



Requisitos de red

Cloud Manager 3.7

NetApp
October 23, 2024

Tabla de contenidos

- Requisitos de red 1
 - Requisitos de red para Cloud Manager 1
 - Requisitos de red para Cloud Volumes ONTAP en AWS 5
 - Configuración de una puerta de enlace de tránsito de AWS para parejas de alta disponibilidad en AZs múltiples 12
 - Requisitos de red para Cloud Volumes ONTAP en Azure 16
 - Requisitos de red para Cloud Volumes ONTAP en GCP 17

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
<p>Servicios de AWS (amazonaws.com):</p> <ul style="list-style-type: none">• Formación CloudFormation• Cloud computing elástico (EC2)• Servicio de gestión de claves (KMS)• Servicio de token de seguridad (STS)• Simple Storage Service (S3) <p>El extremo exacto depende de la región en la que se implemente Cloud Volumes ONTAP. "Consulte la documentación de AWS para obtener más detalles."</p>	<p>Permite que Cloud Manager ponga en marcha y gestione Cloud Volumes ONTAP en AWS.</p>

Puntos finales	Específico
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	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: <ul style="list-style-type: none"> • 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.
<p>Diversas ubicaciones de terceros, por ejemplo:</p> <ul style="list-style-type: none"> • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org <p>Las ubicaciones de terceros están sujetas a cambios.</p>	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: <ul style="list-style-type: none"> • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org <p>Las ubicaciones de terceros están sujetas a cambios.</p>	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	<p>Debe introducir la dirección IP del host desde un explorador web para cargar la consola de Cloud Manager.</p> <p>Según su conectividad con el proveedor de cloud, puede usar la IP privada o una IP pública asignada al host:</p> <ul style="list-style-type: none">• 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 <p>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.</p>
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 alta disponibilidad 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.



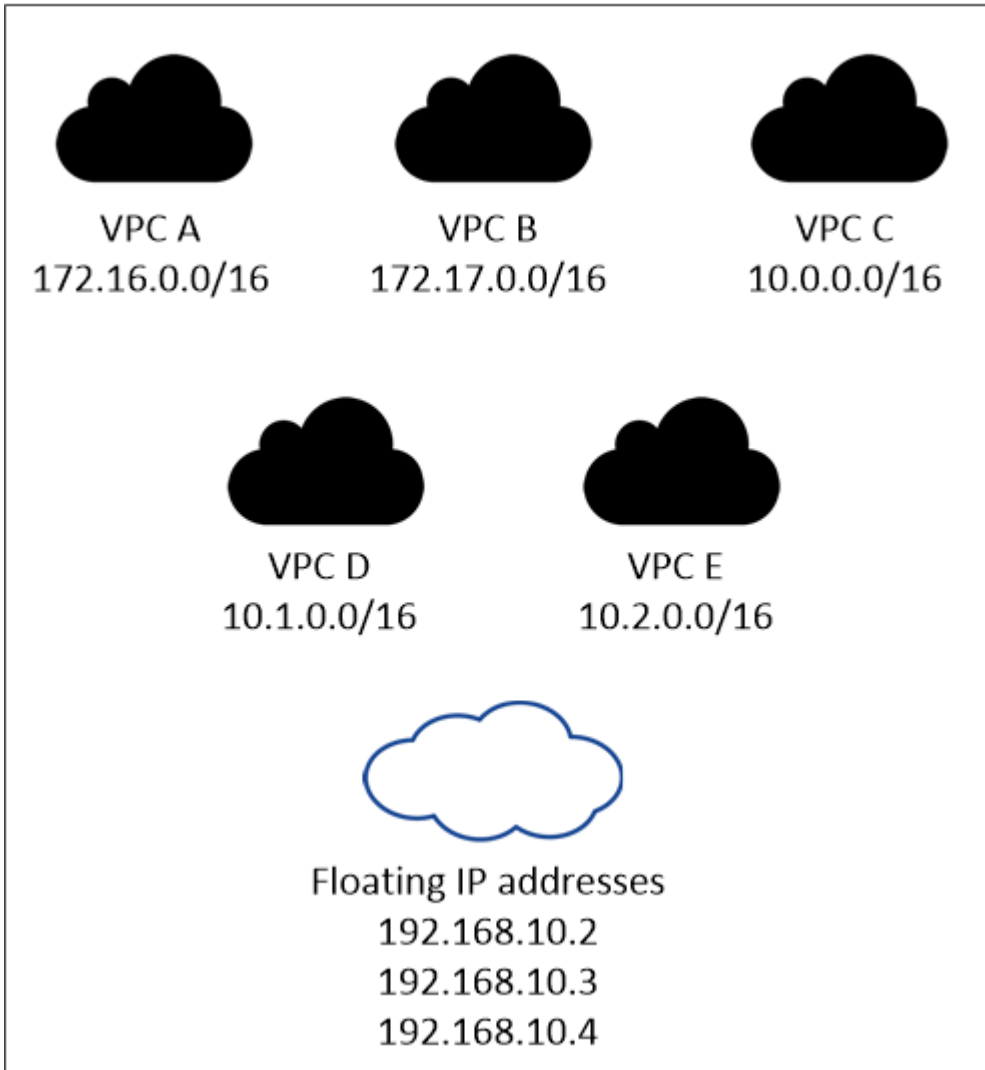
Se requiere una dirección IP flotante para el LIF de gestión de SVM si se usa SnapDrive para Windows o SnapCenter con el par de alta disponibilidad. Si no especifica la dirección IP al implementar el sistema, puede crear la LIF más adelante. Para obtener más información, consulte ["Configurar Cloud Volumes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

