Configura tu red

Cloud Volumes ONTAP

NetApp
February 13, 2026

Tabla de contenidos

Configura tu red

Configurar la red de AWS para Cloud Volumes ONTAP

La NetApp Console maneja la configuración de componentes de red para Cloud Volumes ONTAP, como direcciones IP, máscaras de red y rutas. Debe asegurarse de que el acceso a Internet saliente esté disponible, que haya suficientes direcciones IP privadas disponibles, que existan las conexiones correctas y más.

Requisitos generales

Asegúrese de haber cumplido los siguientes requisitos en AWS.

Acceso a Internet saliente para nodos de Cloud Volumes ONTAP

Los sistemas Cloud Volumes ONTAP requieren acceso a Internet saliente para acceder a puntos finales externos para diversas funciones. Cloud Volumes ONTAP no puede funcionar correctamente si estos puntos finales están bloqueados en entornos con requisitos de seguridad estrictos.

El agente de consola se comunica con varios puntos finales para realizar operaciones diarias. Para obtener información sobre los puntos finales utilizados, consulte "Ver los puntos finales contactados desde el agente de la consola" y "Preparar la red para usar la consola" .

Puntos finales de Cloud Volumes ONTAP

Cloud Volumes ONTAP utiliza estos puntos finales para comunicarse con varios servicios.

Puntos finales	Aplicable para	Objetivo	Modos de implementación	Impacto si el punto final no está disponible
\ https://netapp-cloud-account.auth0.com	Autenticación	Se utiliza para la autenticación en la consola.	Modos estándar y restringido.	La autenticación del usuario falla y los siguientes servicios permanecen no disponibles: • Servicios de Cloud Volumes ONTAP • Servicios de ONTAP • Protocolos y servicios proxy

Puntos finales	Aplicable para	Objetivo	Modos de implementación	Impacto si el punto final no está disponible
\ https://api.bluexp.netapp.com/tenancy	Tenencia	Se utiliza para recuperar recursos de Cloud Volumes ONTAP desde la consola para autorizar recursos y usuarios.	Modos estándar y restringido.	Los recursos de Cloud Volumes ONTAP y los usuarios no están autorizados.
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Se utiliza para enviar datos de telemetría de AutoSupport al soporte de NetApp .	Modos estándar y restringido.	La información de AutoSupport sigue sin entregarse.
El punto final comercial exacto para el servicio de AWS (con el sufijo `amazonaws.com`) depende de la región de AWS que esté utilizando. Consulte la "Documentación de AWS para más detalles" .	• Formación de nubes • Nube de cómputo elástica (EC2) • Gestión de identidad y acceso (IAM) • Servicio de gestión de claves (KMS) • Servicio de token de seguridad (STS) • Amazon Simple Storage Service (S3)	Comunicación con los servicios de AWS.	Modos estándar y privado.	Cloud Volumes ONTAP no puede comunicarse con el servicio AWS para realizar operaciones específicas en AWS.

Puntos finales	Aplicable para	Objetivo	Modos de implementación	Impacto si el punto final no está disponible
El punto final gubernamental exacto para el servicio de AWS depende de la región de AWS que esté utilizando. Los puntos finales tienen el sufijo `amazonaws.com` y `c2s.ic.gov`. Referirse a "Kit de desarrollo de software de AWS" y "Documentación de AWS" Para más información.	• Formación de nubes • Nube de cómputo elástica (EC2) • Gestión de identidad y acceso (IAM) • Servicio de gestión de claves (KMS) • Servicio de token de seguridad (STS) • Servicio de almacenamiento simple (S3)	Comunicación con los servicios de AWS.	Modo restringido.	Cloud Volumes ONTAP no puede comunicarse con el servicio AWS para realizar operaciones específicas en AWS.

Acceso a Internet saliente para el mediador de HA

La instancia del mediador de HA debe tener una conexión saliente al servicio AWS EC2 para que pueda ayudar con la conmutación por error 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 punto final de VPC de interfaz desde la subred de destino al servicio AWS EC2. Para obtener detalles sobre los puntos finales de VPC, consulte la "Documentación de AWS: Puntos de conexión de la VPC de interfaz (AWS PrivateLink)" .

Configuración del proxy de red del agente de la NetApp Console

Puede utilizar la configuración de servidores proxy del agente de la NetApp Console para habilitar el acceso a Internet saliente desde Cloud Volumes ONTAP. La consola admite dos tipos de proxies:

- **Proxy explícito**: el tráfico saliente de Cloud Volumes ONTAP utiliza la dirección HTTP del servidor proxy especificado durante la configuración del proxy del agente de la consola. Es posible que el administrador también haya configurado credenciales de usuario y certificados CA raíz para autenticación adicional. Si hay un certificado de CA raíz disponible para el proxy explícito, asegúrese de obtener y cargar el mismo certificado en su sistema Cloud Volumes ONTAP utilizando el "CLI de ONTAP : instalación del certificado de seguridad" dominio.
- **Proxy transparente**: la red está configurada para enrutar automáticamente el tráfico saliente desde Cloud Volumes ONTAP a través del proxy del agente de la consola. Al configurar un proxy transparente, el administrador solo debe proporcionar un certificado CA raíz para la conectividad desde Cloud Volumes ONTAP, no la dirección HTTP del servidor proxy. Asegúrese de obtener y cargar el mismo certificado de CA raíz en su sistema Cloud Volumes ONTAP utilizando el "CLI de ONTAP : instalación del certificado de seguridad" dominio.

Para obtener información sobre cómo configurar servidores proxy, consulte la "Configurar el agente de la

consola para utilizar un servidor proxy" .

Direcciones IP privadas

La consola asigna automáticamente la cantidad necesaria de direcciones IP privadas a Cloud Volumes ONTAP. Debe asegurarse de que su red tenga suficientes direcciones IP privadas disponibles.

El número de LIFs que la NetApp Console asigna para Cloud Volumes ONTAP depende de si despliegas un sistema de nodo único o un par HA. Un LIF es una dirección IP asociada con un puerto físico.

Direcciones IP para un sistema de nodo único

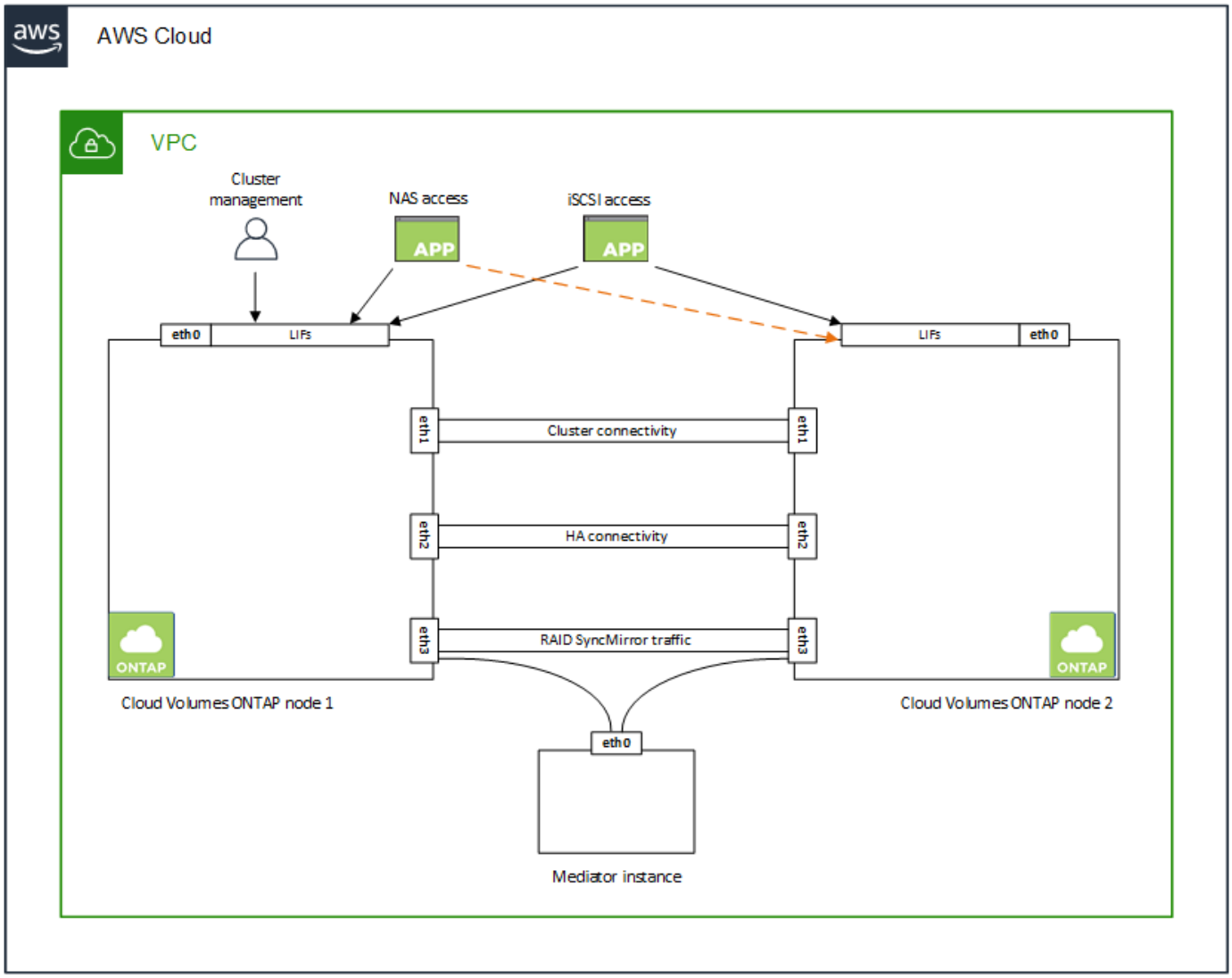
NetApp Console asigna 6 direcciones IP a un sistema de nodo único.

