



## **Configure su red**

### Cloud Volumes ONTAP

NetApp  
March 06, 2023

# Tabla de Contenido

- Configure su red ..... 1
  - Requisitos de red para Cloud Volumes ONTAP en AWS ..... 1
  - Configuración de una puerta de enlace de tránsito de AWS para parejas de alta disponibilidad en AZs múltiples ..... 9
  - Ponga en marcha un par de alta disponibilidad en una subred compartida ..... 14
  - Reglas de grupos de seguridad para AWS ..... 16

# Configure su red

## Requisitos de red para Cloud Volumes ONTAP en AWS

BlueXP gestiona la configuración de componentes de red para Cloud Volumes ONTAP, como direcciones IP, máscaras de red y rutas. Debe asegurarse de que el acceso saliente a Internet está disponible, de que hay suficientes direcciones IP privadas disponibles, de que las conexiones correctas están en su lugar, y mucho más.

### Requisitos generales

Los siguientes requisitos deben satisfacerse en AWS.

#### Acceso a Internet saliente para nodos Cloud Volumes ONTAP

Los nodos Cloud Volumes ONTAP requieren acceso a Internet de salida para AutoSupport de NetApp, que supervisa de forma proactiva el estado del sistema y envía mensajes al soporte técnico de NetApp.

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>

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.

Si una conexión a Internet saliente no está disponible para enviar mensajes AutoSupport, BlueXP configura automáticamente sus sistemas Cloud Volumes ONTAP para utilizar el conector como servidor proxy. El único requisito es asegurarse de que el grupo de seguridad del conector permita conexiones *entrante* a través del puerto 3128. Tendrá que abrir este puerto después de desplegar el conector.

Si ha definido reglas de salida estrictas para Cloud Volumes ONTAP, también tendrá que asegurarse de que el grupo de seguridad Cloud Volumes ONTAP permita conexiones *saliente* a través del puerto 3128.

Una vez que haya comprobado que el acceso saliente a Internet está disponible, puede probar AutoSupport para asegurarse de que puede enviar mensajes. Para obtener instrucciones, consulte ["Documentos de ONTAP: Configure AutoSupport"](#).

Si BlueXP notifica que los mensajes de AutoSupport no se pueden enviar, ["Solucione problemas de configuración de AutoSupport"](#).

#### Acceso saliente a Internet para el mediador de alta disponibilidad

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

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

## **Direcciones IP privadas**

BlueXP asigna automáticamente el número requerido de direcciones IP privadas a Cloud Volumes ONTAP. Debe asegurarse de que las redes tengan suficientes direcciones IP privadas disponibles.

El número de LIF que BlueXP asigna a Cloud Volumes ONTAP depende de si pone en marcha un sistema de nodo único o un par de alta disponibilidad. Una LIF es una dirección IP asociada con un puerto físico.

### **Direcciones IP para un sistema de nodo único**

BlueXP asigna 6 direcciones IP a un sistema de un solo nodo:

- LIF de gestión de clústeres
- LIF de gestión de nodos
- LIF entre clústeres
- LIF de datos NAS
- LIF de datos iSCSI
- LIF de gestión de máquinas virtuales de almacenamiento

Una LIF de gestión de máquinas virtuales de almacenamiento se utiliza con herramientas de gestión como SnapCenter.

### **Direcciones IP para pares de alta disponibilidad**

Los pares de ALTA DISPONIBILIDAD requieren más direcciones IP que un sistema de nodo único. Estas direcciones IP se distribuyen entre interfaces ethernet diferentes, como se muestra en la siguiente imagen:



El número de direcciones IP privadas necesarias para un par de alta disponibilidad depende del modelo de puesta en marcha que elija. Un par de alta disponibilidad implementado en una zona de disponibilidad de AWS (AZ) *single* requiere 15 direcciones IP privadas, mientras que un par de alta disponibilidad implementado en *Multiple AZs* requiere 13 direcciones IP privadas.

En las tablas siguientes se ofrecen detalles acerca de las LIF asociadas con cada dirección IP privada.

