Comience a usar Amazon Web Services

Cloud Volumes ONTAP

NetApp
June 11, 2024

Tabla de contenidos

Comience a usar Amazon Web Services

Inicio rápido para Cloud Volumes ONTAP en AWS

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

1 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"

Tenga en cuenta que si desea implementar Cloud Volumes ONTAP en una subred en la que no haya acceso a Internet disponible, deberá instalar manualmente el conector y acceder a la interfaz de usuario de BlueXP que se esté ejecutando en ese conector. "Aprenda a instalar manualmente el conector en una ubicación sin acceso a Internet"

2 Planificación de la configuración

BlueXP ofrece paquetes preconfigurados que se ajustan a sus necesidades de carga de trabajo, o puede crear su propia configuración. Si elige su propia configuración, debe conocer las opciones disponibles. "Leer más".

3 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 AutoSupport de NetApp.

   Este paso no es necesario si está instalando Cloud Volumes ONTAP en una ubicación en la que no hay acceso a Internet disponible.

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".

4 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".

5 Inicie Cloud Volumes ONTAP con BlueXP

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

- "Cree un conector en AWS desde BlueXP"
- "Cree un conector desde AWS Marketplace"
- "Instalar y configurar un conector en las instalaciones"
- "Permisos de AWS para Connector"

Planifique 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 una licencia de Cloud Volumes ONTAP

Hay varias opciones de licencia disponibles para Cloud Volumes ONTAP. Cada opción le permite elegir un modelo de consumo que cumpla sus necesidades.

- "Obtenga información sobre las opciones de licencia para Cloud Volumes ONTAP"
- "Aprenda a configurar las licencias"

Seleccione una región admitida

Cloud Volumes ONTAP se admite en la mayoría de las regiones de AWS. "Consulte la lista completa de las regiones admitidas".

Para poder crear y gestionar recursos en esas regiones, deben habilitarse las nuevas regiones de AWS. "Aprenda a habilitar una región".

Seleccione una zona local compatible

Cloud Volumes ONTAP es compatible con algunas zonas locales de AWS, incluida Singapur. La selección de una zona local es opcional.

"Ver la lista completa de zonas locales".
Las zonas locales deben estar activadas antes de poder crear y gestionar recursos en esas zonas.

"Aprenda a habilitar una zona local".

Phoenix no es una zona local compatible.

Elija una instancia admitida

Cloud Volumes ONTAP admite varios tipos de instancia, según el tipo de licencia que elija.

"Configuraciones compatibles para Cloud Volumes ONTAP 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 en AWS"

Configure el 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

En líneas generales, las diferencias entre los tipos de discos de EBS son las siguientes. Para obtener más información acerca de los casos de uso para discos EBS, consulte "Documentación de AWS: Tipos de volúmenes de EBS".

- *Los discos SSD de uso general (gp3)* son los SSD de menor coste que equilibran los costes y el rendimiento con una amplia variedad de cargas de trabajo. El rendimiento se define en términos de IOPS y rendimiento. Los discos gp3 son compatibles con Cloud Volumes ONTAP 9.7 y versiones posteriores.

  Al seleccionar un disco gp3, BlueXP rellena los valores predeterminados de IOPS y rendimiento que proporcionan un rendimiento equivalente a un disco gp2 basado en el tamaño de disco seleccionado. Puede aumentar los valores para obtener un mejor rendimiento a un coste más alto, pero no apoyamos valores más bajos porque puede resultar en un rendimiento inferior. En resumen, cíñase a los valores predeterminados o aumentarlos. No los baje. "Más información sobre los discos gp3 y su rendimiento".

  Tenga en cuenta que Cloud Volumes ONTAP admite la función Amazon EBS Elastic Volumes con discos gp3. "Obtenga más información sobre la compatibilidad con Elastic Volumes".

- *SSD de uso general (gp2)* los discos equilibran los costes y el rendimiento para una amplia gama de cargas de trabajo. El rendimiento se define en términos de IOPS.
- Los discos SSD (io1)_ de _IOPS aprovisionados están destinados a aplicaciones críticas que requieren el máximo rendimiento por un coste superior.

  Tenga en cuenta que Cloud Volumes ONTAP es compatible con la función de volúmenes Elastic de Amazon EBS con discos io1. "Obtenga más información sobre la compatibilidad con Elastic Volumes".

- Los discos *HDD optimizados para rendimiento (st1)* se utilizan para cargas de trabajo de acceso frecuente que requieren un rendimiento rápido y constante a un precio más reducido.

No se recomienda la organización en niveles de los datos para el almacenamiento de objetos cuando se utilizan unidades HDD optimizadas para el rendimiento (st1).

Tamaño del disco de EBS

Si elige una configuración que no sea compatible con "Función Elastic Volumes de Amazon EBS", Luego necesita elegir un tamaño de disco inicial al iniciar un sistema Cloud Volumes ONTAP. Después de eso, usted puede "Deje que BlueXP 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 elija discos más grandes (por ejemplo, seis discos de 4 TIB), es posible que no obtenga 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".

  Como se ha mencionado anteriormente, no es posible elegir un tamaño de disco para las configuraciones de Cloud Volumes ONTAP compatibles con la función Amazon EBS Elastic Volumes. "Obtenga más información sobre la compatibilidad con Elastic Volumes".

Ver los discos del sistema predeterminados

Además del almacenamiento de los datos de usuario, BlueXP también adquiere almacenamiento en cloud para los datos del sistema Cloud Volumes ONTAP (datos de arranque, datos raíz, datos principales y NVRAM). Para fines de planificación, es posible que le ayude a revisar estos detalles antes de implementar Cloud Volumes ONTAP.

"Ver los discos predeterminados para los datos del sistema Cloud Volumes ONTAP en AWS".

El conector también requiere un disco del sistema. "Ver detalles sobre la configuración predeterminada del conector".

Prepárese para implementar Cloud Volumes ONTAP en una entrada de AWS

Si tiene una publicación externa de AWS, puede implementar Cloud Volumes ONTAP en esa publicación seleccionando el VPC de salida en el asistente del entorno de trabajo. La experiencia es la misma que cualquier otro VPC que resida en AWS. Tenga en cuenta que primero deberá implementar un conector en su AWS Outpost.

Hay algunas limitaciones que señalar:

- Solo se admiten sistemas Cloud Volumes ONTAP de un solo nodo a. esta vez
- Las instancias de EC2 que se pueden utilizar con Cloud Volumes ONTAP está limitado a lo que hay disponible en su mensaje de salida

- Actualmente, solo se admiten las unidades SSD de uso general (gp2)

Recopilar información de red

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.

Un único nodo o un par de alta disponibilidad en un único nodo de disponibilidad

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

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	

Elija una velocidad de escritura

BlueXP permite elegir una configuración de velocidad de escritura para Cloud Volumes ONTAP. 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. "Más información sobre la velocidad de escritura".

Seleccione 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 BlueXP, puede elegir un perfil que habilite estas funciones o un perfil que las desactive. Debe obtener más información sobre estas funciones para ayudarle a decidir qué perfil utilizar.

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

Aprovisionamiento ligero

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

Deduplicación

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

Compresión

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

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.

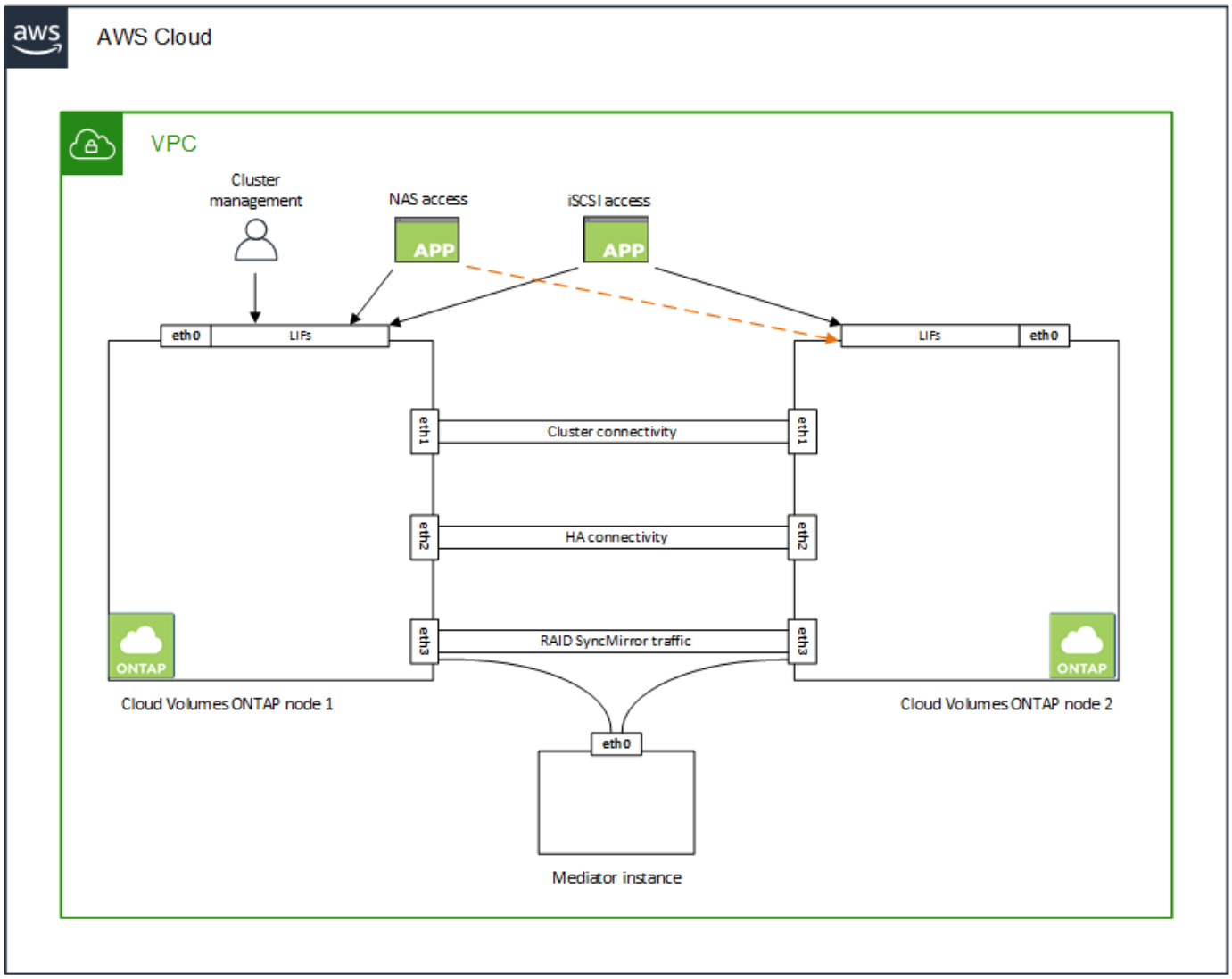
La tabla siguiente proporciona detalles acerca de las LIF asociadas con cada dirección IP privada.

LUN	Específico
Gestión de clústeres	Gestión administrativa de todo el clúster (pareja de alta disponibilidad).
Gestión de nodos	La gestión administrativa de un nodo.
Interconexión de clústeres	Comunicación entre clústeres, backup y replicación.
Datos de NAS	Acceso de clientes a través de protocolos NAS.
Datos de iSCSI	Acceso de cliente a través del protocolo iSCSI. También lo utiliza el sistema para otros flujos de trabajo de red importantes. Este LIF es necesario y no debe eliminarse.

LUN	Específico
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.
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 ayudarle 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. Estos LIF también gestionan la migración de direcciones IP flotantes entre nodos. Estos LIF son necesarios y no deben eliminarse.
Conectividad del clúster	eth1	nodo 1 y nodo 2	Permite que los nodos se comuniquen entre sí y 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.

LUN	Interfaz	Nodo	Específico
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 ayudarle a tomar la toma de control y los procesos de devolución del almacenamiento.

Cuando 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".

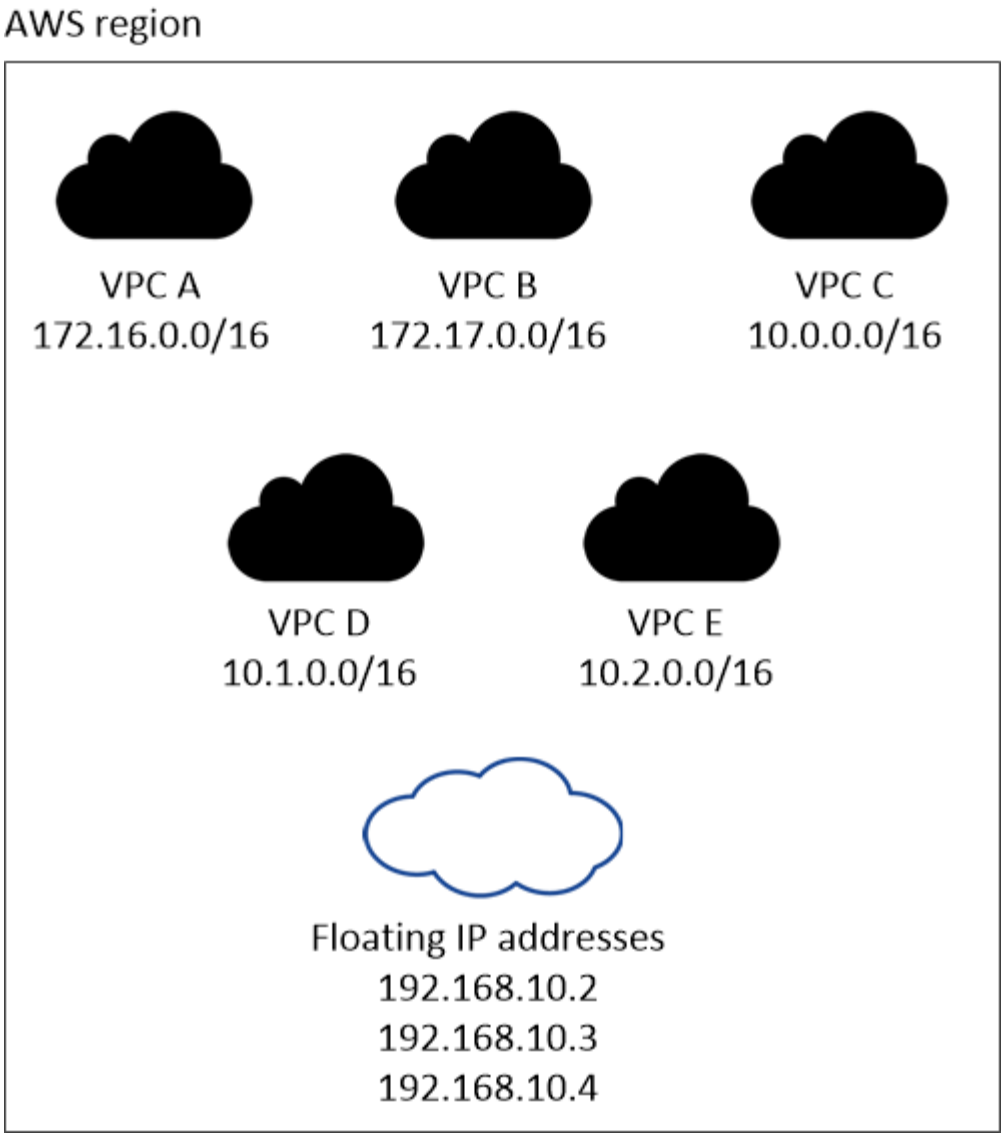
Una dirección IP flotante es para la gestión del clúster, otra para los datos NFS/CIFS del nodo 1 y otra para los datos NFS/CIFS del nodo 2. Una cuarta dirección IP flotante para la gestión de SVM es opcional.