AWS region



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](#)".

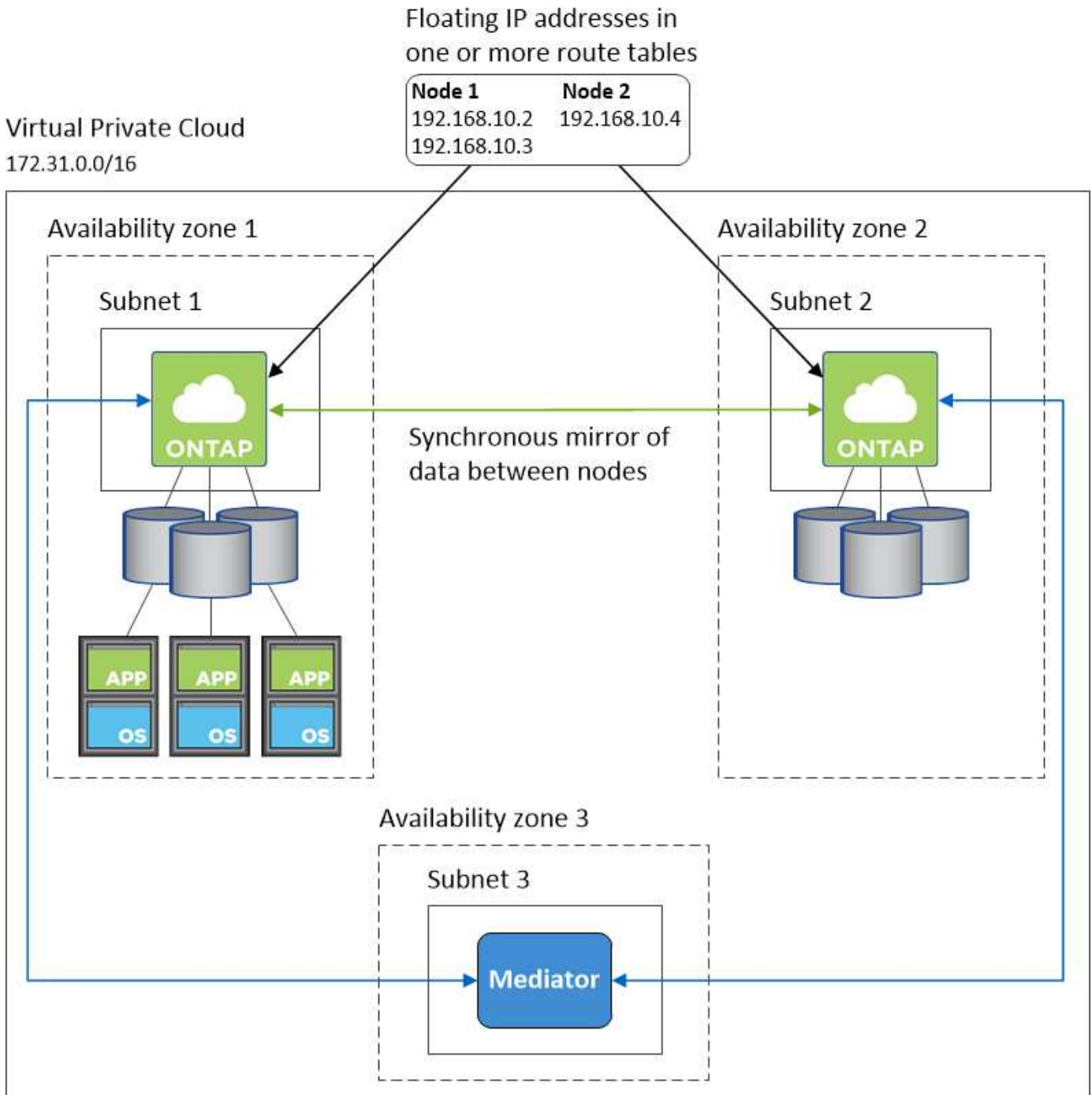
Conexión a herramientas de gestión de NetApp

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.