**LIF para pares de alta disponibilidad en un único AZ**

LUN	Interfaz	Nodo	Específico
Gestión de clústeres	eth0	nodo 1	Gestión administrativa de todo el clúster (pareja de alta disponibilidad).
Gestión de nodos	eth0	nodo 1 y nodo 2	La gestión administrativa de un nodo.
Interconexión de clústeres	eth0	nodo 1 y nodo 2	Comunicación entre clústeres, backup y replicación.
Datos de NAS	eth0	nodo 1	Acceso de clientes a través de protocolos NAS.

LUN	Interfaz	Nodo	Específico
Datos de iSCSI	eth0	nodo 1 y nodo 2	Acceso de cliente a través del protocolo iSCSI. También lo utiliza el sistema 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 que muevan datos dentro del clúster.
Conectividad de alta DISPONIBILIDAD	eth2	nodo 1 y nodo 2	Comunicación entre los dos nodos en caso de conmutación al nodo de respaldo.
Tráfico iSCSI de RSM	eth3	nodo 1 y nodo 2	Tráfico iSCSI de RAID SyncMirror, así como 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 ayudarlo a tomar la toma de control y los procesos de devolución del almacenamiento.

#### LIF para pares de alta disponibilidad en múltiples AZs

LUN	Interfaz	Nodo	Específico
Gestión de nodos	eth0	nodo 1 y nodo 2	La gestión administrativa de un nodo.
Interconexión de clústeres	eth0	nodo 1 y nodo 2	Comunicación entre clústeres, backup y replicación.
Datos de iSCSI	eth0	nodo 1 y nodo 2	Acceso de cliente a través del protocolo iSCSI. Este LIF también gestiona la migración de direcciones IP flotantes entre nodos.
Conectividad del clúster	eth1	nodo 1 y nodo 2	Permite que los nodos se comuniquen entre sí y que muevan datos dentro del clúster.
Conectividad de alta DISPONIBILIDAD	eth2	nodo 1 y nodo 2	Comunicación entre los dos nodos en caso de conmutación al nodo de respaldo.
Tráfico iSCSI de RSM	eth3	nodo 1 y nodo 2	Tráfico iSCSI de RAID SyncMirror, así como 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 ayudarlo a tomar la toma de control y los procesos de devolución del almacenamiento.



Quando se implementan en varias zonas de disponibilidad, hay varias LIF asociadas con "Direcciones IP flotantes", Que no cuentan con el límite de IP privada de AWS.

## Grupos de seguridad

No necesita crear grupos de seguridad porque BlueXP lo hace por usted. Si necesita utilizar el suyo propio, consulte ["Reglas de grupo de seguridad"](#).



¿Busca información sobre el conector? ["Ver reglas de grupo de seguridad para el conector"](#)

## Conexión para la organización en niveles de datos

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

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, la red de la empresa. 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"](#).

## Uso compartido de VPC

A partir del lanzamiento de la versión 9.11.1, se admiten los pares de alta disponibilidad de Cloud Volumes ONTAP en AWS con el uso compartido de VPC. El uso compartido de VPC permite a la organización compartir subredes con otras cuentas de AWS. Para utilizar esta configuración, debe configurar su entorno AWS y después implementar el par de alta disponibilidad mediante la API.

["Descubra cómo implementar un par de alta disponibilidad en una subred compartida"](#).

## Requisitos para pares de alta disponibilidad en varios AZs

Los requisitos de red adicionales de AWS se aplican a configuraciones de alta disponibilidad de Cloud Volumes ONTAP que utilizan varias zonas de disponibilidad (AZs). Debe revisar estos requisitos antes de iniciar un par ha porque debe introducir los detalles de red en BlueXP al crear el entorno de trabajo.

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.

Debe haber una subred disponible en cada zona de 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.

