



Empiece a usar AWS

Cloud Manager 3.8

NetApp
March 25, 2024

Tabla de contenidos

- Empiece a usar AWS 1
- Introducción a Cloud Volumes ONTAP para AWS 1
- Planificar la configuración de Cloud Volumes ONTAP en AWS 2
- Configure su red 5
- Configuración de AWS KMS 24
- Inicio de Cloud Volumes ONTAP en AWS 27

Empiece a usar AWS

Introducción a Cloud Volumes ONTAP para AWS

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



Cree un conector

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

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



Planificación de la configuración

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



Configure su red

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

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

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

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

["Obtenga más información sobre los requisitos de red"](#).



Configure el KMS de AWS

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



Inicie Cloud Volumes ONTAP mediante Cloud Manager

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

Enlaces relacionados

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

Planificar la configuración de Cloud Volumes ONTAP en AWS

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

Seleccione un tipo de licencia

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

["Configuraciones compatibles para Cloud Volumes ONTAP 9.7 en AWS"](#)

Comprender los límites de almacenamiento

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

["Límites de almacenamiento para Cloud Volumes ONTAP 9.7 en AWS"](#)

Ajuste de tamaño de su sistema en AWS

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

Tipo de instancia

- Relacione los requisitos de carga de trabajo con el rendimiento máximo y las IOPS para cada tipo de instancia de EC2.
- Si varios usuarios escriben en el sistema al mismo tiempo, elija un tipo de instancia que tenga suficientes CPU para administrar las solicitudes.

- Si tiene una aplicación que está mayormente en lectura, elija un sistema con suficiente RAM.
 - ["Documentación de AWS: Tipos de instancias de Amazon EC2"](#)
 - ["Documentación de AWS: Instancias optimizadas para Amazon EBS"](#)

Tipo de disco de EBS

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

Tamaño del disco de EBS

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

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

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

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

 | <https://img.youtube.com/vi/GELcXmOuYPw/maxresdefault.jpg>

Elegir una configuración compatible con Flash Cache

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

Hoja de trabajo de información de red de AWS

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

Información de red para Cloud Volumes ONTAP

Información de AWS	Su valor
Región	
VPC	
Subred	

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

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

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

Elegir una velocidad de escritura

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

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

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

Al elegir una alta velocidad de escritura, los datos se guardan en búfer en la memoria antes de que se escriban en el disco, lo que proporciona un rendimiento de escritura más rápido. Gracias al almacenamiento

en caché, existe la posibilidad de perder datos en caso de que se produzca una interrupción no planificada del sistema.

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

Cuándo utilizar alta velocidad de escritura

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

Recomendaciones cuando se utiliza una alta velocidad de escritura

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

Selección de un perfil de uso de volumen

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

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

Aprovisionamiento ligero

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

Deduplicación

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

Compresión

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

Configure su red

Requisitos de red para Cloud Volumes ONTAP en AWS

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

Requisitos generales para Cloud Volumes ONTAP

Los siguientes requisitos deben satisfacerse en AWS.

Acceso a Internet saliente para nodos Cloud Volumes ONTAP

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

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

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

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

["Aprenda a configurar AutoSupport"](#).

Acceso saliente a Internet para el mediador de alta disponibilidad

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

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

Número de direcciones IP

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

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

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



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

Grupos de seguridad

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

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

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

[Crear un extremo de puerta de enlace](#)".

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

Si experimenta algún problema, consulte ["Centro de conocimientos de soporte de AWS: ¿por qué no puedo conectarme a un bloque de S3 mediante un extremo de VPC de puerta de enlace?"](#)

Conexiones a sistemas ONTAP en otras redes

Para replicar datos entre un sistema Cloud Volumes ONTAP en AWS y sistemas ONTAP en otras redes, debe tener una conexión VPN entre el VPC de AWS y la otra red, por ejemplo, un vnet de Azure o una red corporativa. Para ver instrucciones, consulte ["Documentación de AWS: Configuración de una conexión VPN de AWS"](#).

DNS y Active Directory para CIFS

Si desea aprovisionar almacenamiento CIFS, debe configurar DNS y Active Directory en AWS o ampliar la configuración de sus instalaciones a AWS.

El servidor DNS debe proporcionar servicios de resolución de nombres para el entorno de Active Directory. Puede configurar los conjuntos de opciones DHCP para que utilicen el servidor DNS EC2 predeterminado, que no debe ser el servidor DNS utilizado por el entorno de Active Directory.

Para obtener instrucciones, consulte ["Documentación de AWS: Active Directory Domain Services en AWS Cloud: Implementación de referencia de inicio rápido"](#).

Requisitos para pares de alta disponibilidad en varios AZs

Los requisitos de red adicionales de AWS se aplican a configuraciones de alta disponibilidad de Cloud Volumes ONTAP que utilizan varias zonas de disponibilidad (AZs). Debe revisar estos requisitos antes de iniciar una pareja de ha porque debe introducir los detalles de redes en Cloud Manager.

Para comprender cómo funcionan los pares de alta disponibilidad, consulte ["Pares de alta disponibilidad"](#).

Zonas de disponibilidad

Este modelo de puesta en marcha de alta disponibilidad utiliza varios AZs para garantizar una alta disponibilidad de sus datos. Debería utilizar una zona de disponibilidad dedicada para cada instancia de Cloud Volumes ONTAP y la instancia de mediador, que proporciona un canal de comunicación entre el par de alta disponibilidad.

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

Las configuraciones de ALTA DISPONIBILIDAD de varios AZs utilizan direcciones IP flotantes que migran entre nodos en caso de que se produzcan fallos. No se puede acceder a ellos de forma nativa desde fuera del VPC, a menos que usted ["Configure una puerta de enlace de tránsito de AWS"](#).

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



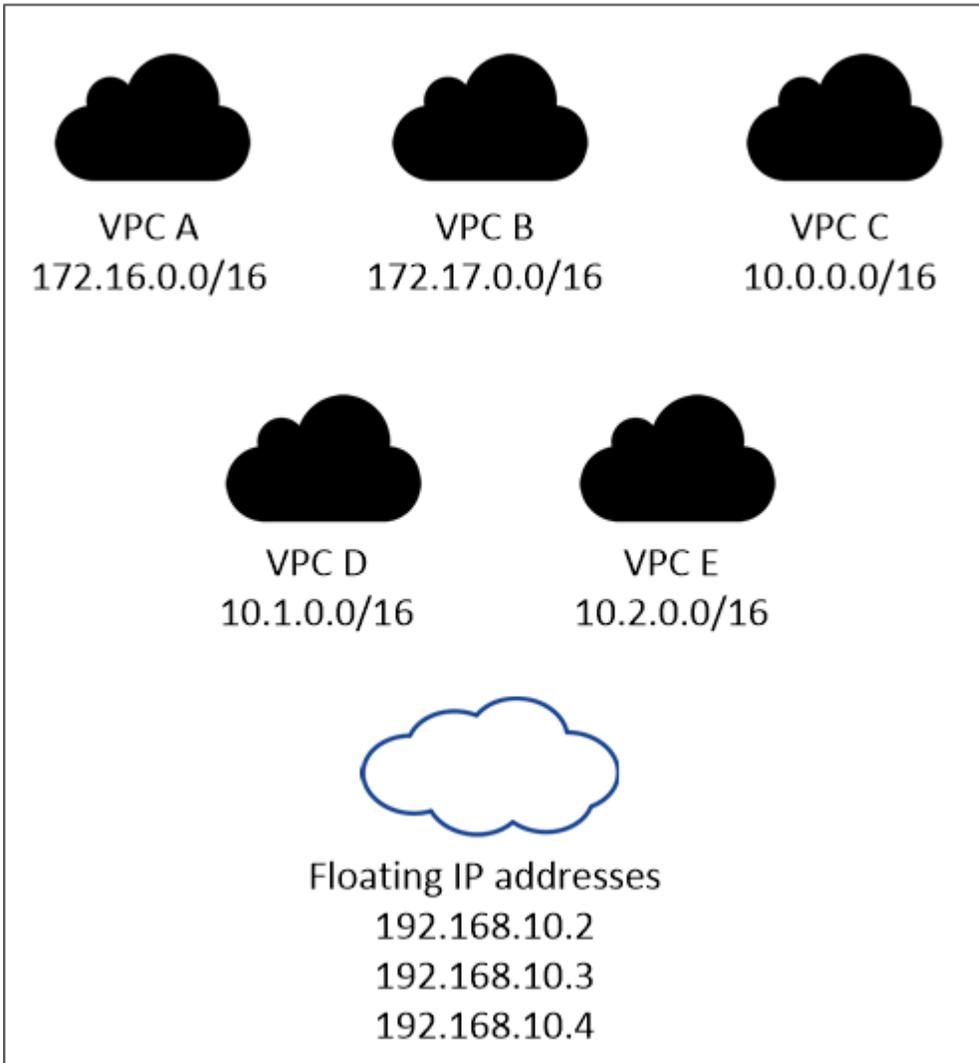
Se requiere una dirección IP flotante para el LIF de gestión de SVM si se usa SnapDrive para Windows o SnapCenter con el par de alta disponibilidad. Si no especifica la dirección IP al implementar el sistema, puede crear la LIF más adelante. Para obtener más información, consulte ["Configurar Cloud Volumes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

Debe introducir las direcciones IP flotantes en Cloud Manager cuando crea un entorno de trabajo de alta disponibilidad de Cloud Volumes ONTAP. Cloud Manager asigna las direcciones IP a la pareja de alta disponibilidad cuando arranca el sistema.