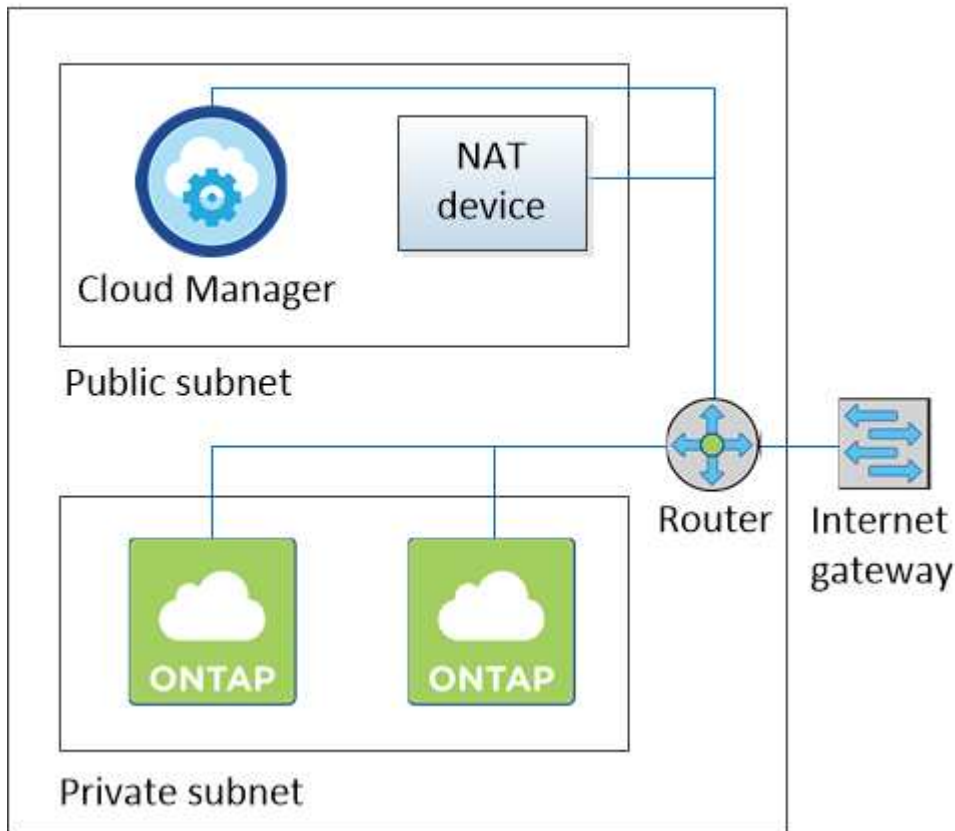


En lugar de un dispositivo NAT, puede utilizar un proxy HTTP para proporcionar conectividad a Internet.

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:

Virtual Private Cloud



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.

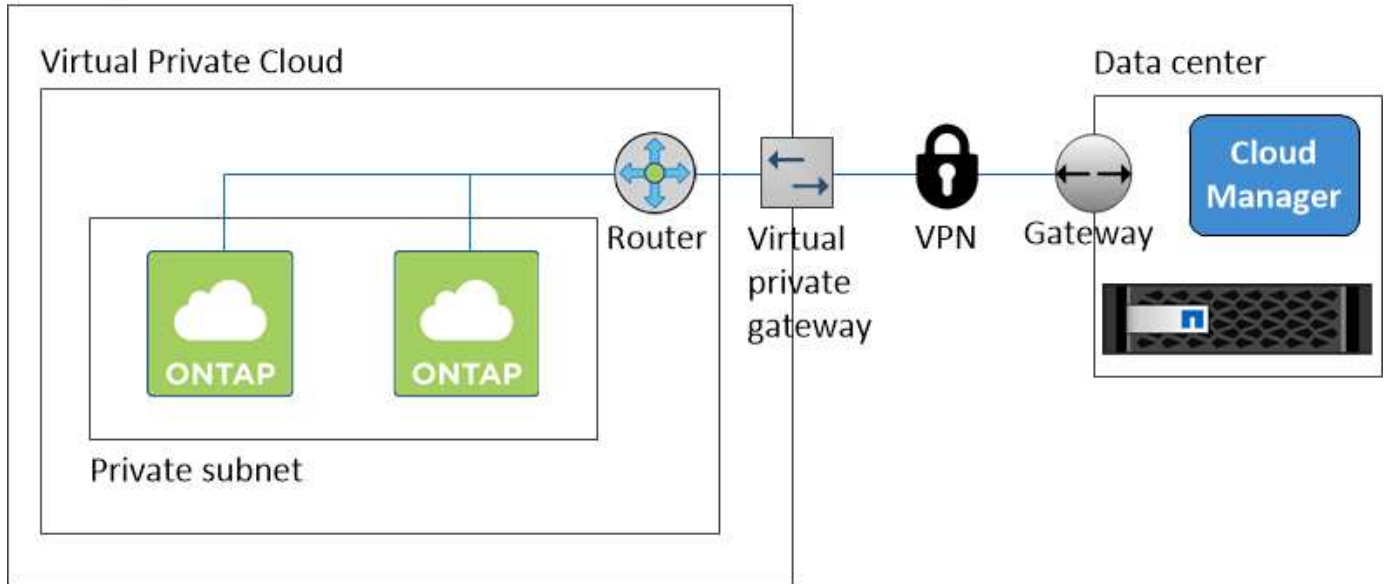
Si desea replicar datos entre los sistemas FAS de su centro de datos y los sistemas Cloud Volumes ONTAP