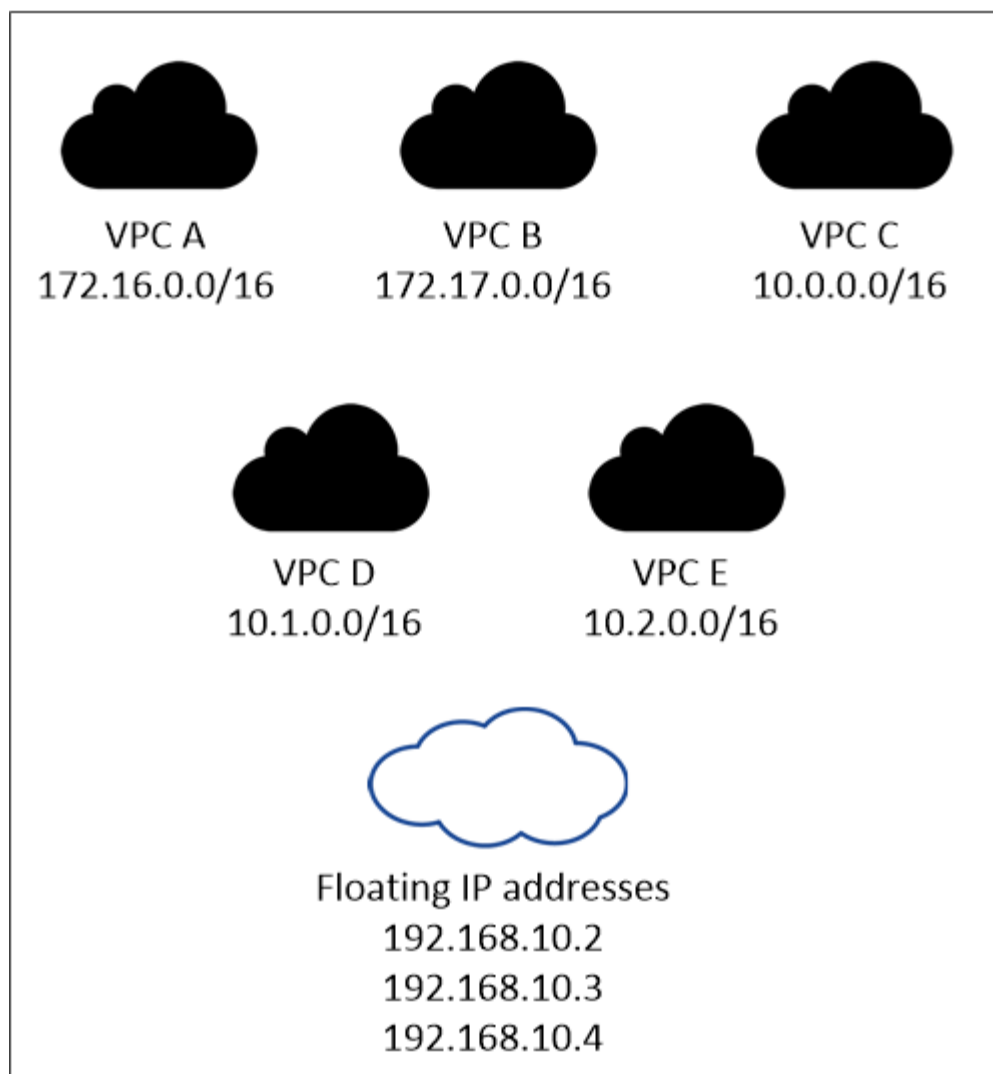
Debe introducir las direcciones IP flotantes en BlueXP cuando cree un entorno de trabajo de alta disponibilidad de Cloud Volumes ONTAP. BlueXP asigna las direcciones IP al par ha cuando ejecuta el sistema.

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



BlueXP 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

Si es necesario, ["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 BlueXP, se le pedirá que seleccione las tablas de rutas que deben 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 su VPC (la tabla de rutas principal), BlueXP agrega automáticamente las direcciones IP flotantes a esa tabla de rutas. Si dispone de más de una tabla de rutas, es muy importante seleccionar las tablas de rutas correctas al iniciar el par ha. De lo contrario, es posible que algunos clientes no tengan acceso a Cloud Volumes ONTAP.

Por ejemplo, puede tener dos subredes asociadas a diferentes tablas de rutas. Si selecciona la tabla DE rutas A, pero no la tabla de rutas B, los clientes de la subred asociada a la tabla DE rutas A pueden acceder al par de alta disponibilidad, pero los clientes de la subred asociada a la tabla de rutas B no pueden.

Para obtener más información sobre las tablas de rutas, consulte ["Documentación de AWS: Tablas de rutas"](#).