La siguiente tabla proporciona detalles sobre los LIF que están asociados con cada dirección IP privada.

LIF	Objetivo
Gestión de clústeres	Gestión administrativa de todo el cluster (par HA).
Gestión de nodos	Gestión administrativa de un nodo.
Intercluster	Comunicación, copia de seguridad y replicación entre clústeres.
Datos NAS	Acceso de clientes a través de protocolos NAS.
Datos iSCSI	Acceso de cliente a través del protocolo iSCSI. El sistema también lo utiliza para otros flujos de trabajo de red importantes. Este LIF es obligatorio y no debe eliminarse.
Administración de máquinas virtuales de almacenamiento	Un LIF de administración de máquinas virtuales de almacenamiento se utiliza con herramientas de administración como SnapCenter.

Direcciones IP para pares HA

Las parejas de alta disponibilidad necesitan más direcciones IP que un sistema de un solo nodo. Estas direcciones IP están repartidas en diferentes interfaces ethernet, como se muestra en la siguiente imagen:



La cantidad de direcciones IP privadas necesarias para un par HA depende del modelo de implementación que elija. Un par de alta disponibilidad implementado en una *única* zona de disponibilidad de AWS (AZ) requiere 15 direcciones IP privadas, mientras que un par de alta disponibilidad implementado en *múltiples* AZ requiere 13 direcciones IP privadas.

Las siguientes tablas proporcionan detalles sobre los LIF que están asociados con cada dirección IP privada.

LIF	Interfaz	Node	Objetivo
Gestión de clústeres	eth0	nodo 1	Gestión administrativa de todo el cluster (par HA).
Gestión de nodos	eth0	nodo 1 y nodo 2	Gestión administrativa de un nodo.
Intercluster	eth0	nodo 1 y nodo 2	Comunicación, copia de seguridad y replicación entre clústeres.
Datos NAS	eth0	nodo 1	Acceso de clientes a través de protocolos NAS.

LIF	Interfaz	Node	Objetivo
Datos iSCSI	eth0	nodo 1 y nodo 2	Acceso de cliente a través del protocolo iSCSI. El sistema también lo utiliza para otros flujos de trabajo de red importantes. Estos LIF son necesarios y no deben eliminarse.
Conectividad del clúster	eth1	nodo 1 y nodo 2	Permite que los nodos se comuniquen entre sí y muevan datos dentro del clúster.
Conectividad HA	eth2	nodo 1 y nodo 2	Comunicación entre los dos nodos en caso de conmutación por error.
Tráfico iSCSI de RSM	eth3	nodo 1 y nodo 2	Tráfico iSCSI RAID SyncMirror , así como la comunicación entre los dos nodos de Cloud Volumes ONTAP y el mediador.
Mediador	eth0	Mediador	Un canal de comunicación entre los nodos y el mediador para ayudar en los procesos de adquisición y devolución de almacenamiento.

LIF	Interfaz	Node	Objetivo
Gestión de nodos	eth0	nodo 1 y nodo 2	Gestión administrativa de un nodo.
Intercluster	eth0	nodo 1 y nodo 2	Comunicación, copia de seguridad y replicación entre clústeres.
Datos iSCSI	eth0	nodo 1 y nodo 2	Acceso de cliente a través del protocolo iSCSI. Estos LIF también gestionan la migración de direcciones IP flotantes entre nodos. Estos LIF son necesarios y no deben eliminarse.
Conectividad del clúster	eth1	nodo 1 y nodo 2	Permite que los nodos se comuniquen entre sí y muevan datos dentro del clúster.
Conectividad HA	eth2	nodo 1 y nodo 2	Comunicación entre los dos nodos en caso de conmutación por error.
Tráfico iSCSI de RSM	eth3	nodo 1 y nodo 2	Tráfico iSCSI RAID SyncMirror , así como la comunicación entre los dos nodos de Cloud Volumes ONTAP y el mediador.
Mediador	eth0	Mediador	Un canal de comunicación entre los nodos y el mediador para ayudar en los procesos de adquisición y devolución de almacenamiento.

Cuando se implementa en múltiples zonas de disponibilidad, varios LIF se asocian con"direcciones IP flotantes" , que no cuentan para el límite de IP privada de AWS.

Grupos de seguridad

No es necesario crear grupos de seguridad porque la consola lo hace por usted. Si necesita utilizar el suyo propio, consulte"Reglas del grupo de seguridad" .

¿Buscas información sobre el agente de consola? "Ver las reglas del grupo de seguridad para el agente de la consola"

Conexión para la estratificación de datos

Si quieres usar EBS como capa de rendimiento y Amazon S3 como capa de capacidad, debes asegurarte de que Cloud Volumes ONTAP tiene una conexión a S3. La mejor manera de proporcionar esa conexión es creando un VPC Endpoint para el servicio S3. Para instrucciones, consulta "Documentación de AWS: Creación de un punto final de puerta de enlace".

Al crear el punto final de VPC, asegúrese de seleccionar la región, la VPC y la tabla de rutas que corresponden a la instancia de Cloud Volumes ONTAP . También debe modificar el grupo de seguridad para agregar una regla HTTPS saliente que habilite el tráfico al punto final S3. De lo contrario, Cloud Volumes ONTAP no podrá conectarse al servicio S3.

Si experimenta algún problema, consulte la "Centro de conocimiento de soporte de AWS: ¿Por qué no puedo conectarme a un bucket S3 mediante un punto final de VPC de puerta de enlace?"

Conexiones a sistemas ONTAP

Para replicar datos entre un sistema Cloud Volumes ONTAP en AWS y sistemas ONTAP en otras redes, debe tener una conexión VPN entre AWS VPC y la otra red (por ejemplo, su red corporativa). Para obtener instrucciones, consulte la "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 extender su configuración local 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 utilizar el servidor DNS EC2 predeterminado, que no debe ser el servidor DNS utilizado por el entorno de Active Directory.

Para obtener instrucciones, consulte la "Documentación de AWS: Servicios de dominio de Active Directory en la nube de AWS: Implementación de referencia de inicio rápido" .

Uso compartido de VPC

A partir de la versión 9.11.1, los pares de Cloud Volumes ONTAP HA son compatibles con AWS con uso compartido de VPC. El uso compartido de VPC permite que su organización comparta subredes con otras cuentas de AWS. Para utilizar esta configuración, debe configurar su entorno de AWS y luego implementar el par HA mediante la API.

"Aprenda a implementar un par HA en una subred compartida" .