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.



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".

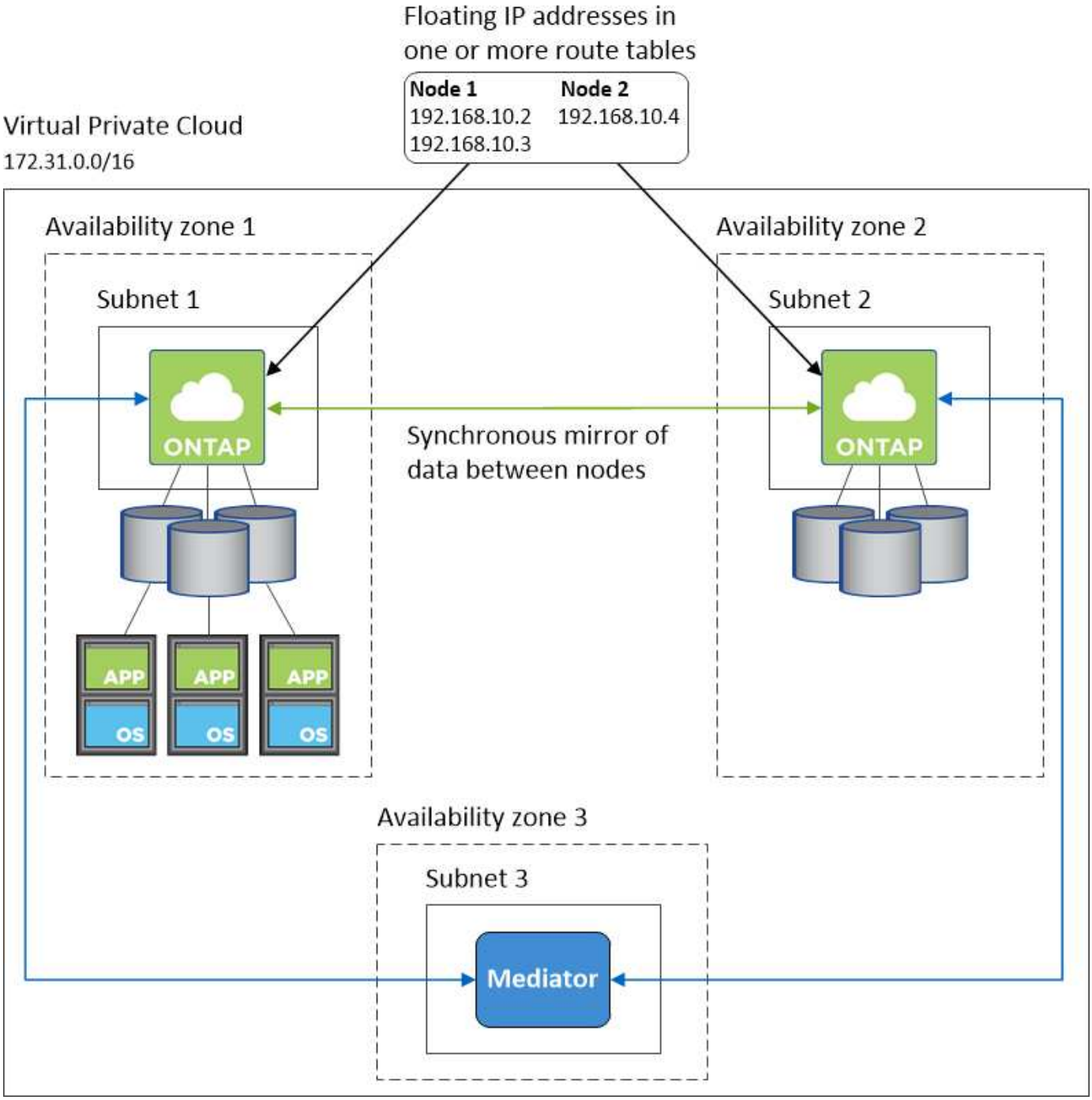
Conexión a herramientas de gestión de NetApp

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

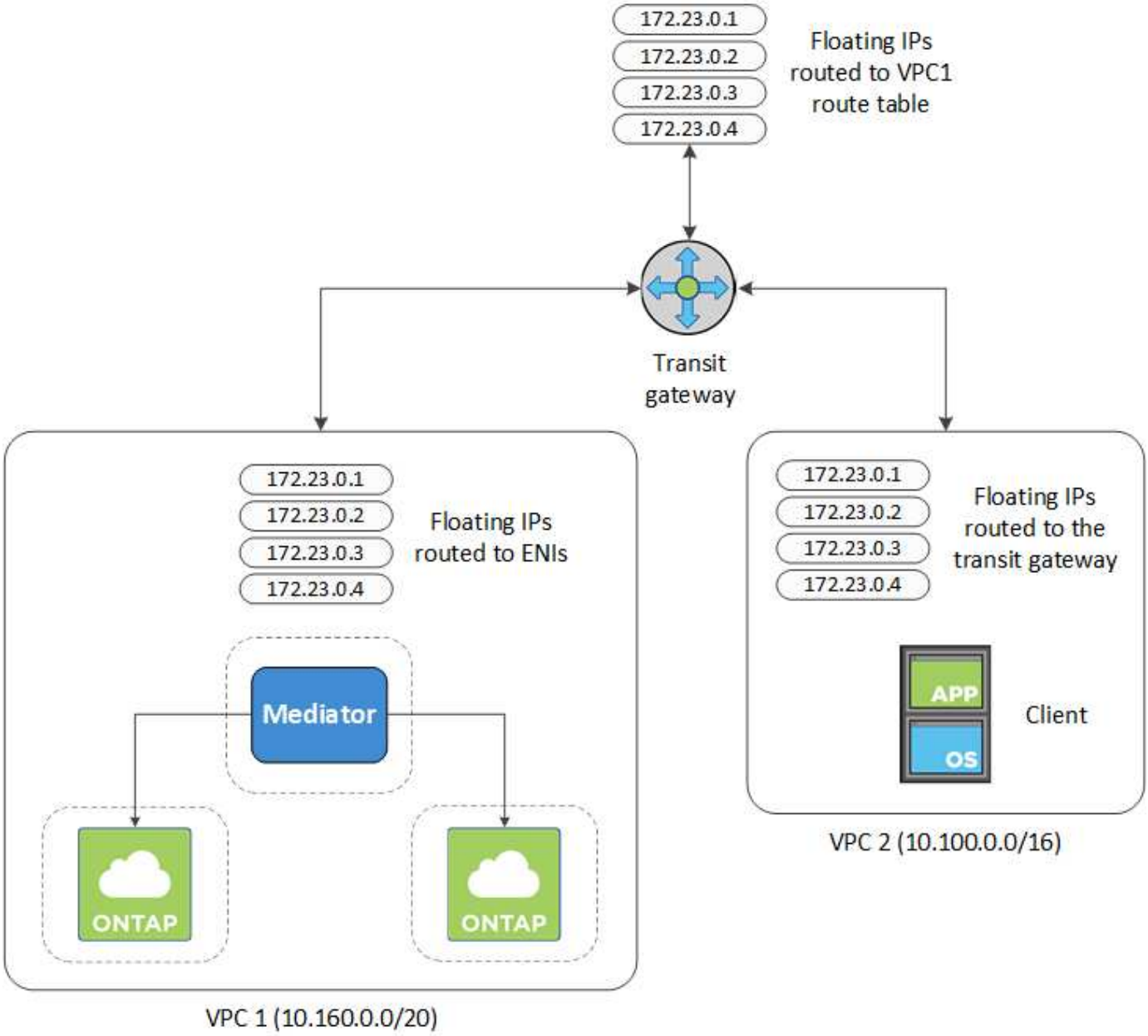
alta disponibilidad.

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.



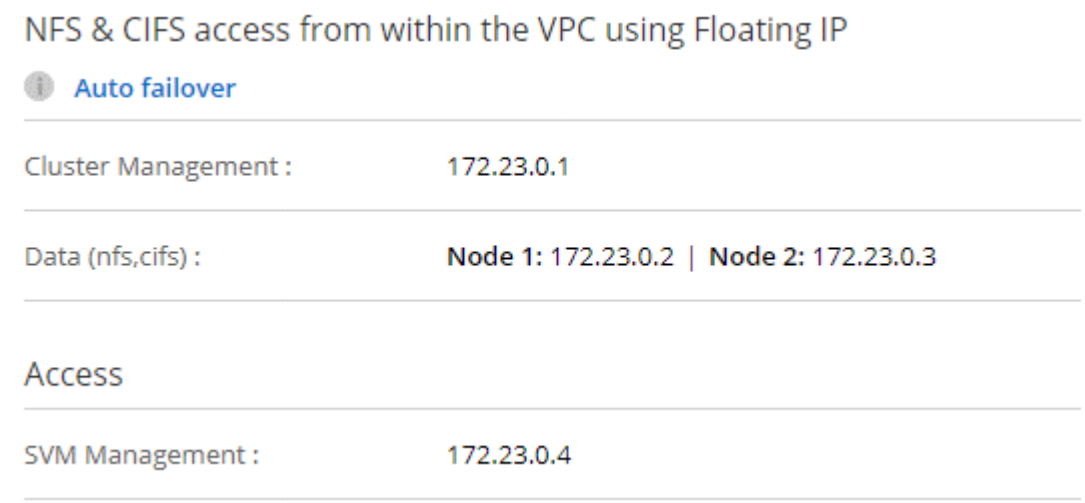
Los siguientes pasos ilustran cómo configurar una configuración similar.

Pasos

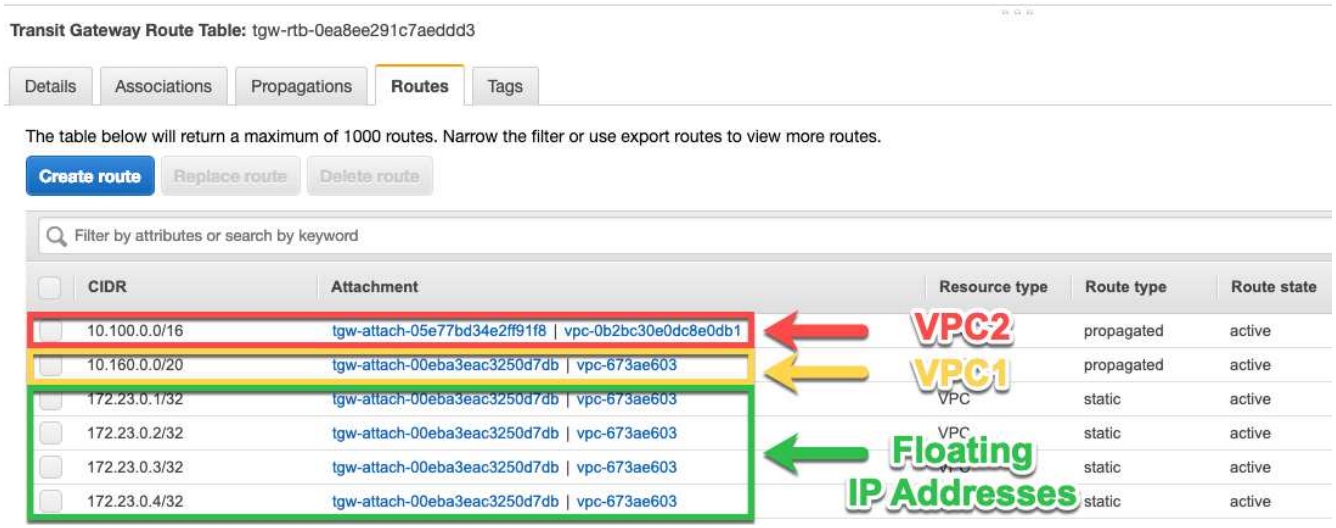
1. "Cree una puerta de enlace de tránsito y conecte las VPC al puerta de enlace".
2. Asocie las VPC a la tabla de rutas de la puerta de enlace de tránsito.
   a. En el servicio **VPC**, haga clic en **tablas de rutas de puerta de enlace de tránsito**.
   b. Seleccione la tabla de rutas.
   c. Haga clic 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:



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.

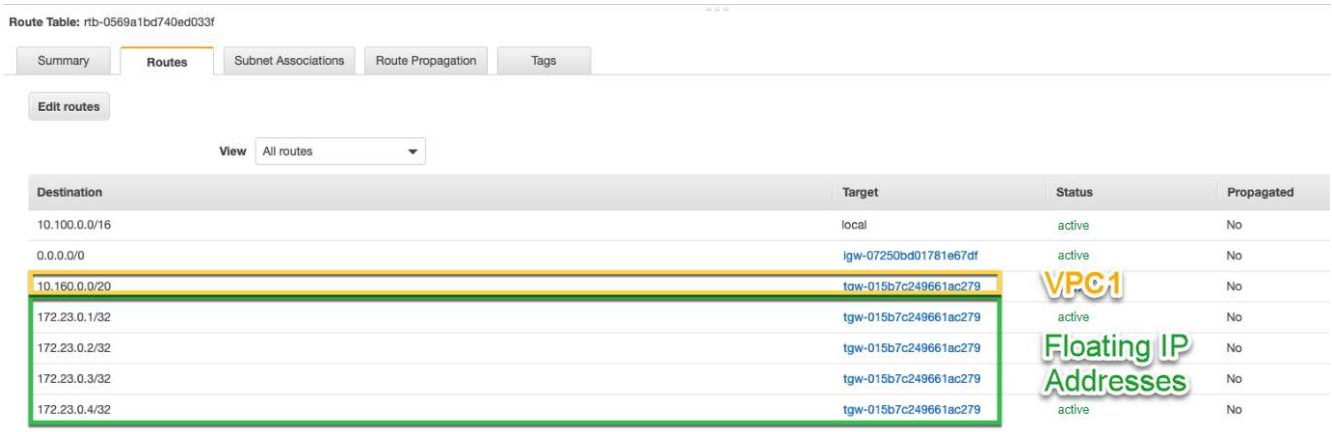


4. Modifique la tabla de rutas de las VPC que necesitan acceder a las direcciones IP flotantes.

   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.