### **Conexión a herramientas de gestión de NetApp**

Para utilizar las herramientas de gestión de NetApp con configuraciones de alta disponibilidad que se encuentran en múltiples AZs, tiene dos opciones de conexión:

1. Puesta en marcha de las herramientas de gestión de NetApp en otro VPC y otras ["Configure una puerta de enlace de tránsito de AWS"](#). La puerta de enlace permite el acceso a la dirección IP flotante para la interfaz de gestión del clúster desde fuera del VPC.
2. Ponga en marcha las herramientas de gestión de NetApp en el mismo VPC con una configuración de enrutamiento similar a las de los clientes NAS.

### **Ejemplo de configuración de alta disponibilidad**

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



## Requisitos para el conector

Si aún no ha creado un conector, debe revisar los requisitos de red para el conector también.

- ["Ver los requisitos de red del conector"](#)
- ["Reglas del grupo de seguridad en AWS"](#)

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

Configure una puerta de enlace de tránsito de AWS para permitir el acceso a. Pares de

alta disponibilidad "**Direcciones IP flotantes**" Desde fuera del VPC, donde reside el par de alta disponibilidad.

Cuando una configuración de alta disponibilidad de Cloud Volumes ONTAP se distribuye por varias zonas de disponibilidad de AWS, se necesitan direcciones IP flotantes para el acceso a datos de NAS desde el VPC. Estas direcciones IP flotantes pueden migrar entre nodos cuando se producen fallos, pero no están accesibles desde fuera del VPC de forma nativa. Las direcciones IP privadas independientes proporcionan acceso a los datos desde fuera del VPC, pero no proporcionan una recuperación tras fallos automática.

Las direcciones IP flotantes también se requieren para la interfaz de gestión de clústeres y la LIF de gestión de SVM opcional.

Si configura una puerta de enlace de tránsito de AWS, debe habilitar el acceso a las direcciones IP flotantes desde fuera del VPC donde reside el par de alta disponibilidad. Esto significa que los clientes NAS y las herramientas de gestión de NetApp fuera del VPC pueden acceder a las IP flotantes.

Este es un ejemplo que muestra dos VPC conectados por una puerta de enlace de tránsito. Un sistema de alta disponibilidad reside en un VPC, mientras que un cliente reside en el otro. A continuación, podría montar un volumen NAS en el cliente mediante la dirección IP flotante.



Los siguientes pasos ilustran cómo configurar una configuración similar.

#### Pasos

1. "Cree una puerta de enlace de tránsito y conecte las VPC al puerta de enlace".
2. Asocie las VPC a 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, a continuación, seleccione **Crear asociación**.
  - d. Elija los archivos adjuntos (los VPC) que desea asociar y, a continuación, 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 de alta disponibilidad.

Puede encontrar las direcciones IP flotantes en la página Información del entorno de trabajo de BlueXP.

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-0ea8ee291c7aedd3

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

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

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

- Agregar entradas de ruta a las direcciones IP flotantes.
- 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	lgw-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

5. 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. BlueXP agregó automáticamente las IP flotantes a la tabla de rutas cuando implementó el par ha.

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	lgw-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

6. Montar volúmenes en clientes con la dirección IP flotante.

Puede encontrar la dirección IP correcta en BlueXP seleccionando un volumen y haciendo clic en **comando de montaje**.

## Volumes

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



7. Si va a montar un volumen de NFS, configure la política de exportación para que coincida con la subred del 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"](#)

## Ponga en marcha un par de alta disponibilidad en una subred compartida

A partir del lanzamiento de la versión 9.11.1, se admiten los pares de alta disponibilidad de Cloud Volumes ONTAP en AWS con el uso compartido de VPC. El uso compartido de VPC permite a la organización compartir subredes con otras cuentas de AWS. Para utilizar esta configuración, debe configurar su entorno AWS y después implementar el par de alta disponibilidad mediante la API.