Requisitos para pares de alta disponibilidad en varias zonas de disponibilidad

Se aplican requisitos de red de AWS adicionales a las configuraciones de HA de Cloud Volumes ONTAP que utilizan múltiples zonas de disponibilidad (AZ). Debe revisar estos requisitos antes de lanzar un par de alta disponibilidad porque debe ingresar los detalles de red en la consola cuando agrega un sistema Cloud Volumes ONTAP .

Para comprender cómo funcionan los pares HA, consulte"Pares de alta disponibilidad" .

Zonas de disponibilidad

Este modelo de implementación de HA utiliza múltiples AZ para garantizar una alta disponibilidad de sus datos. Debe utilizar una AZ dedicada para cada instancia de Cloud Volumes ONTAP y la instancia del mediador, que proporciona un canal de comunicación entre el par de alta disponibilidad.

Debe haber una subred disponible en cada zona de disponibilidad.

Direcciones IP flotantes para datos NAS y gestión de clústeres/SVM

Las configuraciones de alta disponibilidad en múltiples zonas de disponibilidad utilizan direcciones IP flotantes que migran entre nodos si ocurren fallas. No son accesibles de forma nativa desde fuera de la VPC, a menos que"Configurar una puerta de enlace de tránsito de AWS" .

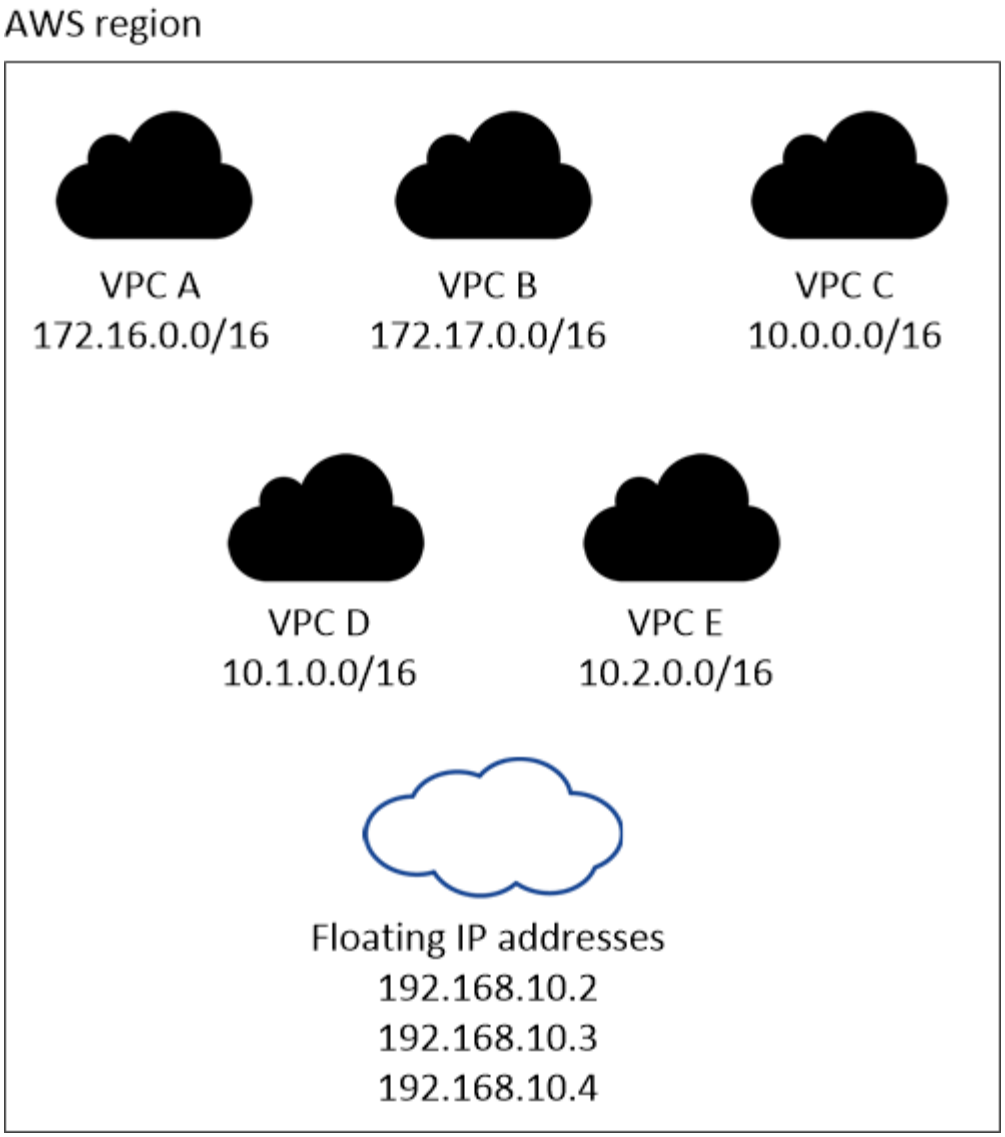
Una dirección IP flotante es para la administración del clúster, otra es para los datos NFS/CIFS en el nodo 1 y otra es para los datos NFS/CIFS en el nodo 2. Una cuarta dirección IP flotante para la gestión de SVM es opcional.

> Se requiere una dirección IP flotante para el LIF de administración de SVM si usa SnapDrive para Windows o SnapCenter con el par HA.

Debe ingresar las direcciones IP flotantes cuando agrega un sistema Cloud Volumes ONTAP HA. La consola asigna las direcciones IP al par HA cuando inicia el sistema.

Las direcciones IP flotantes deben estar fuera de los bloques CIDR para todas las VPC en la región de AWS en la que implementa la configuración de HA. Piense en las direcciones IP flotantes como una subred lógica que está fuera de las VPC de su región.

El siguiente ejemplo muestra la relación entre las direcciones IP flotantes y las VPC en una región de AWS. Si bien las direcciones IP flotantes están fuera de los bloques CIDR para todas las VPC, se pueden enrutar a subredes a través de tablas de rutas.



La consola crea automáticamente direcciones IP estáticas para el acceso iSCSI y para el acceso NAS desde clientes fuera de la VPC. No es necesario cumplir ningún requisito para este tipo de direcciones IP.

Puerta de enlace de tránsito para habilitar el acceso a IP flotante desde fuera de la VPC

Si es necesario,"Configurar una puerta de enlace de tránsito de AWS" para permitir el acceso a las direcciones IP flotantes de un par HA desde fuera de la VPC donde reside el par HA.

Tablas de rutas

Después de especificar las direcciones IP flotantes, se le solicitará que seleccione las tablas de rutas que deben incluir rutas a las direcciones IP flotantes. Esto permite el acceso del cliente al par HA.

Si solo tiene una tabla de rutas para las subredes en su VPC (la tabla de rutas principal), la consola agrega automáticamente las direcciones IP flotantes a esa tabla de rutas. Si tiene más de una tabla de rutas, es muy importante seleccionar las tablas de rutas correctas al lanzar el par HA. De lo contrario, es posible que algunos clientes no tengan acceso a Cloud Volumes ONTAP.

Por ejemplo, es posible que tenga dos subredes que estén asociadas con diferentes tablas de rutas. Si selecciona la tabla de rutas A, pero no la tabla de rutas B, entonces los clientes en la subred asociada con

la tabla de rutas A pueden acceder al par HA, pero los clientes en la subred asociada con la tabla de rutas B no pueden.

Para obtener más información sobre las tablas de rutas, consulte la "Documentación de AWS: Tablas de rutas" .