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:

AWS region



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

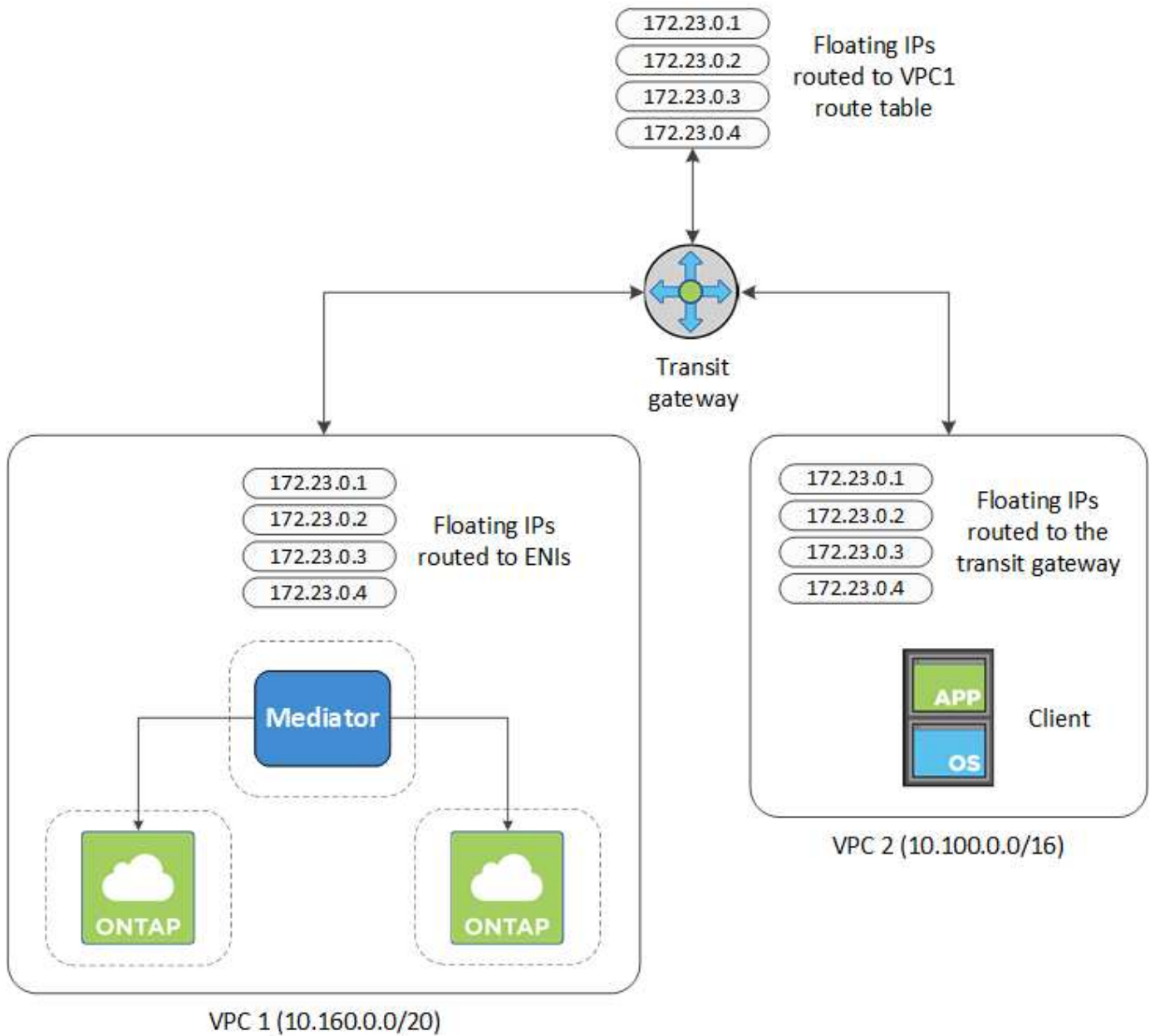
Configure una puerta de enlace de tránsito de AWS para permitir el acceso a las direcciones IP flotantes de un par de alta disponibilidad desde fuera del VPC donde reside el par de alta disponibilidad.