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

En el siguiente ejemplo se muestra la relación entre las direcciones IP flotantes y las VPC en una región de AWS. Mientras las direcciones IP flotantes están fuera de los bloques CIDR para todos los VPC, se pueden enrutar a subredes a través de tablas de ruta.

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](#)".

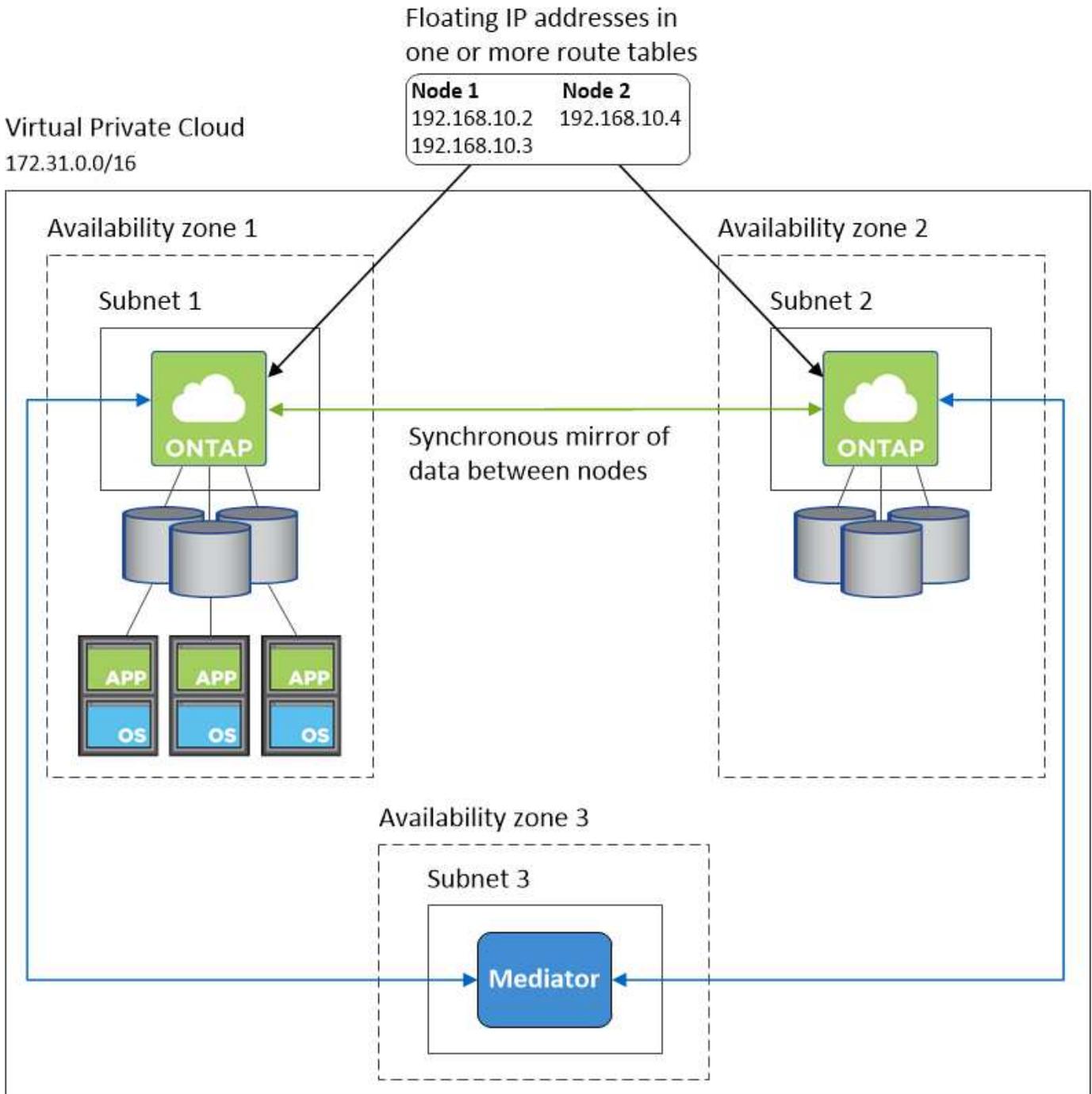
Conexión a herramientas de gestión de NetApp

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.

Ejemplo de configuración de alta disponibilidad

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



Requisitos para el conector

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



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

Conexión a redes de destino

Un conector requiere una conexión de red a los VPC y VNETs en los que desea implementar Cloud Volumes

ONTAP.

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

Acceso a Internet de salida

El conector requiere acceso saliente a Internet para gestionar recursos y procesos dentro de su entorno de nube pública. Un conector se pone en contacto con los siguientes extremos cuando se gestionan recursos en AWS:

Puntos finales	Específico
Servicios de AWS (amazonaws.com): <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) El extremo exacto depende de la región en la que se implemente Cloud Volumes ONTAP. "Consulte la documentación de AWS para obtener más detalles."	Permite que Cloud Manager ponga en marcha y gestione Cloud Volumes ONTAP en AWS.
https://api.services.cloud.netapp.com:443	Solicitudes de API a Cloud Central de NetApp.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Proporciona acceso a imágenes, manifiestos y plantillas de software.
https://repo.cloud.support.netapp.com	Se utiliza para descargar las dependencias de Cloud Manager.
http://repo.mysql.com/	Se utiliza para descargar MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Permite a Cloud Manager acceder y descargar manifiestos, plantillas e imágenes de actualización de Cloud Volumes ONTAP.
https://cloudmanagerinfraprod.azurecr.io	Acceso a imágenes de software de componentes de contenedor para una infraestructura que ejecuta Docker y proporciona una solución para las integraciones de servicios con Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Permite a NetApp transmitir datos desde registros de auditoría.
https://cloudmanager.cloud.netapp.com	Comunicación con el servicio Cloud Manager, que incluye cuentas de Cloud Central.
https://netapp-cloud-account.auth0.com	Comunicación con Cloud Central de NetApp para la autenticación de usuario centralizada.

Puntos finales	Específico
https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist	Se utiliza para añadir su ID de cuenta de AWS a la lista de usuarios permitidos para Backup en S3.
https://support.netapp.com/aods/asupmessage https://support.netapp.com/asupprod/post/1.0/postAsup	Comunicación con AutoSupport de NetApp.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Comunicación con NetApp para la licencia del sistema y el registro de soporte.
https://ipa-signer.cloudmanager.netapp.com	Permite que Cloud Manager genere licencias (por ejemplo, una licencia de FlexCache para Cloud Volumes ONTAP).
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Necesario para conectar los sistemas Cloud Volumes ONTAP con un clúster de Kubernetes. Los extremos permiten la instalación de Trident de NetApp.
Diversas ubicaciones de terceros, por ejemplo: <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.

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

Puntos finales	Específico
El host del conector	<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>

Puntos finales	Específico
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	El explorador web se conecta con estos extremos para conseguir una autenticación de usuario centralizada mediante NetApp Cloud Central.
https://widget.intercom.io	Si busca un chat integrado en los productos que le permita hablar con expertos en cloud de NetApp.