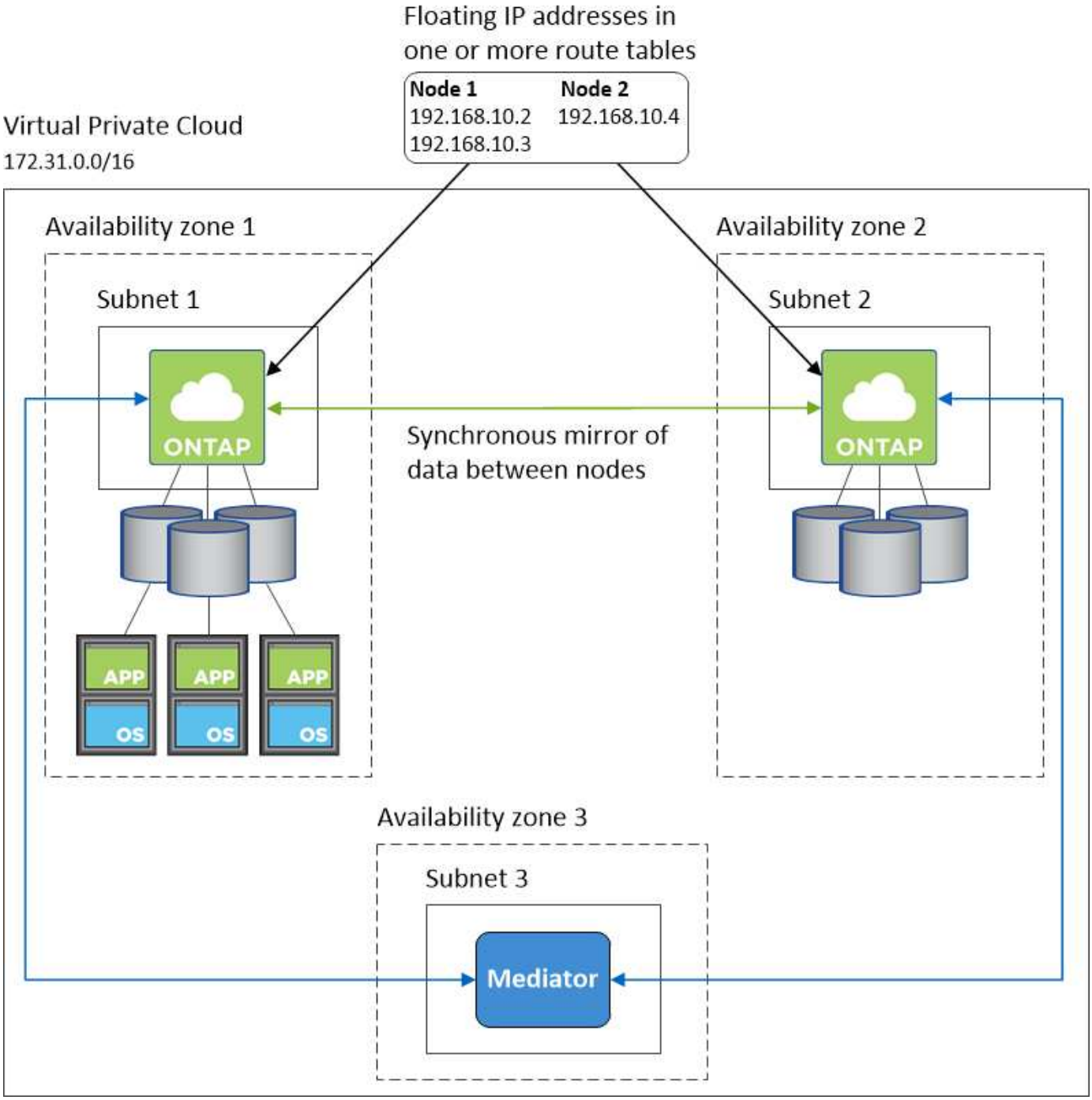
Conexión a las herramientas de gestión de NetApp

Para utilizar las herramientas de administración de NetApp con configuraciones de alta disponibilidad que se encuentran en varias zonas de disponibilidad, tiene dos opciones de conexión:

1. Implemente las herramientas de administración de NetApp en una VPC diferente y"Configurar una puerta de enlace de tránsito de AWS" . La puerta de enlace permite el acceso a la dirección IP flotante para la interfaz de administración del clúster desde fuera de la VPC.
2. Implemente las herramientas de administración de NetApp en la misma VPC con una configuración de enrutamiento similar a la de los clientes NAS.

Ejemplo de configuración de alta disponibilidad

La siguiente imagen ilustra los componentes de red específicos de un par de alta disponibilidad en varias zonas de disponibilidad: tres zonas de disponibilidad, tres subredes, direcciones IP flotantes y una tabla de rutas.



Requisitos para el agente de consola

Si aún no ha creado un agente de consola, debe revisar los requisitos de red.

- "Ver los requisitos de red para el agente de consola"
- "Reglas de grupo de seguridad en AWS"

Temas relacionados

- "Verificar la configuración de AutoSupport para Cloud Volumes ONTAP"
- "Obtenga más información sobre los puertos internos de ONTAP" .

Configurar una puerta de enlace de tránsito de AWS para pares de alta disponibilidad de Cloud Volumes ONTAP

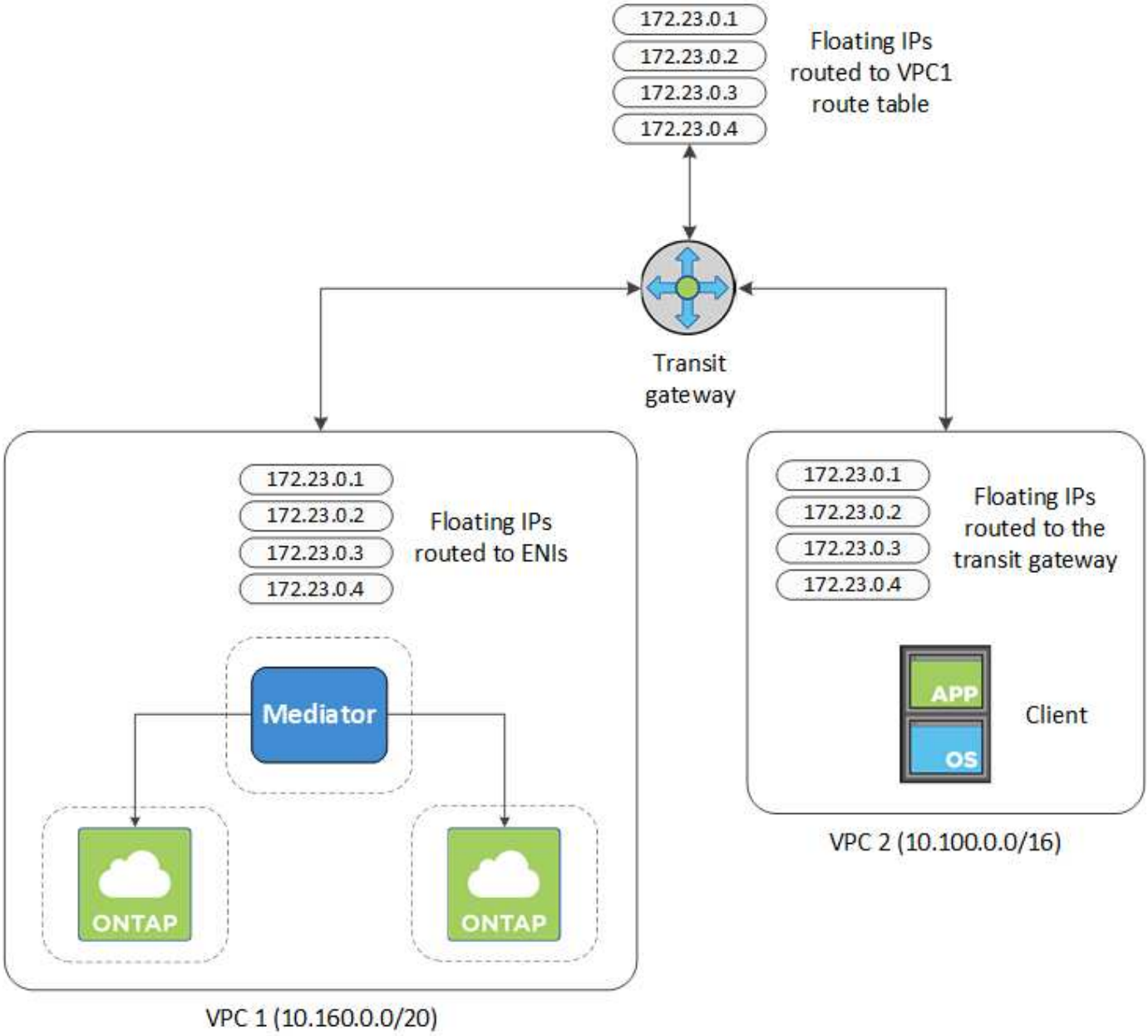
Configurar una puerta de enlace de tránsito de AWS para habilitar el acceso a un par de alta disponibilidad"direcciones IP flotantes" desde fuera de la VPC donde reside el par HA.

