Manos a la obra

Cloud Volumes ONTAP

NetApp
June 11, 2024

Tabla de contenidos

Manos a la obra

Más información sobre Cloud Volumes ONTAP

Cloud Volumes ONTAP le permite optimizar los costes y el rendimiento del almacenamiento en cloud, a la vez que mejora la protección de datos, la seguridad y el cumplimiento de normativas.

Cloud Volumes ONTAP es un dispositivo de almacenamiento exclusivamente de software que ejecuta el software de gestión de datos ONTAP en el cloud. Ofrece almacenamiento empresarial con las siguientes funciones clave:

- Eficiencias del almacenamiento

  Aproveche las funciones integradas de deduplicación de datos, compresión de datos, thin provisioning y clonado para minimizar los costes en almacenamiento.

- Alta disponibilidad

  Garantice la fiabilidad de su empresa y la continuidad de las operaciones en caso de fallos en su entorno cloud.

- Protección de datos

  Cloud Volumes ONTAP aprovecha SnapMirror, la tecnología de replicación líder del sector de NetApp, para replicar los datos en las instalaciones al cloud para que sea fácil disponer de copias secundarias para varios casos de uso.

  Cloud Volumes ONTAP también se integra con el backup y la recuperación de datos de BlueXP para ofrecer funcionalidades de backup y restauración con el fin de proteger y archivar a largo plazo tus datos en la nube.

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

- Organización en niveles de los datos

  Cambie entre pools de almacenamiento de alto y bajo rendimiento bajo demanda sin desconectar las aplicaciones.

- Consistencia de las aplicaciones

  Garantice la consistencia de las copias Snapshot de NetApp mediante SnapCenter de NetApp.

  "Obtenga más información acerca de SnapCenter"

- Seguridad de datos

  Cloud Volumes ONTAP admite el cifrado de datos y proporciona protección contra virus y ransomware.

- Controles de cumplimiento de normas de privacidad

  La integración con la clasificación de BlueXP te ayuda a comprender el contexto de los datos e identificar los datos confidenciales.

"Más información sobre la clasificación de BlueXP"

Con Cloud Volumes ONTAP se incluyen las licencias para funciones de ONTAP.

"Consulte las configuraciones de Cloud Volumes ONTAP admitidas"

"Obtenga más información acerca de Cloud Volumes ONTAP"

Versiones de ONTAP admitidas para nuevas puestas en marcha

BlueXP le permite elegir entre varias versiones diferentes de ONTAP al crear un nuevo entorno de trabajo de Cloud Volumes ONTAP.

Las versiones de Cloud Volumes ONTAP que no son las enumeradas aquí no están disponibles para nuevas implementaciones. Para obtener más información sobre la actualización, consulte "Rutas de actualización admitidas".

AWS

Un solo nodo

- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

Pareja de HA

- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA

- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

Azure

Un solo nodo

- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3
- 9.9.1 P8
- 9.9.1 P7
- 9.8 P10
- 9.7 P6
- 9.5 P6

Pareja de HA

- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3
- 9.9.1 P8
- 9.9.1 P7

- 9.8 P10
- 9.7 P6

Google Cloud

Un solo nodo

- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5

Pareja de HA

- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8

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	

Información de AWS	Su valor
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

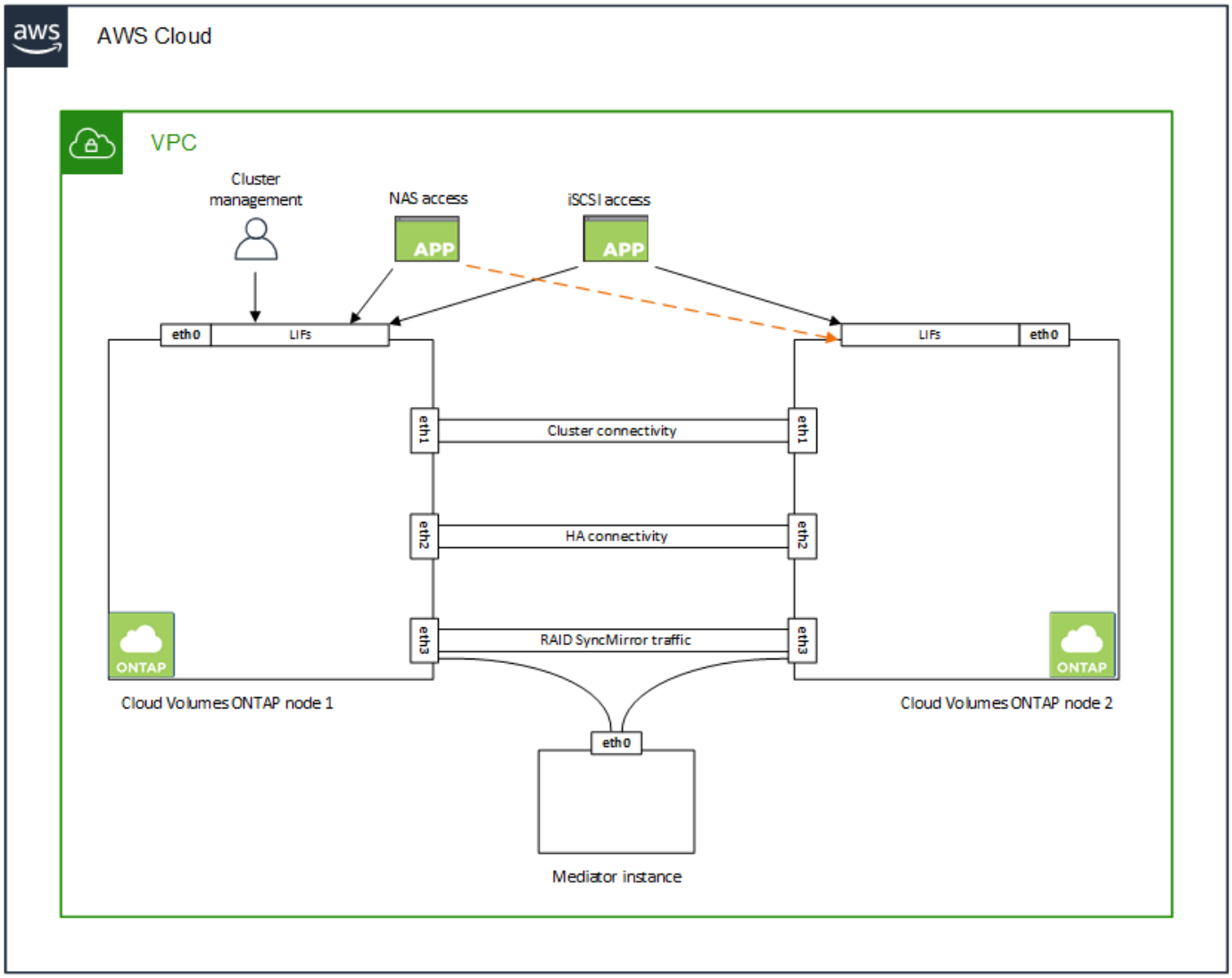
BlueXP asigna 6 direcciones IP a un sistema de un solo nodo.

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

Direcciones IP para pares de alta disponibilidad

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



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

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

LIF para pares de alta disponibilidad en un único AZ

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

LUN	Interfaz	Nodo	Específico
Datos de iSCSI	eth0	nodo 1 y nodo 2	Acceso de cliente a través del protocolo iSCSI. También lo utiliza el sistema para otros flujos de trabajo de red importantes. Estos LIF son necesarios y no deben eliminarse.
Conectividad del clúster	eth1	nodo 1 y nodo 2	Permite que los nodos se comuniquen entre sí y que muevan datos dentro del clúster.
Conectividad de alta DISPONIBILIDAD	eth2	nodo 1 y nodo 2	Comunicación entre los dos nodos en caso de conmutación al nodo de respaldo.
Tráfico iSCSI de RSM	eth3	nodo 1 y nodo 2	Tráfico iSCSI de RAID SyncMirror, así como comunicación entre los dos nodos de Cloud Volumes ONTAP y el mediador.
Mediador	eth0	Mediador	Un canal de comunicación entre los nodos y el mediador para 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.
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".

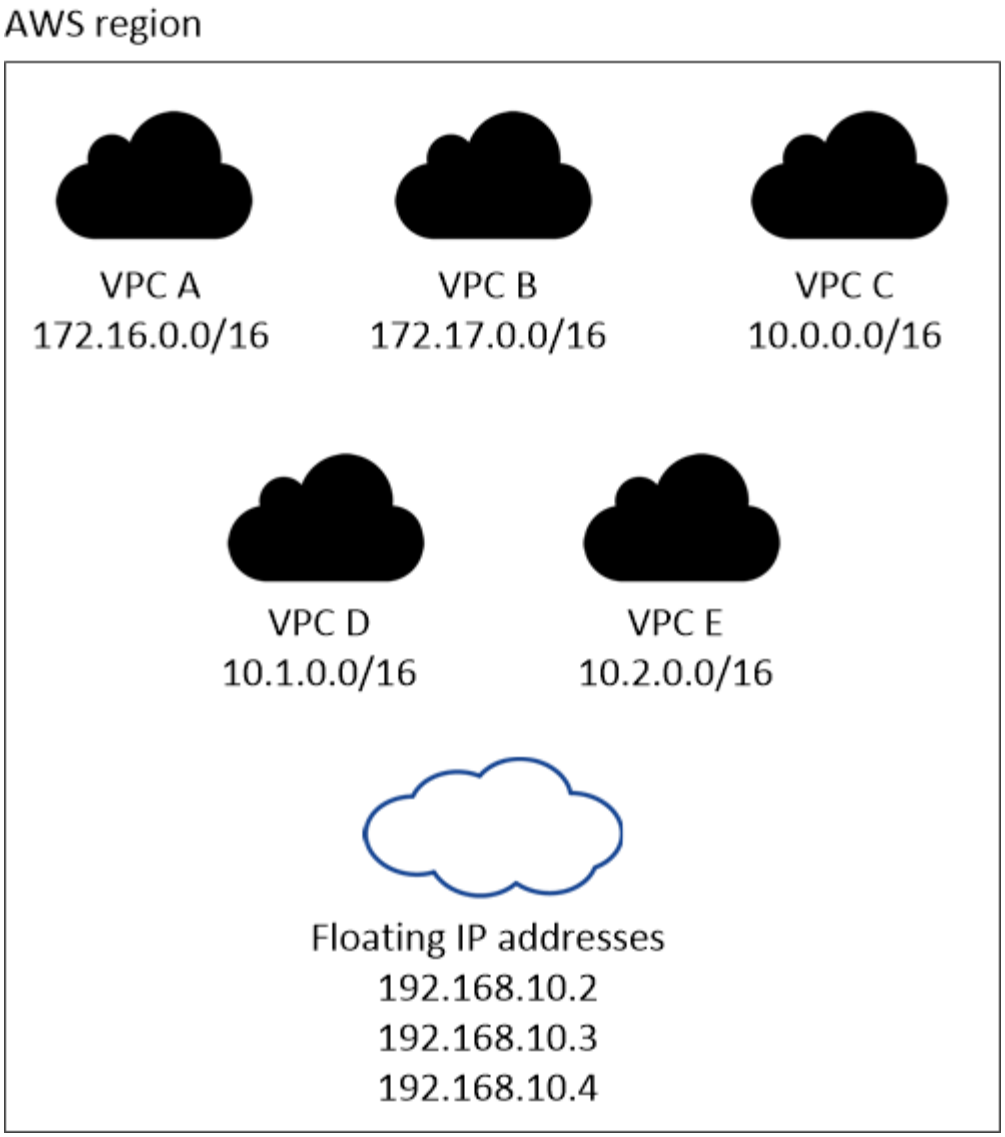
Una dirección IP flotante es para la gestión del clúster, otra para los datos NFS/CIFS del nodo 1 y otra para los datos NFS/CIFS del nodo 2. Una cuarta dirección IP flotante para la gestión de SVM es opcional.

> 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".

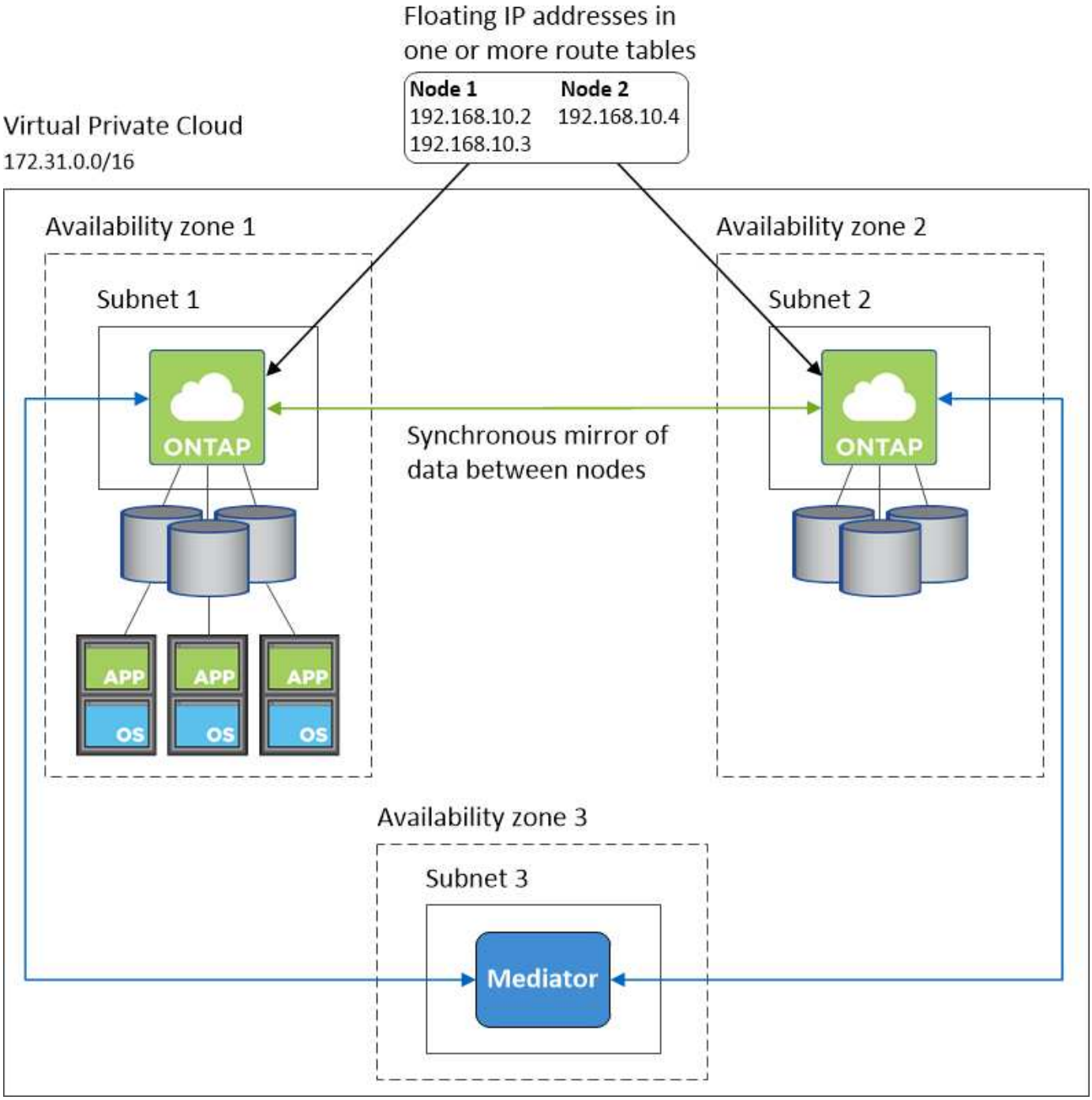
Conexión a herramientas de gestión de NetApp

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

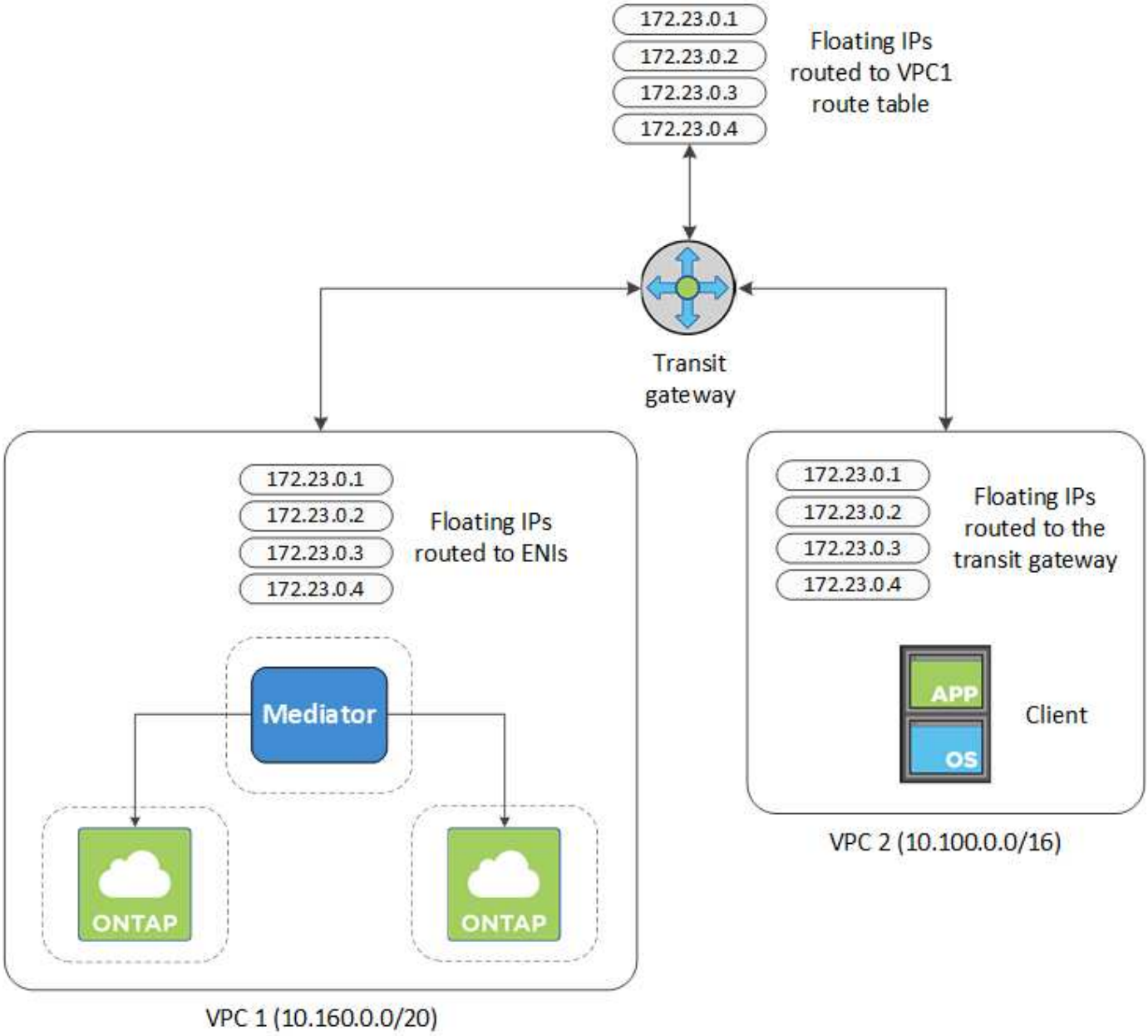
alta disponibilidad.

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.



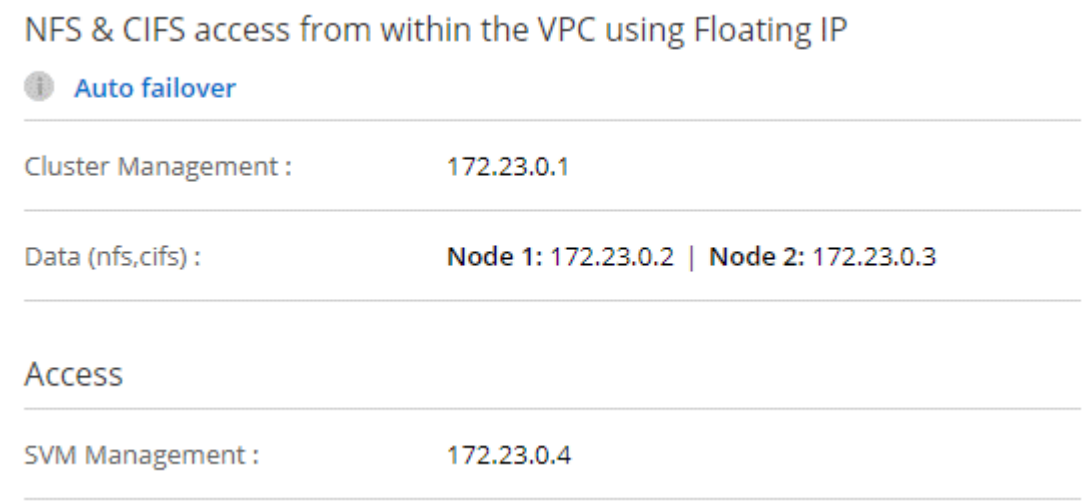
Los siguientes pasos ilustran cómo configurar una configuración similar.