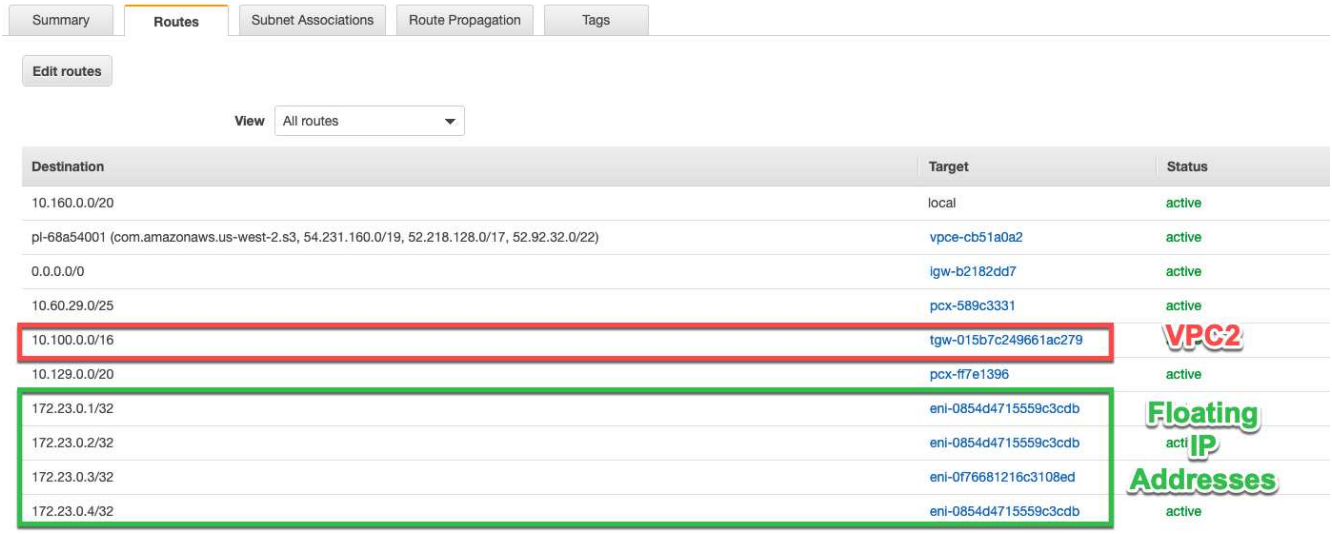
      La siguiente imagen de ejemplo muestra la tabla de rutas para VPC 2, que incluye las rutas hasta VPC 1 y las direcciones IP flotantes.



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.

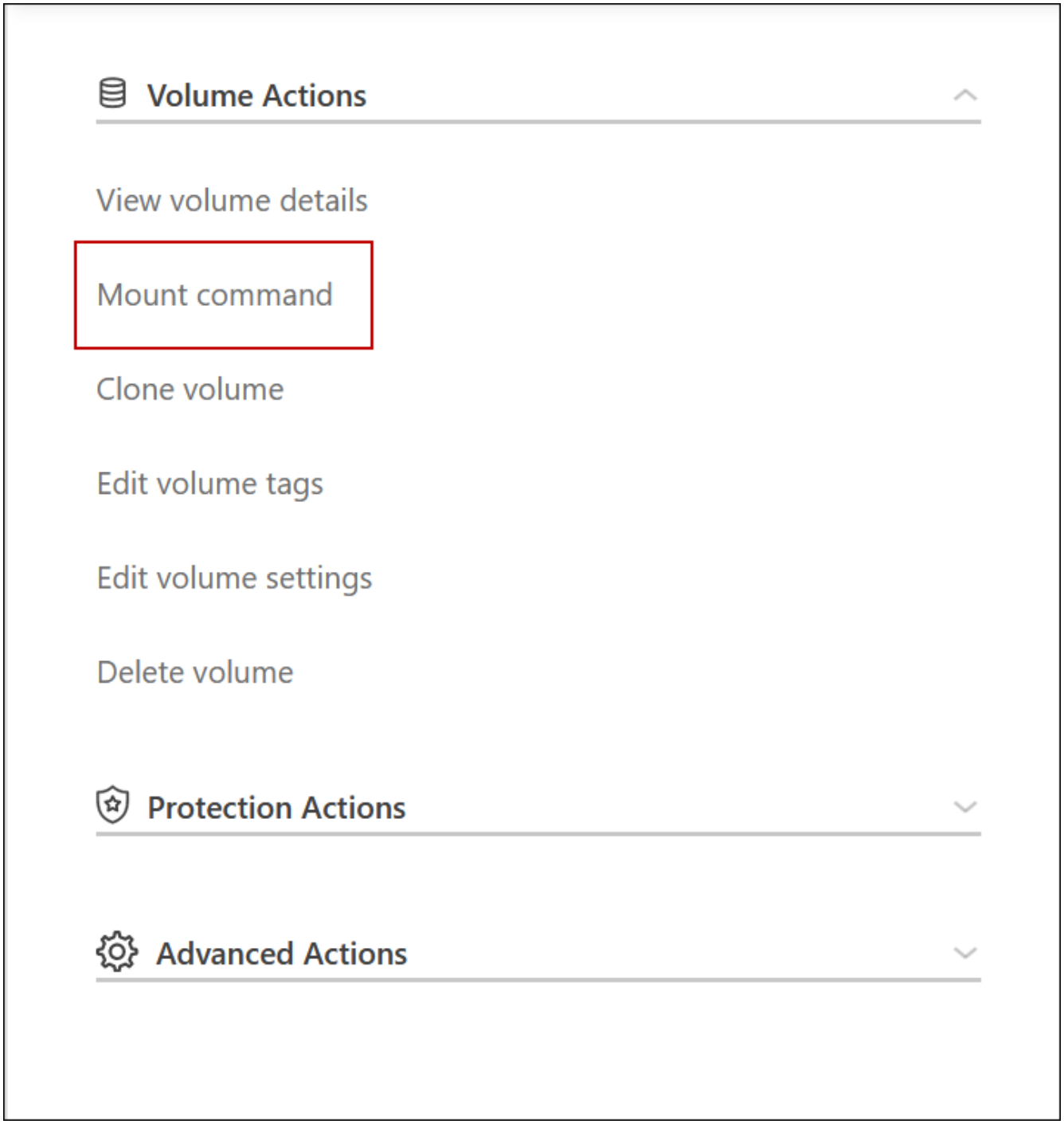
   La siguiente imagen de ejemplo muestra la tabla de rutas para VPC 1. Incluye una ruta a las direcciones IP flotantes y al VPC 2, que es donde reside un cliente. BlueXP agregó automáticamente las IP flotantes a la tabla de rutas cuando implementó el par ha.



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

   Puede encontrar la dirección IP correcta en BlueXP a través de la opción **comando de montaje** en el

panel Administrar volúmenes de BlueXP.



8. 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

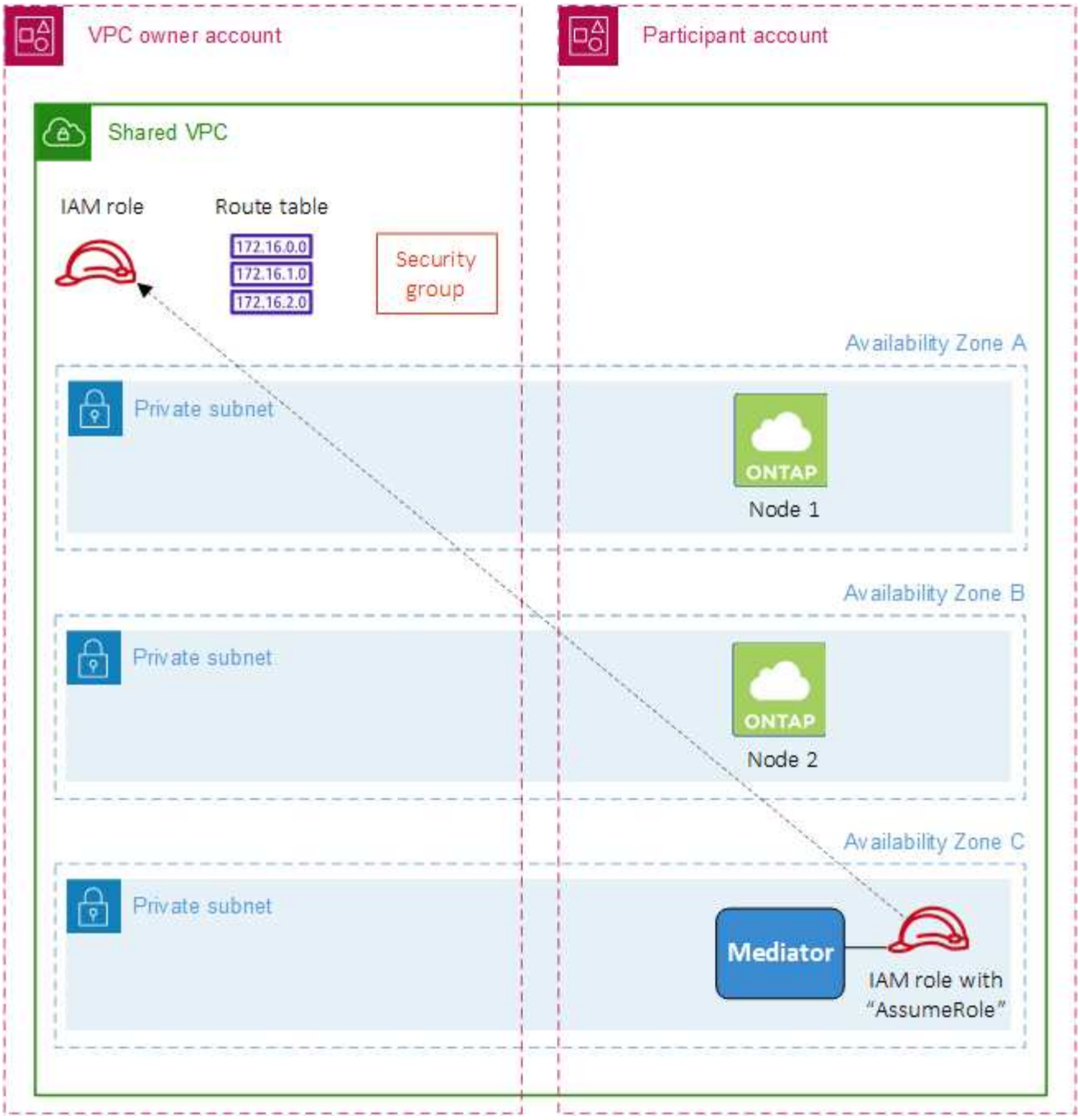
A partir del lanzamiento de la versión 9.11.1, se admiten los pares de alta disponibilidad de Cloud Volumes ONTAP en AWS con el uso compartido de VPC. El uso compartido de VPC permite a la organización compartir subredes con otras cuentas de AWS. Para utilizar esta configuración, debe configurar su entorno 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)
Backups de configuración	HTTP	80	LIF de gestión de nodos	\Http://<connector-IP-address>/occm/offboxconfig	Enviar copias de seguridad de configuración al conector. "Obtener información acerca de los archivos de copia de seguridad de configuración".
DHCP	UDP	68	LIF de gestión de nodos	DHCP	Cliente DHCP para la configuración inicial
DHCPS	UDP	67	LIF de gestión de nodos	DHCP	Servidor DHCP
DNS	UDP	53	LIF de gestión de nodos y LIF de datos (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	LIF de gestión de nodos	Servidores de destino	Copia NDMP
SMTP	TCP	25	LIF de gestión de nodos	Servidor de correo	Alertas SMTP, que se pueden utilizar para AutoSupport

Servicio	Protocolo	Puerto	Origen	Destino	Específico
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

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

Protocolo	Puerto	Origen	Específico
TCP	3000	CIDR del conector	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 en la instancia de AWS EC2	Descargar actualizaciones para el mediador
HTTPS	443	ec2.amazonaws.com	Ayudar en la recuperación tras fallos de almacenamiento
UDP	53	ec2.amazonaws.com	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"

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 estar en la misma cuenta de AWS que BlueXP y Cloud Volumes ONTAP o en una cuenta diferente de AWS.

"Documentación de AWS: Claves maestras de clientes (CMKs)"

2. Modifique la política de clave para cada CMK agregando la función IAM que proporciona permisos a BlueXP como *Key user*.

   La adición de la función IAM como usuario clave permite a BlueXP 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.

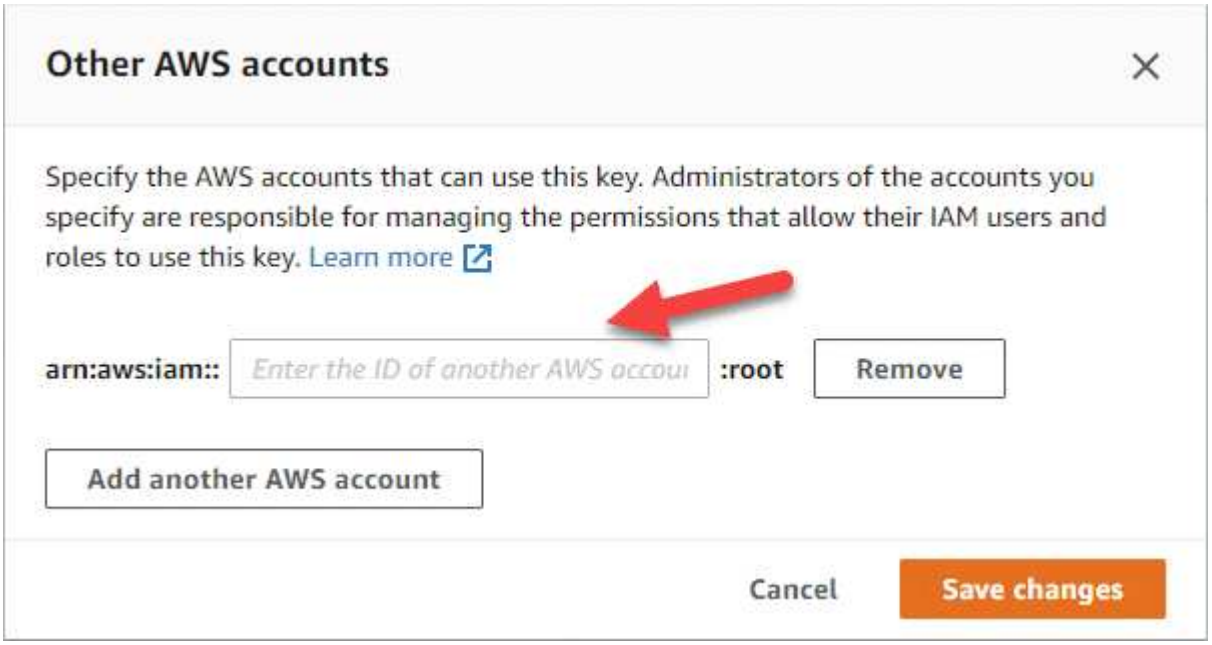
   b. Seleccione la tecla.

   c. En el panel **Configuración general**, copie el ARN de la clave.

      Deberá proporcionar el ARN a BlueXP cuando cree el sistema Cloud Volumes ONTAP.

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

      En la mayoría de los casos, esta es la cuenta en la que reside BlueXP. Si BlueXP no estaba instalada en AWS, sería la cuenta para la que proporcionaste claves de acceso de AWS a BlueXP.



e. Ahora cambie a la cuenta de AWS que proporciona permisos a BlueXP y abra la consola IAM.

f. Cree una política de IAM que incluya los permisos que se indican a continuación.

g. Adjunte la directiva al rol IAM o al usuario IAM que proporciona permisos a BlueXP.

   La siguiente directiva proporciona los permisos que BlueXP necesita para utilizar el 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 los usuarios de otras cuentas usen una clave KMS".

4. Si está utilizando un CMK gestionado por el cliente, modifique la política de clave del CMK agregando el rol Cloud Volumes ONTAP IAM como *Key USER*.

Este paso es necesario si habilitó la organización en niveles de datos en Cloud Volumes ONTAP y desea cifrar los datos almacenados en el bloque de S3.