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

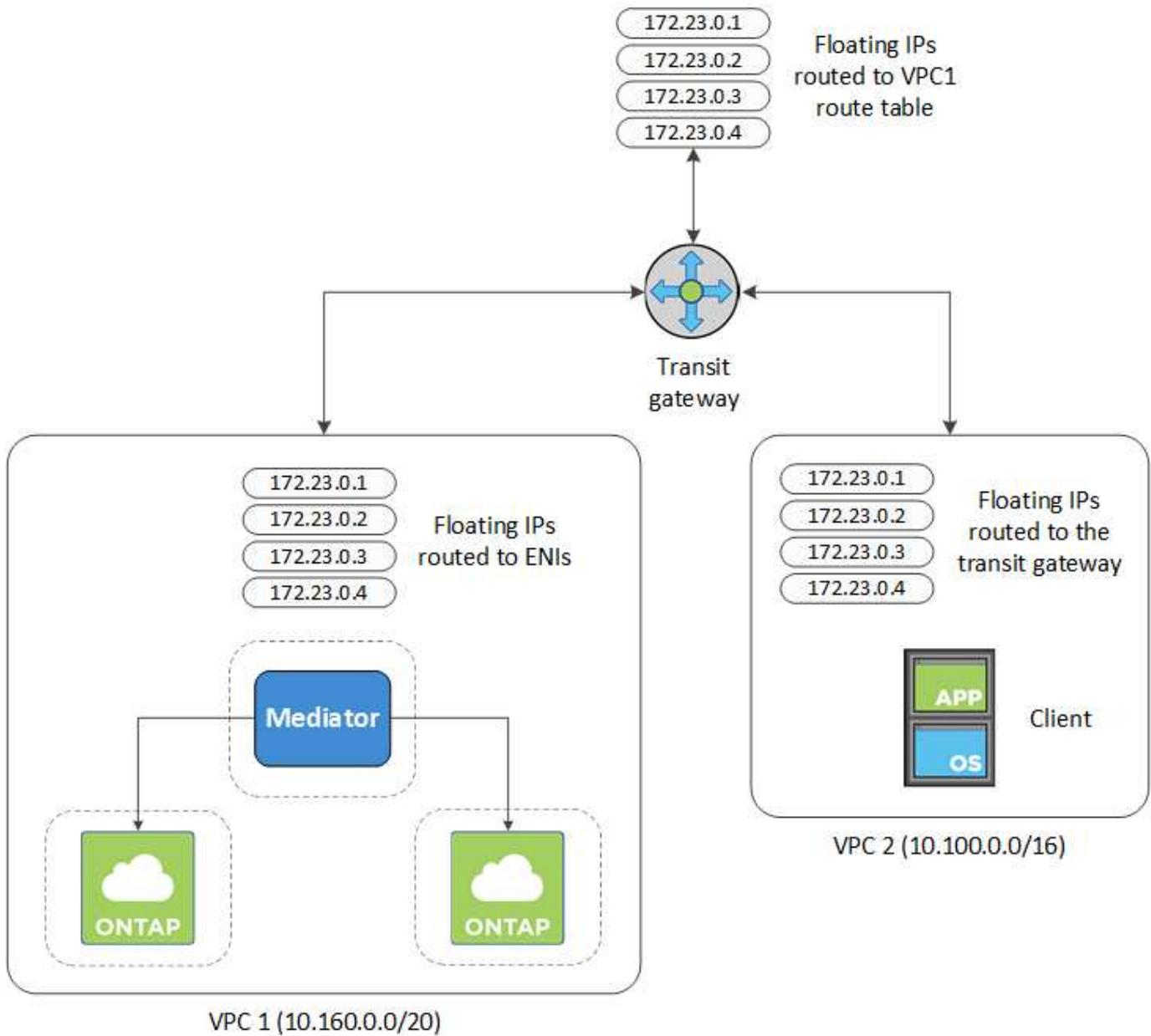
Configure una puerta de enlace de tránsito de AWS para permitir el acceso a Pares de alta disponibilidad "[Direcciones IP flotantes](#)" Desde fuera del VPC, donde reside el par de alta disponibilidad.

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

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

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

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



Los siguientes pasos ilustran cómo configurar una configuración similar.

Pasos

1. "Cree una puerta de enlace de tránsito y conecte las VPC al puerta de enlace".
2. Cree rutas en la tabla de rutas de la puerta de enlace de tránsito especificando las direcciones IP flotantes del par de alta disponibilidad.

Puede encontrar las direcciones IP flotantes en la página Información del entorno de trabajo de Cloud Manager. Veamos un ejemplo:

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

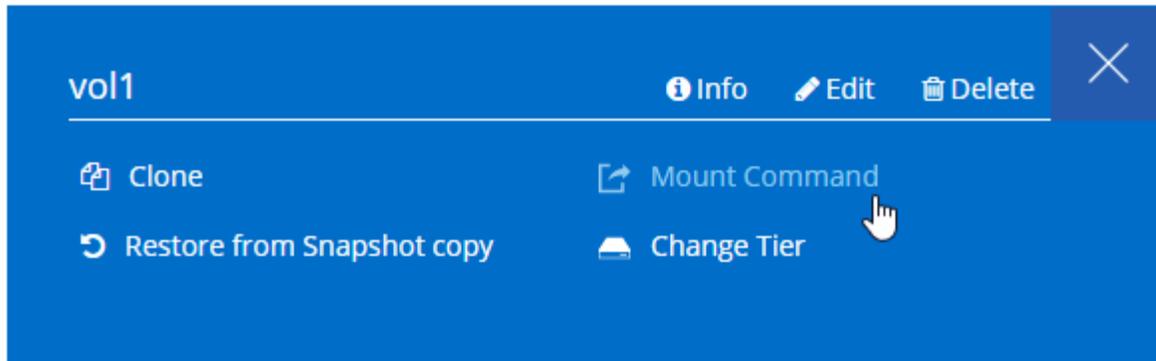
VPC2
Floating act IP Addresses

- 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"](#)

Reglas de grupos de seguridad para AWS

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

Reglas para Cloud Volumes ONTAP

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

Reglas de entrada

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

Protocolo	Puerto	Específico
Todos los ICMP	Todo	Hacer ping a la instancia
HTTP	80	Acceso HTTP a la consola web de System Manager mediante el La dirección IP de la LIF de gestión del clúster
HTTPS	443	Acceso HTTPS a la consola web de System Manager mediante el La dirección IP de la LIF de gestión del clúster
SSH	22	Acceso SSH a la dirección IP de administración del clúster LIF o una LIF de gestión de nodos
TCP	111	Llamada a procedimiento remoto para NFS

Protocolo	Puerto	Específico
TCP	139	Sesión de servicio NetBIOS para CIFS
TCP	161-162	Protocolo simple de gestión de red
TCP	445	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
TCP	635	Montaje NFS
TCP	749	Kerberos
TCP	2049	Daemon del servidor NFS
TCP	3260	Acceso iSCSI mediante la LIF de datos iSCSI
TCP	4045	Daemon de bloqueo NFS
TCP	4046	Supervisor de estado de red para NFS
TCP	10000	Backup con NDMP
TCP	11104	Gestión de sesiones de comunicación de interconexión de clústeres para SnapMirror
TCP	11105	Transferencia de datos de SnapMirror mediante LIF de interconexión de clústeres
UDP	111	Llamada a procedimiento remoto para NFS
UDP	161-162	Protocolo simple de gestión de red
UDP	635	Montaje NFS
UDP	2049	Daemon del servidor NFS
UDP	4045	Daemon de bloqueo NFS
UDP	4046	Supervisor de estado de red para NFS
UDP	4049	Protocolo rquotad NFS

Reglas de salida

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

Reglas de salida básicas

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

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

Reglas salientes avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede utilizar la siguiente información para abrir sólo los

puertos necesarios para la comunicación saliente por Cloud Volumes ONTAP.



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

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

Servicio	Protocolo	Puerto	Origen	Destino	Específico
Backup en S3	TCP	5010	LIF entre clústeres	Extremo de backup o extremo de restauración	Realizar backups y restaurar operaciones para el backup en S3 función
Clúster	Todo el tráfico	Todo el tráfico	Todos los LIF de un nodo	Todas las LIF del otro nodo	Comunicaciones de interconexión de clústeres (solo Cloud Volumes ONTAP de alta disponibilidad)
	TCP	3000	LIF de gestión de nodos	Mediador DE ALTA DISPONIBILIDAD	Llamadas ZAPI (solo alta disponibilidad de Cloud Volumes ONTAP)
	ICMP	1	LIF de gestión de nodos	Mediador DE ALTA DISPONIBILIDAD	Mantener activos (solo alta disponibilidad de Cloud Volumes ONTAP)
DHCP	UDP	68	LIF de gestión de nodos	DHCP	Cliente DHCP para la configuración inicial
DHCPS	UDP	67	LIF de gestión de nodos	DHCP	Servidor DHCP
DNS	UDP	53	LIF de gestión de nodos y LIF de datos (NFS, CIFS)	DNS	DNS
NDMP	TCP	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
SnapMirror	TCP	11104	LIF entre clústeres	LIF de interconexión de clústeres de ONTAP	Gestión de sesiones de comunicación de interconexión de clústeres para SnapMirror
	TCP	11105	LIF entre clústeres	LIF de interconexión de clústeres de ONTAP	Transferencia de datos de SnapMirror
Syslog	UDP	514	LIF de gestión de nodos	Servidor de syslog	Mensajes de syslog Reenviar

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

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

Reglas de entrada

La fuente de las reglas entrantes es 0.0.0.0/0.