Cuando una configuración de HA de Cloud Volumes ONTAP se distribuye en varias zonas de disponibilidad de AWS, se requieren direcciones IP flotantes para el acceso a los datos NAS desde dentro de la VPC. Estas direcciones IP flotantes pueden migrar entre nodos cuando ocurren fallas, pero no son accesibles de forma nativa desde fuera de la VPC. Las direcciones IP privadas independientes proporcionan acceso a datos desde fuera de la VPC, pero no proporcionan conmutación por error automática.

También se requieren direcciones IP flotantes para la interfaz de administración del clúster y el LIF de administración de SVM opcional.

Si configura una puerta de enlace de tránsito de AWS, habilita el acceso a las direcciones IP flotantes desde fuera de la VPC donde reside el par HA. Esto significa que los clientes NAS y las herramientas de administración de NetApp fuera de la VPC pueden acceder a las IP flotantes.

A continuación se muestra un ejemplo que muestra dos VPC conectadas mediante una puerta de enlace de tránsito. Un sistema HA reside en una VPC, mientras que un cliente reside en la otra. Luego podría montar un volumen NAS en el cliente usando la dirección IP flotante.

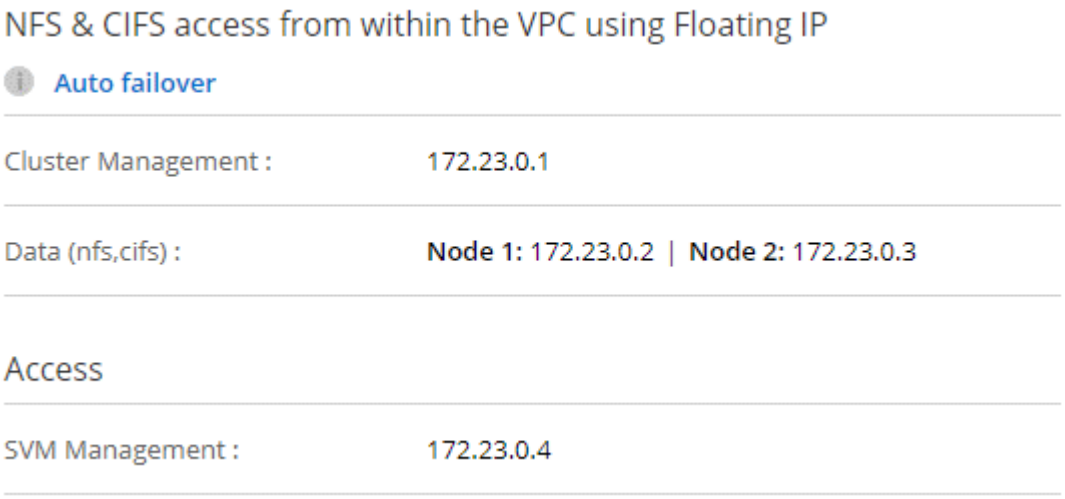


Los siguientes pasos ilustran cómo establecer una configuración similar.

Pasos

1. "Cree una puerta de enlace de tránsito y adjunte las VPC a la puerta de enlace" .
2. Asocie las VPC con la tabla de rutas de la puerta de enlace de tránsito.
   a. En el servicio **VPC**, haga clic en **Tablas de rutas de puerta de enlace de tránsito**.
   b. Seleccione la tabla de rutas.
   c. Haga clic en **Asociaciones** y luego seleccione **Crear asociación**.
   d. Seleccione los archivos adjuntos (las VPC) que desea asociar y luego haga clic en **Crear asociación**.
3. Cree rutas en la tabla de rutas de la puerta de enlace de tránsito especificando las direcciones IP flotantes del par HA.

   Puede encontrar las direcciones IP flotantes en la página de información del sistema en la NetApp Console. He aquí un ejemplo:



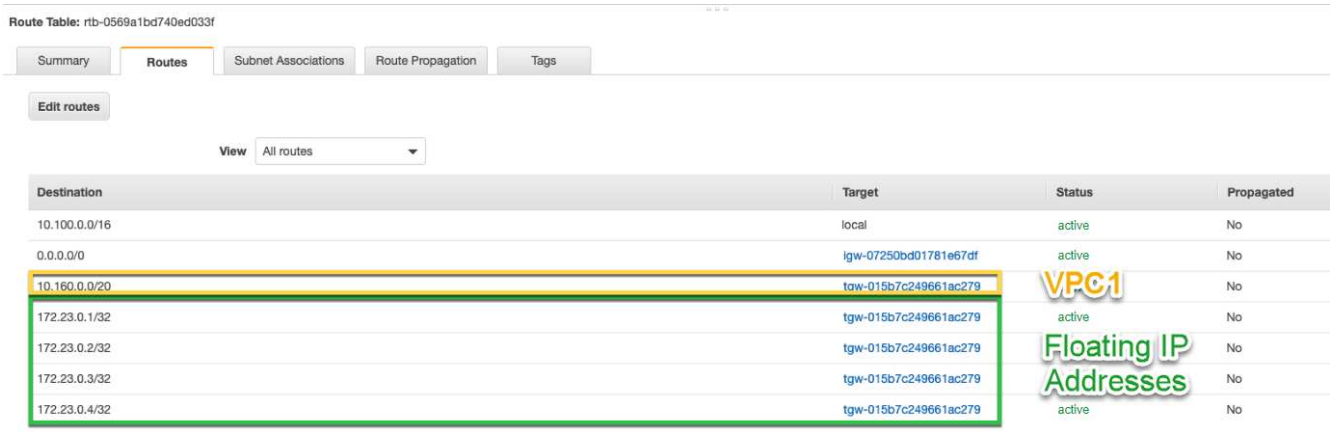
La siguiente imagen de muestra muestra la tabla de rutas para la puerta de enlace de tránsito. Incluye rutas a los bloques CIDR de las dos VPC y cuatro direcciones IP flotantes utilizadas por Cloud Volumes ONTAP.

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

   a. Agregue entradas de ruta a las direcciones IP flotantes.

   b. Agregue una entrada de ruta al bloque CIDR de la VPC donde reside el par HA.

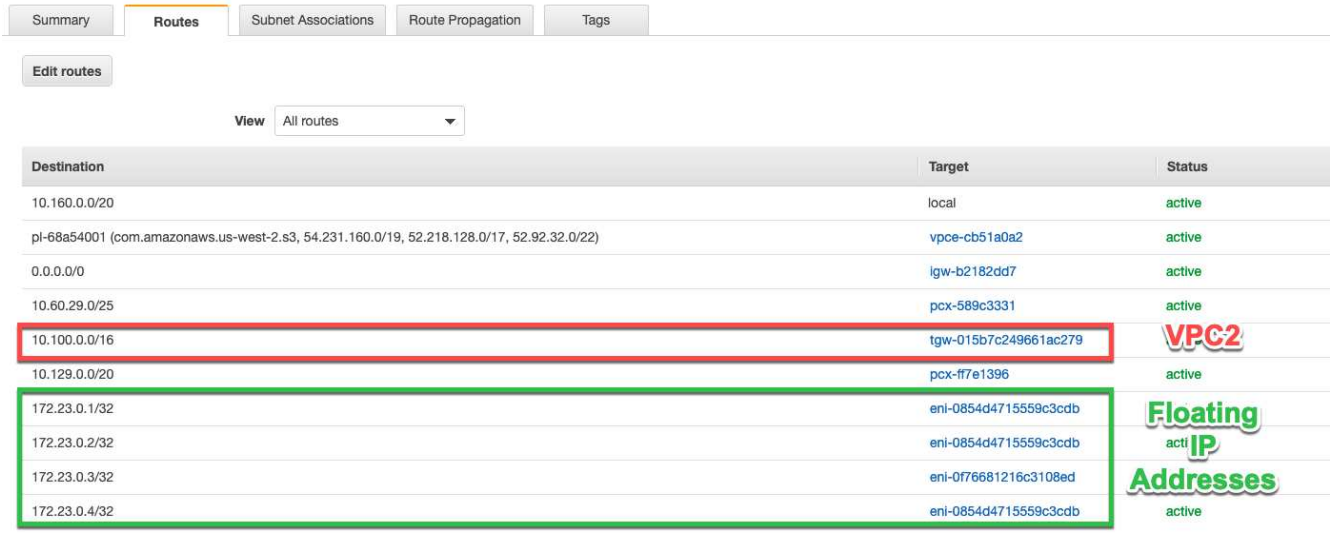
      La siguiente imagen de muestra muestra la tabla de rutas para VPC 2, que incluye rutas a VPC 1 y las direcciones IP flotantes.