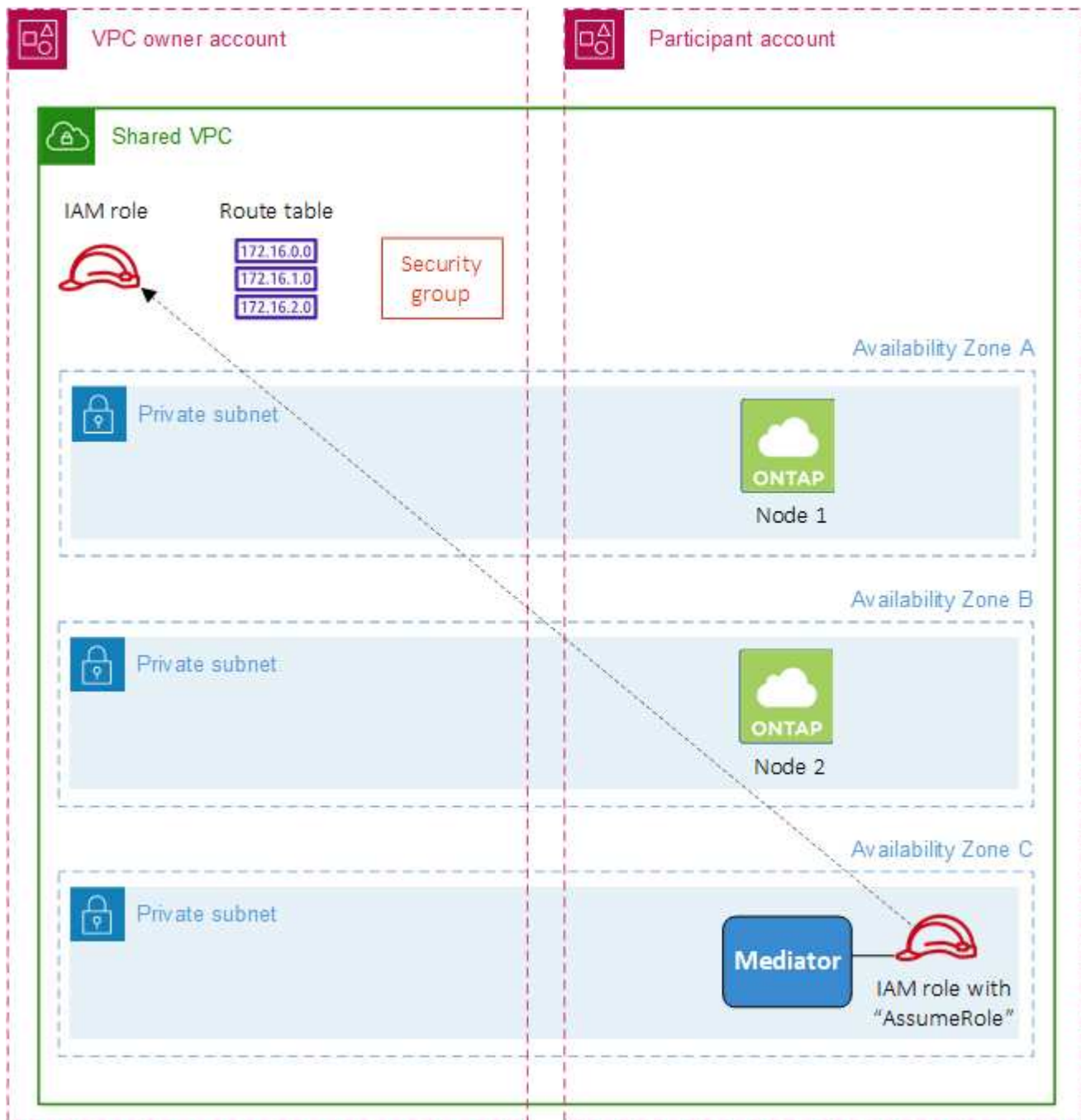
Con ["Uso compartido de VPC"](#), Una configuración de alta disponibilidad de Cloud Volumes ONTAP se distribuye entre dos cuentas:

- La cuenta de propietario de VPC, que posee las redes (el VPC, subredes, tablas de rutas y grupo de seguridad Cloud Volumes ONTAP).
- La cuenta de participante, donde las instancias de EC2 se ponen en marcha en subredes compartidas (esto incluye los dos nodos de alta disponibilidad y el mediador).