Pasos

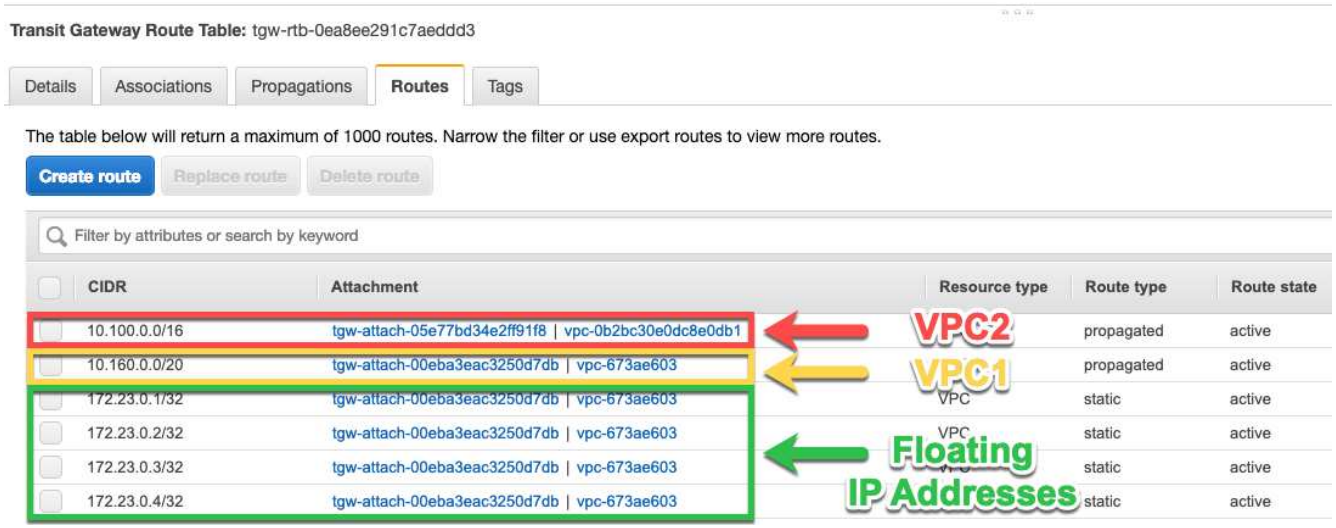
1. "Cree una puerta de enlace de tránsito y conecte las VPC al puerta de enlace".
2. Asocie las VPC a la tabla de rutas de la puerta de enlace de tránsito.
   a. En el servicio **VPC**, haga clic en **tablas de rutas de puerta de enlace de tránsito**.
   b. Seleccione la tabla de rutas.
   c. Haga clic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

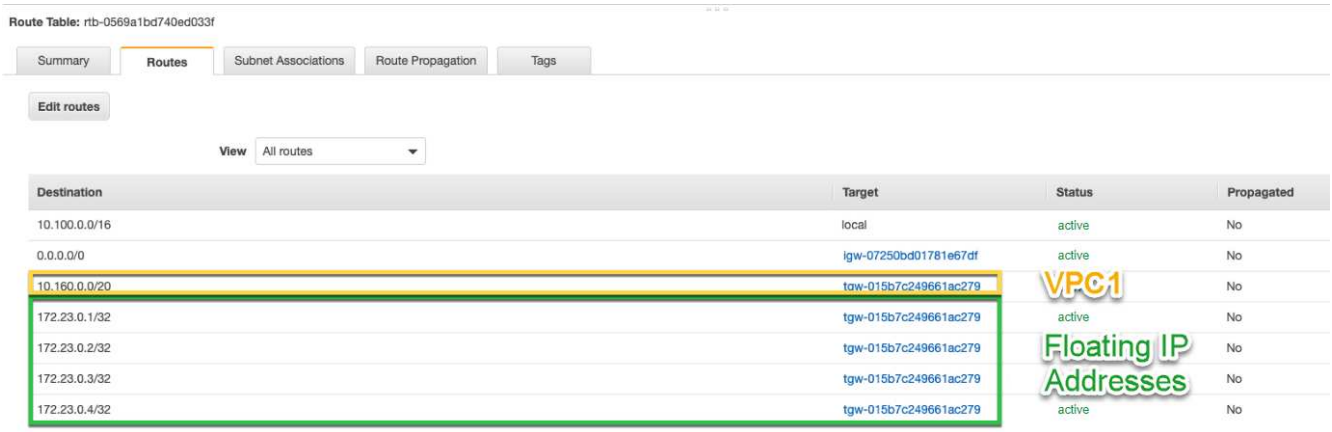


4. Modifique la tabla de rutas de las VPC que necesitan acceder a las direcciones IP flotantes.

   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.

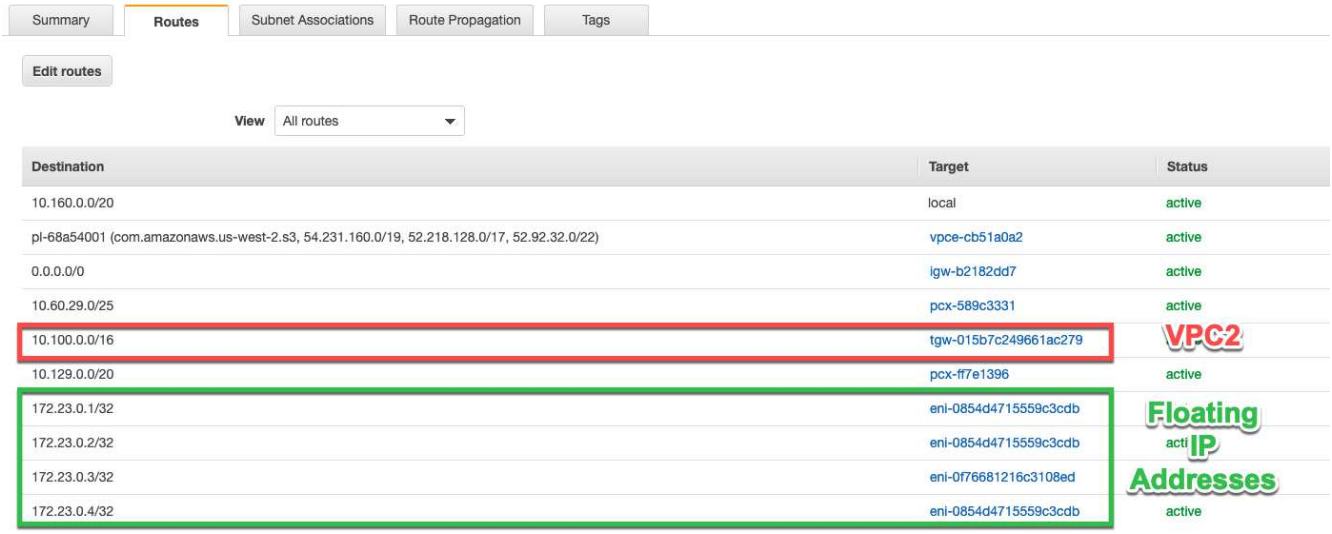
      La siguiente imagen de ejemplo muestra la tabla de rutas para VPC 2, que incluye las rutas hasta VPC 1 y las direcciones IP flotantes.



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.

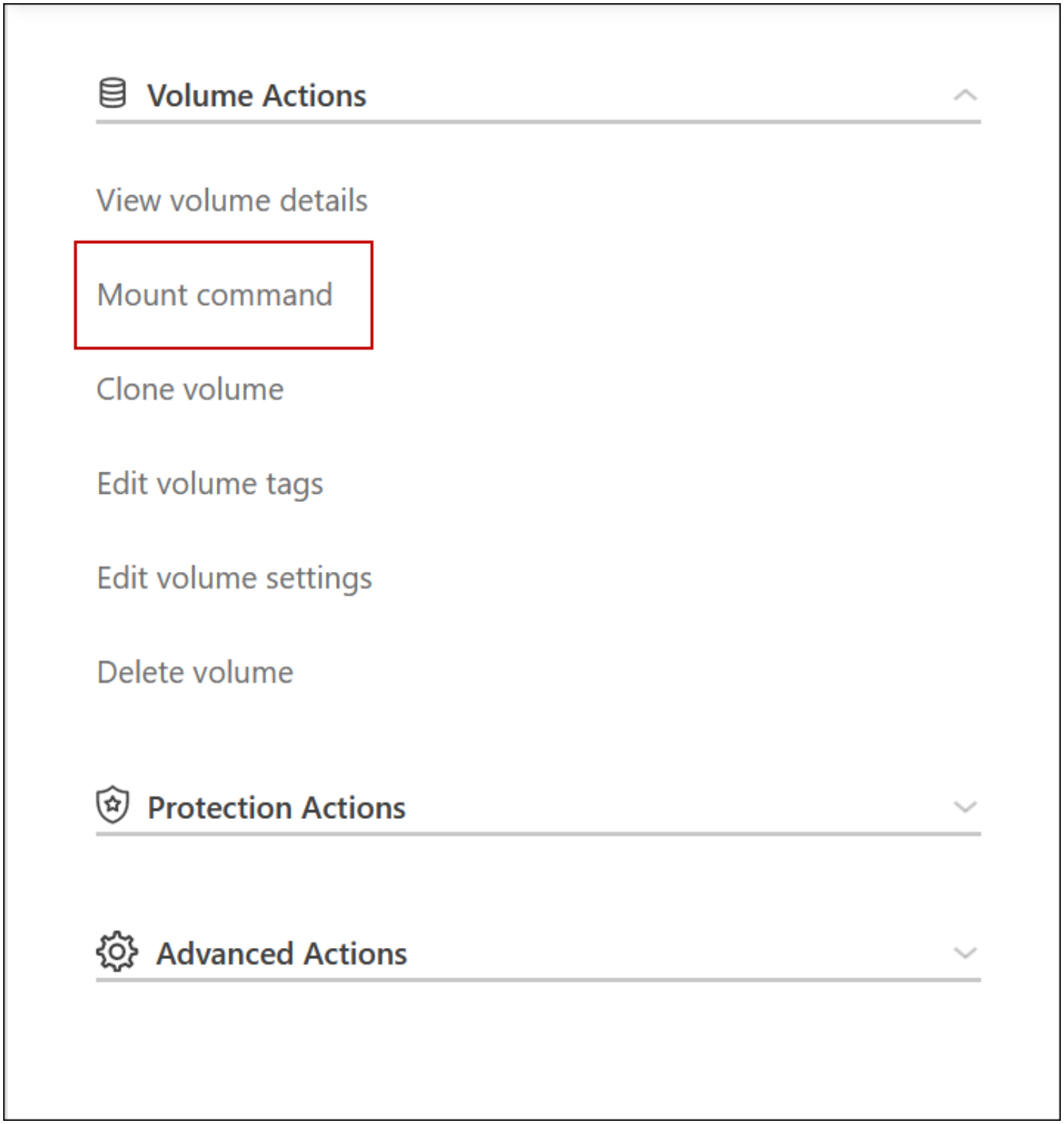
   La siguiente imagen de ejemplo muestra la tabla de rutas para VPC 1. Incluye una ruta a las direcciones IP flotantes y al VPC 2, que es donde reside un cliente. BlueXP agregó automáticamente las IP flotantes a la tabla de rutas cuando implementó el par ha.



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

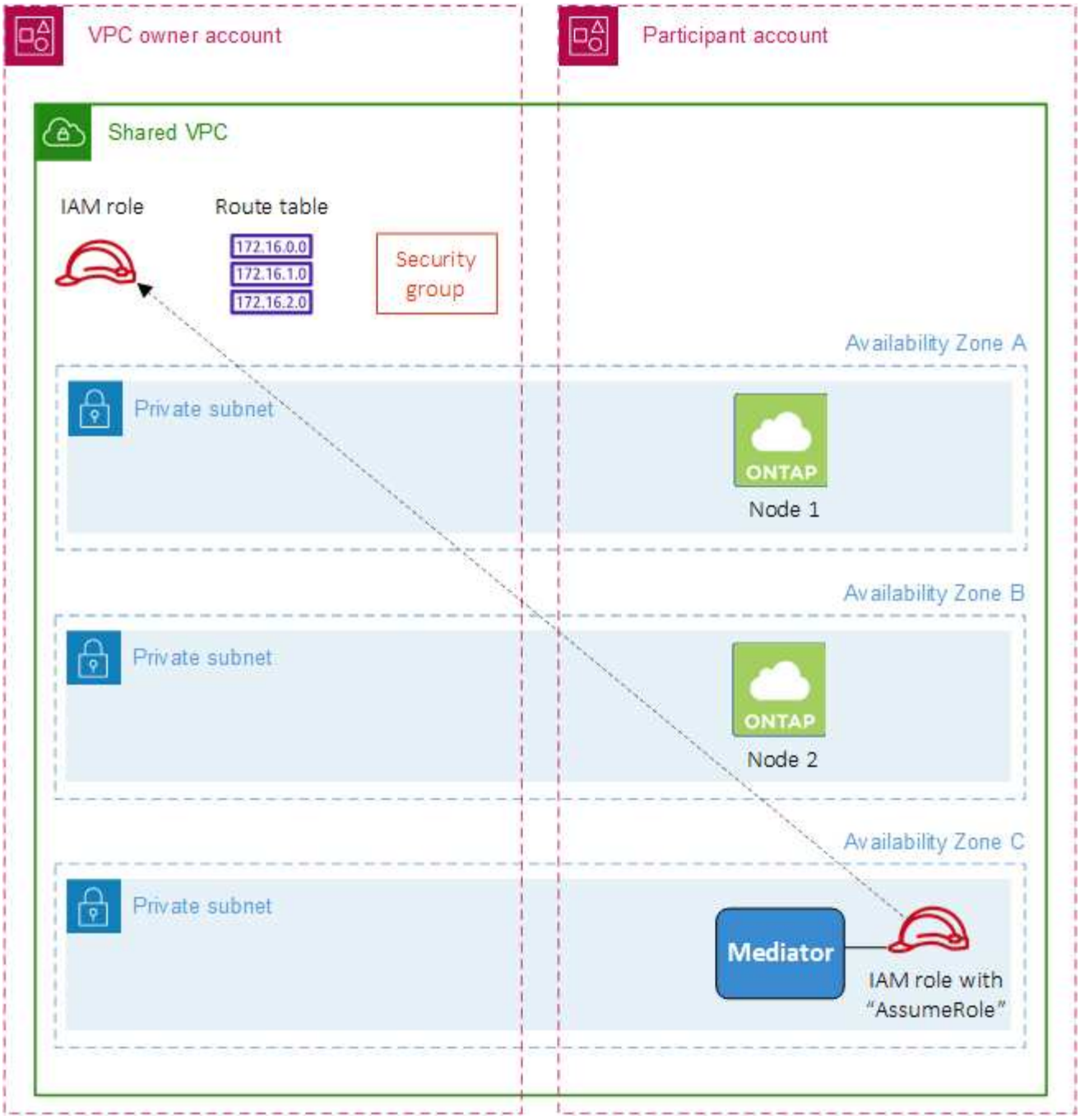
A partir del lanzamiento de la versión 9.11.1, se admiten los pares de alta disponibilidad de Cloud Volumes ONTAP en AWS con el uso compartido de VPC. El uso compartido de VPC permite a la organización compartir subredes con otras cuentas de AWS. Para utilizar esta configuración, debe configurar su entorno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

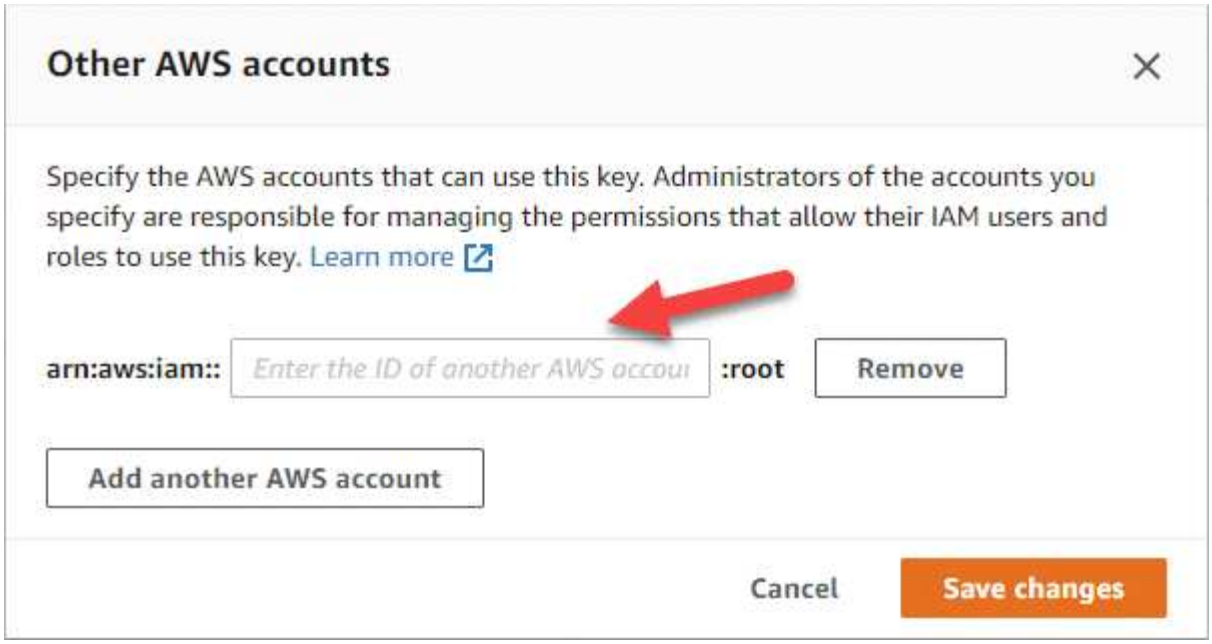
   b. Seleccione la tecla.

   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

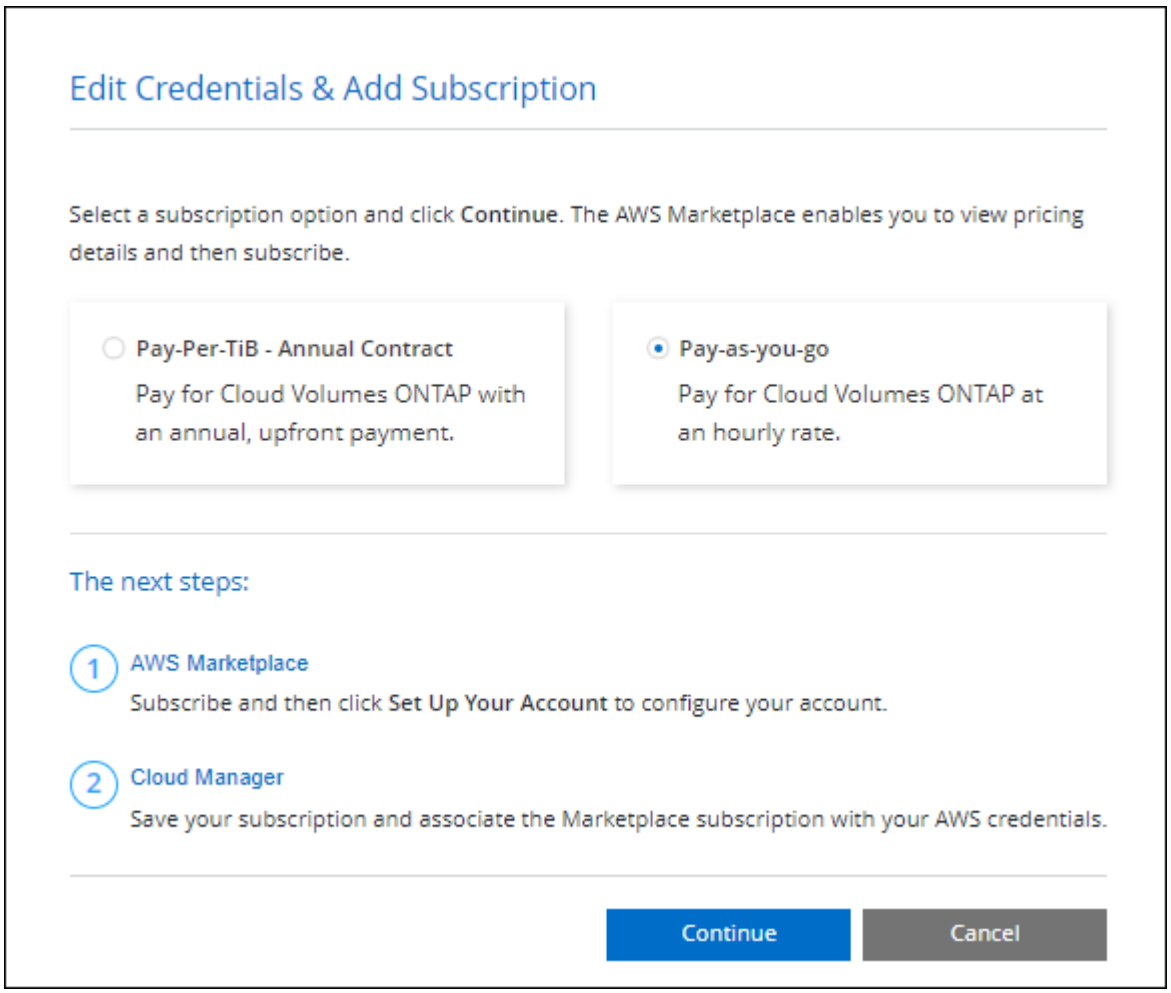
Seleccione la oferta freemium para utilizar Cloud Volumes ONTAP de forma gratuita con hasta 500 GIB de capacidad aprovisionada. "Obtenga más información sobre la oferta de Freemium".