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

Reglas de salida

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

Reglas de salida básicas

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

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

Reglas salientes avanzadas

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

Protocolo	Puerto	Destino	Específico
HTTP	80	Dirección IP del conector	Descargar actualizaciones para el mediador
HTTPS	443	Servicios API de AWS	Ayudar en la recuperación tras fallos de almacenamiento
UDP	53	Servicios API de AWS	Ayudar en la recuperación tras fallos de almacenamiento



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

Reglas para el grupo de seguridad interna de mediador de alta disponibilidad

El grupo de seguridad interna predefinido para el mediador de alta disponibilidad de Cloud Volumes ONTAP incluye las siguientes reglas. Cloud Manager siempre crea este grupo de seguridad. No tiene la opción de utilizar la suya propia.

Reglas de entrada

El grupo de seguridad predefinido incluye las siguientes reglas entrantes.

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

Reglas de salida

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

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

Reglas para el conector

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

Reglas de entrada

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

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

Reglas de salida

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

Reglas de salida básicas

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

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

Reglas salientes avanzadas

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



La dirección IP de origen es el host del conector.

Servicio	Protocolo	Puerto	Destino	Específico
Active Directory	TCP	88	Bosque de Active Directory	Autenticación Kerberos V.
	TCP	139	Bosque de Active Directory	Sesión de servicio NetBIOS
	TCP	389	Bosque de Active Directory	LDAP
	TCP	445	Bosque de Active Directory	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
	TCP	464	Bosque de Active Directory	Kerberos V cambiar y establecer contraseña (SET_CHANGE)
	TCP	749	Bosque de Active Directory	Contraseña de modificación y definición de Kerberos V de Active Directory (RPCSEC_GSS)
	UDP	137	Bosque de Active Directory	Servicio de nombres NetBIOS
	UDP	138	Bosque de Active Directory	Servicio de datagramas NetBIOS
	UDP	464	Bosque de Active Directory	Administración de claves Kerberos
Llamadas API y AutoSupport	HTTPS	443	LIF de gestión de clústeres de ONTAP y Internet saliente	API llama a AWS y ONTAP y envía mensajes de AutoSupport a NetApp
Llamadas API	TCP	3000	LIF de gestión de clústeres de ONTAP	Llamadas API a ONTAP
	TCP	8088	Backup en S3	Llamadas API a Backup en S3
DNS	UDP	53	DNS	Utilizado para resolver DNS por Cloud Manager

Servicio	Protocolo	Puerto	Destino	Específico
Cumplimiento de normativas en el cloud	HTTP	80	Instancia de cumplimiento de normativas cloud	Cumplimiento de normativas cloud para Cloud Volumes ONTAP

Configuración de AWS KMS

Si desea usar el cifrado de Amazon con Cloud Volumes ONTAP, debe configurar el servicio de gestión de claves (KMS) de AWS.

Pasos

1. Asegúrese de que existe una clave maestra de cliente (CMK) activa.

El CMK puede ser un CMK gestionado por AWS o un CMK gestionado por el cliente. Puede encontrarse en la misma cuenta de AWS que Cloud Manager y Cloud Volumes ONTAP, o en una cuenta de AWS diferente.

["Documentación de AWS: Claves maestras de clientes \(CMKs\)"](#)

2. Modifique la política de claves de cada CMK añadiendo el rol IAM que proporciona permisos a Cloud Manager como *key user*.

La adición del rol IAM como usuario clave permite a Cloud Manager utilizar el CMK con Cloud Volumes ONTAP.

["Documentación de AWS: Editar claves"](#)

3. Si el CMK se encuentra en una cuenta de AWS diferente, realice los pasos siguientes:

- a. Vaya a la consola KMS desde la cuenta donde reside el CMK.
- b. Seleccione la tecla.
- c. En el panel **Configuración general**, copie el ARN de la clave.

Deberá proporcionar el ARN al Cloud Manager cuando cree el sistema Cloud Volumes ONTAP.

- d. En el panel **otras cuentas de AWS**, agregue la cuenta de AWS que proporciona permisos a Cloud Manager.

En la mayoría de los casos, esta es la cuenta en la que reside Cloud Manager. Si Cloud Manager no se instaló en AWS, sería la cuenta para la que proporcionó las claves de acceso de AWS a Cloud Manager.



Other AWS accounts ✕

Specify the AWS accounts that can use this key. Administrators of the accounts you specify are responsible for managing the permissions that allow their IAM users and roles to use this key. [Learn more](#) 

arn:aws:iam:: :root

- e. Cambie ahora a la cuenta de AWS que proporciona permisos a Cloud Manager y abra la consola IAM.
- f. Cree una política de IAM que incluya los permisos que se indican a continuación.
- g. Asocie la política al rol de IAM o al usuario IAM que proporciona permisos a Cloud Manager.

La siguiente directiva proporciona los permisos que Cloud Manager necesita para utilizar CMK desde la cuenta de AWS externa. Asegúrese de modificar la región y el ID de cuenta en las secciones "Recursos".

