias Snapshot y metadatos. El acceso a los datos se proporciona mediante una clave XTS-AES-256 exclusiva, una por volumen.

Cloud Volumes ONTAP admite el cifrado de volúmenes de NetApp con un servidor de gestión de claves

externo. No se admite un administrador de claves incorporado. Los administradores de claves compatibles se encuentran en la "Herramienta de matriz de interoperabilidad de NetApp" Bajo la solución **Key Managers**.

Puede habilitar el cifrado de volúmenes de NetApp en un volumen nuevo o existente mediante la interfaz de línea de comandos o System Manager. Cloud Manager no admite el cifrado de volúmenes de NetApp. Para ver instrucciones, consulte "Cifrar volúmenes con cifrado de volúmenes 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.

Cloud Volumes ONTAP no admite las claves gestionadas por el cliente.

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.

Consulte la "Guía para desarrolladores de API" Para obtener más información sobre el uso de los parámetros "GcpEncryption".

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".

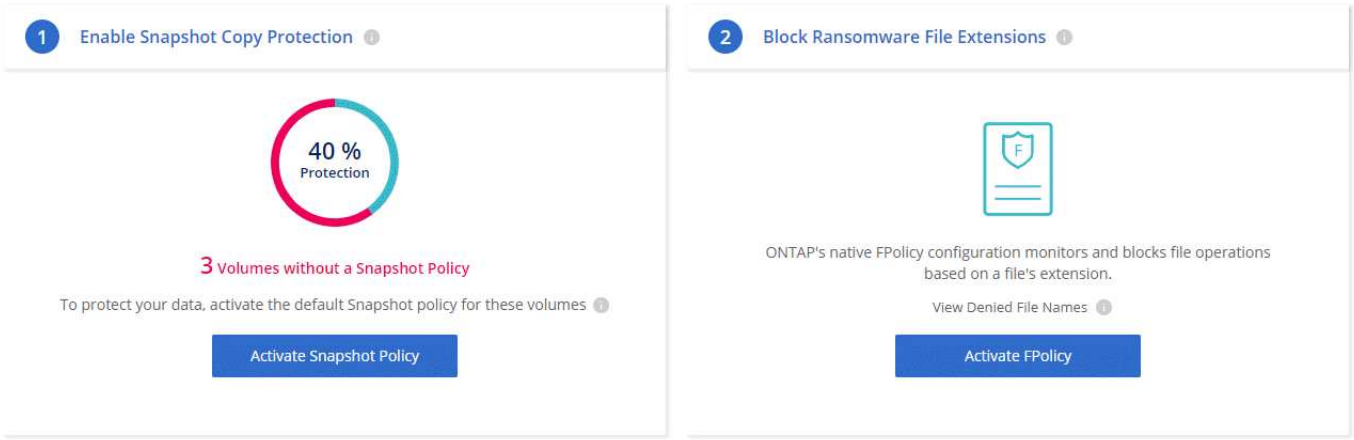
Protección contra ransomware

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.

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

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

Manos a la obra

Información general sobre la implementación

Antes de empezar, es posible que desee comprender mejor las opciones que existen para poner en marcha Cloud Manager y Cloud Volumes ONTAP.

Instalación de Cloud Manager

Se necesita software Cloud Manager para poner en marcha y gestionar Cloud Volumes ONTAP. Puede implementar Cloud Manager en cualquiera de las siguientes ubicaciones:

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform

  Cloud Manager debe estar en Google Cloud Platform cuando se ponga en marcha Cloud Volumes ONTAP en GCP.

- Cloud de IBM
- En su propia red

La forma en que ponga en marcha Cloud Manager depende de la ubicación que elija:

Ubicación de Cloud Manager	Cómo poner en marcha Cloud Manager
AWS	1. "Ponga en marcha Cloud Manager desde NetApp Cloud Central" (recomendado) 2. "Ponga en marcha desde AWS Marketplace" 3. "Descargue e instale el software en un host Linux"
AWS C2S	"Ponga en marcha Cloud Manager desde AWS Intelligence Community Marketplace"
Azure región generalmente disponible	1. "Ponga en marcha Cloud Manager desde NetApp Cloud Central" (recomendado) 2. "Ponga en marcha desde Azure Marketplace" 3. "Descargue e instale el software en un host Linux"
Gobierno de Azure	"Ponga en marcha Cloud Manager desde Azure US Government Marketplace"
Azure Alemania	"Descargue e instale el software en un host Linux"

Ubicación de Cloud Manager	Cómo poner en marcha Cloud Manager
Google Cloud Platform	1. "Ponga en marcha Cloud Manager desde NetApp Cloud Central" (recomendado) 2. "Descargue e instale el software en un host Linux" No puede poner en marcha Cloud Manager en Google Cloud desde GCP Marketplace
Cloud de IBM	"Descargue e instale el software en un host Linux"
Red local	"Descargue e instale el software en un host Linux"

Configuración de Cloud Manager

Puede que desee realizar una configuración adicional después de instalar Cloud Manager, como añadir cuentas de proveedor de cloud adicionales, instalar un certificado HTTPS, etc.

- "Configurar la cuenta de Cloud Central"
- "Añadiendo cuentas de AWS a Cloud Manager"
- "Adición de cuentas de Azure a Cloud Manager"
- "Instalar un certificado HTTPS"
- "Configuración de AWS KMS"

Puesta en marcha de Cloud Volumes ONTAP

Después de poner en marcha Cloud Manager, puede empezar a poner en marcha Cloud Volumes ONTAP en su proveedor de cloud.

"Introducción a AWS", "Introducción a Azure", y. "Introducción a GCP" Proporcionar instrucciones para poner en funcionamiento Cloud Volumes ONTAP rápidamente. Si necesita ayuda adicional, consulte lo siguiente:

- "Configuraciones compatibles para Cloud Volumes ONTAP 9.7 en AWS"
- "Configuraciones compatibles para Cloud Volumes ONTAP 9.7 en Azure"
- "Configuraciones admitidas para Cloud Volumes ONTAP 9.7 en GCP"
- "Planificación de la configuración"
- "Inicio de Cloud Volumes ONTAP en AWS"
- "Inicio de Cloud Volumes ONTAP en Azure"
- "Lanzamiento de Cloud Volumes ONTAP en GCP"

Introducción a Cloud Volumes ONTAP en AWS

Empiece a usar Cloud Volumes ONTAP configurando AWS e inicie el software Cloud Manager desde NetApp Cloud Central. Está disponible una prueba gratuita de 30 días para el primer sistema Cloud Volumes ONTAP que se lanza en AWS.

Configure su red

1. Habilite el acceso a Internet de salida desde el VPC de destino, de modo que Cloud Manager y Cloud Volumes ONTAP puedan ponerse en contacto con varios extremos.

   Este paso es importante porque Cloud Manager no puede poner en marcha Cloud Volumes ONTAP sin acceso saliente a Internet. Si necesita limitar la conectividad saliente, consulte la lista de puntos finales para "Cloud Manager" y.. "Cloud Volumes ONTAP".

2. 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.

Proporcione los permisos de AWS necesarios

Al implementar Cloud Manager desde NetApp Cloud Central, tiene que utilizar una cuenta de AWS con permisos para implementar la instancia.

1. Vaya a la consola AWS IAM y cree una política copiando y pegando el contenido de "Política central de Cloud de NetApp para AWS".
2. Adjunte la política al usuario del IAM.

Suscríbase desde el AWS Marketplace

"Suscríbase a Cloud Manager desde AWS Marketplace" Para garantizar que no se interrumpe el servicio una vez que finaliza la prueba gratuita de Cloud Volumes ONTAP. A partir de esta suscripción se le cobrará cada sistema de Cloud Volumes ONTAP PAYGO que cree y cada función complementaria que habilite.

Si inicia Cloud Volumes ONTAP con su propia licencia (BYOL), "Después, tendrá que suscribirse a esta oferta en AWS Marketplace".

Inicie Cloud Manager desde NetApp Cloud Central

Se necesita software Cloud Manager para poner en marcha y gestionar Cloud Volumes ONTAP. Se tarda unos pocos minutos en iniciar una instancia de Cloud Manager desde "Cloud Central".

Inicie Cloud Volumes ONTAP mediante Cloud Manager

Una vez que Cloud Manager esté listo, solo tiene que hacer clic en Create, seleccionar el tipo de sistema que le gustaría iniciar y completar los pasos del asistente. Tras 25 minutos, el primer sistema Cloud Volumes ONTAP debe estar listo para funcionar.

Vea el siguiente vídeo para conocer estos pasos:

► https://docs.netapp.com/es-es/occm37//media/video_getting_started_aws.mp4 *(video)*

Enlaces relacionados

- "Evaluación"
- "Requisitos de red para Cloud Manager"
- "Requisitos de red para Cloud Volumes ONTAP en AWS"
- "Reglas de grupos de seguridad para AWS"
- "Añadiendo cuentas de AWS a Cloud Manager"
- "Qué hace Cloud Manager con los permisos de AWS"
- "Inicio de Cloud Volumes ONTAP en AWS"
- "Ejecute Cloud Manager desde AWS Marketplace"

Introducción a Cloud Volumes ONTAP en Azure

Empiece a usar Cloud Volumes ONTAP configurando Azure y, a continuación, ponga en marcha el software Cloud Manager desde Cloud Central de NetApp. Hay disponibles instrucciones adicionales para implementar Cloud Manager en "Regiones gubernamentales de Azure EE. UU" y en "Regiones de Azure Alemania".

Configure su red

Habilite el acceso saliente a Internet desde la red virtual de destino para que Cloud Manager y Cloud Volumes ONTAP puedan ponerse en contacto con varios extremos.

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

Proporcione los permisos de Azure necesarios

Al poner en marcha Cloud Manager desde NetApp Cloud Central, necesita utilizar una cuenta de Azure con permisos para implementar la máquina virtual de Cloud Manager.

1. Descargue el "Política Cloud Central de NetApp para Azure".
2. Modifique el archivo JSON añadiendo el ID de suscripción de Azure al campo "AssignableScopes".
3. Utilice el archivo JSON para crear una función personalizada en Azure denominada *Azure SetupAsService*.

   Ejemplo: **Az role definition create --role-definition C:\Policy_for_Setup_as_Service_Azure.json**

4. En el portal de Azure, asigne la función personalizada al usuario que pondrá en marcha Cloud Manager desde Cloud Central.

Inicie Cloud Manager desde NetApp Cloud Central

Se necesita software Cloud Manager para poner en marcha y gestionar Cloud Volumes ONTAP. Se tarda unos

pocos minutos en iniciar una instancia de Cloud Manager desde "Cloud Central".

Inicie Cloud Volumes ONTAP mediante Cloud Manager

Una vez que Cloud Manager esté listo, haga clic en Create, seleccione el tipo de sistema que desea implementar y complete los pasos del asistente. Tras 25 minutos, el primer sistema Cloud Volumes ONTAP debe estar listo para funcionar.

Enlaces relacionados

- "Evaluación"
- "Requisitos de red para Cloud Manager"
- "Requisitos de red para Cloud Volumes ONTAP en Azure"
- "Reglas de grupos de seguridad para Azure"
- "Adición de cuentas de Azure a Cloud Manager"
- "Qué hace Cloud Manager con permisos de Azure"
- "Inicio de Cloud Volumes ONTAP en Azure"
- "Ejecute Cloud Manager desde Azure Marketplace"

Introducción a Cloud Volumes ONTAP en Google Cloud Platform

Empiece a usar Cloud Volumes ONTAP configurando GCP y, a continuación, poniendo en marcha el software Cloud Manager de NetApp Cloud Central.

Cloud Manager debe instalarse en Google Cloud Platform para poder poner en marcha Cloud Volumes ONTAP en GCP.

Configure su red

Habilite el acceso a Internet de salida desde el VPC de destino, de modo que Cloud Manager y Cloud Volumes ONTAP puedan ponerse en contacto con varios extremos.

Este paso es importante porque Cloud Manager no puede poner en marcha Cloud Volumes ONTAP sin acceso saliente a Internet. Si necesita limitar la conectividad saliente, consulte la lista de puntos finales para "Cloud Manager" y.. "Cloud Volumes ONTAP".

Configure los permisos y proyectos de GCP

Asegúrese de que existen dos conjuntos de permisos:

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

   Esta cuenta de servicio se asociará a la máquina virtual de Cloud Manager en el paso 6.

   - "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.

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

Configure GCP para la organización en niveles de datos

Deben cumplirse dos requisitos para agrupar los datos fríos en niveles de Cloud Volumes ONTAP 9.7 en un almacenamiento de objetos de bajo coste (un bucket de almacenamiento en cloud de Google):

1. "Cree una cuenta de servicio" Que tiene el rol de administrador de almacenamiento predefinido y la cuenta de servicio de Cloud Manager como usuario.

   Deberá seleccionar esta cuenta de servicio más adelante al crear un entorno de trabajo de Cloud Volumes ONTAP. Esta cuenta de servicio es diferente de la cuenta de servicio que creó en el paso 2.

2. "Configure la subred de Cloud Volumes ONTAP para acceso privado a Google".

Si desea utilizar la organización en niveles de datos con Cloud Volumes ONTAP 9.6, "a continuación, siga estos pasos".

Habilite las API de Google Cloud

"Habilite las siguientes API de Google Cloud en su proyecto". Estas API son necesarias para poner en marcha Cloud Manager y Cloud Volumes ONTAP.

- API de Cloud Deployment Manager V2
- API de Cloud Resource Manager
- API del motor de computación
- API de registro de Stackdriver

Suscríbase en el mercado de GCP

"Suscríbase a Cloud Volumes ONTAP en el mercado de GCP" para asegurarse de que no haya interrupción del servicio después de que finalice su prueba gratuita. Se le cobrará de esta suscripción por cada sistema Cloud Volumes ONTAP PAYGO que cree.

Inicie Cloud Manager desde NetApp Cloud Central

Se necesita software Cloud Manager para poner en marcha y gestionar Cloud Volumes ONTAP. Se tarda solo unos minutos en lanzar una instancia de Cloud Manager en GCP desde "Cloud Central".

Cuando elige GCP como proveedor de cloud, Google le pide que inicie sesión en su cuenta y que conceda permisos. Al hacer clic en "permitir", se concede acceso a las API de computación necesarias para implementar Cloud Manager.

Inicie Cloud Volumes ONTAP mediante Cloud Manager

Una vez que Cloud Manager esté listo, haga clic en Create, seleccione el tipo de sistema que desea implementar y complete los pasos del asistente. Tras 25 minutos, el primer sistema Cloud Volumes ONTAP debe estar listo para funcionar.

Enlaces relacionados

- "Evaluación"
- "Requisitos de red para Cloud Manager"
- "Requisitos de red para Cloud Volumes ONTAP en GCP"
- "Reglas de firewall para GCP"
- "Qué hace Cloud Manager con los permisos de GCP"
- "Lanzamiento de Cloud Volumes ONTAP en GCP"
- "Descargue e instale el software Cloud Manager en un host Linux"

Configure Cloud Manager

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

Cada sistema de Cloud Manager está asociado con una cuenta *de Cloud Central de NetApp*. Configure la cuenta de Cloud Central asociada con su sistema de Cloud Manager para que los usuarios puedan acceder a Cloud Manager e implementar sistemas Cloud Volumes ONTAP en espacios de trabajo. Solo tiene que agregar un usuario o agregar varios usuarios y espacios de trabajo.

La cuenta se mantiene en Cloud Central, por lo que cualquier cambio que haga estará disponible para otros sistemas de Cloud Manager y para otros servicios de datos en el cloud de NetApp. "Obtenga más información sobre cómo funcionan las cuentas de Cloud Central".

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 los espacios de trabajo.

Pasos

1. Haga clic en **Configuración de cuenta**.

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

Después de terminar

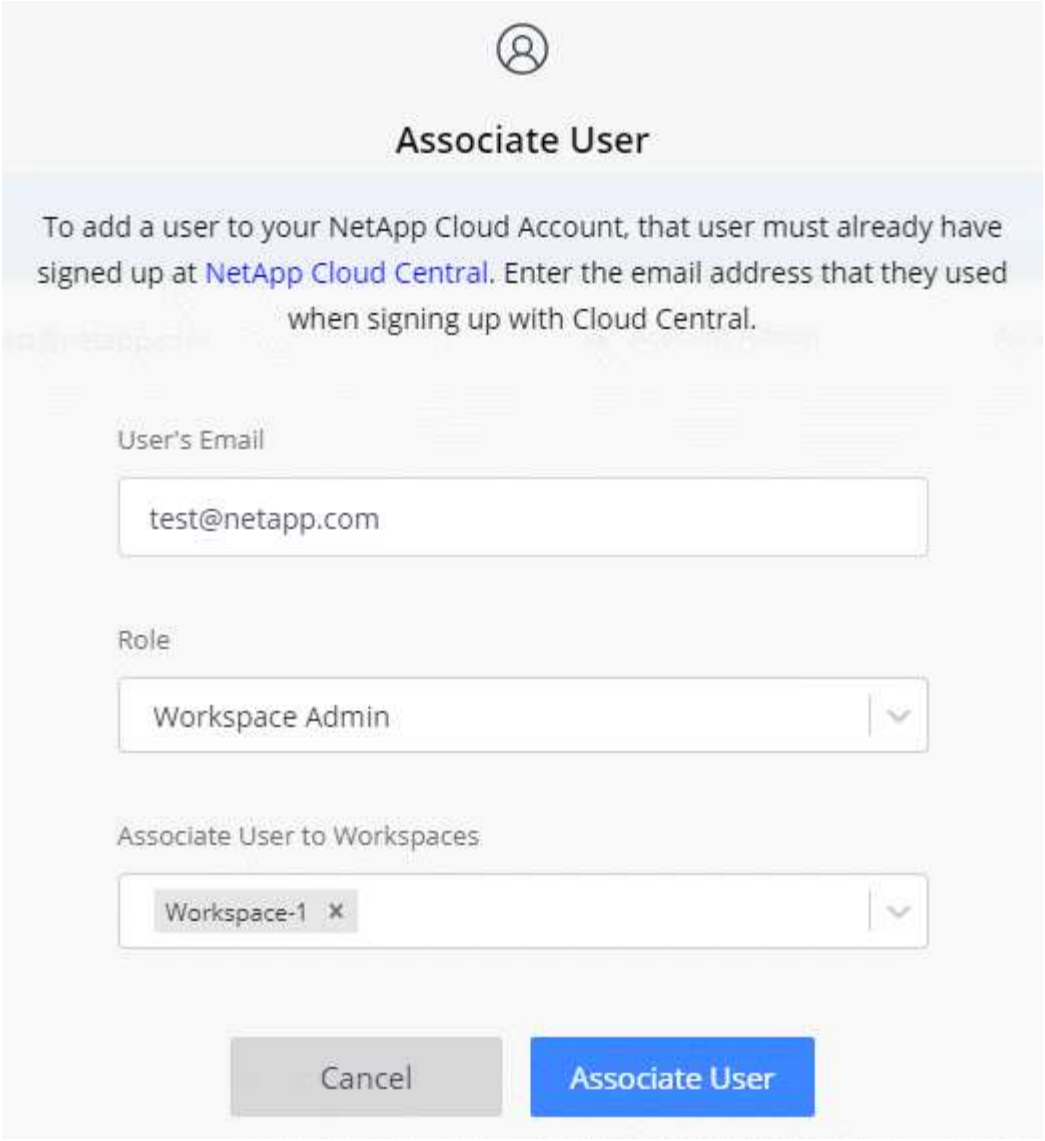
Ahora puede asociar usuarios y conectores de servicio al espacio de trabajo.

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 crear una cuenta.
2. En Cloud Manager, haga clic en **Configuración de 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.
5. Si ha seleccionado Administrador de área de trabajo, seleccione una o más áreas de trabajo para asociarlas a ese usuario.



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

Resultado

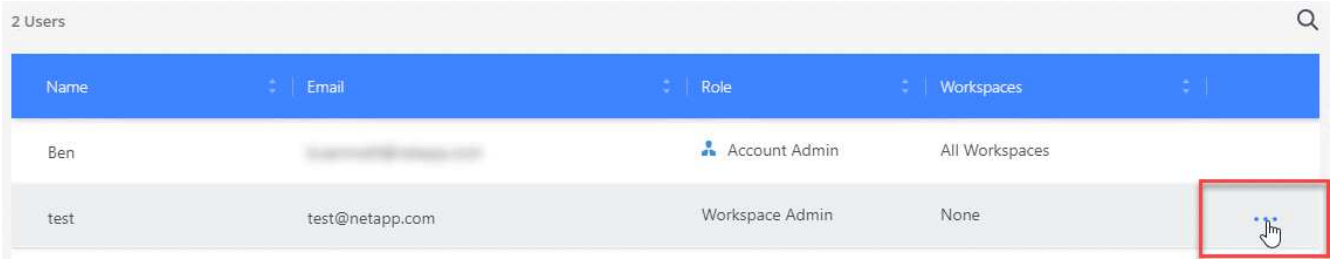
El usuario debe recibir un correo electrónico de Cloud Central de NetApp titulado "Account Association". El correo electrónico incluye la información necesaria para acceder a Cloud Manager.

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. Haga clic en **Configuración de cuenta**.
2. Haga clic en el menú de 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 estos espacios de trabajo desde Cloud Manager, siempre y cuando el conector del servicio también esté asociado a los espacios de trabajo.

Asociación de conectores de servicio con áreas de trabajo

Un conector de servicio forma parte del sistema Cloud Manager. Se ejecuta en la instancia de máquina virtual que se implementó en su proveedor de cloud o en un host en las instalaciones que configuró. Debe asociar este conector de servicio a espacios de trabajo para que los administradores de espacio de trabajo puedan acceder a estos espacios de trabajo desde Cloud Manager.

Si sólo tiene Administradores de cuentas, no es necesario asociar el conector de servicio 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, espacios de trabajo y conectores de servicio".

Pasos

1. Haga clic en **Configuración de cuenta**.
2. Haga clic en **Service Connector**.
3. Haga clic en **Administrar áreas de trabajo** para el conector de servicio 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 acceder a los espacios de trabajo asociados, siempre que el usuario también esté asociado al área de trabajo.

Configurar y añadir cuentas de AWS en Cloud Manager

Si desea poner en marcha Cloud Volumes ONTAP en diferentes cuentas de AWS, debe proporcionar los permisos necesarios y añadir los detalles a Cloud Manager. 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 pone en marcha Cloud Manager desde Cloud Central, Cloud Manager agrega automáticamente la cuenta de AWS en la que implementó Cloud Manager. No se agrega una cuenta inicial si instaló manualmente el software Cloud Manager en un sistema existente. "Obtenga más información acerca de los permisos y las cuentas de AWS".

opciones

- Concesión de permisos proporcionando claves AWS
- Otorgar permisos asumiendo roles de IAM en otras cuentas

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

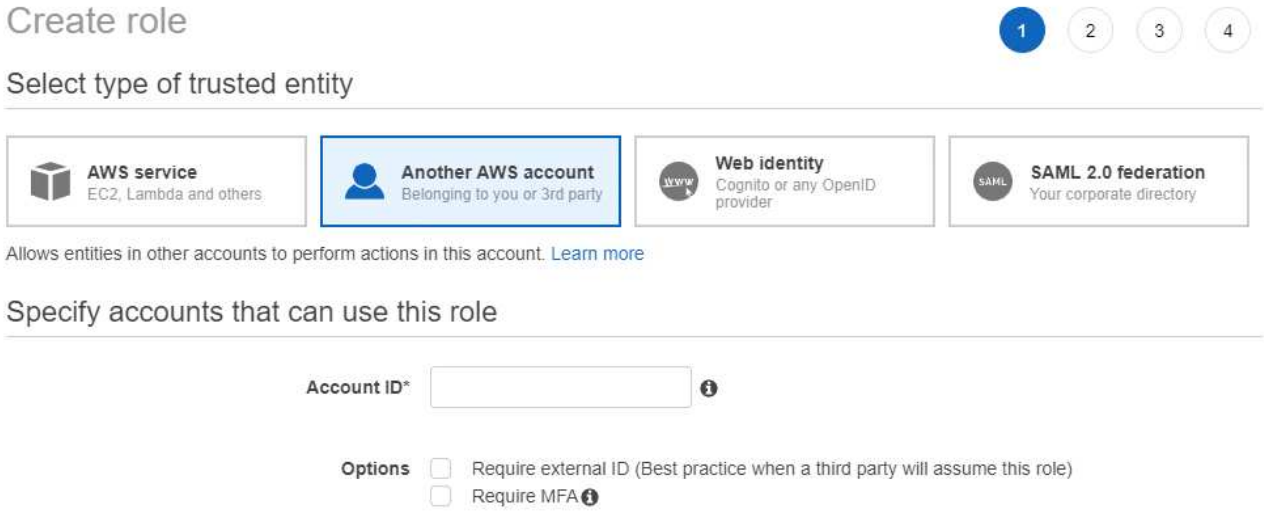
Puede configurar una relación de confianza entre la cuenta de AWS de origen en la que implementó la instancia de Cloud Manager y otras cuentas de AWS mediante los roles de IAM. A continuación, debe proporcionar a Cloud Manager el ARN de las funciones de IAM de las cuentas de confianza.

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 ID de la cuenta en la que reside la instancia de Cloud Manager.
   - Adjunte la política IAM de Cloud Manager, que está disponible en la "Directivas de Cloud Manager".



2. Vaya a la cuenta de origen donde reside la instancia de Cloud Manager y seleccione la función IAM que se adjunta a la instancia.

   a. Haga clic en **Relaciones de confianza > Editar relación de confianza**.

   b. Agregue la acción "sts:AssumeRole" y el ARN de la función 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

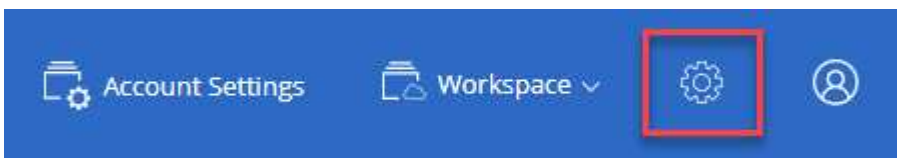
La cuenta ahora tiene los permisos necesarios. Ahora puede añadirlo a Cloud Manager.

Añadiendo cuentas de AWS a Cloud Manager

Después de proporcionar una cuenta de AWS con los permisos necesarios, puede añadir la cuenta a Cloud Manager. Esto le permite iniciar sistemas de Cloud Volumes ONTAP en esa cuenta.

Pasos

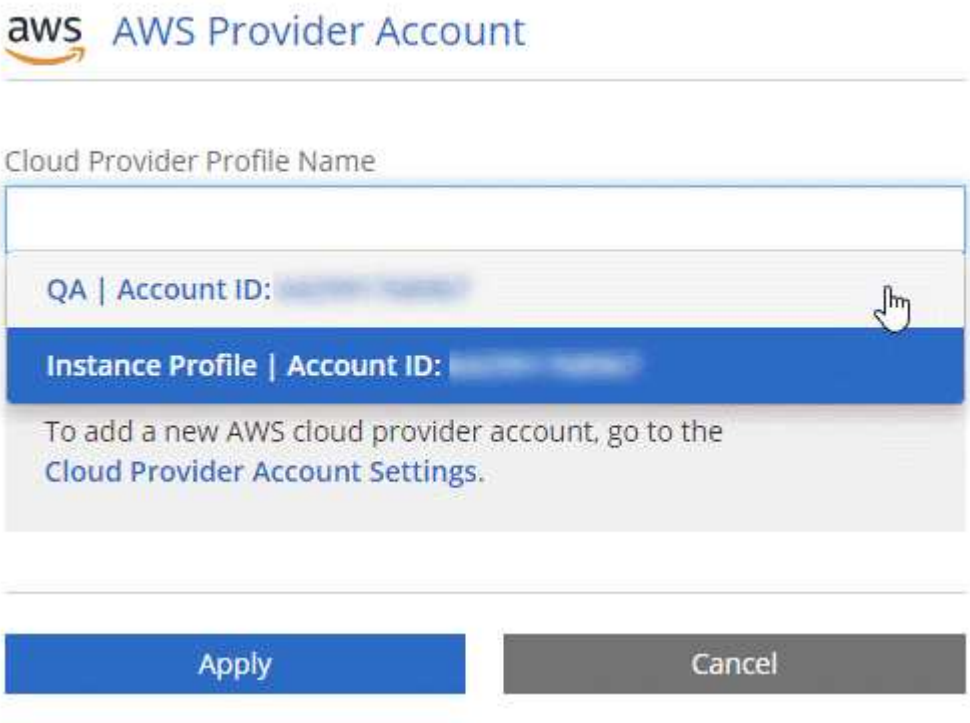
1. En la esquina superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **Proveedor de cloud y Cuentas de soporte**.



2. Haga clic en **Agregar nueva cuenta** y seleccione **AWS**.
3. Elija si desea proporcionar las claves AWS o el ARN de un rol de IAM de confianza.
4. Confirme que se han cumplido los requisitos de la directiva y, a continuación, haga clic en **Crear cuenta**.

Resultado

Ahora puede cambiar a otra cuenta desde la página Details y Credentials al crear un nuevo entorno de trabajo:



Configurar y añadir cuentas de Azure a Cloud Manager

Si desea poner en marcha Cloud Volumes ONTAP en diferentes cuentas de Azure, tendrá que proporcionar los permisos necesarios para esas cuentas y, a continuación, añadir detalles acerca de las cuentas a Cloud Manager.

Cuando se pone en marcha Cloud Manager desde Cloud Central, Cloud Manager agrega automáticamente la cuenta de Azure en la que implementó Cloud Manager. No se agrega una cuenta inicial si instaló manualmente el software Cloud Manager en un sistema existente. "Obtenga más información acerca de las cuentas y los permisos de Azure".

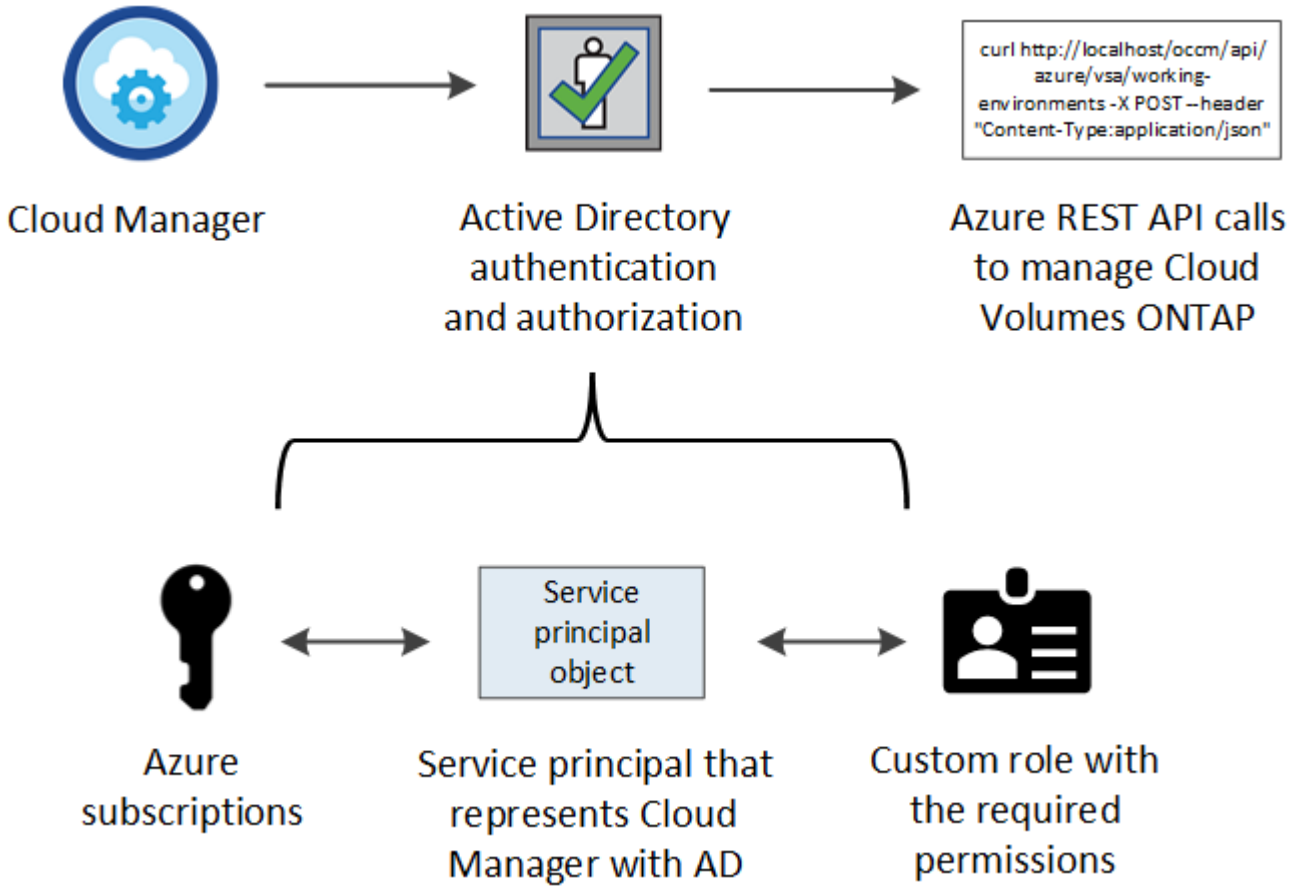
Concesión de permisos de Azure con un director de servicio

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

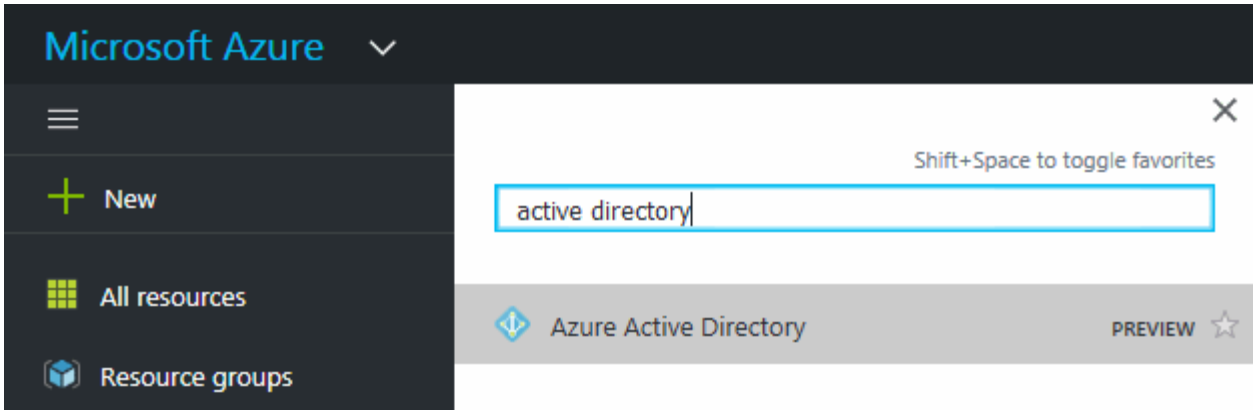
Cree una aplicación de Azure Active Directory (AD) y una entidad de servicio que Cloud Manager pueda usar para el control de acceso basado en roles.

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_3.7.4.json

Ahora debe tener un rol personalizado denominado *OnCommand Cloud Manager Operator*.

2. Asigne la aplicación al rol:

   a. En el portal de Azure, abra el servicio **Suscripciones**.

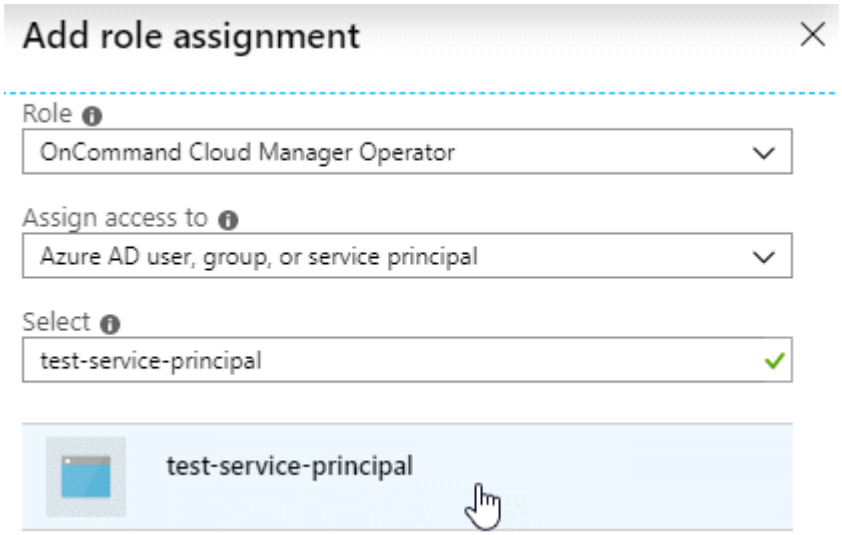
   b. Seleccione la suscripción.

   c. Haga clic en **Control de acceso (IAM) > Agregar > Agregar asignación de funciones**.

   d. Seleccione el rol **operador de Cloud Manager de OnCommand**.

   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.

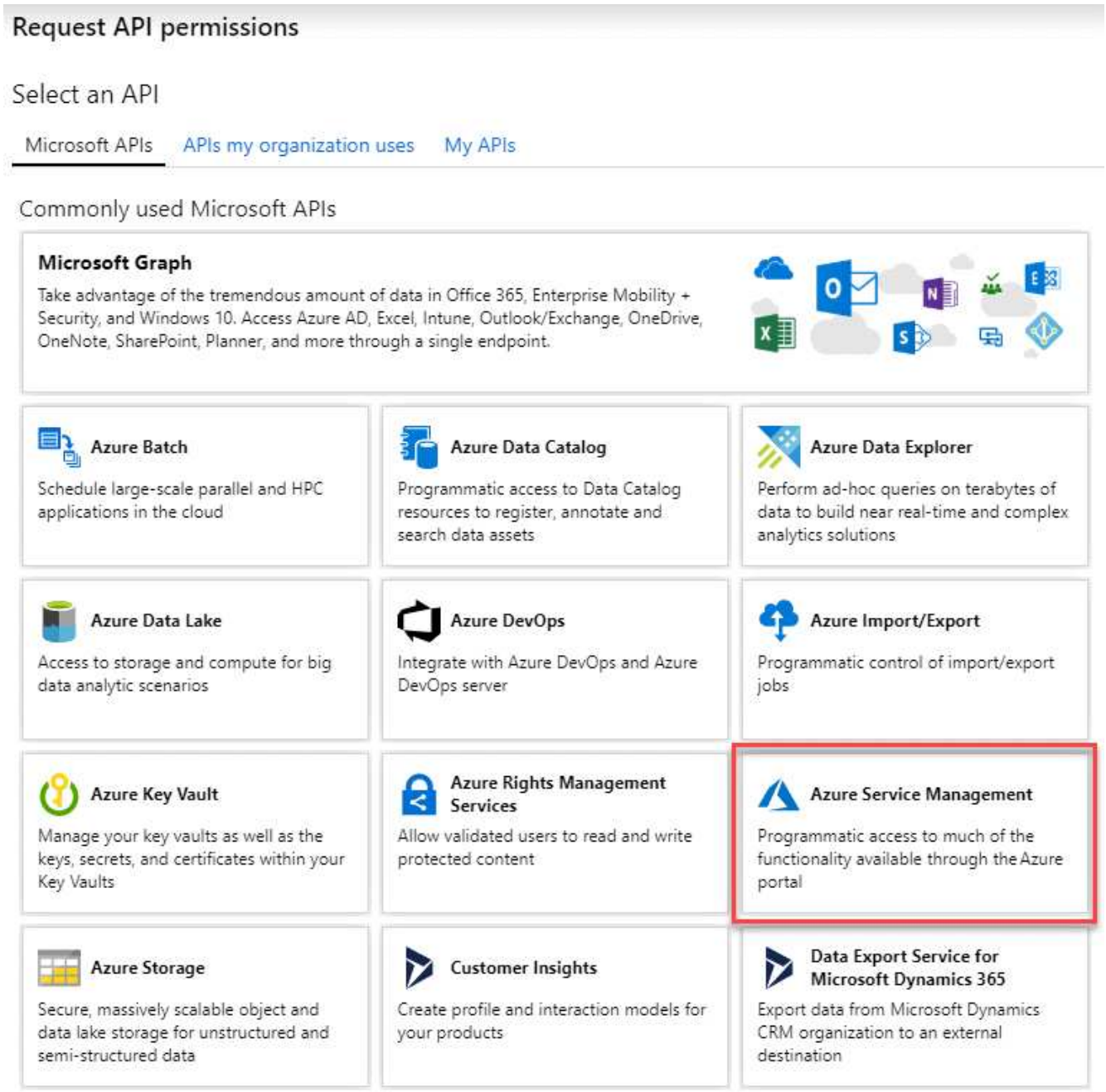
Si desea implementar Cloud Volumes ONTAP desde varias suscripciones a Azure, debe enlazar el principal del servicio con cada una de ellas. Cloud Manager le permite seleccionar la suscripción que desea utilizar al poner en marcha Cloud Volumes ONTAP.

Agregar permisos de API de administración de servicios de Windows Azure

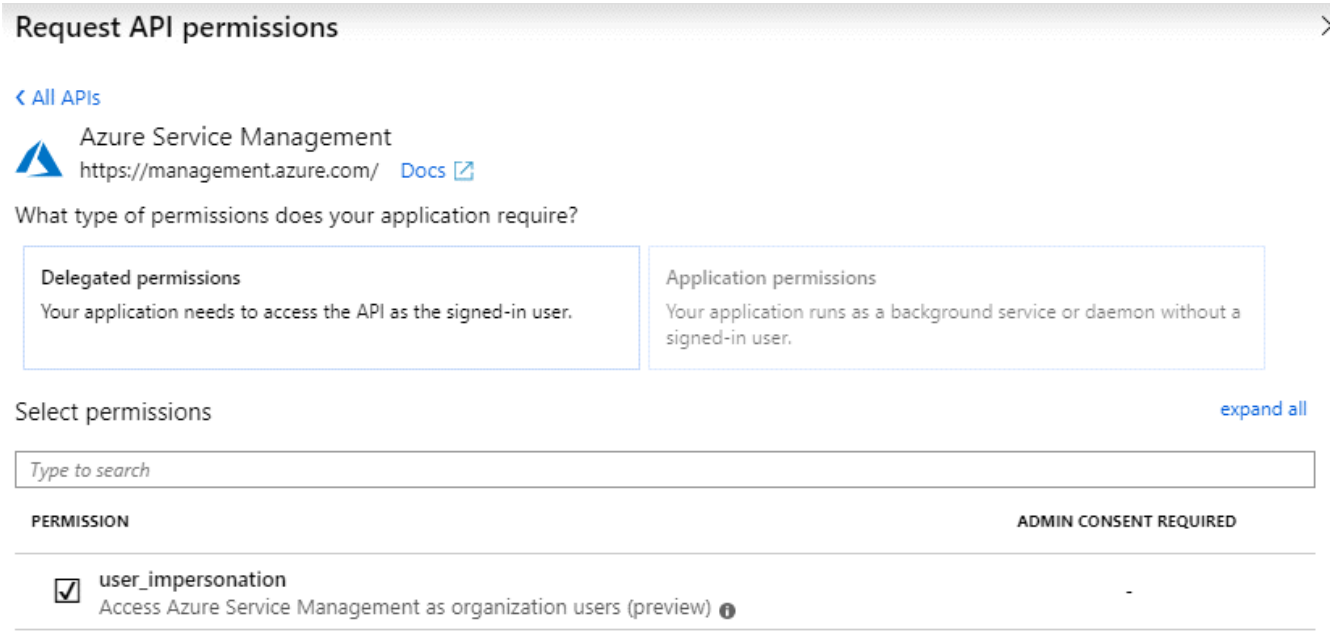
El principal de servicio debe tener permisos de "API de administración de servicios de Windows Azure".