Deberá realizar este paso *After* implementa Cloud Volumes ONTAP porque se crea la función IAM al crear un entorno de trabajo. (Por supuesto, tiene la opción de utilizar la función de IAM de Cloud Volumes ONTAP existente, de modo que es posible realizar este paso antes).

"Documentación de AWS: Editar claves"

Configure los roles IAM para Cloud Volumes ONTAP

Se deben conectar los roles IAM con los permisos necesarios a cada nodo Cloud Volumes ONTAP. Lo mismo sucede con el mediador de alta disponibilidad. Es más fácil dejar que BlueXP cree las funciones de IAM para usted, pero puede utilizar sus propias funciones.

Esta tarea es opcional. Al crear un entorno de trabajo Cloud Volumes ONTAP, la opción predeterminada es dejar que BlueXP cree las funciones IAM para usted. Si las políticas de seguridad de su empresa requieren que usted mismo cree los roles de IAM, siga estos pasos.

Es necesario proporcionar su propia función de IAM en la nube secreta de AWS. "Descubra cómo instalar Cloud Volumes ONTAP en C2S".

Pasos

1. Vaya a la consola IAM de AWS.
2. Cree políticas IAM que incluyan los siguientes permisos:
    - La política base para los nodos de Cloud Volumes ONTAP