Pasos

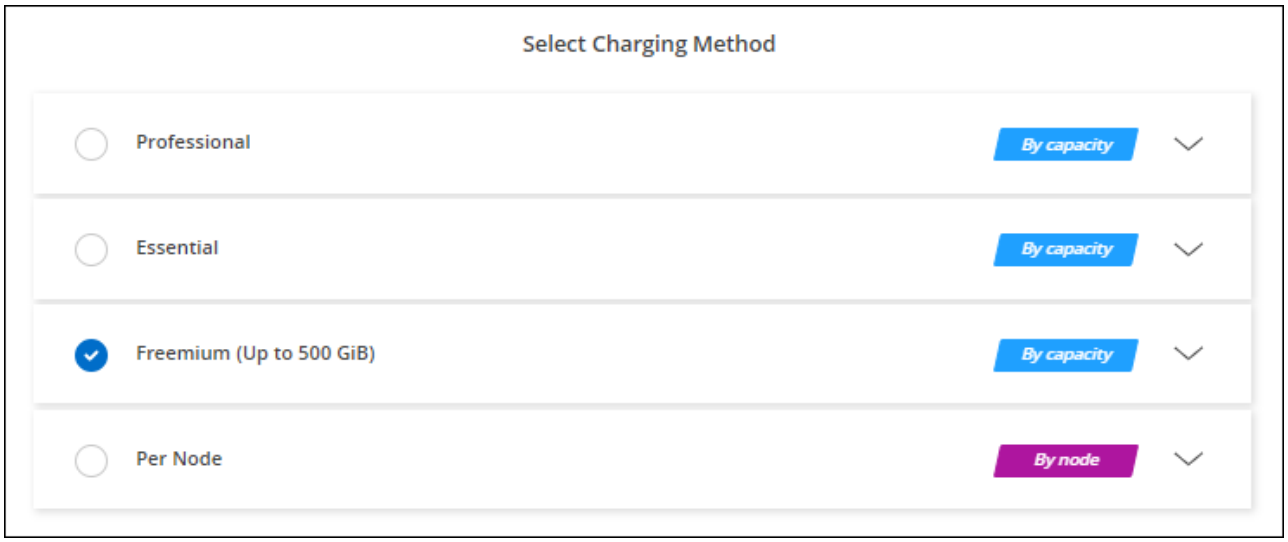
1. En el menú de navegación de la izquierda, selecciona **almacenamiento > Canvas**.
2. En la página Canvas, haga clic en **Agregar entorno de trabajo** y siga los pasos de BlueXP.

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"

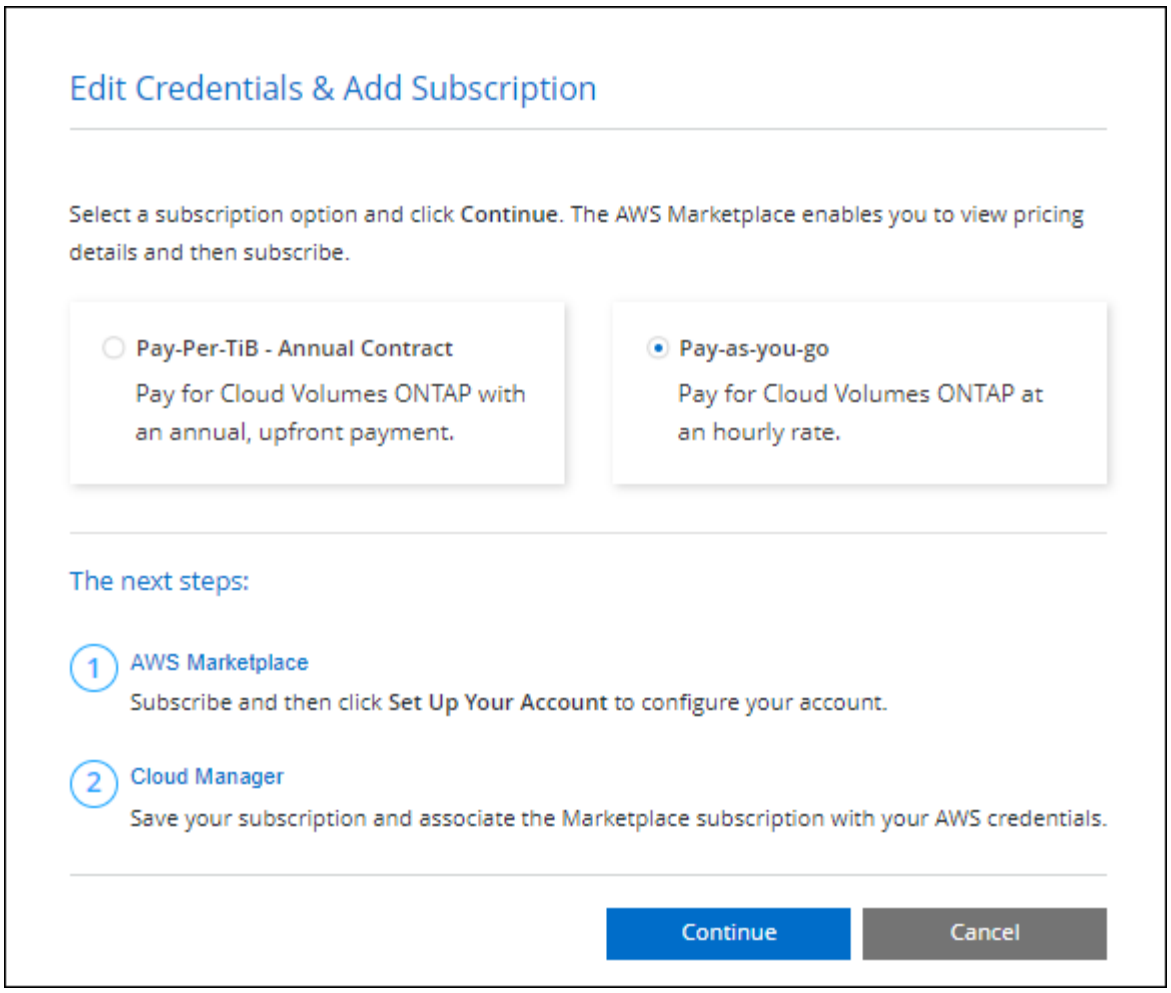
   BlueXP consulta automáticamente al servicio de licencias de NetApp para obtener detalles sobre las licencias asociadas a su cuenta del sitio de soporte de NetApp. Si no se producen errores, BlueXP añade automáticamente las licencias a la cartera digital.

   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".

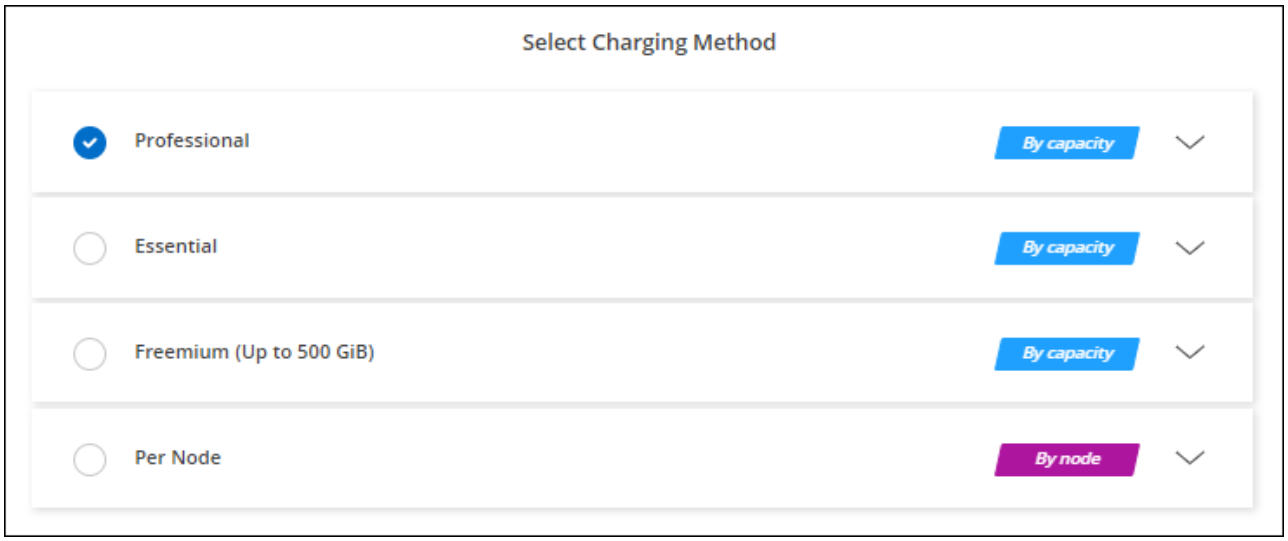
3. En la página Canvas, haga clic en **Agregar entorno de trabajo** y siga los pasos de BlueXP.

   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".

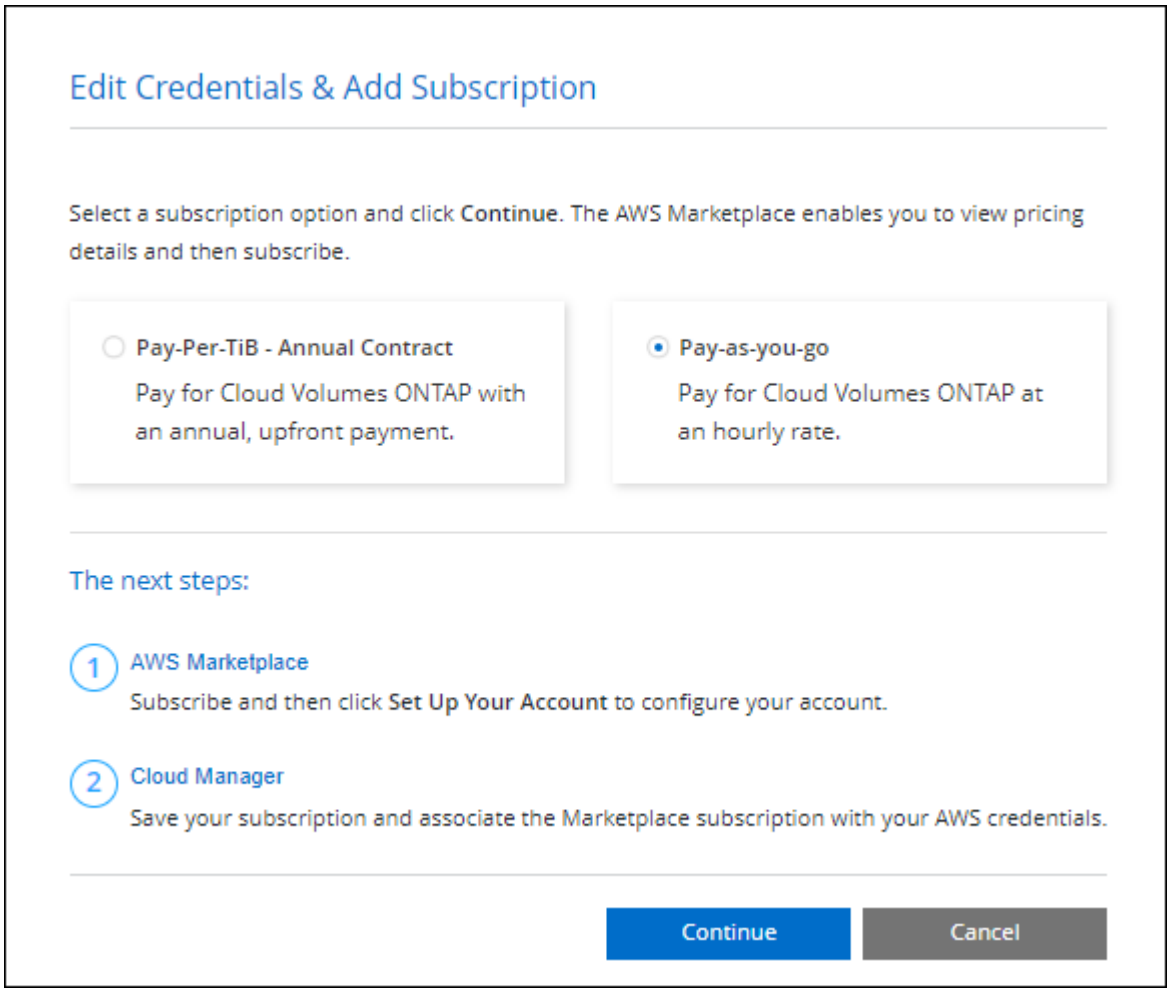
Suscripción a PAYGO

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

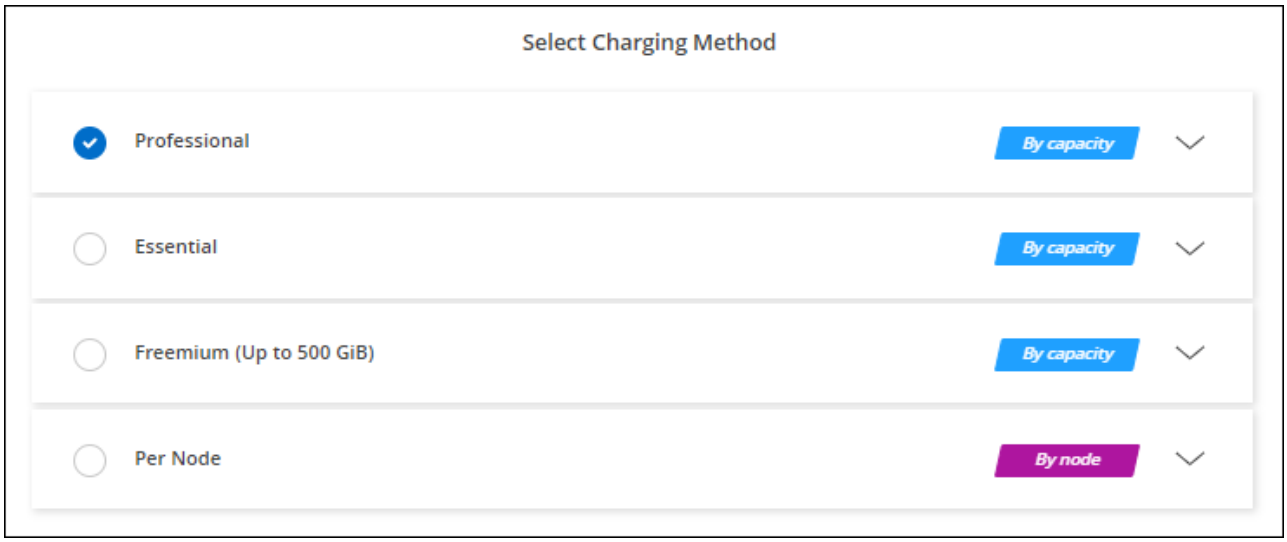
Al crear un entorno de trabajo de Cloud Volumes ONTAP, BlueXP le solicita que se suscriba al acuerdo que está disponible en AWS Marketplace. Esa suscripción se asocia entonces con el entorno de trabajo para la carga. Puede utilizar la misma suscripción para entornos de trabajo adicionales.

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"

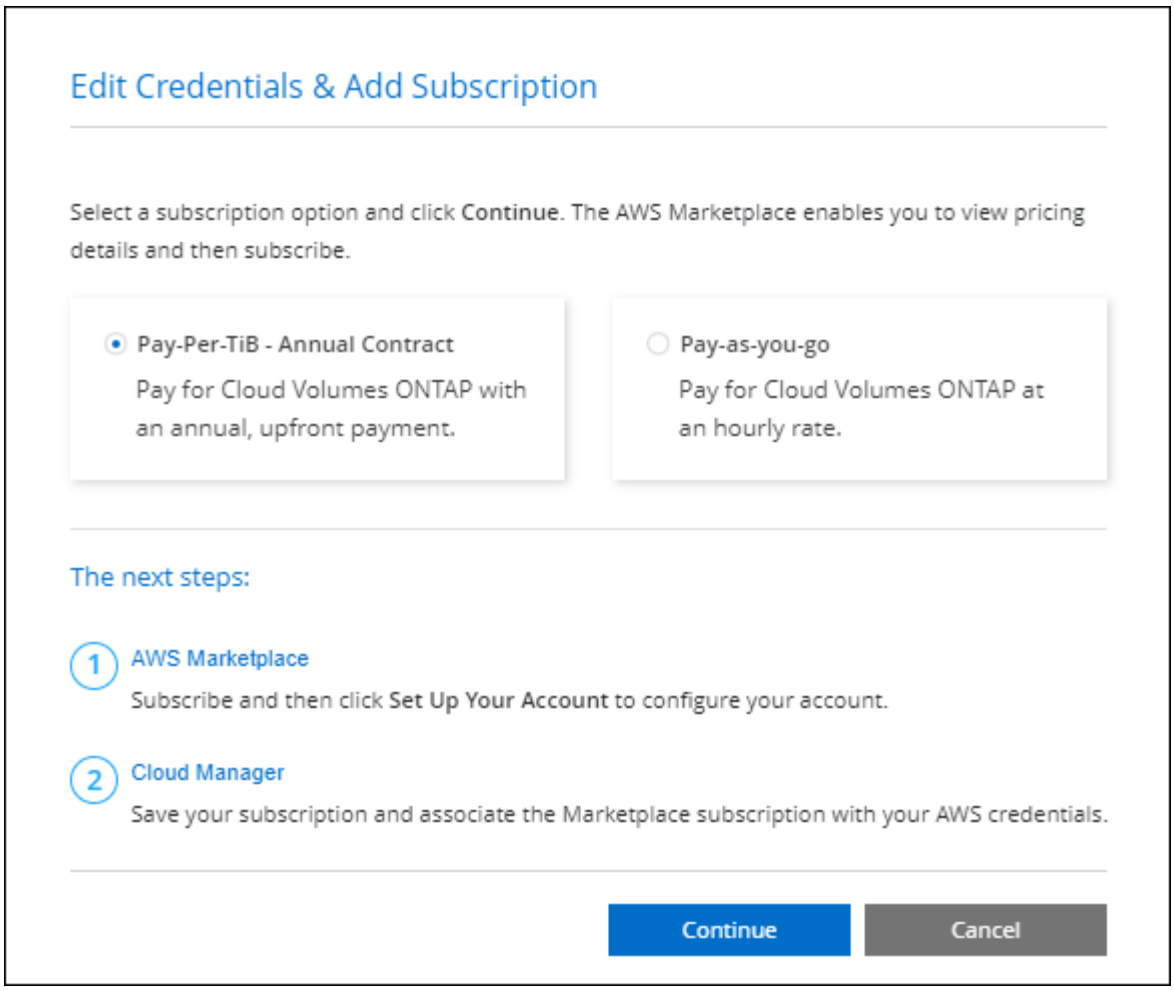
Contrato anual

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

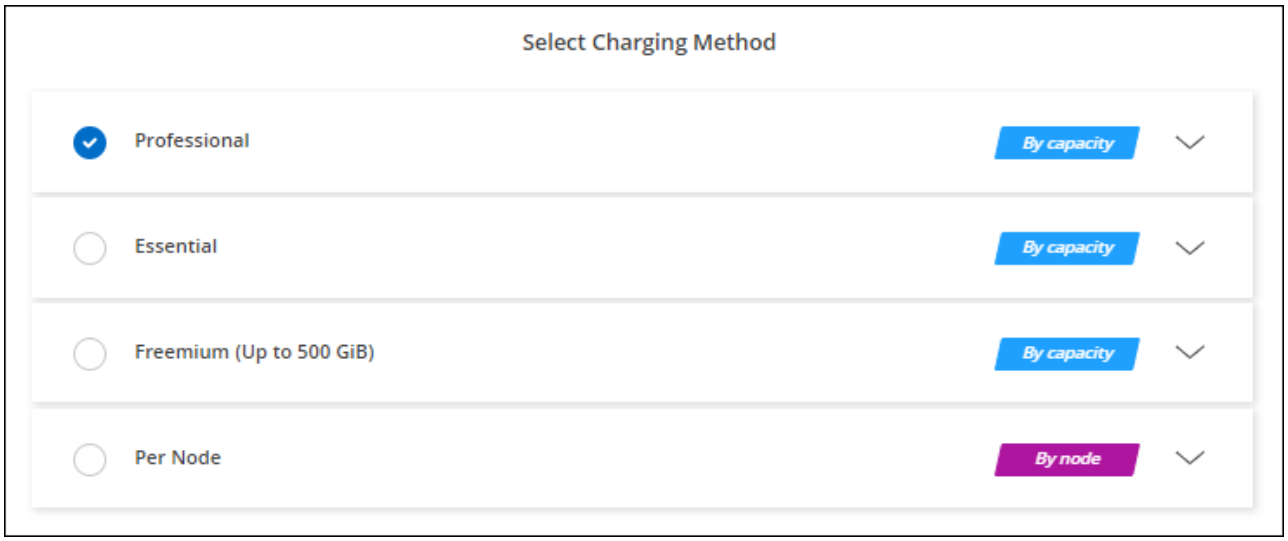
Al igual que una suscripción por horas, BlueXP solicita que se suscriba al contrato anual que está disponible en AWS Marketplace.