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**.

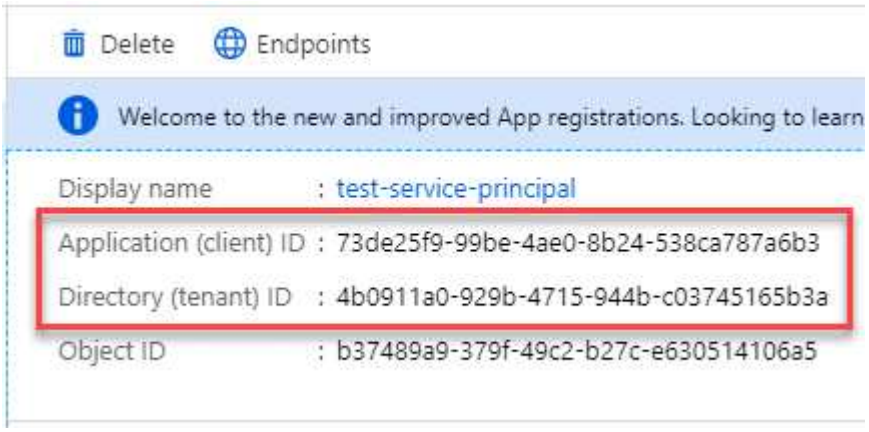


Obteniendo el ID de aplicación y el ID de directorio

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.

Adición de cuentas de Azure a Cloud Manager

Después de proporcionar una cuenta de Azure con los permisos necesarios, puede añadir la cuenta a Cloud Manager. Esto le permite iniciar sistemas de Cloud Volumes ONTAP en esa cuenta.

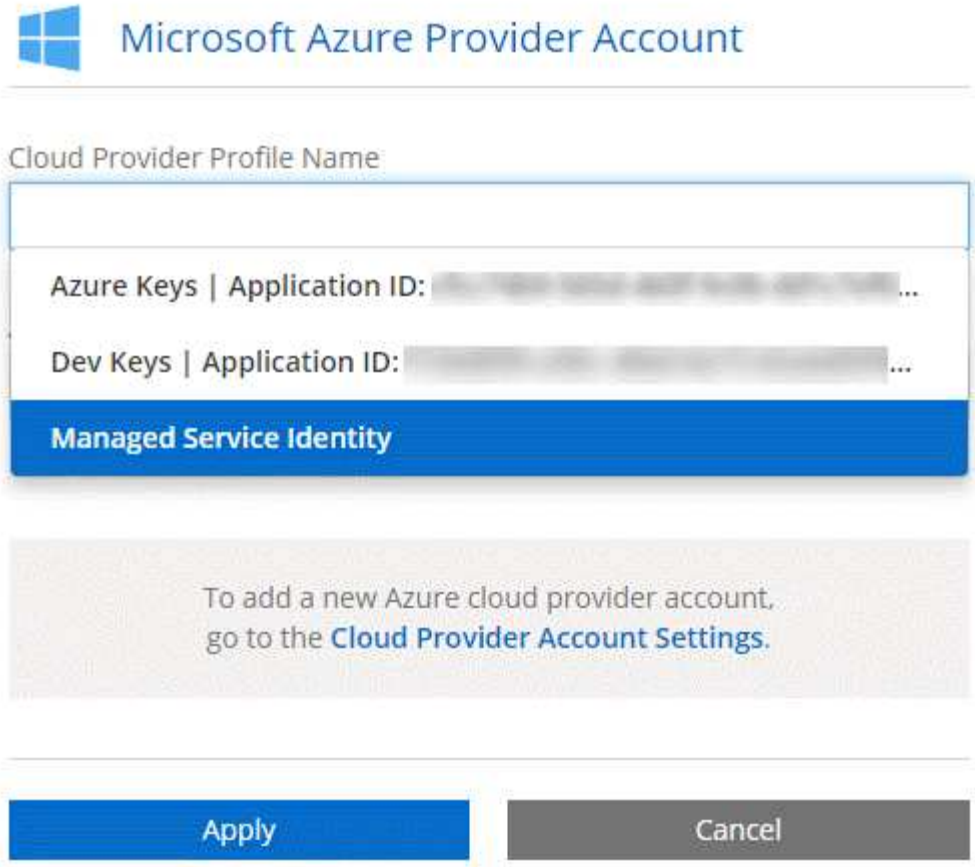
Pasos

1. En la esquina superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **Proveedor de cloud y Cuentas de soporte**.

2. Haga clic en **Agregar nueva cuenta** 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: Consulte Obteniendo el ID de aplicación y el ID de directorio.
   - ID de inquilino (o ID de directorio): Consulte Obteniendo el ID de aplicación y el ID de directorio.
   - Clave de aplicación (el secreto de cliente): Consulte Crear un secreto de cliente.
4. Confirme que se han cumplido los requisitos de la directiva y, a continuación, haga clic en **Crear cuenta**.

Resultado

Ahora puede cambiar a otra cuenta desde la página Details y Credentials al crear un nuevo entorno de trabajo:



Asociar suscripciones de Azure adicionales a una identidad administrada

Cloud Manager le permite elegir la cuenta y la suscripción de Azure en la que desee 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" Cuando pone en marcha Cloud Manager desde NetApp Cloud Central. Cuando implementó Cloud Manager, Cloud Central creó la función del operador de Cloud Manager de OnCommand y la asignó a la máquina virtual de Cloud Manager.

Pasos

1. Inicie sesión en el portal de Azure.
2. Abra el servicio **Suscripciones** y seleccione la suscripción en la que desea implementar sistemas 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 de OnCommand**.

        El nombre predeterminado que se proporciona en la es el operador de OnCommand Cloud Manager "Política de Cloud Manager". Si seleccionó otro nombre para el rol, seleccione ese nombre.

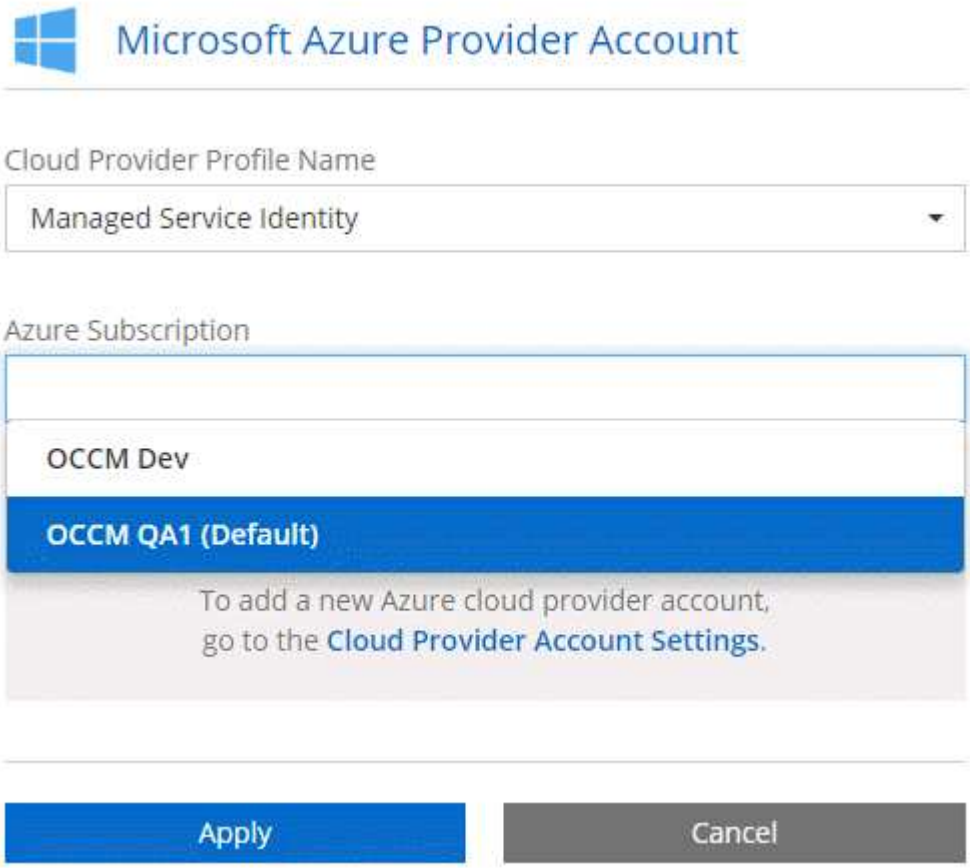
      - Asigne acceso a una **máquina virtual**.

- Seleccione la suscripción en la que se creó la máquina virtual de Cloud Manager.
- Seleccione la máquina virtual Cloud Manager.
- 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.



Configuración y adición de cuentas de GCP a Cloud Manager

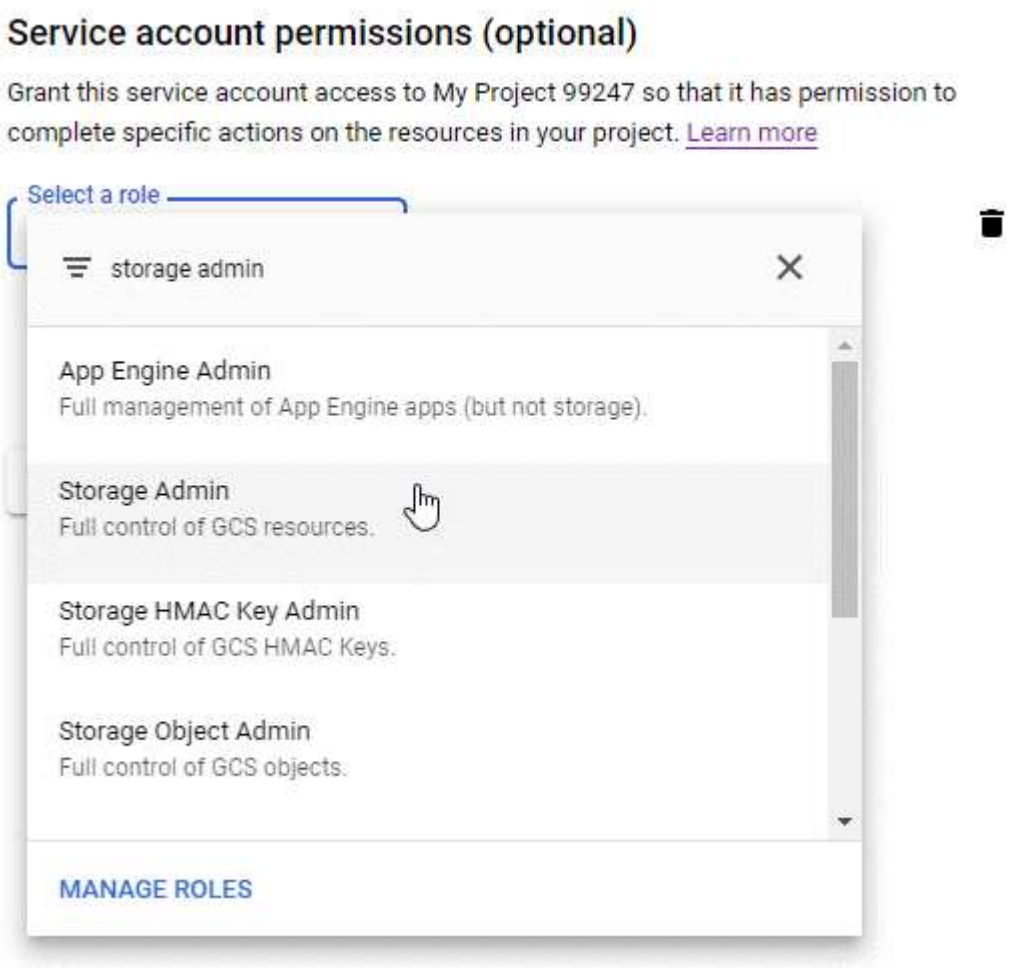
Si desea habilitar "organización en niveles de los datos" En un sistema Cloud Volumes ONTAP, debe proporcionar a Cloud Manager una clave de acceso al almacenamiento para una cuenta de servicio con permisos de administrador de almacenamiento. Cloud Manager utiliza las claves de acceso para configurar y gestionar un bucket de Cloud Storage para la organización de datos en niveles.

Configuración de una cuenta de servicio y claves de acceso para Google Almacenamiento en cloud

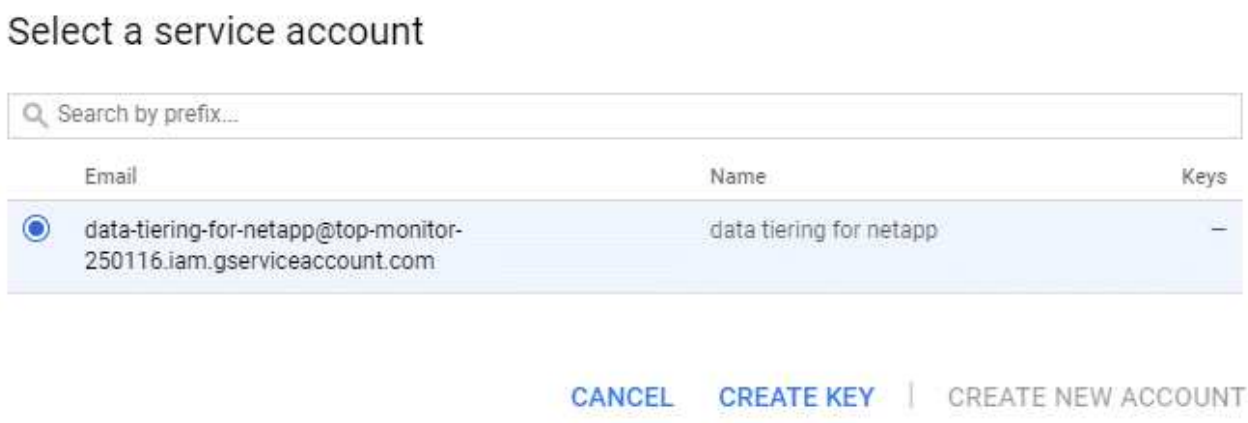
Una cuenta de servicio permite que Cloud Manager autentique y acceda a los bloques de almacenamiento en cloud que se utilizan para la organización en niveles de los datos. Las claves son necesarias para que Google Cloud Storage sepa quién está haciendo la solicitud.

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.

Pasos

1. En la esquina superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **Proveedor de cloud y Cuentas de soporte**.

2. Haga clic en **Agregar nueva cuenta** y seleccione **GCP**.
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 al crearlos, modificarlos o replicarlos. 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*

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 **Proveedor de cloud y Cuentas de soporte**.

3. Haga clic en **Agregar nueva cuenta** 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"

Instalar un certificado HTTPS para obtener 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.

Pasos

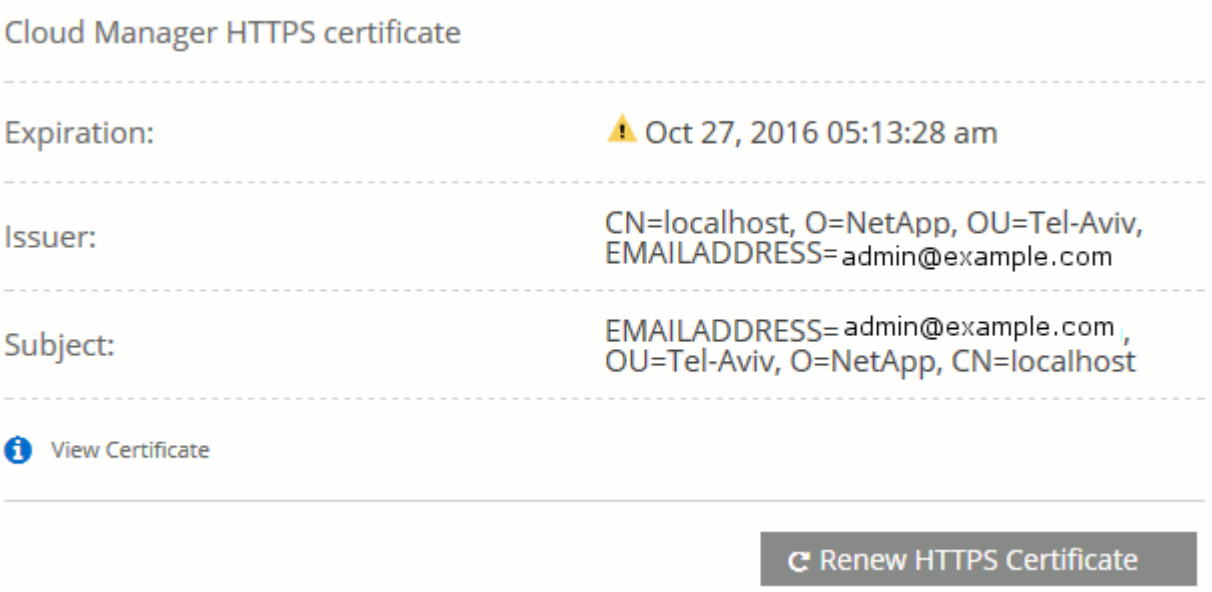
1. En la parte superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **Configuración HTTPS**.

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 de Cloud Manager (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:



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.

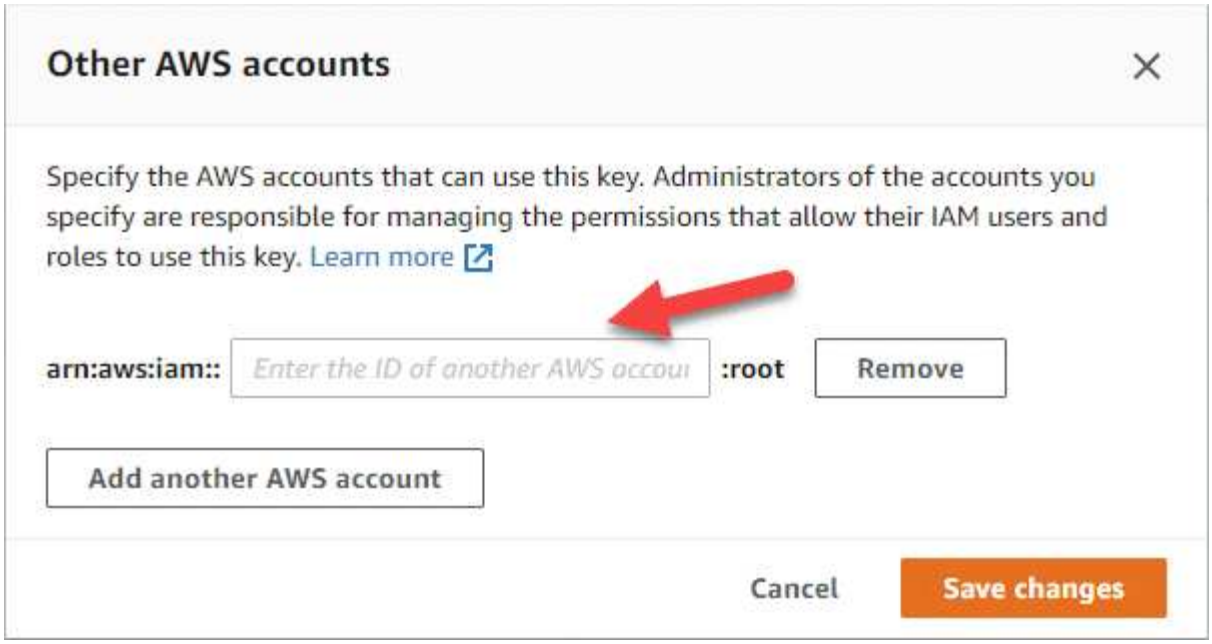
   b. Seleccione la tecla.

   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".

Requisitos de red

Requisitos de red para Cloud Manager

Configure su red para que Cloud Manager pueda poner en marcha sistemas de Cloud Volumes ONTAP en AWS, Microsoft Azure o Google Cloud Platform. 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, Cloud Manager le solicita que especifique el proxy durante la instalación. También puede especificar el servidor proxy en la página Configuración. Consulte "Configuración de Cloud Manager para usar un servidor proxy".

Conexión a redes de destino

Cloud Manager requiere una conexión de red a los VPC y VNets en los que desea implementar Cloud Volumes ONTAP.

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

Acceso a Internet de salida

Cloud Manager requiere acceso a Internet de salida para poner en marcha y gestionar Cloud Volumes ONTAP. También es necesario acceder a Internet de salida al acceder a Cloud Manager desde el explorador web y al ejecutar el instalador de Cloud Manager en un host Linux.

En las siguientes secciones se identifican los puntos finales específicos.

Extremos para gestionar Cloud Volumes ONTAP en AWS

Cloud Manager requiere acceso saliente a Internet para contactar con los siguientes extremos al implementar y gestionar Cloud Volumes ONTAP 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.

Puntos finales	Específico
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Proporciona acceso a imágenes, manifiestos y plantillas de software.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com	Permite a Cloud Manager acceder y descargar manifiestos, plantillas e imágenes de actualización de Cloud Volumes ONTAP.
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.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement	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.

Extremos para gestionar Cloud Volumes ONTAP en Azure

Cloud Manager requiere acceso saliente a Internet para contactar con los siguientes extremos al poner en marcha y gestionar Cloud Volumes ONTAP en Microsoft 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://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com	Permite a Cloud Manager acceder y descargar manifiestos, plantillas e imágenes de actualización de Cloud Volumes ONTAP.
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	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.

Extremos para gestionar Cloud Volumes ONTAP en GCP

Cloud Manager requiere acceso saliente a Internet para contactar con los siguientes extremos cuando se pone en marcha y se gestiona Cloud Volumes ONTAP en GCP:

Puntos finales	Específico
https://www.googleapis.com	Permite que Cloud Manager 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://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com	Permite a Cloud Manager acceder y descargar manifiestos, plantillas e imágenes de actualización de Cloud Volumes ONTAP.
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	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.

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
El host de Cloud Manager	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.

Extremos para instalar Cloud Manager en un host Linux

El instalador de Cloud Manager 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

Puertos y grupos de seguridad

- Si implementa Cloud Manager desde Cloud Central o desde imágenes de mercado, consulte lo siguiente:
  - "Reglas de grupo de seguridad para Cloud Manager en AWS"
  - "Reglas de grupo de seguridad para Cloud Manager en Azure"
  - "Reglas de firewall para Cloud Manager en GCP"
- Si instala Cloud Manager en un host Linux existente, consulte "Requisitos del host de Cloud Manager".

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 de la red de AWS 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.

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 de red de AWS para alta disponibilidad de Cloud Volumes ONTAP en múltiples 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.

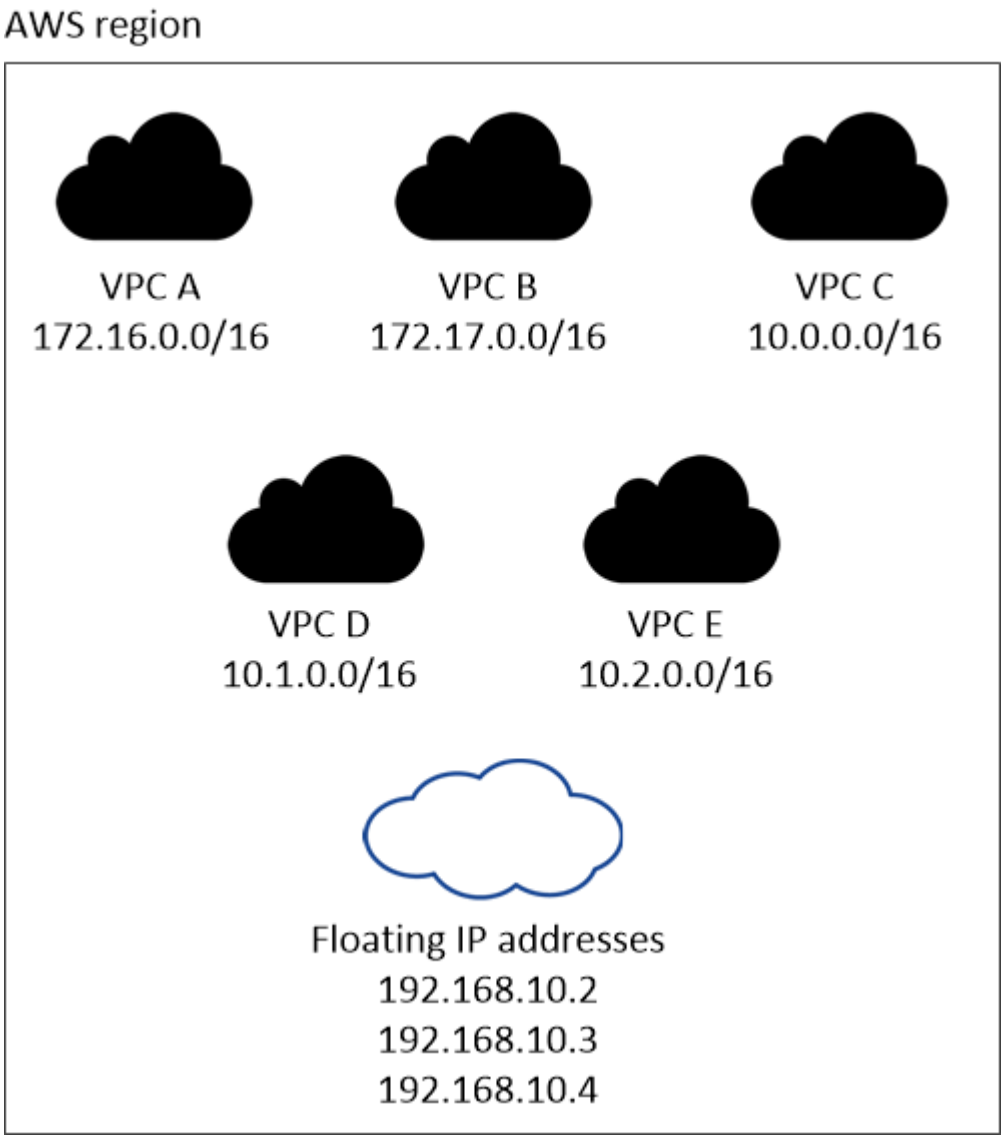
Se requiere una dirección IP flotante para el LIF de gestión de SVM si se usa SnapDrive para Windows o SnapCenter con el par de alta disponibilidad. Si no especifica la dirección IP al implementar el sistema, puede crear la LIF más adelante. Para obtener más información, consulte "Configurar Cloud Volumes 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".

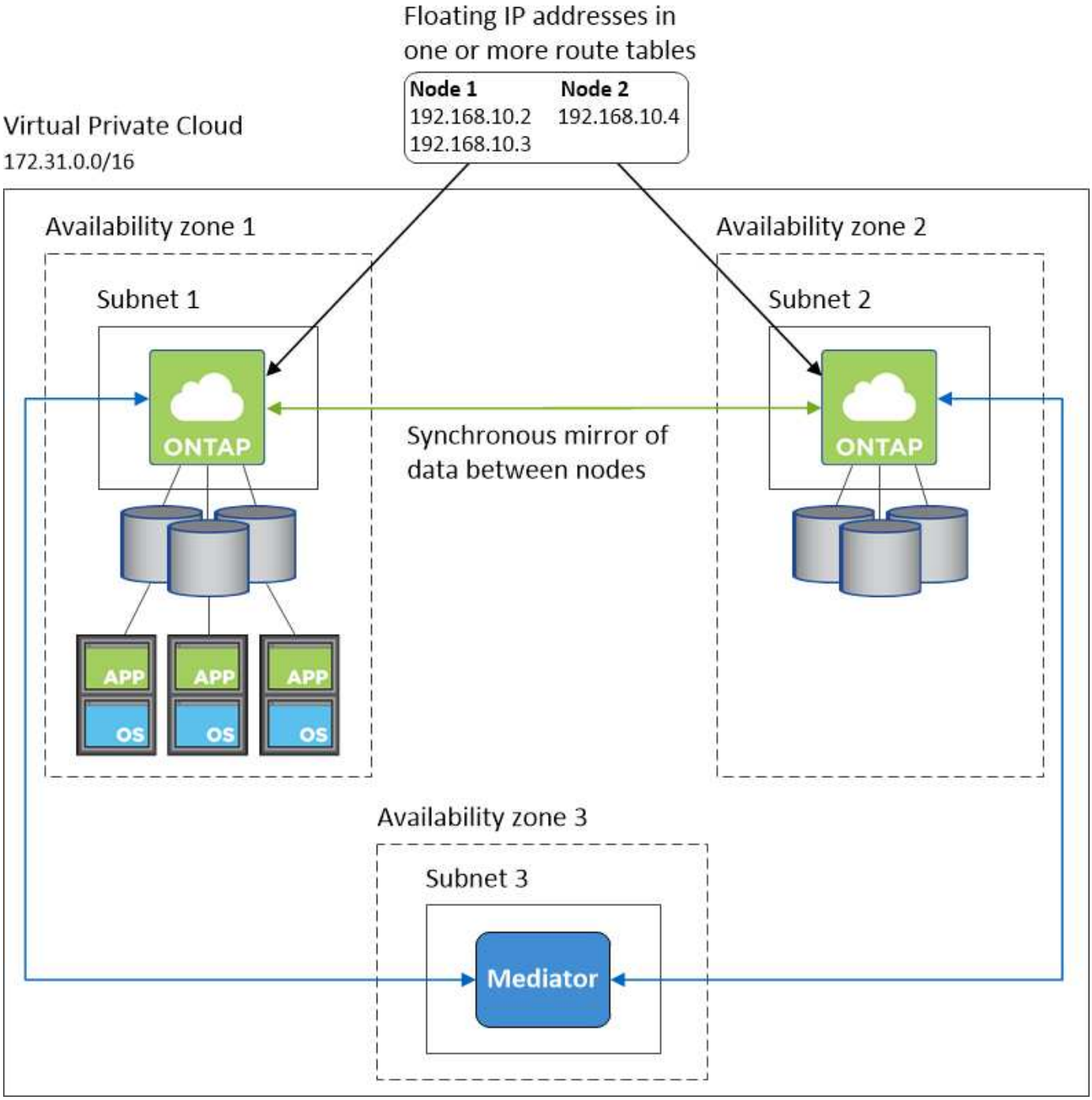
Conexión a herramientas de gestión de NetApp

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.

Configuración de ejemplo

En la siguiente imagen, se muestra una configuración de alta disponibilidad óptima en AWS que funciona como una configuración activo-pasivo:



Configuraciones VPC de muestra

Para comprender mejor cómo poner en marcha Cloud Manager y Cloud Volumes ONTAP en AWS, debe revisar las configuraciones más habituales del VPC.

- VPC con subredes públicas y privadas y un dispositivo NAT
- Un VPC con una subred privada y una conexión VPN a la red

VPC con subredes públicas y privadas y un dispositivo NAT

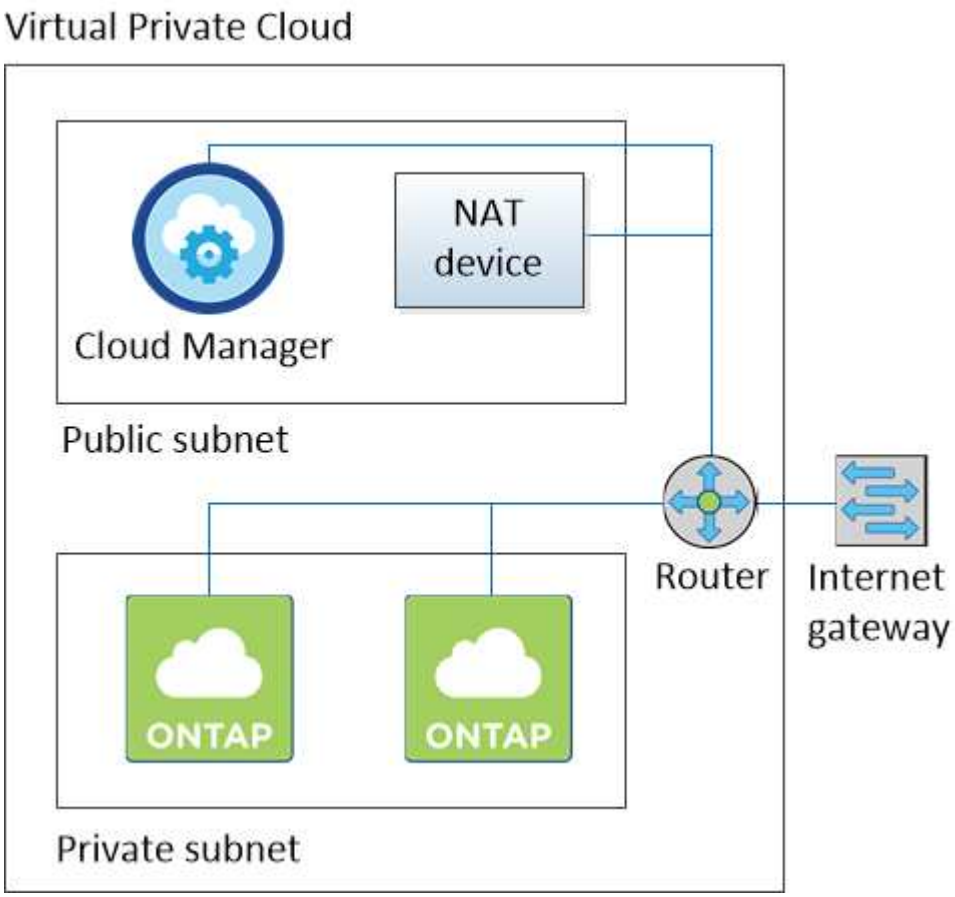
Esta configuración de VPC incluye subredes públicas y privadas, una puerta de enlace de Internet que conecta el VPC a Internet y una instancia de NAT o de NAT en la subred pública que permita el tráfico de

Internet saliente desde la subred privada. En esta configuración, puede ejecutar Cloud Manager en una subred pública o una subred privada, pero se recomienda la subred pública porque permite el acceso de hosts fuera del VPC. A continuación, puede iniciar instancias de Cloud Volumes ONTAP en la subred privada.

> En lugar de un dispositivo NAT, puede utilizar un proxy HTTP para proporcionar conectividad a Internet.

Para obtener más información sobre este escenario, consulte "Documentación de AWS: Escenario 2: VPC con subredes públicas y privadas (NAT)".

En el siguiente gráfico se muestra la ejecución de Cloud Manager en una subred pública y sistemas de solo nodos que se ejecutan en una subred privada:



Un VPC con una subred privada y una conexión VPN a la red

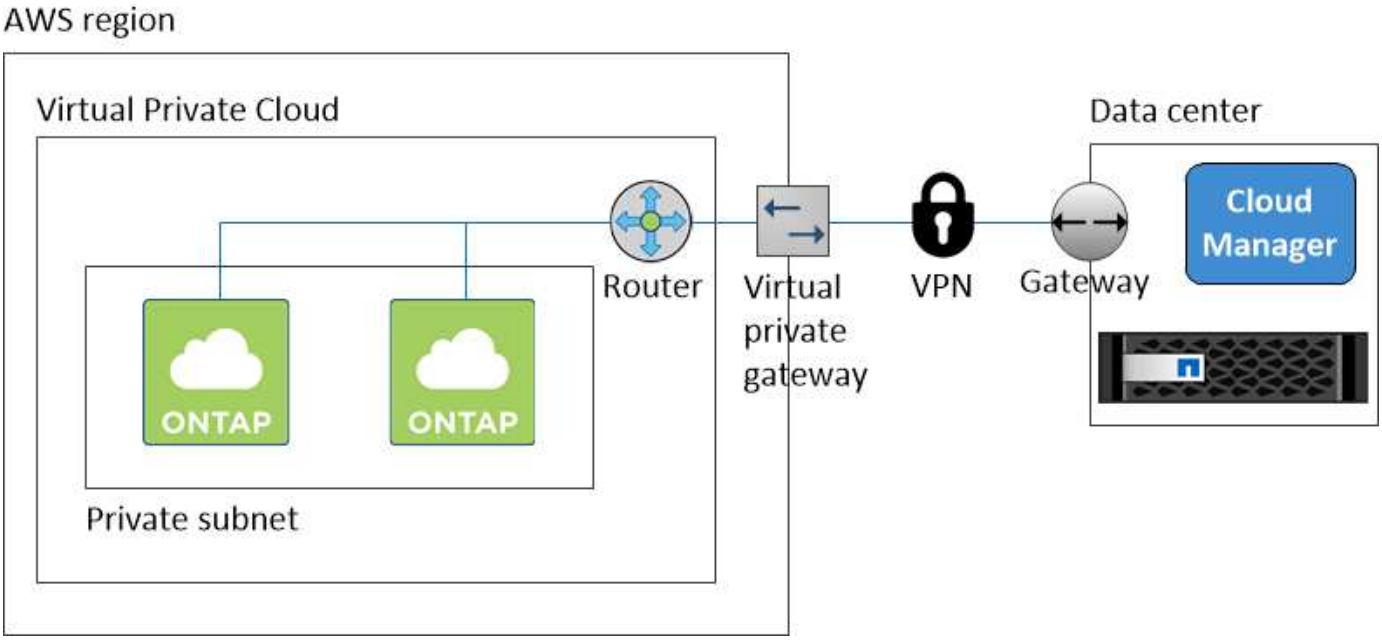
Esta configuración de VPC es una configuración de cloud híbrido en la que Cloud Volumes ONTAP se convierte en una extensión del entorno privado. La configuración incluye una subred privada y una puerta de enlace privada virtual con una conexión VPN a la red. El enrutamiento a través del túnel VPN permite que las instancias EC2 accedan a Internet a través de la red y los firewalls. Puede ejecutar Cloud Manager en la subred privada o en su centro de datos. A continuación, debe iniciar Cloud Volumes ONTAP en la subred privada.

> También puede utilizar un servidor proxy en esta configuración para permitir el acceso a Internet. El servidor proxy puede estar en su centro de datos o en AWS.

Si desea replicar datos entre los sistemas FAS de su centro de datos y los sistemas Cloud Volumes ONTAP de AWS, debe utilizar una conexión VPN para que el enlace sea seguro.

Para obtener más información sobre este escenario, consulte "Documentación de AWS: Escenario 4: VPC con solo una subred privada y acceso de VPN gestionado de AWS".

El siguiente gráfico muestra la ejecución de Cloud Manager en su centro de datos y los sistemas de un solo nodo que se ejecutan en una subred privada:



Configuración de una puerta de enlace de tránsito de AWS para parejas de alta disponibilidad en AZs múltiples

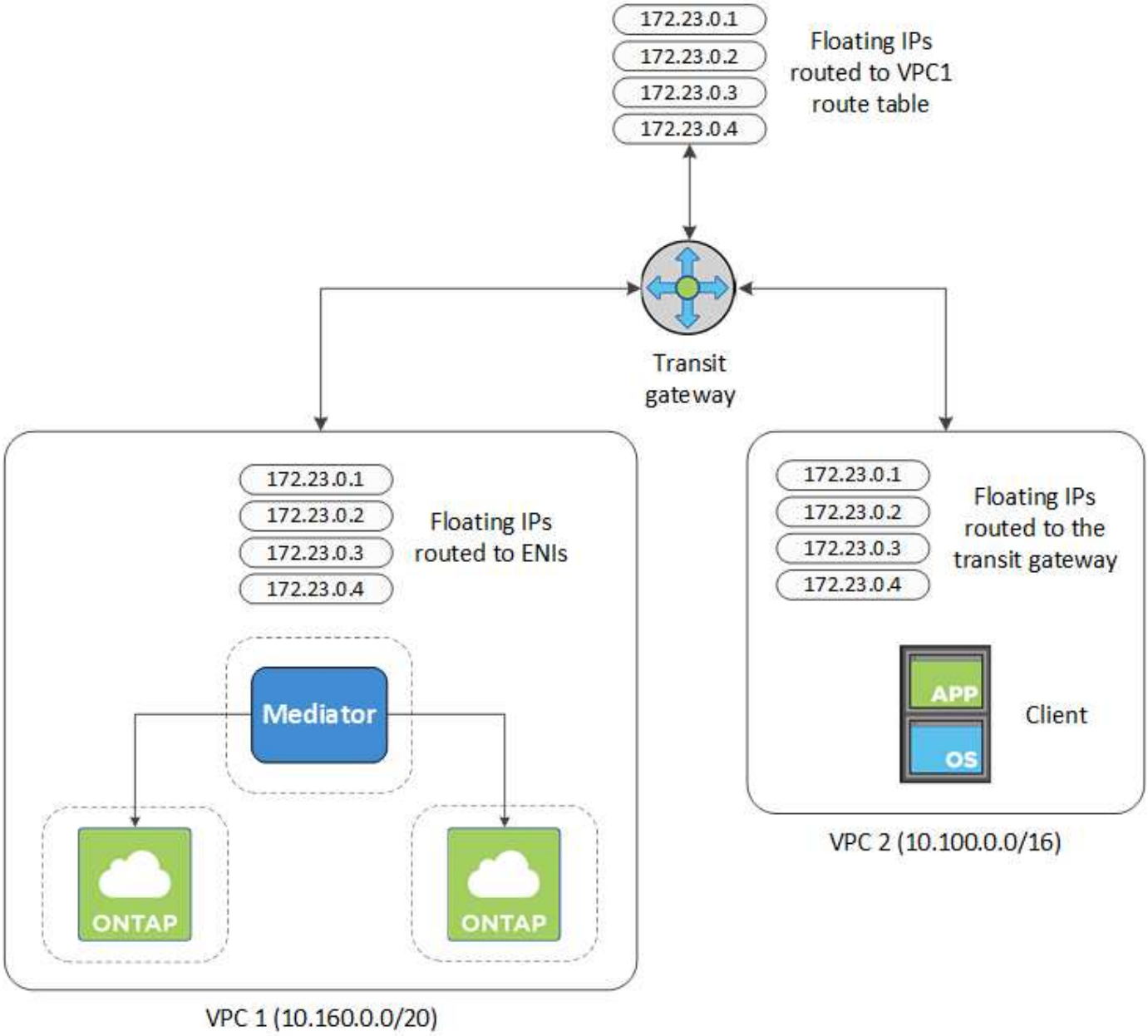
Configure una puerta de enlace de tránsito de AWS para permitir el acceso a las direcciones IP flotantes de un par de alta disponibilidad desde fuera del VPC donde reside el par de alta disponibilidad.

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.

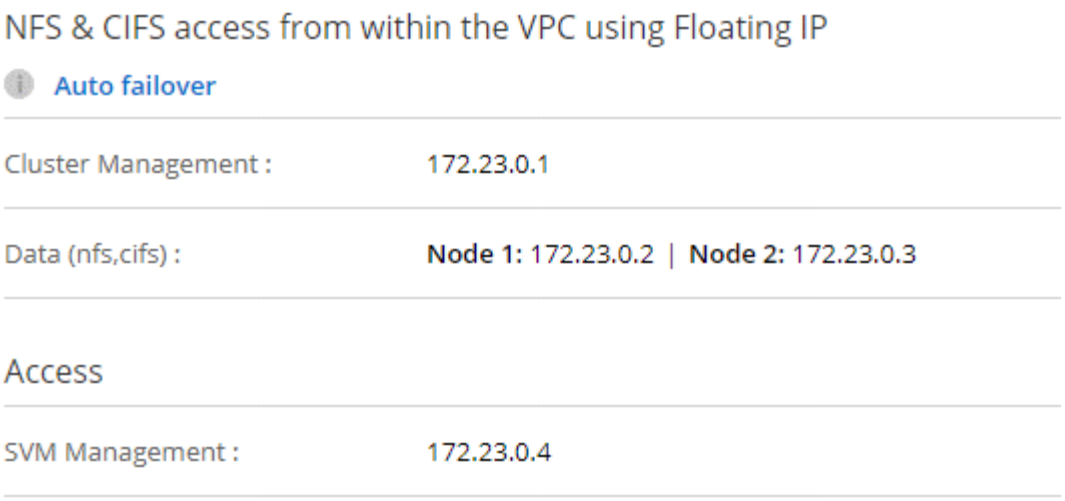


Los siguientes pasos ilustran cómo configurar una configuración similar.