Regiones estándar

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Action": "s3:ListAllMyBuckets",
            "Resource": "arn:aws:s3:::*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }
    ]
}
```

Regiones GovCloud (EE. UU.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-us-gov:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

Regiones Top Secret

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

Regiones secretas

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso-b:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

- Política de backup para nodos Cloud Volumes ONTAP

  Si tiene pensado utilizar el backup y la recuperación de datos de BlueXP con tus sistemas Cloud Volumes ONTAP, el rol de IAM para los nodos debe incluir la segunda política que se muestra a continuación.

Regiones estándar

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

Regiones GovCloud (EE. UU.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

Regiones Top Secret

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

Regiones secretas

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso-b:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-iso-b:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

- Mediador DE ALTA DISPONIBILIDAD

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses",
                "sts:AssumeRole",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

3. Crear un rol IAM y asociar las políticas que ha creado al rol.

Resultado

Ahora dispone de los roles IAM que se pueden seleccionar al crear un nuevo entorno de trabajo Cloud Volumes ONTAP.

Más información

- "Documentación de AWS: Crear políticas de IAM"
- "Documentación de AWS: Crear roles de IAM"

Configure las licencias para Cloud Volumes ONTAP en AWS

Después de decidir qué opción de licencia desea utilizar con Cloud Volumes ONTAP, es necesario realizar algunos pasos antes de elegir esa opción de licencia al crear un nuevo entorno de trabajo.

Freemium

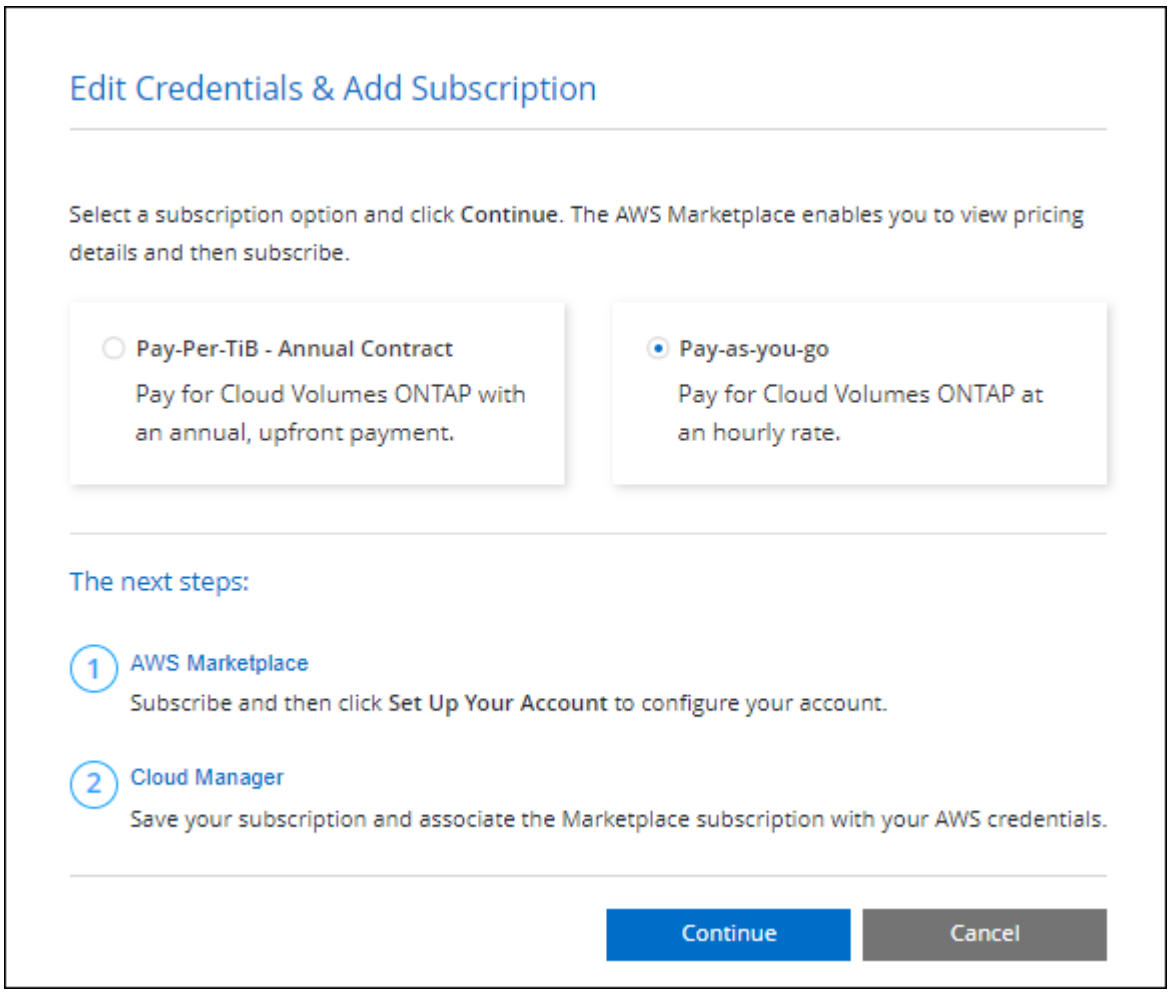
Seleccione la oferta freemium para utilizar Cloud Volumes ONTAP de forma gratuita con hasta 500 GIB de capacidad aprovisionada. "Obtenga más información sobre la oferta de Freemium".

Pasos

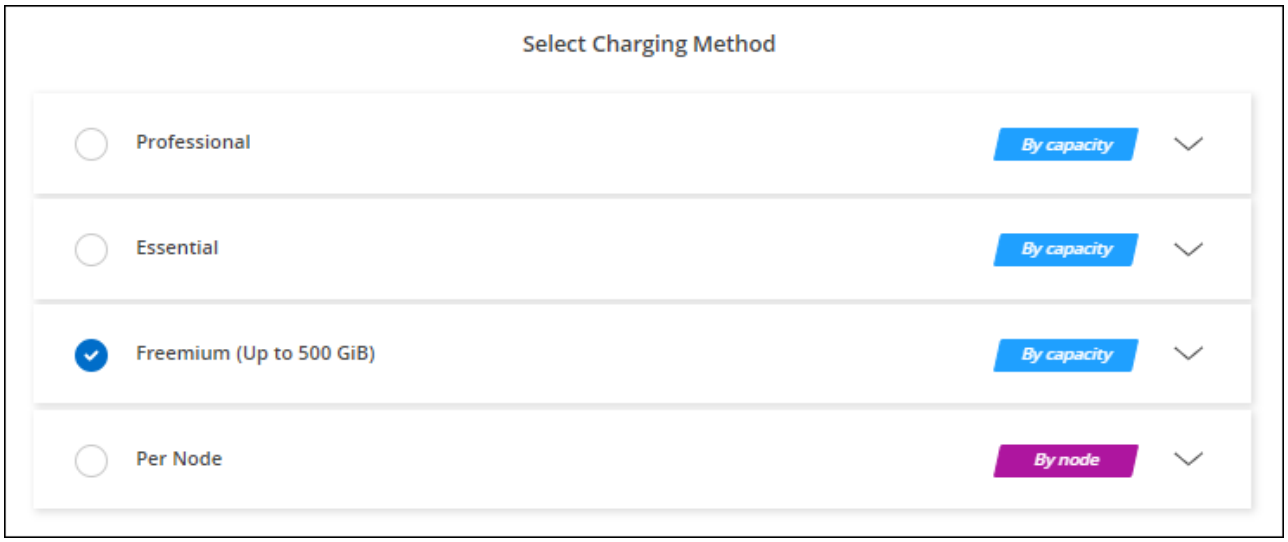
1. En el menú de navegación de la izquierda, selecciona **almacenamiento > Canvas**.
2. En la página Canvas, haga clic en **Agregar entorno de trabajo** y siga los pasos de BlueXP.

a. En la página **Detalles y credenciales**, haga clic en **Editar credenciales > Agregar suscripción** y siga las indicaciones para suscribirse a la oferta de pago por uso en el mercado de AWS.

   No se le cobrará en la suscripción al mercado a menos que supere los 500 GIB de capacidad aprovisionada; en ese momento, el sistema se convertirá automáticamente en la "Paquete Essentials".



a. Después de volver a BlueXP, seleccione **Freemium** cuando llegue a la página de métodos de carga.



"Consulte instrucciones paso a paso para iniciar Cloud Volumes ONTAP en AWS".

Licencia basada en capacidad

Las licencias basadas en la capacidad le permiten pagar por Cloud Volumes ONTAP por TIB de capacidad. La licencia basada en la capacidad está disponible en forma de un *package*: El paquete Essentials o el paquete Professional.

Los paquetes Essentials y Professional están disponibles con los siguientes modelos de consumo:

- Una licencia (BYOL) adquirida a NetApp
- Una suscripción de pago por uso por hora (PAYGO) desde AWS Marketplace
- Un contrato anual del AWS Marketplace

"Más información sobre las licencias basadas en capacidad".

En las siguientes secciones se describe cómo empezar a usar cada uno de estos modelos de consumo.

BYOL

Pague por adelantado al comprar una licencia (BYOL) de NetApp para poner en marcha sistemas Cloud Volumes ONTAP en cualquier proveedor de cloud.

Pasos

1. "Póngase en contacto con el equipo de ventas de NetApp para obtener una licencia"
2. "Agregue su cuenta de la página de soporte de NetApp a BlueXP"

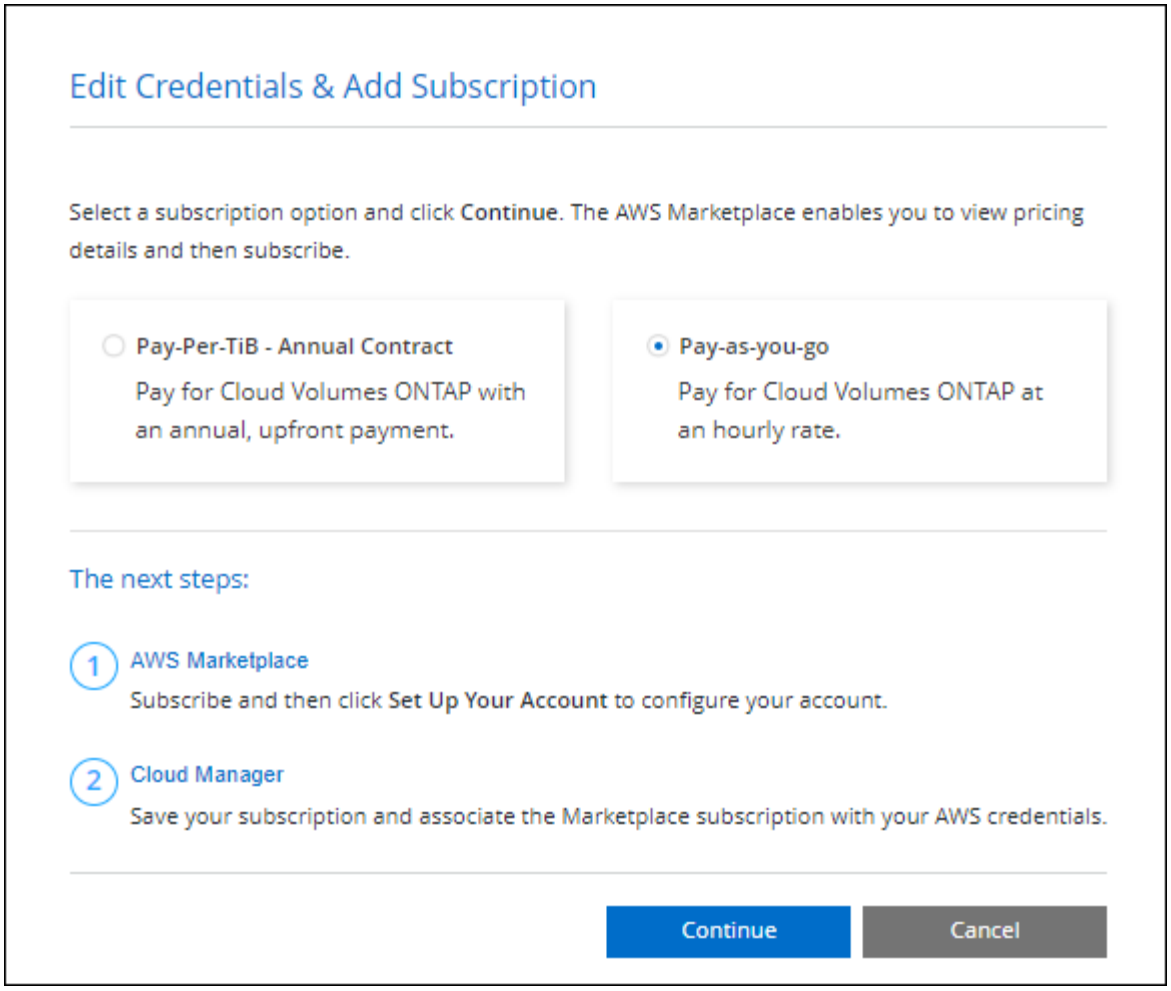
   BlueXP consulta automáticamente al servicio de licencias de NetApp para obtener detalles sobre las licencias asociadas a su cuenta del sitio de soporte de NetApp. Si no se producen errores, BlueXP añade automáticamente las licencias a la cartera digital.

   Tu licencia debe estar disponible en la cartera digital de BlueXP para poder utilizarla con Cloud Volumes ONTAP. Si es necesario, puede "Añade manualmente la licencia a la cartera digital de BlueXP".

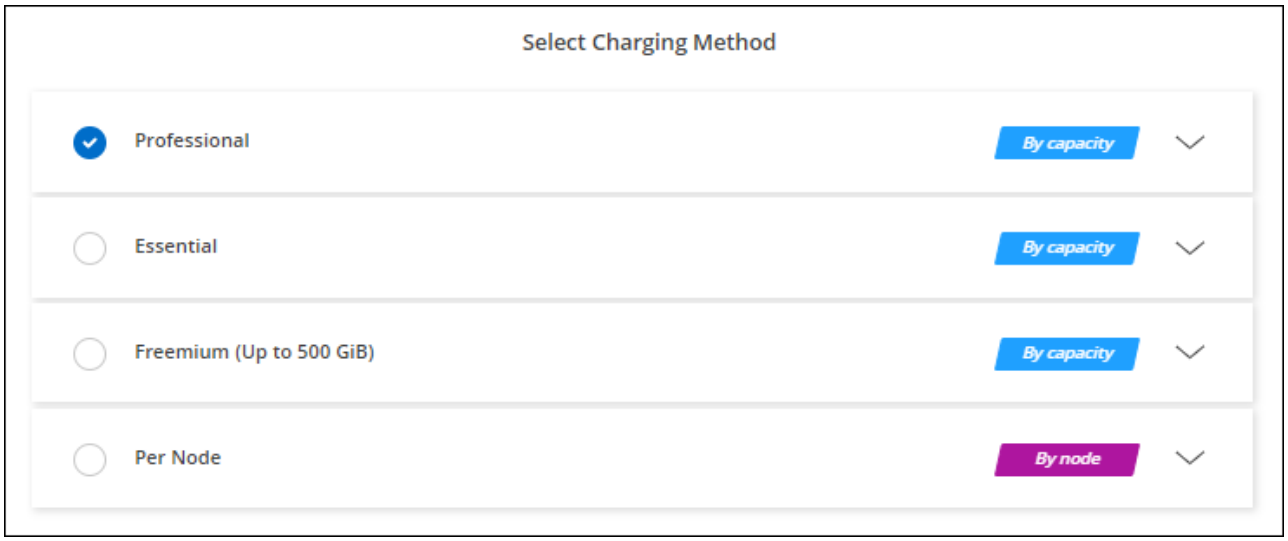
3. En la página Canvas, haga clic en **Agregar entorno de trabajo** y siga los pasos de BlueXP.

   a. En la página **Detalles y credenciales**, haga clic en **Editar credenciales > Agregar suscripción** y siga las indicaciones para suscribirse a la oferta de pago por uso en el mercado de AWS.

      La licencia que ha adquirido de NetApp siempre se factura de primera mano, pero se le cobrará de la tarifa por horas del mercado si sobrepasa la capacidad de la licencia o si caduca el período de su licencia.



a. Después de volver a BlueXP, seleccione un paquete basado en la capacidad cuando llegue a la página de métodos de carga.



"Consulte instrucciones paso a paso para iniciar Cloud Volumes ONTAP en AWS".

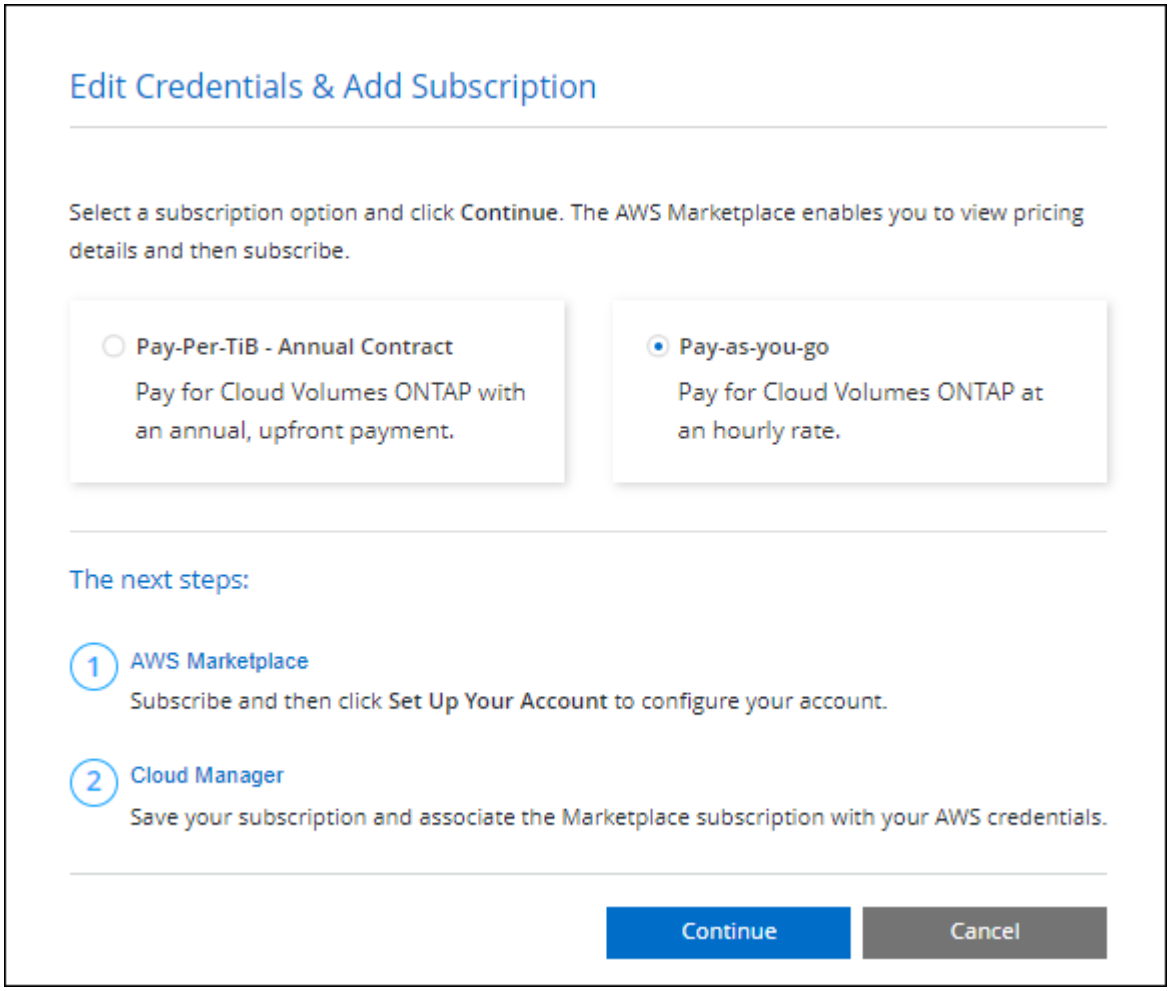
Suscripción a PAYGO

Pague por horas suscribiendo la oferta del mercado de su proveedor de cloud.

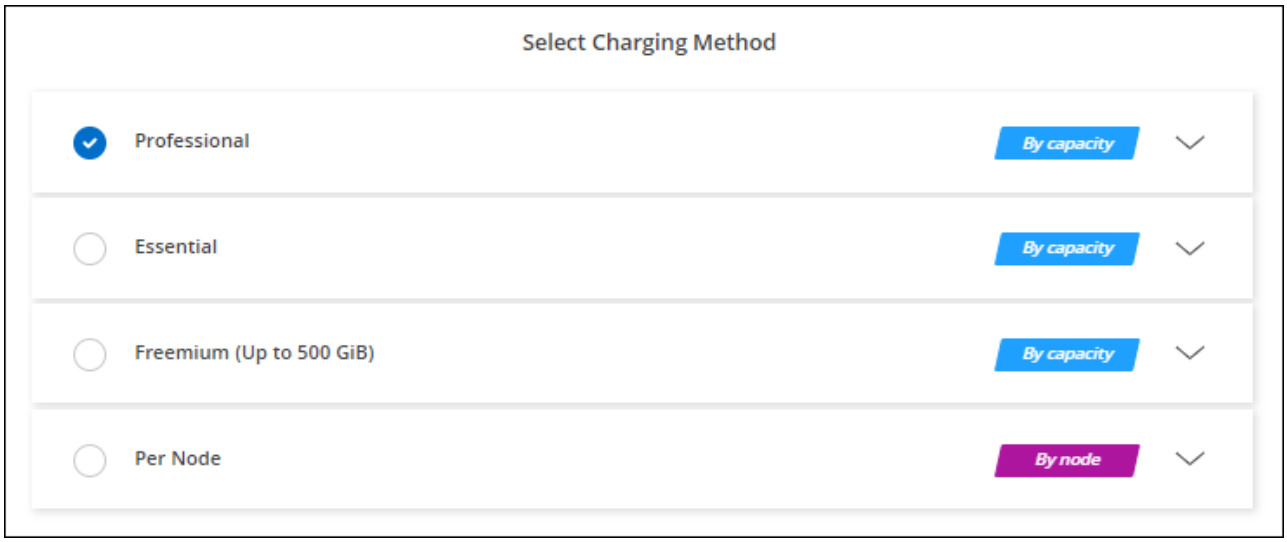
Al crear un entorno de trabajo de Cloud Volumes ONTAP, BlueXP le solicita que se suscriba al acuerdo que está disponible en AWS Marketplace. Esa suscripción se asocia entonces con el entorno de trabajo para la carga. Puede utilizar la misma suscripción para entornos de trabajo adicionales.

Pasos

1. En el menú de navegación de la izquierda, selecciona **almacenamiento > Canvas**.
2. En la página Canvas, haga clic en **Agregar entorno de trabajo** y siga los pasos de BlueXP.
   a. En la página **Detalles y credenciales**, haga clic en **Editar credenciales > Agregar suscripción** y siga las indicaciones para suscribirse a la oferta de pago por uso en el mercado de AWS.



   b. Después de volver a BlueXP, seleccione un paquete basado en la capacidad cuando llegue a la página de métodos de carga.



"Consulte instrucciones paso a paso para iniciar Cloud Volumes ONTAP en AWS".

Puede gestionar las suscripciones de AWS Marketplace asociadas con sus cuentas de AWS desde la página Settings > Credentials. "Aprenda a gestionar sus cuentas y suscripciones de AWS"

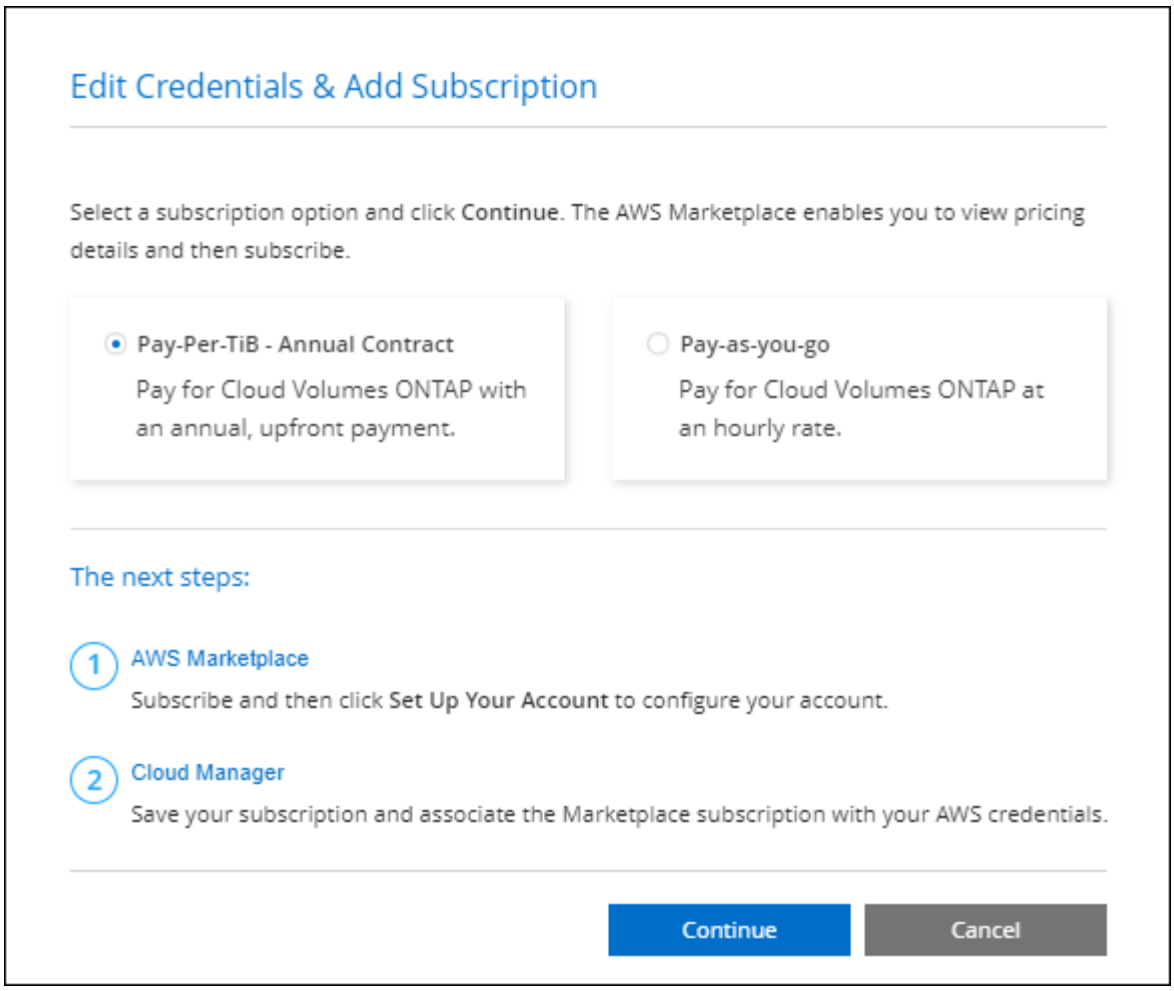
Contrato anual

Pague anualmente al comprar un contrato anual del mercado de su proveedor de cloud.

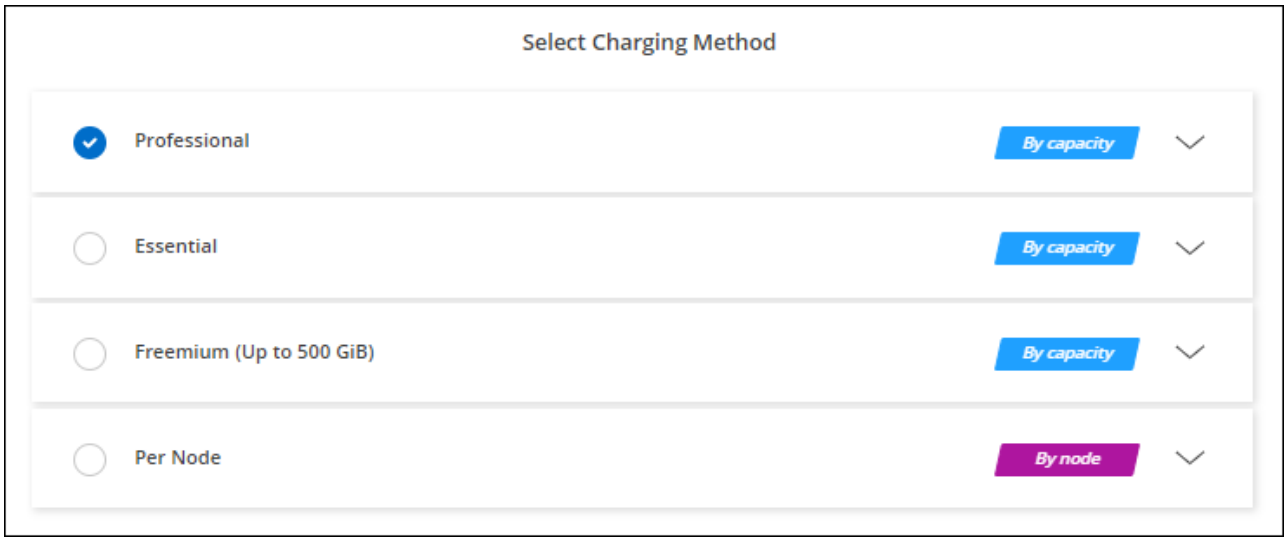
Al igual que una suscripción por horas, BlueXP solicita que se suscriba al contrato anual que está disponible en AWS Marketplace.

Pasos

1. En la página Canvas, haga clic en **Agregar entorno de trabajo** y siga los pasos de BlueXP.
    a. En la página **Detalles y credenciales**, haga clic en **Editar credenciales > Agregar suscripción** y, a continuación, siga las indicaciones para suscribirse al contrato anual en AWS Marketplace.



b. Después de volver a BlueXP, seleccione un paquete basado en la capacidad cuando llegue a la página de métodos de carga.



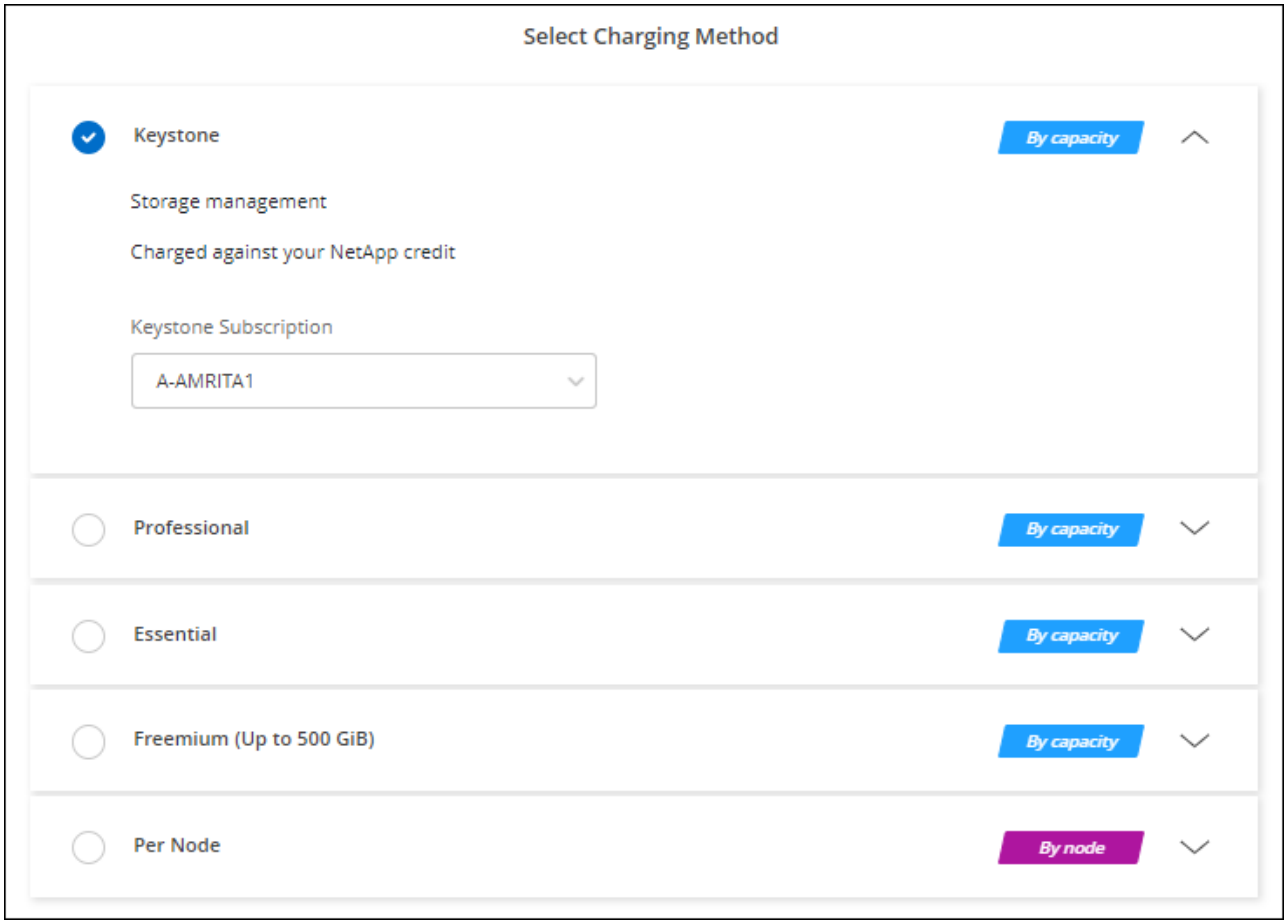
"Consulte instrucciones paso a paso para iniciar Cloud Volumes ONTAP en AWS".

Suscripción a Keystone

Una suscripción a Keystone es un servicio basado en suscripción de pago por crecimiento. "Obtenga más información sobre las suscripciones a NetApp Keystone".

Pasos

1. Si aún no tiene una suscripción, "Póngase en contacto con NetApp"
2. Mailto:ng-keystone-success@netapp.com[Contactar con NetApp] para autorizar tu cuenta de usuario de BlueXP con una o más suscripciones de Keystone.
3. Una vez que NetApp le autorice a su cuenta, "Vincule sus suscripciones para su uso con Cloud Volumes ONTAP".
4. En la página Canvas, haga clic en **Agregar entorno de trabajo** y siga los pasos de BlueXP.
   a. Seleccione el método de carga de Keystone Subscription cuando se le solicite que elija un método de carga.



"Consulte instrucciones paso a paso para iniciar Cloud Volumes ONTAP en AWS".

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.

Antes de empezar

Necesita lo siguiente para crear un entorno de trabajo.

- Un conector que está listo y en funcionamiento.
  - Usted debe tener un "Conector asociado al área de trabajo".
  - "Debe estar preparado para dejar el conector funcionando en en todo momento".
- Descripción de la configuración que desea usar.

  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".
- Comprender qué es necesario para configurar las licencias para Cloud Volumes ONTAP.

  "Aprenda a configurar las licencias".
- Configuraciones DNS y Active Directory para CIFS.

  Para obtener más información, consulte "Requisitos de red para Cloud Volumes ONTAP en AWS".

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

Si desea iniciar Cloud Volumes ONTAP en AWS, debe crear un nuevo entorno de trabajo en BlueXP

Acerca de esta tarea

Inmediatamente después de crear el entorno de trabajo, BlueXP inicia una instancia de prueba en el VPC especificado para verificar la conectividad. Si se realiza correctamente, BlueXP finaliza inmediatamente la instancia y, a continuación, inicia la implementación del sistema Cloud Volumes ONTAP. Si BlueXP no puede verificar la conectividad, la creación del entorno de trabajo falla. 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 el menú de navegación de la izquierda, selecciona **almacenamiento > Canvas**.
2. en la página Canvas, haga clic en **Agregar entorno de trabajo** y siga las indicaciones.
3. **Elija una ubicación**: Seleccione **Amazon Web Services** y **Cloud Volumes ONTAP Single Node**.
4. Si se le solicita, "Cree un conector".
5. **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:

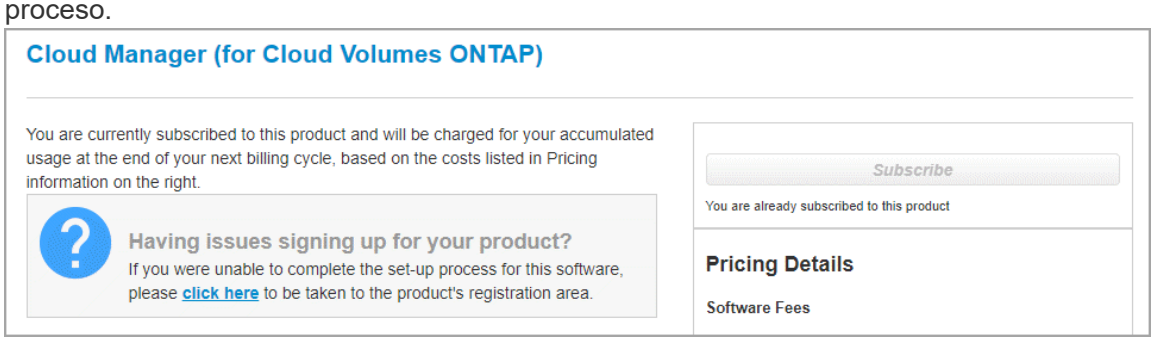
Campo	Descripción