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.



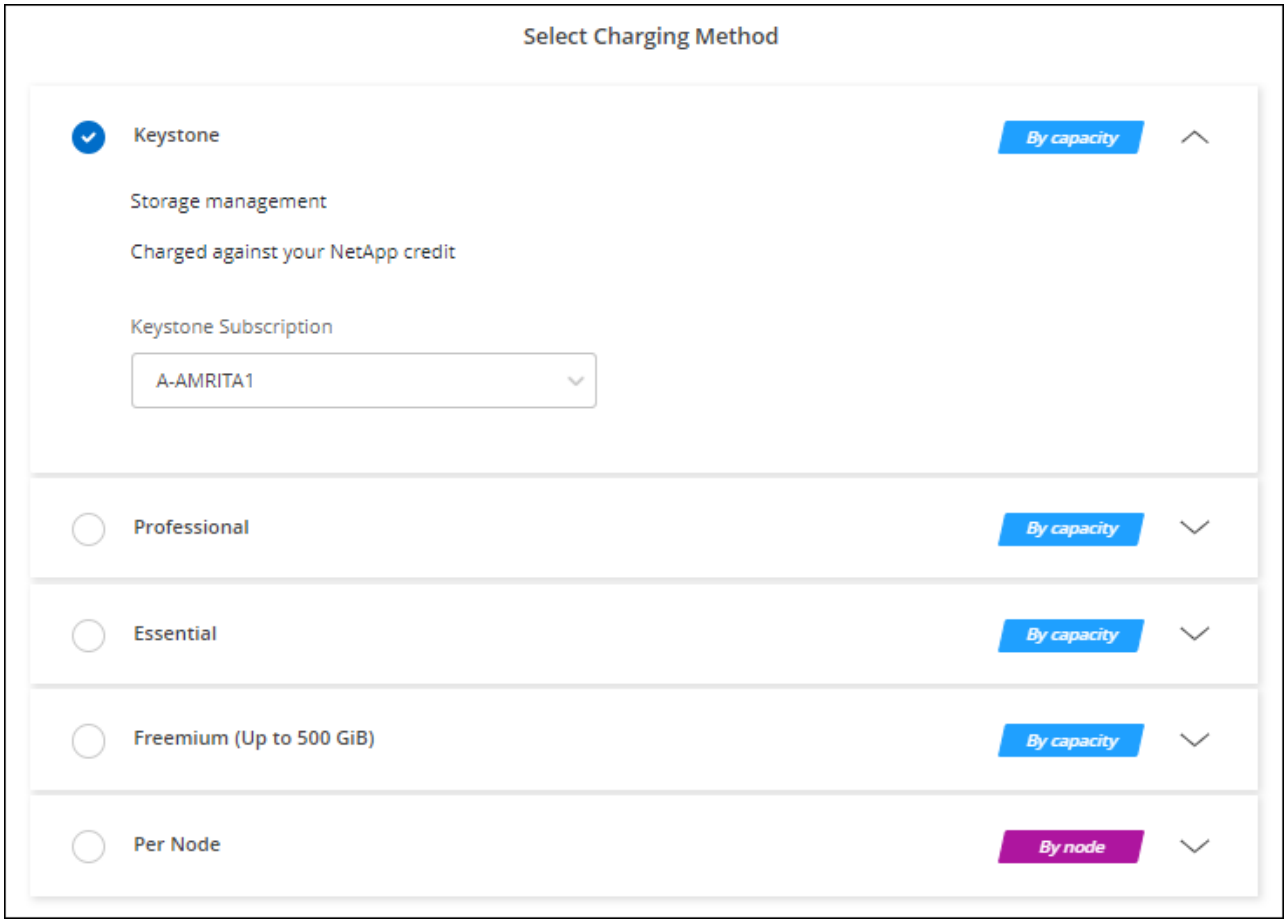
"Consulte instrucciones paso a paso para iniciar Cloud Volumes ONTAP en AWS".

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:

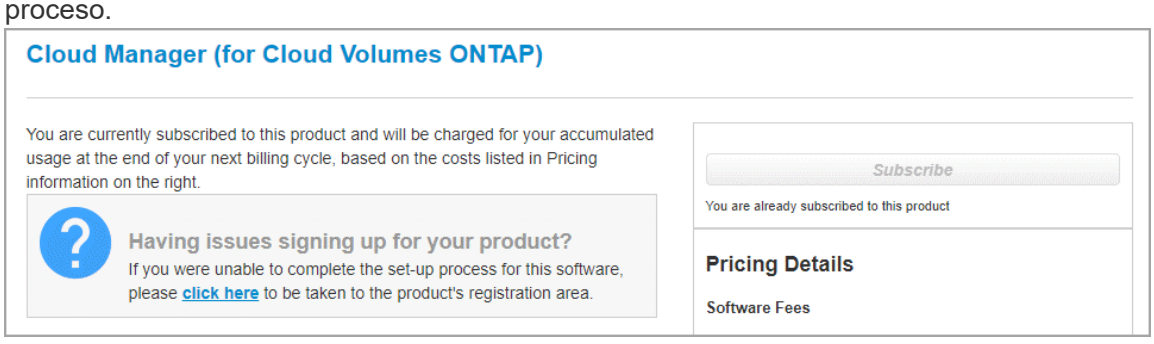
Campo	Descripción
Nombre del entorno de trabajo	BlueXP usa el nombre del entorno de trabajo para asignar un nombre tanto al sistema Cloud Volumes ONTAP como a la instancia de Amazon EC2. También utiliza el nombre como prefijo para el grupo de seguridad predefinido si selecciona esa opción.

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.

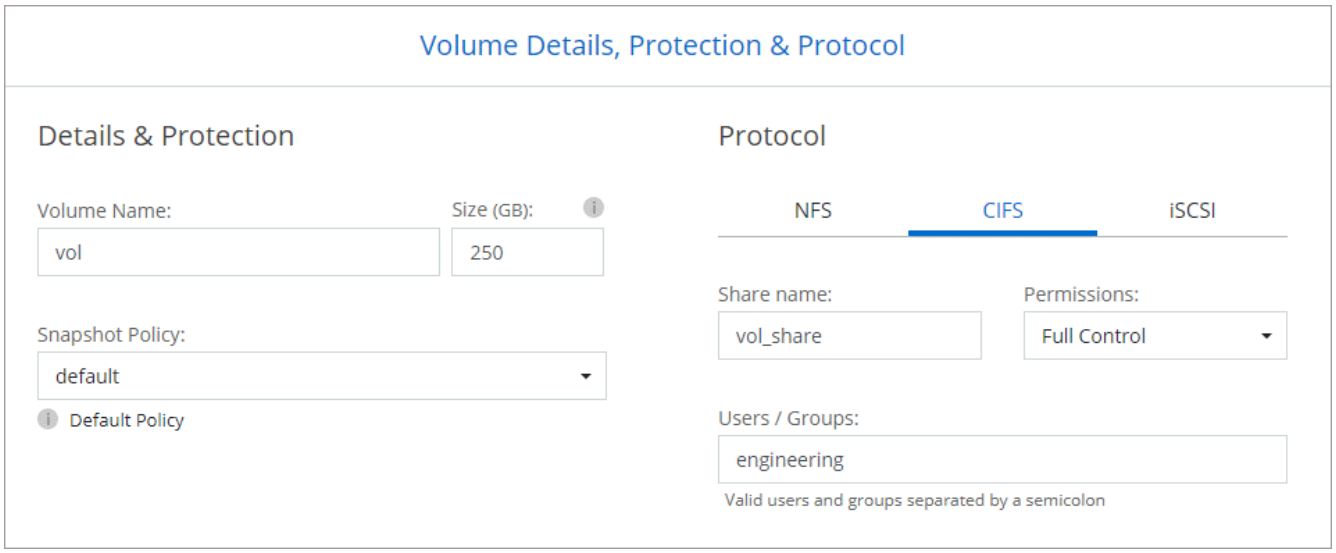
16. **Crear volumen**: Introduzca los detalles del nuevo volumen o haga clic en **Omitir**.

"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.

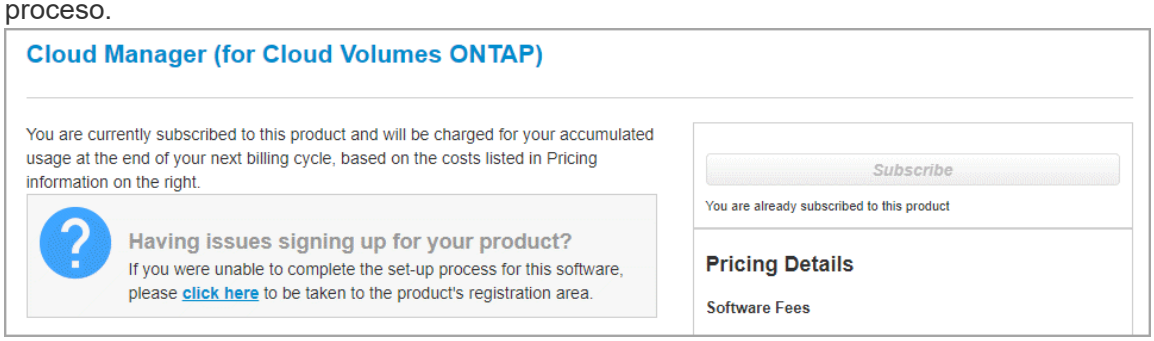
   Algunos de los campos en esta página son claros y explicativos. En la siguiente tabla se describen los campos que podrían presentar dificultades:

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.

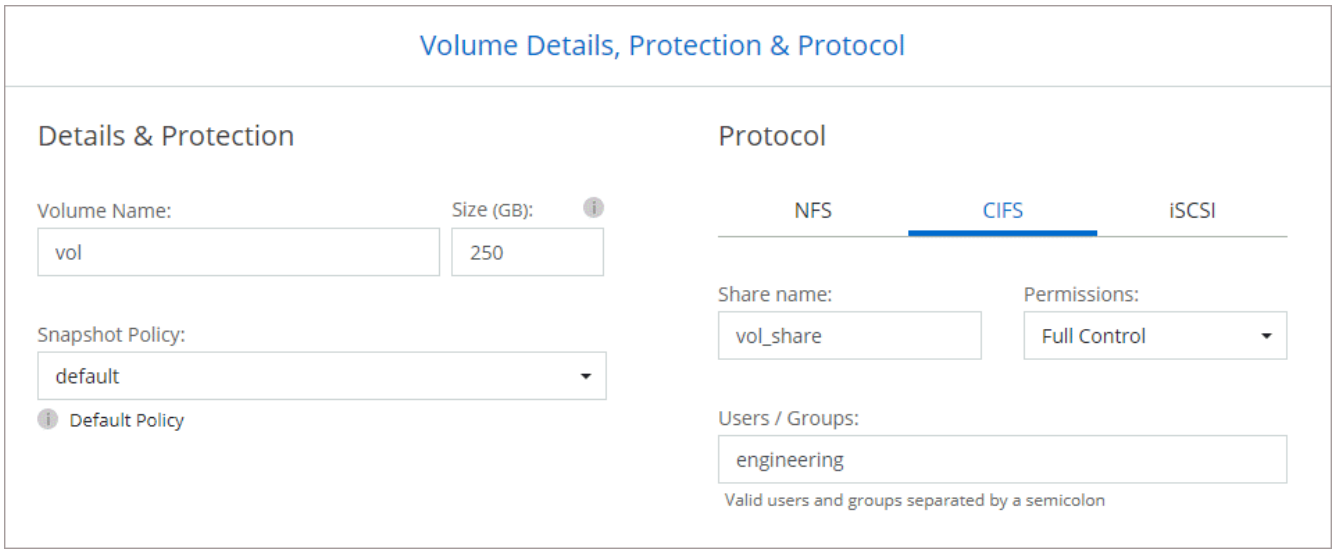
19. **Crear volumen**: Introduzca los detalles del nuevo volumen o haga clic en **Omitir**.

    "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>`

Empiece a usar Microsoft Azure

Inicio rápido para Cloud Volumes ONTAP en Azure

Empiece a usar Cloud Volumes ONTAP para Azure 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 Azure"

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 vnet 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.

"Obtenga más información sobre los requisitos de red".

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

- "Creación de un conector desde BlueXP"
- "Creación de un conector desde Azure Marketplace"
- "Instalar el software del conector en un host Linux"
- "Qué hace BlueXP con permisos"

Planifique la configuración de Cloud Volumes ONTAP en Azure

Al poner en marcha Cloud Volumes ONTAP en Azure, 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 es compatible en la mayoría de las regiones de Microsoft Azure. "Consulte la lista completa de las regiones admitidas".

Seleccione un tipo de máquina virtual admitido

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

"Configuraciones compatibles para Cloud Volumes ONTAP en Azure"

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 Azure"

Configure el tamaño de su sistema en Azure

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

Tipo de máquina virtual

Observe los tipos de máquina virtual admitidos en la "Notas de la versión de Cloud Volumes ONTAP" Y, a continuación, revise los detalles sobre cada tipo de máquina virtual admitido. Tenga en cuenta que cada tipo de máquina virtual admite un número específico de discos de datos.

- "Documentación de Azure: Tamaños de máquinas virtuales de uso general"
- "Documentación de Azure: Tamaños de máquinas virtuales optimizadas con memoria"

Tipo de disco de Azure con sistemas de nodo único

Cuando crea volúmenes para Cloud Volumes ONTAP, debe elegir el almacenamiento en cloud subyacente que Cloud Volumes ONTAP utiliza como disco.

Los sistemas de un solo nodo pueden usar tres tipos de discos gestionados de Azure:

- *Premium SSD Managed Disks* proporciona un alto rendimiento para cargas de trabajo con un gran volumen de I/o a un coste más elevado.
- *Standard SSD Managed Disks* proporciona un rendimiento constante para cargas de trabajo que requieren un bajo nivel de IOPS.
- *Standard HDD Managed Disks* es una buena opción si no necesita un alto nivel de IOPS y desea reducir sus costes.

Si quiere más información sobre los casos de uso de estos discos, consulte "Documentación de Microsoft Azure: ¿qué tipos de discos están disponibles en Azure?".

Tipo de disco de Azure con pares de alta disponibilidad

Los sistemas DE ALTA DISPONIBILIDAD utilizan discos gestionados compartidos SSD de Premium, que proporcionan un alto rendimiento para las cargas de trabajo con un gran volumen de I/o a un coste más elevado. Las implementaciones DE ALTA DISPONIBILIDAD creadas antes de la versión 9.12.1 utilizan Blobs de página Premium.

Tamaño de disco de Azure

Al iniciar las instancias de Cloud Volumes ONTAP, debe elegir el tamaño de disco predeterminado para los agregados. BlueXP usa este tamaño de disco para el agregado inicial y para cualquier agregado adicional que cree cuando utilice la opción de aprovisionamiento simple. Puede crear agregados con un tamaño de disco diferente desde el valor predeterminado por "mediante la opción de asignación avanzada".

Todos los discos de un agregado deben tener el mismo tamaño.

Al elegir un tamaño de disco, se deben tener en cuenta varios factores. El tamaño del disco afecta a la cantidad de almacenamiento que se paga, el tamaño de los volúmenes que se pueden crear en un agregado, la capacidad total disponible para Cloud Volumes ONTAP y el rendimiento del almacenamiento.

El rendimiento del almacenamiento Premium de Azure está ligado al tamaño del disco. Los discos más grandes permiten mejorar la tasa de IOPS y el rendimiento. Por ejemplo, al seleccionar discos de 1 TIB, se puede proporcionar un mejor rendimiento que con discos de 500 GIB, con un costo más alto.

No existen diferencias de rendimiento entre los tamaños de disco para Standard Storage. Debe elegir el tamaño del disco en función de la capacidad que necesite.

Consulte Azure para obtener información sobre IOPS y rendimiento por tamaño de disco:

- "Microsoft Azure: Precios de discos gestionados"
- "Microsoft Azure: Precios para Blobs de página"

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.

"Vea los discos predeterminados para los datos del sistema Cloud Volumes ONTAP en Azure".

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

Recopilar información de red

Al implementar Cloud Volumes ONTAP en Azure, tiene que especificar detalles acerca de su red virtual. Puede utilizar una hoja de cálculo para recopilar la información del administrador.

Información de Azure	Su valor
Región	
Red virtual (vnet)	
Subred	
Grupo de seguridad de red (si utiliza el suyo propio)	

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.

Requisitos de red para Cloud Volumes ONTAP en Azure

Configure sus redes de Azure para que los sistemas Cloud Volumes ONTAP funcionen correctamente.

Requisitos para Cloud Volumes ONTAP

Los siguientes requisitos de red deben satisfacerse en Azure.

Acceso a Internet de salida

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 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".

Direcciones IP

BlueXP asigna automáticamente el número requerido de direcciones IP privadas a Cloud Volumes ONTAP en Azure. Debe asegurarse de que la red tenga 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. Se requiere una LIF de gestión de SVM para herramientas de gestión como SnapCenter.

> Un LIF iSCSI proporciona acceso a los clientes a través del protocolo iSCSI y el sistema lo utiliza para otros flujos de trabajo de red importantes. Estos LIF son necesarios y no deben eliminarse.

Direcciones IP para un sistema de nodo único

BlueXP asigna direcciones IP 5 o 6 a un sistema de un solo nodo:

- IP de gestión del clúster
- IP de gestión de nodos
- IP de interconexión de clústeres para SnapMirror
- IP NFS/CIFS
- IP de iSCSI

> El IP de iSCSI proporciona acceso de cliente a través del protocolo iSCSI. El sistema también lo utiliza para otros flujos de trabajo importantes de redes. Este LIF es necesario y no debe eliminarse.

- Gestión de SVM (opcional: No configurado de forma predeterminada)

Direcciones IP para pares de alta disponibilidad

BlueXP asigna direcciones IP a 4 NIC (por nodo) durante la implementación.

Tenga en cuenta que BlueXP crea una LIF de gestión de SVM en parejas de alta disponibilidad, pero no en sistemas de un único nodo en Azure.

NIC0

- IP de gestión de nodos
- IP de interconexión de clústeres
- IP de iSCSI

> El IP de iSCSI proporciona acceso de cliente a través del protocolo iSCSI. El sistema también lo utiliza para otros flujos de trabajo importantes de redes. Este LIF es necesario y no debe eliminarse.

NIC1

- La IP de red del clúster

NIC2

- IP de interconexión de clúster (IC de alta disponibilidad)

NIC3

- IP de NIC Pageblob (acceso al disco)

> NIC3 solo se aplica a implementaciones de alta disponibilidad que usan almacenamiento BLOB de página.

Las direcciones IP anteriores no migran en eventos de conmutación al nodo de respaldo.

Además, 4 IP de interfaz (FIPS) están configuradas para migrar eventos de conmutación por error. Estas IP de front-end residen en el equilibrador de carga.

- IP de gestión del clúster
- IP de datos NODEA (NFS/CIFS)
- IP de datos de NodeB (NFS/CIFS)
- La IP de gestión de SVM

Conexiones seguras con servicios de Azure

De forma predeterminada, BlueXP habilita un vínculo privado de Azure para las conexiones entre las cuentas de almacenamiento BLOB de Cloud Volumes ONTAP y Azure.

En la mayoría de los casos, no hay nada que hacer: BlueXP gestiona el vínculo privado de Azure para usted. Pero si utiliza DNS privado de Azure, tendrá que editar un archivo de configuración. También debe estar al tanto de un requisito para la ubicación del conector en Azure.

También puede desactivar la conexión de enlace privado, si así lo requieren las necesidades de su empresa. Si deshabilita el vínculo, BlueXP configura Cloud Volumes ONTAP para que use un extremo de servicio en su lugar.

"Obtenga más información sobre el uso de enlaces privados de Azure o extremos de servicio con Cloud Volumes ONTAP".