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowUseOfTheKey",
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": [
        "arn:aws:kms:us-east-
1:externalaccountid:key/externalkeyid"
      ]
    },
    {
      "Sid": "AllowAttachmentOfPersistentResources",
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": [
        "arn:aws:kms:us-east-
1:externalaccountid:key/externalaccountid"
      ],
      "Condition": {
        "Bool": {
          "kms:GrantIsForAWSResource": true
        }
      }
    }
  ]
}

```

+

Para obtener más información sobre este proceso, consulte ["Documentación de AWS: Permitir que las cuentas de AWS externas puedan acceder a un CMK"](#).

Inicio de Cloud Volumes ONTAP en AWS

Puede iniciar Cloud Volumes ONTAP en una configuración con un único sistema o como par de alta disponibilidad en AWS.

Lanzar un sistema Cloud Volumes ONTAP de un único nodo en AWS

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

Antes de empezar

- Usted debe tener un ["Conector asociado al área de trabajo"](#).



Debe ser un administrador de cuentas para crear un conector. Al crear el primer entorno de trabajo de Cloud Volumes ONTAP, Cloud Manager le solicita que cree un conector si todavía no lo tiene.

- ["Debe estar preparado para dejar el conector funcionando en todo momento"](#).
- Debe haberse preparado eligiendo una configuración y obteniendo información de red de AWS de su administrador. Para obtener más información, consulte ["Planificación de la configuración de Cloud Volumes ONTAP"](#).
- Si desea iniciar un sistema BYOL, debe tener el número de serie de 20 dígitos (clave de licencia).
- Si desea usar CIFS, debe haber configurado DNS y Active Directory. Para obtener más información, consulte ["Requisitos de red para Cloud Volumes ONTAP en AWS"](#).

Acerca de esta tarea

Inmediatamente después de crear el entorno de trabajo, Cloud Manager inicia una instancia de prueba en el VPC especificado para verificar la conectividad. Si se realiza correctamente, Cloud Manager finaliza inmediatamente la instancia y después inicia la implementación del sistema Cloud Volumes ONTAP. Si Cloud Manager no puede verificar la conectividad, se produce un error en la creación del entorno de trabajo. La instancia de prueba es t2.nano (para el tenancy por defecto de VPC) o m3.medium (para el uso dedicado de VPC).

Pasos

1. En la página entornos de trabajo, haga clic en **Agregar entorno de trabajo** y siga las indicaciones.
2. **Elija una ubicación:** Seleccione **Amazon Web Services y Cloud Volumes ONTAP Single Node**.
3. **Detalles y credenciales:** Si lo desea, puede cambiar las credenciales y la suscripción de AWS, introducir un nombre de entorno de trabajo, agregar etiquetas y, a continuación, introducir una contraseña.

Algunos de los campos en esta página son claros y explicativos. En la siguiente tabla se describen los campos que podrían presentar dificultades:

Campo	Descripción
Nombre del entorno de trabajo	Cloud Manager utiliza el nombre del entorno de trabajo para asignar un nombre tanto al sistema Cloud Volumes ONTAP como a la instancia de Amazon EC2. También utiliza el nombre como prefijo para el grupo de seguridad predefinido si selecciona esa opción.

Campo	Descripción
Agregar etiquetas	Las etiquetas de AWS son metadatos para sus recursos de AWS. Cloud Manager agrega las etiquetas a la instancia de Cloud Volumes ONTAP y a cada recurso de AWS asociado con la instancia. Puede agregar hasta cuatro etiquetas desde la interfaz de usuario al crear un entorno de trabajo y, a continuación, puede agregar más después de crear. Tenga en cuenta que la API no le limita a cuatro etiquetas al crear un entorno de trabajo. Para obtener información sobre etiquetas, consulte " Documentación de AWS: Etiquetado de los recursos de Amazon EC2 ".
Nombre de usuario y contraseña	Estas son las credenciales de la cuenta de administrador del clúster de Cloud Volumes ONTAP. Puede usar estas credenciales para conectarse a Cloud Volumes ONTAP a través de OnCommand System Manager o de su CLI.
Editar credenciales	Elija las credenciales de AWS y la suscripción al mercado para utilizar con este sistema Cloud Volumes ONTAP. Haga clic en Agregar suscripción para asociar las credenciales seleccionadas a una suscripción. Para crear un sistema Cloud Volumes ONTAP de pago por uso, debe seleccionar las credenciales de AWS asociadas con una suscripción a Cloud Volumes ONTAP desde AWS Marketplace. Se le cobrará de esta suscripción por cada sistema Cloud Volumes ONTAP 9.6 y posterior de PAYGO que cree y cada función complementaria que habilite. " Aprenda a añadir credenciales de AWS adicionales a Cloud Manager ".

En el siguiente vídeo se muestra cómo asociar una suscripción de pago por uso a Marketplace en sus credenciales de AWS:

► https://docs.netapp.com/es-es/occm38//media/video_subscribing_aws.mp4 (video)

Si varios usuarios de IAM trabajan en la misma cuenta de AWS, cada usuario debe suscribirse. Una vez que el primer usuario se haya suscrito, AWS Marketplace informa a los usuarios posteriores de que ya están suscritos, tal como se muestra en la siguiente imagen. Mientras se ha establecido una suscripción para la cuenta de AWS, cada usuario de IAM debe asociarse a dicha suscripción. Si ve el mensaje que aparece a continuación, haga clic en el enlace **haga clic aquí** para ir a Cloud Central y completar el proceso.



Cloud Manager (for Cloud Volumes ONTAP)

You are currently subscribed to this product and will be charged for your accumulated usage at the end of your next billing cycle, based on the costs listed in Pricing information on the right.

?

Having issues signing up for your product?

If you were unable to complete the set-up process for this software, please [click here](#) to be taken to the product's registration area.

[Subscribe](#)

You are already subscribed to this product

Pricing Details

Software Fees

4. **Servicios:** Mantenga activados los servicios o desactive los servicios individuales que no desea utilizar con Cloud Volumes ONTAP.

- "[Más información sobre Cloud Compliance](#)".
- "[Más información sobre el backup en el cloud](#)".
- "[Más información sobre la supervisión](#)".

5. **ubicación y conectividad:** Introduzca la información de red que ha grabado en la hoja de trabajo de AWS.

La siguiente imagen muestra la página llena:

Location	Connectivity
<p>AWS Region</p> <p>US West Oregon</p>	<p>Security Group</p> <p><input checked="" type="radio"/> Generated security group <input type="radio"/> Use existing security group</p>
<p>VPC</p> <p>vpc-3a01e05f - 172.31.0.0/16</p>	<p>SSH Authentication Method</p> <p><input checked="" type="radio"/> Password <input type="radio"/> Key Pair</p>
<p>Subnet</p> <p>172.31.5.0/24 (OCCM subnet)</p>	

6. **cifrado de datos:** Elija sin cifrado de datos o cifrado gestionado por AWS.

Para el cifrado gestionado por AWS, puede elegir una clave maestra de cliente (CMK) diferente de su cuenta u otra cuenta de AWS.



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

["Aprenda a configurar AWS KMS para el cloud Volumes ONTAP"](#).

["Obtenga más información sobre las tecnologías de cifrado compatibles"](#).

7. **cuenta del sitio de soporte y licencia:** Indique si desea usar el modelo de pago por uso o con su licencia y, a continuación, especifique una cuenta del sitio de soporte de NetApp.

Para comprender cómo funcionan las licencias, consulte ["Licencia"](#).

Una cuenta del sitio de soporte de NetApp es opcional para el pago por uso, pero obligatoria para los sistemas BYOL. ["Aprenda a añadir cuentas del sitio de soporte de NetApp"](#).

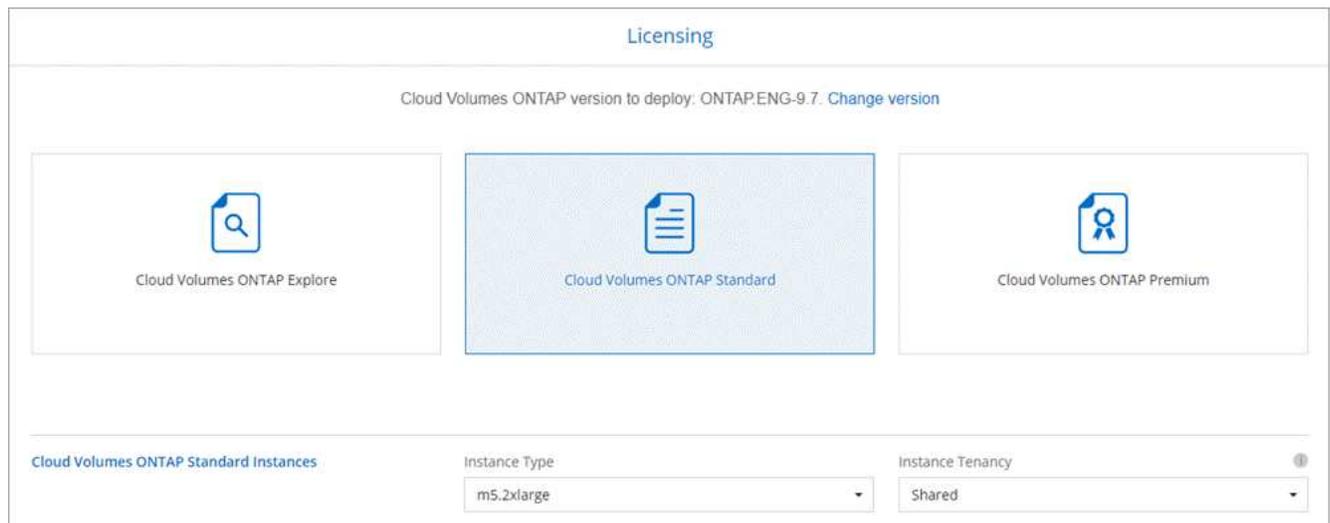
8. **Paquetes preconfigurados:** Seleccione uno de los paquetes para iniciar rápidamente Cloud Volumes ONTAP, o haga clic en **Crear mi propia configuración**.

Si selecciona uno de los paquetes, solo tiene que especificar un volumen y, a continuación, revisar y aprobar la configuración.

9. **función IAM:** Debe mantener la opción predeterminada para que Cloud Manager pueda crear la función que le corresponde.

Si prefiere utilizar su propia política, debe cumplirla ["Requisitos de políticas para los nodos Cloud Volumes ONTAP"](#).

10. **Licencia:** Cambie la versión de Cloud Volumes ONTAP según sea necesario, seleccione una licencia, un tipo de instancia y el uso de la instancia.



Si sus necesidades cambian después de iniciar la instancia, puede modificar la licencia o el tipo de instancia más adelante.