Nombre del entorno de trabajo	BlueXP usa el nombre del entorno de trabajo para asignar un nombre tanto al sistema Cloud Volumes ONTAP como a la instancia de Amazon EC2. También utiliza el nombre como prefijo para el grupo de seguridad predefinido si selecciona esa opción.

Campo	Descripción
Agregar etiquetas	Las etiquetas de AWS son metadatos para sus recursos de AWS. BlueXP agrega las etiquetas a la instancia de Cloud Volumes ONTAP y cada recurso de AWS asociado a 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 System Manager o de la CLI. Mantenga el nombre de usuario predeterminado *admin* o cámbielo por un nombre de usuario personalizado.
Editar credenciales	Seleccione las credenciales de AWS asociadas con la cuenta en la que desea implementar este sistema. También puede asociar la suscripción a AWS Marketplace para utilizarla con este sistema Cloud Volumes ONTAP. Haga clic en **Agregar suscripción** para asociar las credenciales seleccionadas con una nueva suscripción a AWS Marketplace. La suscripción puede ser por un contrato anual o para pagar por Cloud Volumes ONTAP a una tarifa por hora. "Aprenda a añadir credenciales de AWS adicionales a BlueXP".

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

Suscríbete a BlueXP desde AWS Marketplace

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 al sitio Web de BlueXP y completar el proceso.



6. **Servicios**: Mantenga activados los servicios o desactive los servicios individuales que no desea utilizar con Cloud Volumes ONTAP.
   - "Más información sobre la clasificación de BlueXP"

- "Más información sobre el backup y la recuperación de datos de BlueXP"

> Si quieres utilizar WORM y organización de datos en niveles, debes deshabilitar el backup y la recuperación de BlueXP y poner en marcha un entorno de trabajo de Cloud Volumes ONTAP con la versión 9,8 o posterior.

7. **Ubicación y conectividad**: Introduzca la información de red que grabó en "Hoja de cálculo de AWS".

   En la siguiente tabla se describen los campos que podrían presentar dificultades:

Campo	Descripción
VPC	Si tiene una publicación externa de AWS, puede implementar un sistema Cloud Volumes ONTAP de un solo nodo en esa publicación seleccionando el VPC de salida. La experiencia es la misma que cualquier otro VPC que resida en AWS.
Grupo de seguridad generado	Si deja que BlueXP genere el grupo de seguridad para usted, debe elegir cómo permitirá el tráfico: • Si elige **VPC seleccionado sólo**, el origen del tráfico entrante es el rango de subred del VPC seleccionado y el rango de subred del VPC donde reside el conector. Esta es la opción recomendada. • Si elige **All VPC**, el origen del tráfico entrante es el rango IP 0.0.0.0/0.
Utilizar grupo de seguridad existente	Si utiliza una directiva de firewall existente, asegúrese de que incluye las reglas requeridas. "Obtenga más información sobre las reglas de firewall para Cloud Volumes ONTAP".

8. **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".

9. **Métodos de carga y cuenta de NSS**: Especifique la opción de carga que desea utilizar con este sistema y, a continuación, especifique una cuenta en la página de soporte de NetApp.
   - "Obtenga información sobre las opciones de licencia para Cloud Volumes ONTAP".
   - "Aprenda a configurar las licencias".
10. **Configuración de Cloud Volumes ONTAP** (sólo contrato anual de AWS Marketplace): Revise la configuración predeterminada y haga clic en **continuar** o haga clic en **Cambiar configuración** para seleccionar su propia configuración.

    Si mantiene la configuración predeterminada, solo necesita especificar un volumen y, a continuación, revisar y aprobar la configuración.

11. **Paquetes preconfigurados**: Seleccione uno de los paquetes para iniciar rápidamente Cloud Volumes ONTAP, o haga clic en **Cambiar configuración** para seleccionar su propia configuración.

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

12. **Función IAM**: Es mejor mantener la opción predeterminada para que BlueXP cree el papel que le corresponde.

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

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

    > Si hay disponible una versión más reciente de Release Candidate, General Availability o Patch para la versión seleccionada, BlueXP actualiza el sistema a esa versión al crear el entorno de trabajo. Por ejemplo, la actualización se produce si selecciona Cloud Volumes ONTAP 9.10.1 y 9.10.1 P4 está disponible. La actualización no se produce de una versión a otra; por ejemplo, de 9.6 a 9.7.

14. **Recursos de almacenamiento subyacentes**: Elija un tipo de disco, configure el almacenamiento subyacente y elija si desea mantener activada la organización en niveles de datos.

    Tenga en cuenta lo siguiente:

    - El tipo de disco es para el volumen inicial (y el agregado). Es posible elegir un tipo de disco diferente para los volúmenes (y agregados) posteriores.
    - Si elige un disco gp3 o io1, BlueXP utiliza la función Elastic Volumes en AWS para aumentar de forma automática la capacidad de disco de almacenamiento subyacente según sea necesario. Es posible elegir la capacidad inicial según las necesidades de almacenamiento y revisarla después de poner en marcha Cloud Volumes ONTAP. "Obtenga más información sobre el soporte para volúmenes Elastic en AWS".
    - Si elige un disco gp2 o st1, puede seleccionar un tamaño de disco para todos los discos del agregado inicial y para cualquier agregado adicional que BlueXP cree al utilizar la opción de aprovisionamiento simple. Puede crear agregados que utilicen un tamaño de disco diferente mediante la opción de asignación avanzada.
    - 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".

15. **Escribir velocidad y GUSANO**:

    a. Seleccione **normal** o **Alta** velocidad de escritura, si lo desea.

       "Más información sobre la velocidad de escritura".

    b. Si lo desea, active el almacenamiento DE escritura única y lectura múltiple (WORM).

       No se puede habilitar WORM si la organización en niveles de datos se habilitó con las versiones 9.7 y anteriores de Cloud Volumes ONTAP. Revertir o degradar a Cloud Volumes ONTAP 9.8 debe estar

bloqueado después de habilitar WORM y organización en niveles.

"Más información acerca del almacenamiento WORM".

a. Si activa el almacenamiento WORM, seleccione el período de retención.

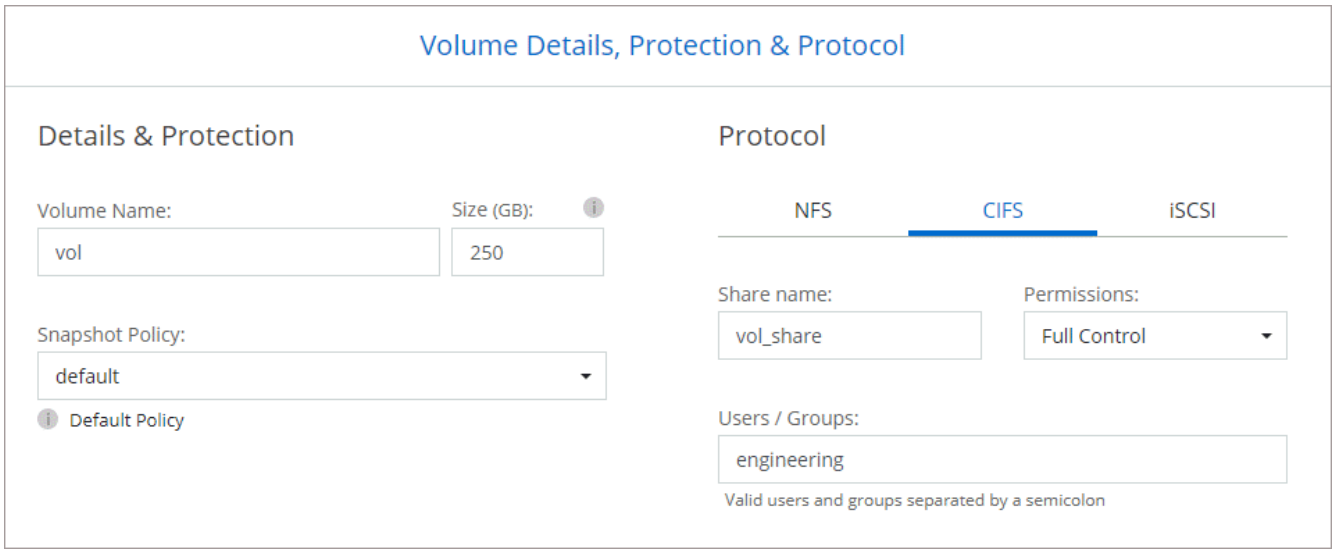
16. **Crear volumen**: Introduzca los detalles del nuevo volumen o haga clic en **Omitir**.

"Obtenga información sobre las versiones y los protocolos de cliente compatibles".

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, BlueXP 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, BlueXP crea automáticamente una LUN para usted. 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:



17. **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 "Documentos de automatización de BlueXP" para obtener más detalles. Tenga en cuenta que solo puede configurar un servidor NTP cuando cree un servidor CIFS. No se puede configurar después de crear el servidor CIFS.

18. **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".

19. **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 la asistencia técnica y los recursos de AWS que BlueXP adquirirá.
    c. Active las casillas de verificación **comprendo…**.
    d. Haga clic en **Ir**.

Resultado

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

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

Para obtener más ayuda, vaya a. "Soporte Cloud Volumes ONTAP de NetApp".

Después de terminar

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

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

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

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

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, BlueXP inicia una instancia de prueba en el VPC especificado para verificar la conectividad. Si se realiza correctamente, BlueXP finaliza inmediatamente la instancia y, a continuación, inicia la implementación del sistema Cloud Volumes ONTAP. Si BlueXP no puede verificar la conectividad, la creación del entorno de trabajo falla. 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 el menú de navegación de la izquierda, selecciona **almacenamiento > Canvas**.
2. En la página Canvas, haga clic en **Agregar entorno de trabajo** y siga las indicaciones.
3. **Elija una ubicación**: Seleccione **Servicios Web de Amazon** y **Cloud Volumes ONTAP ha**.

   Algunas zonas locales de AWS están disponibles.

   Antes de poder utilizar las zonas locales de AWS, debe habilitar las zonas locales y crear una subred en la

zona local en su cuenta de AWS. Siga los pasos de **Opt in to an AWS Local Zone** y **Extend Your Amazon VPC to the Local Zone** en la "Tutorial de AWS «Comience a implementar aplicaciones de baja latencia con las zonas locales de AWS".

Si ejecuta una versión de Connector 3.9.36 o anterior, debe agregar el siguiente permiso al rol de AWS Connector en la consola de AWS EC2: Descripción de las zonas disponibles.

4. **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.

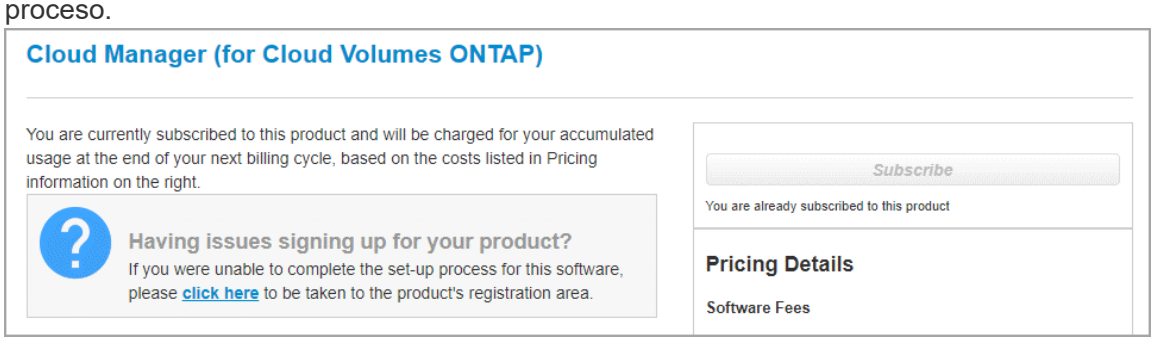
   Algunos de los campos en esta página son claros y explicativos. En la siguiente tabla se describen los campos que podrían presentar dificultades:

Campo	Descripción
Nombre del entorno de trabajo	BlueXP usa 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. BlueXP agrega las etiquetas a la instancia de Cloud Volumes ONTAP y cada recurso de AWS asociado a 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 System Manager o de la CLI. Mantenga el nombre de usuario predeterminado *admin* o cámbielo por un nombre de usuario personalizado.
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 con una nueva suscripción a AWS Marketplace. La suscripción puede ser por un contrato anual o para pagar por Cloud Volumes ONTAP a una tarifa por hora. Si se adquiere una licencia directamente a NetApp (BYOL), no será necesaria una suscripción a AWS. "Aprenda a añadir credenciales de AWS adicionales a BlueXP".

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