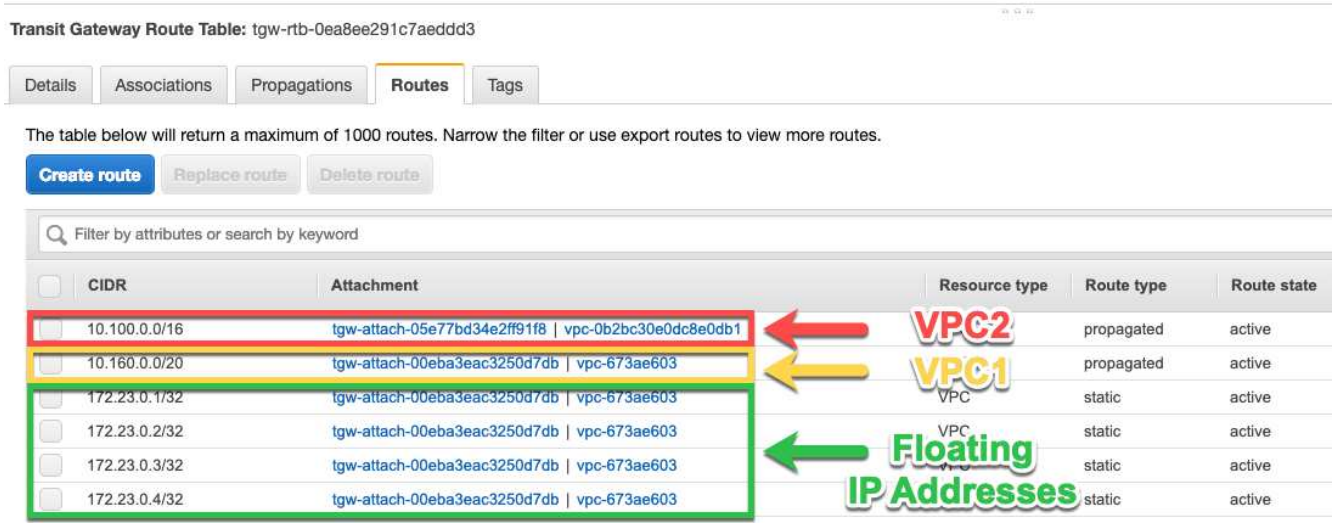
Pasos

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.

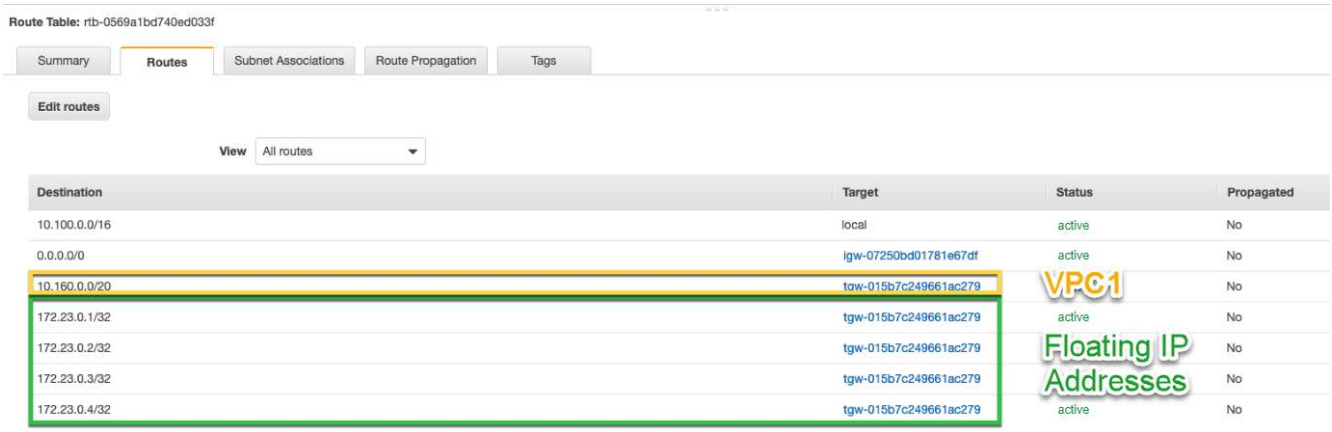


3. Modifique la tabla de rutas de las VPC que necesitan acceder a las direcciones IP flotantes.

   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.

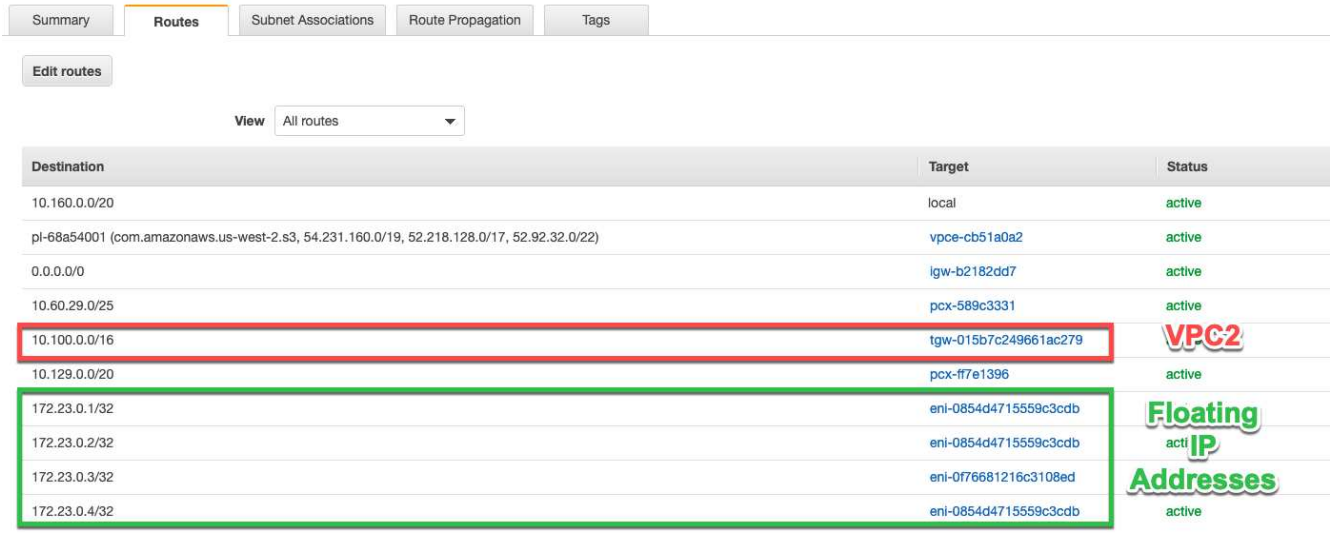
      La siguiente imagen de ejemplo muestra la tabla de rutas para VPC 2, que incluye las rutas hasta VPC 1 y las direcciones IP flotantes.



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.

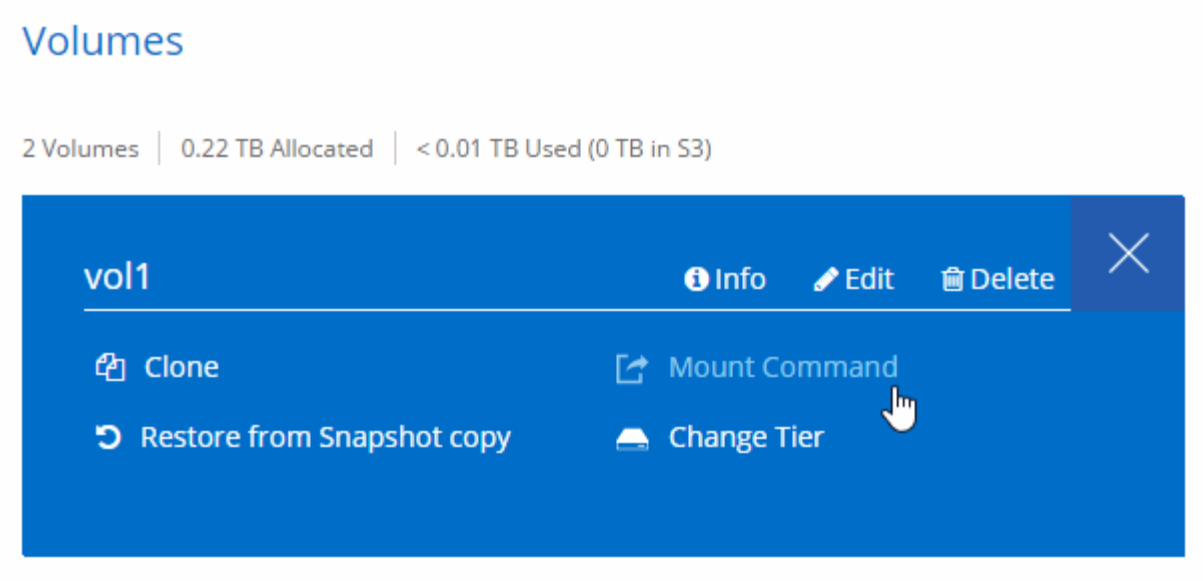
   Este paso es importante porque completa el enrutamiento entre las VPC.

   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"

Requisitos de red para Cloud Volumes ONTAP en Azure

Configure sus redes de Azure para que los sistemas Cloud Volumes ONTAP funcionen correctamente.

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

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".

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 de red para Cloud Volumes ONTAP en GCP

Configure sus redes de Google Cloud Platform para que los sistemas Cloud Volumes ONTAP puedan funcionar correctamente.

VPC compartido

Cloud Manager y Cloud Volumes ONTAP son compatibles con un VPC compartido de Google Cloud Platform.

Un VPC compartido permite configurar y gestionar de forma centralizada las redes virtuales de varios proyectos. Puede configurar redes VPC compartidas en el *host project* e implementar las instancias de máquina virtual de Cloud Manager y Cloud Volumes ONTAP en un *service project*. "Documentación de Google Cloud: Información general sobre VPC compartido".

El único requisito es proporcionar los siguientes permisos a la cuenta de servicio de Cloud Manager en el proyecto de host del VPC compartido:

compute.firewalls.* compute.networks.* compute.subredes.*

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

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 "Reglas de firewall para GCP".

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".

Opciones adicionales de puesta en marcha

Requisitos del host de Cloud Manager

Si instala Cloud Manager en su propio host, debe verificar la compatibilidad con su configuración, que incluye requisitos del sistema operativo, de puertos, etc.

Puede instalar Cloud Manager en su propio host en GCP, pero no en la red local. Cloud Manager debe instalarse en GCP para poder poner en marcha Cloud Volumes ONTAP en GCP.

Se requiere un host dedicado

Cloud Manager no es compatible con un host que se comparte con otras aplicaciones. El host debe ser un host dedicado.

Tipos de instancia de AWS EC2 admitidos

- t2.medium
- t3.medium (recomendado)
- m4.grande
- m5.xlarge
- m5,2xgrande
- m5.4xgrande
- m5.8xlarge

Tamaños de máquina virtual de Azure admitidos

A2, D2 v2 o D2 v3 (según disponibilidad)

Tipos de máquinas GCP admitidos

Tipo de máquina con al menos 2 vCPU y 4 GB de memoria.

Sistemas operativos compatibles

- CentOS 7.2
- CentOS 7.3
- CentOS 7.4
- CentOS 7.5
- Red Hat Enterprise Linux 7.2
- Red Hat Enterprise Linux 7.3
- Red Hat Enterprise Linux 7.4
- Red Hat Enterprise Linux 7.5

  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 de terceros necesario durante la instalación de Cloud Manager.

  Cloud Manager 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?"^]

CPU

2.27 GHz o superior con dos núcleos

RAM

4 GB

Libere espacio en disco

50 GB

Acceso a Internet de salida

Se requiere acceso saliente a Internet cuando se instala Cloud Manager y cuando se utiliza Cloud Manager para implementar Cloud Volumes ONTAP. Para ver una lista de extremos, consulte "Requisitos de red para Cloud Manager".

Puertos

Deben estar disponibles los siguientes puertos:

- 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

Si otros servicios utilizan estos puertos, se produce un error en la instalación de Cloud Manager.

> Existe un posible conflicto con el puerto 3306. Si otra instancia de MySQL se ejecuta en el host, utiliza el puerto 3306 de manera predeterminada. Debe cambiar el puerto que utiliza la instancia de MySQL existente.

Puede cambiar los puertos HTTP y HTTPS predeterminados al instalar Cloud Manager. No puede cambiar el puerto predeterminado para la base de datos MySQL. Si cambia los puertos HTTP y HTTPS, debe asegurarse de que los usuarios puedan acceder a la consola web de Cloud Manager desde un host remoto:

- Modifique el grupo de seguridad para permitir las conexiones entrantes a través de los puertos.
- Especifique el puerto cuando introduzca la URL en la consola web de Cloud Manager.

Instalar Cloud Manager en un host Linux existente

El método más habitual de poner en marcha Cloud Manager es desde Cloud Central o desde el mercado de un proveedor de cloud. Pero tiene la opción de descargar e instalar el software Cloud Manager en un host Linux existente de su red o en la nube.

> Puede instalar Cloud Manager en su propio host en GCP, pero no en la red local. Cloud Manager debe instalarse en GCP para poder poner en marcha Cloud Volumes ONTAP en GCP.

Antes de empezar

- 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 de terceros necesario durante la instalación de Cloud Manager.
- El instalador de Cloud Manager accede a varias URL durante el proceso de instalación. Debe asegurarse de que se permite el acceso saliente a Internet a esos puntos finales. Consulte "Requisitos de red para Cloud Manager".

Acerca de esta tarea

- No se requieren privilegios de usuario raíz para instalar Cloud Manager.
- Cloud Manager 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. Cloud Manager 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, Cloud Manager se actualiza automáticamente si hay una nueva versión disponible.

Pasos

1. Revisar los requisitos de red:
   - "Requisitos de red para Cloud Manager"
   - "Requisitos de red para Cloud Volumes ONTAP en AWS"
   - "Requisitos de red para Cloud Volumes ONTAP en Azure"
   - "Requisitos de red para Cloud Volumes ONTAP en GCP"
2. Revisar "Requisitos del host de Cloud Manager".
3. Descargue el software desde la "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".

4. Asigne permisos para ejecutar el script.

   ejemplo

   ```
    chmod +x OnCommandCloudManager-V3.7.0.sh
   . Ejecute el script de instalación:
   ```

   ```
   ./OnCommandCloudManager-V3.7.0.sh [silent] [proxy=ipaddress]
   [proxyport=port] [proxyuser=user_name] [proxypwd=password]
   ```

   silent ejecuta la instalación sin solicitar información.

   Se requiere *proxy* si el host de Cloud Manager 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.

5. 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.

   Si cambia los puertos HTTP y HTTPS, debe asegurarse de que los usuarios puedan acceder a la consola web de Cloud Manager desde un host remoto:

   - Modifique el grupo de seguridad para permitir las conexiones entrantes a través de los puertos.
   - Especifique el puerto cuando introduzca la URL en la consola web de Cloud Manager.

     Cloud Manager ya está instalado. Al finalizar la instalación, el servicio Cloud Manager (occm) se

reinicia dos veces si especificó un servidor proxy.

6. Abra un explorador web e introduzca la siguiente URL:

   https://ipaddress:port

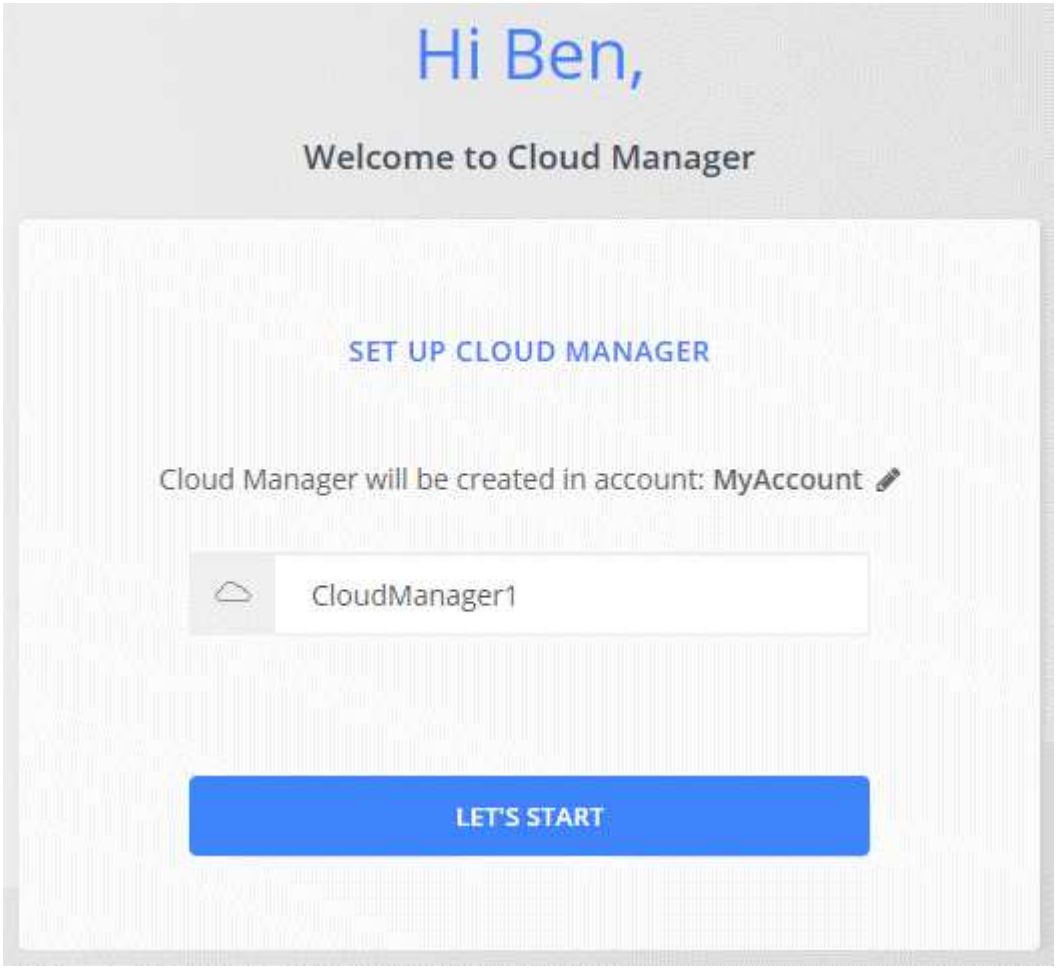
   Ipaddress puede ser localhost, una dirección IP privada o una dirección IP pública, dependiendo de la configuración del host de Cloud Manager. Por ejemplo, si Cloud Manager se encuentra en el cloud público sin una dirección IP pública, debe introducir una dirección IP privada desde un host que tenga una conexión con el host de Cloud Manager.

   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

7. Regístrese en NetApp Cloud Central o inicie sesión.
8. Después de iniciar sesión, configure Cloud Manager:
   a. Especifique la cuenta de Cloud Central que desea asociar con este sistema de Cloud Manager.

      "Obtenga más información acerca de las cuentas de Cloud Central".

   b. Escriba un nombre para el sistema.



Después de terminar

Configure permisos para que Cloud Manager pueda implementar Cloud Volumes ONTAP en su proveedor de cloud:

- 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 de Cloud Manager".
  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.

Ejecute Cloud Manager desde AWS Marketplace

Se recomienda iniciar Cloud Manager en AWS mediante "Cloud Central de NetApp", Pero puede iniciarlo desde el AWS Marketplace, si es necesario.

Si ejecuta Cloud Manager desde AWS Marketplace, Cloud Manager sigue estando integrado con Cloud Central de NetApp. "Obtenga más información sobre la integración".

Acerca de esta tarea

En los siguientes pasos se describe cómo iniciar la instancia desde la consola de 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**.

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:

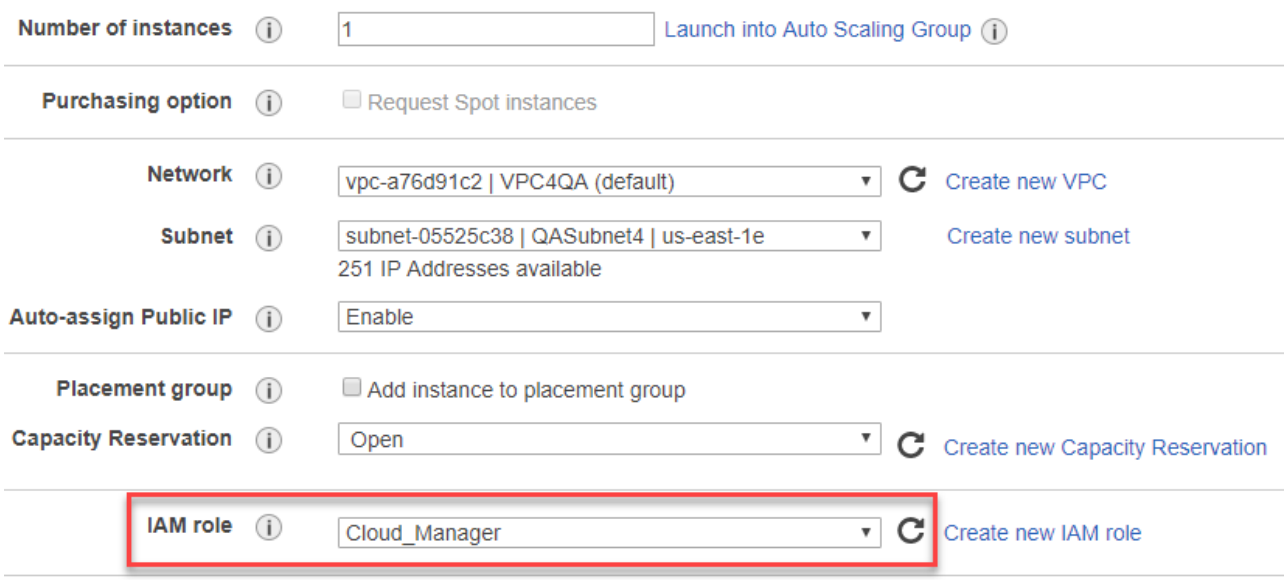
      "NetApp Cloud Manager: Políticas de AWS, Azure y GCP"

   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. "Suscríbase desde el AWS Marketplace" Para garantizar que no se interrumpe el servicio una vez que finaliza la prueba gratuita de Cloud Volumes ONTAP. 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.
3. Ahora vaya a la "Cloud Manager en el mercado de AWS" Para poner en marcha Cloud Manager desde una AMI.
4. En la página Marketplace, haga clic en **continuar a Suscribirse** y luego haga clic en **continuar a Configuración**.
5. Cambie cualquiera de las opciones predeterminadas y haga clic en **continuar a Iniciar**.
6. En **elegir acción**, seleccione **Iniciar a través de EC2** y, a continuación, haga clic en **Iniciar**.

7. 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.medium).

     "Revise la lista de tipos de instancia admitidos".

   - **Configurar instancia**: Seleccione un VPC y una subred, la función IAM que creó en el paso 1 y otras opciones de configuración que cumplan 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 Cloud Manager: 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 de Cloud Manager deben ejecutarse en aproximadamente cinco minutos.

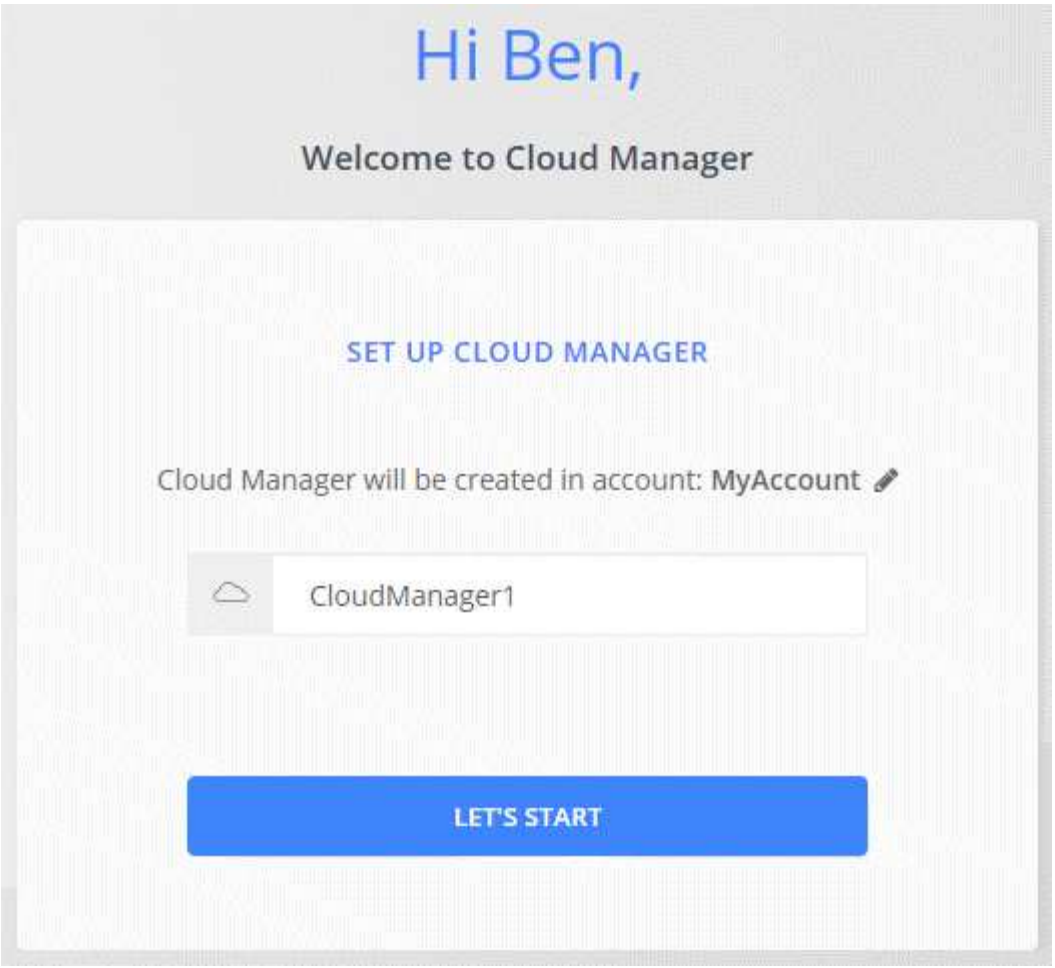
8. Abra un explorador web desde un host que tenga una conexión con la máquina virtual de Cloud Manager e introduzca la siguiente URL:

   http://ipaddress:80

9. Después de iniciar sesión, configure Cloud Manager:
   a. Especifique la cuenta de Cloud Central que desea asociar con este sistema de Cloud Manager.

      "Obtenga más información acerca de las cuentas de Cloud Central".

   b. Escriba un nombre para el sistema.



Resultado

Cloud Manager ya está instalado y configurado.

Ponga en marcha Cloud Manager desde Azure Marketplace

Se recomienda poner en marcha Cloud Manager en Azure con "Cloud Central de NetApp", Pero puede implementarlo desde Azure Marketplace, si es necesario.

Hay disponibles instrucciones adicionales para implementar Cloud Manager en "Regiones gubernamentales de Azure EE. UU" y en "Regiones de Azure Alemania".

Si pone en marcha Cloud Manager desde Azure Marketplace, Cloud Manager sigue estando integrado con Cloud Central de NetApp. "Obtenga más información sobre la integración".

Implementar Cloud Manager en Azure

Es necesario instalar y configurar Cloud Manager para que pueda usarlo para ejecutar Cloud Volumes ONTAP en Azure.

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 uno de los tamaños de máquina virtual recomendados: A2, D2 v2 o D2 v3 (según disponibilidad).
   - Para el grupo de seguridad de red, Cloud Manager requiere conexiones entrantes mediante SSH, HTTP y HTTPS.

     "Obtenga más información sobre las reglas de los grupos de seguridad para Cloud Manager".

   - En **Administración**, active **identidad administrada asignada por el sistema** para Cloud Manager seleccionando **On**.

     Esta configuración es importante porque una identidad gestionada permite que la máquina virtual de Cloud Manager se identifique a sí misma en Azure Active Directory sin necesidad de 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. La máquina virtual y el software Cloud Manager deben ejecutarse en aproximadamente cinco minutos.

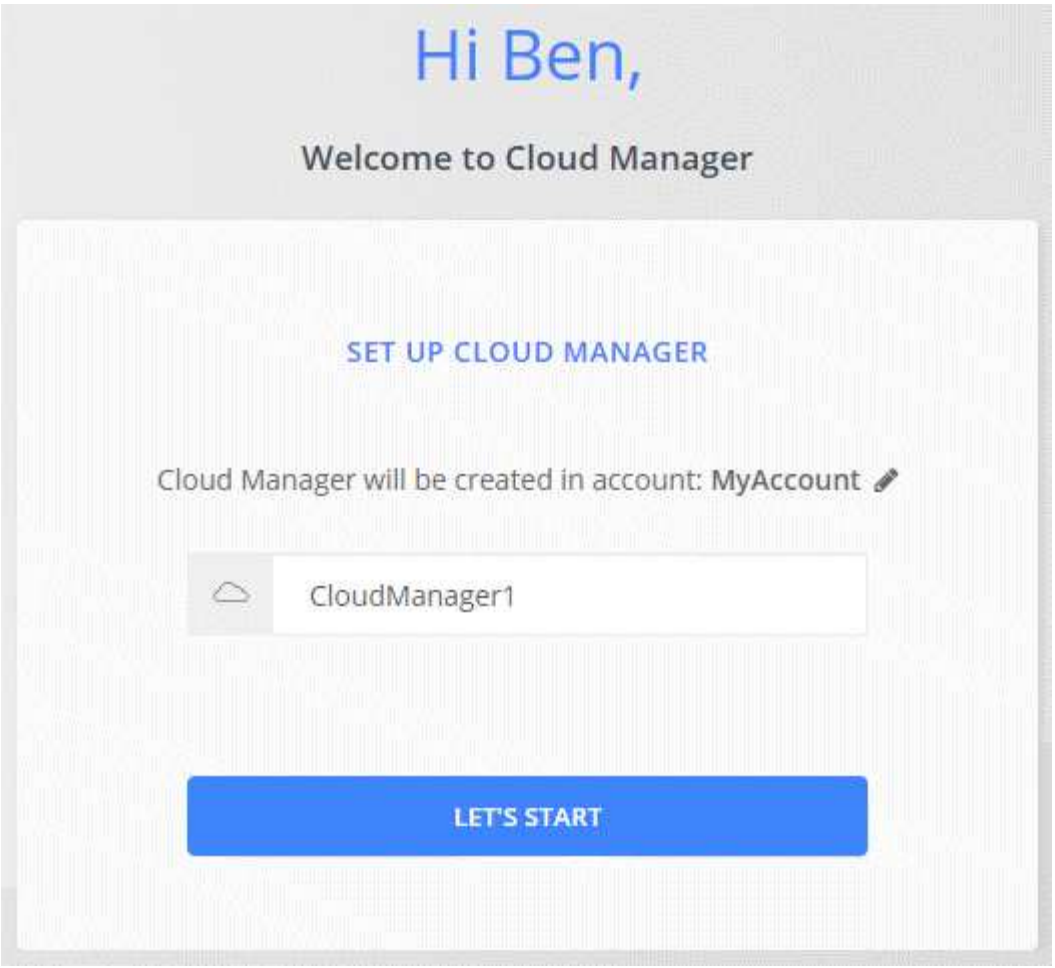
5. Abra un explorador web desde un host que tenga una conexión con la máquina virtual de Cloud Manager e introduzca la siguiente URL:

   http://ipaddress:80

6. Después de iniciar sesión, configure Cloud Manager:
   a. Especifique la cuenta de Cloud Central que desea asociar con este sistema de Cloud Manager.

      "Obtenga más información acerca de las cuentas de Cloud Central".

   b. Escriba un nombre para el sistema.



Resultado

Cloud Manager ya está instalado y configurado. Debe conceder permisos de Azure para que los usuarios puedan poner en marcha Cloud Volumes ONTAP en Azure.

Otorgando permisos de Azure a Cloud Manager

Al implementar Cloud Manager en Azure, debe haber habilitado un "identidad administrada asignada por el sistema". Ahora debe conceder los permisos de Azure necesarios creando un rol personalizado y, a continuación, asignando el rol a la máquina virtual de Cloud Manager 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_3.7.4.json

Ahora debe tener un rol personalizado llamado operador de Cloud Manager de OnCommand que puede asignar a la máquina virtual de Cloud Manager.

2. Asigne el rol a la máquina virtual de Cloud Manager 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 de OnCommand**.

        El nombre predeterminado que se proporciona en la es el operador de OnCommand Cloud Manager "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 de Cloud Manager.
      - Seleccione la máquina virtual Cloud Manager.
      - Haga clic en **Guardar**.
   d. Si desea implementar Cloud Volumes ONTAP desde suscripciones adicionales, cambie a esa suscripción y repita estos pasos.

Resultado

Cloud Manager ahora tiene los permisos que se necesitan para poner en marcha y gestionar Cloud Volumes ONTAP en Azure.

Implementar Cloud Manager en una región gubernamental de Azure Estados Unidos

Para tener Cloud Manager en una región gubernamental de Estados Unidos, ponga en marcha Cloud Manager desde Azure Government Marketplace. A continuación, proporcione los permisos que necesita Cloud Manager para implementar y gestionar sistemas Cloud Volumes ONTAP.

Para obtener una lista de las regiones gubernamentales de EE. UU. De Azure admitidas, consulte "Regiones globales de Cloud Volumes".

Ponga en marcha Cloud Manager desde Azure US Government Marketplace

Cloud Manager está disponible como imagen en el mercado gubernamental de Azure de Estados Unidos.

Pasos

1. Compruebe que Azure Government Marketplace esté habilitado en su suscripción:

a. Inicie sesión en el portal como administrador de empresa.
b. Vaya a **Administrar**.
c. En **Detalles de inscripción**, haga clic en el icono de lápiz junto a **Azure Marketplace**.
d. Seleccione **Activado**.
e. Haga clic en **Guardar**.

"Documentación de Microsoft Azure: Azure Government Marketplace"

2. Busque Cloud Manager de OnCommand en el portal gubernamental de Azure Estados Unidos.
3. 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.
- Debe elegir uno de los tamaños de máquina virtual recomendados: A2, D2 v2 o D2 v3 (según disponibilidad).
- Para el grupo de seguridad de red, es mejor elegir **Avanzado**.

  La opción **Avanzado** crea un nuevo grupo de seguridad que incluye las reglas entrantes necesarias para Cloud Manager. Si selecciona básico, consulte "Reglas de grupo de seguridad" para ver la lista de reglas requeridas.

4. En la página de resumen, revise sus selecciones y haga clic en **Crear** para iniciar la implementación.

Azure implementa la máquina virtual con los ajustes especificados. La máquina virtual y el software Cloud Manager deben ejecutarse en aproximadamente cinco minutos.

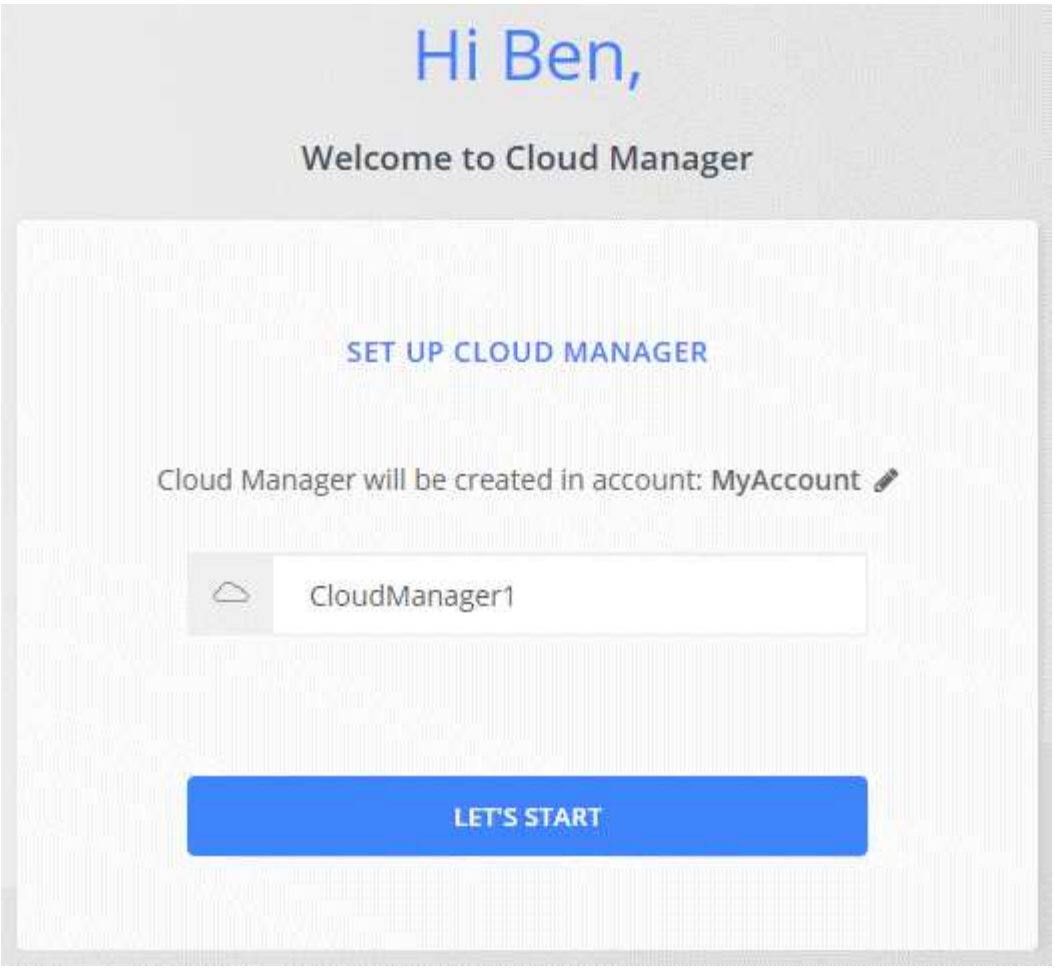
5. Abra un explorador web desde un host que tenga una conexión con la máquina virtual de Cloud Manager e introduzca la siguiente URL:

http://ipaddress:80

6. Después de iniciar sesión, configure Cloud Manager:
   a. Especifique la cuenta de Cloud Central que desea asociar con este sistema de Cloud Manager.

      "Obtenga más información acerca de las cuentas de Cloud Central".

   b. Escriba un nombre para el sistema.



Resultado

Cloud Manager ya 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 a Cloud Manager mediante una identidad gestionada

La forma más sencilla de proporcionar permisos consiste en habilitar un "identidad administrada" En la máquina virtual de Cloud Manager, y luego asignando los permisos necesarios a la máquina virtual. Si se prefiere, una forma alternativa es a. "Conceda permisos de Azure con un director de servicio".

Pasos

1. Habilite una identidad administrada en la máquina virtual de Cloud Manager:
   a. Desplácese a la máquina virtual de Cloud Manager y seleccione **identidad**.
   b. En **sistema asignado**, haga clic en **On** y, a continuación, en **Guardar**.
2. 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_3.7.4.json

Ahora debe tener un rol personalizado llamado operador de Cloud Manager de OnCommand que puede asignar a la máquina virtual de Cloud Manager.

3. Asigne el rol a la máquina virtual de Cloud Manager 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**, haga clic en **Agregar asignación de rol** y, a continuación, agregue los permisos:
      - Seleccione el rol **operador de Cloud Manager de OnCommand**.

        El nombre predeterminado que se proporciona en la es el operador de OnCommand Cloud Manager "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 de Cloud Manager.
      - Escriba el nombre de la máquina virtual y, a continuación, selecciónelo.
      - Haga clic en **Guardar**.
   d. Si desea implementar Cloud Volumes ONTAP desde suscripciones adicionales, cambie a esa suscripción y repita estos pasos.

Resultado

Cloud Manager ahora tiene los permisos que se necesitan para poner en marcha y gestionar Cloud Volumes ONTAP en Azure.

Instalando Cloud Manager en una región de Azure Alemania

Azure Marketplace no está disponible en las regiones de Azure Alemania, por lo que debe descargar el instalador de Cloud Manager del sitio de soporte de NetApp e instalarlo en un host Linux existente en la región.

Pasos

1. "Revise los requisitos de red para Azure".
2. "Revise los requisitos del host de Cloud Manager".
3. "Descargue e instale Cloud Manager".
4. "Conceda permisos de Azure a Cloud Manager con un director de servicio".

Después de terminar

Cloud Manager ya está listo para poner en marcha Cloud Volumes ONTAP en la región de Azure Alemania, como en cualquier otra región. Sin embargo, es posible que desee realizar primero la configuración adicional.

Mantener Cloud Manager en funcionamiento

Cloud Manager debe seguir ejecutándose en todo momento.

Cloud Manager es un componente clave en el estado y la facturación de Cloud Volumes ONTAP. Si Cloud Manager se apaga, los sistemas Cloud Volumes ONTAP se apagarán tras perder la comunicación con Cloud Manager durante más de 4 días.

Ponga en marcha Cloud Volumes ONTAP

Antes de crear sistemas Cloud Volumes ONTAP

Antes de usar Cloud Manager para crear y gestionar sistemas Cloud Volumes ONTAP, su administrador de Cloud Manager debe haber preparado una red, instalar y configurar Cloud Manager.

Antes de iniciar la implementación de Cloud Volumes ONTAP, deben existir las siguientes condiciones:

- Se cumplieron los requisitos de red de Cloud Manager y Cloud Volumes ONTAP.
- Cloud Manager cuenta con permisos para realizar operaciones en el proveedor de cloud que elija.
- Para AWS, está suscrito a la página correspondiente de AWS Marketplace:
  - Si desea implementar un sistema PAYGO o activar una función complementaria: "La página Cloud Manager (para Cloud Volumes ONTAP)".
  - Si desea poner en marcha un sistema con su propia licencia: "El único nodo o la página de alta disponibilidad en el AWS Marketplace".
- Se instaló Cloud Manager.

Enlaces relacionados

- "Introducción a AWS"
- "Introducción a Azure"
- "Introducción a GCP"
- "Configurar Cloud Manager"

Inicio de sesión en Cloud Manager

Puede iniciar sesión en Cloud Manager desde cualquier explorador web que tenga conexión con el sistema Cloud Manager. Debe iniciar sesión mediante un "Cloud Central de NetApp" cuenta de usuario.