5. Modifique la tabla de rutas para la VPC del par HA agregando una ruta a la VPC que necesita acceso a las direcciones IP flotantes.

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

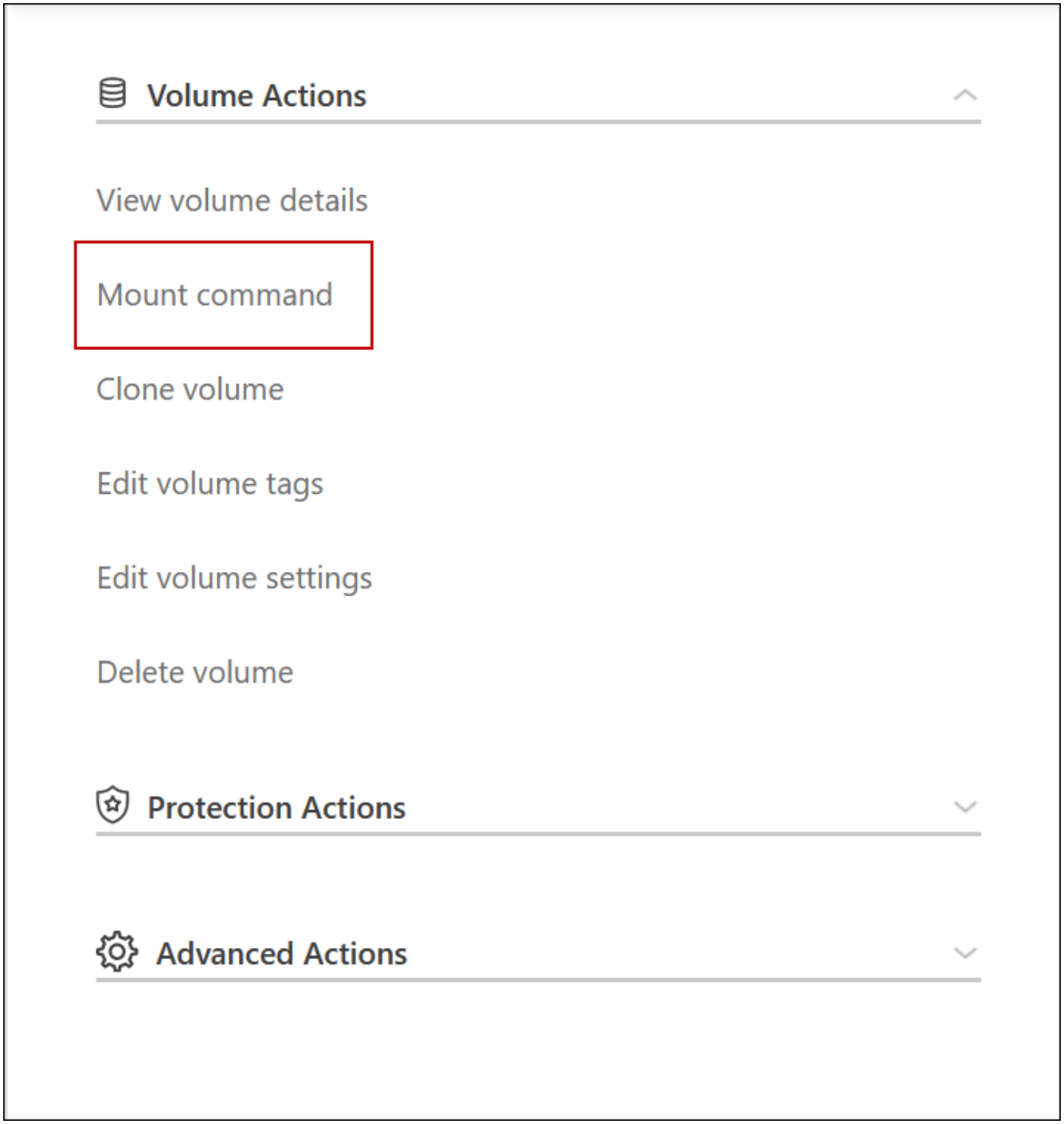
   La siguiente imagen de muestra muestra la tabla de rutas para VPC 1. Incluye una ruta a las direcciones IP flotantes y a VPC 2, que es donde reside un cliente. La consola agregó automáticamente las IP flotantes a la tabla de rutas cuando implementó el par HA.



6. Actualice la configuración de los grupos de seguridad a Todo el tráfico para la VPC.
   a. En Nube privada virtual, haga clic en **Subredes**.
   b. Haga clic en la pestaña **Tabla de rutas** y seleccione el entorno deseado para una de las direcciones IP flotantes para un par HA.
   c. Haga clic en **Grupos de seguridad**.
   d. Seleccione **Editar reglas de entrada**.
   e. Haga clic en **Agregar regla**.
   f. En Tipo, seleccione **Todo el tráfico** y, a continuación, seleccione la dirección IP de VPC.
   g. Haga clic en **Guardar reglas** para aplicar los cambios.
7. Montar volúmenes en clientes utilizando la dirección IP flotante.

   Puede encontrar la dirección IP correcta en la consola a través de la opción **Comando de montaje** en el

panel Administrar volúmenes en la consola.



8. Si está montando un volumen NFS, configure la política de exportación para que coincida con la subred de la VPC del cliente.

   "Aprenda a editar un volumen" .

Enlaces relacionados

- "Pares de alta disponibilidad en AWS"
- "Requisitos de red para Cloud Volumes ONTAP en AWS"