   Suscríbete a BlueXP desde AWS Marketplace

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 la página web de BlueXP y completar el proceso.



5. **Servicios**: Mantenga activados o desactive los servicios individuales que no desea utilizar con este sistema Cloud Volumes ONTAP.
   - "Más información sobre la clasificación de BlueXP"
   - "Más información sobre el backup y la recuperación de datos de BlueXP"

   Si quieres utilizar WORM y organización de datos en niveles, debes deshabilitar el backup y la recuperación de BlueXP y poner en marcha un entorno de trabajo de Cloud Volumes ONTAP con la versión 9,8 o posterior.

6. **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".

7. **Ubicación y conectividad** (Single AZ) o **Región y VPC** (varios AZs): Introduzca la información de red que haya grabado en la hoja de trabajo de AWS.

   En la siguiente tabla se describen los campos que podrían presentar dificultades:

Campo	Descripción
Grupo de seguridad generado	Si deja que BlueXP genere el grupo de seguridad para usted, debe elegir cómo permitirá el tráfico: • Si elige **VPC seleccionado sólo**, el origen del tráfico entrante es el rango de subred del VPC seleccionado y el rango de subred del VPC donde reside el conector. Esta es la opción recomendada. • Si elige **All VPC**, el origen del tráfico entrante es el rango IP 0.0.0.0/0.
Utilizar grupo de seguridad existente	Si utiliza una directiva de firewall existente, asegúrese de que incluye las reglas requeridas. "Obtenga más información sobre las reglas de firewall para Cloud Volumes ONTAP".

8. **conectividad y autenticación SSH**: Elija los métodos de conexión para el par ha y el mediador.

9. **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".

10. * 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".

11. **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".

12. **Métodos de carga y cuenta de NSS**: Especifique la opción de carga que desea utilizar con este sistema y, a continuación, especifique una cuenta en la página de soporte de NetApp.
    - "Obtenga información sobre las opciones de licencia para Cloud Volumes ONTAP".
    - "Aprenda a configurar las licencias".
13. **Configuración de Cloud Volumes ONTAP** (sólo contrato anual de AWS Marketplace): Revise la configuración predeterminada y haga clic en **continuar** o haga clic en **Cambiar configuración** para seleccionar su propia configuración.

    Si mantiene la configuración predeterminada, solo necesita especificar un volumen y, a continuación, revisar y aprobar la configuración.

14. **Paquetes preconfigurados** (sólo por hora o por licencia): Seleccione uno de los paquetes para iniciar rápidamente Cloud Volumes ONTAP, o haga clic en **Cambiar configuración** para seleccionar su propia configuración.

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

15. **Función IAM**: Es mejor mantener la opción predeterminada para que BlueXP cree el papel que le corresponde.

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

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

Si hay disponible una versión más reciente de Release Candidate, General Availability o Patch para la versión seleccionada, BlueXP actualiza el sistema a esa versión al crear el entorno de trabajo. Por ejemplo, la actualización se produce si selecciona Cloud Volumes ONTAP 9.10.1 y 9.10.1 P4 está disponible. La actualización no se produce de una versión a otra; por ejemplo, de 9.6 a 9.7.

17. **Recursos de almacenamiento subyacentes**: Elija un tipo de disco, configure el almacenamiento subyacente y elija si desea mantener activada la organización en niveles de datos.

    Tenga en cuenta lo siguiente:

    - El tipo de disco es para el volumen inicial (y el agregado). Es posible elegir un tipo de disco diferente para los volúmenes (y agregados) posteriores.
    - Si elige un disco gp3 o io1, BlueXP utiliza la función Elastic Volumes en AWS para aumentar de forma automática la capacidad de disco de almacenamiento subyacente según sea necesario. Es posible elegir la capacidad inicial según las necesidades de almacenamiento y revisarla después de poner en marcha Cloud Volumes ONTAP. "Obtenga más información sobre el soporte para volúmenes Elastic en AWS".
    - Si elige un disco gp2 o st1, puede seleccionar un tamaño de disco para todos los discos del agregado inicial y para cualquier agregado adicional que BlueXP cree al utilizar la opción de aprovisionamiento simple. Puede crear agregados que utilicen un tamaño de disco diferente mediante la opción de asignación avanzada.
    - 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".

18. **Escribir velocidad y GUSANO**:

    a. Seleccione **normal** o **Alta** velocidad de escritura, si lo desea.

       "Más información sobre la velocidad de escritura".

    b. Si lo desea, active el almacenamiento DE escritura única y lectura múltiple (WORM).

       No se puede habilitar WORM si la organización en niveles de datos se habilitó con las versiones 9.7 y anteriores de Cloud Volumes ONTAP. Revertir o degradar a Cloud Volumes ONTAP 9.8 debe estar bloqueado después de habilitar WORM y organización en niveles.

    "Más información acerca del almacenamiento WORM".

    a. Si activa el almacenamiento WORM, seleccione el período de retención.

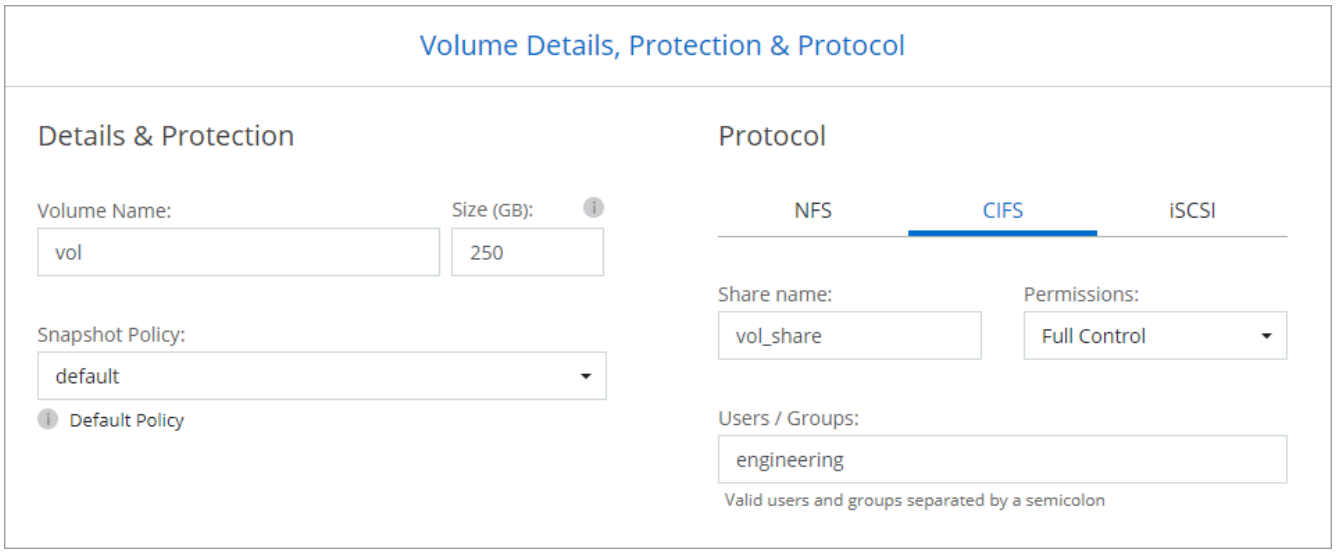
19. **Crear volumen**: Introduzca los detalles del nuevo volumen o haga clic en **Omitir**.

    "Obtenga información sobre las versiones y los protocolos de cliente compatibles".

    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, BlueXP 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, BlueXP crea automáticamente una LUN para usted. 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:



20. **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 "Documentos de automatización de BlueXP" para obtener más detalles. Tenga en cuenta que solo puede configurar un servidor NTP cuando cree un servidor CIFS. No se puede configurar después de crear el servidor CIFS.

21. **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 "Seleccione un perfil de uso de volumen" y.. "Información general sobre organización en niveles de datos".

22. **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 la asistencia técnica y los recursos de AWS que BlueXP adquirirá.
    c. Active las casillas de verificación **comprendo…**.
    d. Haga clic en **Ir**.

Resultado

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

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

Para obtener más ayuda, vaya a. "Soporte Cloud Volumes ONTAP de NetApp".

Después de terminar

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

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

Implemente Cloud Volumes ONTAP en el cloud secreto de AWS y las regiones Top Secret Cloud

Similar a una región estándar de AWS, puedes usar BlueXP en "Cloud secreto de AWS" y en "Cloud secreto principal de AWS" Para poner en marcha Cloud Volumes ONTAP, que ofrece funciones empresariales para su almacenamiento en cloud. AWS Secret Cloud y Top Secret Cloud son regiones cerradas específicas de EE. UU Comunidad de inteligencia; las instrucciones de esta página solo se aplican a los usuarios de la región de AWS Secret Cloud y Top Secret Cloud.

Antes de empezar

Antes de comenzar, revise las versiones compatibles en AWS Secret Cloud y Top Secret Cloud y obtenga información acerca del modo privado en BlueXP.

- Revise las siguientes versiones compatibles en AWS Secret Cloud y Top Secret Cloud:
  - Cloud Volumes ONTAP 9.12.1 P2
  - Versión 3.9.32 del conector

    El conector es un software necesario para poner en marcha y gestionar Cloud Volumes ONTAP en AWS. Iniciarás sesión en BlueXP desde el software que se instala en la instancia de Connector. El sitio web de SaaS para BlueXP no es compatible con AWS Secret Cloud y Top Secret Cloud.

- Aprende sobre el modo privado

  En AWS Secret Cloud y Top Secret Cloud, BlueXP funciona en *modo privado*. En el modo privado, no existe conectividad a la capa SaaS de BlueXP. Los usuarios acceden a BlueXP de forma local desde la consola basada en web que está disponible desde Connector, no desde la capa SaaS.

  Para obtener más información sobre cómo funciona el modo privado, consulte "Modo de implementación privada de BlueXP".

Paso 1: Configure su red

Configurar sus redes de AWS para que Cloud Volumes ONTAP pueda funcionar correctamente.

Pasos

1. Elija el VPC y las subredes en las que desea iniciar las instancias de Connector y Cloud Volumes ONTAP.
2. Asegúrese de que VPC y las subredes admitan la conectividad entre 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.

Paso 2: Configurar permisos

Configure las políticas y roles de IAM que proporcionen a Connector y a Cloud Volumes ONTAP los permisos que necesitan para realizar acciones en la nube secreta de AWS o en la nube secreta superior.

Necesita una política IAM y un rol IAM para cada una de las siguientes acciones:

- La instancia de conector
- Instancias de Cloud Volumes ONTAP
- Para pares de alta disponibilidad, la instancia de mediador de alta disponibilidad de Cloud Volumes ONTAP (si desea poner en marcha pares de alta disponibilidad).

Pasos

1. Vaya a la consola AWS IAM y haga clic en **Directivas**.
2. Cree una directiva para la instancia de Connector.

Estas políticas se crean para dar soporte a los buckets S3 en su entorno AWS. Al crear los cubos más tarde, asegúrese de que los nombres de los cubos tengan el prefijo `fabric-pool-`. Este requisito se aplica tanto a las regiones de la nube secreta de AWS como a la nube secreta superior.

Regiones secretas

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
```

```
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso-b:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
```

```
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

Regiones Top Secret

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
```

```
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso:ec2:*:*:volume/*"
            ]
        }
    ]
```

```
}
```