Pasos

1. Abra un explorador web e inicie sesión en "Cloud Central de NetApp".

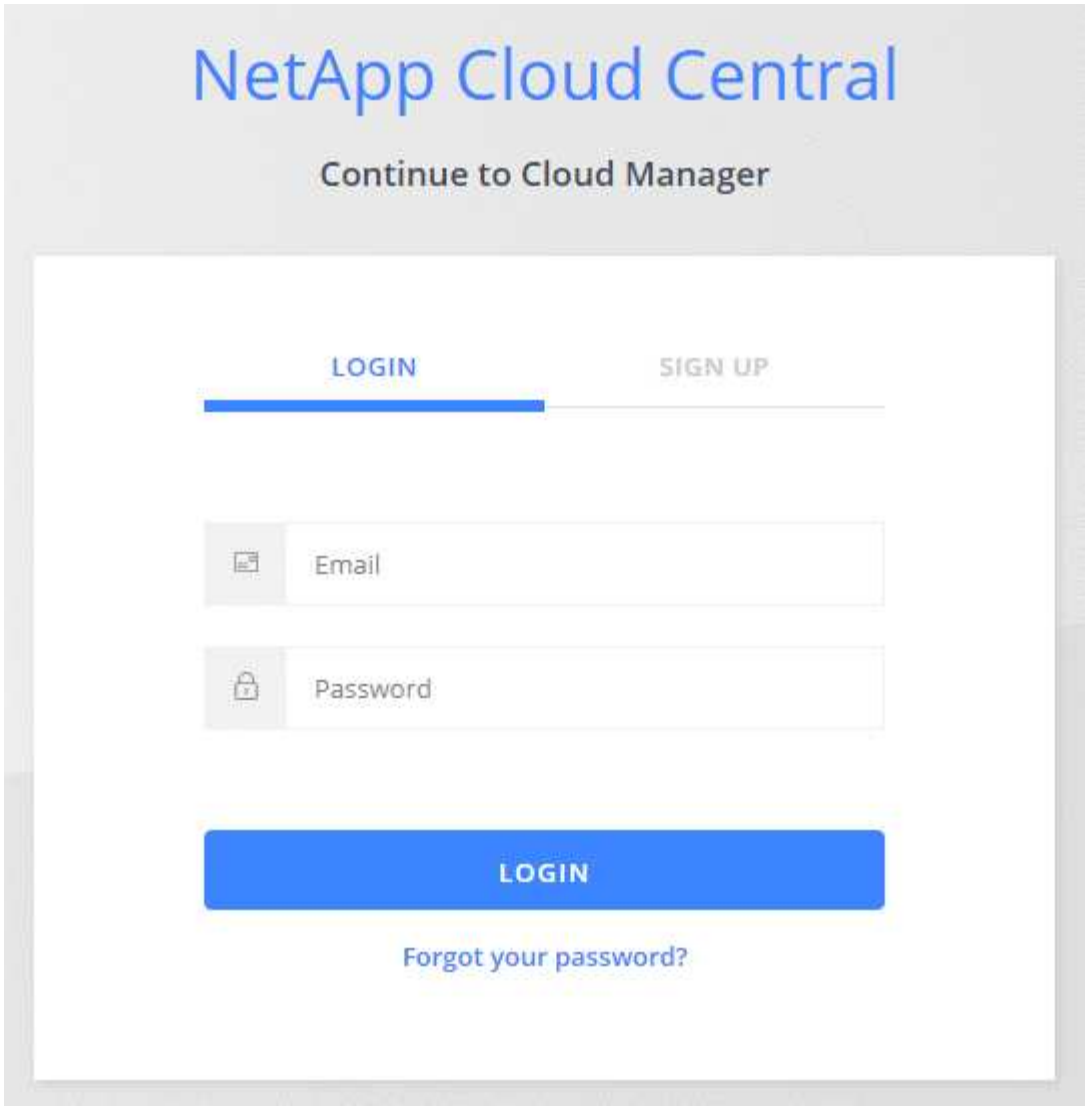
   Este paso le dirigirá automáticamente a la vista de estructura. Si no lo hace, haga clic en **Fabric View**.

2. Seleccione el sistema Cloud Manager al que desea acceder.

   Si no ve ningún sistema en la lista, asegúrese de que el administrador de cuentas le haya añadido a la cuenta de Cloud Central asociada con el sistema Cloud Manager.

3. Inicie sesión en Cloud Manager con sus credenciales de Cloud Central de NetApp.



Planificación de la configuración de Cloud Volumes ONTAP

Al poner en marcha Cloud Volumes ONTAP, 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"
- "Configuraciones compatibles para Cloud Volumes ONTAP 9.7 en Azure"
- "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 AWS"
- "Límites de almacenamiento para Cloud Volumes ONTAP 9.7 en Azure"
- "Límites de almacenamiento para Cloud Volumes ONTAP 9.7 en GCP"

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.

Planificación de AWS

Planifique la implementación de Cloud Volumes ONTAP en AWS ajustando el tamaño del sistema y revisando la información de red necesaria para acceder.

- Ajuste de tamaño de su sistema en AWS
- Hoja de trabajo de información de red de 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*

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	

Información de AWS	Su valor
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	

Planificación de Azure

Planifique la implementación de Cloud Volumes ONTAP en Azure mediante la configuración de su sistema y la revisión de la información de red que debe introducir.

- Ajuste de tamaño de su sistema en Azure
- Hoja de trabajo de información de red de 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: Introducción a Microsoft Azure Storage".

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"

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)	

Planificación para GCP

Planifique la implementación de Cloud Volumes ONTAP en Google Cloud Platform ajustando el tamaño de su sistema y revisando la información de red a la que debe acceder.

- Ajuste de tamaño de su sistema en GCP
- Hoja de trabajo de información de red para 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)	

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.

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

Activación de Flash Cache en Cloud Volumes ONTAP

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 efectivo para cargas de trabajo de lectura intensiva aleatoria, como bases de datos, correo electrónico y servicios de archivos.

Limitaciones

- La compresión debe deshabilitarse en todos los volúmenes para aprovechar las mejoras de rendimiento de Flash Cache.
- Cloud Volumes ONTAP no admite el recalentamiento de la caché después de un reinicio.

Habilitación de Flash Cache en Cloud Volumes ONTAP en AWS

Flash Cache es compatible con Cloud Volumes ONTAP Premium y BYOL en AWS.

Pasos

1. 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
   - r5d.2xgrande
2. Deshabilite la compresión 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".

Activación de Flash Cache en Cloud Volumes ONTAP en Azure

Flash Cache es compatible con Cloud Volumes ONTAP BYOL en sistemas de un solo nodo.

Pasos

1. Seleccione el tipo de máquina virtual Standard_L8S_v2 con un sistema BYOL de Cloud Volumes ONTAP de un solo nodo en Azure.
2. Deshabilite la compresión 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".

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.

Suscribirse desde AWS Marketplace

Suscríbase al mercado de AWS y pague por Cloud Volumes ONTAP según lo vaya o ponga en marcha su modelo BYOL de Cloud Volumes ONTAP.

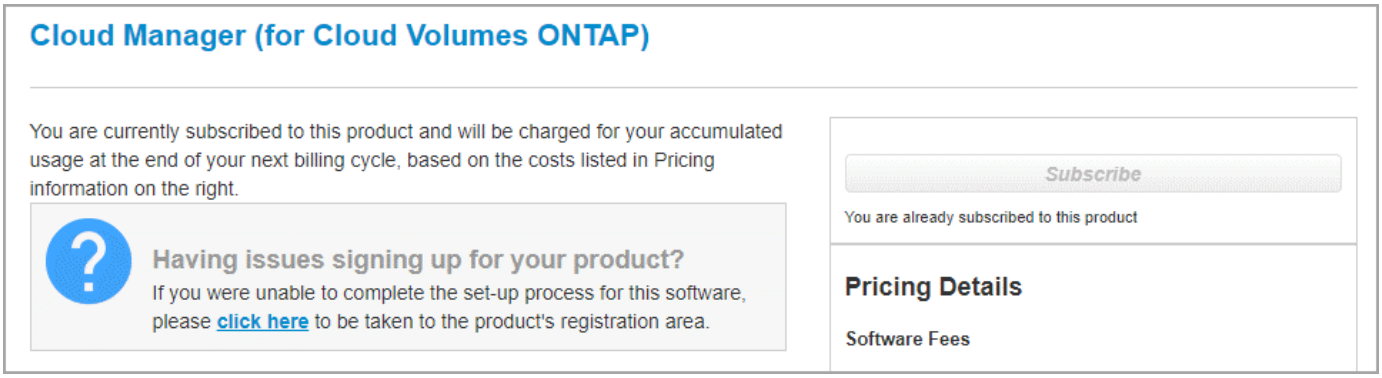
Suscripción a PAYGO

"Suscríbase desde el AWS Marketplace" Para garantizar que no se interrumpe el servicio una vez que finaliza la prueba gratuita de Cloud Volumes ONTAP. 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.

El siguiente vídeo muestra el proceso de suscripción:

► https://docs.netapp.com/es-es/occm37//media/video_subscribing_aws.mp4 *(video)*

Si varios usuarios de IAM trabajan en la misma cuenta de AWS, cada usuario debe suscribirse. Después de que el primer usuario se haya suscrito, AWS muestra a los usuarios posteriores que ya están suscritos, tal como se muestra en la siguiente imagen. Mientras se dispone de una suscripción para la cuenta de AWS, cada usuario de IAM debe asociarse a la 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.



Suscripción a BYOL

Si inicia Cloud Volumes ONTAP con su propia licencia (BYOL), "Después, tendrá que suscribirse a esta oferta en AWS Marketplace".

"Obtenga más información sobre cada página de AWS Marketplace".

Lanzar un único sistema Cloud Volumes ONTAP en AWS

Si desea iniciar Cloud Volumes ONTAP en AWS, tiene que crear un nuevo entorno de trabajo en Cloud Manager.

Antes de empezar

- 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 **Crear Cloud Volumes ONTAP** y siga las indicaciones.
2. **Defina su entorno de trabajo**: Seleccione **Servicios Web de Amazon** y **Cloud Volumes ONTAP**.
3. **Detalles y credenciales**: Si lo desea, puede cambiar la suscripción a la cuenta de AWS y a la plataforma,

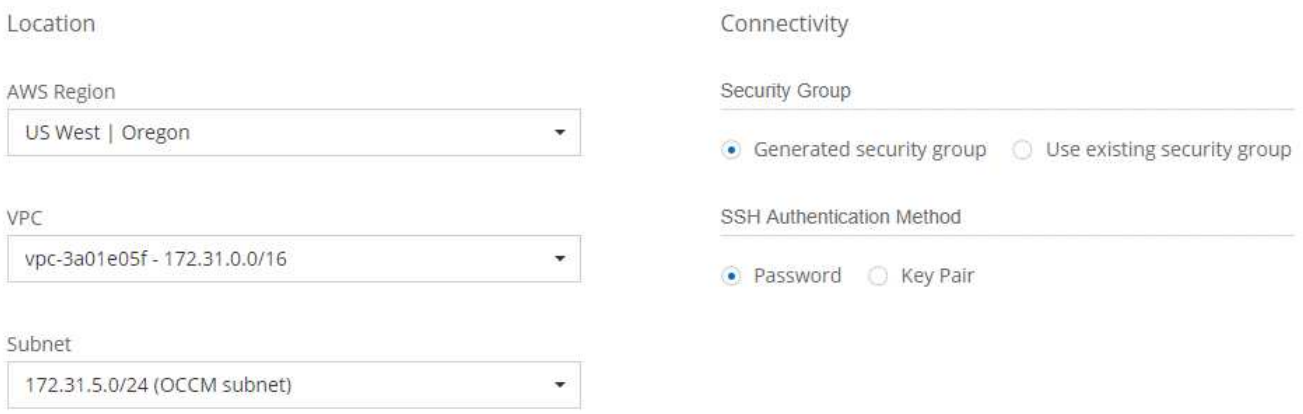
introducir un nombre de entorno de trabajo, añadir etiquetas, si es necesario y, a continuación, introducir una contraseña.

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
Cuenta	Puede elegir una cuenta diferente si lo desea "Se añadieron cuentas de AWS adicionales a Cloud Manager".
Suscripción a Marketplace	Seleccione una suscripción diferente si desea cambiar la cuenta de AWS a partir de la cual se le cobra. Para añadir una nueva suscripción, "Acceda a la oferta en el AWS Marketplace".
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".
Credenciales	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.

4. **Servicios**: Mantenga activados o desactive los servicios individuales que no desea utilizar con este sistema Cloud Volumes ONTAP.
   - "Más información acerca de Backup en S3".
   - "Más información sobre Cloud Compliance".
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 9.4 RC1 y 9.4 GA está disponible. La actualización no se produce de una versión a otra; por ejemplo, de 9.3 a 9.4.

11. **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 S3.

    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".

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.

    "Más información sobre la velocidad de escritura".

    "Más información acerca del almacenamiento WORM".

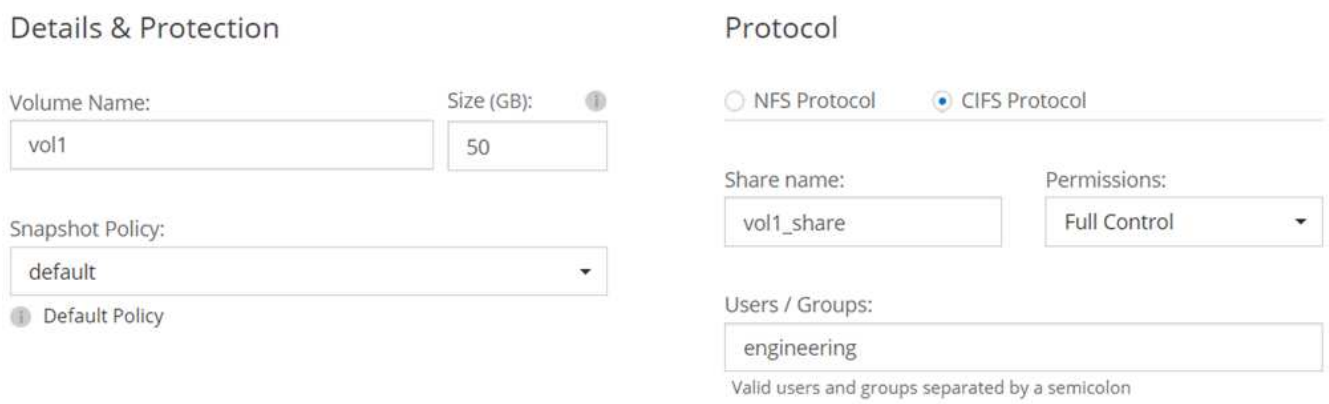
13. **Crear volumen**: Introduzca los detalles del nuevo volumen o haga clic en **Omitir**.

    Este paso se puede omitir si desea crear un volumen para iSCSI. Cloud Manager configura volúmenes solo para NFS y CIFS.

    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.

    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 habilitar las funciones de eficiencia del almacenamiento y editar la política de organización en niveles de S3, 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

- 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".

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 **Crear Cloud Volumes ONTAP** y siga las indicaciones.
2. **Defina su entorno de trabajo**: Seleccione **Servicios Web de Amazon** y **Cloud Volumes ONTAP ha**.
3. **Detalles y credenciales**: Si lo desea, puede cambiar la suscripción a la cuenta de AWS y a la plataforma,

introducir un nombre de entorno de trabajo, añadir etiquetas, si es necesario 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:

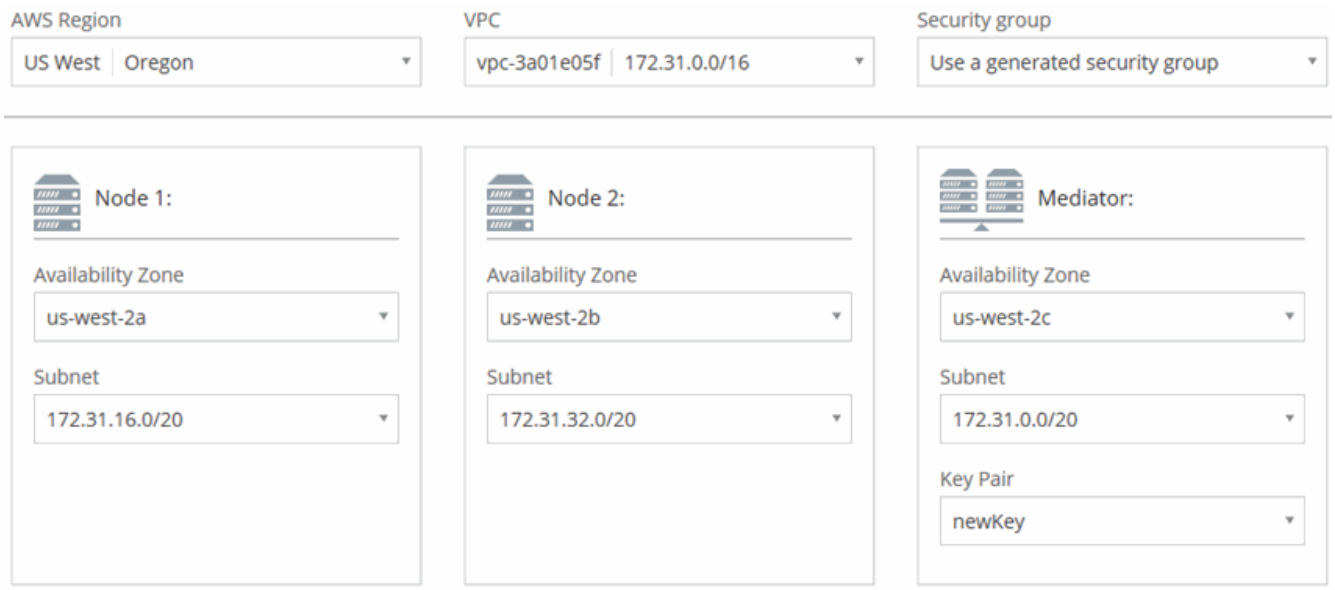
Campo	Descripción
Cuenta	Puede elegir una cuenta diferente si lo desea "Se añadieron cuentas de AWS adicionales a Cloud Manager".
Suscripción a Marketplace	Seleccione una suscripción diferente si desea cambiar la cuenta de AWS a partir de la cual se le cobra. Para añadir una nueva suscripción, "Acceda a la oferta en el AWS Marketplace".
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".
Credenciales	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.

4. **Servicios**: Mantenga activados o desactive los servicios individuales que no desea utilizar con este sistema Cloud Volumes ONTAP.
   - "Más información acerca de Backup en S3".
   - "Más información sobre Cloud Compliance".
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 9.4 RC1 y 9.4 GA está disponible. La actualización no se produce de una versión a otra; por ejemplo, de 9.3 a 9.4.

15. **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 S3.

    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".

16. **WORM**: Active el almacenamiento de escritura única y lectura múltiple (WORM), si lo desea.

    "Más información acerca del almacenamiento WORM".

17. **Crear volumen**: Introduzca los detalles del nuevo volumen o haga clic en **Omitir**.

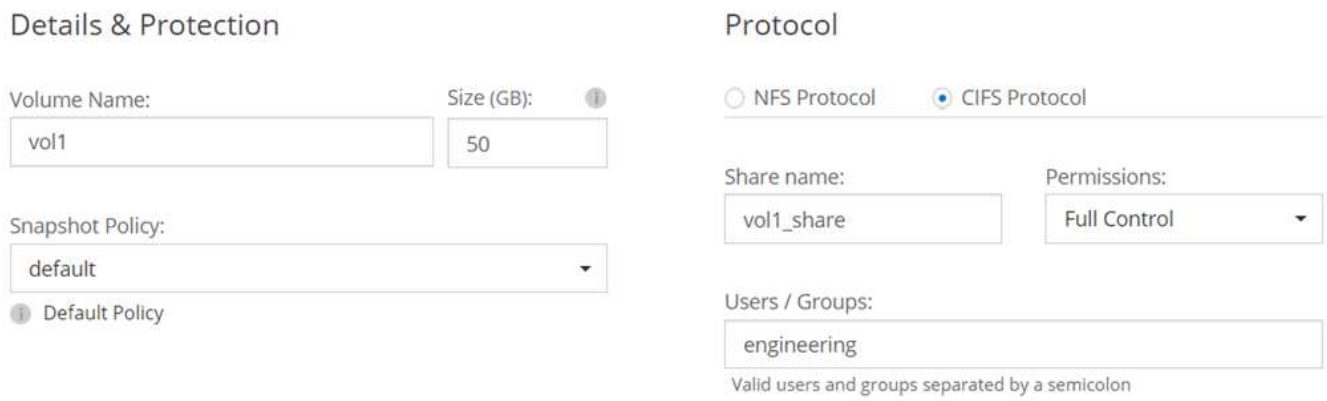
    Este paso se puede omitir si desea crear un volumen para iSCSI. Cloud Manager configura volúmenes solo para NFS y CIFS.

    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.

Campo	Descripción
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.

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.

Campo	Descripción
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 habilitar las funciones de eficiencia del almacenamiento y editar la política de organización en niveles de S3, 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.

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

- Asegúrese de que su cuenta de Azure tenga los permisos necesarios, especialmente si actualizó desde una versión anterior y está implementando por primera vez un sistema de alta disponibilidad.

  Los permisos más recientes se encuentran en la "Política Cloud Central de NetApp para Azure".

- 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.

Pasos

1. En la página entornos de trabajo, haga clic en **Crear Cloud Volumes ONTAP** y siga las indicaciones.
2. **Defina su entorno de trabajo**: Seleccione **Microsoft Azure** y, a continuación, elija un solo nodo o par de alta disponibilidad.
3. **Detalles y credenciales**: De forma opcional, cambie la cuenta o 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
Cambiar cuenta	Si lo desea, puede elegir una cuenta o suscripción diferente "Configúrelas y los añada a Cloud Manager".
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.
Nombre del grupo de recursos	Si desactiva **Use Default**, puede introducir el nombre de un nuevo grupo de recursos. Si desea utilizar un grupo de recursos existente, debe usar la API.
Etiquetas	Las etiquetas son metadatos para sus recursos de Azure. Cloud Manager agrega las etiquetas al sistema Cloud Volumes ONTAP y cada recurso de Azure asociado con el sistema. 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".
Credenciales	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.

4. **Servicios**: Mantenga activado el cumplimiento de la nube o inactívelo si no desea utilizarlo con este sistema Cloud Volumes ONTAP.

   "Más información sobre Cloud Compliance".

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 9.5 RC1 y 9.5 GA está disponible. La actualización no se produce de una versión a otra; por ejemplo, de 9.4 a 9.5.

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.

    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".

11. **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".

"Más información acerca del almacenamiento WORM".

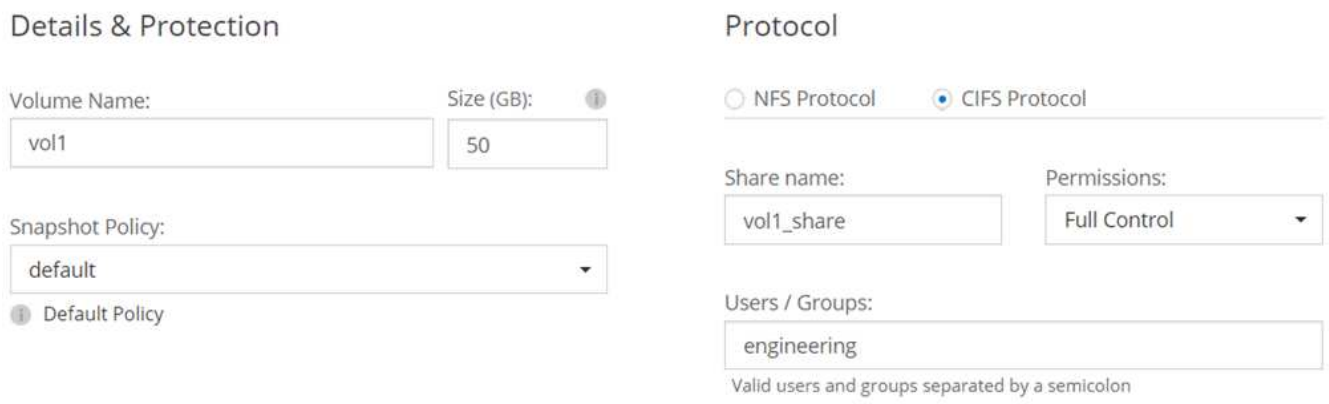
12. **Crear volumen**: Introduzca los detalles del nuevo volumen o haga clic en **Omitir**.

    Debe omitir este paso si desea usar iSCSI. Cloud Manager le permite crear volúmenes solo para NFS y CIFS.

    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.

    En la siguiente imagen, se muestra la página volumen rellenada para el protocolo CIFS:



13. **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. 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.

14. **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, 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".

15. **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.

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.

Antes de empezar

- 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.

Pasos

1. en la página entornos de trabajo, haga clic en **Crear Cloud Volumes ONTAP** y siga las indicaciones.
2. **Defina su entorno de trabajo**: Haga clic en **continuar**.
3. **Suscribirse a Cloud Volumes ONTAP**: Si se le solicita, suscríbase a Cloud Volumes ONTAP en el mercado de GCP.

   El siguiente vídeo muestra el proceso de suscripción:

   ► https://docs.netapp.com/es-es/occm37//media/video_subscribing_gcp.mp4 *(video)*

4. **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
Proyecto de Google Cloud	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 4b en esta página".

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".
Credenciales	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.

5. **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".

6. **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".

7. **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.

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 9.5 RC1 y 9.5 GA está disponible. La actualización no se produce de una versión a otra; por ejemplo, de 9.4 a 9.5.

9. **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.

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".

10. **escribir velocidad y GUSANO**: Elija **velocidad de escritura normal** o **Alta**, y active el almacenamiento de escritura única, lectura múltiple (WORM), si lo desea.

    "Más información sobre la velocidad de escritura".

    "Más información acerca del almacenamiento WORM".

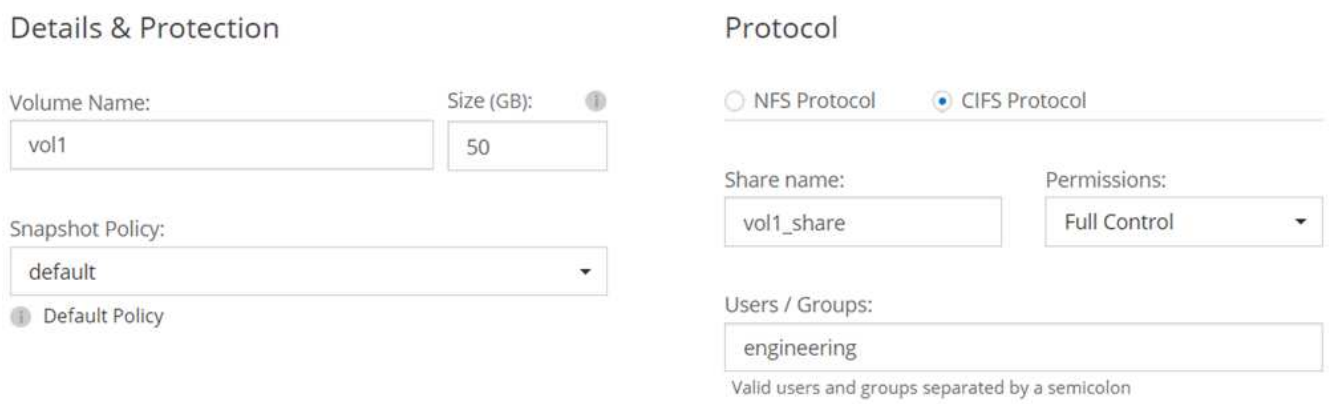
11. **Crear volumen**: Introduzca los detalles del nuevo volumen o haga clic en **Omitir**.

    Debe omitir este paso si desea usar iSCSI. Cloud Manager le permite crear volúmenes solo para NFS y CIFS.

    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.

    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.
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, 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. **Cuenta de Google Cloud Platform para la organización en niveles de datos**: Configure la organización en niveles de los datos proporcionando claves de acceso al almacenamiento interoperable para una cuenta de Google Cloud Platform. Haga clic en **Omitir** para desactivar la organización en niveles de datos.

    Las claves permiten a Cloud Manager configurar un bucket de almacenamiento en cloud para la

organización de datos en niveles. Para obtener información detallada, consulte "Configuración y adición de cuentas de GCP a Cloud Manager".

15. **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.

Registro de sistemas de pago por uso

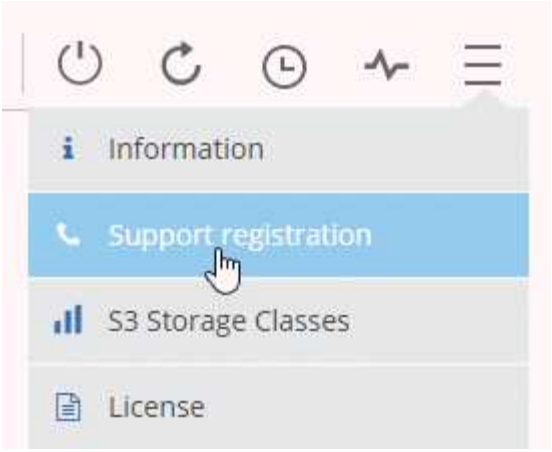
El soporte de NetApp se incluye en los sistemas Explore, estándar y Premium de Cloud Volumes ONTAP, pero primero debe activar el soporte registrando los sistemas en NetApp.

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**:



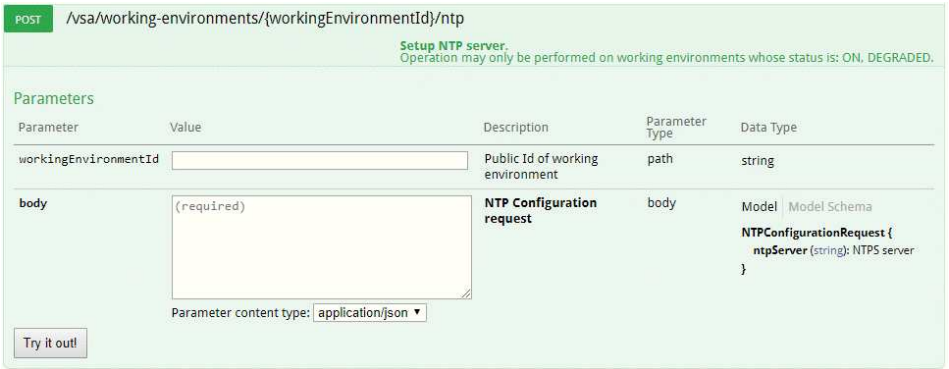
4. Seleccione una cuenta en la página de soporte de NetApp y haga clic en **Register**.

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: 

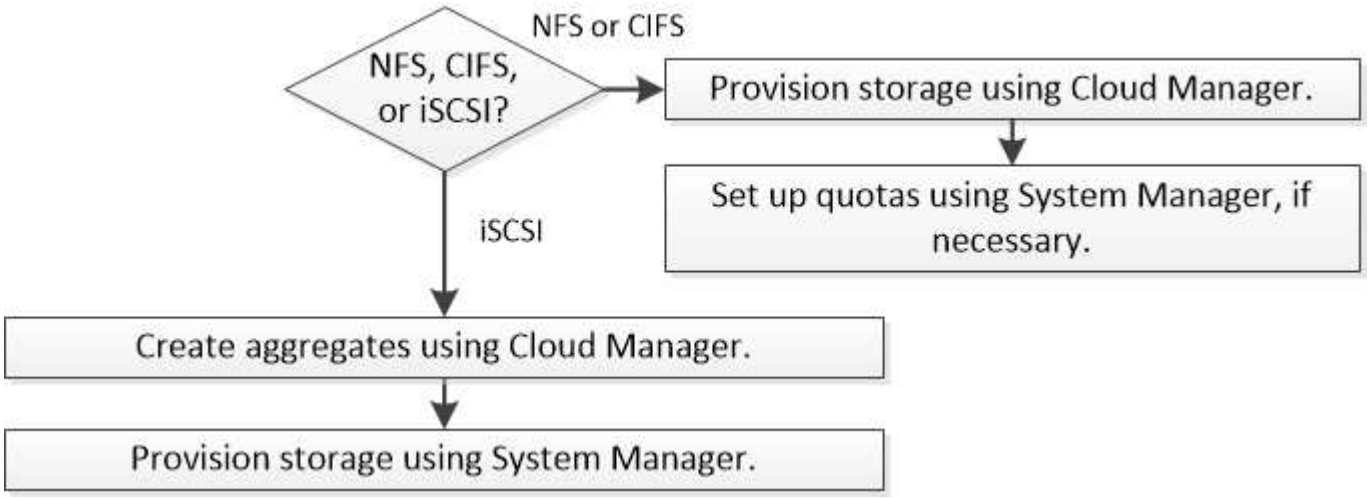
Tarea	Descripción
Opcional: Configure AutoSupport	AutoSupport supervisa de manera proactiva el estado del sistema y envía automáticamente mensajes al soporte técnico de NetApp de forma predeterminada. Si el administrador de cuentas agregó un servidor proxy a Cloud Manager antes de iniciar la instancia, 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 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".
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 backup de los archivos en el host de Cloud Manager 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".

Aprovisionar almacenamiento

Aprovisionar almacenamiento

Puede aprovisionar almacenamiento NFS y CIFS adicional para sus sistemas Cloud Volumes ONTAP desde Cloud Manager gestionando volúmenes y agregados. Si necesita crear almacenamiento iSCSI, debe hacerlo desde System Manager.

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 de FlexVol para NFS o CIFS desde Cloud Manager.

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**.

Acción	Pasos
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.
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.

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.

Campo	Descripción
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. • 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**.

Aprovisionar LUN de iSCSI

Si desea crear LUN iSCSI, debe hacerlo desde System Manager.

Antes de empezar

- Las utilidades de host deben estar instaladas y configuradas en los hosts que se conectan a la LUN.
- Debe haber registrado el nombre del iniciador de iSCSI del host. Debe proporcionar este nombre cuando cree un igroup para la LUN.

- Antes de crear volúmenes en System Manager, debe asegurarse de contar con un agregado con espacio suficiente. Debe crear agregados en Cloud Manager. Para obtener más información, consulte "Creación de agregados".

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".
2. Haga clic en **almacenamiento > LUN**.
3. Haga clic en **Crear** y siga las indicaciones para crear la LUN.
4. Conéctese al LUN desde sus hosts.

   Para ver instrucciones, consulte "Documentación de utilidades de host" para su sistema operativo.

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.

Organización en niveles de los datos inactivos en almacenamiento de objetos de bajo coste

Puede reducir los costes de almacenamiento 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 añadir una cuenta de GCP a Cloud Manager y configurar la subred para Google Private Access. 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

- Para añadir una cuenta de Google Cloud Platform a Cloud Manager, debe introducir claves de acceso al almacenamiento para una cuenta de servicio. Las claves permiten a Cloud Manager configurar un bucket de almacenamiento en cloud para la organización de datos en niveles. Para ver instrucciones, consulte "Configuración y adición de cuentas de GCP a Cloud Manager".
- 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".

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

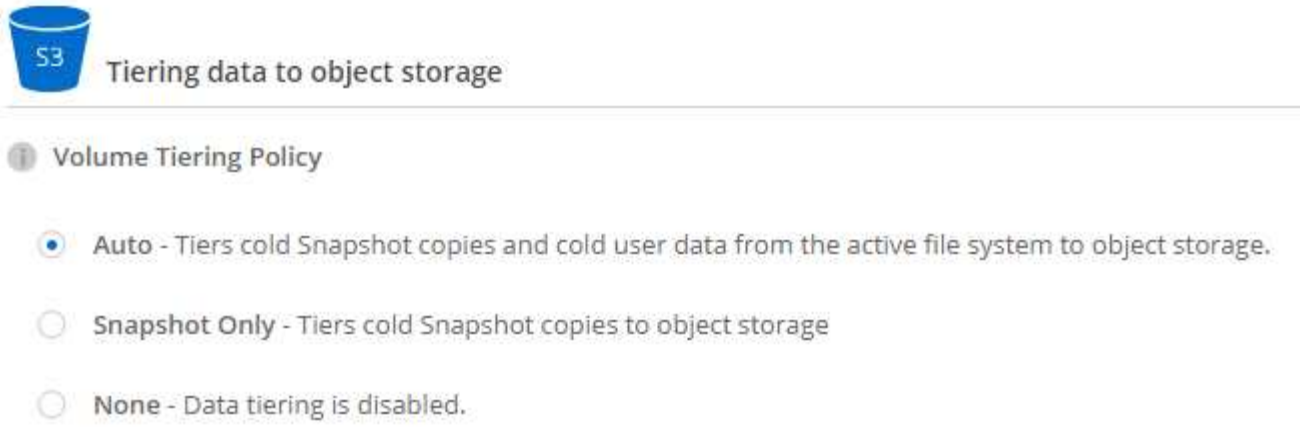
1. En el entorno de trabajo, cree un volumen nuevo o cambie el nivel de un volumen existente:

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 la política de solo Snapshot o la política de Auto.

   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.

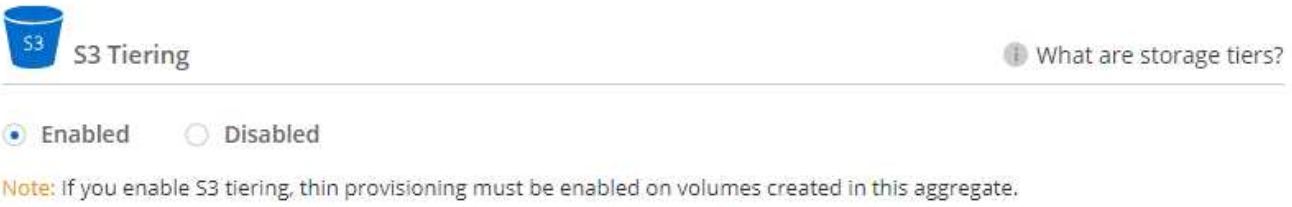
Organización en niveles de los datos de los volúmenes de protección de datos

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".

Cambiar el nivel de organización en niveles en AWS o Azure

Al habilitar la organización en niveles de los datos, Cloud Volumes ONTAP organiza los datos inactivos en la clase de almacenamiento S3 *Standard* en AWS o en el nivel de almacenamiento *hot* en Azure. Después de poner en marcha Cloud Volumes ONTAP, puede reducir sus costes de almacenamiento cambiando el nivel de organización en niveles para los datos inactivos a los que no se ha accedido durante 30 días. Los costes de acceso son más elevados si accede a los datos, por lo que debe tener en cuenta antes de cambiar el nivel de

organización en niveles.

> No se puede cambiar el nivel de organización en niveles en GCP porque solo se admite la clase de almacenamiento *Regional* en este momento.

Acerca de esta tarea

El nivel de organización en niveles no se corresponde con todo el sistema, aunque it no es por volumen.

En AWS, puede cambiar el nivel de organización en niveles para que los datos inactivos se muevan a una de las siguientes clases de almacenamiento después de 30 días de inactividad:

- Organización en niveles inteligente
- Acceso Estándar-poco frecuente
- Una Zona de acceso poco frecuente

En Azure, puede cambiar el nivel de organización en niveles para que los datos inactivos se muevan al nivel de almacenamiento *COOL* tras 30 días de inactividad.

Para obtener más información acerca del funcionamiento de los niveles de organización en niveles, 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 **S3 Storage Classes** o **almacenamiento BLOB Storage Tiering**.
2. Elija el nivel de organización en niveles y, a continuación, haga clic en **Guardar**.

Use ONTAP como almacenamiento persistente para Kubernetes

Cloud Manager puede automatizar la puesta en marcha de "Trident de NetApp" En los clústeres de Kubernetes, puede usar ONTAP como almacenamiento persistente para contenedores. Esto funciona con clústeres Cloud Volumes ONTAP y ONTAP en las instalaciones.

Antes de completar estos pasos, debe hacerlo "Cree un sistema Cloud Volumes ONTAP" o. "Detectar un clúster de ONTAP en las instalaciones" De Cloud Manager.

Si se implementan clústeres de Kubernetes mediante el "Servicio Kubernetes de NetApp", Cloud Manager puede detectar automáticamente los clústeres desde la cuenta de Cloud Central de NetApp. Si ese es el caso, omita los dos primeros pasos y comience con el paso 3.

1 Verifique la conectividad de red

1. Debe haber una conexión de red entre Cloud Manager y los clústeres de Kubernetes, y desde los clústeres de Kubernetes a los sistemas ONTAP.
2. Cloud Manager necesita una conexión a Internet de salida para acceder a los siguientes extremos al instalar Trident:

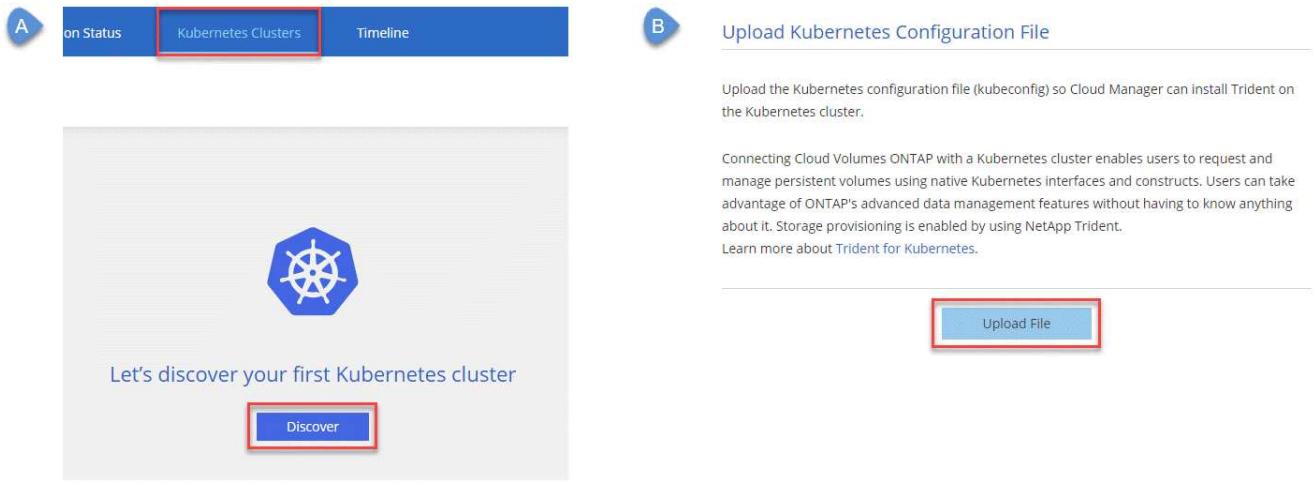
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/

Cloud Manager instala Trident en un clúster de Kubernetes cuando se conecta un entorno de trabajo al clúster.

Cargue los archivos de configuración de Kubernetes en Cloud Manager

Para cada clúster de Kubernetes, el administrador de cuentas debe cargar un archivo de configuración (kubeconfig) que tenga el formato YAML. Después de cargar el archivo, Cloud Manager verifica la conectividad al clúster y guarda una copia cifrada del archivo kubeconfig.

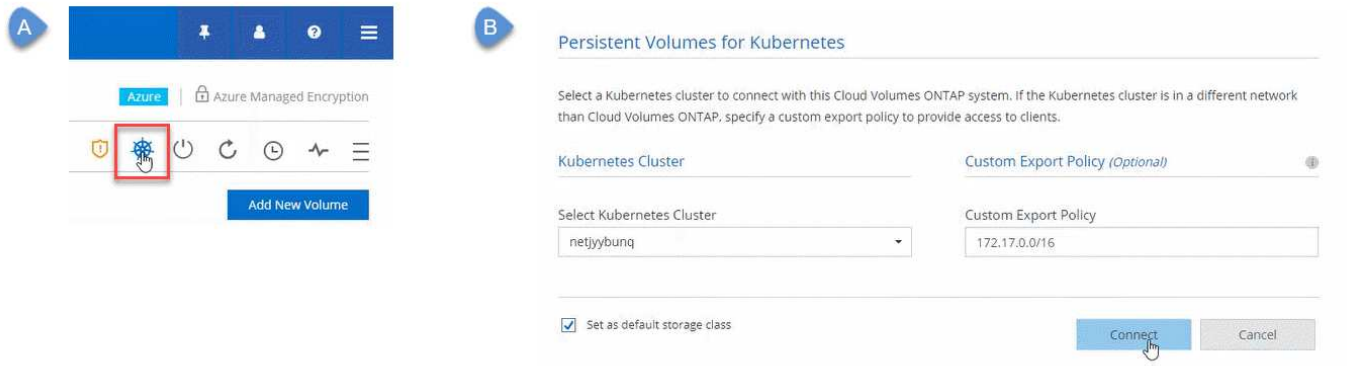
Haga clic en **Kubernetes Clusters > Discover > Upload File** y seleccione el archivo kubeconfig.