Implementar pares de Cloud Volumes ONTAP HA en una subred compartida de AWS

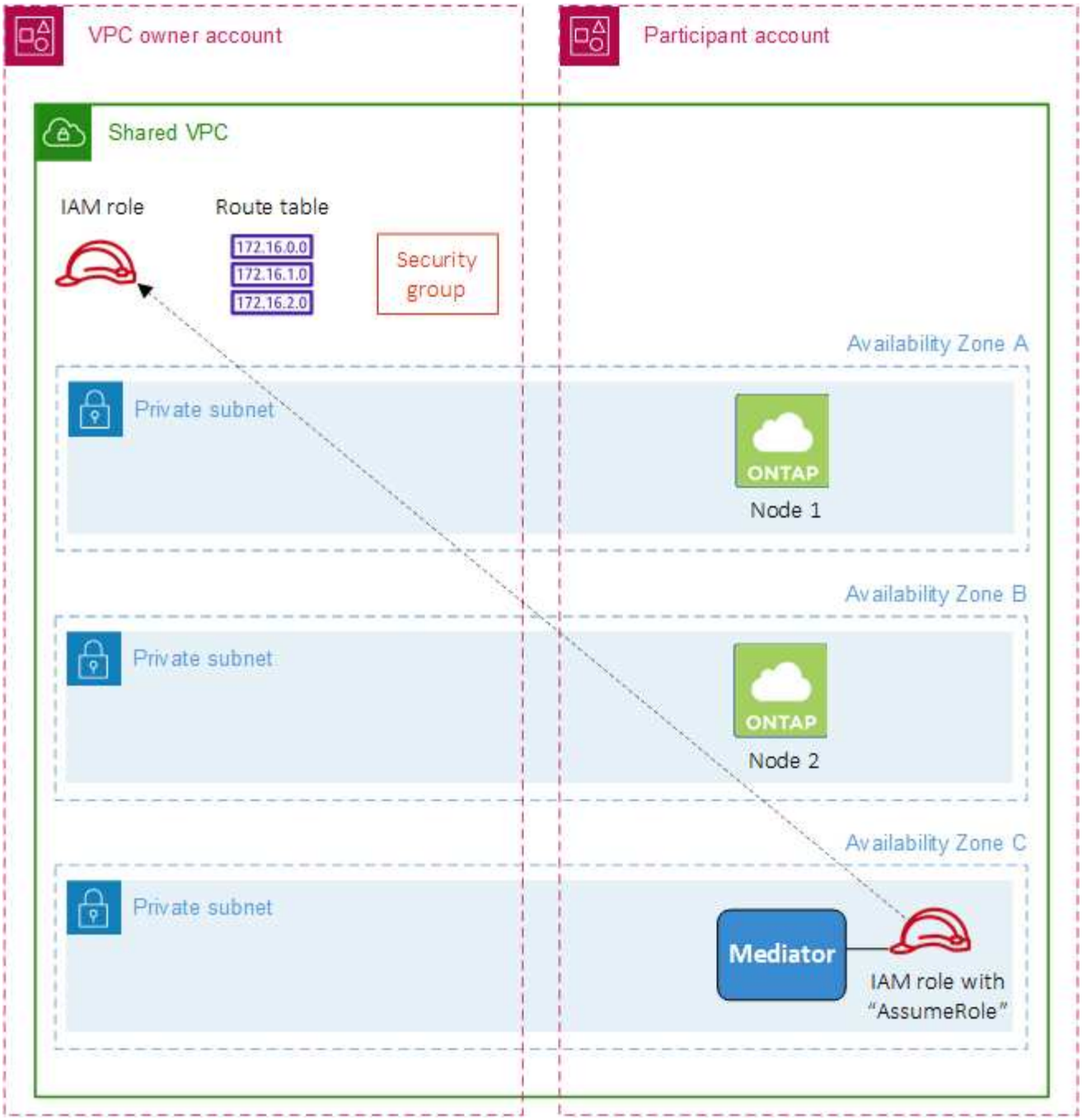
A partir de la versión 9.11.1, los pares de Cloud Volumes ONTAP HA son compatibles con AWS con uso compartido de VPC. El uso compartido de VPC permite que su organización comparta subredes con otras cuentas de AWS. Para utilizar esta configuración, debe configurar su entorno de AWS y luego implementar el par HA mediante la API.

Con "Uso compartido de VPC" Una configuración de Cloud Volumes ONTAP HA se distribuye en dos cuentas:

- La cuenta del propietario de VPC, que posee la red (la VPC, las subredes, las tablas de rutas y el grupo de seguridad de Cloud Volumes ONTAP)
- La cuenta del participante, donde se implementan las instancias EC2 en subredes compartidas (esto incluye los dos nodos HA y el mediador)

En el caso de una configuración de HA de Cloud Volumes ONTAP que se implementa en múltiples zonas de disponibilidad, el mediador de HA necesita permisos específicos para escribir en las tablas de rutas en la cuenta del propietario de VPC. Debe proporcionar esos permisos configurando un rol de IAM que el mediador pueda asumir.

La siguiente imagen muestra los componentes involucrados en esta implementación:



Como se describe en los pasos a continuación, deberá compartir las subredes con la cuenta del participante y luego crear la función de IAM y el grupo de seguridad en la cuenta del propietario de VPC.

Cuando se crea el sistema Cloud Volumes ONTAP , la NetApp Console crea y adjunta automáticamente una función de IAM al mediador. Esta función asume la función de IAM que creó en la cuenta del propietario de VPC para realizar cambios en las tablas de rutas asociadas con el par HA.

Pasos

1. Comparta las subredes en la cuenta del propietario de VPC con la cuenta del participante.

   Este paso es necesario para implementar el par HA en subredes compartidas.

   "Documentación de AWS: Compartir una subred"

2. En la cuenta del propietario de VPC, cree un grupo de seguridad para Cloud Volumes ONTAP.

   "Consulte las reglas del grupo de seguridad para Cloud Volumes ONTAP" . Tenga en cuenta que no es necesario crear un grupo de seguridad para el mediador de HA. La consola lo hace por ti.

3. En la cuenta del propietario de VPC, cree un rol de IAM que incluya los siguientes permisos:

```
Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
```

4. Utilice la API para crear un nuevo sistema Cloud Volumes ONTAP .

   Tenga en cuenta que debe especificar los siguientes campos:

   - "ID de grupo de seguridad"

     El campo "securityGroupId" debe especificar el grupo de seguridad que creó en la cuenta del propietario de VPC (consulte el paso 2 anterior).

   - "assumeRoleArn" en el objeto "haParams"

     El campo "assumeRoleArn" debe incluir el ARN del rol de IAM que creó en la cuenta del propietario de VPC (consulte el paso 3 anterior).

     Por ejemplo:

```
"haParams": {
     "assumeRoleArn":
"arn:aws:iam::642991768967:role/mediator_role_assume_fromdev"
}
```

   +
   "Obtenga más información sobre la API de Cloud Volumes ONTAP"

Configurar la creación de grupos de ubicación para pares de alta disponibilidad de Cloud Volumes ONTAP en zonas de disponibilidad únicas de AWS

Las implementaciones de alta disponibilidad (HA) de Cloud Volumes ONTAP en la zona de disponibilidad única (AZ) de AWS pueden fallar y revertirse si falla la creación del

grupo de ubicación. La creación del grupo de ubicación también falla y la implementación se revierte si el nodo de Cloud Volumes ONTAP y la instancia del mediador no están disponibles. Para evitar esto, puede modificar la configuración para permitir que la implementación finalice incluso si falla la creación del grupo de ubicación.

Al omitir el proceso de reversión, el proceso de implementación de Cloud Volumes ONTAP se completa correctamente y le notifica que la creación del grupo de ubicación está incompleta.

Pasos

1. Utilice SSH para conectarse al host del agente de la NetApp Console e iniciar sesión.
2. Navegar a `/opt/application/netapp/cloudmanager/docker_occm/data` .
3. Editar `app.conf` cambiando el valor de la `rollback-on-placement-group-failure` parámetro a `false` . El valor predeterminado de este parámetro es `true` .

```
{
    "occm" : {
        "aws" : {
            "rollback-on-placement-group-failure" : false
        }
    }
}
```

4. Guarde el archivo y cierre la sesión del agente de la consola. No es necesario reiniciar el agente de la consola.

Reglas de entrada y salida del grupo de seguridad de AWS para Cloud Volumes ONTAP

La NetApp Console crea grupos de seguridad de AWS que incluyen las reglas de entrada y salida que Cloud Volumes ONTAP necesita para funcionar correctamente. Es posible que desees consultar los puertos para fines de prueba o si prefieres utilizar tus propios grupos de seguridad.

Reglas para Cloud Volumes ONTAP

El grupo de seguridad de Cloud Volumes ONTAP requiere reglas entrantes y salientes.

Reglas de entrada

Cuando agrega un sistema Cloud Volumes ONTAP y elige un grupo de seguridad predefinido, puede optar por permitir el tráfico dentro de uno de los siguientes:

- **Solo VPC seleccionada**: la fuente del tráfico entrante es el rango de subred de la VPC para el sistema Cloud Volumes ONTAP y el rango de subred de la VPC donde reside el agente de la consola. Esta es la opción recomendada.
- **Todas las VPC**: la fuente del tráfico entrante es el rango de IP 0.0.0.0/0.