Si hay disponible un candidato de versión, disponibilidad general o versión de revisión más reciente para la versión seleccionada, Cloud Manager actualiza el sistema a esa versión al crear el entorno de trabajo. Por ejemplo, la actualización se produce si selecciona Cloud Volumes ONTAP 9.6 RC1 y 9.6 GA está disponible. La actualización no se produce de una versión a otra; por ejemplo, de 9.6 a 9.7.

11. **Recursos de almacenamiento subyacentes:** Elija la configuración para el agregado inicial: Un tipo de disco, un tamaño para cada disco y si la organización en niveles de datos debe estar activada.

Tenga en cuenta lo siguiente:

- El tipo de disco es para el volumen inicial. Es posible seleccionar un tipo de disco diferente para volúmenes posteriores.
- El tamaño de disco es para todos los discos del agregado inicial y para cualquier agregado adicional que Cloud Manager cree cuando utilice la opción de aprovisionamiento simple. Puede crear agregados que utilicen un tamaño de disco diferente mediante la opción de asignación avanzada.

Para obtener ayuda a elegir el tipo y el tamaño de disco, consulte ["Ajuste de tamaño de su sistema en AWS"](#).

- Se puede elegir una política de organización en niveles de volumen específica cuando se crea o se edita un volumen.
- Si deshabilita la organización en niveles de datos, puede habilitarla en agregados posteriores.

["Descubra cómo funciona la organización en niveles de datos"](#).

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

Además, es posible seleccionar una velocidad de escritura con sistemas de un solo nodo.

["Más información sobre la velocidad de escritura"](#).

NO se puede habilitar WORM si la organización en niveles de datos está habilitada.

["Más información acerca del almacenamiento WORM".](#)

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

Algunos de los campos en esta página son claros y explicativos. En la siguiente tabla se describen los campos que podrían presentar dificultades:

Campo	Descripción
Tamaño	El tamaño máximo que puede introducir depende en gran medida de si habilita thin provisioning, lo que le permite crear un volumen que sea mayor que el almacenamiento físico que hay disponible actualmente.
Control de acceso (solo para NFS)	Una política de exportación define los clientes de la subred que pueden acceder al volumen. De forma predeterminada, Cloud Manager introduce un valor que proporciona acceso a todas las instancias de la subred.
Permisos y usuarios/grupos (solo para CIFS)	Estos campos permiten controlar el nivel de acceso a un recurso compartido para usuarios y grupos (también denominados listas de control de acceso o ACL). Es posible especificar usuarios o grupos de Windows locales o de dominio, o usuarios o grupos de UNIX. Si especifica un nombre de usuario de Windows de dominio, debe incluir el dominio del usuario con el formato domain\username.
Política de Snapshot	Una política de copia de Snapshot especifica la frecuencia y el número de copias de Snapshot de NetApp creadas automáticamente. Una copia snapshot de NetApp es una imagen del sistema de archivos puntual que no afecta al rendimiento y requiere un almacenamiento mínimo. Puede elegir la directiva predeterminada o ninguna. Es posible que no elija ninguno para los datos transitorios: Por ejemplo, tempdb para Microsoft SQL Server.
Opciones avanzadas (solo para NFS)	Seleccione una versión de NFS para el volumen: NFSv3 o NFSv4.
Grupo del iniciador y IQN (solo para iSCSI)	Los destinos de almacenamiento iSCSI se denominan LUN (unidades lógicas) y se presentan a los hosts como dispositivos de bloque estándar. Los iGroups son tablas de los nombres de los nodos de host iSCSI y controlan qué iniciadores tienen acceso a qué LUN. Los destinos iSCSI se conectan a la red a través de adaptadores de red Ethernet (NIC) estándar, tarjetas DEL motor de descarga TCP (TOE) con iniciadores de software, adaptadores de red convergente (CNA) o adaptadores de host de salida dedicados (HBA) y se identifican mediante nombres cualificados de iSCSI (IQN). Cuando se crea un volumen iSCSI, Cloud Manager crea automáticamente un LUN. Lo hemos hecho sencillo creando sólo una LUN por volumen, por lo que no hay que realizar ninguna gestión. Después de crear el volumen, "Utilice el IQN para conectarse con la LUN del hosts" .

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

Volume Details, Protection & Protocol

Details & Protection	Protocol
<p>Volume Name: <input style="width: 200px;" type="text" value="vol"/> Size (GB): <input style="width: 80px;" type="text" value="250"/></p> <p>Snapshot Policy: <input style="width: 300px;" type="text" value="default"/></p> <p><small>Default Policy</small></p>	<p style="text-align: center;"> <input type="radio"/> NFS <input checked="" type="radio"/> CIFS <input type="radio"/> iSCSI </p> <hr/> <p>Share name: <input style="width: 150px;" type="text" value="vol_share"/> Permissions: <input style="width: 150px;" type="text" value="Full Control"/></p> <p>Users / Groups: <input style="width: 300px;" type="text" value="engineering"/></p> <p><small>Valid users and groups separated by a semicolon</small></p>

14. **Configuración CIFS:** Si elige el protocolo CIFS, configure un servidor CIFS.

Campo	Descripción
DNS Dirección IP principal y secundaria	Las direcciones IP de los servidores DNS que proporcionan resolución de nombres para el servidor CIFS. Los servidores DNS enumerados deben contener los registros de ubicación de servicio (SRV) necesarios para localizar los servidores LDAP de Active Directory y los controladores de dominio del dominio al que se unirá el servidor CIFS.
Dominio de Active Directory al que unirse	El FQDN del dominio de Active Directory (AD) al que desea que se una el servidor CIFS.
Credenciales autorizadas para unirse al dominio	Nombre y contraseña de una cuenta de Windows con privilegios suficientes para agregar equipos a la unidad organizativa (OU) especificada dentro del dominio AD.
Nombre NetBIOS del servidor CIFS	Nombre de servidor CIFS que es único en el dominio de AD.
Unidad organizacional	La unidad organizativa del dominio AD para asociarla con el servidor CIFS. El valor predeterminado es CN=Computers. Si configura Microsoft AD administrado de AWS como servidor AD para Cloud Volumes ONTAP, debe introducir OU=equipos,OU=corp en este campo.
Dominio DNS	El dominio DNS para la máquina virtual de almacenamiento (SVM) de Cloud Volumes ONTAP. En la mayoría de los casos, el dominio es el mismo que el dominio de AD.
Servidor NTP	Seleccione usar dominio de Active Directory para configurar un servidor NTP mediante el DNS de Active Directory. Si necesita configurar un servidor NTP con una dirección diferente, debe usar la API. Consulte "Guía para desarrolladores de API de Cloud Manager" para obtener más detalles.

15. **Perfil de uso, Tipo de disco y Directiva de organización en niveles:** Elija si desea activar las funciones de eficiencia del almacenamiento y editar la política de organización en niveles de volumen, si es necesario.

Para obtener más información, consulte ["Descripción de los perfiles de uso de volumen"](#) y.. ["Información general sobre organización en niveles de datos"](#).

16. **revisar y aprobar:** Revise y confirme sus selecciones.
- Consulte los detalles de la configuración.
 - Haga clic en **más información** para consultar detalles sobre el soporte técnico y los recursos de AWS que adquirirá Cloud Manager.
 - Active las casillas de verificación **comprendo....**
 - Haga clic en **Ir**.

Resultado

Cloud Manager inicia la instancia de Cloud Volumes ONTAP. Puede realizar un seguimiento del progreso en la línea de tiempo.

Si tiene algún problema con el inicio de la instancia de Cloud Volumes ONTAP, revise el mensaje de error. También puede seleccionar el entorno de trabajo y hacer clic en **Volver a crear entorno**.

Para obtener más ayuda, vaya a ["Soporte Cloud Volumes ONTAP de NetApp"](#).

Después de terminar

- Si ha provisionado un recurso compartido CIFS, proporcione permisos a usuarios o grupos a los archivos y carpetas y compruebe que esos usuarios pueden acceder al recurso compartido y crear un archivo.
- Si desea aplicar cuotas a los volúmenes, use System Manager o la interfaz de línea de comandos.

Las cuotas le permiten restringir o realizar un seguimiento del espacio en disco y del número de archivos que usan un usuario, un grupo o un qtree.

Iniciar una pareja de alta disponibilidad de Cloud Volumes ONTAP en AWS

Si desea iniciar un par de alta disponibilidad de Cloud Volumes ONTAP en AWS, debe crear un entorno de trabajo de alta disponibilidad en Cloud Manager.