Conecte sus entornos de trabajo a los clústeres de Kubernetes

En el entorno de trabajo, haga clic en el icono Kubernetes y siga las indicaciones. Puede conectar distintos clústeres en diferentes sistemas de ONTAP y varios clústeres en el mismo sistema ONTAP.

Puede definir la clase de almacenamiento de NetApp como la clase de almacenamiento predeterminada para el clúster de Kubernetes. Cuando un usuario crea un volumen persistente, el clúster de Kubernetes puede utilizar sistemas ONTAP conectados de forma predeterminada como almacenamiento back-end.



Inicie el aprovisionamiento de volúmenes persistentes

Solicite y gestione volúmenes persistentes mediante construcciones e interfaces de Kubernetes nativas. Cloud Manager crea cuatro clases de almacenamiento Kubernetes que se pueden usar cuando se aprovisionan volúmenes persistentes:

- **netapp-file**: Para vincular volúmenes persistentes a sistemas ONTAP de un solo nodo
- **netapp-File-san**: Para vincular volúmenes persistentes iSCSI a sistemas ONTAP de un solo nodo
- **netapp-file-redundante**: Para vincular volúmenes persistentes a pares de alta disponibilidad ONTAP
- **netapp-File-redundante-san**: Para vincular volúmenes persistentes iSCSI a pares de alta disponibilidad ONTAP

Cloud Manager configura Trident para que utilice las siguientes opciones de aprovisionamiento de forma predeterminada:

- Volúmenes finos
- La política de Snapshot predeterminada
- Directorio Snapshot accesible

"Más información sobre el aprovisionamiento de su primer volumen con Trident para Kubernetes"

¿Cuáles son los volúmenes trident_trident?

Cloud Manager crea un volumen en el primer sistema ONTAP que se conecta a un clúster de Kubernetes. El nombre del volumen se añade con "_trident_trident". ONTAP usa este volumen para conectarse al clúster de Kubernetes. No debe eliminar estos volúmenes.

¿Qué ocurre cuando se desconecta o se quita un clúster de Kubernetes?

Cloud Manager permite desconectar sistemas individuales de ONTAP de un clúster de Kubernetes. Cuando se desconecta un sistema, ya no se puede utilizar ese sistema ONTAP como almacenamiento persistente para contenedores. No se eliminan los volúmenes persistentes existentes.

Después de desconectar todos los sistemas de un clúster de Kubernetes, también puede eliminar toda la configuración de Kubernetes de Cloud Manager. Cloud Manager no desinstala Trident cuando se quita el clúster y no elimina ningún volumen persistente.

Estas dos acciones están disponibles únicamente mediante API. Tenemos previsto añadir las acciones a la interfaz en una futura versión."Haga clic aquí para obtener más información sobre las API".

Cifrar volúmenes con cifrado de volúmenes de NetApp

El cifrado de volúmenes de NetApp (NVE) es una tecnología basada en software para cifrar datos en reposo un volumen por vez. Se cifran datos, copias Snapshot y metadatos. El acceso a los datos se proporciona mediante una clave XTS-AES-256 exclusiva, una por volumen.

Acerca de esta tarea

- 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.

- En este momento, Cloud Volumes ONTAP admite el cifrado de volúmenes de NetApp con un servidor de gestión de claves externo. No se admite un administrador de claves incorporado.
- Debe configurar el cifrado de volúmenes de NetApp desde la interfaz de línea de comandos de ONTAP.

  A continuación, puede usar la interfaz de línea de comandos o System Manager para habilitar el cifrado en volúmenes específicos. Cloud Manager no es compatible con el cifrado de volúmenes de NetApp desde la interfaz de usuario y desde las API de.

"Obtenga más información sobre las tecnologías de cifrado compatibles".

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"

4. Cree un volumen cifrado nuevo o convierta un volumen no cifrado existente mediante la CLI o System Manager.
   - CLI:
     - Para volúmenes nuevos, utilice el comando **volume create** con el parámetro -encrypt.

       "Guía completa de cifrado de NetApp para ONTAP 9: Habilitar el cifrado en un nuevo volumen"

     - Para los volúmenes existentes, utilice el comando **VOLUME Encryption conversion start**.

       "Guía completa de cifrado de NetApp para ONTAP 9: Habilitar el cifrado en un volumen existente con el comando volume Encryption conversion start"

   - System Manager:
     - Para volúmenes nuevos, haga clic en **almacenamiento > volúmenes > Crear > Crear FlexVol** y, a continuación, seleccione **cifrado**.

       "Gestión de clústeres de ONTAP 9 mediante System Manager: Creación de volúmenes de FlexVol"

     - Para los volúmenes existentes, seleccione el volumen, haga clic en **Editar** y, a continuación, seleccione **cifrado**.

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 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.
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**.

Tarea	Acción
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**.
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.
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.
Habilite o deshabilite la sincronización con S3 para un volumen	Seleccione un volumen y, a continuación, haga clic en **Sincronizar a S3** o **Eliminar relación de sincronización**. Para poder usar estas opciones, es necesario habilitar la función Sync to S3. Para ver instrucciones, consulte "Sincronizando datos en AWS S3"
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**.
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.

Tarea	Acción
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.

3. Haga clic en **Guardar**.

Resultado

Cloud Volumes ONTAP actualiza el servidor CIFS con los cambios.

Mover un volumen para evitar problemas de capacidad

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

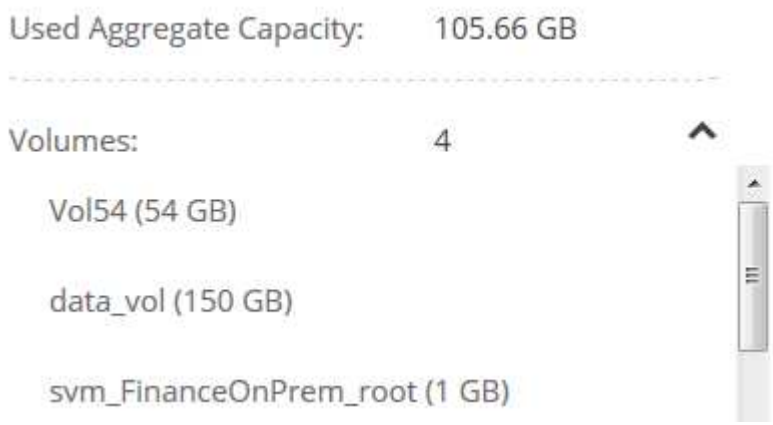
Si Cloud Manager no puede proporcionar recomendaciones para mover un volumen para evitar problemas de capacidad, debe identificar los volúmenes que debe mover y si debe moverlos a otro agregado del mismo sistema o a otro sistema.

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.

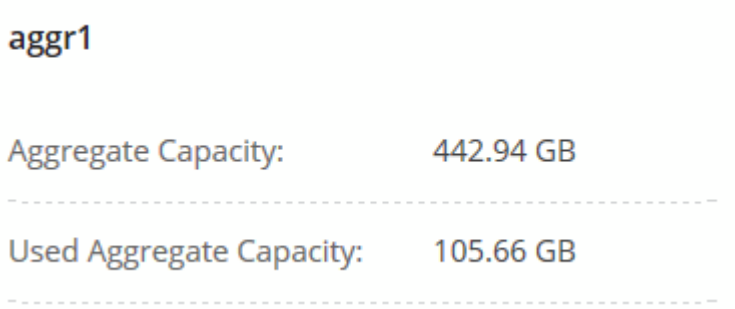
Acerca de esta tarea

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".

Replique y proteja datos

Detectar y gestionar 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. La detección de estos clústeres le permite replicar datos fácilmente en su entorno de cloud híbrido directamente desde Cloud Manager.

Detección de clústeres de ONTAP

Detectar un clúster de ONTAP en Cloud Manager le permite aprovisionar almacenamiento y replicar datos en el cloud híbrido.

Antes de empezar

Debe tener la dirección IP de gestión 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 de Cloud Manager debe permitir el acceso HTTPS de salida a través del puerto 443.

  Si Cloud Manager se encuentra en AWS, 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 modificó esta política predeterminada o si creó su propia política de firewall, debe asociar el protocolo HTTPS con esa política y habilitar el acceso desde el host de Cloud Manager.

Pasos

1. En la página entornos de trabajo, haga clic en **descubrir** y seleccione **clúster ONTAP**.
2. 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.

3. 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 a y desde el clúster, y ejecutar System Manager de OnCommand para realizar tareas avanzadas.

Aprovisionar volúmenes en clústeres de ONTAP

Cloud Manager le permite aprovisionar volúmenes NFS y CIFS en clústeres de ONTAP.

Antes de empezar

Debe configurarse NFS o CIFS en el clúster. Puede configurar NFS y CIFS con System Manager o la CLI.

Acerca de esta tarea

Es posible crear volúmenes en agregados existentes. No se pueden crear agregados nuevos 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.
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.
Perfil de uso	Los perfiles de uso definen las funciones de eficiencia del almacenamiento de NetApp habilitadas para un volumen.
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.

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.

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 10000, 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

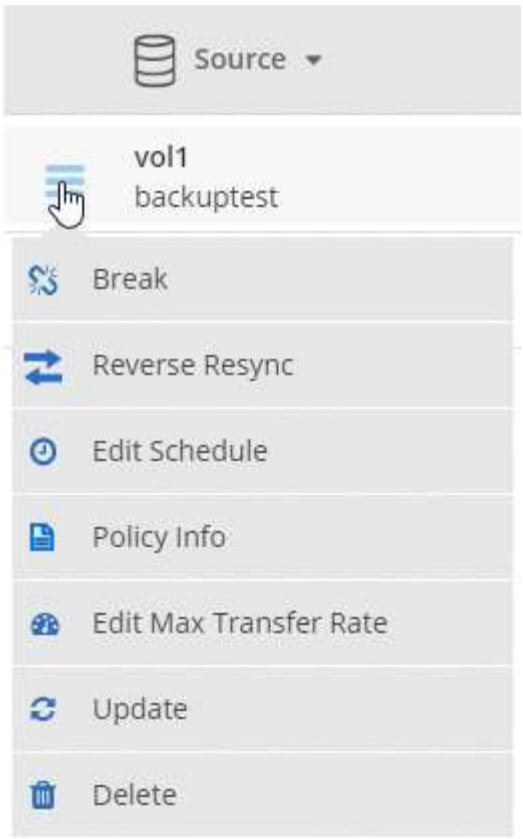
1. En la página entornos de trabajo, consulte el estado de replicación de todos los entornos de trabajo del área de trabajo o de un entorno de trabajo específico:

Opción	Acción
Todos los entornos de trabajo del espacio de trabajo	En la parte superior de Cloud Manager, haga clic en **Estado de 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.

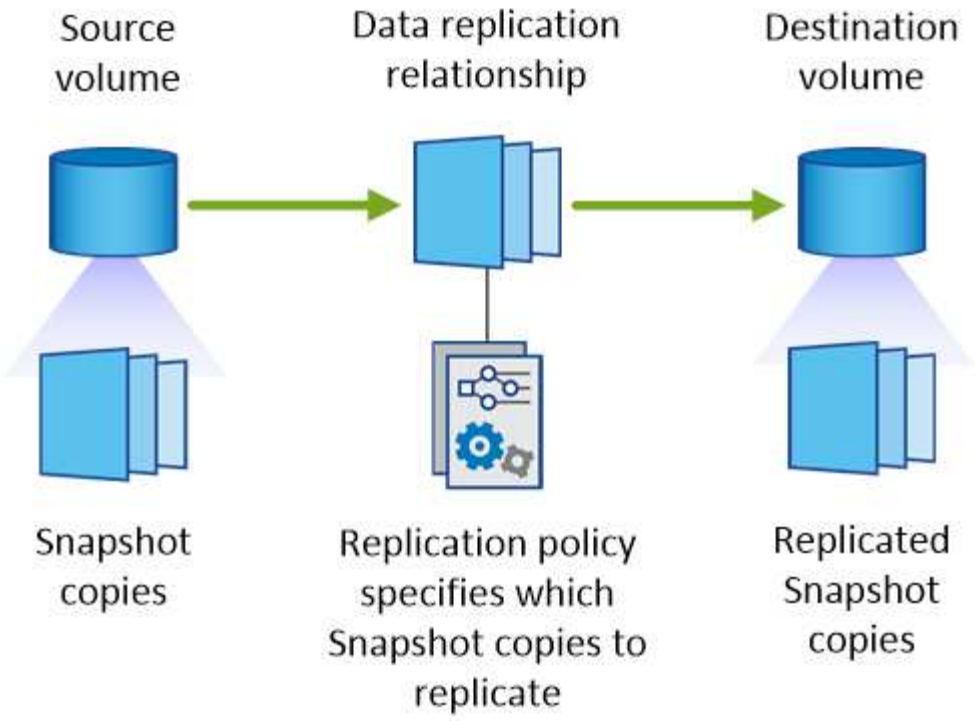
Lo que hacen las políticas de replicación

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.

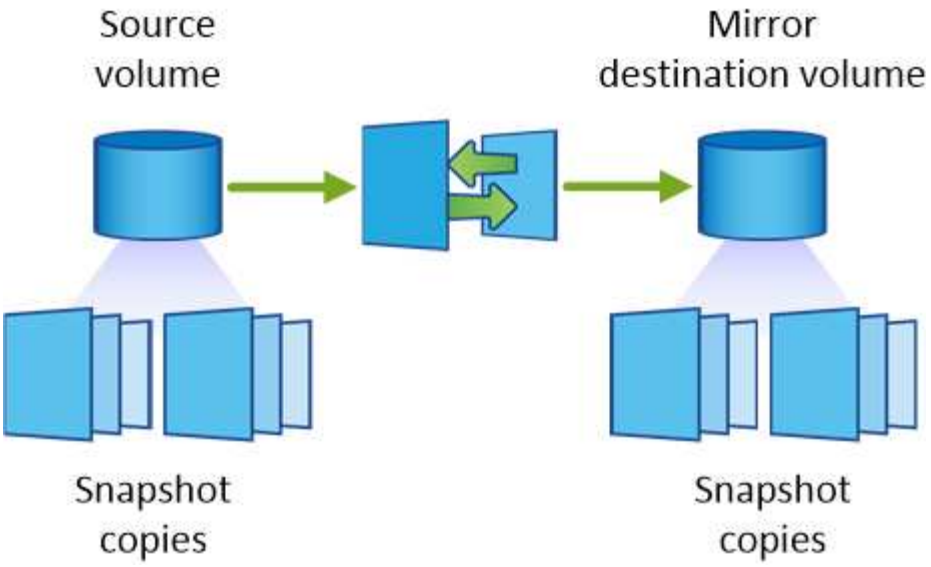
- Una política de *Backup* replica copias Snapshot específicas a un volumen de destino y, normalmente, las conserva durante un período de tiempo más largo del que tendría en el volumen de origen.

  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.

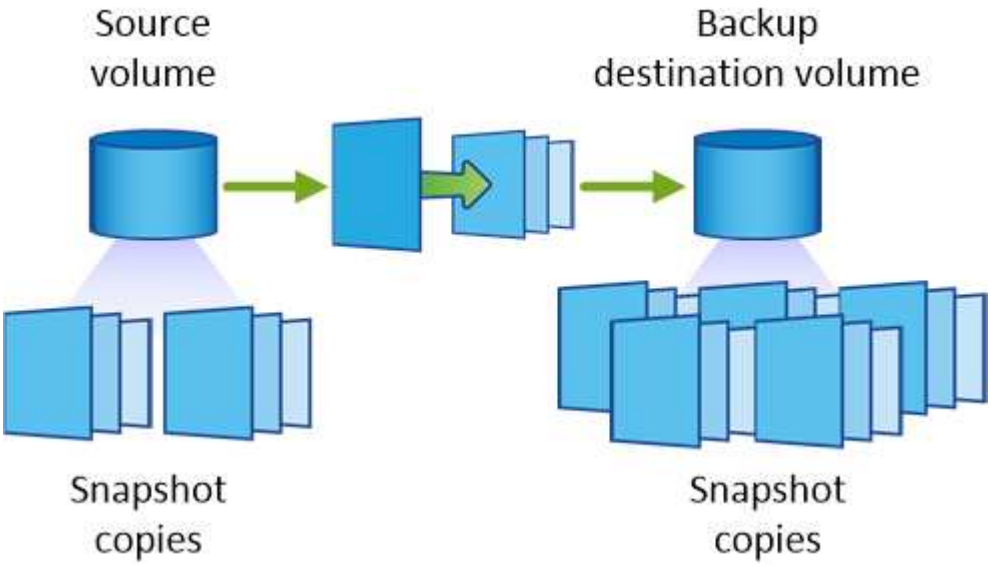
- Una política de *Mirror and Backup* proporciona recuperación ante desastres y retención a largo plazo.

  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.

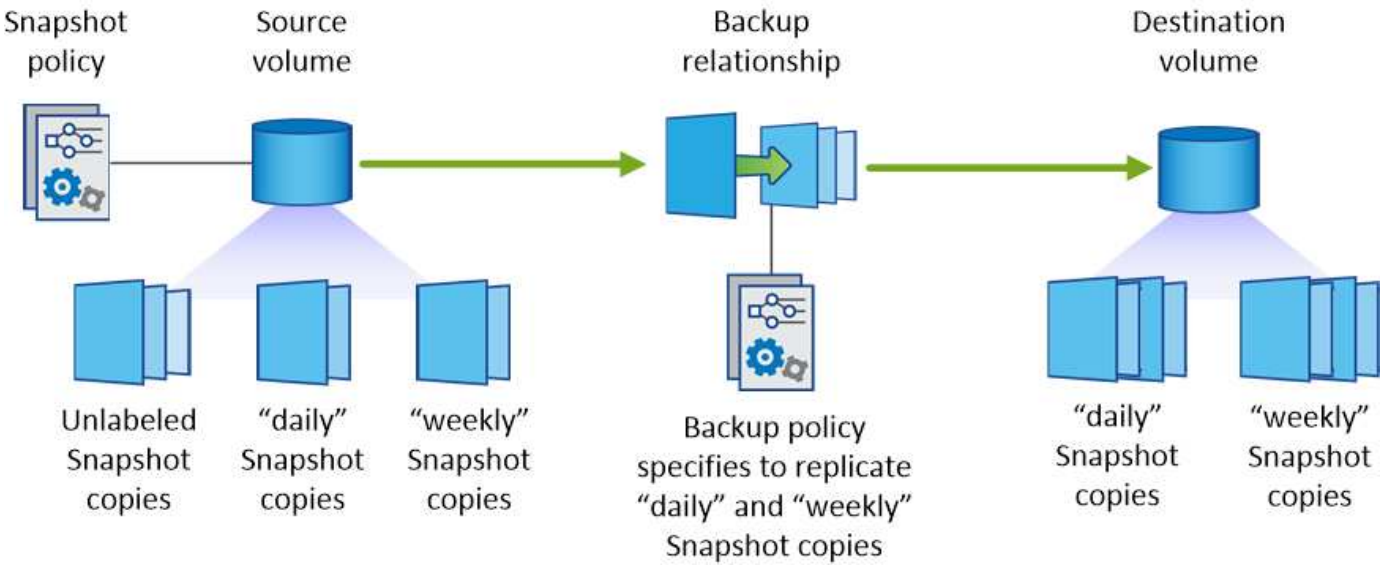
Descripción de la relación entre las etiquetas de copia de Snapshot y las políticas de backup

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.

Realizar backups de datos en Amazon S3

Backup en S3 es una función complementaria para Cloud Volumes ONTAP que ofrece funcionalidades de backup y restauración totalmente gestionadas para la protección y el archivado a largo plazo de sus datos en el cloud. Los backups se almacenan en el almacenamiento de objetos de S3, independientemente de las copias Snapshot de volúmenes que se utilicen para la recuperación o el clonado a corto plazo.

Cuando se habilita Backup en S3, el servicio realiza un backup completo de los datos. Todos los backups adicionales son incrementales, lo que significa que solo se realiza un backup de los bloques modificados y los nuevos bloques.

"Visite Cloud Central de NetApp para obtener más información sobre los precios".

Tenga en cuenta que debe usar Cloud Manager para todas las operaciones de backup y restauración. Cualquier acción que se haga directamente desde ONTAP o Amazon S3 tendrá como resultado una configuración no compatible.

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

Compruebe lo siguiente:

- Cloud Volumes ONTAP 9.4 o una versión posterior se ejecuta en una región AWS admitida: N. Virginia, Oregón, Irlanda, Frankfurt o Sydney
- Se ha suscrito al nuevo "Oferta Cloud Manager Marketplace"
- El puerto TCP 5010 está abierto para el tráfico saliente en el grupo de seguridad para Cloud Volumes ONTAP (está abierto de forma predeterminada)
- El puerto TCP 8088 está abierto para tráfico saliente en el grupo de seguridad para Cloud Manager (está abierto de forma predeterminada)
- Desde Cloud Manager se puede acceder al siguiente extremo:

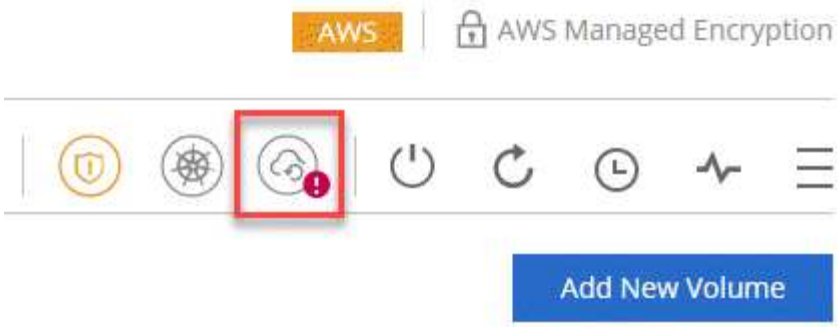
  https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist

- Hay espacio para que Cloud Manager asigne hasta dos extremos de VPC de interfaz en el VPC (el límite de AWS por VPC es de 20).
- Cloud Manager tiene permiso para usar los permisos de extremo de VPC que se enumeran en las versiones más recientes "Política de Cloud Manager":

```
"ec2:DescribeVpcEndpoints",
"ec2:CreateVpcEndpoint",
"ec2:ModifyVpcEndpoint",
"ec2:DeleteVpcEndpoints"
```

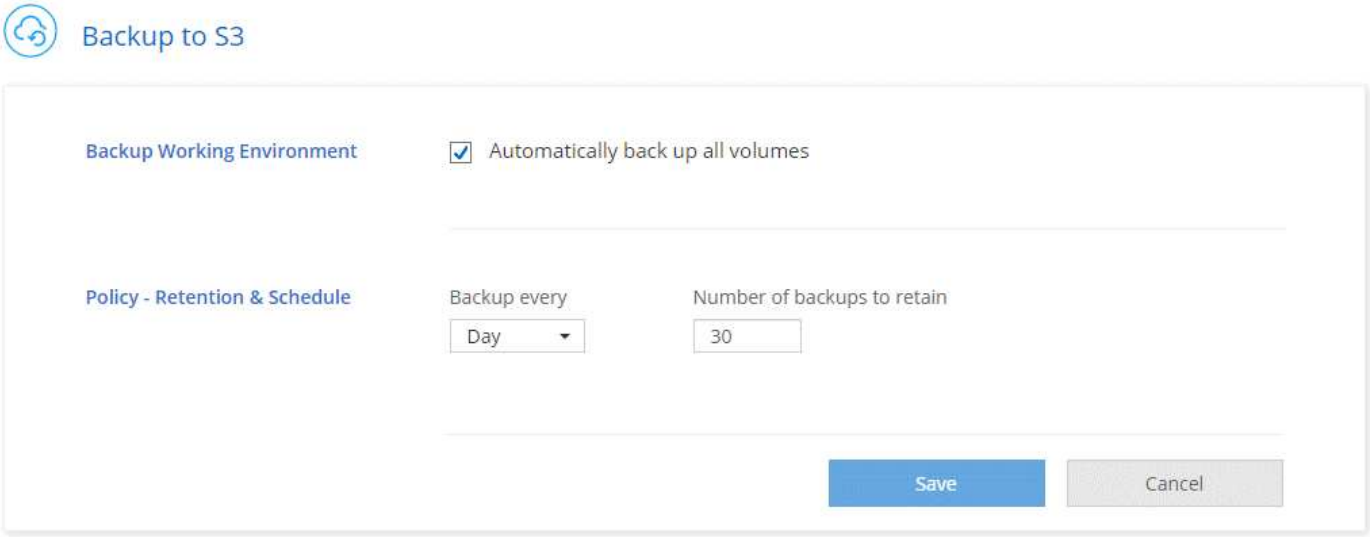
Habilite Backup en S3 en su sistema nuevo o existente

- Nuevos sistemas: La función Backup en S3 está habilitada de forma predeterminada en el asistente del entorno de trabajo. Asegúrese de mantener la opción habilitada.
- Sistemas existentes: Abra el entorno de trabajo, haga clic en el icono de configuración de copia de seguridad y habilite las copias de seguridad.



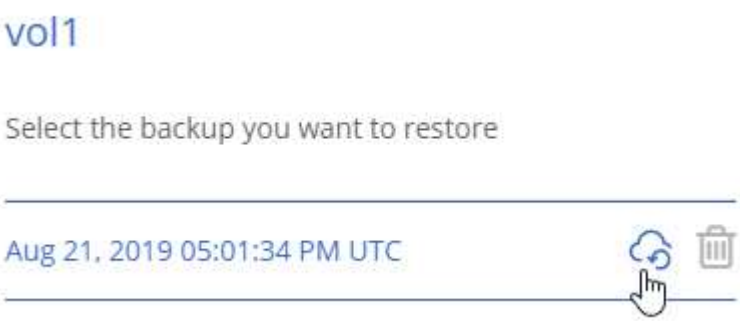
Si es necesario, modifique la política de backup

La política predeterminada realiza backups de los volúmenes todos los días y retiene 30 copias de backup de cada volumen. Si es necesario, puede cambiar la cantidad de copias de backup que se conservan.



Restaure sus datos, según sea necesario

En la parte superior de Cloud Manager, haga clic en **copia de seguridad y restauración**, seleccione un volumen, seleccione una copia de seguridad y, a continuación, restaure los datos de la copia de seguridad a un volumen nuevo.



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

El backup en S3 es compatible con Cloud Volume ONTAP 9.4 y versiones posteriores.

Regiones admitidas de AWS

El backup en S3 es compatible con Cloud Volumes ONTAP en las siguientes regiones de AWS:

- Este DE EE. UU. (N. Virginia)
- Oeste DE EE. UU. (Oregón)
- UE (Irlanda)
- UE (Frankfurt)
- APAC (Sidney)

Se requieren permisos de AWS

El rol IAM que proporciona permisos a Cloud Manager debe incluir lo siguiente:

```
"ec2:DescribeVpcEndpoints",
"ec2:CreateVpcEndpoint",
"ec2:ModifyVpcEndpoint",
"ec2:DeleteVpcEndpoints"
```

Requisito de suscripción de AWS

A partir del lanzamiento de la versión 3.7.3, hay una nueva suscripción de Cloud Manager disponible en AWS Marketplace. Esta suscripción permite la puesta en marcha de los sistemas Cloud Volumes ONTAP 9.6 y posteriores de PAYGO y la función Backup to S3. Necesita hacerlo "suscríbase a esta nueva suscripción a Cloud Manager" Antes de habilitar Backup en S3. La facturación de la función Backup to S3 se realiza mediante esta suscripción.

Requisitos de puertos

- El puerto TCP 5010 debe estar abierto para el tráfico saliente de Cloud Volumes ONTAP al servicio de respaldo.
- El puerto TCP 8088 debe estar abierto para tráfico saliente en el grupo de seguridad para Cloud Manager.

  Estos puertos ya están abiertos si se usan los grupos de seguridad predefinidos. No obstante, si ha utilizado los suyos, deberá abrir estos puertos.

Acceso a Internet de salida

Asegúrese de que se pueda acceder al siguiente extremo desde Cloud Manager: https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist

Cloud Manager se pone en contacto con este extremo para añadir su ID de cuenta de AWS a la lista de usuarios permitidos para Backup en S3.

Extremos de la interfaz VPC

Cuando se habilita la función Backup en S3, Cloud Manager crea un extremo de interfaz VPC en el VPC, donde se ejecuta Cloud Volumes ONTAP. Este *terminal de backup* se conecta al VPC de NetApp, donde se ejecuta el backup a S3. Si restaura un volumen, Cloud Manager crea un extremo de la interfaz adicional VPC, que es el *restore Endpoint*.

Todos los sistemas Cloud Volumes ONTAP adicionales del VPC utilizan estos dos extremos de VPC.

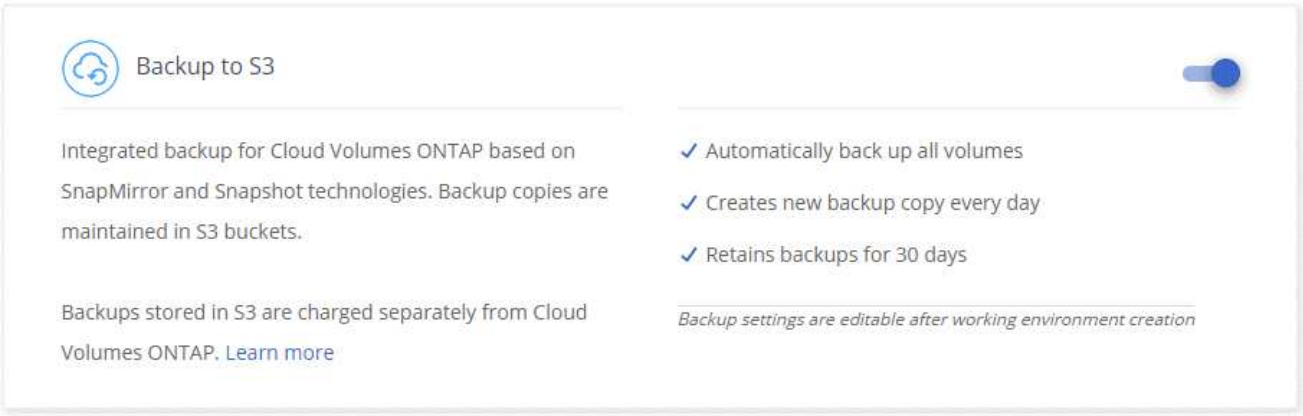
"El límite predeterminado para los extremos de VPC de la interfaz es de 20 por VPC". Asegúrese de que VPC no haya alcanzado el límite antes de habilitar la función.

Habilitar backups en S3 en un nuevo sistema

La función Backup to S3 está habilitada de manera 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 copia de seguridad en S3, deje activada la función y haga clic en **continuar**.



5. Complete las páginas del asistente para implementar el sistema.

Resultado

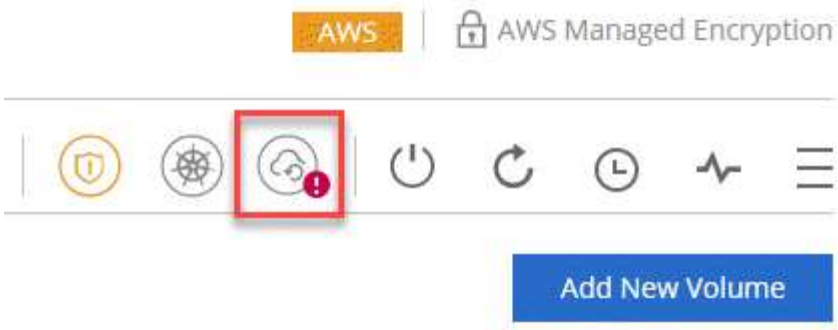
La función Backup to S3 está habilitada en el sistema y realiza un backup de volúmenes todos los días y retiene 30 copias de backup. Aprenda a modificar la retención de backup.

Habilitar backups en S3 en un sistema existente

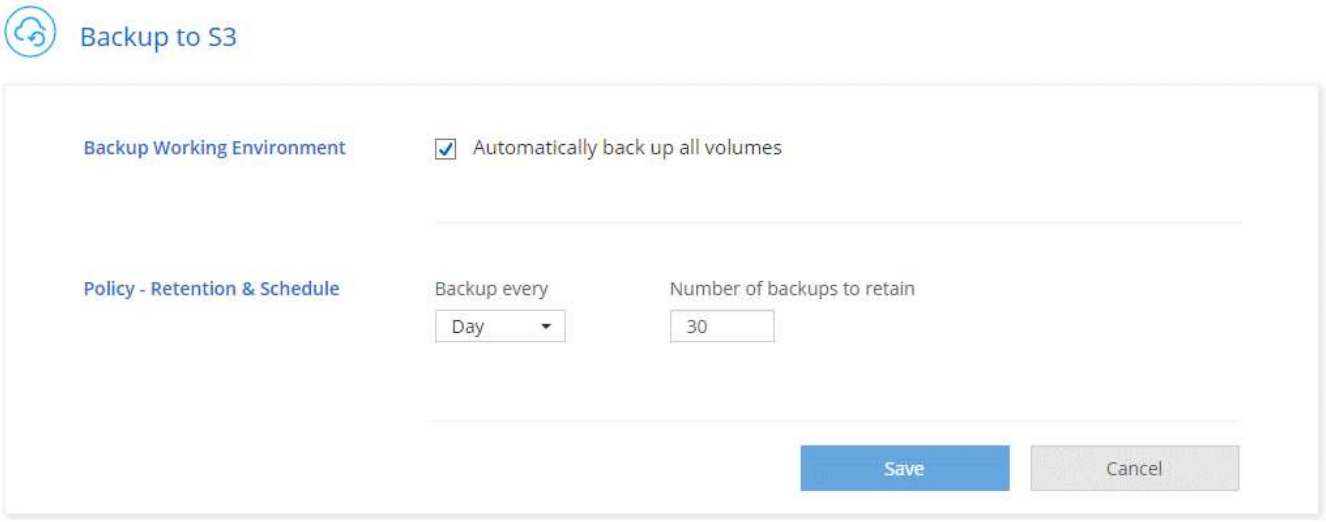
Es posible habilitar backups en S3 en un sistema Cloud Volumes ONTAP existente, siempre que se ejecute una configuración compatible. Para obtener más información, consulte Requisitos.

Pasos

1. Abra el entorno de trabajo.
2. Haga clic en el icono de configuración de copia de seguridad.



3. Seleccione **copia de seguridad automática de todos los volúmenes**.
4. Elija su retención de copia de seguridad y, a continuación, haga clic en **Guardar**.



Resultado

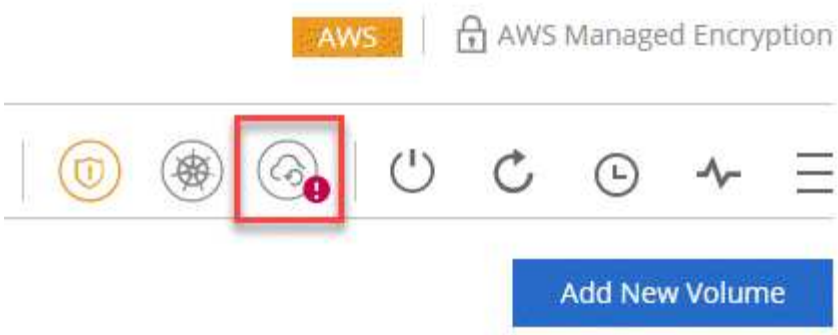
La función Backup to S3 comienza a tomar los backups iniciales de cada volumen.

Cambiar la retención de backups

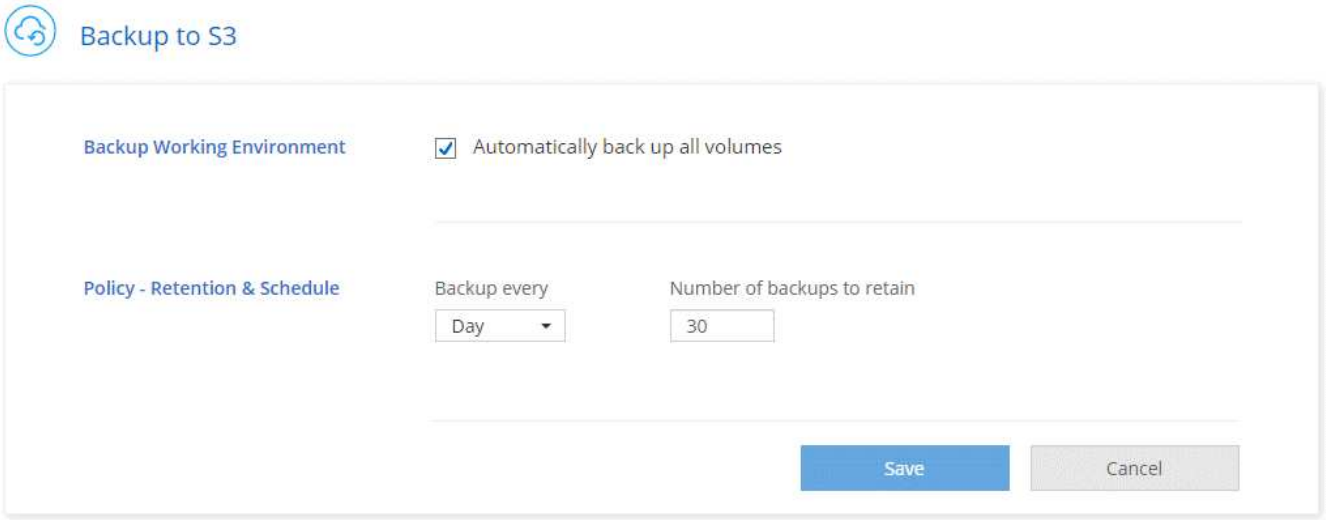
La política predeterminada realiza backups de los volúmenes todos los días y retiene 30 copias de backup de cada volumen. Es posible cambiar el número de copias de backup que se conservan.

Pasos

1. Abra el entorno de trabajo.
2. Haga clic en el icono de configuración de copia de seguridad.



3. Cambie la retención de la copia de seguridad y, a continuación, haga clic en **Guardar**.



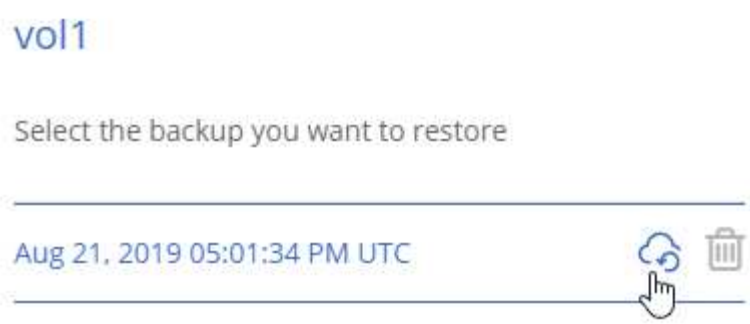
Restaurar un volumen

Cuando restaura datos de un backup, Cloud Manager realiza una restauración completa de un volumen en un volumen *new*. Puede restaurar los datos en el mismo entorno de trabajo o en otro de trabajo.

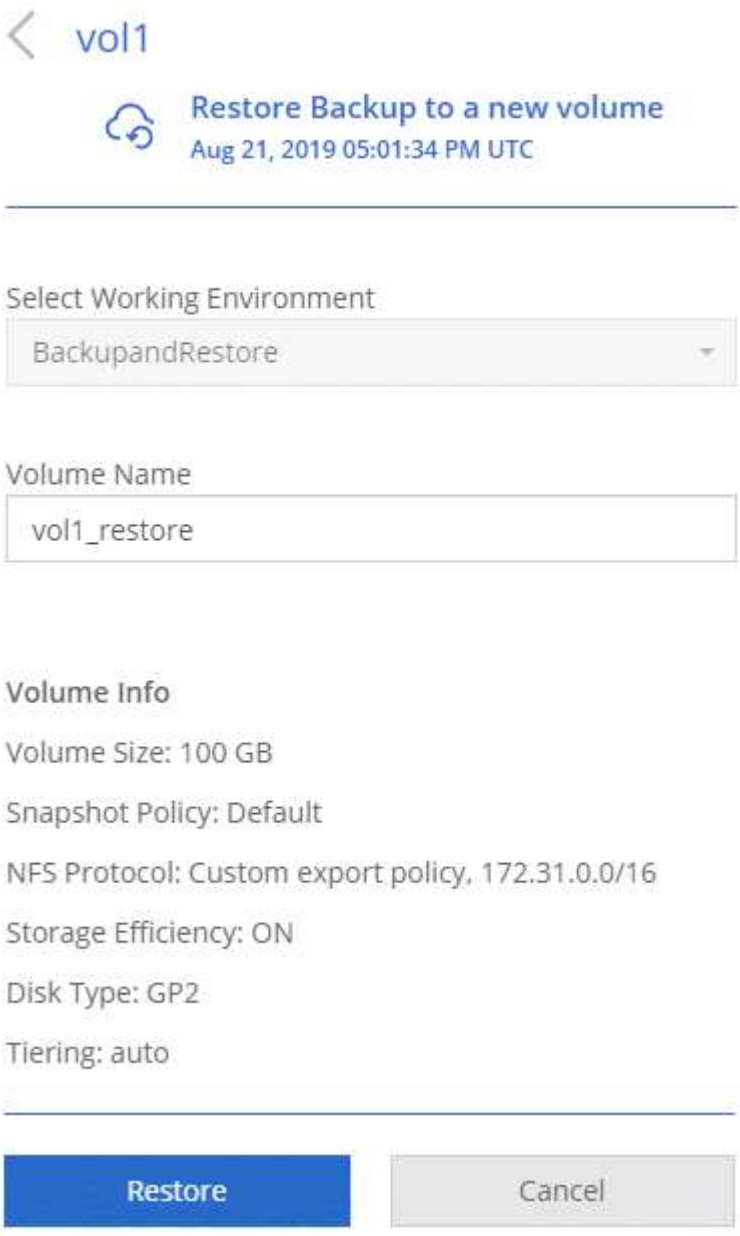
Pasos

1. En la parte superior de Cloud Manager, haga clic en **copia de seguridad y restauración**.
2. Seleccione el volumen que desea restaurar.

3. Busque el backup desde el que desea restaurar y haga clic en el icono de restauración.



4. Seleccione el entorno de trabajo al que desea restaurar el volumen.
5. Escriba un nombre para el volumen.
6. Haga clic en **Restaurar**.

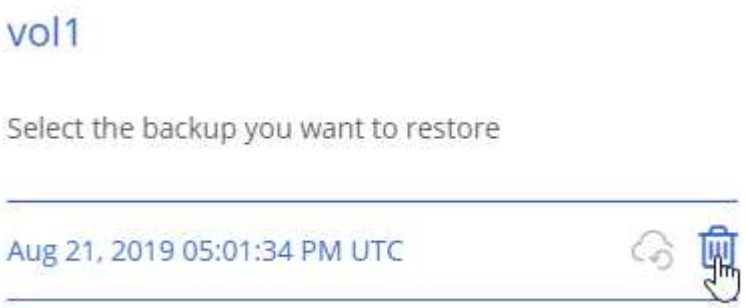


Eliminar backups

Todos los backups se retienen en S3 hasta que se los elimina de Cloud Manager. Los backups no se eliminan al eliminar un volumen o al eliminar el sistema Cloud Volumes ONTAP.