En el caso de una configuración de alta disponibilidad de Cloud Volumes ONTAP que se ponga en marcha en varias zonas de disponibilidad, el mediador de alta disponibilidad necesita permisos específicos para escribir en las tablas de rutas de la cuenta de propietario de VPC. Debe proporcionar estos permisos configurando una función de IAM que el mediador puede asumir.

La siguiente imagen muestra los componentes implicados en esta implementación:





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

Al crear el entorno de trabajo de Cloud Volumes ONTAP, BlueXP crea y adjunta automáticamente una función de IAM al mediador. Este rol asume la función IAM que se creó en la cuenta de propietario de VPC con el fin de realizar cambios en las tablas de ruta asociadas con el par de alta disponibilidad.

## Pasos

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

Este paso es necesario para poner en marcha el par de alta disponibilidad en subredes compartidas.

["Documentación de AWS: Comparta una subred"](#)

2. En la cuenta de 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 tiene que crear un grupo de seguridad para el mediador de alta disponibilidad. BlueXP lo hace por ti.

3. En la cuenta de 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. Use la API de BlueXP para crear un nuevo entorno de trabajo de Cloud Volumes ONTAP.

Tenga en cuenta que debe especificar los siguientes campos:

- "SecurityGroupId"

El campo "securityGroupId" debe especificar el grupo de seguridad que ha creado en la cuenta de 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 de propietario de VPC (consulte el paso 3 anterior).

Por ejemplo:

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

+

["Obtenga más información acerca de la API de Cloud Volumes ONTAP"](#)

## Reglas de grupos de seguridad para AWS

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

## Reglas para Cloud Volumes ONTAP

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

### Reglas de entrada

Al crear un entorno de trabajo y elegir un grupo de seguridad predefinido, puede optar por permitir el tráfico de una de las siguientes opciones:

- **VPC seleccionado sólo:** El origen del tráfico entrante es el rango de subred del VPC para el sistema Cloud Volumes ONTAP y el rango de subred del VPC donde reside el conector. Esta es la opción recomendada.
- **Todos los VPC:** La fuente de tráfico entrante es el rango IP 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	Conectividad con el acceso HTTPS y el conector a la consola web de System Manager mediante 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

Protocolo	Puerto	Específico
UDP	4045	Daemon de bloqueo NFS
UDP	4046	Supervisor de estado de red para NFS
UDP	4049	Protocolo rquotad NFS

## Reglas de salida

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

### Reglas de salida básicas

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

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

### Reglas salientes avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede utilizar la siguiente información para abrir sólo los puertos necesarios para la comunicación saliente por Cloud Volumes ONTAP.



El origen es la interfaz (dirección IP) en el sistema Cloud Volumes ONTAP.

Servicio	Protocolo	Puerto	Origen	Destino	Específico
Active Directory	TCP	88	LIF de gestión de nodos	Bosque de Active Directory	Autenticación Kerberos V.
	UDP	137	LIF de gestión de nodos	Bosque de Active Directory	Servicio de nombres NetBIOS
	UDP	138	LIF de gestión de nodos	Bosque de Active Directory	Servicio de datagramas NetBIOS
	TCP	139	LIF de gestión de nodos	Bosque de Active Directory	Sesión de servicio NetBIOS
	TCP Y UDP	389	LIF de gestión de nodos	Bosque de Active Directory	LDAP
	TCP	445	LIF de gestión de nodos	Bosque de Active Directory	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
	TCP	464	LIF de gestión de nodos	Bosque de Active Directory	Kerberos V cambiar y establecer contraseña (SET_CHANGE)
	UDP	464	LIF de gestión de nodos	Bosque de Active Directory	Administración de claves Kerberos
	TCP	749	LIF de gestión de nodos	Bosque de Active Directory	Contraseña de Kerberos V Change & Set (RPCSEC_GSS)
	TCP	88	LIF de datos (NFS, CIFS e iSCSI)	Bosque de Active Directory	Autenticación Kerberos V.
	UDP	137	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Servicio de nombres NetBIOS
	UDP	138	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Servicio de datagramas NetBIOS
	TCP	139	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Sesión de servicio NetBIOS
	TCP Y UDP	389	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	LDAP
	TCP	445	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
	TCP	464	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Kerberos V cambiar y establecer contraseña (SET_CHANGE)
	UDP	464	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Administración de claves Kerberos
	TCP	749	LIF DE DATOS (NFS, CIFS)	Bosque de Active Directory	Contraseña de Kerberos V change & set (RPCSEC_GSS)