Antes de empezar

- Usted debe tener un ["Conector asociado al área de trabajo"](#).



Debe ser un administrador de cuentas para crear un conector. Al crear el primer entorno de trabajo de Cloud Volumes ONTAP, Cloud Manager le solicita que cree un conector si todavía no lo tiene.

- ["Debe estar preparado para dejar el conector funcionando en todo momento"](#).
- Debe haberse preparado eligiendo una configuración y obteniendo información de red de AWS de su administrador. Para obtener más información, consulte ["Planificación de la configuración de Cloud Volumes ONTAP"](#).
- Si ha adquirido licencias BYOL, debe tener un número de serie (clave de licencia) de 20 dígitos para cada nodo.
- Si desea usar CIFS, debe haber configurado DNS y Active Directory. Para obtener más información, consulte ["Requisitos de red para Cloud Volumes ONTAP en AWS"](#).

Limitación

En este momento, no se admiten pares de alta disponibilidad con entradas externas de AWS.

Acerca de esta tarea

Inmediatamente después de crear el entorno de trabajo, Cloud Manager inicia una instancia de prueba en el VPC especificado para verificar la conectividad. Si se realiza correctamente, Cloud Manager finaliza inmediatamente la instancia y después inicia la implementación del sistema Cloud Volumes ONTAP. Si Cloud Manager no puede verificar la conectividad, se produce un error en la creación del entorno de trabajo. La instancia de prueba es t2.nano (para el tenancy por defecto de VPC) o m3.medium (para el uso dedicado de VPC).

Pasos

1. En la página entornos de trabajo, haga clic en **Agregar entorno de trabajo** y siga las indicaciones.
2. **Elija una ubicación:** Seleccione **Amazon Web Services** y **Cloud Volumes ONTAP Single Node**.
3. **Detalles y credenciales:** Si lo desea, puede cambiar las credenciales y la suscripción de AWS, introducir un nombre de entorno de trabajo, agregar etiquetas y, a continuación, introducir una contraseña.

Algunos de los campos en esta página son claros y explicativos. En la siguiente tabla se describen los campos que podrían presentar dificultades:

Campo	Descripción
Nombre del entorno de trabajo	Cloud Manager utiliza el nombre del entorno de trabajo para asignar un nombre tanto al sistema Cloud Volumes ONTAP como a la instancia de Amazon EC2. También utiliza el nombre como prefijo para el grupo de seguridad predefinido si selecciona esa opción.
Agregar etiquetas	Las etiquetas de AWS son metadatos para sus recursos de AWS. Cloud Manager agrega las etiquetas a la instancia de Cloud Volumes ONTAP y a cada recurso de AWS asociado con la instancia. Puede agregar hasta cuatro etiquetas desde la interfaz de usuario al crear un entorno de trabajo y, a continuación, puede agregar más después de crear. Tenga en cuenta que la API no le limita a cuatro etiquetas al crear un entorno de trabajo. Para obtener información sobre etiquetas, consulte " Documentación de AWS: Etiquetado de los recursos de Amazon EC2 ".
Nombre de usuario y contraseña	Estas son las credenciales de la cuenta de administrador del clúster de Cloud Volumes ONTAP. Puede usar estas credenciales para conectarse a Cloud Volumes ONTAP a través de OnCommand System Manager o de su CLI.
Editar credenciales	Elija las credenciales de AWS y la suscripción al mercado para utilizar con este sistema Cloud Volumes ONTAP. Haga clic en Agregar suscripción para asociar las credenciales seleccionadas a una suscripción. Para crear un sistema Cloud Volumes ONTAP de pago por uso, debe seleccionar las credenciales de AWS asociadas con una suscripción a Cloud Volumes ONTAP desde AWS Marketplace. Se le cobrará de esta suscripción por cada sistema Cloud Volumes ONTAP 9.6 y posterior de PAYGO que cree y cada función complementaria que habilite. " Aprenda a añadir credenciales de AWS adicionales a Cloud Manager ".

En el siguiente vídeo se muestra cómo asociar una suscripción de pago por uso a Marketplace en sus credenciales de AWS:

► https://docs.netapp.com/es-es/occm38//media/video_subscribing_aws.mp4 (video)

Si varios usuarios de IAM trabajan en la misma cuenta de AWS, cada usuario debe suscribirse. Una vez que el primer usuario se haya suscrito, AWS Marketplace informa a los usuarios posteriores de que ya están suscritos, tal como se muestra en la siguiente imagen. Mientras se ha establecido una suscripción para la cuenta de AWS, cada usuario de IAM debe asociarse a dicha suscripción. Si ve el mensaje que aparece a continuación, haga clic en el enlace **haga clic aquí** para ir a Cloud Central y completar el proceso.



Cloud Manager (for Cloud Volumes ONTAP)

You are currently subscribed to this product and will be charged for your accumulated usage at the end of your next billing cycle, based on the costs listed in Pricing information on the right.

?

Having issues signing up for your product?

If you were unable to complete the set-up process for this software, please [click here](#) to be taken to the product's registration area.

[Subscribe](#)

You are already subscribed to this product

Pricing Details

Software Fees

4. **Servicios:** Mantenga activados o desactive los servicios individuales que no desea utilizar con este sistema Cloud Volumes ONTAP.

- ["Más información sobre Cloud Compliance"](#).
- ["Más información sobre el backup en el cloud"](#).
- ["Más información sobre la supervisión"](#).

5. **modelos de implementación de alta disponibilidad:** Elija una configuración de alta disponibilidad.

Para obtener información general sobre los modelos de puesta en marcha, consulte ["Alta disponibilidad de Cloud Volumes ONTAP para AWS"](#).

6. **Región y VPC:** Introduzca la información de red que ha grabado en la hoja de cálculo de AWS.

La siguiente imagen muestra la página rellena para una configuración de AZ múltiple:

Region & VPC

AWS Region

US East | N. Virginia

VPC

vpc-a76d91c2 - 172.31.0.0/16

Security group

Use a generated security group

Node 1:

Availability Zone

us-east-1a

Subnet

172.31.8.0/24

Node 2:

Availability Zone

us-east-1b

Subnet

172.31.9.0/24

Mediator:

Availability Zone

us-east-1c

Subnet

172.31.2.0/24

7. **conectividad y autenticación SSH:** Elija los métodos de conexión para el par ha y el mediador.
8. **IP flotantes:** Si elige varios AZs, especifique las direcciones IP flotantes.

Las direcciones IP deben estar fuera del bloque CIDR para todas las VPC de la región. Para obtener detalles adicionales, consulte ["Requisitos de red de AWS para alta disponibilidad de Cloud Volumes ONTAP en múltiples AZS"](#).

9. * tablas de rutas*: Si elige varios AZs, seleccione las tablas de rutas que deben incluir rutas a las direcciones IP flotantes.

Si tiene más de una tabla de rutas, es muy importante seleccionar las tablas de rutas correctas. De lo contrario, es posible que algunos clientes no tengan acceso al par de alta disponibilidad de Cloud Volumes ONTAP. Para obtener más información sobre las tablas de rutas, consulte ["Documentación de AWS: Tablas de rutas"](#).

10. **cifrado de datos:** Elija sin cifrado de datos o cifrado gestionado por AWS.

Para el cifrado gestionado por AWS, puede elegir una clave maestra de cliente (CMK) diferente de su cuenta u otra cuenta de AWS.



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

["Aprenda a configurar AWS KMS para el cloud Volumes ONTAP"](#).

["Obtenga más información sobre las tecnologías de cifrado compatibles"](#).

11. **cuenta del sitio de soporte y licencia:** Indique si desea usar el modelo de pago por uso o con su licencia y, a continuación, especifique una cuenta del sitio de soporte de NetApp.

Para comprender cómo funcionan las licencias, consulte ["Licencia"](#).

Una cuenta del sitio de soporte de NetApp es opcional para el pago por uso, pero obligatoria para los sistemas BYOL. ["Aprenda a añadir cuentas del sitio de soporte de NetApp"](#).

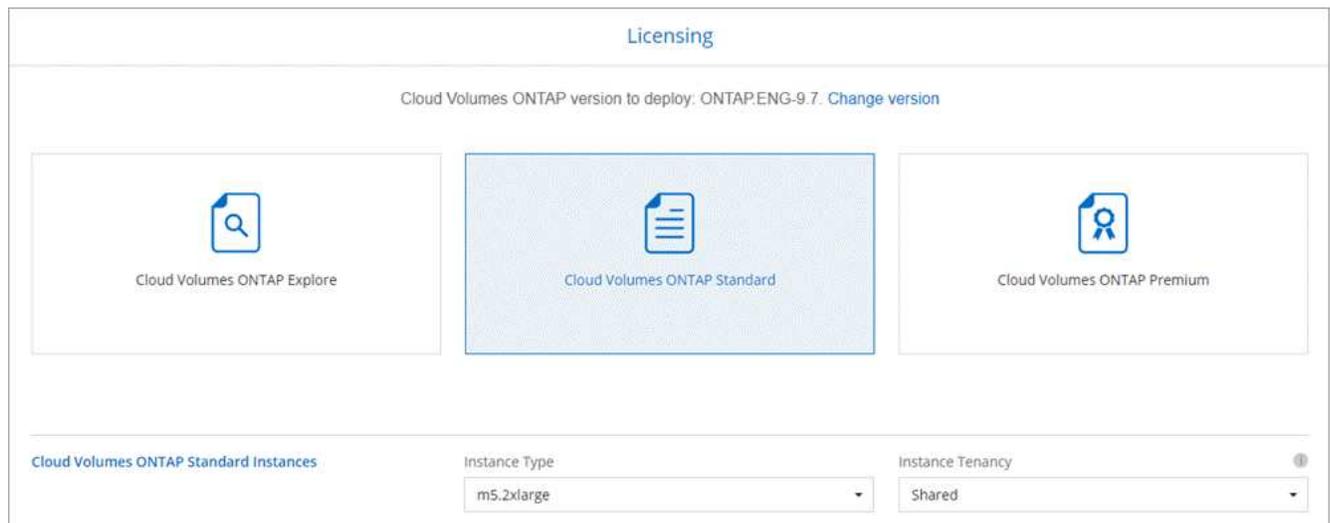
12. **Paquetes preconfigurados:** Seleccione uno de los paquetes para iniciar rápidamente un sistema Cloud Volumes ONTAP, o haga clic en **Crear mi propia configuración**.

Si selecciona uno de los paquetes, solo tiene que especificar un volumen y, a continuación, revisar y aprobar la configuración.

13. **función IAM:** Debe mantener la opción predeterminada para que Cloud Manager pueda crear las funciones que le corresponde.

Si prefiere utilizar su propia política, debe cumplirla ["Requisitos normativos para los nodos Cloud Volumes ONTAP y la alta disponibilidad mediador"](#).