Pasos

1. En la parte superior de Cloud Manager, haga clic en **copia de seguridad y restauración**.
2. Seleccionar un volumen.
3. Busque el backup que desea eliminar y haga clic en el icono de eliminar.



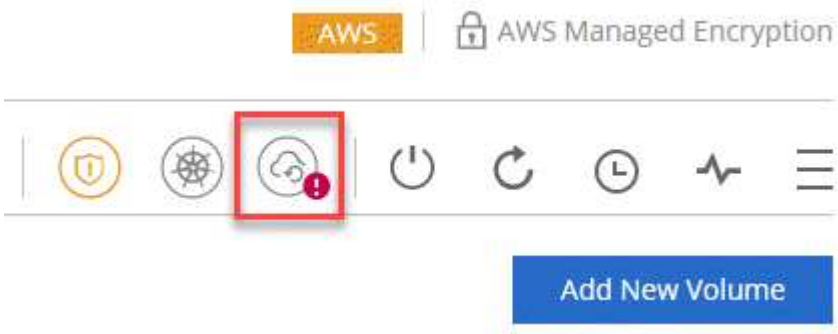
4. Confirme que desea eliminar el backup.

Deshabilitar los backups en S3

Al deshabilitar los backups en S3, se deshabilitan los backups de cada volumen del sistema. No se eliminarán los backups existentes.

Pasos

1. Abra el entorno de trabajo.
2. Haga clic en el icono de configuración de copia de seguridad.



3. Desactivar **hacer una copia de seguridad automática de todos los volúmenes** y, a continuación, hacer clic en **Guardar**.

Cómo funciona el backup en S3

En las siguientes secciones, se proporciona más información sobre la función Backup to S3.

La ubicación de los backups

Las copias de backup se almacenan en un bloque de S3 propiedad de NetApp, en la misma región donde se encuentra el sistema Cloud Volumes ONTAP.

Los backups son incrementales

Tras el primer backup completo de sus datos, todos los backups adicionales son incrementales, lo que significa que solo se realiza un backup de los bloques modificados y los nuevos bloques.

Los backups se realizan a medianoche

Los backups diarios comienzan justo después de la medianoche cada día. En este momento, no puede programar operaciones de backup a una hora específica del 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 las instancias de Cloud Volumes ONTAP desde otros sistemas de Cloud Manager.

La política de respaldo es de todo el sistema

La cantidad de backups que se retendrán se define en el nivel del sistema. No puede establecer una política diferente para cada volumen del sistema.

Seguridad

Los datos de los backups se protegen con conexiones HTTPS en reposo con cifrado AES de 256 bits y TLS 1.2.

Los datos viajan a través de enlaces de Direct Connect seguros al servicio, y permanecen protegidos en reposo gracias al cifrado de 256 bits de AES. A continuación, los datos cifrados se escriben en el cloud mediante conexiones HTTPS TLS 1.2. Además, los datos también se trasladan a Amazon S3 solo a través de conexiones terminales, de manera que no se envía tráfico por Internet.

A cada usuario se le asigna una clave de inquilino, además de una clave de cifrado general propiedad del servicio. Este requisito es similar a necesitar un par de claves para abrir un cliente seguro en un banco. Todas las claves, como credenciales de cloud, se almacenan de forma segura mediante el servicio y solo están restringidas a cierto personal de NetApp responsable de mantenimiento del servicio.

Limitaciones

- Si utiliza cualquiera de los siguientes tipos de instancia, un sistema Cloud Volumes ONTAP puede realizar un backup de un máximo de 20 volúmenes a S3:
  - m4.xlarge
  - m5.xlarge
  - r4.xlarge
  - r5.xlarge
- Los volúmenes que cree fuera de Cloud Manager no se podrán realizar automáticamente backups en S3.

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, debe deshabilitar la función Backup en S3 y, a continuación, volver a habilitarla.

- Cuando restaura datos de un backup, Cloud Manager realiza una restauración completa de un volumen en un volumen *new*. No se realiza automáticamente backups de este nuevo volumen en S3.

  Si se desea realizar un backup de volúmenes creados desde una operación de restauración, se debe deshabilitar la función Backup en S3 y, luego, volver a habilitarla.

- Es posible realizar backups de volúmenes con un tamaño mínimo de 50 TB.
- El backup en S3 puede mantener hasta 245 backups totales de un volumen.
- El almacenamiento WORM no es compatible en un sistema Cloud Volumes ONTAP cuando se habilita el backup en S3.

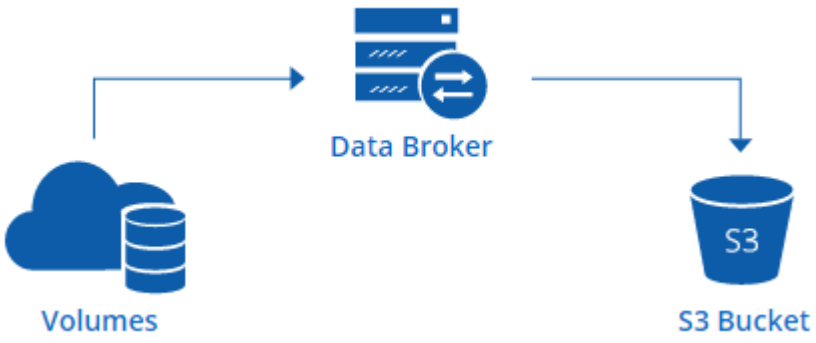
Sincronizando datos en Amazon S3

Puede sincronizar datos de ONTAP Volumes en un bloque de Amazon S3 mediante la integración de un entorno de trabajo con "Cloud Sync de NetApp". A continuación, puede utilizar los datos sincronizados como una copia secundaria o para el procesamiento de datos con servicios de AWS como EMR y Redshift.

Cómo funciona la función de sincronización con S3

Puede integrar un entorno de trabajo con el servicio Cloud Sync en cualquier momento. Cuando se integra un entorno de trabajo, el servicio Cloud Sync sincroniza los datos de los volúmenes seleccionados en un único bloque de S3. La integración funciona con entornos de trabajo de Cloud Volumes ONTAP, así como clústeres de ONTAP que están en las instalaciones o forman parte de una configuración de almacenamiento privado de NetApp (NPS).

Para sincronizar los datos, el servicio inicia una instancia de agente de datos en el VPC. Cloud Sync utiliza un agente de datos por entorno de trabajo para sincronizar datos de volúmenes en un bloque de S3. Después de la sincronización inicial, el servicio sincroniza los datos modificados una vez al día a medianoche.



Si desea realizar acciones Cloud Sync avanzadas, vaya directamente al servicio Cloud Sync. A partir de ahí, puede realizar acciones como sincronizar de S3 con un servidor NFS, elegir distintos bloques S3 para volúmenes y modificar programaciones.

prueba gratuita de 14 días

Si usted es un nuevo usuario de Cloud Sync, sus primeros 14 días son gratis. Después de que finalice la prueba gratuita, deberá pagar por cada *SYNC Relationship* a una tarifa por hora o mediante la compra de licencias. Cada volumen que se sincroniza con un bloque de S3 se considera una relación de sincronización. Puede configurar ambas opciones de pago directamente desde Cloud Sync en la página Configuración de licencia.

Cómo obtener ayuda

Use las siguientes opciones para cualquier soporte relacionado con la función Cloud Manager Sync to S3 o con Cloud Sync en general:

- Comentarios generales sobre productos: ng-cloudsync-contact@netapp.com
- Opciones de soporte técnico:
  - Comunidades Cloud Sync de NetApp
  - Chat en el producto (en la esquina inferior derecha de Cloud Manager)

Integración de un entorno de trabajo con el servicio Cloud Sync

Si desea sincronizar volúmenes en Amazon S3 directamente desde Cloud Manager, debe integrar el entorno de trabajo con el servicio Cloud Sync.

[] | *https://img.youtube.com/vi/3hOtLs70_xE/maxresdefault.jpg*

Pasos

1. Abra un entorno de trabajo y haga clic en **Sincronizar a S3**.
2. Haga clic en **Sincronizar** y siga las indicaciones para sincronizar los datos con S3.

No es posible sincronizar los volúmenes de protección de datos en S3. Los volúmenes deben ser editables.

Gestión de relaciones de sincronización de volúmenes

Tras integrar un entorno de trabajo con el servicio Cloud Sync, puede sincronizar volúmenes adicionales, detener la sincronización de un volumen y eliminar la integración con Cloud Sync.

Pasos

1. En la página entornos de trabajo, haga doble clic en el entorno de trabajo en el que desea gestionar las relaciones de sincronización.
2. Si desea activar o desactivar la sincronización con S3 para un volumen, seleccione el volumen y, a continuación, haga clic en **Sincronizar con S3** o **Eliminar relación de sincronización**.
3. Si desea eliminar todas las relaciones de sincronización de un entorno de trabajo, haga clic en la ficha **Sincronizar a S3** y, a continuación, haga clic en **Eliminar sincronización**.

   Esta acción no elimina los datos sincronizados del bloque de S3. Si el agente de datos no se está utilizando en ninguna otra relación de sincronización, el servicio Cloud Sync elimina el agente de datos.

Obtenga información sobre la privacidad de sus datos

Más información sobre Cloud Compliance

Cloud Compliance es un servicio de privacidad y cumplimiento de normativas de datos para Cloud Volumes ONTAP en AWS y Azure. Mediante la tecnología basada en la inteligencia artificial (IA), Cloud Compliance ayuda a las organizaciones a comprender el contexto de los datos e identificar los datos confidenciales en los sistemas de Cloud Volumes ONTAP.

Cloud Compliance está actualmente disponible como versión de disponibilidad controlada.

"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)

Coste

Cloud Compliance es un servicio complementario para Cloud Volumes ONTAP que proporciona NetApp sin coste adicional. La activación de Cloud Compliance requiere la puesta en marcha de una instancia cloud que su proveedor de cloud le cobrará. La entrada o salida de datos no supone ningún coste porque los datos no fluyen fuera de la red.

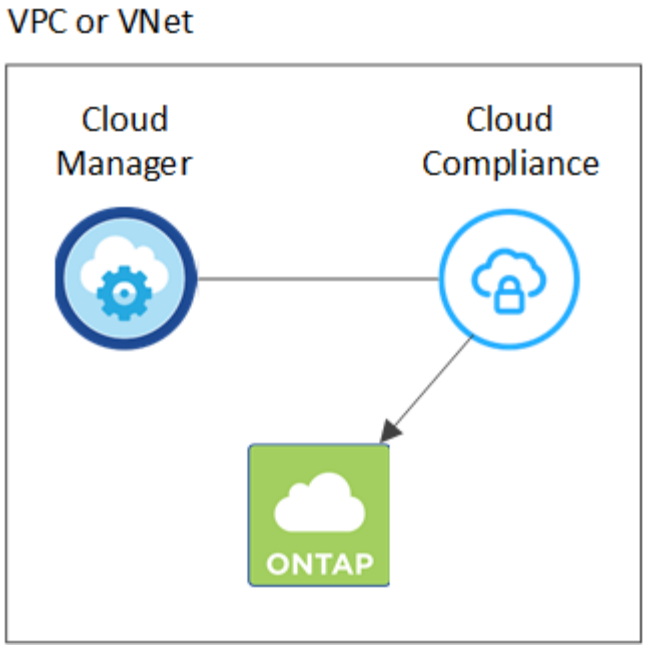
Cómo funciona Cloud Compliance

En un nivel superior, Cloud Compliance funciona como esta:

1. Habilite el cumplimiento de normativas cloud en uno o más sistemas de Cloud Volumes ONTAP.
2. Cloud Compliance analiza los datos mediante un proceso de aprendizaje de IA.
3. 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 en uno o más sistemas de Cloud Volumes ONTAP, Cloud Manager pone en marcha una instancia de Cloud Compliance en el mismo VPC o vnet que el primer sistema de 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 io1 de 500 GB.

  En regiones donde no hay m5.4xLarge disponible, Cloud Compliance se ejecuta en lugar de una instancia m4.4xLarge.

- La instancia se denomina *CloudCompliance* con un hash generado (UUID) concatenado. Por ejemplo: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*
- Solo se pone en marcha una instancia de Cloud Compliance por sistema Cloud Manager.
- Las actualizaciones del software de Cloud Compliance se automatizan, ya que no tiene que preocuparse por ello.

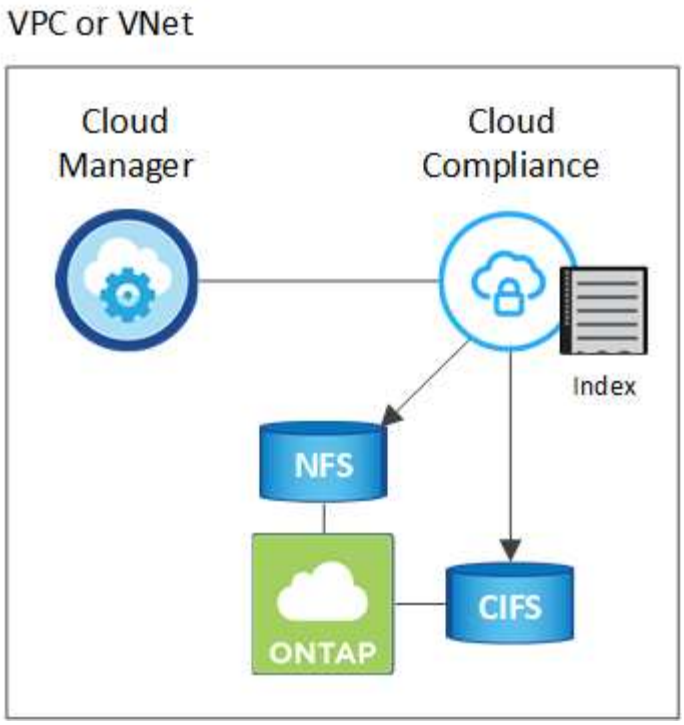
La instancia debe permanecer en ejecución en todo momento debido a que Cloud Compliance analiza continuamente los datos en sistemas Cloud Volumes ONTAP.

Cómo funcionan las exploraciones

Después de activar Cloud Compliance, comienza inmediatamente a analizar sus datos para identificar datos personales y confidenciales.

Cloud Compliance se conecta a Cloud Volumes ONTAP 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.

Cloud Compliance analiza los datos no estructurados en cada volumen para obtener una amplia información personal. 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.



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 entorno de trabajo, pero no en el nivel de volumen. "Vea cómo".

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 una dirección IP privada y un grupo de seguridad que permite conexiones HTTP entrantes desde Cloud Manager. Esta conexión le permite acceder a la consola de Cloud Compliance desde la interfaz de Cloud Manager.

Las reglas salientes están completamente abiertas. La instancia se conecta a los sistemas Cloud Volumes ONTAP y a Internet a través de un proxy desde Cloud Manager. Se necesita acceso a Internet para actualizar el software Cloud Compliance y enviar métricas de uso.

Si tiene requisitos estrictos de red, "Obtenga información sobre los extremos con los que se contacta Cloud Compliance".

Los datos indexados nunca salen de la instancia de cumplimiento en nube. Los datos no se transmiten fuera de su red virtual y no se envían a Cloud Manager.

Acceso de los usuarios a la información de cumplimiento

Los administradores de Cloud Manager pueden ver información de cumplimiento de normativas para todos los entornos de trabajo.

Los administradores de área de trabajo pueden 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.

"Más información acerca de los roles de Cloud Manager".

Primeros pasos con Cloud Compliance para Cloud Volumes ONTAP

Complete unos pasos para comenzar a usar Cloud Compliance para Cloud Volumes ONTAP en AWS o Azure.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

Compruebe que la configuración cumple los requisitos

- Asegúrese de que la instancia de Cloud Compliance tenga acceso saliente a Internet.

  Cloud Manager pone en marcha la instancia en el mismo VPC o vnet que el primer sistema de Cloud Volumes ONTAP de la solicitud.

- Asegúrese de que los usuarios puedan acceder a la interfaz de Cloud Manager desde un host que tenga una conexión directa con AWS o Azure, o desde un host que esté dentro de la misma red que la instancia de Cloud Compliance (la instancia tendrá una dirección IP privada).
- Asegúrese de mantener en funcionamiento la instancia de Cloud Compliance.

Habilite Cloud Compliance en Cloud Volumes ONTAP

- Nuevos entornos de trabajo: Asegúrese de mantener la conformidad con la nube habilitada al crear el entorno de trabajo (está activada de forma predeterminada).
- Entornos de trabajo existentes: Haga clic en **conformidad**, edite opcionalmente la lista de entornos de trabajo y haga clic en **Mostrar panel de cumplimiento**.

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.
- 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 **cumplimiento** > **Estado de exploración CIFS** > **Editar credenciales CIFS** 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.

Garantice la conectividad entre Cloud Manager y Cloud Compliance

- El grupo de seguridad para Cloud Manager debe permitir el tráfico entrante y saliente a través del puerto 80 hacia y desde la instancia de Cloud Compliance.
- Si la red AWS no utiliza NAT o proxy para el acceso a Internet, el grupo de seguridad para Cloud Manager debe permitir el tráfico entrante a través del puerto TCP 3128 desde la instancia de Cloud Compliance.

Revisión de requisitos previos

Revise los siguientes requisitos previos para asegurarse de tener una configuración compatible antes de habilitar Cloud Compliance. Deberá garantizar la conectividad entre los componentes después de habilitar Cloud Compliance. Esto se trata a continuación.

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:

Puntos finales	Específico
https://cloudmanager.cloud.netapp.com	Comunicación con el servicio Cloud Manager, que incluye cuentas de Cloud Central.

Puntos finales	Específico
https://netapp-cloud-account.auth0.com	Comunicación con Cloud Central de NetApp para la autenticación de usuario centralizada.
https://cloud-compliance-support-netapp.s3.us-west-1.amazonaws.com https://hub.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 la conectividad del explorador web con 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.

Si accede a Cloud Manager desde una dirección IP pública, es probable que su navegador web no se ejecute en un host dentro de la red.

Mantenga Cloud Compliance en ejecución

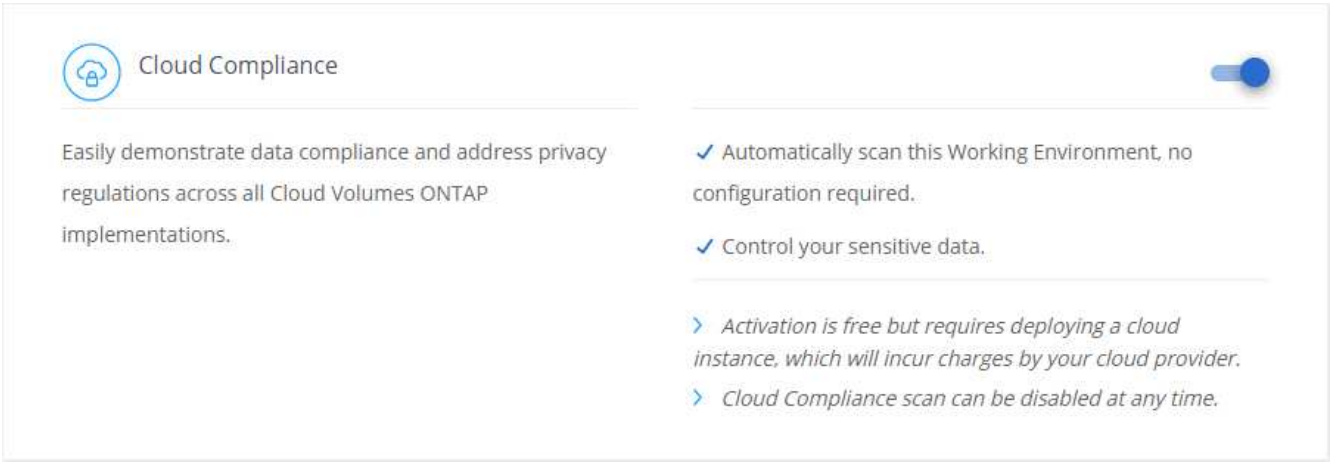
La instancia de Cloud Compliance debe permanecer activa para analizar sus datos de forma continua.

Habilitar Cloud Compliance en un nuevo entorno de trabajo

Cloud Compliance se habilita de forma predeterminada 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 o Microsoft Azure como proveedor de cloud y, a continuación, elija un sistema de alta disponibilidad o nodo único.
3. Rellene la página Details & Credentials.
4. En la página Servicios, deje Cloud Compliance activado y haga clic en **continuar**.



5. Complete las páginas del asistente para implementar el sistema.

   Para obtener ayuda, consulte "Inicio de Cloud Volumes ONTAP en AWS" y.. "Inicio de Cloud Volumes ONTAP en Azure".

Resultado

Cloud Compliance se habilita en el sistema Cloud Volumes ONTAP. Si es la primera vez que habilita Cloud Compliance, Cloud Manager pone en marcha la instancia de Cloud Compliance en su proveedor de cloud. En cuanto la instancia esté disponible, comienza a analizar los datos a medida que se escriben en cada volumen que cree.

Habilitar Cloud Compliance en entornos de trabajo existentes

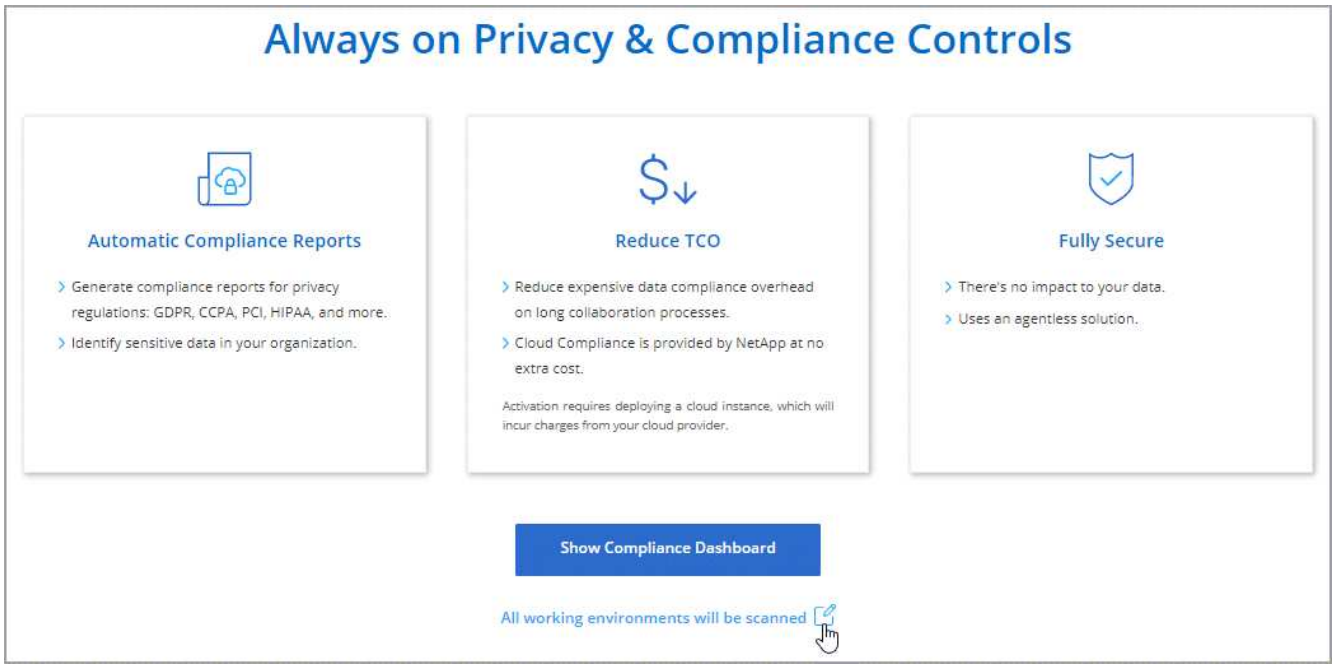
Habilite el cumplimiento de la nube en sus sistemas Cloud Volumes ONTAP existentes desde la pestaña **conformidad** de Cloud Manager.

Otra opción es habilitar Cloud Compliance desde la ficha **entornos de trabajo** seleccionando cada entorno de trabajo individualmente. Tardará más en completarse, a menos que solo tenga un sistema.

Pasos para múltiples entornos de trabajo

1. En la parte superior de Cloud Manager, haga clic en **cumplimiento**.
2. Si desea habilitar Cloud Compliance en entornos de trabajo específicos, haga clic en el icono de edición.

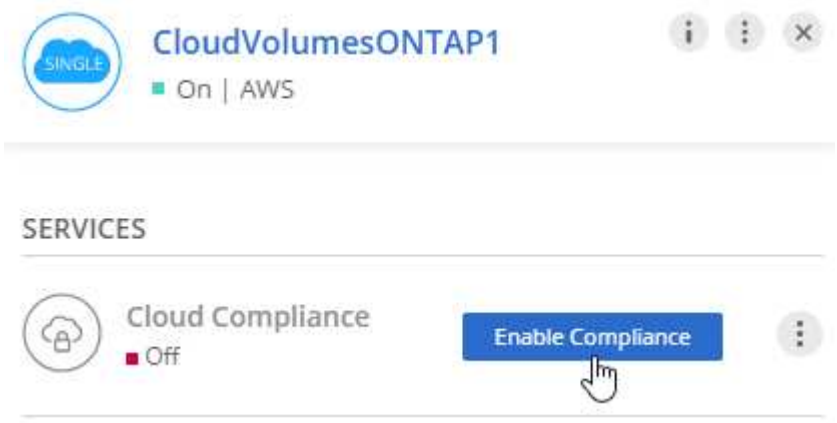
   De lo contrario, Cloud Manager se establece para habilitar Cloud Compliance en todos los entornos de trabajo a los que tenga acceso.



3. Haga clic en **Mostrar panel de cumplimiento**.

Pasos para un único entorno de trabajo

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 **Activar cumplimiento**.



Resultado

Si es la primera vez que habilita Cloud Compliance, Cloud Manager pone en marcha la instancia de Cloud Compliance en su proveedor de cloud.

Cloud Compliance comienza a analizar los datos en cada entorno de trabajo. Los datos estarán disponibles en la consola de cumplimiento de normativas tan pronto como Cloud Compliance finalice 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 garantizar que Cloud Compliance pueda acceder a los volúmenes en Cloud Volumes ONTAP, compruebe sus redes, grupos de seguridad y políticas de exportación. Necesitará proporcionar cumplimiento normativo

del cloud con credenciales CIFS para poder acceder a volúmenes CIFS.

Pasos

1. Asegúrese de que hay una conexión de red entre la instancia de Cloud Compliance y cada subred de Cloud Volumes ONTAP.

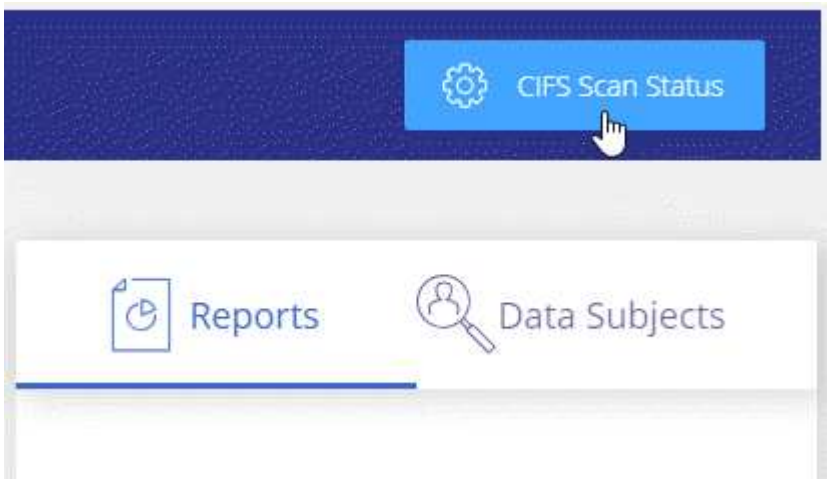
   Cloud Manager pone en marcha la instancia de Cloud Compliance en el mismo VPC o vnet que el primer sistema de Cloud Volumes ONTAP de la solicitud. Por lo tanto, este paso es importante si algunos sistemas Cloud Volumes ONTAP están en subredes o redes virtuales diferentes.

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 **cumplimiento**.
   b. En la parte superior derecha, haga clic en **Estado de exploración CIFS**.



   c. Para cada sistema Cloud Volumes ONTAP, 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.

Verificar que Cloud Manager puede acceder a Cloud Compliance

Garantice la conectividad entre Cloud Manager y Cloud Compliance para poder ver los datos sobre el cumplimiento de normativas que encontró Cloud Compliance.

Pasos

1. Asegúrese de que el grupo de seguridad de Cloud Manager permite el tráfico entrante y saliente a través del puerto 80 hacia y desde la instancia de Cloud Compliance.

   Esta conexión le permite ver información en la ficha cumplimiento.

2. Si la red AWS no utiliza NAT o proxy para el acceso a Internet, modifique el grupo de seguridad para Cloud Manager para permitir el tráfico entrante a través del puerto TCP 3128 desde la instancia de Cloud Compliance.

   Esto es necesario porque la instancia de Cloud Compliance utiliza Cloud Manager como proxy para acceder a Internet.

   Este puerto está abierto de forma predeterminada en todas las nuevas instancias de Cloud Manager, a partir de la versión 3.7.5. No está abierto en las instancias de Cloud Manager creadas antes de esa versión.

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.

Datos personales

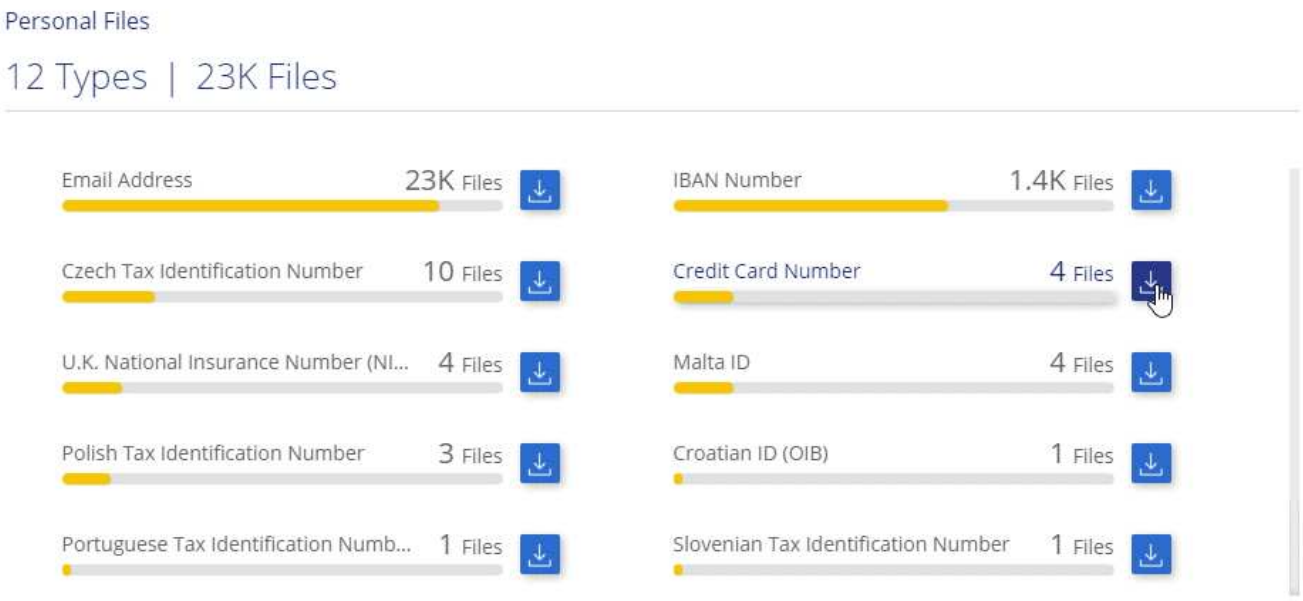
Cloud Compliance identifica automáticamente palabras, cadenas y patrones específicos (Regex) dentro de los datos. Por ejemplo, Información de identificación personal (PII), números de tarjeta de crédito, números de seguridad social, números de cuenta bancaria y mucho más. Consulte la lista completa.

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**.
2. Descargue los detalles de uno de los dos tipos de archivo principales directamente desde la pantalla principal, o haga clic en **Ver todo** y descargue la lista para cualquiera de los tipos de datos personales encontrados.



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
	Dirección IP	Sí

Tipo	Identificador	¿validación de proximidad?
Identificadores nacionales	ID belga (Numero Nacional)	Sí
	ID búlgaro (número civil unificado)	Sí
	Número de identificación fiscal de Chipre (TIC)	Sí
	Número de identificación fiscal danés (CPR)	Sí
	ID de Estonia (Isikukood)	Sí
	Finlandés ID (henkilötunnu)	Sí
	Número de identificación fiscal francés (SPI)	Sí
	Número de identificación fiscal alemán (Steuerliche Identifikationsnummer)	Sí
	Número de identificación fiscal húngara (Adóazonosísó jel)	Sí
	Irish ID (PPS)	Sí
	Documento de identidad israelí	Sí
	Italiano ID (Codice Fiscale)	Sí
	Número de identificación fiscal letón	Sí
	Lituano ID (Asmens kodas)	Sí
	ID de Luxemburgo	Sí
	Malta ID	Sí
	Netherlands ID (BSN)	Sí
	Número de identificación fiscal polaco	Sí
	Número de identificación fiscal (NIF) en portugués	Sí
	Número de identificación fiscal rumano	Sí
	Número de identificación fiscal eslovaca	Sí
	Número de identificación fiscal esloveno	Sí
	ID sudafricano	Sí
	Número de identificación fiscal en español	Sí
	Número de identificación fiscal sueco	Sí
	REINO UNIDO Número de Seguro Nacional (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.

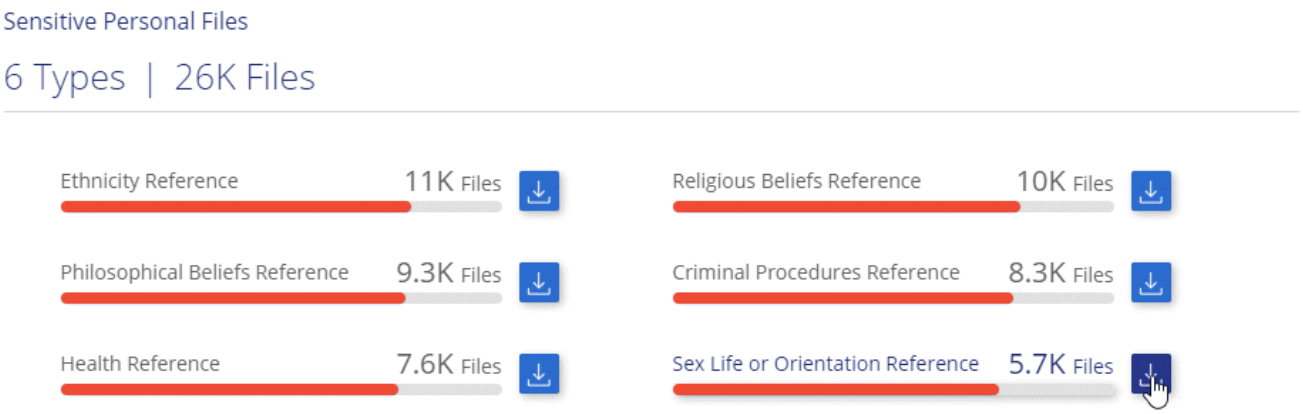
Por ejemplo, una categoría de datos confidenciales sobre el GDPR es su origen étnico. Debido a sus habilidades para NLP, Cloud Compliance puede distinguir la diferencia entre una frase que dice "George es mexicano" (que indica datos confidenciales como se especifica en el artículo 9 del RGPD), frente 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 **cumplimiento**.
2. Descargue los detalles de uno de los dos tipos de archivo principales directamente desde la pantalla principal, o haga clic en **Ver todo** y, a continuación, descargue la lista para cualquiera de los tipos de datos personales confidenciales que se hayan encontrado.



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.

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.

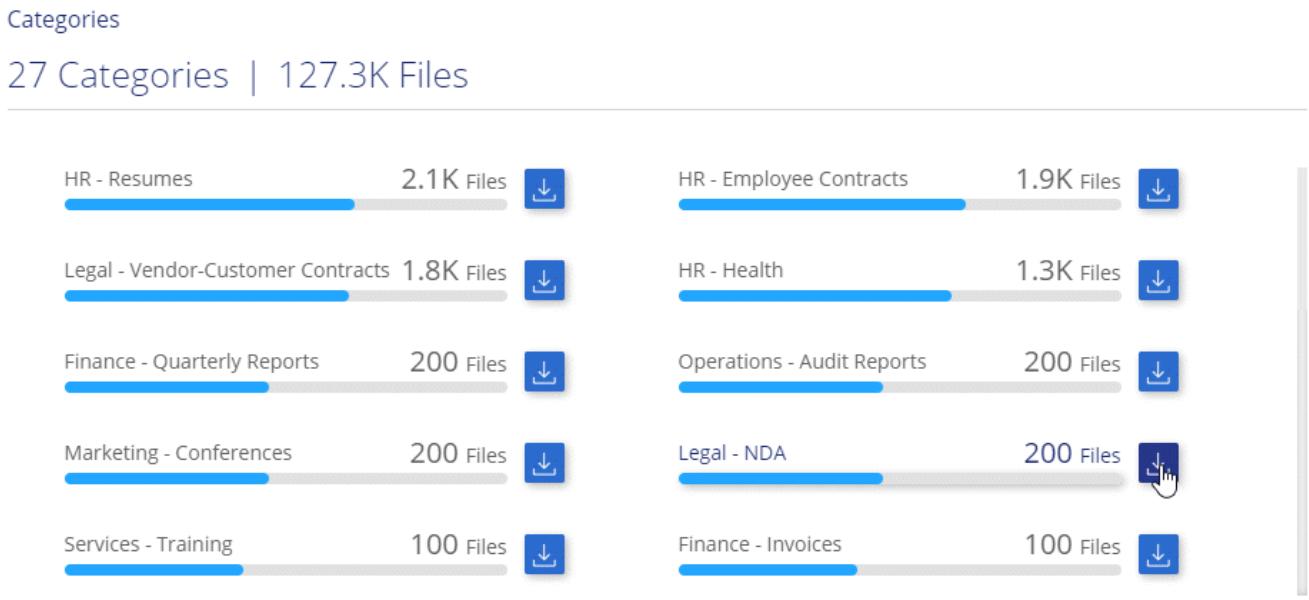
Las categorías pueden ayudarle a entender lo que está pasando con sus datos mostrándole el tipo de información que tiene. Por ejemplo, una categoría como currículos o contratos de empleados puede incluir datos confidenciales. Al descargar el informe CSV, es posible que encuentre que los contratos de empleados se almacenan en una ubicación no segura. 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 **cumplimiento**.
2. Descargue los detalles de uno de los 4 tipos de archivo principales directamente desde la pantalla principal, o haga clic en **Ver todos** y descargue la lista para cualquiera de las categorías.



Tipos de categorías

Cloud Compliance categoriza sus datos de la siguiente manera:

Finanzas

- Hojas de balance
- Órdenes de compra
- Facturas
- Informes trimestrales

RR. HH

- Comprobación de fondo
- Planes de compensación
- Contratos de empleados
- Revisión de empleados
- Salud
- Se reanudará

Legal

- NDA
- Contratos con el proveedor y el cliente

Marketing

- Campañas
- Conferencias

Operaciones

- Informes de auditoría

Ventas

- Pedidos de ventas

Servicios

- RFI
- RFP
- Entrenamiento

Soporte técnico

- Quejas y boletos

Otros

- Archivos de archivo
- Audio
- Archivos CAD
- Codificación
- Ejecutables
- Imágenes

Tipos de archivo

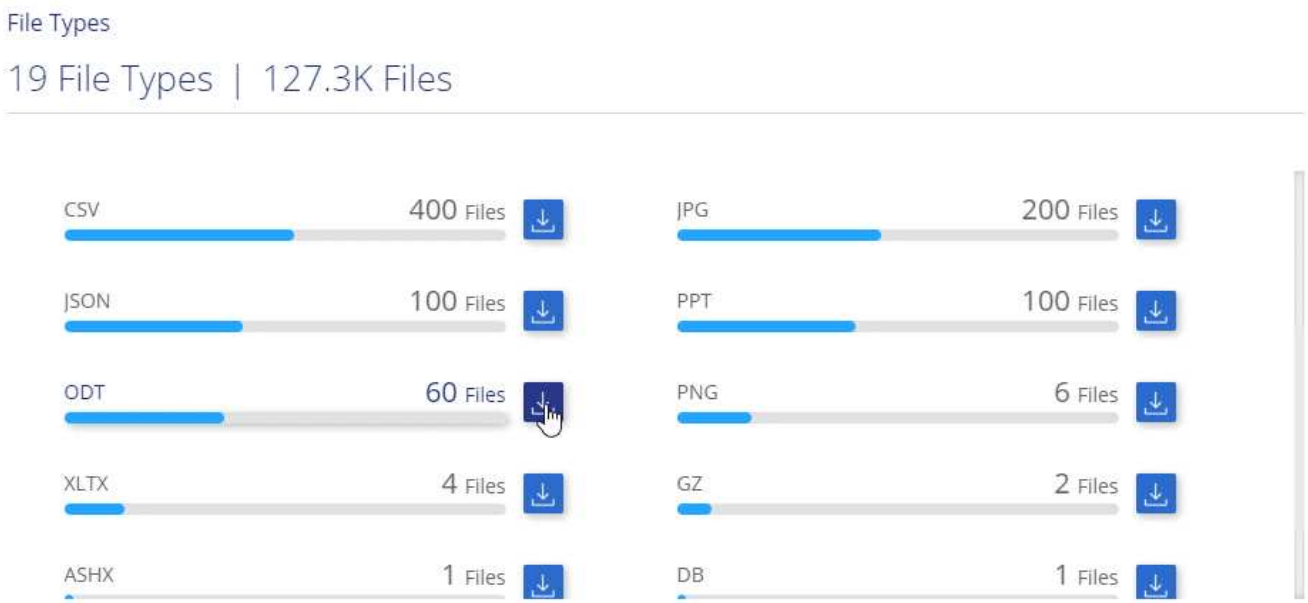
Cloud Compliance toma los datos que ha analizado y los divide por tipo de archivo. Cloud Compliance puede mostrar todos los tipos de archivo que se encuentran en los análisis.

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. 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 **cumplimiento**.
2. Descargue los detalles de uno de los 4 tipos de archivo principales directamente desde la pantalla principal, o haga clic en **Ver todo** y descargue la lista para cualquiera de los tipos de archivo.



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)

La consola permite 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 (se añadirá más adelante la compatibilidad con más).

Cada lista de archivos incluye la siguiente información:

- Nombre de archivo
- Tipo de ubicación
- Ubicación
- 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. Los archivos solo aparecen en los informes CSV.

Ver el Informe de evaluación de 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.

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.

El informe incluye la siguiente información:

Estado de cumplimiento
Una puntuación de gravedad (consulte a continuación para obtener más información) 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.