Conexiones con otros sistemas ONTAP

Para replicar datos entre un sistema Cloud Volumes ONTAP en Azure y sistemas ONTAP en otras redes, debe tener una conexión VPN entre la red virtual de Azure y la otra red, por ejemplo, la red corporativa.

Para obtener instrucciones, consulte "Documentación de Microsoft Azure: Cree una conexión de sitio a sitio en el portal de Azure".

Puerto para la interconexión de alta disponibilidad

Un par de alta disponibilidad de Cloud Volumes ONTAP incluye una interconexión de alta disponibilidad, que permite a cada nodo comprobar continuamente si su compañero está funcionando y reflejar los datos de registro de la memoria no volátil del otro. La interconexión de alta disponibilidad utiliza el puerto TCP 10006 para la comunicación.

De forma predeterminada, la comunicación entre los LIF ha Interconnect es abierta y no hay reglas de grupos de seguridad para este puerto. Sin embargo, si crea un firewall entre los LIF de interconexión de alta disponibilidad, tiene que asegurarse de que el tráfico TCP esté abierto para el puerto 10006 de modo que el par de alta disponibilidad pueda funcionar correctamente.

Solo un par de alta disponibilidad en un grupo de recursos de Azure

Debe utilizar un grupo de recursos *dedicado* para cada par de alta disponibilidad de Cloud Volumes ONTAP que implemente en Azure. Solo se admite un par de alta disponibilidad en un grupo de recursos.

BlueXP experimenta problemas de conexión si intenta implementar un segundo par de alta disponibilidad de Cloud Volumes ONTAP en un grupo de recursos de Azure.

Reglas de grupo de seguridad

BlueXP crea grupos de seguridad de Azure 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.

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

¿Busca información sobre el conector? "Ver reglas de grupo de seguridad para el conector"

Reglas de entrada para sistemas de un solo nodo

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:

- **Sólo vnet seleccionado**: El origen del tráfico entrante es el rango de subred del vnet para el sistema Cloud Volumes ONTAP y el rango de subred del vnet donde reside el conector. Esta es la opción recomendada.
- **All VNets**: La fuente de tráfico entrante es el rango IP 0.0.0.0/0.

Prioridad y nombre	Puerto y protocolo	Origen y destino	Descripción
1000 inbound_ssh	22 TCP	De cualquiera a cualquiera	Acceso SSH a la dirección IP de administración del clúster LIF o una LIF de gestión de nodos
1001 inbound_http	80 TCP	De cualquiera a cualquiera	Acceso HTTP a la consola web de System Manager mediante el La dirección IP de la LIF de gestión del clúster
1002 inbound_111_tcp	111 TCP	De cualquiera a cualquiera	Llamada a procedimiento remoto para NFS
1003 inbound_111_udp	111 UDP	De cualquiera a cualquiera	Llamada a procedimiento remoto para NFS
1004 inbound_139	139 TCP	De cualquiera a cualquiera	Sesión de servicio NetBIOS para CIFS
1005 inbound_161-162 _tcp	161-162 TCP	De cualquiera a cualquiera	Protocolo simple de gestión de red
1006 inbound_161-162 _udp	161-162 UDP	De cualquiera a cualquiera	Protocolo simple de gestión de red

Prioridad y nombre	Puerto y protocolo	Origen y destino	Descripción
1007 inbound_443	443 TCP	De cualquiera a cualquiera	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
1008 inbound_445	445 TCP	De cualquiera a cualquiera	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
1009 inbound_635_tcp	635 TCP	De cualquiera a cualquiera	Montaje NFS
1010 inbound_635_udp	635 UDP	De cualquiera a cualquiera	Montaje NFS
1011 inbound_749	749 TCP	De cualquiera a cualquiera	Kerberos
1012 inbound_2049_tcp	2049 TCP	De cualquiera a cualquiera	Daemon del servidor NFS
1013 inbound_2049_udp	2049 UDP	De cualquiera a cualquiera	Daemon del servidor NFS
1014 inbound_3260	3260 TCP	De cualquiera a cualquiera	Acceso iSCSI mediante la LIF de datos iSCSI
1015 inbound_4045-4046_tcp	4045-4046 TCP	De cualquiera a cualquiera	Daemon de bloqueo NFS y monitor de estado de red
1016 inbound_4045-4046_udp	4045-4046 UDP	De cualquiera a cualquiera	Daemon de bloqueo NFS y monitor de estado de red
1017 inbound_10000	10000 TCP	De cualquiera a cualquiera	Backup con NDMP
1018 inbound_11104-11105	11104-11105 TCP	De cualquiera a cualquiera	Transferencia de datos de SnapMirror
3000 inbound_deny _all_tcp	Cualquier puerto TCP	De cualquiera a cualquiera	Bloquear el resto del tráfico entrante TCP
3001 inbound_deny _all_udp	Cualquier puerto UDP	De cualquiera a cualquiera	Bloquee el resto del tráfico de entrada UDP
65000 AllowVnetInBound	Cualquier protocolo	VirtualNetwork para VirtualNetwork	Tráfico entrante desde dentro del vnet
65001 AllowAzureLoad Balance InBound	Cualquier protocolo	AzureLoadBalancer a cualquiera	Tráfico de datos del balanceador de carga estándar de Azure
65500 DenyAllInBound	Cualquier protocolo	De cualquiera a cualquiera	Bloquear el resto del tráfico entrante

Reglas de entrada para sistemas de alta disponibilidad

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:

- **Sólo vnet seleccionado**: El origen del tráfico entrante es el rango de subred del vnet para el sistema Cloud Volumes ONTAP y el rango de subred del vnet donde reside el conector. Esta es la opción recomendada.
- **All VNets**: La fuente de tráfico entrante es el rango IP 0.0.0.0/0.

> Los sistemas de ALTA DISPONIBILIDAD tienen menos reglas entrantes que los sistemas de un solo nodo, porque el tráfico de datos entrantes pasa por el balanceador de carga estándar de Azure. Debido a esto, el tráfico del equilibrador de carga debe estar abierto, como se muestra en la regla "AllowAzureLoadBalance InBound".

Prioridad y nombre	Puerto y protocolo	Origen y destino	Descripción
100 inbound_443	443 cualquier protocolo	De cualquiera a cualquiera	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
101 inbound_111_tcp	111 cualquier protocolo	De cualquiera a cualquiera	Llamada a procedimiento remoto para NFS
102 inbound_2049_tcp	2049 cualquier protocolo	De cualquiera a cualquiera	Daemon del servidor NFS
111 inbound_ssh	22 cualquier protocolo	De cualquiera a cualquiera	Acceso SSH a la dirección IP de administración del clúster LIF o una LIF de gestión de nodos
121 inbound_53	53 cualquier protocolo	De cualquiera a cualquiera	DNS y CIFS
65000 AllowVnetInBound	Cualquier protocolo	VirtualNetwork para VirtualNetwork	Tráfico entrante desde dentro del vnet
65001 AllowAzureLoad Balance InBound	Cualquier protocolo	AzureLoadBalancer a cualquiera	Tráfico de datos del balanceador de carga estándar de Azure
65500 DenyAllInBound	Cualquier protocolo	De cualquiera a cualquiera	Bloquear el resto del tráfico entrante

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.

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

Servicio	Puerto	Protocolo	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
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	68	UDP	LIF de gestión de nodos	DHCP	Cliente DHCP para la configuración inicial
DHCPS	67	UDP	LIF de gestión de nodos	DHCP	Servidor DHCP
DNS	53	UDP	LIF de gestión de nodos y LIF de datos (NFS, CIFS)	DNS	DNS
NDMP	18600–18699	TCP	LIF de gestión de nodos	Servidores de destino	Copia NDMP
SMTP	25	TCP	LIF de gestión de nodos	Servidor de correo	Alertas SMTP, que se pueden utilizar para AutoSupport
SNMP	161	TCP	LIF de gestión de nodos	Servidor de supervisión	Supervisión mediante capturas SNMP
	161	UDP	LIF de gestión de nodos	Servidor de supervisión	Supervisión mediante capturas SNMP
	162	TCP	LIF de gestión de nodos	Servidor de supervisión	Supervisión mediante capturas SNMP
	162	UDP	LIF de gestión de nodos	Servidor de supervisión	Supervisión mediante capturas SNMP
SnapMirror	11104	TCP	LIF entre clústeres	LIF de interconexión de clústeres de ONTAP	Gestión de sesiones de comunicación de interconexión de clústeres para SnapMirror
	11105	TCP	LIF entre clústeres	LIF de interconexión de clústeres de ONTAP	Transferencia de datos de SnapMirror
Syslog	514	UDP	LIF de gestión de nodos	Servidor de syslog	Mensajes de syslog Reenviar

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 de grupos de seguridad en Azure"

Configure Cloud Volumes ONTAP para utilizar una clave gestionada por el cliente en Azure

Los datos se cifran automáticamente en Cloud Volumes ONTAP, en Azure mediante "Cifrado del servicio de almacenamiento de Azure" Con una clave gestionada por Microsoft. Pero puede utilizar su propia clave de cifrado siguiendo los pasos de esta página.

Información general de cifrado de datos

Los datos de Cloud Volumes ONTAP se cifran automáticamente en Azure mediante "Cifrado del servicio de almacenamiento de Azure". La implementación predeterminada utiliza una clave administrada por Microsoft. No se requiere configuración.

Si desea utilizar una clave gestionada por el cliente con Cloud Volumes ONTAP, debe realizar los siguientes pasos:

1. Desde Azure, cree un almacén de claves y, a continuación, genere una clave en ese almacén
2. Desde BlueXP, utilice la API para crear un entorno de trabajo de Cloud Volumes ONTAP que utilice la clave

Rotación de la clave

Si crea una nueva versión de la clave, Cloud Volumes ONTAP utiliza automáticamente la última versión de la clave.

Cómo se cifran los datos

BlueXP utiliza un conjunto de cifrado de disco, que permite la gestión de claves de cifrado con discos gestionados no con blobs de página. Todos los discos de datos nuevos también utilizan el mismo conjunto de cifrado de disco. Las versiones inferiores utilizarán la clave gestionada por Microsoft en lugar de la clave gestionada por el cliente.

Después de crear un entorno de trabajo de Cloud Volumes ONTAP configurado para utilizar una clave gestionada por el cliente, los datos de Cloud Volumes ONTAP se cifran de la siguiente manera.

Configuración de Cloud Volumes ONTAP	Discos del sistema utilizados para el cifrado de claves	Discos de datos utilizados para el cifrado de claves
Un solo nodo	• Arranque • Núcleo • NVRAM	• Raíz • SQL Server

Configuración de Cloud Volumes ONTAP	Discos del sistema utilizados para el cifrado de claves	Discos de datos utilizados para el cifrado de claves
Zona de disponibilidad única de Azure HA con blobs de página	• Arranque • Núcleo • NVRAM	Ninguno
Zona de disponibilidad única de Azure HA con discos gestionados compartidos	• Arranque • Núcleo • NVRAM	• Raíz • SQL Server
Azure HA Varias zonas de disponibilidad con discos gestionados compartidos	• Arranque • Núcleo • NVRAM	• Raíz • SQL Server

Todas las cuentas de almacenamiento de Azure para Cloud Volumes ONTAP se cifran con una clave gestionada por los clientes. Si desea cifrar sus cuentas de almacenamiento durante su creación, debe crear y proporcionar el ID del recurso en la solicitud de creación de CVO. Esto se aplica a todo tipo de puesta en marcha. Si no lo proporciona, las cuentas de almacenamiento seguirán estando cifradas, pero BlueXP creará primero las cuentas de almacenamiento con el cifrado de claves gestionado por Microsoft y, a continuación, actualizará las cuentas de almacenamiento para que utilicen la clave gestionada por el cliente.

Crear una identidad gestionada asignada por el usuario

Tiene la opción de crear un recurso denominado identidad gestionada asignada por el usuario. Esto le permite cifrar sus cuentas de almacenamiento cuando crea un entorno de trabajo de Cloud Volumes ONTAP. Recomendamos crear este recurso antes de crear un almacén de claves y generar una clave.

El recurso tiene el siguiente identificador: `userassignedidentity`.

Pasos

1. En Azure, vaya a Servicios de Azure y seleccione **Identidades administradas**.
2. Haga clic en **Crear**.
3. Proporcione los siguientes detalles:
   - **Suscripción**: Elige una suscripción. Recomendamos elegir la misma suscripción que la suscripción a Connector.
   - **Grupo de recursos**: Usa un grupo de recursos existente o crea uno nuevo.
   - **Región**: Opcionalmente, seleccione la misma región que el Conector.
   - **Nombre**: Introduzca un nombre para el recurso.
4. Opcionalmente, agregue etiquetas.
5. Haga clic en **Crear**.

Cree un almacén de claves y genere una clave

El almacén de claves debe residir en la misma suscripción a Azure y la misma región en la que esté previsto crear el sistema Cloud Volumes ONTAP.

Si usted se ha creado una identidad gestionada asignada por el usuario, al crear el almacén de claves, también debe crear una política de acceso para el almacén de claves.

Pasos

1. "Cree un almacén de claves en su suscripción a Azure".

   Tenga en cuenta los siguientes requisitos para el almacén de claves:

   - El almacén de claves debe residir en la misma región que el sistema Cloud Volumes ONTAP.
   - Deben habilitarse las siguientes opciones:
     - **Borrado suave** (esta opción está activada de forma predeterminada, pero debe *no* estar desactivada)
     - **Protección de purga**
     - **Cifrado de disco de Azure para cifrado de volúmenes** (para sistemas de un solo nodo o pares de alta disponibilidad en varias zonas)
   - Se debe activar la siguiente opción si ha creado una identidad gestionada asignada por el usuario:
     - **Política de acceso a Vault**
2. Si seleccionó Política de acceso al almacén, haga clic en Crear para crear una política de acceso para el almacén de claves. Si no es así, vaya al paso 3.
   a. Seleccione los siguientes permisos:
      - obtenga
      - lista
      - descifrar
      - cifrar
      - tecla desajustar
      - tecla ajustar
      - verificación
      - firma
   b. Seleccione la identidad administrada (recurso) asignada por el usuario como principal.
   c. Revise y cree la política de acceso.
3. "Genere una clave en el almacén de claves".

   Tenga en cuenta los siguientes requisitos para la clave:

   - El tipo de clave debe ser **RSA**.
   - El tamaño de clave RSA recomendado es **2048**, pero se admiten otros tamaños.

Cree un entorno de trabajo que utilice la clave de cifrado

Después de crear el almacén de claves y generar una clave de cifrado, puede crear un nuevo sistema Cloud Volumes ONTAP configurado para utilizar la clave. Estos pasos son compatibles con la API de BlueXP.

Permisos necesarios

Si desea utilizar una clave gestionada por el cliente con un sistema Cloud Volumes ONTAP de un solo nodo, asegúrese de que el conector BlueXP tiene los siguientes permisos:

```
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/diskEncryptionSets/write",
"Microsoft.Compute/diskEncryptionSets/delete"
"Microsoft.KeyVault/vaults/deploy/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
```

"Consulte la lista más reciente de permisos"

Pasos

1. Obtenga la lista de almacenes de claves de su suscripción a Azure mediante la siguiente llamada a la API de BlueXP.

   En el caso de un par de alta disponibilidad: `GET /azure/ha/metadata/vaults`

   Para un solo nodo: `GET /azure/vsa/metadata/vaults`

   Tome nota de los **nombre** y **ResourceGroup**. Tendrá que especificar esos valores en el paso siguiente.

   "Obtenga más información acerca de esta llamada API".

2. Obtenga la lista de claves dentro del almacén mediante la siguiente llamada a la API de BlueXP.

   En el caso de un par de alta disponibilidad: `GET /azure/ha/metadata/keys-vault`

   Para un solo nodo: `GET /azure/vsa/metadata/keys-vault`

   Tome nota del **KeyName**. Tendrá que especificar ese valor (junto con el nombre del almacén) en el siguiente paso.

   "Obtenga más información acerca de esta llamada API".

3. Cree un sistema Cloud Volumes ONTAP mediante la siguiente llamada a la API de BlueXP.

   a. En el caso de un par de alta disponibilidad:

      `POST /azure/ha/working-environments`

      El cuerpo de la solicitud debe incluir los siguientes campos:

      ```
      "azureEncryptionParameters": {
                    "key": "keyName",
                    "vaultName": "vaultName"
      }
      ```

      Incluya el `"userAssignedIdentity": " userAssignedIdentityId"` si ha creado este recurso para utilizarlo para el cifrado de cuentas de almacenamiento.

"Obtenga más información acerca de esta llamada API".

b. Para un sistema de un solo nodo:

```
POST /azure/vsa/working-environments
```

El cuerpo de la solicitud debe incluir los siguientes campos:

```
"azureEncryptionParameters": {
                "key": "keyName",
                "vaultName": "vaultName"
}
```

Incluya el `"userAssignedIdentity": " userAssignedIdentityId"` si ha creado este recurso para utilizarlo para el cifrado de cuentas de almacenamiento.

"Obtenga más información acerca de esta llamada API".

Resultado

Tiene un nuevo sistema Cloud Volumes ONTAP configurado para usar su clave gestionada por el cliente para el cifrado de datos.

Configure las licencias para Cloud Volumes ONTAP en Azure

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

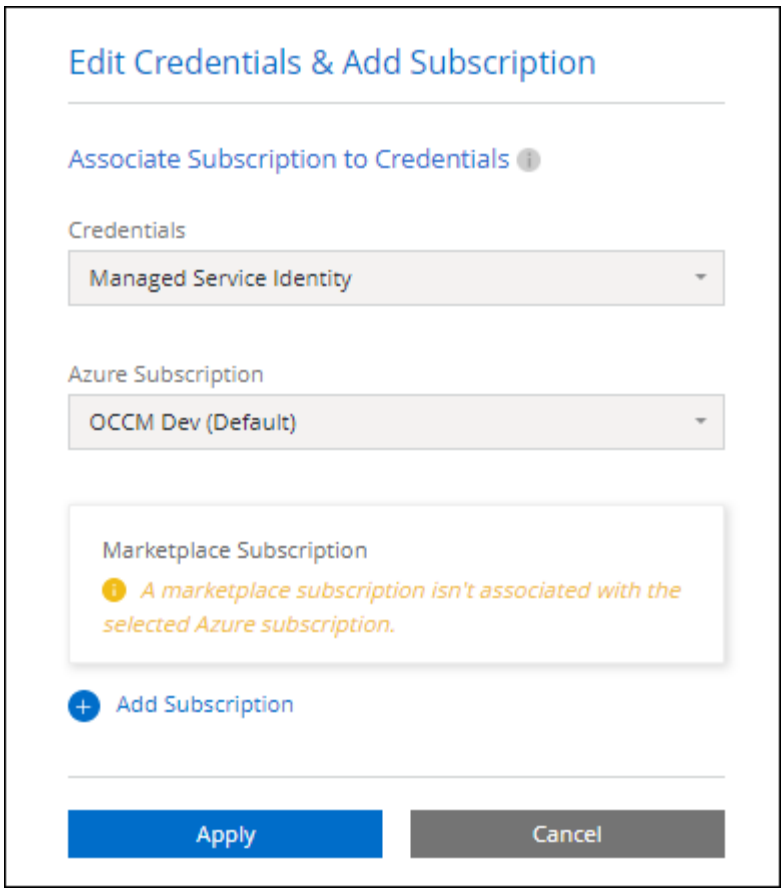
Seleccione la oferta freemium para utilizar Cloud Volumes ONTAP de forma gratuita con hasta 500 GIB de capacidad aprovisionada. "Obtenga más información sobre la oferta de Freemium".

Pasos

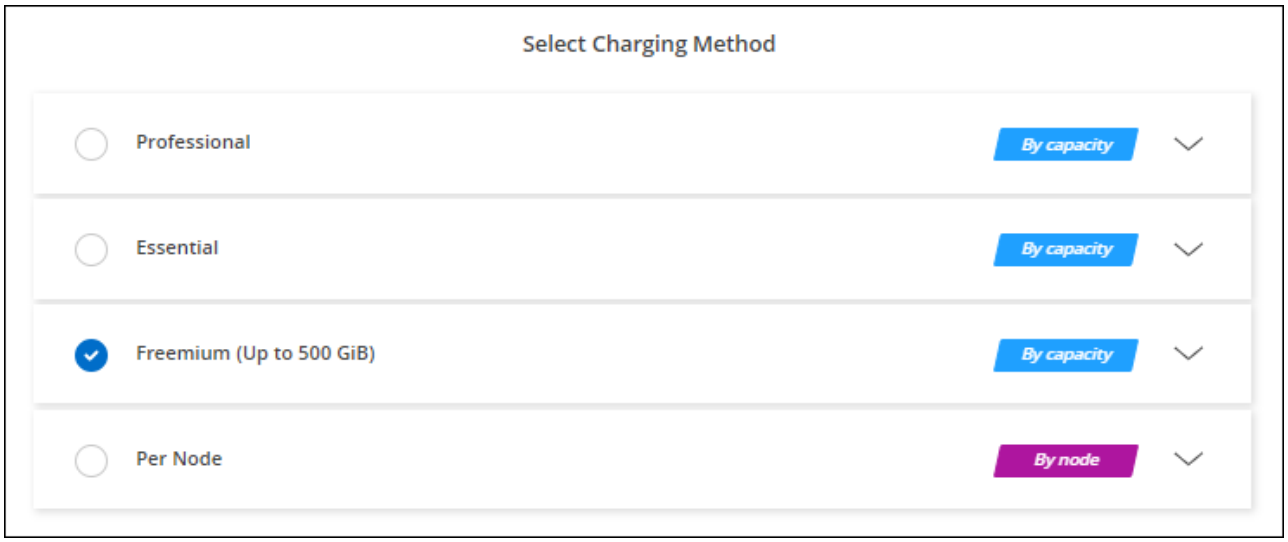
1. En el menú de navegación de la izquierda, selecciona **almacenamiento > Canvas**.
2. En la página Canvas, haga clic en **Agregar entorno de trabajo** y siga los pasos de BlueXP.