Protocolo	Puerto	Objetivo
Todos los ICMP	Todo	Haciendo ping a la instancia
HTTP	80	Acceso HTTP a la consola web de ONTAP System Manager mediante la dirección IP del LIF de administración del clúster
HTTPS	443	Conectividad con el agente de la consola y acceso HTTPS a la consola web de ONTAP System Manager mediante la dirección IP del LIF de administración del clúster
SSH	22	Acceso SSH a la dirección IP del LIF de administración del clúster o de un LIF de administración 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	Demonio del servidor NFS
TCP	3260	Acceso iSCSI a través del LIF de datos iSCSI
TCP	4045	Demonio de bloqueo NFS
TCP	4046	Monitor de estado de red para NFS
TCP	10000	Copia de seguridad mediante NDMP
TCP	11104	Gestión de sesiones de comunicación entre clústeres para SnapMirror
TCP	11105	Transferencia de datos de SnapMirror mediante LIF entre clústeres
UDP	111	Llamada a procedimiento remoto para NFS
UDP	161-162	Protocolo simple de gestión de red
UDP	635	Montaje NFS
UDP	2049	Demonio del servidor NFS
UDP	4045	Demonio de bloqueo NFS
UDP	4046	Monitor de estado de red para NFS
UDP	4049	Protocolo rquotad de NFS

Reglas de salida

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

Reglas básicas de salida

El grupo de seguridad predefinido para Cloud Volumes ONTAP incluye las siguientes reglas de salida.

Protocolo	Puerto	Objetivo
Todos los ICMP	Todo	Todo el tráfico saliente
Todos los TCP	Todo	Todo el tráfico saliente
Todos los UDP	Todo	Todo el tráfico saliente

Reglas de salida avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede usar la siguiente información para abrir solo aquellos puertos que Cloud Volumes ONTAP requiere para la comunicación saliente.

La fuente es la interfaz (dirección IP) en el sistema Cloud Volumes ONTAP .

Servicio	Protocolo	Puerto	Fuente	Destino	Objetivo
Directorio activo	TCP	88	LIF de gestión de nodos	Bosque de Active Directory	Autenticación Kerberos V
	UDP	137	LIF de gestión de nodos	Bosque de Active Directory	Servicio de nombres NetBIOS
	UDP	138	LIF de gestión de nodos	Bosque de Active Directory	Servicio de datagramas NetBIOS
	TCP	139	LIF de gestión de nodos	Bosque de Active Directory	Sesión de servicio NetBIOS
	TCP y UDP	389	LIF de gestión de nodos	Bosque de Active Directory	LDAP
	TCP	445	LIF de gestión de nodos	Bosque de Active Directory	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
	TCP	464	LIF de gestión de nodos	Bosque de Active Directory	Cambiar y establecer contraseña de Kerberos V (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	Cambiar y establecer contraseña de Kerberos V (RPCSEC_GSS)
	TCP	88	Datos LIF (NFS, CIFS, iSCSI)	Bosque de Active Directory	Autenticación Kerberos V
	UDP	137	Datos LIF (NFS, CIFS)	Bosque de Active Directory	Servicio de nombres NetBIOS
	UDP	138	Datos LIF (NFS, CIFS)	Bosque de Active Directory	Servicio de datagramas NetBIOS
	TCP	139	Datos LIF (NFS, CIFS)	Bosque de Active Directory	Sesión de servicio NetBIOS
	TCP y UDP	389	Datos LIF (NFS, CIFS)	Bosque de Active Directory	LDAP
	TCP	445	Datos LIF (NFS, CIFS)	Bosque de Active Directory	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
	TCP	464	Datos LIF (NFS, CIFS)	Bosque de Active Directory	Cambiar y establecer contraseña de Kerberos V (SET_CHANGE)
	UDP	464	Datos LIF (NFS, CIFS)	Bosque de Active Directory	Administración de claves Kerberos
	TCP	749	Datos LIF (NFS, CIFS)	Bosque de Active Directory	Cambiar y establecer contraseña de Kerberos V (RPCSEC_GSS)

Servicio	Protocolo	Puerto	Fuente	Destino	Objetivo
AutoSupport	HTTPS	443	LIF de gestión de nodos	mysupport.netapp.com	AutoSupport (HTTPS es el predeterminado)
	HTTP	80	LIF de gestión de nodos	mysupport.netapp.com	AutoSupport (solo si el protocolo de transporte se cambia de HTTPS a HTTP)
	TCP	3128	LIF de gestión de nodos	Agente de consola	Envío de mensajes de AutoSupport a través de un servidor proxy en el agente de la consola, si no hay una conexión a Internet saliente disponible
Copia de seguridad en S3	TCP	5010	LIF entre clústeres	Realizar una copia de seguridad del punto final o restaurarlo	Operaciones de copia de seguridad y restauración para la función Copia de seguridad en S3
Grupo	Todo el tráfico	Todo el tráfico	Todos los LIF en un nodo	Todos los LIF en el otro nodo	Comunicaciones entre clústeres (solo Cloud Volumes ONTAP HA)
	TCP	3000	LIF de gestión de nodos	mediador de HA	Llamadas ZAPI (solo Cloud Volumes ONTAP HA)
	ICMP	1	LIF de gestión de nodos	mediador de HA	Mantener activo (solo Cloud Volumes ONTAP HA)
Copias de seguridad de configuración	HTTP	80	LIF de gestión de nodos	http://<dirección IP del agente de consola>/occm/offboxconfig	Envía copias de seguridad de la configuración al agente de la consola."Documentación de ONTAP"
DHCP	UDP	68	LIF de gestión de nodos	DHCP	Cliente DHCP para la primera configuración
DHCP	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, se pueden utilizar para AutoSupport

Servicio	Protocolo	Puerto	Fuente	Destino	Objetivo
SNMP	TCP	161	LIF de gestión de nodos	Servidor de monitorización	Monitoreo mediante trampas SNMP
	UDP	161	LIF de gestión de nodos	Servidor de monitorización	Monitoreo mediante trampas SNMP
	TCP	162	LIF de gestión de nodos	Servidor de monitorización	Monitoreo mediante trampas SNMP
	UDP	162	LIF de gestión de nodos	Servidor de monitorización	Monitoreo mediante trampas SNMP
SnapMirror	TCP	11104	LIF entre clústeres	LIF entre clústeres de ONTAP	Gestión de sesiones de comunicación entre clústeres para SnapMirror
	TCP	11105	LIF entre clústeres	LIF entre clústeres de ONTAP	Transferencia de datos de SnapMirror
Registro del sistema	UDP	514	LIF de gestión de nodos	Servidor de syslog	Mensajes de reenvío de syslog

Reglas para el grupo de seguridad externo del mediador de HA

El grupo de seguridad externo predefinido para el mediador de Cloud Volumes ONTAP HA incluye las siguientes reglas de entrada y salida.

Reglas de entrada

El grupo de seguridad predefinido para el mediador de HA incluye la siguiente regla de entrada.

Protocolo	Puerto	Fuente	Objetivo
TCP	3000	CIDR del agente de consola	Acceso a la API RESTful desde el agente de la consola

Reglas de salida

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

Reglas básicas de salida

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

Protocolo	Puerto	Objetivo
Todos los TCP	Todo	Todo el tráfico saliente
Todos los UDP	Todo	Todo el tráfico saliente

Reglas de salida avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede utilizar la siguiente información para abrir únicamente aquellos puertos que el mediador de HA requiere para la comunicación saliente.

Protocolo	Puerto	Destino	Objetivo
HTTP	80	Dirección IP del agente de la consola en la instancia de AWS EC2	Descargar actualizaciones para el mediador
HTTPS	443	ec2.amazonaws.com	Ayudar con la conmutación por error del almacenamiento
UDP	53	ec2.amazonaws.com	Ayudar con la conmutación por error del almacenamiento

En lugar de abrir los puertos 443 y 53, puede crear un punto final de interfaz VPC desde la subred de destino al servicio AWS EC2.

Reglas para el grupo de seguridad interna de configuración de HA

El grupo de seguridad interna predefinido para una configuración de Cloud Volumes ONTAP HA incluye las siguientes reglas. Este grupo de seguridad permite la comunicación entre los nodos HA y entre el mediador y los nodos.

La consola siempre crea este grupo de seguridad. No tienes la opción de utilizar el tuyo propio.

Reglas de entrada

El grupo de seguridad predefinido incluye las siguientes reglas de entrada.

Protocolo	Puerto	Objetivo
Todo el tráfico	Todo	Comunicación entre el mediador de HA y los nodos de HA

Reglas de salida

El grupo de seguridad predefinido incluye las siguientes reglas de salida.

Protocolo	Puerto	Objetivo
Todo el tráfico	Todo	Comunicación entre el mediador de HA y los nodos de HA

Reglas para el agente de consola

"Ver las reglas del grupo de seguridad para el agente de la consola"