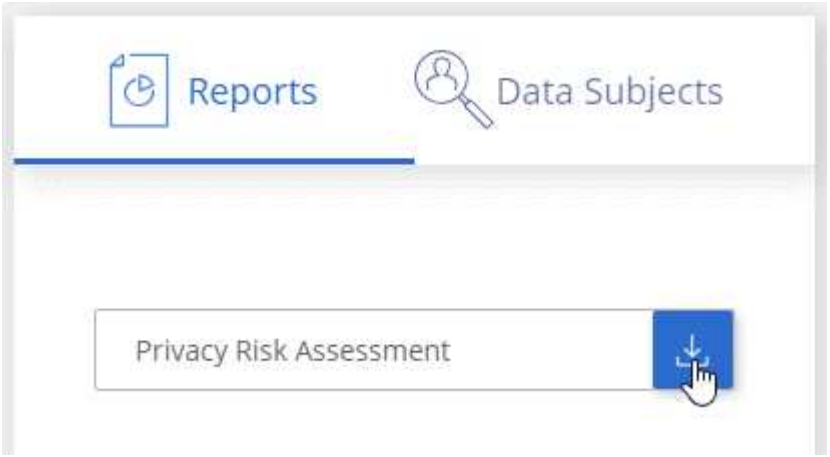
Datos sujetos en esta evaluación
El número de personas por ubicación para las cuales se encontraron identificadores nacionales.

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 **cumplimiento**.
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 más grande el 6 %
6	Dos de las variables son mayores del 6%
7	Tres de las variables son mayores del 6%
8	Una de las variables es más grande el 15 %
9	Dos de las variables son mayores del 15%
10	Tres de las variables son mayores del 15%

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 o un informe de solicitud de acceso de asunto 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

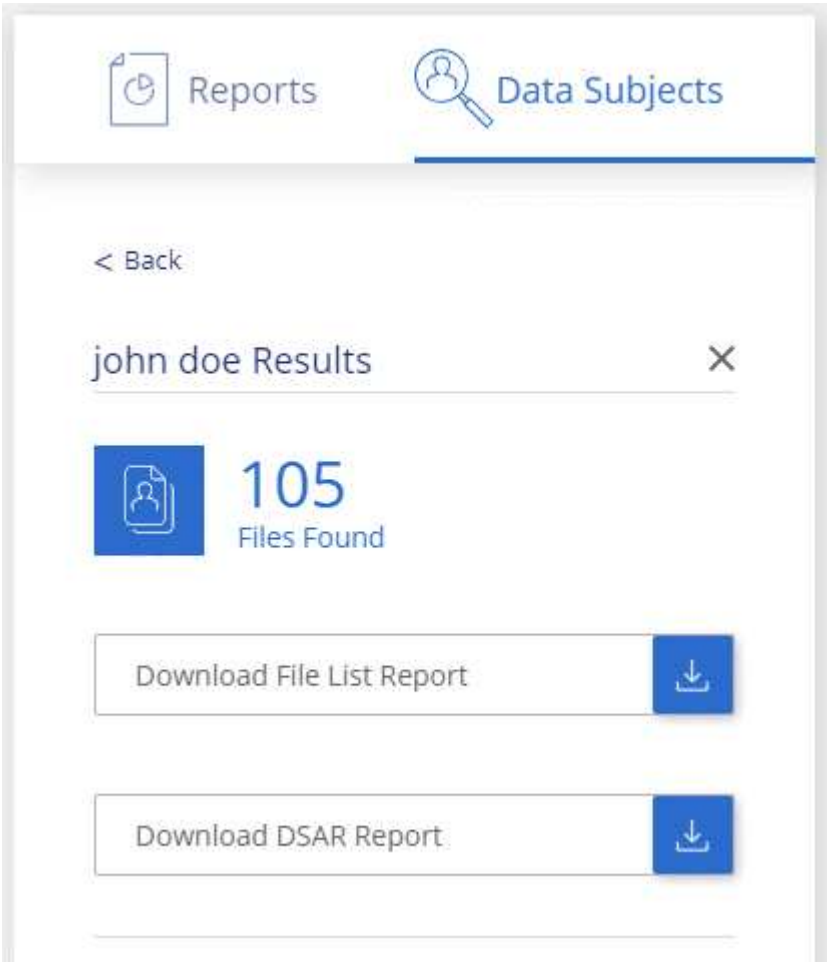
Busque el nombre completo o el identificador conocido del sujeto de datos y, a continuación, descargue un informe de la lista de archivos o un informe DSAR. Puede buscar por "cualquier tipo de información personal".

Sólo se admite inglés al buscar los nombres de los sujetos de datos. Más adelante se añadirá compatibilidad con más idiomas.

Pasos

1. En la parte superior de Cloud Manager, haga clic en **cumplimiento**.
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 de la lista de archivos**: Una lista de los archivos que contienen información sobre el asunto de los datos.

     Si hay más de 10,000 resultados, sólo aparecen los 10,000 primeros en el informe (más adelante se añadirá compatibilidad con más).

   - **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.

Desactivación de Cloud Compliance

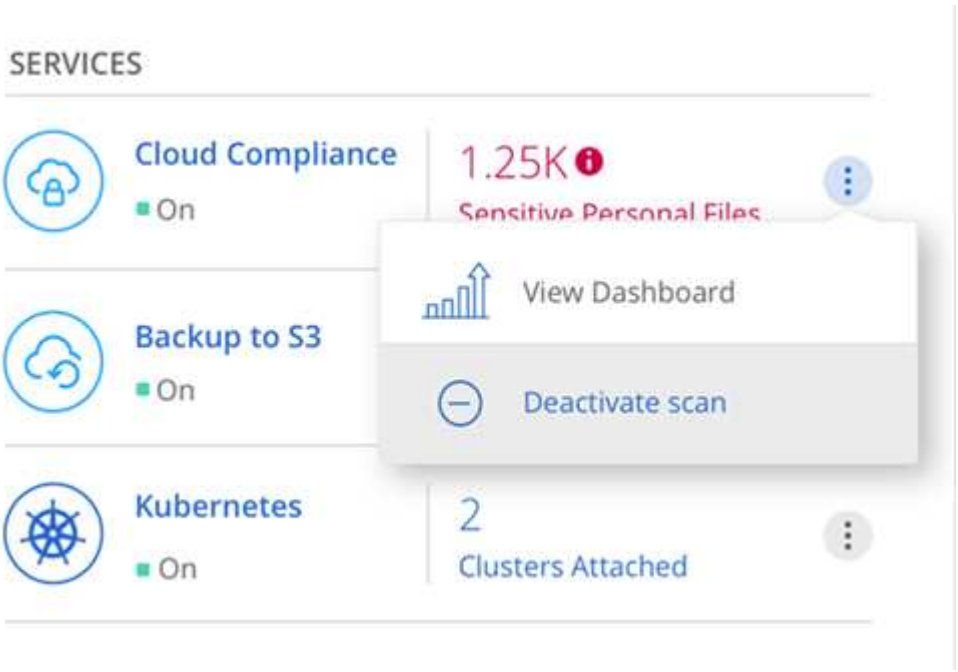
Si lo necesita, puede detener Cloud Compliance de analizar uno o más entornos de trabajo. También puede eliminar la instancia de Cloud Compliance si ya no desea utilizar Cloud Compliance con sus sistemas Cloud Volumes ONTAP.

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 en sí no se eliminan).

Pasos

1. En la parte superior de Cloud Manager, haga clic en **entornos de trabajo**.
2. Seleccione el entorno de trabajo.
3. En el panel derecho, haga clic en el icono de acción del servicio Cloud Compliance y seleccione **Desactivar análisis**.



Eliminación de la instancia de Cloud Compliance

Puede eliminar la instancia de Cloud Compliance si ya no desea utilizar Cloud Compliance con Cloud Volumes ONTAP. 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 nueva oferta de cloud de NetApp. Mediante la tecnología basada en la inteligencia artificial (IA), Cloud Compliance ayuda a las organizaciones a comprender el contexto de los datos e identificar los datos confidenciales en sus sistemas de Cloud Volumes ONTAP alojados en AWS o Azure.

Cloud Compliance ofrece parámetros predefinidos (como tipos y categorías de información confidencial) para abordar nuevas normativas de cumplimiento de normativas de datos en cuanto a privacidad y sensibilidad de los datos, como GDPR, CCPA, 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 y otras normativas de privacidad de 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 permite realizar análisis de datos no estructurados mediante protocolos NFS y CIFS. Actualmente, Cloud Compliance analiza datos gestionados por Cloud Volumes ONTAP.

"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 e instancias de Cloud Volumes ONTAP. A continuación, escanea los datos en Cloud Volumes ONTAP e indexa la información de datos encontrada.

"Más información sobre el funcionamiento de Cloud Compliance".

¿Cuánto cuesta el cumplimiento de las normativas cloud?

Cloud Compliance se ofrece como parte de Cloud Volumes ONTAP y no requiere ningún coste adicional. Es posible que se necesiten costes adicionales en el futuro para lograr funcionalidades personalizadas.

Cloud Compliance requiere la puesta en marcha de una instancia en su proveedor de cloud, para la que su proveedor de cloud le cobrará.

¿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".

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 io1 de 500 GB.

  En regiones donde no hay m5.4xLarge disponible, Cloud Compliance se ejecuta en lugar de una instancia m4.4xLarge.

"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.

¿Cómo hago posible el cumplimiento de normativas para el cloud?

Puede habilitar Cloud Compliance al crear un nuevo entorno de trabajo. Puede activarlo en entornos de trabajo existentes desde la ficha **cumplimiento** (sólo en la primera activación) 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 Cloud Compliance se encuentra actualmente disponible como parte de Cloud Manager y es compatible con Cloud Volumes ONTAP. Tenemos pensado admitir el cumplimiento de normativas cloud con ofertas cloud adicionales como Cloud Volumes Service y Azure NetApp Files.

¿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.

"Leer más".

Administre Cloud Volumes ONTAP

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 de OnCommand

Es posible que deba realizar algunas tareas de Cloud Volumes ONTAP desde OnCommand 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.

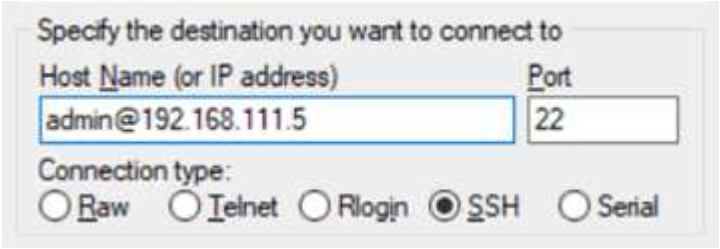
Cuando se implementa en múltiples AZs, las configuraciones de alta disponibilidad de Cloud Volumes ONTAP utilizan una dirección IP flotante para la interfaz de gestión del clúster, lo que significa que el enrutamiento externo no está disponible. Debe conectarse desde un host que forme parte del mismo 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::>
```

Actualización del software Cloud Volumes ONTAP

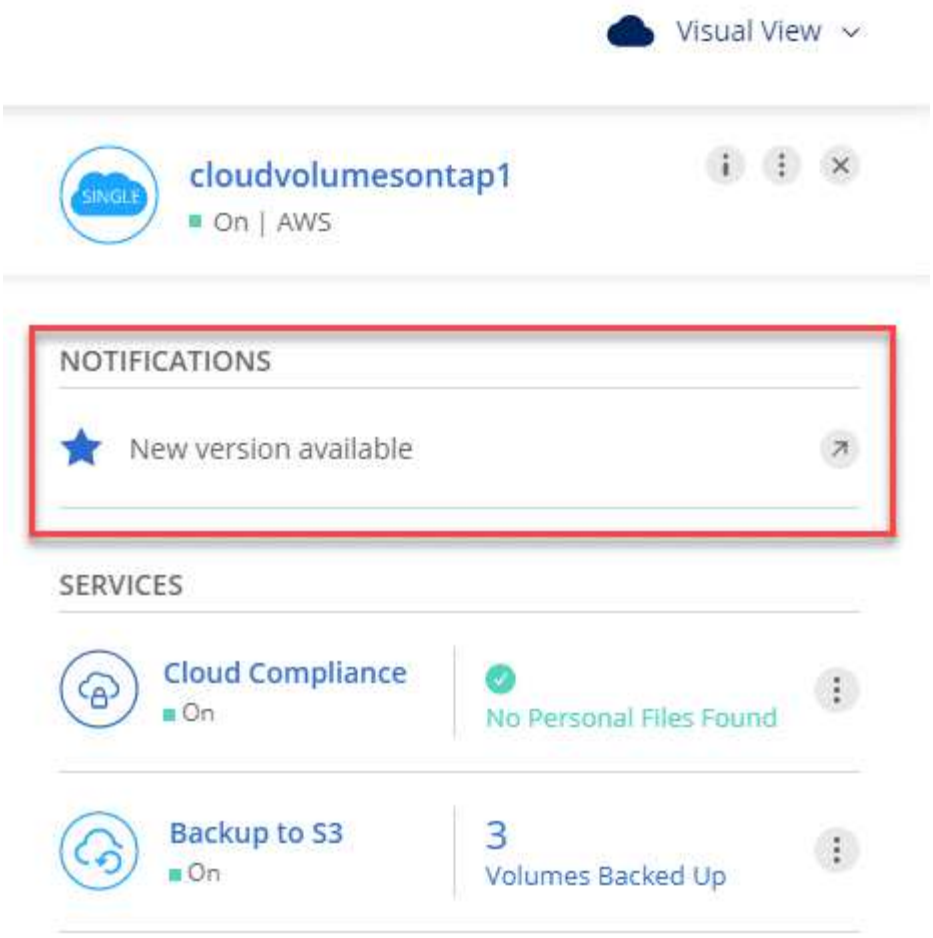
Cloud Manager incluye varias opciones que se pueden utilizar para actualizar a la versión actual de Cloud Volumes ONTAP o degradar Cloud Volumes ONTAP a una versión anterior. Debe preparar los sistemas de Cloud Volumes ONTAP antes de actualizar o degradar el software.

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

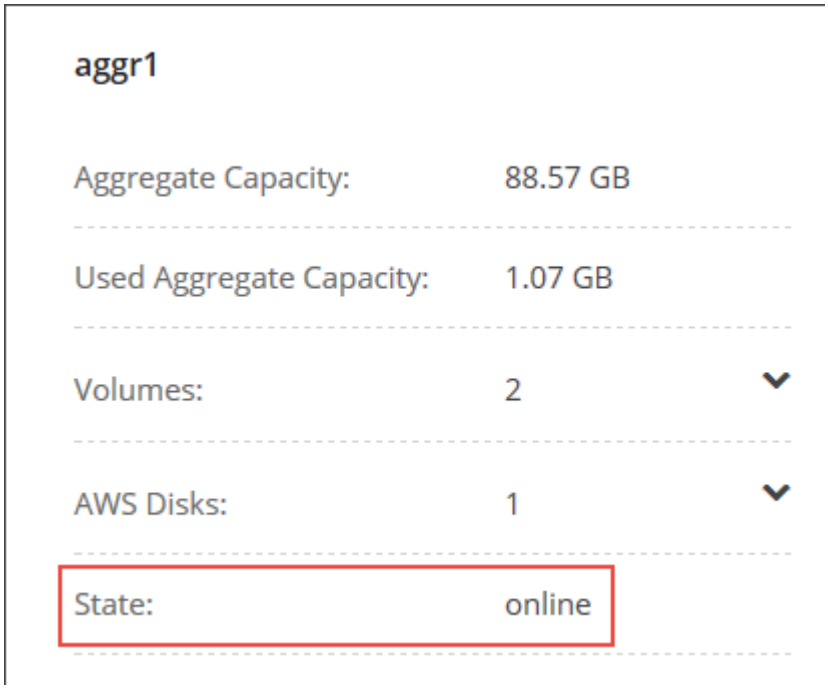
Los agregados para Cloud Volumes ONTAP deben estar en línea antes de actualizar el software. Los agregados deben estar en línea en la mayoría de las configuraciones, pero si no lo están, debe conectarlos conectados.

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.

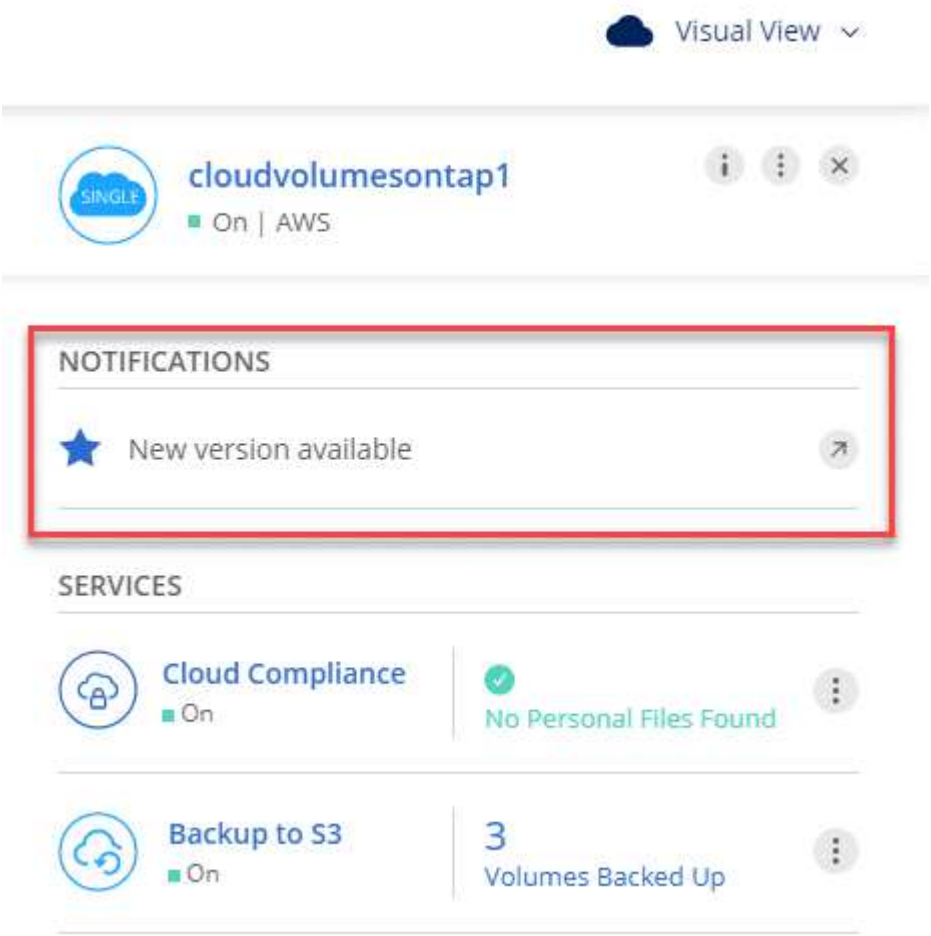
Antes de empezar

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 deba cambiar la configuración de las instancias de Cloud Volumes ONTAP a medida que cambien las necesidades de almacenamiento. Por ejemplo, puede cambiar entre configuraciones de pago por uso, cambiar la instancia o el tipo de equipo virtual y pasar a una suscripción alternativa.

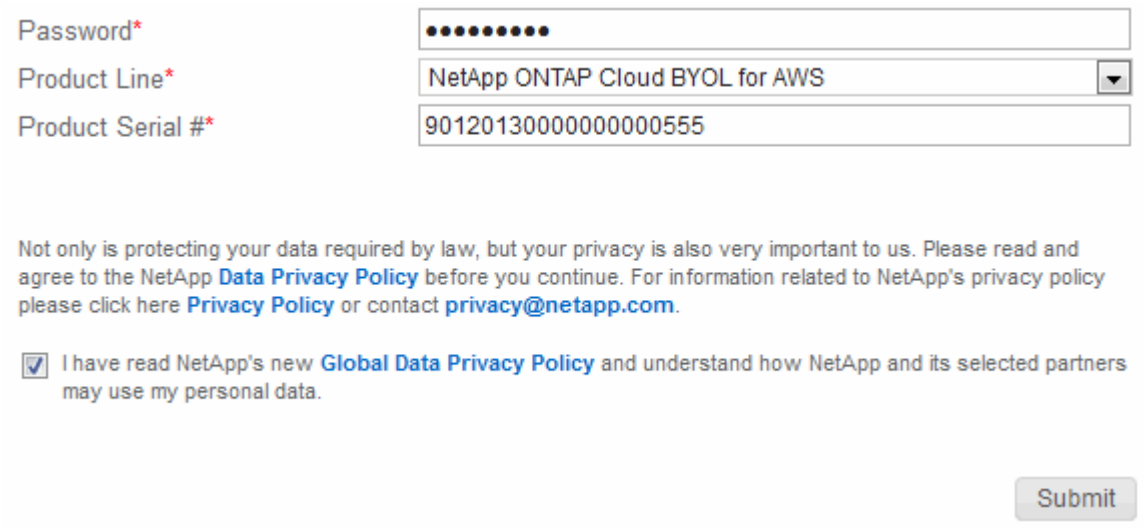
Instalación de archivos de licencia en sistemas BYOL de Cloud Volumes ONTAP

Si Cloud Manager no puede obtener un archivo de licencia de BYOL de NetApp, puede obtener el archivo y cargarlo manualmente a Cloud Manager para que pueda instalar la licencia en el sistema Cloud Volumes ONTAP.

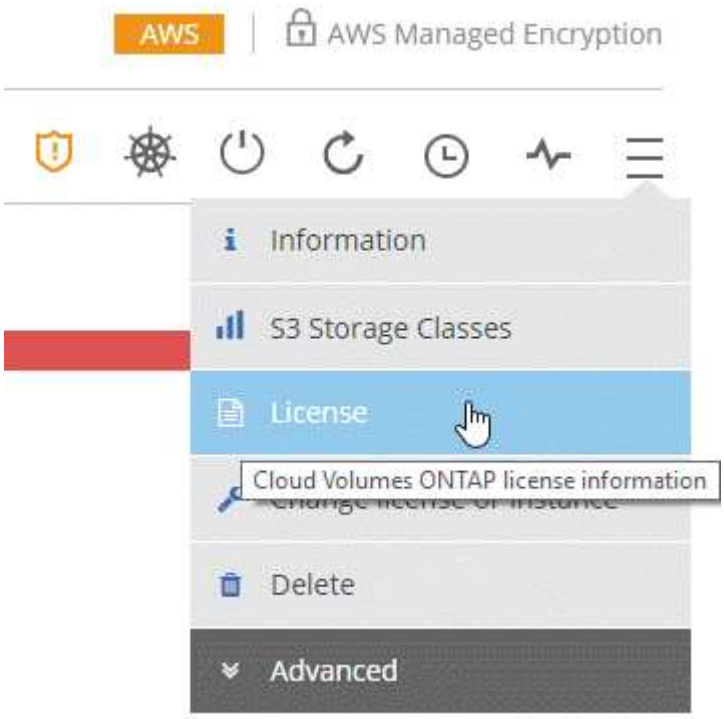
Pasos

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.
4. En Cloud Manager, abra el entorno de trabajo BYOL de Cloud Volumes ONTAP.
5. Haga clic en el icono de menú y, a continuación, haga clic en **Licencia**.



6. Haga clic en **cargar archivo de licencia**.
7. Haga clic en **cargar** y seleccione el archivo.

Resultado

Cloud Manager instala el nuevo archivo de licencia en el sistema Cloud Volumes ONTAP.

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"

- 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. 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 pasar de una suscripción de pago por uso a una suscripción BYOL o entre un único sistema Cloud Volumes ONTAP y un par de alta disponibilidad, puede poner en marcha un nuevo sistema y replicar los datos, a continuación, 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".

Cambiar su suscripción a AWS Marketplace

Cambie la suscripción a AWS Marketplace para su sistema Cloud Volumes ONTAP si desea cambiar la cuenta de AWS desde la que se cobra.

Pasos

1. Si aún no lo ha hecho, añada una nueva suscripción de "La oferta de Cloud Manager en el mercado de AWS".
2. En el entorno de trabajo de Cloud Manager, haga clic en el icono de menú y, a continuación, haga clic en **Suscripción de Marketplace**.
3. Seleccione una suscripción de la lista desplegable.
4. Haga clic en **Guardar**.

Cambio de la velocidad de escritura a normal o alta

La velocidad de escritura predeterminada para las Cloud Volumes ONTAP 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.

  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.

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.

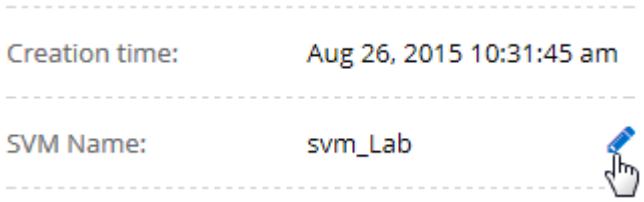
3. Haga clic en **Guardar**, revise el mensaje de confirmación y, a continuación, haga clic en **proseguir**.

Modificación del nombre de la máquina virtual de almacenamiento

Cloud Manager nombra automáticamente a la máquina virtual de almacenamiento (SVM) para Cloud Volumes ONTAP. Puede modificar el nombre de la SVM si tiene estándares de nomenclatura estrictos. Por ejemplo, puede que desee que coincida con el nombre que le tienen las SVM de los clústeres de ONTAP.

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 SVM.



3. En el cuadro de diálogo Modify SVM Name (Modificar nombre de SVM), modifique el nombre de SVM y, a continuación, haga clic en **Save** (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.

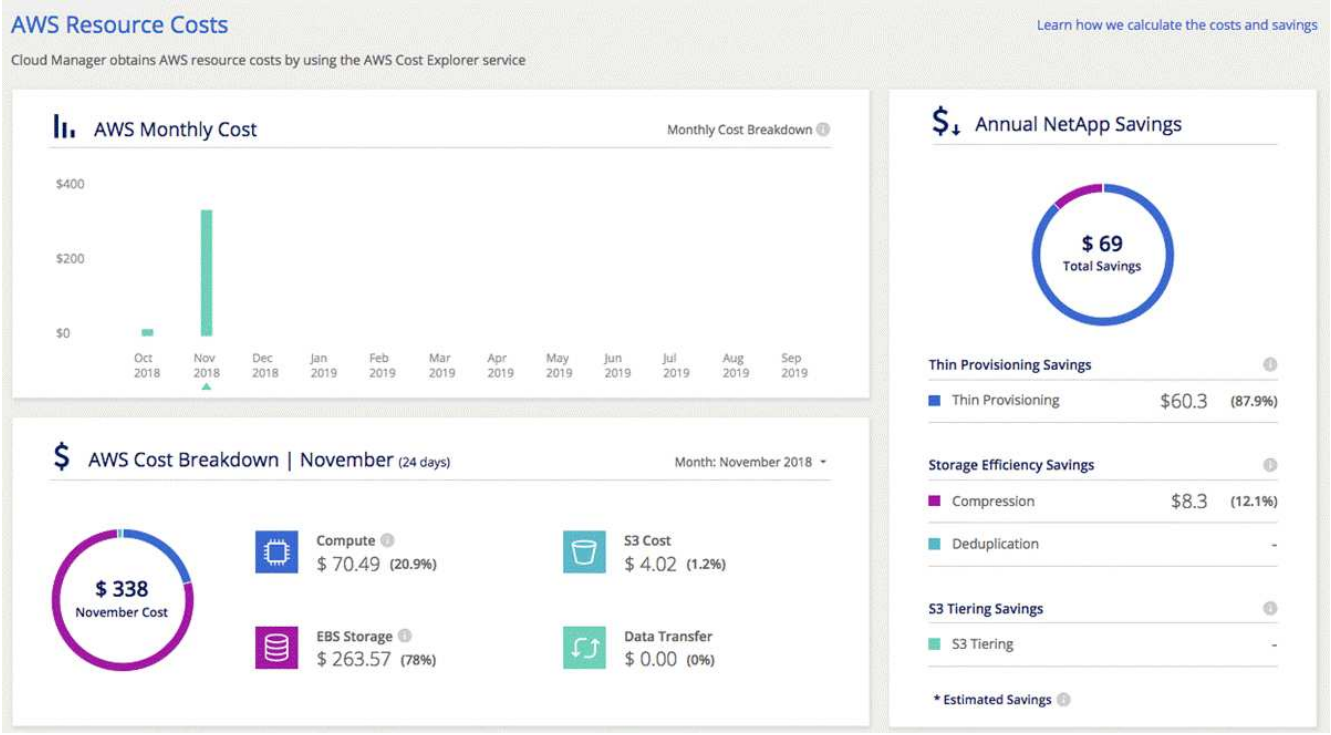
   b. "Active la etiqueta **WorkingEnvironmentId**".

      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:

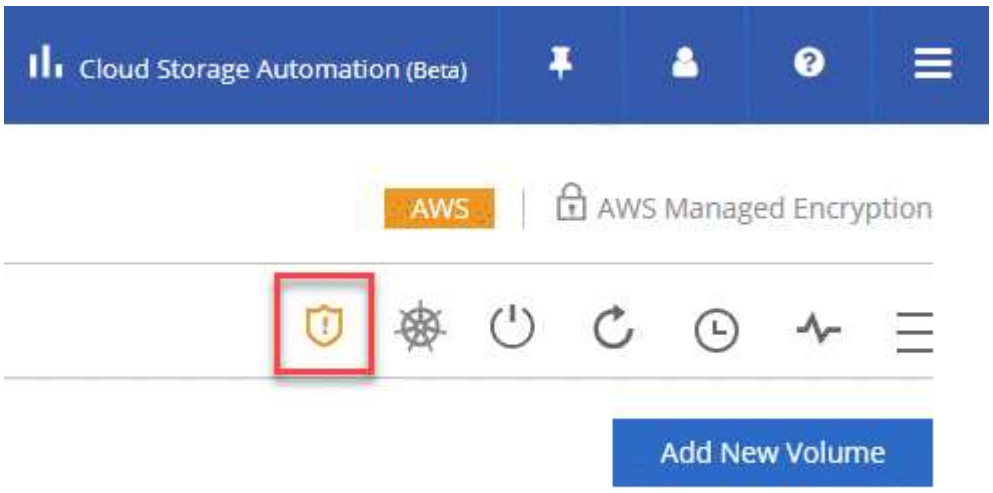


Mejorar la protección contra el ransomware

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**.

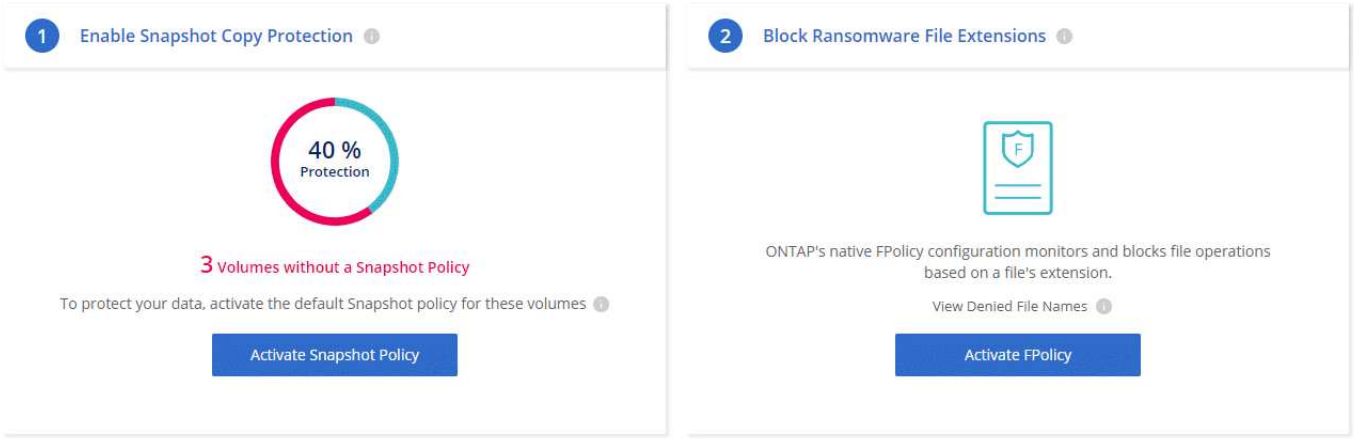


2. Implemente la solución de NetApp para ransomware:
   a. Haga clic en **Activar política de instantánea** si tiene volúmenes que no tienen activada una directiva de instantánea.

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.



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 **descubrir** y seleccione **Cloud Volumes ONTAP**.
2. Seleccione el proveedor de cloud en el que reside el sistema.
3. En la página Región, seleccione la región donde se ejecutan las instancias y, a continuación, seleccione las instancias.
4. 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.

Administre Cloud Manager

Actualizando Cloud Manager

Puede actualizar Cloud Manager a la versión más reciente o con un parche que haya compartido el personal de NetApp.

Activación de actualizaciones automáticas

Cloud Manager se puede actualizar automáticamente cuando haya una nueva versión disponible. Esto garantiza que esté ejecutando la última versión.

Acerca de esta tarea

Cloud Manager se actualiza automáticamente a las 12:00 si no hay operaciones en ejecución.

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. Seleccione la casilla de verificación en actualizaciones automáticas de Cloud Manager y, a continuación, haga clic en **Guardar**.

Actualizar Cloud Manager a la versión más reciente

Debe activar actualizaciones automáticas en Cloud Manager, pero siempre puede realizar una actualización manual directamente desde la consola web. Cloud Manager obtiene la actualización de software de un bloque de S3 propiedad de NetApp en AWS.

Antes de empezar

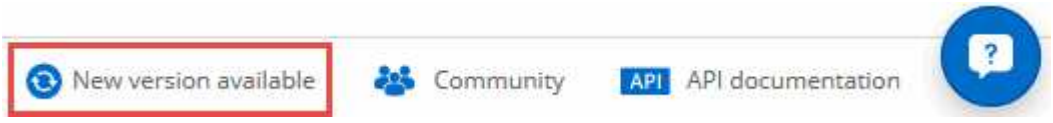
Usted debería haber revisado "novedades de la versión" identificar nuevos requisitos y cambios en el soporte técnico.

Acerca de esta tarea

La actualización del software tarda unos minutos. Cloud Manager no estará disponible durante la actualización.

Pasos

1. Compruebe si hay una nueva versión disponible en la esquina inferior derecha de la consola:



2. Si hay una nueva versión disponible, haga clic en **línea de tiempo** para determinar si hay alguna tarea en curso.

   Si hay alguna tarea en curso, espere a que finalicen antes de continuar con el siguiente paso.

3. En la parte inferior derecha de la consola, haga clic en **Nueva versión disponible**.
4. En la página actualización del software de Cloud Manager, haga clic en **Actualizar** junto a la versión que desee.

5. Complete el cuadro de diálogo de confirmación y, a continuación, haga clic en **Aceptar**.

Resultado

Cloud Manager inicia el proceso de actualización. Puede iniciar sesión en la consola transcurridos unos minutos.

Actualizar Cloud Manager con un parche

Si NetApp ha compartido un parche con usted, puede actualizar Cloud Manager con el parche suministrado directamente desde la consola web de Cloud Manager.

Acerca de esta tarea

La actualización del parche suele tardar unos minutos. Cloud Manager no estará disponible durante la actualización.

Pasos

1. En la parte superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **actualización de software**.

2. Haga clic en el enlace para actualizar Cloud Manager con el parche suministrado.

3. Complete el cuadro de diálogo de confirmación y, a continuación, haga clic en **Aceptar**.
4. Seleccione el parche que ha proporcionado.

Resultado

Cloud Manager aplica el parche. Puede iniciar sesión en la consola transcurridos unos minutos.

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

"Después de realizar la configuración inicial", es posible que necesite administrar posteriormente usuarios, espacios de trabajo y conectores de servicios.

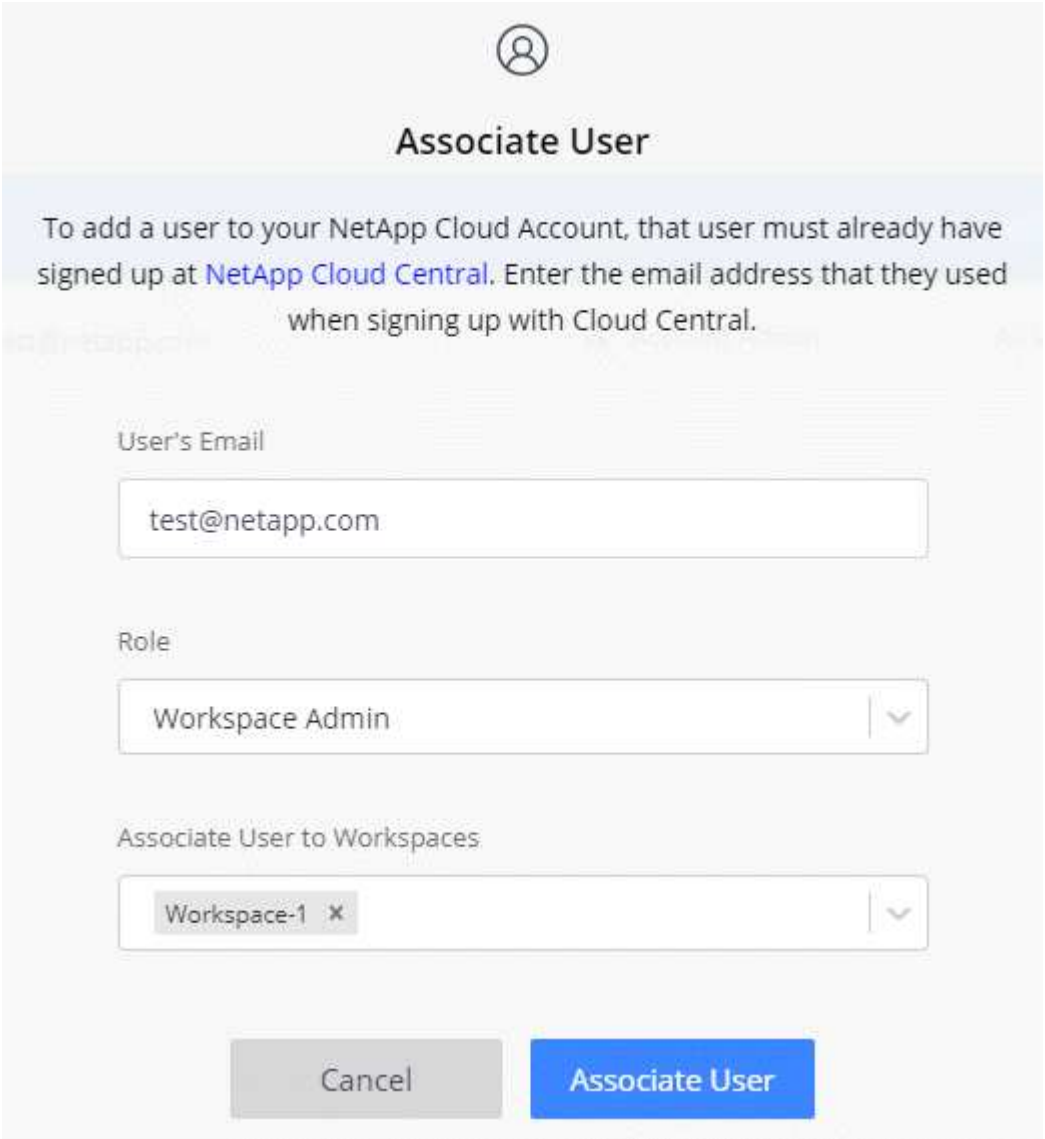
"Obtenga más información sobre cómo funcionan las cuentas de Cloud Central".

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 crear una cuenta.
2. En Cloud Manager, haga clic en **Configuración de 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.
5. Si ha seleccionado Administrador de área de trabajo, seleccione una o más áreas de trabajo para asociarlas a 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.

Resultado

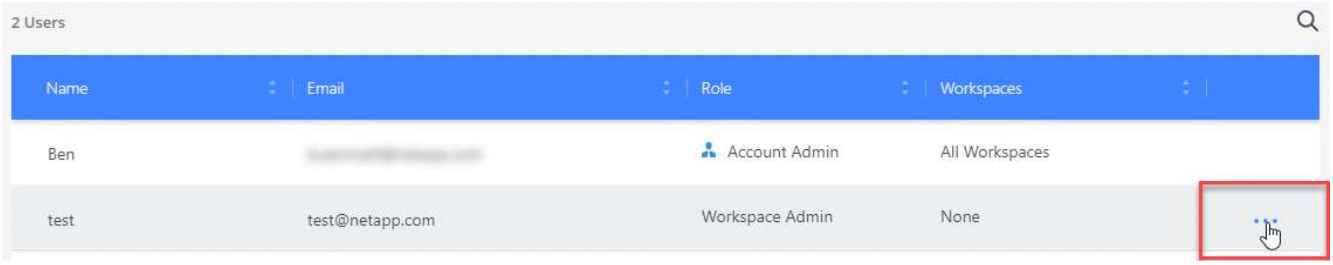
El usuario debe recibir un correo electrónico de Cloud Central de NetApp titulado "Account Association". El correo electrónico incluye la información necesaria para acceder a Cloud Manager.

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. Haga clic en **Configuración de cuenta**.
2. Haga clic en el menú de acción de la fila correspondiente al usuario.



3. Haga clic en **desasociar usuario** y haga clic en **desasociar** para confirmar.

Resultado

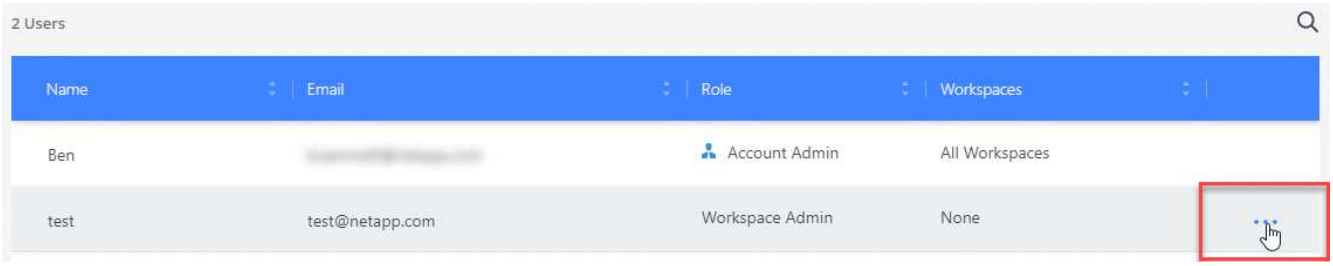
El usuario ya no puede acceder a los recursos de esta cuenta de Cloud Central.

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. Haga clic en **Configuración de cuenta**.
2. Haga clic en el menú de 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 estos espacios de trabajo desde Cloud Manager, siempre y cuando el conector del servicio 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. Haga clic en **Configuración de 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 de servicio

Debe asociar el conector de servicio a espacios de trabajo para que los administradores de Workspace puedan acceder a estos espacios de trabajo desde Cloud Manager.

Si sólo tiene Administradores de cuentas, no es necesario asociar el conector de servicio 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, espacios de trabajo y conectores de servicio".

Pasos

1. Haga clic en **Configuración de cuenta**.
2. Haga clic en **Service Connector**.
3. Haga clic en **Administrar áreas de trabajo** para el conector de servicio que desea asociar.
4. Seleccione las áreas de trabajo que desea asociar con el conector de servicio y haga clic en **aplicar**.

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 Cloud Manager para usar un servidor proxy

Al implementar Cloud Manager por primera vez, se le solicita que introduzca un servidor proxy si el sistema no tiene acceso a Internet. También puede introducir y modificar manualmente el proxy desde la configuración de Cloud Manager.

Acerca de esta tarea

Si sus directivas corporativas dictan que utiliza un servidor proxy para todas las comunicaciones HTTP a Internet, debe configurar Cloud Manager para que utilice ese servidor proxy. El servidor proxy puede estar en la nube o en la red.

Al configurar Cloud Manager para que utilice un servidor proxy, Cloud Manager, Cloud Volumes ONTAP y el mediador de alta disponibilidad utilizan el servidor proxy.

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 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 especifica el servidor proxy antes de que los usuarios creen sistemas Cloud Volumes ONTAP, deben usar System Manager para establecer manualmente el servidor proxy en las opciones de AutoSupport para cada sistema.

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.

Restaurando Cloud Manager

Su "Cuenta de Cloud Central de NetApp" Le facilita la restauración de una configuración de Cloud Manager. La cuenta es un servicio que se ejecuta en Cloud Central, por lo que los usuarios, espacios de trabajo y conectores de servicio que ha asociado a la cuenta siempre están accesibles. Incluso si su sistema Cloud Manager se eliminó por accidente.

A partir de la versión 3.7.1, Cloud Manager ya no admite la descarga de un backup y su uso para restaurar la configuración. Debe seguir estos pasos para restaurar Cloud Manager.

Pasos

1. Implemente un nuevo sistema Cloud Manager en su cuenta actual de Cloud Central.

   "Opciones de puesta en marcha"

2. Añada sus cuentas de proveedores de cloud y las cuentas del sitio de soporte de NetApp a Cloud Manager.

   Con este paso, estará preparado Cloud Manager para que pueda crear sistemas Cloud Volumes ONTAP adicionales en su proveedor de cloud.

   Es importante completar este paso si utilizó claves AWS para implementar un sistema Cloud Volumes ONTAP existente que desea detectar en este nuevo sistema Cloud Manager. Cloud Manager necesita las claves de AWS para detectar y gestionar correctamente Cloud Volumes ONTAP.

   - "Añadiendo cuentas de AWS a Cloud Manager"
   - "Adición de cuentas de Azure a Cloud Manager"

- "Adición de cuentas del sitio de soporte de NetApp a Cloud Manager"

3. Redescubra sus entornos de trabajo: Sistemas Cloud Volumes ONTAP, clústeres en las instalaciones y almacenamiento privado de NetApp para configuraciones cloud.
   - "Adición de sistemas de Cloud Volumes ONTAP existentes a Cloud Manager"
   - "Detección de clústeres de ONTAP"

Resultado

La configuración de Cloud Manager ahora se restaura con sus cuentas, ajustes y entornos de trabajo.

Desinstalando Cloud Manager

Cloud Manager incluye un script de desinstalación que puede utilizar para desinstalar el software para resolver problemas o quitar de forma permanente el software del host.

Pasos

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.

Aprovisionamiento de volúmenes para los servicios de archivos

Gestionar volúmenes para Azure NetApp Files

Consulte y cree volúmenes NFS para "Azure NetApp Files" Directamente de Cloud Manager.

Configuración

Su configuración debe cumplir unos pocos requisitos antes de poder gestionar los volúmenes para Azure NetApp Files en Cloud Manager.

1. La configuración de Azure NetApp Files debe realizarse completando los siguientes pasos del portal de Azure:
   - "Regístrese para Azure NetApp Files"
   - "Cree una cuenta de NetApp"
   - "Configure un pool de capacidad"
   - "Delegar una subred en Azure NetApp Files"
2. Cloud Manager debe configurarse del siguiente modo:
   - Cloud Manager debe ejecutarse en Azure, en la cuenta en la que se configuró Azure NetApp Files.
   - La máquina virtual de Cloud Manager debe recibir permisos a través de un "identidad administrada".

     Si implementó Cloud Manager desde Cloud Central, estará todo listo. Cloud Central activa automáticamente una identidad administrada asignada por el sistema en la máquina virtual de Cloud Manager.

   Si implementó Cloud Manager desde Azure Marketplace, debe haber seguido "instrucciones para habilitar una identidad administrada".

   - El rol de Azure asignado a la máquina virtual de Cloud Manager debe incluir los permisos indicados en el más reciente "Política de Cloud Manager para Azure":