   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 Azure Marketplace.

   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 Azure".

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 Azure Marketplace
- Un contrato anual

"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"

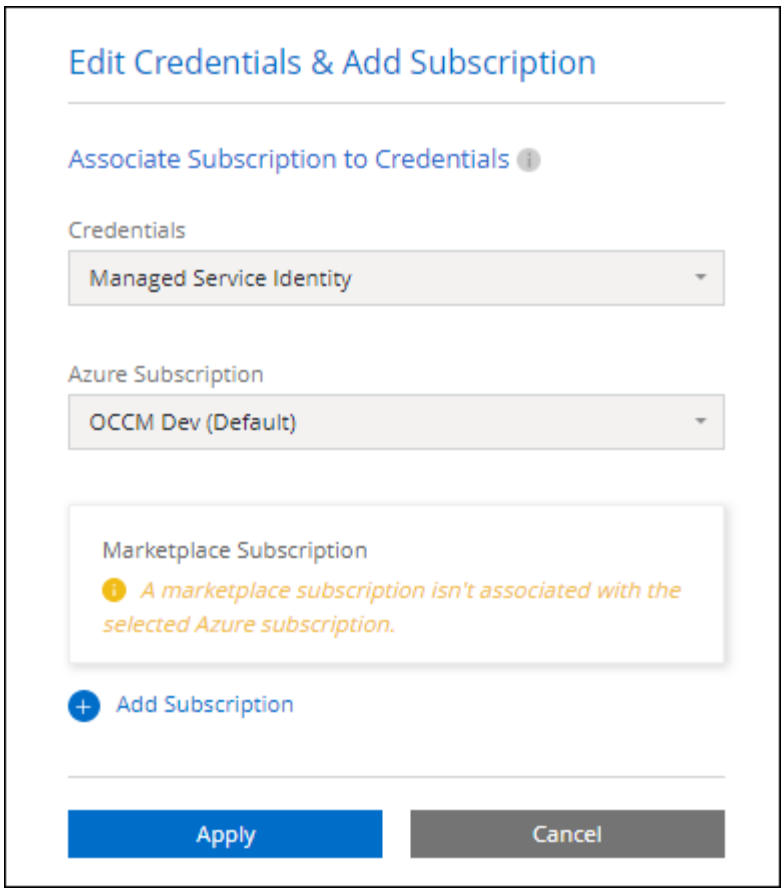
   BlueXP consulta automáticamente al servicio de licencias de NetApp para obtener detalles sobre las licencias asociadas a su cuenta del sitio de soporte de NetApp. Si no se producen errores, BlueXP añade automáticamente las licencias a la cartera digital.

   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".

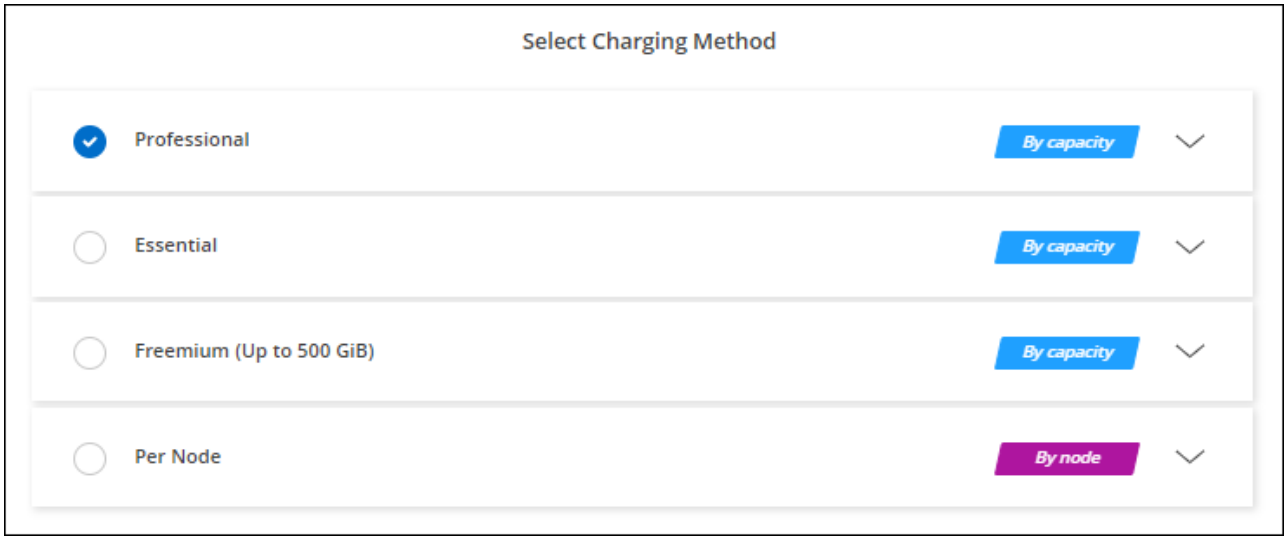
3. En la página Canvas, haga clic en **Agregar entorno de trabajo** y siga los pasos de BlueXP.

   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 Azure Marketplace.

      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 Azure".

Suscripción a PAYGO

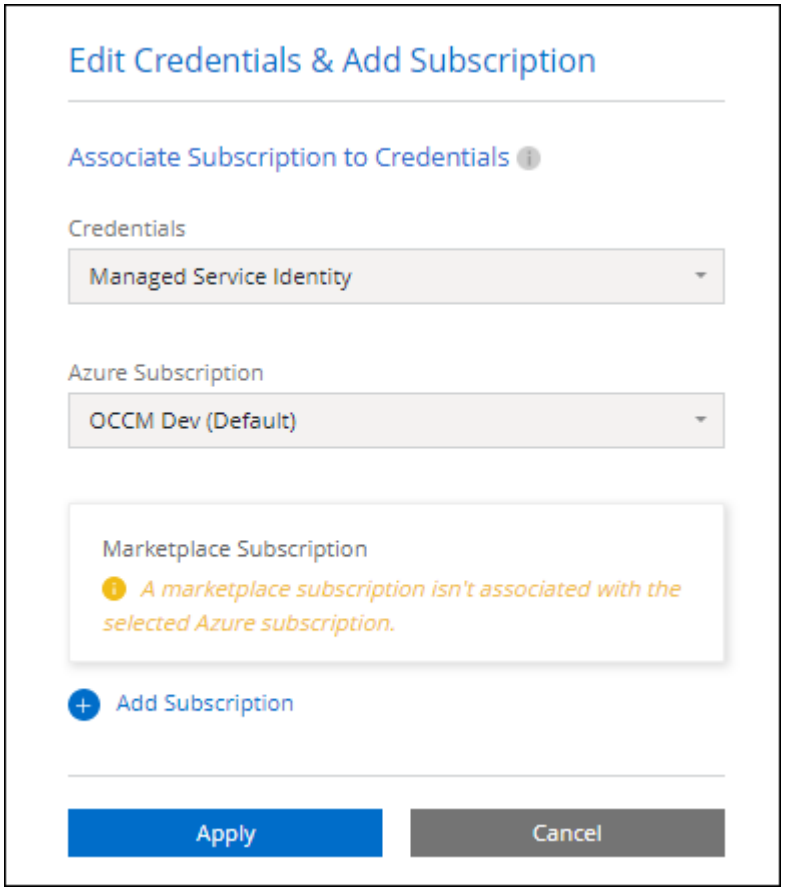
Pague por horas suscribiendo la oferta del mercado de su proveedor de cloud.

Al crear un entorno de trabajo de Cloud Volumes ONTAP, BlueXP le solicita que se suscriba al acuerdo que está disponible en Azure Marketplace. Esa suscripción se asocia entonces con el entorno de trabajo para la

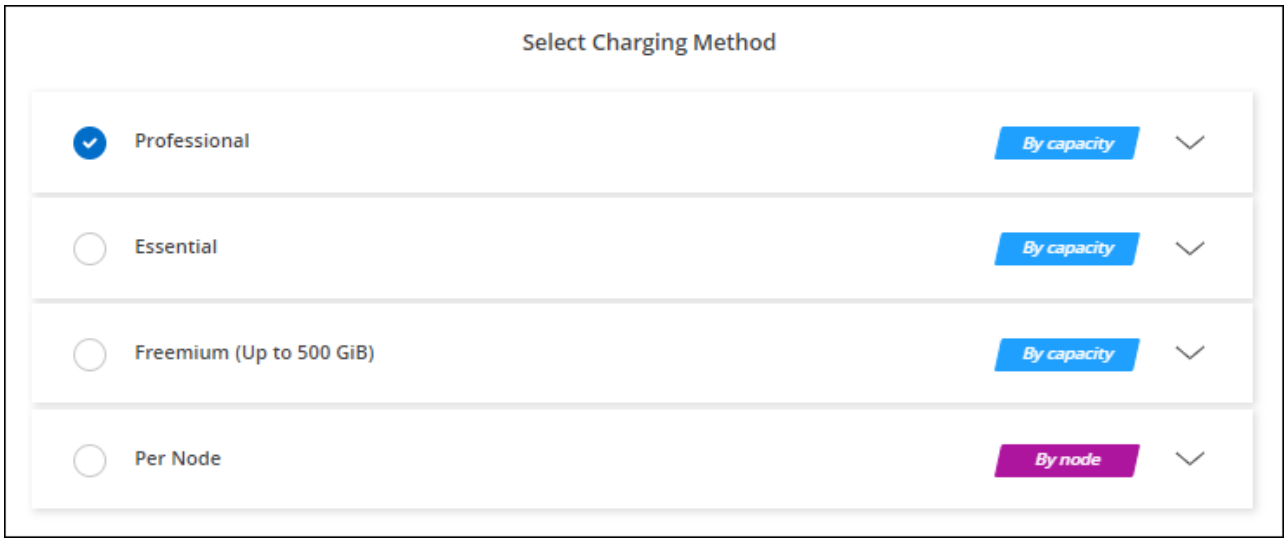
carga. Puede utilizar la misma suscripción para entornos de trabajo adicionales.

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 Azure 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 Azure".

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

Contrato anual

Pague anualmente por Cloud Volumes ONTAP comprando un contrato anual.

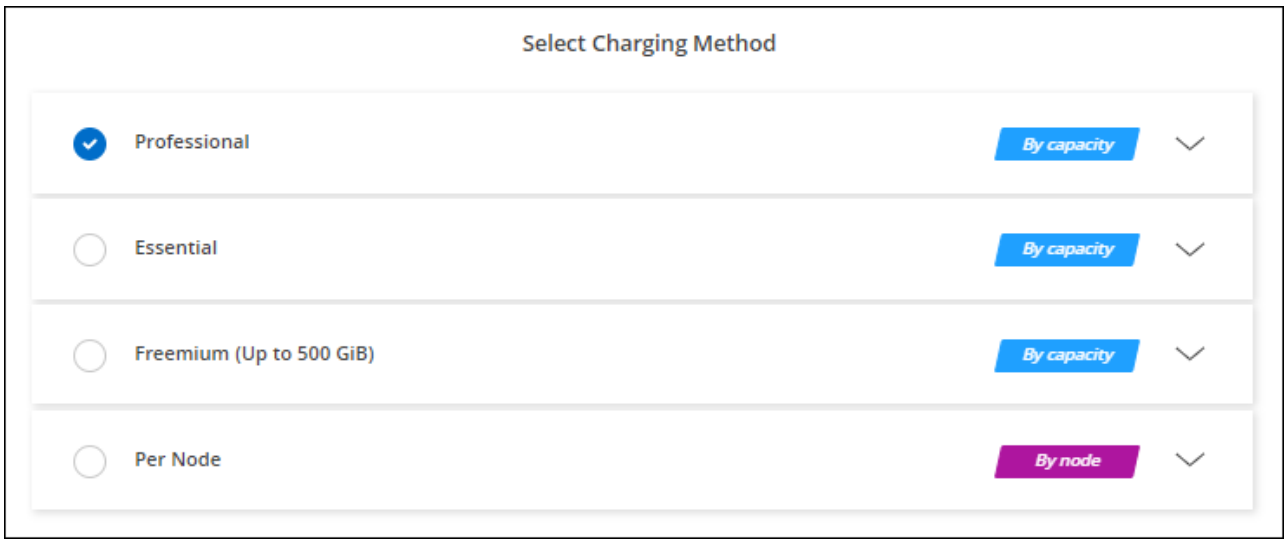
Pasos

1. Póngase en contacto con su representante de ventas de NetApp para adquirir un contrato anual.

   El contrato está disponible como una oferta *private* en Azure Marketplace.

   Una vez que NetApp comparta la oferta privada con usted, podrá seleccionar el plan anual al suscribirse desde Azure Marketplace durante la creación del entorno de trabajo.

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 > continuar**.
   b. En el portal de Azure, seleccione el plan anual que compartió con su cuenta de Azure y, a continuación, haga clic en **Suscribirse**.
   c. 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 Azure".

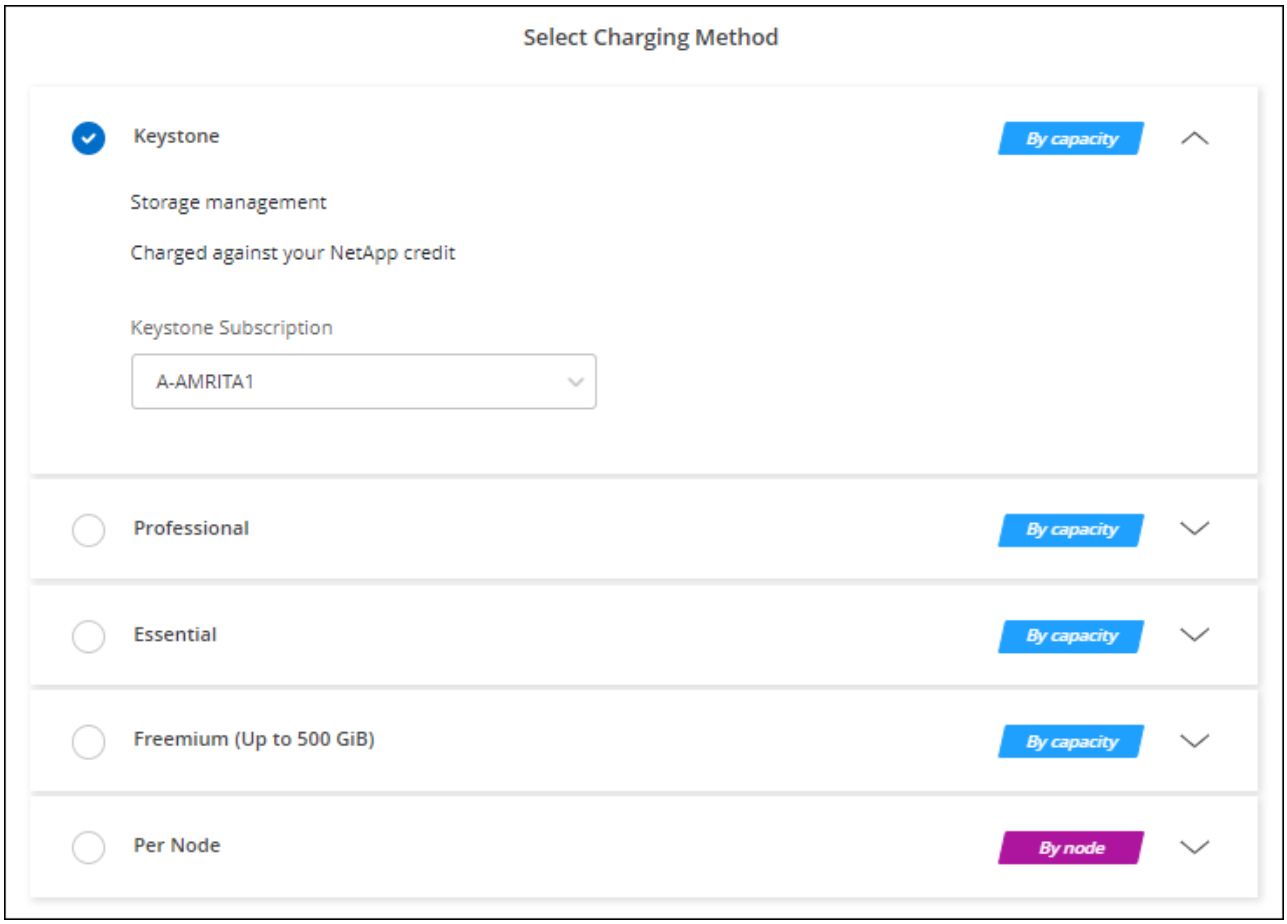
Suscripción a Keystone

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 Azure".

Habilitar el modo de alta disponibilidad en Azure

El modo de alta disponibilidad de Microsoft Azure debe habilitarse para reducir los tiempos de conmutación al nodo de respaldo no planificados y para habilitar el soporte de NFSv4 para Cloud Volumes ONTAP.

A partir de la versión 9.10.1 de Cloud Volumes ONTAP, hemos reducido el tiempo de conmutación por error no planificado para los pares de alta disponibilidad de Cloud Volumes ONTAP que se ejecutan en Microsoft Azure y hemos añadido compatibilidad con NFSv4. Para que estas mejoras estén disponibles en Cloud Volumes ONTAP, debe habilitar la función de alta disponibilidad en su suscripción a Azure.

BlueXP le preguntará estos detalles en un mensaje Action Required cuando tenga que activar esta función en una suscripción a Azure.

Tenga en cuenta lo siguiente:

- No hay problemas con la alta disponibilidad de su par de alta disponibilidad de Cloud Volumes ONTAP. Esta función de Azure trabaja conjuntamente con ONTAP para reducir el tiempo de interrupción de la aplicación observado por el cliente en los protocolos NFS que resultan de eventos de conmutación por error no planificados.
- Habilitar esta función no es disruptiva para los pares de alta disponibilidad Cloud Volumes ONTAP.
- Si habilita esta función en su suscripción a Azure, no se producirán problemas en otras máquinas virtuales.

Un usuario de Azure con privilegios de "propietario" puede habilitar la función desde la CLI de Azure.

Pasos

1. "Acceda a Azure Cloud Shell desde el portal de Azure"
2. Registre la función del modo de alta disponibilidad:

```
az account set -s AZURE_SUBSCRIPTION_NAME_OR_ID
az feature register --name EnableHighAvailabilityMode --namespace
Microsoft.Network
az provider register -n Microsoft.Network
```

3. Si lo desea, compruebe que la función está registrada:

```
az feature show --name EnableHighAvailabilityMode --namespace
Microsoft.Network
```

La CLI de Azure debe devolver un resultado similar a el siguiente:

```
{
  "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/providers/Microsoft.Features/providers/Microsoft.Network/fe
atures/EnableHighAvailabilityMode",
  "name": "Microsoft.Network/EnableHighAvailabilityMode",
  "properties": {
    "state": "Registered"
  },
  "type": "Microsoft.Features/providers/features"
}
```

Inicio de Cloud Volumes ONTAP en Azure

Puede iniciar un sistema de un solo nodo o un par de alta disponibilidad en Azure mediante la creación de un entorno de trabajo de Cloud Volumes ONTAP en BlueXP.

Lo que necesitará

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 haber elegido una configuración y obtener información de redes de Azure 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".

Acerca de esta tarea

Cuando BlueXP crea un sistema Cloud Volumes ONTAP en Azure, crea varios objetos de Azure, como un grupo de recursos, interfaces de red y cuentas de almacenamiento. Puede revisar un resumen de los recursos al final del asistente.

> **Potencial de pérdida de datos**
>
> La mejor práctica es utilizar un nuevo grupo de recursos dedicado para cada sistema de Cloud Volumes ONTAP.
>
> No se recomienda la implementación de Cloud Volumes ONTAP en un grupo de recursos compartidos existente debido al riesgo de pérdida de datos. Si bien BlueXP puede eliminar recursos de Cloud Volumes ONTAP de un grupo de recursos compartidos en caso de error o eliminación de la implementación, es posible que un usuario de Azure elimine accidentalmente los recursos de Cloud Volumes ONTAP de un grupo de recursos compartidos.