3. Crear una política para Cloud Volumes ONTAP.

Regiones secretas

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso-b:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

Regiones Top Secret

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

Para pares de alta disponibilidad, si tiene pensado poner en marcha un par de alta disponibilidad de Cloud Volumes ONTAP, cree una política para el mediador de alta disponibilidad.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": "*"
        }
    ]
}
```

4. Cree roles IAM con el tipo de rol Amazon EC2 y adjunte las políticas que creó en los pasos anteriores.

   Cree el rol:

   Similar a las políticas, debe tener un rol de IAM para el conector y uno para los nodos de Cloud Volumes ONTAP.
   Para pares de alta disponibilidad: Al igual que las políticas, debe tener un rol de IAM para el conector, uno para los nodos de Cloud Volumes ONTAP y otro para el mediador de alta disponibilidad (si desea implementar pares de alta disponibilidad).

   Seleccione el rol:

   Debe seleccionar el rol Connector IAM al iniciar la instancia de Connector. Puedes seleccionar los roles de IAM para Cloud Volumes ONTAP al crear un entorno de trabajo de Cloud Volumes ONTAP desde BlueXP. Para parejas de alta disponibilidad, puedes seleccionar los roles de IAM para Cloud Volumes ONTAP y el mediador de alta disponibilidad al crear un entorno de trabajo de Cloud Volumes ONTAP desde BlueXP.

Paso 3: Configure el AWS KMS

Si desea utilizar el cifrado de Amazon con Cloud Volumes ONTAP, asegúrese de que se cumplan los requisitos del servicio de gestión de claves (KMS) de AWS.

Pasos

1. Asegúrese de que existe una clave maestra de cliente (CMK) activa en su cuenta o en otra cuenta de AWS.

   El CMK puede ser un CMK gestionado por AWS o un CMK gestionado por el cliente.

2. Si el CMK se encuentra en una cuenta de AWS independiente de la cuenta en la que tiene pensado implementar Cloud Volumes ONTAP, deberá obtener el ARN de esa clave.

Deberá proporcionar el ARN a BlueXP cuando cree el sistema Cloud Volumes ONTAP.

3. Añada el rol IAM de la instancia de conector a la lista de usuarios clave de un CMK.

   Esto le otorga permisos a BlueXP para usar el CMK con Cloud Volumes ONTAP.

Paso 4: Instala el conector y configura BlueXP

Antes de empezar a usar BlueXP para implementar Cloud Volumes ONTAP en AWS, debe instalar y configurar el conector BlueXP. El conector permite a BlueXP gestionar recursos y procesos dentro de tu entorno de nube pública (incluye Cloud Volumes ONTAP).

Pasos

1. Obtenga un certificado raíz firmado por una entidad de certificación (CA) en el formato X.509 codificado por Privacy Enhanced Mail (PEM) base-64. Consulte las políticas y procedimientos de su organización para obtener el certificado.

   > Para las regiones de AWS Secret Cloud, debe cargar el `NSS Root CA 2` Certificate y, para Top Secret Cloud, el `Amazon Root CA 4` certificado. Asegúrese de cargar solo estos certificados y no toda la cadena. El archivo para la cadena de certificados es grande y se puede producir un error en la carga. Si tiene certificados adicionales, puede cargarlos más adelante, tal y como se describe en el paso siguiente.

   Deberá cargar el certificado durante el proceso de configuración. BlueXP utiliza el certificado de confianza al enviar solicitudes a AWS a través de HTTPS.

2. Inicie la instancia de conector:
   a. Ve a la página AWS Intelligence Community Marketplace para BlueXP.
   b. En la pestaña Inicio personalizado, seleccione la opción para iniciar la instancia desde la consola EC2.
   c. Siga las instrucciones para configurar la instancia.

      Tenga en cuenta lo siguiente al configurar la instancia:

      - Recomendamos t3.xlarge.
      - Debe elegir el rol de IAM que creó al configurar los permisos.
      - Debe conservar las opciones de almacenamiento predeterminadas.
      - Los métodos de conexión necesarios para el conector son los siguientes: SSH, HTTP y HTTPS.
3. Configura BlueXP desde un host que tenga una conexión a la instancia de Connector:
   a. Abra un explorador web e introduzca https://ipaddress Donde ipaddress es la dirección IP del host Linux en el que instaló el conector.
   b. Especifique un servidor proxy para la conectividad con los servicios de AWS.
   c. Cargue el certificado obtenido en el paso 1.
   d. Selecciona **Configurar nuevo BlueXP** y sigue las indicaciones para configurar el sistema.
      - **Detalles del sistema**: Introduzca un nombre para el conector y el nombre de su empresa.
      - **Crear usuario administrador**: Cree el usuario administrador para el sistema.

Esta cuenta de usuario se ejecuta localmente en el sistema. No hay conexión con el servicio auth0 disponible a través de BlueXP.

- **Revisión**: Revisa los detalles, acepta el contrato de licencia y luego selecciona **Configurar**.

e. Para completar la instalación del certificado firmado por CA, reinicie la instancia del conector desde la consola EC2.

4. Después de reiniciar el conector, inicie sesión con la cuenta de usuario de administrador que creó en el asistente de configuración.

Paso 5: (Opcional) Instale un certificado de modo privado

Este paso es opcional para las regiones de AWS Secret Cloud y Top Secret Cloud, y solo es necesario si tiene certificados adicionales aparte de los certificados raíz que instaló en el paso anterior.

Pasos

1. Enumera los certificados instalados existentes.

a. Para recopilar el identificador de Docker de contenedor occm (nombre identificado “ds-occm-1”), ejecute el siguiente comando:

```
docker ps
```

b. Para acceder al contenedor occm, ejecute el siguiente comando:

```
docker exec -it <docker-id> /bin/sh
```

c. Para recopilar la contraseña de la variable de entorno “TRUST_STORE_PASSWORD”, ejecute el siguiente comando:

```
env
```

d. Para enumerar todos los certificados instalados en el almacén de confianza, ejecute el siguiente comando y utilice la contraseña recopilada en el paso anterior:

```
keytool -list -v -keystore occm.truststore
```

2. Agregue un certificado.

a. Para recoger el identificador de occm Container docker (nombre identificado “ds-occm-1”), ejecute el siguiente comando:

```
docker ps
```

b. Para acceder al contenedor occm, ejecute el siguiente comando:

```
docker exec -it <docker-id> /bin/sh
```

Guarde el nuevo archivo de certificado dentro.

c. Para recopilar la contraseña de la variable de entorno “TRUST_STORE_PASSWORD”, ejecute el siguiente comando:

```
env
```

d. Para agregar el certificado al almacén de confianza, ejecute el siguiente comando y utilice la contraseña del paso anterior:

```
keytool -import -alias <alias-name> -file <certificate-file-name>
-keystore occm.truststore
```

e. Para comprobar que el certificado está instalado, ejecute el siguiente comando:

```
keytool -list -v -keystore occm.truststore -alias <alias-name>
```

f. Para salir del contenedor occm, ejecute el siguiente comando:

```
exit
```

g. Para restablecer el contenedor occm, ejecute el siguiente comando:

```
docker restart <docker-id>
```

Paso 6: Añadir una licencia a la cartera digital de BlueXP

Si compró una licencia de NetApp, debe añadirla a la cartera digital de BlueXP para que pueda seleccionar la licencia cuando cree un nuevo sistema Cloud Volumes ONTAP. La cartera digital identifica estas licencias como no asignadas.

Pasos

1. En el menú de navegación de BlueXP, seleccione **Gobierno > cartera digital**.
2. En la ficha **Cloud Volumes ONTAP**, seleccione **licencias basadas en nodos** en la lista desplegable.
3. Haga clic en **sin asignar**.
4. Haga clic en **Agregar licencias sin asignar**.
5. Escriba el número de serie de la licencia o cargue el archivo de licencia.
6. Si aún no tiene el archivo de licencia, deberá cargar manualmente el archivo de licencia desde

netapp.com.

a. Vaya a la "Generador de archivos de licencia de NetApp" E inicie sesión con sus credenciales del sitio de soporte de NetApp.

b. Introduzca su contraseña, elija su producto, introduzca el número de serie, confirme que ha leído y aceptado la política de privacidad y, a continuación, haga clic en **Enviar**.

c. Elija si desea recibir el archivo serialnumber.NLF JSON a través del correo electrónico o la descarga directa.

7. Haga clic en **Agregar licencia**.

Resultado

BlueXP añade la licencia a la cartera digital. La licencia se identificará como sin asignar hasta que se asocie con un nuevo sistema Cloud Volumes ONTAP. Una vez que esto sucede, la licencia se traslada a la pestaña BYOL de la cartera digital.

Paso 7: Inicia Cloud Volumes ONTAP de BlueXP

Puedes iniciar instancias de Cloud Volumes ONTAP en la nube secreta de AWS y Top Secret Cloud creando nuevos entornos de trabajo en BlueXP.

Antes de empezar

En el caso de los pares de alta disponibilidad, se requiere un par de claves para habilitar la autenticación SSH basada en claves en el mediador de alta disponibilidad.

Pasos

1. En la página entornos de trabajo, haga clic en **Agregar entorno de trabajo**.
2. En **Crear**, selecciona Cloud Volumes ONTAP.

   Para HA: En **Crear**, seleccione Cloud Volumes ONTAP o Cloud Volumes ONTAP HA.

3. Complete los pasos del asistente para iniciar el sistema Cloud Volumes ONTAP.

Mientras realiza selecciones a través del asistente, no seleccione **Detección de datos y cumplimiento** ni **Copia de seguridad en la nube** en **Servicios**. En **Paquetes preconfigurados**, selecciona **Cambiar configuración** solamente, y asegúrate de que no has seleccionado ninguna otra opción. Los paquetes preconfigurados no son compatibles con las regiones de AWS Secret Cloud y Top Secret Cloud, y si se selecciona, su implementación fallará.

Notas para implementar HA de Cloud Volumes ONTAP en varias zonas de disponibilidad

Tenga en cuenta lo siguiente a medida que completa el asistente para las parejas de alta disponibilidad.

- Debe configurar una puerta de enlace de tránsito cuando implemente Cloud Volumes ONTAP HA en varias zonas de disponibilidad (AZ). Consulte "Configure una puerta de enlace de tránsito de AWS".
- Implemente la configuración de la siguiente manera porque solo había dos AZs disponibles en la nube de AWS Top Secret en el momento de la publicación:
  - Nodo 1: Zona De disponibilidad A
  - Nodo 2: Zona de disponibilidad B
  - Mediador: Zona de disponibilidad A o B

Notas para poner en marcha Cloud Volumes ONTAP en nodos únicos y de alta disponibilidad

Tenga en cuenta lo siguiente al completar el asistente:

- Debe dejar la opción predeterminada para utilizar un grupo de seguridad generado.

  El grupo de seguridad predefinido incluye las reglas que Cloud Volumes ONTAP necesita para funcionar correctamente. Si tiene un requisito para utilizar el suyo propio, puede consultar la sección de grupos de seguridad que aparece a continuación.

- Debe elegir el rol de IAM que ha creado al preparar el entorno AWS.
- El tipo de disco de AWS subyacente es para el volumen Cloud Volumes ONTAP inicial.

  Es posible seleccionar un tipo de disco diferente para volúmenes posteriores.

- El rendimiento de los discos AWS está ligado al tamaño del disco.

  Elija el tamaño de disco que le proporcione el rendimiento sostenido que necesita. Consulte la documentación de AWS para obtener más detalles sobre el rendimiento de EBS.

- El tamaño de disco es el tamaño predeterminado para todos los discos del sistema.

  Si después necesita un tamaño diferente, puede utilizar la opción asignación avanzada para crear un agregado que utilice discos de un tamaño específico.

Resultado

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

Paso 8: Instale certificados de seguridad para la organización de datos en niveles

Debes instalar manualmente certificados de seguridad para habilitar la organización de datos en niveles en las regiones de AWS Secret Cloud y Top Secret Cloud.

Antes de empezar

1. Cree bloques S3.

   Asegúrese de que los nombres de los depósitos tienen el prefijo `fabric-pool-`. Por ejemplo `fabric-pool-testbucket`.

2. Conserve los certificados raíz en los que ha instalado `step 4` práctico.

Pasos

1. Copie el texto de los certificados raíz en los que ha instalado `step 4`.
2. Conéctese de forma segura al sistema Cloud Volumes ONTAP utilizando la CLI.
3. Instale los certificados raíz. Es posible que tenga que pulsar el `ENTER` teclas varias veces:

```
security certificate install -type server-ca -cert-name <certificate-
name>
```

4. Cuando se le solicite, introduzca todo el texto copiado, incluido y desde `----- BEGIN CERTIFICATE -----` para `----- END CERTIFICATE -----`.
5. Conserve una copia del certificado digital firmado por CA para futuras referencias.
6. Conserve el nombre de CA y el número de serie del certificado.
7. Configure el almacén de objetos para las regiones de AWS Secret Cloud y Top Secret Cloud: `set -privilege advanced -confirmations off`
8. Ejecute este comando para configurar el almacén de objetos.

> Todos los nombres de recursos de Amazon (ARN) deben estar sufijos con `-iso-b`, por ejemplo `arn:aws-iso-b`. Por ejemplo, si un recurso requiere un ARN con una región, para la nube de secreto superior, utilice la convención de nomenclatura como `us-iso-b` para la `-server` bandera. Para el cloud secreto de AWS, uso `us-iso-b-1`.

```
storage aggregate object-store config create -object-store-name
<S3Bucket> -provider-type AWS_S3 -auth-type EC2-IAM -server <s3.us-iso-
b-1.server_name> -container-name <fabric-pool-testbucket> -is-ssl
-enabled true -port 443
```

9. Compruebe que el almacén de objetos se ha creado correctamente: `storage aggregate object-store show -instance`
10. Adjunte el almacén de objetos al agregado. Esto se debe repetir para cada agregado nuevo: `storage aggregate object-store attach -aggregate <aggr1> -object-store-name <S3Bucket>`