Servicio	Protocolo	Puerto	Origen	Destino	Específico
AutoSupport	HTTPS	443	LIF de gestión de nodos	support.netapp.com	AutoSupport (HTTPS es la predeterminada)
	HTTP	80	LIF de gestión de nodos	support.netapp.com	AutoSupport (solo si el protocolo de transporte cambia de HTTPS a HTTP)
	TCP	3128	LIF de gestión de nodos	Conector	Envío de mensajes AutoSupport a través de un servidor proxy en el conector, si no hay disponible una conexión a Internet saliente
Backup en S3	TCP	5010	LIF entre clústeres	Extremo de backup o extremo de restauración	Realizar backups y restaurar operaciones para el backup en S3 función
Clúster	Todo el tráfico	Todo el tráfico	Todos los LIF de un nodo	Todas las LIF del otro nodo	Comunicaciones de interconexión de clústeres (solo Cloud Volumes ONTAP de alta disponibilidad)
	TCP	3000	LIF de gestión de nodos	Mediador DE ALTA DISPONIBILIDAD	Llamadas ZAPI (solo alta disponibilidad de Cloud Volumes ONTAP)
	ICMP	1	LIF de gestión de nodos	Mediador DE ALTA DISPONIBILIDAD	Mantener activos (solo alta disponibilidad de Cloud Volumes ONTAP)
DHCP	UDP	68	LIF de gestión de nodos	DHCP	Cliente DHCP para la configuración inicial
DHCPs	UDP	67	LIF de gestión de nodos	DHCP	Servidor DHCP
DNS	UDP	53	LIF de gestión de nodos y LIF de datos (NFS, CIFS)	DNS	DNS
NDMP	TCP	1860–18699	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

Servicio	Protocolo	Puerto	Origen	Destino	Específico
SnapMirror	TCP	11104	LIF entre clústeres	LIF de interconexión de clústeres de ONTAP	Gestión de sesiones de comunicación de interconexión de clústeres para SnapMirror
	TCP	11105	LIF entre clústeres	LIF de interconexión de clústeres de ONTAP	Transferencia de datos de SnapMirror
Syslog	UDP	514	LIF de gestión de nodos	Servidor de syslog	Mensajes de syslog Reenviar

## Reglas para el grupo de seguridad externo de mediador de alta disponibilidad

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

### Reglas de entrada

La fuente de las reglas entrantes es 0.0.0.0/0.

Protocolo	Puerto	Específico
SSH	22	Conexiones SSH al mediador de alta disponibilidad
TCP	3000	Acceso a API RESTful desde el conector

### Reglas de salida

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

#### Reglas de salida básicas

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

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

#### Reglas salientes avanzadas

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

Protocolo	Puerto	Destino	Específico
HTTP	80	Dirección IP del conector	Descargar actualizaciones para el mediador
HTTPS	443	Servicios API de AWS	Ayudar en la recuperación tras fallos de almacenamiento

Protocolo	Puerto	Destino	Específico
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 interno de configuración de alta disponibilidad

El grupo de seguridad interno predefinido para una configuración de alta disponibilidad de Cloud Volumes ONTAP incluye las siguientes reglas. Este grupo de seguridad habilita la comunicación entre los nodos de alta disponibilidad y el mediador y los nodos.

BlueXP siempre crea este grupo de seguridad. No tiene la opción de utilizar la suya propia.

### Reglas de entrada

El grupo de seguridad predefinido incluye las siguientes reglas entrantes.

Protocolo	Puerto	Específico
Todo el tráfico	Todo	Comunicación entre el mediador de alta disponibilidad y los nodos de alta disponibilidad

### Reglas de salida

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

Protocolo	Puerto	Específico
Todo el tráfico	Todo	Comunicación entre el mediador de alta disponibilidad y los nodos de alta disponibilidad

## Reglas para el conector

["Ver reglas de grupo de seguridad para el conector"](#)



## Información de copyright

Copyright © 2023 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 INTERRUPCIÓN 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.