Iniciar un sistema Cloud Volumes ONTAP de un único nodo en Azure

Si desea iniciar un sistema Cloud Volumes ONTAP de un solo nodo en Azure, tendrá que crear un entorno de trabajo de nodo único en BlueXP.

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 **Microsoft Azure** y **Cloud Volumes ONTAP Single Node**.
4. Si se le solicita, "Cree un conector".
5. **Detalles y credenciales**: De forma opcional, cambie las credenciales y la suscripción de Azure, especifique un nombre de clúster, añada etiquetas si es necesario y, a continuación, especifique credenciales.

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

Campo	Descripción
Nombre del entorno de trabajo	BlueXP usa el nombre de entorno de trabajo para nombrar tanto el sistema Cloud Volumes ONTAP como la máquina virtual de Azure. También utiliza el nombre como prefijo para el grupo de seguridad predefinido si selecciona esa opción.
Etiquetas del grupo de recursos	Las etiquetas son metadatos para sus recursos de Azure. Cuando introduce etiquetas en este campo, BlueXP las añade al grupo de recursos asociado al sistema Cloud Volumes ONTAP. 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 Microsoft Azure: Uso de etiquetas para organizar los recursos de Azure".
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	Puede elegir diferentes credenciales de Azure y una suscripción de Azure diferente para utilizarlo con este sistema de Cloud Volumes ONTAP. Tiene que asociar una suscripción a Azure Marketplace con la suscripción de Azure seleccionada para poner en marcha un sistema Cloud Volumes ONTAP de pago por uso. "Aprenda a añadir credenciales".

En el siguiente vídeo se muestra cómo asociar una suscripción de Marketplace a una suscripción de Azure:

Suscríbete a BlueXP desde Azure Marketplace

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**: Seleccione una región, zona de disponibilidad, vnet y subred y, a continuación, active la casilla de verificación para confirmar la conectividad de red entre el conector y la ubicación de destino.

   En el caso de los sistemas de nodo único, puede elegir la zona de disponibilidad en la que desea poner en marcha Cloud Volumes ONTAP. Si no selecciona un AZ, BlueXP seleccionará uno para usted.

8. **Conectividad**: Elija un grupo de recursos nuevo o existente y, a continuación, elija si desea utilizar el grupo de seguridad predefinido o si desea utilizar el suyo.

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

Campo	Descripción
Grupo de recursos	Crear un nuevo grupo de recursos para Cloud Volumes ONTAP o utilizar un grupo de recursos existente. La mejor práctica es utilizar un nuevo grupo de recursos dedicado para Cloud Volumes ONTAP. Aunque es posible implementar Cloud Volumes ONTAP en un grupo de recursos compartidos existente, no se recomienda debido al riesgo de pérdida de datos. Consulte la advertencia anterior para obtener más detalles. Si la cuenta de Azure que está utilizando tiene el "permisos necesarios", BlueXP quita los recursos de Cloud Volumes ONTAP de un grupo de recursos, en caso de error o eliminación de la implementación.
Grupo de seguridad generado	Si deja que BlueXP genere el grupo de seguridad para usted, debe elegir cómo permitirá el tráfico: • Si selecciona **sólo vnet seleccionado**, el origen del tráfico entrante es el intervalo de subred del vnet seleccionado y el rango de subred del vnet donde reside el conector. Esta es la opción recomendada. • Si elige **All VNets**, el origen del tráfico entrante es el intervalo IP 0.0.0.0/0.
Utilice la existente	Si elige un grupo de seguridad existente, este debe cumplir con los requisitos de Cloud Volumes ONTAP. "Consulte el grupo de seguridad predeterminado".

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

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

11. **Licencia**: Cambie la versión de Cloud Volumes ONTAP según sea necesario y seleccione un tipo de máquina virtual.

    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.

12. **Suscribirse desde Azure Marketplace**: Verás esta página si BlueXP no pudo habilitar implementaciones programáticas de Cloud Volumes ONTAP. Siga los pasos que aparecen en la pantalla. Consulte "Puesta en marcha programática de productos Marketplace" si quiere más información.
13. **Recursos de almacenamiento subyacentes**: Elija la configuración para el agregado inicial: Un tipo de disco, un tamaño para cada disco y si se debe habilitar la organización en niveles de datos para el almacenamiento BLOB.

Tenga en cuenta lo siguiente:

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

  Para obtener ayuda a elegir el tipo y el tamaño de disco, consulte "Ajuste de tamaño de su sistema en Azure".

- 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.

  "Más información acerca de la organización en niveles de los datos".

14. **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).

       Esta opción solo está disponible para ciertos tipos de máquina virtual. Para saber qué tipos de máquina virtual son compatibles, consulte "Configuraciones compatibles con licencia para pares de alta disponibilidad".

       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.

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

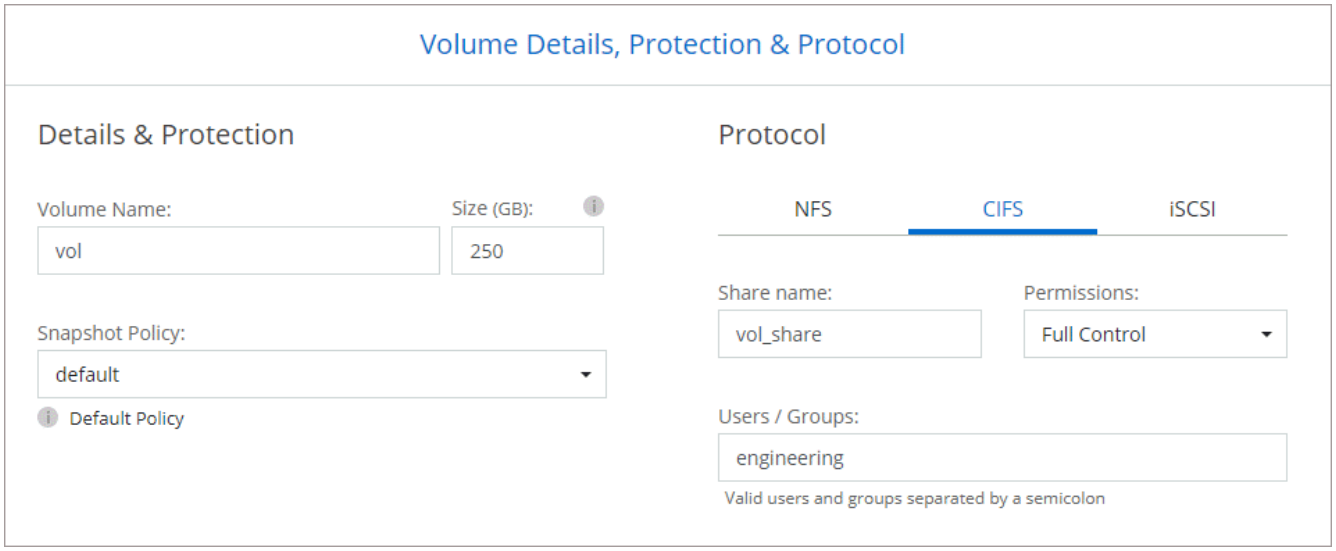
    "Obtenga información sobre las versiones y los protocolos de cliente compatibles".

    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.

Campo	Descripción
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:



16. **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. Para configurar los Servicios de dominio de Azure AD como servidor AD para Cloud Volumes ONTAP, debe introducir **OU=equipos ADDC** o **OU=usuarios ADDC** en este campo.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Documentación de Azure: Cree una unidad organizativa (OU) en un dominio gestionado de Azure AD Domain Services"^]
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.

17. **Perfil de uso, Tipo de disco y Directiva de organización en niveles**: Elija si desea activar las funciones de eficiencia del almacenamiento y cambiar 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".

18. **revisar y aprobar**: Revise y confirme sus selecciones.
    a. Consulte los detalles de la configuración.
    b. Haga clic en **más información** para consultar detalles sobre el soporte técnico y los recursos de Azure que BlueXP comprará.
    c. Active las casillas de verificación **comprendo…**.
    d. Haga clic en **Ir**.

Resultado

BlueXP despliega el sistema Cloud Volumes ONTAP. Puede realizar un seguimiento del progreso en la línea de tiempo.

Si tiene algún problema con la implementación del sistema 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 Azure

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

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. Si se le solicita, "Cree un conector".
4. **Detalles y credenciales**: De forma opcional, cambie las credenciales y la suscripción de Azure, especifique un nombre de clúster, añada etiquetas si es necesario y, a continuación, especifique credenciales.

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

Campo	Descripción
Nombre del entorno de trabajo	BlueXP usa el nombre de entorno de trabajo para nombrar tanto el sistema Cloud Volumes ONTAP como la máquina virtual de Azure. También utiliza el nombre como prefijo para el grupo de seguridad predefinido si selecciona esa opción.
Etiquetas del grupo de recursos	Las etiquetas son metadatos para sus recursos de Azure. Cuando introduce etiquetas en este campo, BlueXP las añade al grupo de recursos asociado al sistema Cloud Volumes ONTAP. 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 Microsoft Azure: Uso de etiquetas para organizar los recursos de Azure".
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.

Campo	Descripción
Editar credenciales	Puede elegir diferentes credenciales de Azure y una suscripción de Azure diferente para utilizarlo con este sistema de Cloud Volumes ONTAP. Tiene que asociar una suscripción a Azure Marketplace con la suscripción de Azure seleccionada para poner en marcha un sistema Cloud Volumes ONTAP de pago por uso. "Aprenda a añadir credenciales".

En el siguiente vídeo se muestra cómo asociar una suscripción de Marketplace a una suscripción de Azure:

Suscríbete a BlueXP desde Azure Marketplace

5. **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.

6. **Modelos de despliegue de alta disponibilidad**:
   a. Seleccione **Zona de disponibilidad única** o **Zona de disponibilidad múltiple**.
   b. **Ubicación y conectividad** (AZ único) y **Región y conectividad** (AZs múltiples)
      - Para AZ único, seleccione una región, vnet y una subred.
      - Para varios AZs, seleccione una región, vnet, subred, zona para el nodo 1 y zona para el nodo 2.
   c. Active la casilla de verificación **he verificado la conectividad de red…**.
7. **Conectividad**: Elija un grupo de recursos nuevo o existente y, a continuación, elija si desea utilizar el grupo de seguridad predefinido o si desea utilizar el suyo.

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

Campo	Descripción
Grupo de recursos	Crear un nuevo grupo de recursos para Cloud Volumes ONTAP o utilizar un grupo de recursos existente. La mejor práctica es utilizar un nuevo grupo de recursos dedicado para Cloud Volumes ONTAP. Aunque es posible implementar Cloud Volumes ONTAP en un grupo de recursos compartidos existente, no se recomienda debido al riesgo de pérdida de datos. Consulte la advertencia anterior para obtener más detalles. Tiene que utilizar un grupo de recursos dedicado para cada par de alta disponibilidad de Cloud Volumes ONTAP que implemente en Azure. Solo se admite un par de alta disponibilidad en un grupo de recursos. BlueXP experimenta problemas de conexión si intenta implementar un segundo par de alta disponibilidad de Cloud Volumes ONTAP en un grupo de recursos de Azure. Si la cuenta de Azure que está utilizando tiene el "permisos necesarios", BlueXP quita los recursos de Cloud Volumes ONTAP de un grupo de recursos, en caso de error o eliminación de la implementación.
Grupo de seguridad generado	Si deja que BlueXP genere el grupo de seguridad para usted, debe elegir cómo permitirá el tráfico: • Si selecciona **sólo vnet seleccionado**, el origen del tráfico entrante es el intervalo de subred del vnet seleccionado y el rango de subred del vnet donde reside el conector. Esta es la opción recomendada. • Si elige **All VNets**, el origen del tráfico entrante es el intervalo IP 0.0.0.0/0.
Utilice la existente	Si elige un grupo de seguridad existente, este debe cumplir con los requisitos de Cloud Volumes ONTAP. "Consulte el grupo de seguridad predeterminado".

8. **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".
9. **Paquetes preconfigurados**: Seleccione uno de los paquetes para implementar rápidamente un sistema Cloud Volumes ONTAP, o haga clic en **Cambiar configuración**.

   Si selecciona uno de los paquetes, solo tiene que especificar un volumen y, a continuación, revisar y aprobar la configuración.
10. **Licencia**: Cambie la versión de Cloud Volumes ONTAP según sea necesario y seleccione un tipo de máquina virtual.

    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.

11. **Suscribirse al mercado de Azure**: Siga los pasos si BlueXP no pudo permitir la implementación programática de Cloud Volumes ONTAP.
12. **Recursos de almacenamiento subyacentes**: Elija la configuración para el agregado inicial: Un tipo de disco, un tamaño para cada disco y si se debe habilitar la organización en niveles de datos para el almacenamiento BLOB.

    Tenga en cuenta lo siguiente:

    - El tamaño del disco es para todos los discos de la agrupación inicial y para cualquier agregado adicional que BlueXP cree cuando se utiliza la opción de aprovisionamiento simple. Puede crear agregados que utilicen un tamaño de disco diferente mediante la opción de asignación avanzada.

      Para obtener más ayuda a la hora de elegir el tamaño de disco, consulte "Configure el tamaño de su sistema en Azure".

    - 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.

      "Más información acerca de la organización en niveles de los datos".

13. **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).

       Esta opción solo está disponible para ciertos tipos de máquina virtual. Para saber qué tipos de máquina virtual son compatibles, consulte "Configuraciones compatibles con licencia para pares de alta disponibilidad".

       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.
14. **Secure Communication to Storage & WORM**: Elija si desea activar una conexión HTTPS a cuentas de almacenamiento de Azure y activar el almacenamiento WORM (escritura única, lectura múltiple), si lo desea.

    La conexión HTTPS es de un par de alta disponibilidad de Cloud Volumes ONTAP 9.7 a cuentas de almacenamiento BLOB de Azure. Tenga en cuenta que al habilitar esta opción, el rendimiento de escritura puede afectar. No se puede cambiar la configuración después de crear el entorno de trabajo.

    "Más información acerca del almacenamiento WORM".

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

    "Más información acerca del almacenamiento WORM".

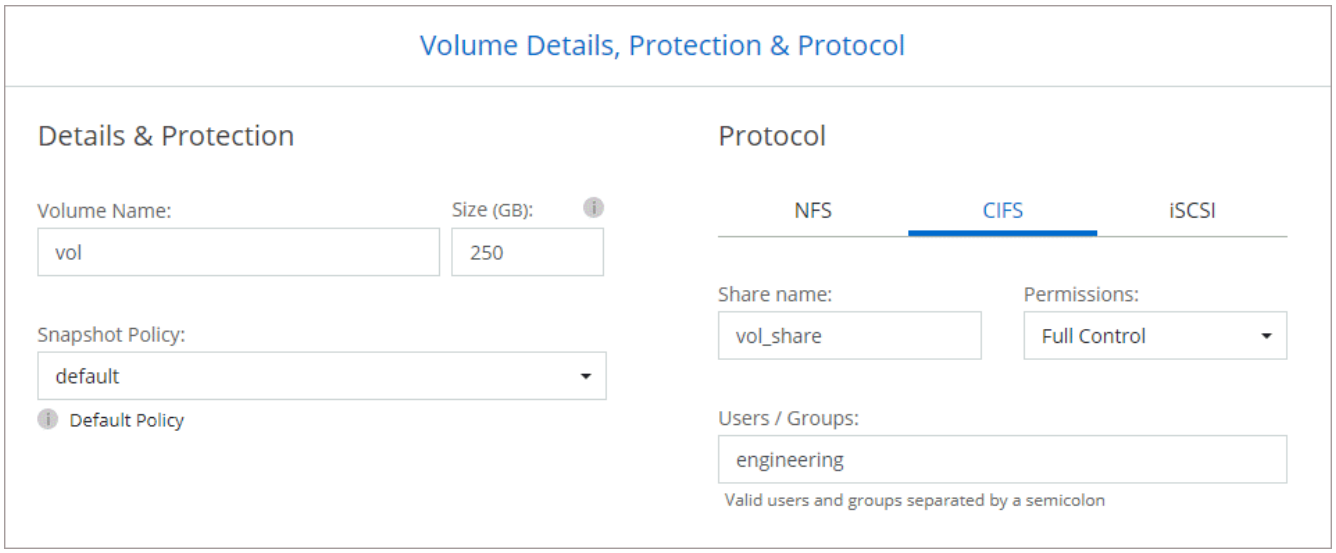
15. **Crear volumen**: Introduzca los detalles del nuevo volumen o haga clic en **Omitir**.

    "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:



16. **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. Para configurar los Servicios de dominio de Azure AD como servidor AD para Cloud Volumes ONTAP, debe introducir **OU=equipos ADDC** o **OU=usuarios ADDC** en este campo.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Documentación de Azure: Cree una unidad organizativa (OU) en un dominio gestionado de Azure AD Domain Services"^]
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.

17. **Perfil de uso, Tipo de disco y Directiva de organización en niveles**: Elija si desea activar las funciones de eficiencia del almacenamiento y cambiar 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".

18. **revisar y aprobar**: Revise y confirme sus selecciones.
    a. Consulte los detalles de la configuración.
    b. Haga clic en **más información** para consultar detalles sobre el soporte técnico y los recursos de Azure que BlueXP comprará.
    c. Active las casillas de verificación **comprendo…**.
    d. Haga clic en **Ir**.

Resultado

BlueXP despliega el sistema Cloud Volumes ONTAP. Puede realizar un seguimiento del progreso en la línea de tiempo.

Si tiene algún problema con la implementación del sistema 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.

Verificación de imagen de la plataforma Azure

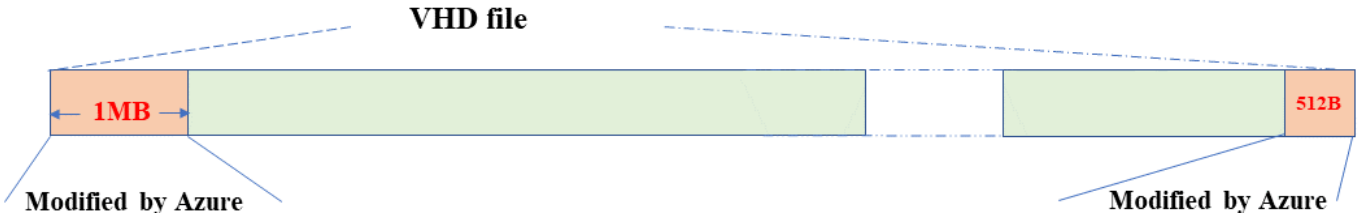
Información general sobre la verificación de imágenes de Azure

La verificación de imágenes de Azure cumple con los requisitos de seguridad de NetApp mejorada. Si bien la verificación de un archivo de imagen es un proceso sencillo, la verificación de la firma de imagen de Azure requiere una manipulación especial del conocido archivo de imagen de Azure VHD debido a una alternativa realizada por Azure Marketplace.

La verificación de imágenes de Azure es compatible con la versión 9.15.0 del software Cloud Volumes ONTAP o posterior.

Modificación de Azure de los archivos VHD publicados

Los 1MB (1048576 bytes) iniciales y los 512 bytes finales del archivo VHD son modificados por Azure. La firma de imágenes NetApp omite los 1MB primeros y los 512 bytes finales y firma la parte de imagen VHD restante.