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:

NFS & CIFS access from within the VPC using Floating IP

Auto failover

Cluster Management : 172.23.0.1

Data (nfs,cifs) : Node 1: 172.23.0.2 | Node 2: 172.23.0.3

Access

SVM Management : 172.23.0.4

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.

Transit Gateway Route Table: tgw-rtb-0ea8ee291c7aeddd3

Details Associations Propagations **Routes** Tags

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

Create route Replace route Delete route

Filter by attributes or search by keyword

CIDR	Attachment	Resource type	Route type	Route state
10.100.0.0/16	tgw-attach-05e77bd34e2ff91f8 vpc-0b2bc30e0dc8e0db1	VPC2	propagated	active
10.160.0.0/20	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC1	propagated	active
172.23.0.1/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC	static	active
172.23.0.2/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC	static	active
172.23.0.3/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC	static	active
172.23.0.4/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC	static	active

Floating IP Addresses

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.

Route Table: rtb-0569a1bd740ed033f

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
10.100.0.0/16	local	active	No
0.0.0.0/0	igw-07250bd01781e67df	active	No
10.160.0.0/20	tgw-015b7c249661ac279	active	No
172.23.0.1/32	tgw-015b7c249661ac279	active	No
172.23.0.2/32	tgw-015b7c249661ac279	active	No
172.23.0.3/32	tgw-015b7c249661ac279	active	No
172.23.0.4/32	tgw-015b7c249661ac279	active	No

VPC1
Floating IP Addresses

- 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.

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status
10.160.0.0/20	local	active
pl-68a54001 (com.amazonaws.us-west-2.s3, 54.231.160.0/19, 52.218.128.0/17, 52.92.32.0/22)	vpce-cb51a0a2	active
0.0.0.0/0	igw-b2182dd7	active
10.60.29.0/25	pcx-589c3331	active
10.100.0.0/16	tgw-015b7c249661ac279	active
10.129.0.0/20	pcx-ff7e1396	active
172.23.0.1/32	eni-0854d4715559c3cdb	active
172.23.0.2/32	eni-0854d4715559c3cdb	active
172.23.0.3/32	eni-0f76681216c3108ed	active
172.23.0.4/32	eni-0854d4715559c3cdb	active

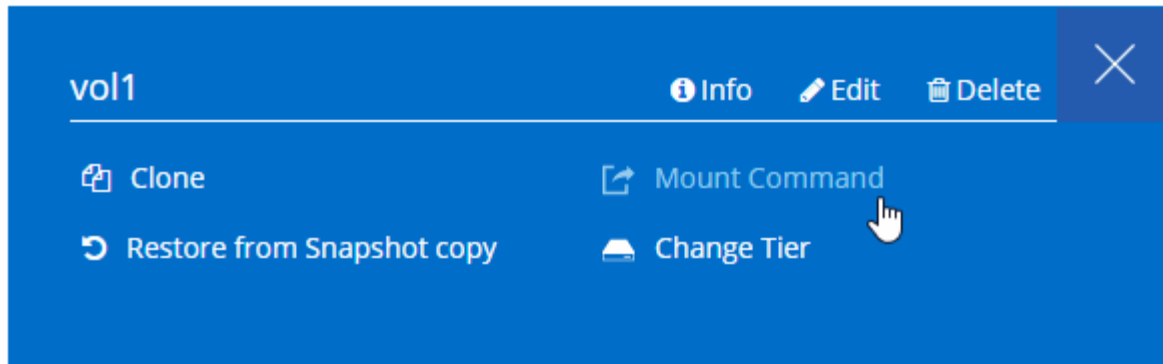
VPC2
Floating act IP Addresses

- 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**.

Volumes

2 Volumes | 0.22 TB Allocated | < 0.01 TB Used (0 TB in S3)



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](#)".

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPTIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.