```
"Microsoft.NetApp/netAppAccounts/read",
"Microsoft.NetApp/netAppAccounts/capacityPools/read",
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete"
```

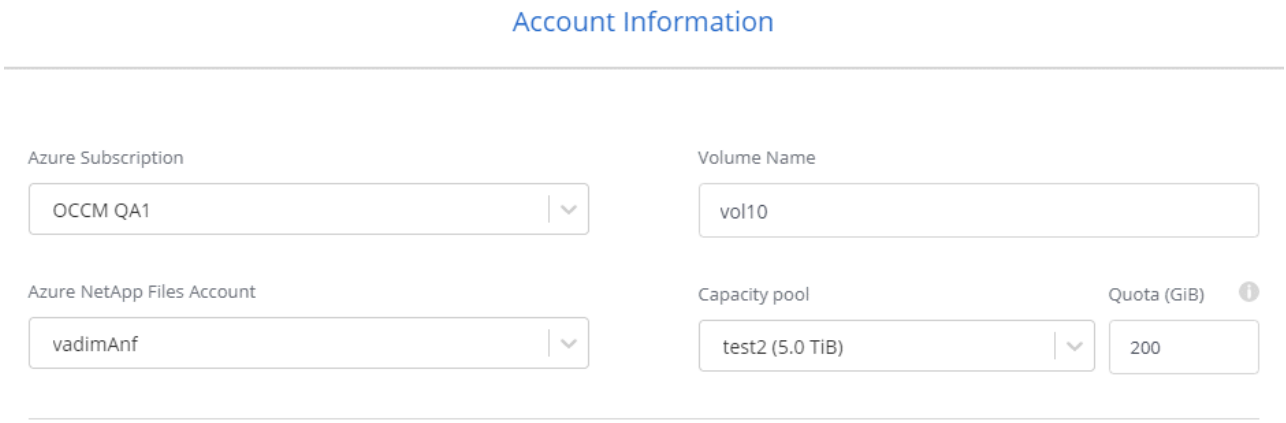
Una vez configurada la configuración, Cloud Manager muestra automáticamente Azure NetApp Files en la página entornos de trabajo:

Crear volúmenes

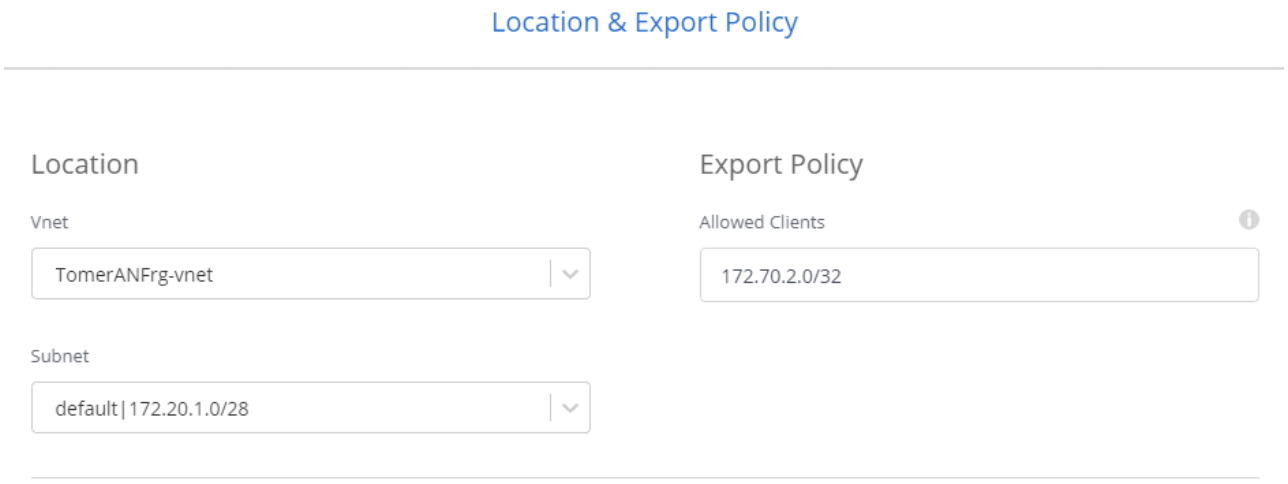
Cloud Manager le permite crear volúmenes NFSv3 para Azure NetApp Files.

Pasos

1. Abra el entorno de trabajo.
2. Haga clic en **Añadir nuevo volumen**.
3. Introduzca los detalles básicos sobre el volumen en la página **Información de cuenta**:
   a. Seleccione una suscripción de Azure y una cuenta de Azure NetApp Files.
   b. Escriba un nombre para el volumen.
   c. Seleccione un pool de capacidad y especifique una cuota, que es la cantidad de almacenamiento lógico asignado al volumen.



4. Rellene la página **Política de ubicación y exportación**:
   a. Seleccione una vnet y una subred.
   b. Configure una política de exportación para controlar el acceso al volumen.



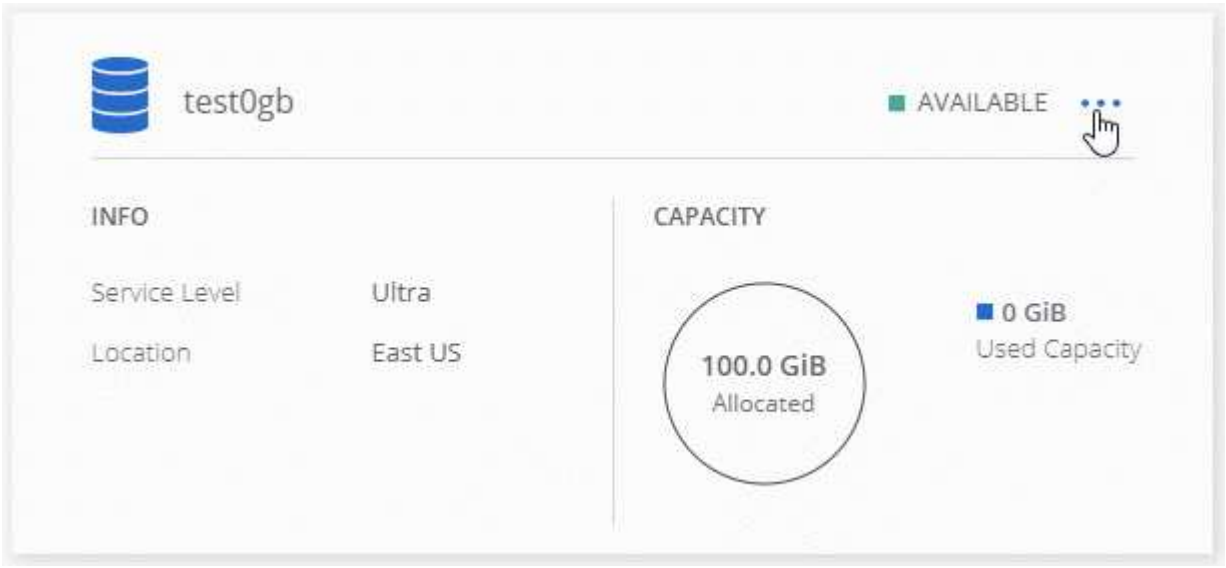
5. Haga clic en **Ir**.

Obtener la ruta de montaje de un volumen

Copie la ruta de montaje de un volumen para que pueda montar el volumen en un equipo Linux.

Pasos

1. Abra el entorno de trabajo.
2. Pase el ratón sobre el volumen y haga clic en el menú.



3. Haga clic en **comando de montaje**.

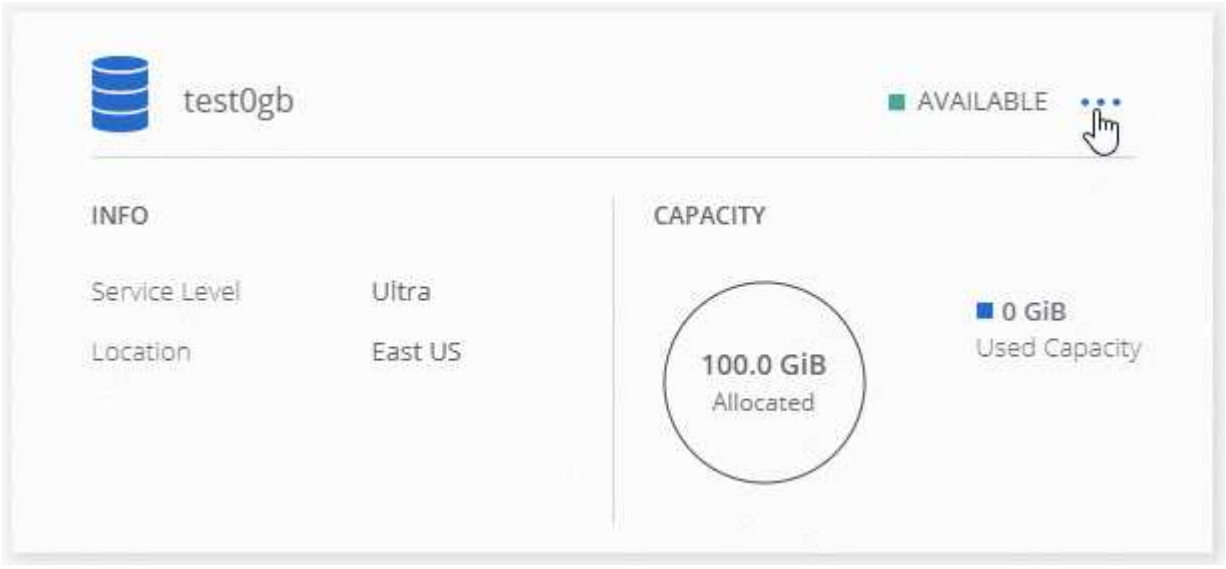
4. Copie la ruta de montaje y utilice el texto copiado para montar el volumen en un equipo Linux.

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 el menú.



3. Haga clic en **Eliminar**.
4. Confirme que desea eliminar el volumen.

Obtener ayuda

Use el chat de Cloud Manager para formular preguntas generales de servicio.

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.

Cloud Manager ofrece una descarga local de AutoSupport en la opción de menú **Panel de soporte**. Este archivo 7z contiene un archivo de depuración de Azure para mostrar comunicación entrante y saliente a su cuenta de Azure NetApp Files.

Limitaciones

- Cloud Manager no es compatible con SMB Volumes.
- Cloud Manager no le permite gestionar pools de capacidad ni snapshots de volúmenes.
- Se pueden crear volúmenes con un tamaño inicial y una única política de exportación. La edición de un volumen debe realizarse desde la interfaz de Azure NetApp Files en el portal de Azure.
- Cloud Manager no es compatible con la replicación de datos desde o hacia Azure NetApp Files.

Enlaces relacionados

- "Cloud Central de NetApp: Azure NetApp Files"
- "Documentación de Azure NetApp Files"

Gestionar Cloud Volumes Service para AWS

Cloud Manager le permite detectar los volúmenes de cloud NFS de su "Cloud Volumes Service para AWS" suscripción. Después de la detección, puede añadir volúmenes cloud de NFS adicionales directamente desde Cloud Manager.

Cloud Manager no es compatible con volúmenes SMB ni con dos protocolos con Cloud Volumes Service para AWS.

Antes de empezar

- Cloud Manager permite descubrir suscripciones de *existing* 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 y aprovisionar el primer volumen desde Cloud Volumes Service antes de poder detectar la región 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".

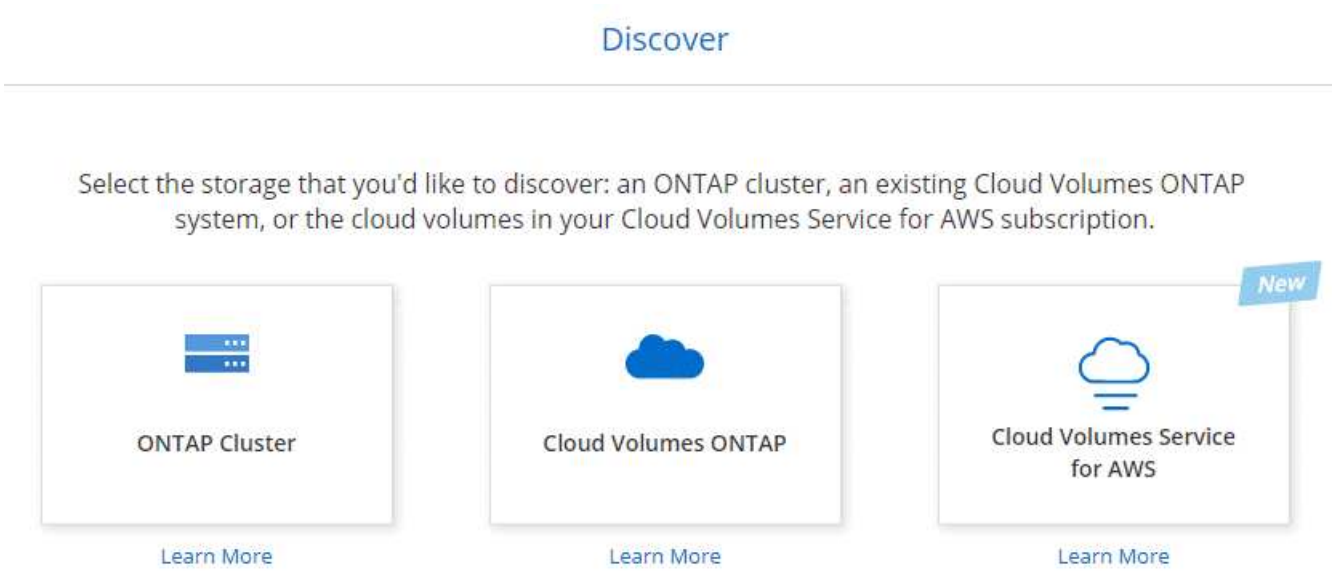
Descubrir la suscripción a Cloud Volumes Service para AWS

Para comenzar, debe detectar los volúmenes de cloud en una región de AWS. Posteriormente, podrá descubrir otras regiones.

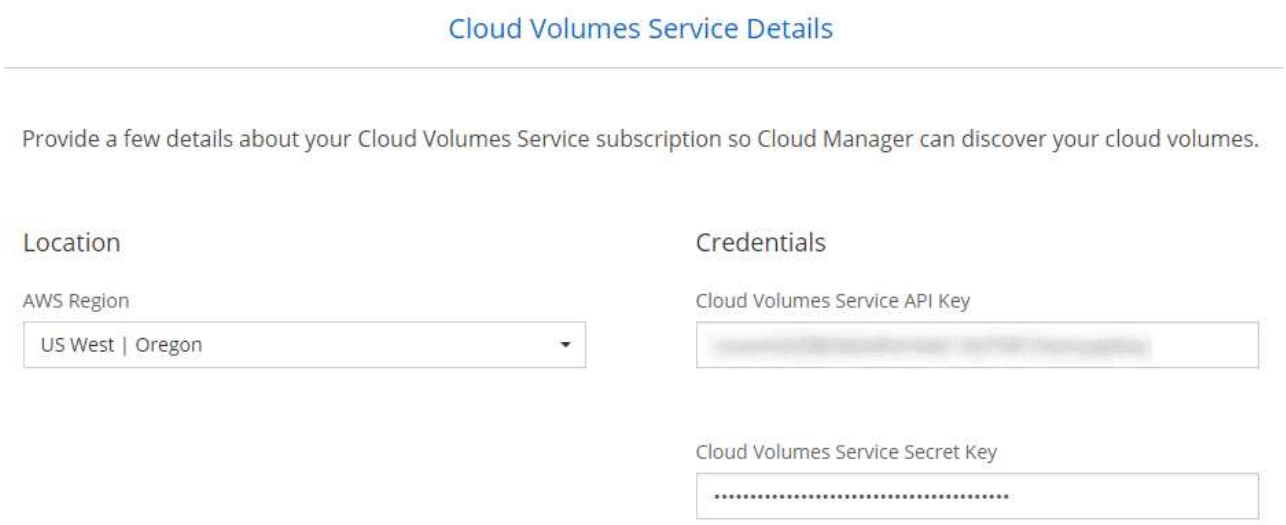
Pasos

1. En la página entornos de trabajo, haga clic en **Discover**.

2. Seleccione **Cloud Volumes Service para AWS**.



3. Proporcione información sobre su suscripción a Cloud Volumes Service:
   a. Seleccione la región de AWS donde residen los volúmenes de cloud.
   b. Introduzca la clave de API de Cloud Volumes y la clave secreta. "Para obtener instrucciones, consulte la documentación de Cloud Volumes Service para AWS".
   c. Haga clic en **Ir**.



Resultado

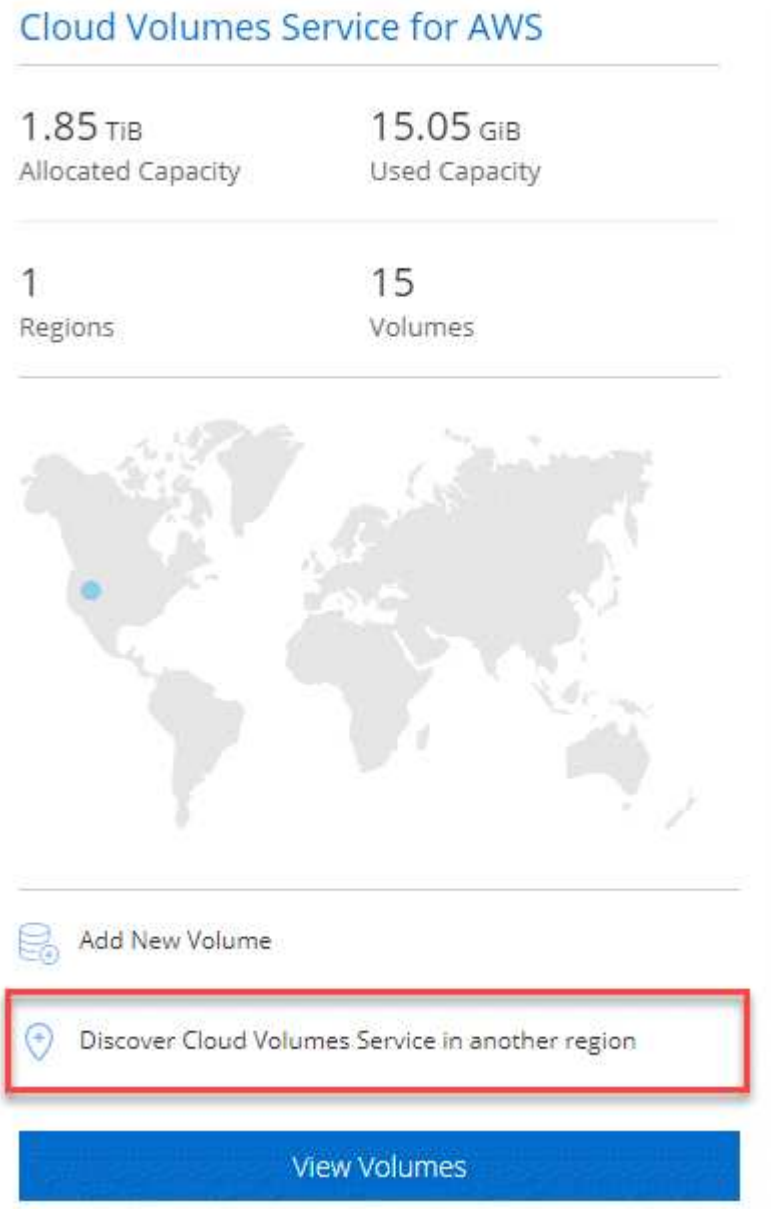
Cloud Manager ahora debe mostrar su configuración de Cloud Volumes Service para AWS en la página entornos de trabajo.

Descubrir otras regiones

Si tiene volúmenes de cloud en regiones adicionales, debe descubrir cada región individual.

Pasos

1. En la página entornos de trabajo, seleccione el entorno de trabajo (pero no lo abra haciendo doble clic).
2. En el panel derecho, haga clic en **descubrir Cloud Volumes Service en otra región**.



3. Proporcione información sobre su suscripción a Cloud Volumes Service:
   a. Seleccione la región de AWS donde residen los volúmenes de cloud.
   b. Introduzca la clave de API de Cloud Volumes y la clave secreta. "Para obtener instrucciones, consulte la documentación de Cloud Volumes Service para AWS".
   c. Haga clic en **Ir**.

Resultado

Cloud Manager detecta información sobre los volúmenes de cloud en la región seleccionada.

Creando volúmenes de cloud

Cloud Manager le permite crear volúmenes cloud NFSv3. Solo puede crear volúmenes de cloud con un tamaño inicial y una única política de exportación. La edición del volumen debe realizarse desde la interfaz de usuario de Cloud Volume Service.

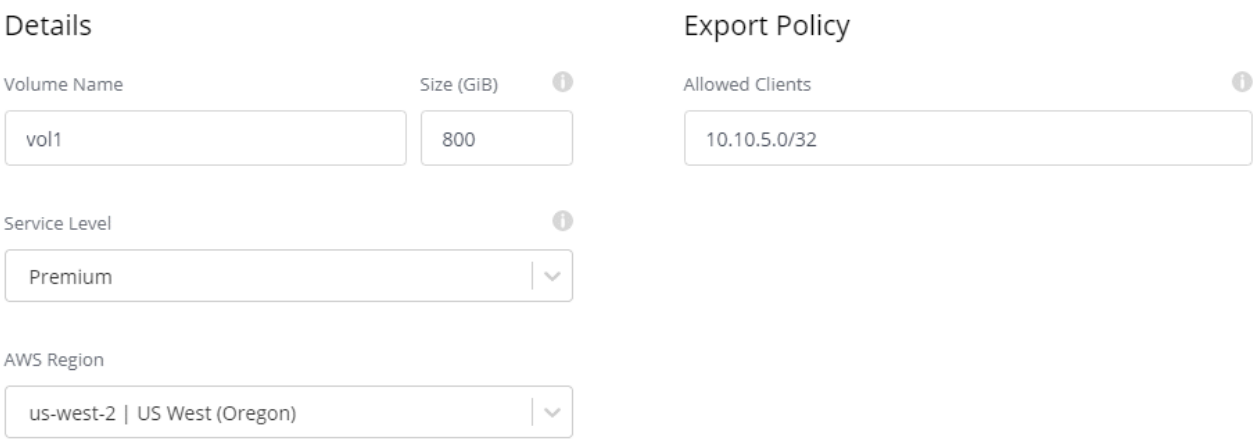
1. Abra el entorno de trabajo.
2. Haga clic en **Añadir nuevo volumen**.
3. Introduzca detalles sobre el volumen:
   a. Escriba un nombre para el volumen.
   b. Especifique un tamaño dentro del intervalo de 100 GIB a 90,000 GIB (equivalente a 88 TIBs).

      Cloud Manager muestra los volúmenes en GIB, mientras que Cloud Volumes Service muestra los volúmenes en GB.

   c. Especifique un nivel de servicio: Standard, Premium o Extreme.

      "Obtenga más información sobre estos niveles de servicio".

   d. Seleccione una región. Es posible crear el volumen en una región que se detectó Cloud Manager.
   e. Restrinja el acceso del cliente especificando una dirección IP o Ruta entre dominios sin clase (CIDR).



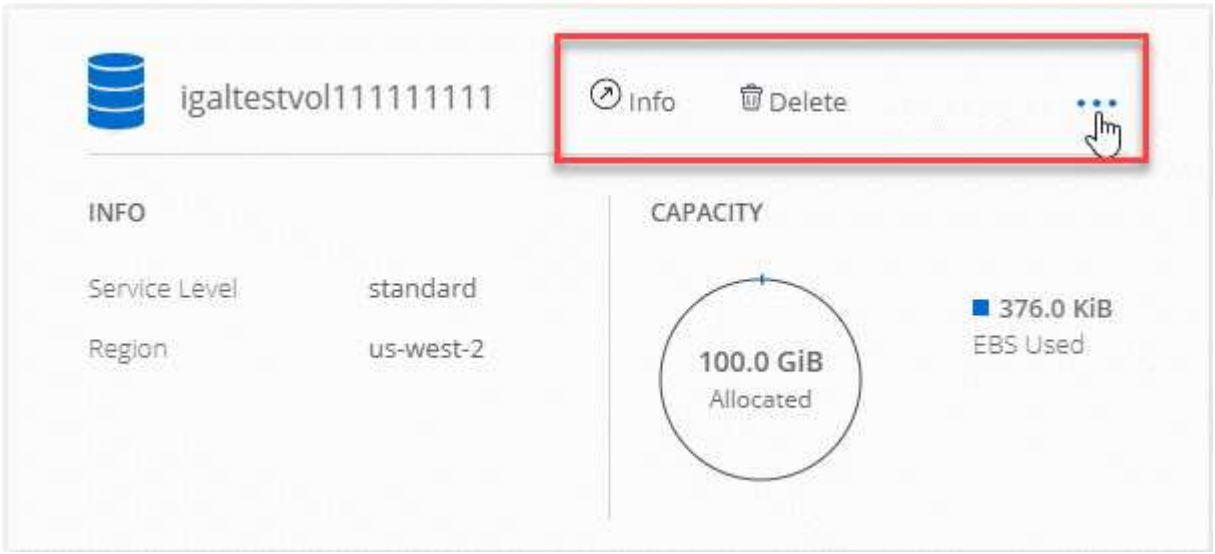
4. Haga clic en **Ir**.

Eliminación de volúmenes en cloud

Elimine los volúmenes de cloud que ya no necesita.

Pasos

1. Abra el entorno de trabajo.
2. Pase el ratón sobre el volumen y haga clic en el menú. Haga clic en **Eliminar**.



3. Confirme que desea eliminar el volumen.

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 es compatible con volúmenes con SMB ni con protocolo doble.
- Solo puede crear volúmenes de cloud con un tamaño inicial y una única política de exportación. La edición del volumen debe realizarse desde la interfaz de usuario de Cloud Volume Service.
- Cloud Manager no admite replicación de datos en una suscripción de Cloud Volumes Service para AWS ni desde ella.
- No es posible eliminar su suscripción a Cloud Volumes Service para AWS desde Cloud Manager. Cloud Manager no es necesario pagar solo por descubrir una región.

Enlaces relacionados

- "NetApp Cloud Central: Cloud Volumes Service para AWS"
- "Documentación de Cloud Volumes Service de NetApp para AWS"

API y automatización

Muestras 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. Dos de estas herramientas son Ansible y Terraform. Hemos desarrollado muestras de Ansible y Terraform que el equipo de DevOps puede usar con Cloud Manager para automatizar e integrar Cloud Volumes ONTAP con la infraestructura como código.

"Vea las muestras de automatización".

Por ejemplo, puede usar libros de estrategia de Ansible de muestra para poner en marcha Cloud Manager y Cloud Volumes ONTAP, crear un agregado y crear un volumen. Modifique las muestras para su entorno o cree nuevos libros de estrategia basados en las muestras.

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"

Referencia

Preguntas frecuentes: Integración de Cloud Manager con NetApp Cloud Central

Al actualizar desde Cloud Manager 3.4 o una versión anterior, NetApp elegirá sistemas de Cloud Manager específicos para integrarse con Cloud Central de NetApp, si no están ya integrados. Estas preguntas frecuentes pueden responder a las preguntas que pueda tener sobre el proceso.

¿Qué es Cloud Central de NetApp?

Cloud Central de NetApp proporciona una ubicación centralizada para acceder y gestionar los servicios de datos en el cloud de NetApp. Estos servicios le permiten ejecutar aplicaciones críticas en el cloud, crear sitios de recuperación ante desastres automatizados, realizar backups de sus datos SaaS y migrar y controlar datos de forma efectiva entre varios clouds.

¿Por qué integra NetApp mi sistema Cloud Manager con Cloud Central?

La integración de Cloud Manager con Cloud Central de NetApp ofrece varias ventajas, como una experiencia de implementación simplificada, una única ubicación para ver y gestionar varios sistemas de Cloud Manager y una autenticación de usuario centralizada.

¿Qué ocurre durante el proceso de integración?

NetApp migra todas las cuentas de usuario locales del sistema Cloud Manager a la autenticación de usuario centralizada disponible en Cloud Central.

¿Cómo funciona la autenticación de usuarios centralizada?

Con la autenticación de usuarios centralizada, puede usar el mismo conjunto de credenciales en los sistemas de Cloud Manager y entre Cloud Manager y otros servicios de datos, como Cloud Sync. También es fácil restablecer la contraseña si la olvida.

¿Debo inscribirme en una cuenta de usuario de Cloud Central?

NetApp creará una cuenta de usuario de Cloud Central para usted cuando integremos su sistema Cloud Manager con Cloud Central. Sólo tiene que restablecer su contraseña para completar el proceso de registro.

¿Qué ocurre si ya tengo una cuenta de usuario de Cloud Central?

Si la dirección de correo electrónico que utiliza para iniciar sesión en Cloud Manager coincide con la dirección de correo electrónico de una cuenta de usuario de Cloud Central, puede iniciar sesión directamente en el sistema Cloud Manager.

¿Qué sucede si mi sistema Cloud Manager tiene varias cuentas de usuario?

NetApp migra todas las cuentas de usuario locales a cuentas de usuario de Cloud Central. Cada usuario necesita restablecer su contraseña.

¿Qué sucede si tengo una cuenta de usuario que utiliza la misma dirección de correo electrónico en varios sistemas de Cloud Manager?

Sólo tiene que restablecer su contraseña una vez y, a continuación, puede utilizar la misma cuenta de usuario de Cloud Central para iniciar sesión en cada sistema de Cloud Manager.

¿Qué ocurre si mi cuenta de usuario local utiliza una dirección de correo electrónico no válida?

Para restablecer la contraseña es necesario disponer de una dirección de correo electrónico válida. Póngase en contacto con nosotros a través del icono de chat disponible en la parte inferior derecha de la interfaz de Cloud Manager.

¿Qué sucede si cuento con secuencias de comandos de automatización para las API de Cloud Manager?

Todas las API son compatibles con versiones anteriores. Deberá actualizar los scripts que utilizan contraseñas, si cambia la contraseña cuando la restablezca.

¿Qué sucede si mi sistema Cloud Manager utiliza LDAP?

Si su sistema utiliza LDAP, NetApp no puede integrar automáticamente el sistema con Cloud Central. Debe realizar manualmente los siguientes pasos:

1. Ponga en marcha un nuevo sistema Cloud Manager desde "Cloud Central de NetApp".
2. "Configure LDAP con el nuevo sistema".
3. "Descubra los sistemas Cloud Volumes ONTAP existentes" Del nuevo sistema Cloud Manager.
4. Elimine el sistema Cloud Manager antiguo.

¿Importa dónde he instalado mi sistema Cloud Manager?

No NetApp integrará sistemas con Cloud Central sin importar dónde residan, ya sea en AWS, Azure o en sus instalaciones.

La única excepción es el entorno de servicios de cloud comercial de AWS.

Reglas de grupos de seguridad para AWS

Cloud Manager crea grupos de seguridad de AWS que incluyen las reglas entrantes y salientes que Cloud Manager y Cloud Volumes ONTAP deben operar correctamente. Tal vez desee consultar los puertos para fines de prueba o si prefiere utilizar sus propios grupos de seguridad.

Reglas para Cloud Manager

El grupo de seguridad para Cloud Manager requiere reglas tanto entrantes como salientes.

Reglas de entrada para Cloud Manager

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 Cloud Manager
HTTP	80	Proporciona acceso HTTP desde exploradores web de cliente a la consola web de Cloud Manager y conexiones desde Cloud Compliance
HTTPS	443	Proporciona acceso HTTPS desde exploradores web de cliente a la consola web de Cloud Manager
TCP	3128	Proporciona a la instancia de Cloud Compliance acceso a Internet si la red AWS no utiliza NAT o proxy

Reglas de salida para Cloud Manager

El grupo de seguridad predefinido para Cloud Manager 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 Manager 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 únicamente los puertos necesarios para la comunicación saliente de Cloud Manager.

La dirección IP de origen es el host de Cloud Manager.

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
Cumplimiento de normativas en el cloud	HTTP	80	Instancia de cumplimiento de normativas cloud	Cumplimiento de normativas cloud para Cloud Volumes ONTAP

Reglas para Cloud Volumes ONTAP

El grupo de seguridad para Cloud Volumes ONTAP requiere reglas tanto entrantes como salientes.

Reglas de entrada para Cloud Volumes ONTAP

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 para Cloud Volumes ONTAP

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	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)	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	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)
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

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 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 API RESTful desde Cloud Manager

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 de Cloud Manager	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 de grupos de seguridad para Azure

Cloud Manager crea grupos de seguridad de Azure que incluyen las reglas entrantes y salientes que Cloud Manager y Cloud Volumes ONTAP deben operar correctamente. Tal vez desee consultar los puertos para fines de prueba o si prefiere utilizar sus propios grupos de seguridad.

Reglas para Cloud Manager

El grupo de seguridad para Cloud Manager requiere reglas tanto entrantes como salientes.

Reglas de entrada para Cloud Manager

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 Cloud Manager
80	HTTP	Proporciona acceso HTTP desde exploradores web de cliente a la consola web de Cloud Manager
443	HTTPS	Proporciona acceso HTTPS desde exploradores web de cliente a la consola web de Cloud Manager

Reglas de salida para Cloud Manager

El grupo de seguridad predefinido para Cloud Manager 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 Manager 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 únicamente los puertos necesarios para la comunicación saliente de Cloud Manager.

La dirección IP de origen es el host de Cloud Manager.

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 Cloud Volumes ONTAP

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

Prioridad y nombre	Puerto y protocolo	Origen y destino	Descripción
1011 inbound_749	749 TCP	De cualquiera a cualquiera	Kerberos
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
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 para Cloud Volumes ONTAP

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	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)	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	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
DHCPS	67	UDP	LIF de gestión de nodos	DHCP	Servidor DHCP

Servicio	Puerto	Protocolo	Origen	Destino	Específico
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 firewall para GCP

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.

Reglas para Cloud Manager

Las reglas de firewall para Cloud Manager requieren reglas tanto entrantes como salientes.

Reglas de entrada para Cloud Manager

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 Cloud Manager
HTTP	80	Proporciona acceso HTTP desde exploradores web de cliente a la consola web de Cloud Manager
HTTPS	443	Proporciona acceso HTTPS desde exploradores web de cliente a la consola web de Cloud Manager

Reglas de salida para Cloud Manager

Las reglas de firewall predefinidas para Cloud Manager 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 Cloud Manager 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 únicamente los puertos necesarios para la comunicación saliente de Cloud Manager.

La dirección IP de origen es el host de Cloud Manager.

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

Reglas para Cloud Volumes ONTAP

El grupo de seguridad para Cloud Volumes ONTAP requiere reglas tanto entrantes como salientes.

Reglas de entrada para Cloud Volumes ONTAP

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 para Cloud Volumes ONTAP

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	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)	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	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

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 no está seguro de qué página debe utilizar, lea a continuación y le dirigiremos a la página correcta según su objetivo.

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
Permitir la puesta en funcionamiento de Cloud Volumes ONTAP PAYGO para versiones 9.6 y posteriores	"Cloud Manager (para Cloud Volumes ONTAP)"	Esta página de AWS Marketplace permite el cobro de la versión PAYGO de Cloud Volumes ONTAP 9.6 y posterior. También permite cargar las funciones complementarias de Cloud Volumes ONTAP. Esta página no 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 4 de esta tabla.
Activar funciones complementarias para Cloud Volumes ONTAP (PAYGO o BYOL)		
Puesta en marcha de Cloud Volumes ONTAP mediante una licencia que he comprado a NetApp (BYOL)	• "Cloud Volumes ONTAP para AWS (BYOL)" • "Cloud Volumes ONTAP para AWS - Alta disponibilidad (BYOL)"	Estas páginas de AWS Marketplace le permiten suscribirse a las versiones de nodo único o de alta disponibilidad de BYOL de Cloud Volumes ONTAP.
Ponga en marcha Cloud Manager desde AWS Marketplace mediante un AMI	"Cloud Manager de NetApp (para Cloud Volumes ONTAP de NetApp)"	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.

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.
"ec2:DescribDhcpOptions",	Determina los servidores DNS y el nombre de dominio predeterminado al iniciar instancias de Cloud Volumes ONTAP.

Acciones	Específico
"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",	Gestiona el bloque de S3 que un sistema Cloud Volumes ONTAP usa como nivel de capacidad.
"Kms:List*", "kms:describir*"	Obtiene información acerca de las claves del servicio de gestión de claves de AWS.
"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.

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.
"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.

Acciones	Específico
"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.
"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.

Acciones	Específico
"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.

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.
- 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.

Acciones	Específico
- 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.
- 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	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.

Configuraciones predeterminadas

Los detalles sobre la configuración predeterminada de Cloud Manager y Cloud Volumes ONTAP pueden ayudarle a administrar los sistemas.

Configuración predeterminada para Cloud Manager en Linux

Si necesita solucionar problemas con Cloud Manager o su host Linux, puede ser útil comprender cómo se configura Cloud Manager.

- Si implementó Cloud Manager desde NetApp Cloud Central (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 de Cloud Manager es Red Hat Enterprise Linux 7.4 (HVM).

    El sistema operativo no incluye una GUI. Debe utilizar un terminal para acceder al sistema.
- La carpeta de instalación de Cloud Manager reside 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
  - Java
  - Kubectl
  - MySQL
  - Tridentctl
  - Consiga

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.

- 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 SVM que sirve datos cuando pone en marcha Cloud Volumes ONTAP. No se puede usar varias SVM que sirva datos.

- 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 a Cloud Manager mediante HTTPS.

  Cuando inició sesión en Cloud Manager, es posible acceder a los backups desde https://ipaddress/occm/offboxconfig/

- 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

Atributo	Valor definido por Cloud Manager
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 SSD de uso general:
  - Un disco de 140 GB para los datos raíz (uno por nodo)
  - 9.6 y posteriores: Un disco de 86 GB para datos de arranque (uno por nodo)
  - 9.5 y versiones anteriores: Un disco de 45 GB para datos de arranque (uno por nodo)
- 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)

- Dos discos SSD premium:
  - Un disco de 90 GB para los datos de arranque
  - Un disco de 140 GB para datos raíz
- Una instantánea de Azure para cada disco de arranque y disco raíz

Azure (parejas de alta disponibilidad)

- Dos discos SSD Premium de 90 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 128 GB para ahorrar núcleos (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.

Funciones

Los roles Administrador de cuentas y Administrador de área de trabajo proporcionan permisos específicos a los usuarios.

Tarea	Administrador de cuentas	Administrador de área de trabajo
Gestionar entornos de trabajo	Sí	Sí, para espacios de trabajo asociados
Ver el estado de replicación de datos	Sí	Sí, para espacios de trabajo asociados
Visualice la línea de tiempo	Sí	Sí, para espacios de trabajo asociados
Eliminar entornos de trabajo	Sí	No
Conecte los clústeres de Kubernetes a Cloud Volumes ONTAP	Sí	No

Tarea	Administrador de cuentas	Administrador de área de trabajo
Reciba el informe de Cloud Volumes ONTAP	Sí	No
Administrar cuentas de Cloud Central	Sí	No
Gestione las cuentas de proveedores de cloud	Sí	No
Modifique la configuración de Cloud Manager	Sí	No
Consulte y gestione la consola de soporte	Sí	No
Elimine entornos de trabajo de Cloud Manager	Sí	No
Actualice Cloud Manager	Sí	No
Instale un certificado HTTPS	Sí	No
Configurar Active Directory	Sí	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"

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.

- "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"
- 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 los datos access.es cómo activar rápidamente una SVM de destino después de un desastre y, a continuación, reactivar la SVM de origen.

- "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.

- "Soporte Cloud Volumes ONTAP de NetApp"

  Acceda a recursos de soporte para obtener ayuda y solucionar problemas con 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 por si no está ejecutando la versión más reciente.

"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 3.7.4"
- "Aviso para Cloud Manager 3.7.1"
- "Aviso para Cloud Manager 3.7"
- "Aviso para el Cloud Backup Service"