14. **Licencia:** Cambie la versión de Cloud Volumes ONTAP según sea necesario, seleccione una licencia, un tipo de instancia y el uso de la instancia.



Si sus necesidades cambian después de iniciar las instancias, puede modificar la licencia o el tipo de instancia más adelante.



Si hay disponible un candidato de versión, disponibilidad general o versión de revisión más reciente para la versión seleccionada, Cloud Manager actualiza el sistema a esa versión al crear el entorno de trabajo. Por ejemplo, la actualización se produce si selecciona Cloud Volumes ONTAP 9.6 RC1 y 9.6 GA está disponible. La actualización no se produce de una versión a otra; por ejemplo, de 9.6 a 9.7.

15. **Recursos de almacenamiento subyacentes:** Elija la configuración para el agregado inicial: Un tipo de disco, un tamaño para cada disco y si la organización en niveles de datos debe estar activada.

Tenga en cuenta lo siguiente:

- El tipo de disco es para el volumen inicial. Es posible seleccionar un tipo de disco diferente para volúmenes posteriores.
- El tamaño de disco es para todos los discos del agregado inicial y para cualquier agregado adicional que Cloud Manager cree cuando utilice la opción de aprovisionamiento simple. Puede crear agregados que utilicen un tamaño de disco diferente mediante la opción de asignación avanzada.

Para obtener ayuda a elegir el tipo y el tamaño de disco, consulte ["Ajuste de tamaño de su sistema en AWS"](#).

- Se puede elegir una política de organización en niveles de volumen específica cuando se crea o se edita un volumen.
- Si deshabilita la organización en niveles de datos, puede habilitarla en agregados posteriores.

["Descubra cómo funciona la organización en niveles de datos"](#).

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

NO se puede habilitar WORM si la organización en niveles de datos está habilitada.

["Más información acerca del almacenamiento WORM"](#).

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

Algunos de los campos en esta página son claros y explicativos. En la siguiente tabla se describen los campos que podrían presentar dificultades:

Campo	Descripción
Tamaño	El tamaño máximo que puede introducir depende en gran medida de si habilita thin provisioning, lo que le permite crear un volumen que sea mayor que el almacenamiento físico que hay disponible actualmente.
Control de acceso (solo para NFS)	Una política de exportación define los clientes de la subred que pueden acceder al volumen. De forma predeterminada, Cloud Manager introduce un valor que proporciona acceso a todas las instancias de la subred.
Permisos y usuarios/grupos (solo para CIFS)	Estos campos permiten controlar el nivel de acceso a un recurso compartido para usuarios y grupos (también denominados listas de control de acceso o ACL). Es posible especificar usuarios o grupos de Windows locales o de dominio, o usuarios o grupos de UNIX. Si especifica un nombre de usuario de Windows de dominio, debe incluir el dominio del usuario con el formato domain\username.
Política de Snapshot	Una política de copia de Snapshot especifica la frecuencia y el número de copias de Snapshot de NetApp creadas automáticamente. Una copia snapshot de NetApp es una imagen del sistema de archivos puntual que no afecta al rendimiento y requiere un almacenamiento mínimo. Puede elegir la directiva predeterminada o ninguna. Es posible que no elija ninguno para los datos transitorios: Por ejemplo, tempdb para Microsoft SQL Server.
Opciones avanzadas (solo para NFS)	Seleccione una versión de NFS para el volumen: NFSv3 o NFSv4.
Grupo del iniciador y IQN (solo para iSCSI)	Los destinos de almacenamiento iSCSI se denominan LUN (unidades lógicas) y se presentan a los hosts como dispositivos de bloque estándar. Los iGroups son tablas de los nombres de los nodos de host iSCSI y controlan qué iniciadores tienen acceso a qué LUN. Los destinos iSCSI se conectan a la red a través de adaptadores de red Ethernet (NIC) estándar, tarjetas DEL motor de descarga TCP (TOE) con iniciadores de software, adaptadores de red convergente (CNA) o adaptadores de host de salida dedicados (HBA) y se identifican mediante nombres cualificados de iSCSI (IQN). Cuando se crea un volumen iSCSI, Cloud Manager crea automáticamente un LUN. Lo hemos hecho sencillo creando sólo una LUN por volumen, por lo que no hay que realizar ninguna gestión. Después de crear el volumen, "Utilice el IQN para conectarse con la LUN del hosts" .

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

Volume Details, Protection & Protocol

Details & Protection	Protocol
<p>Volume Name: <input style="width: 200px;" type="text" value="vol"/> Size (GB): <input style="width: 80px;" type="text" value="250"/></p> <p>Snapshot Policy: <input style="width: 300px;" type="text" value="default"/></p> <p><small>Default Policy</small></p>	<p style="text-align: center;"> <input type="radio"/> NFS <input checked="" type="radio"/> CIFS <input type="radio"/> iSCSI </p> <hr/> <p>Share name: <input style="width: 150px;" type="text" value="vol_share"/> Permissions: <input style="width: 150px;" type="text" value="Full Control"/></p> <p>Users / Groups: <input style="width: 300px;" type="text" value="engineering"/></p> <p><small>Valid users and groups separated by a semicolon</small></p>

18. **Configuración CIFS:** Si ha seleccionado el protocolo CIFS, configure un servidor CIFS.

Campo	Descripción
DNS Dirección IP principal y secundaria	Las direcciones IP de los servidores DNS que proporcionan resolución de nombres para el servidor CIFS. Los servidores DNS enumerados deben contener los registros de ubicación de servicio (SRV) necesarios para localizar los servidores LDAP de Active Directory y los controladores de dominio del dominio al que se unirá el servidor CIFS.
Dominio de Active Directory al que unirse	El FQDN del dominio de Active Directory (AD) al que desea que se una el servidor CIFS.
Credenciales autorizadas para unirse al dominio	Nombre y contraseña de una cuenta de Windows con privilegios suficientes para agregar equipos a la unidad organizativa (OU) especificada dentro del dominio AD.
Nombre NetBIOS del servidor CIFS	Nombre de servidor CIFS que es único en el dominio de AD.
Unidad organizacional	La unidad organizativa del dominio AD para asociarla con el servidor CIFS. El valor predeterminado es CN=Computers. Si configura Microsoft AD administrado de AWS como servidor AD para Cloud Volumes ONTAP, debe introducir OU=equipos,OU=corp en este campo.
Dominio DNS	El dominio DNS para la máquina virtual de almacenamiento (SVM) de Cloud Volumes ONTAP. En la mayoría de los casos, el dominio es el mismo que el dominio de AD.
Servidor NTP	Seleccione usar dominio de Active Directory para configurar un servidor NTP mediante el DNS de Active Directory. Si necesita configurar un servidor NTP con una dirección diferente, debe usar la API. Consulte "Guía para desarrolladores de API de Cloud Manager" para obtener más detalles.

19. **Perfil de uso, Tipo de disco y Directiva de organización en niveles:** Elija si desea activar las funciones de eficiencia del almacenamiento y editar la política de organización en niveles de volumen, si es necesario.

Para obtener más información, consulte ["Descripción de los perfiles de uso de volumen"](#) y ["Información general sobre organización en niveles de datos"](#).

20. **revisar y aprobar:** Revise y confirme sus selecciones.

- a. Consulte los detalles de la configuración.
- b. Haga clic en **más información** para consultar detalles sobre el soporte técnico y los recursos de AWS que adquirirá Cloud Manager.
- c. Active las casillas de verificación **comprendo....**
- d. Haga clic en **Ir**.

Resultado

Cloud Manager inicia el par de alta disponibilidad de Cloud Volumes ONTAP. Puede realizar un seguimiento del progreso en la línea de tiempo.

Si tiene algún problema con el inicio de la pareja de alta disponibilidad, revise el mensaje de error. También puede seleccionar el entorno de trabajo y hacer clic en Volver a crear entorno.

Para obtener más ayuda, vaya a. ["Soporte Cloud Volumes ONTAP de NetApp"](#).

Después de terminar

- Si ha provisionado un recurso compartido CIFS, proporcione permisos a usuarios o grupos a los archivos y carpetas y compruebe que esos usuarios pueden acceder al recurso compartido y crear un archivo.
- Si desea aplicar cuotas a los volúmenes, use System Manager o la interfaz de línea de comandos.

Las cuotas le permiten restringir o realizar un seguimiento del espacio en disco y del número de archivos que usan un usuario, un grupo o un qtree.

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.