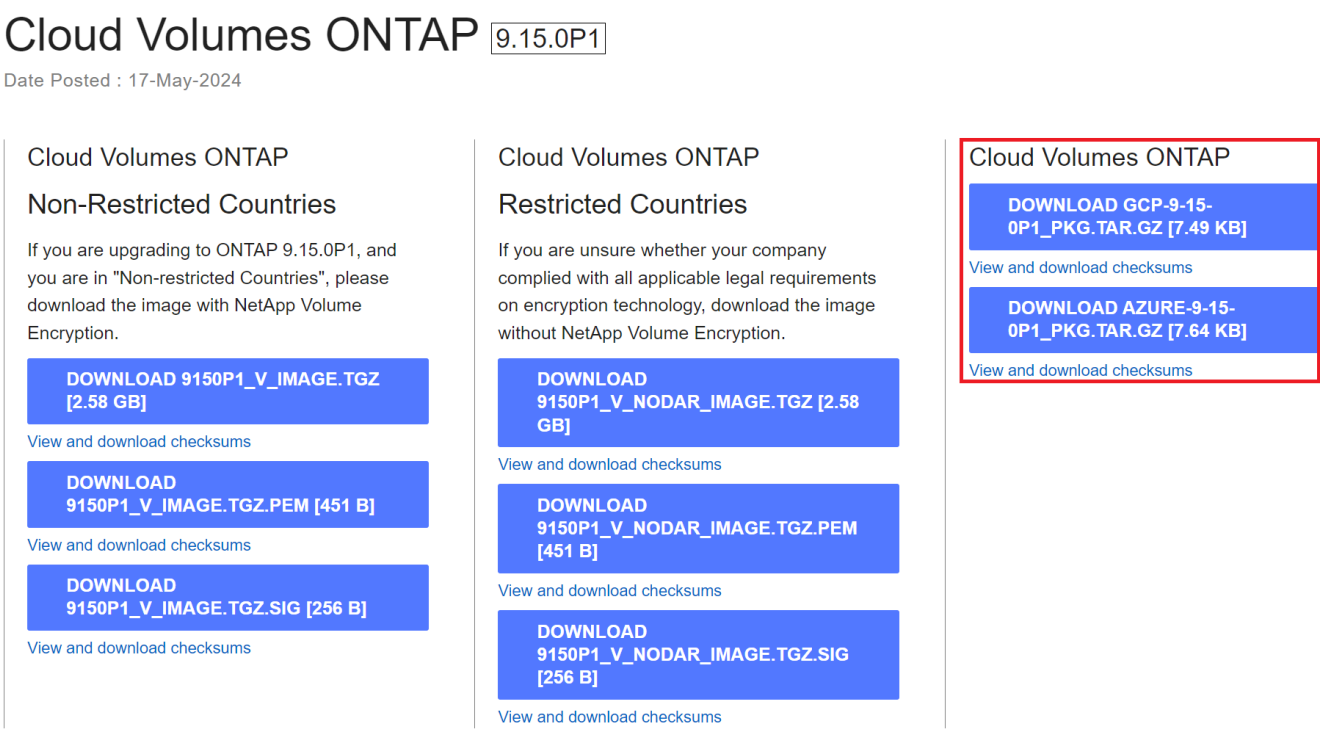
Como ejemplo, el diagrama anterior muestra un archivo VHD con un tamaño de 10GB MB. Pero la porción firmada de NetApp está marcada en verde con un tamaño de 10GB - 1MB - 512B.

Descargue Azure Image Digest File

El archivo Azure Image Digest File se puede descargar de la "Sitio de soporte de NetApp". La descarga está en formato tar.gz y contiene archivos para la verificación de firma de imagen.

Pasos

1. Vaya a la "Página del producto de Cloud Volumes ONTAP en el sitio de soporte de NetApp" Y descargue la versión de software deseada en la sección Descargas.
2. En la página de descarga de Cloud Volumes ONTAP, haga clic en el botón **download** para el archivo de resumen de imágenes de Azure para descargar el TAR. Archivo GZ.



3. Para Linux y macOS, debe realizar lo siguiente para obtener md5sum y sha256sum para el archivo Azure Image Digest descargado.
   a. Para md5sum, introduzca la `md5sum` comando.
   b. Para sha256sum, introduzca la `sha256sum` comando.
4. Compruebe el `md5sum` y.. `sha256sum` Los valores coinciden con la descarga de Azure Image Digest File.
5. En Linux y Mac OS, realice el `tar -xzf` comando para extraer el archivo tar.gz.

El TAR extraído. El archivo GZ contiene el archivo digest(.sig), el archivo de certificado de clave pública(.pem) y el archivo de certificado de cadena(.pem).

Lista de resultados de untar tar.gz archivo

```
$ ls cert/ -l
-rw-r----- 1 netapp netapp  384 May  13 13:00 9.15.0P1_azure_digest.sig
-rw-r----- 1 netapp netapp 2365 May  13 13:00 Certificate-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 Certificate-Chain-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 version_readme
```

Exportación de imágenes desde Azure Marketplace

Una vez que la imagen del disco duro virtual se publica en la nube de Azure, la imagen deja de ser gestionada por NetApp. En su lugar, la imagen publicada se coloca en Azure Marketplace. La alteración de Azure a los 1MB líderes y 512B finales del VHD se produce cuando la imagen se almacena en un lugar y se publica en Azure Marketplace. Para verificar la firma del archivo VHD, la imagen VHD modificada por Azure debe exportarse primero desde Azure Marketplace.

Lo que necesitará

Debe instalar los programas necesarios en su sistema.

- Azure CLI está instalado o Azure Cloud Shell a través del portal de Azure está disponible en todo momento.

> Para obtener más información sobre cómo instalar la CLI de Azure, consulte "Documentación de Azure: Cómo instalar la CLI de Azure".

Pasos

1. Asigne la versión de ONTAP a la versión de la imagen de Azure Marketplace utilizando el contenido del archivo version_readme.

   Para cada asignación de versiones enumerada en el archivo version_readme, la versión de ONTAP se representa con «buildname» y la versión de la imagen de Azure Marketplace se representa con «version».

   Por ejemplo, en el siguiente archivo version_readme, la versión de ONTAP «9.15.0P1» está asignada a la versión de la imagen de Azure Marketplace «9150.01000024.05090105». Esta versión de imagen de Azure Marketplace se utiliza más adelante para establecer la imagen URN.

```
[
    {
        "buildname": "9.15.0P1",
        "publisher": "netapp",
        "version": "9150.01000024.05090105"
    }
]
```

2. Identifique el nombre de la región en la que pretende crear máquinas virtuales.

   Este nombre de región se utiliza como valor para la variable “locName” al definir el URN de la imagen de mercado.

   a. Para recibir una lista de regiones disponibles, introduzca la `az account list-locations -o table` comando.

      En la siguiente tabla, el nombre de la región se denomina campo Nombre.

```
$ az account list-locations -o table
DisplayName               Name                 RegionalDisplayName
------------------------  -------------------
-------------------------------------
East US                   eastus               (US) East US
East US 2                 eastus2              (US) East US 2
South Central US          southcentralus       (US) South Central US
...
```

3. Revise el nombre de SKU para el tipo de puesta en marcha de VM correspondiente en la tabla siguiente.

   El nombre de SKU se utiliza como valor para la variable skuName al establecer el URN de la imagen de mercado.

   Por ejemplo, las puestas en marcha de un solo nodo deben utilizar el nombre SKU «ontap_cloud_byol».

Tipo de despliegue de máquinas virtuales	Nombre de SKU
Nodo único	ontap_cloud_byol
Alta disponibilidad	ontap_cloud_byol_ha

4. Una vez que se hayan asignado la versión de ONTAP y la imagen de Azure Marketplace, exporte el archivo VHD desde Azure Marketplace a través de Azure Cloud Shell o la interfaz de línea de comandos de Azure.

Exporte el archivo VHD a través de Azure Cloud Shell en el portal de Azure

1. Desde Azure Cloud Shell, exporte la imagen del mercado a un vhd (image2, por ejemplo, 9150.01000024.05090105.vhd) y descárguela en su equipo local (por ejemplo, una máquina Linux o un PC con Windows).

Haga clic para mostrar

```
#Azure Cloud Shell on Azure portal to get VHD image from Azure
Marketplace
a) Set the URN and other parameters of the marketplace image. URN is
with format "<publisher>:<offer>:<sku>:<version>". Optionally, a
user can list NetApp marketplace images to confirm the proper image
version.
PS /home/user1> $urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
PS /home/user1> $locName="eastus2"
PS /home/user1> $pubName="netapp"
PS /home/user1> $offerName="netapp-ontap-cloud"
PS /home/user1> $skuName="ontap_cloud_byol"
PS /home/user1> Get-AzVMImage -Location $locName -PublisherName
$pubName -Offer $offerName -Sku $skuName |select version
...
141.20231128
9.141.20240131
9.150.20240213
9150.01000024.05090105
...

b) Create a new managed disk from the Marketplace image with the
matching image version
PS /home/user1> $diskName = “9150.01000024.05090105-managed-disk"
PS /home/user1> $diskRG = “fnf1”
PS /home/user1> az disk create -g $diskRG -n $diskName --image
-reference $urn
PS /home/user1> $sas = az disk grant-access --duration-in-seconds
3600 --access-level Read --name $diskName --resource-group $diskRG
PS /home/user1> $diskAccessSAS = ($sas | ConvertFrom-
Json)[0].accessSas

c) Export a VHD from the managed disk to Azure Storage
Create a container with proper access level. As an example, a
container named 'vm-images' with 'Container' access level is used
here.
Get storage account access key, on Azure portal, 'Storage
Accounts'/'examplesaname'/'Access Key'/'key1'/'key'/'show'/<copy>.
PS /home/user1> $storageAccountName = “examplesaname”
PS /home/user1> $containerName = “vm-images”
PS /home/user1> $storageAccountKey = "<replace with the above access
key>"
PS /home/user1> $destBlobName = “9150.01000024.05090105.vhd”
PS /home/user1> $destContext = New-AzureStorageContext
```

```
-StorageAccountName $storageAccountName -StorageAccountKey
$storageAccountKey
PS /home/user1> Start-AzureStorageBlobCopy -AbsoluteUri
$diskAccessSAS -DestContainer $containerName -DestContext
$destContext -DestBlob $destBlobName
PS /home/user1> Get-AzureStorageBlobCopyState –Container
$containerName –Context $destContext -Blob $destBlobName

d) Download the generated image to your server, e.g., a Linux
machine.
Use "wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>".
The URL is organized in a formatted way. For automation tasks, the
following example could be used to derive the URL string. Otherwise,
Azure CLI 'az' command could be issued to get the URL, which is not
covered in this guide. URL Example:
https://examplesaname.blob.core.windows.net/vm-
images/9150.01000024.05090105.vhd

e) Clean up the managed disk
PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG
-DiskName $diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName
$diskName
```

Exporte el archivo VHD a través de la CLI de Azure desde el equipo Linux local

1. Exporte la imagen de mercado a un vhd a través de la CLI de Azure desde una máquina Linux local.

Haga clic para mostrar

```
#Azure CLI on local Linux machine to get VHD image from Azure
Marketplace
a) Login Azure CLI and list marketplace images
% az login --use-device-code
To sign in, use a web browser to open the page
https://microsoft.com/devicelogin and enter the code XXXXXXXXX to
authenticate.

% az vm image list --all --publisher netapp --offer netapp-ontap-
cloud --sku ontap_cloud_byol
...
{
"architecture": "x64",
"offer": "netapp-ontap-cloud",
"publisher": "netapp",
"sku": "ontap_cloud_byol",
"urn": "netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105",
"version": "9150.01000024.05090105"
},
...

b) Create a new managed disk from the Marketplace image with the
matching image version
% export urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
% export diskName="9150.01000024.05090105-managed-disk"
% export diskRG="new_rg_your_rg"
% az disk create -g $diskRG -n $diskName --image-reference $urn
% az disk grant-access --duration-in-seconds 3600 --access-level
Read --name $diskName --resource-group $diskRG
{
  "accessSas": "https://md-
xxxxxx.blob.core.windows.net/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxx"
}

% export diskAccessSAS="https://md-
xxxxxx.blob.core.windows.net/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxx"
#To automate the process, the SAS needs to be extracted from the
standard output. This is not included in this guide.
```

```
c) export vhd from managed disk
Create a container with proper access level. As an example, a
container named 'vm-images' with 'Container' access level is used
here.
Get storage account access key, on Azure portal, 'Storage
Accounts'/'examplesaname'/'Access Key'/'key1'/'key'/'show'/<copy>.
There should be az command that can achieve the same, but this is
not included in this guide.
% export storageAccountName="examplesaname"
% export containerName="vm-images"
% export storageAccountKey="xxxxxxxxxx"
% export destBlobName="9150.01000024.05090105.vhd"

% az storage blob copy start --source-uri $diskAccessSAS
--destination-container $containerName --account-name
$storageAccountName --account-key $storageAccountKey --destination
-blob $destBlobName

{
  "client_request_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_status": "pending",
  "date": "2022-11-02T22:02:38+00:00",
  "etag": "\"0xXXXXXXXXXXXXXXXXX\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
  "version": "2020-06-12",
  "version_id": null
}

#to check the status of the blob copying
% az storage blob show --name $destBlobName --container-name
$containerName --account-name $storageAccountName

....
    "copy": {
      "completionTime": null,
      "destinationSnapshot": null,
      "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxx",
      "incrementalCopy": null,
      "progress": "10737418752/10737418752",
      "source": "https://md-
xxxxxx.blob.core.windows.net/xxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
      "status": "success",
      "statusDescription": null
```

```
    },
....

d) Download the generated image to your server, e.g., a Linux
machine.
Use "wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>".
The URL is organized in a formatted way. For automation tasks, the
following example could be used to derive the URL string. Otherwise,
Azure CLI 'az' command could be issued to get the URL, which is not
covered in this guide. URL Example:
https://examplesaname.blob.core.windows.net/vm-
images/9150.01000024.05090105.vhd

e) Clean up the managed disk
az disk revoke-access --name $diskName --resource-group $diskRG
az disk delete --name $diskName --resource-group $diskRG --yes
```

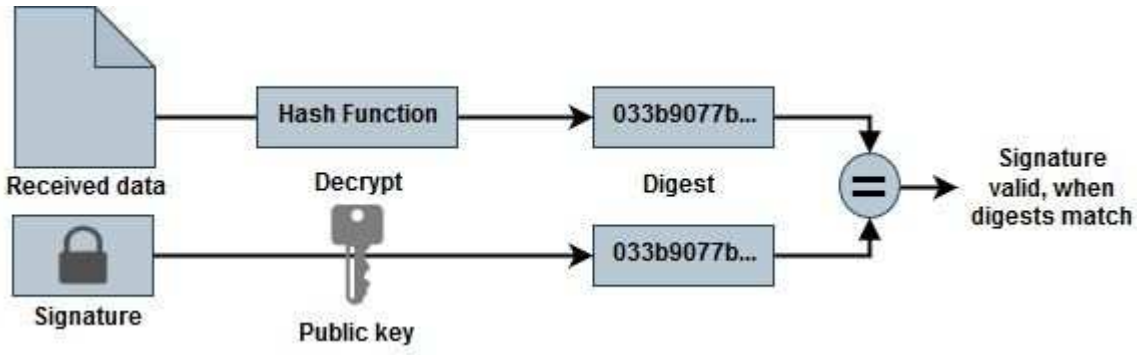
Verificación de firma de archivo

Verificación de firma de archivo

El proceso de verificación de imágenes de Azure generará un resumen del archivo VHD con el 1MB principal y el 512B final segmentado mediante la función hash. Para que coincida con el procedimiento de firma, SHA256 se utiliza para hash. Debe eliminar los 1MB principales y los 512B finales del archivo VHD y, a continuación, verificar la parte restante del archivo VHD.

Resumen del flujo de trabajo de verificación de firmas de archivos

A continuación se ofrece una descripción general del proceso de flujo de trabajo de verificación de firmas de archivos.



- Descargue el archivo Azure Image Digest de la "Sitio de soporte de NetApp" y extraiga el archivo digest(.sig), el archivo de certificado de clave pública(.pem) y el archivo de certificado de cadena(.pem).

  Consulte la "Descargue Azure Image Digest File" si quiere más información.

- Verifique la cadena de confianza.
- Extraiga la clave pública(.pub) del certificado de clave pública(.pem).
- La clave pública extraída se utiliza para descifrar el archivo de resumen. El resultado se compara con un nuevo resumen no cifrado del archivo temporal creado a partir del archivo de imagen con 1MB inicial y 512 bytes finales eliminados.

  Este paso se logra a través del siguiente comando openssl.

  - La sentencia CLI general aparece de la siguiente manera:

    ```
    openssl dgst -verify <public_key> -keyform <form> <hash_function>
    -signature <digest_file> -binary <temporary_file>
    ```

  - La herramienta CLI de OpenSSL muestra un mensaje de confirmación verificada si ambos archivos coinciden y si no coinciden.

Verificación de firma de archivo en Linux

Puede verificar una firma de archivo VHD exportada para Linux siguiendo los pasos que se indican a continuación.

Pasos

1. Descargue el archivo Azure Image Digest de la "Sitio de soporte de NetApp" y extraiga el archivo digest(.sig), el archivo de certificado de clave pública(.pem) y el archivo de certificado de cadena(.pem).

   Consulte la "Descargue Azure Image Digest File" si quiere más información.

2. Verifique la cadena de confianza.

   ```
   % openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
   Certificate-9.15.0P1_azure.pem
   Certificate-9.15.0P1_azure.pem: OK
   ```

3. Elimine los 1MB primeros (1048576 bytes) y los 512 bytes finales del archivo VHD.

   Si se utiliza 'tail', la opción '-c +K' genera bytes que comienzan con los bytes KTH del archivo especificado. Por lo tanto, 1048577 se pasa a 'tail -c'.

   ```
   % tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
   % head -c -512 ./sign.tmp.tail > sign.tmp
   % rm ./sign.tmp.tail
   ```

4. Utilice openssl para extraer la clave pública del certificado y verificar el archivo segmentado (sign.tmp) con el archivo de firma y la clave pública.

   Si el archivo de entrada pasa la verificación, se mostrará el comando
   Verificación correcta. De lo contrario, aparecerá el mensaje Fallo de verificación.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verification OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. Limpie el espacio de trabajo.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

Verificación de firma de archivo en Mac OS

Puede verificar una firma de archivo VHD exportada para Mac OS siguiendo los pasos que se indican a continuación.

Pasos

1. Descargue el archivo Azure Image Digest de la "Sitio de soporte de NetApp" y extraiga el archivo digest(.sig), el archivo de certificado de clave pública(.pem) y el archivo de certificado de cadena(.pem).

   Consulte la "Descargue Azure Image Digest File" si quiere más información.

2. Verifique la cadena de confianza.

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. Elimine los 1MB primeros (1048576 bytes) y los 512 bytes finales del archivo VHD.

   Si se utiliza 'tail', la opción '-c +K' genera bytes que comienzan con los bytes KTH del archivo especificado. Por lo tanto, 1048577 se pasa a 'tail -c'. Toma alrededor de 13m Para que el comando tail se complete en Mac OS.

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. Utilice openssl para extraer la clave pública del certificado y verificar la rayada

archivo (sign.tmp) con el archivo de firma y la clave pública.

Si el archivo de entrada pasa la verificación, el comando mostrará “Verificación correcta”.
De lo contrario, aparecerá el mensaje Fallo de verificación.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verified OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. Limpie el espacio de trabajo.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

Dónde encontrar información adicional sobre la verificación de imágenes de Azure

Consulte los siguientes enlaces para obtener información adicional sobre la verificación de imágenes de Azure. Los siguientes enlaces le llevan a sitios ajenos a NetApp.

Referencias

- "Page Fault Blog: Cómo firmar y verificar usando OpenSSL"
- "Utilice la imagen de Azure Marketplace para crear una imagen de VM para su GPU Azure Stack Edge Pro | Microsoft Learn"
- "Exportar/Copiar un disco gestionado a una cuenta de almacenamiento mediante la CLI de Azure | Microsoft Learn"
- "Inicio rápido de Azure Cloud Shell - Bash | Microsoft Learn"
- "Cómo instalar la CLI de Azure | Microsoft Learn"
- "Copia blob de almacenamiento az | Microsoft Learn"
- "Iniciar sesión con Azure CLI — Inicio de sesión y autenticación | Microsoft Learn"

Comience a usar Google Cloud

Inicio rápido de Cloud Volumes ONTAP en Google Cloud

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

1 Cree un conector

Si usted no tiene un "Conector" Sin embargo, un administrador de cuentas necesita crear uno. "Descubra cómo crear un conector en Google Cloud"

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.

"Obtenga más información acerca de la planificación de la configuración".

3 Configure su red

1. Asegúrese de que VPC y las subredes admitan la conectividad entre el conector y Cloud Volumes ONTAP.
2. Si tiene pensado habilitar la organización en niveles de datos, "Configure la subred de Cloud Volumes ONTAP para acceso privado a Google".
3. Si va a implementar un par de alta disponibilidad, asegúrese de tener cuatro VPC, cada uno con su propia subred.
4. Si está utilizando un VPC compartido, proporcione la función *Compute Network User* a la cuenta de servicio Connector.
5. 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.

"Obtenga más información sobre los requisitos de red".

4 Configure una cuenta de servicio

Cloud Volumes ONTAP requiere una cuenta de servicio de Google Cloud para dos finalidades. La primera es cuando se activa "organización en niveles de los datos" Para organizar los datos inactivos en niveles en almacenamiento de objetos de bajo coste en Google Cloud. La segunda es cuando se activa la "Backup y recuperación de BlueXP" para realizar backups de volúmenes en un almacenamiento de objetos de bajo coste.

Puede configurar una cuenta de servicio y utilizarla para ambos fines. La cuenta de servicio debe tener el rol **Administrador de almacenamiento**.

"Lea las instrucciones paso a paso".

5 Habilite las API de Google Cloud

"Habilite las siguientes API de Google Cloud en su proyecto". Estas API son necesarias para poner en marcha el conector y Cloud Volumes ONTAP.

- API de Cloud Deployment Manager V2
- API de registro en la nube
- API de Cloud Resource Manager
- API del motor de computación
- API de gestión de acceso e identidad (IAM)

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

- "Creación de un conector desde BlueXP"
- "Instalar el software del conector en un host Linux"
- "Qué hace BlueXP con los permisos de Google Cloud"

Planifique la configuración de Cloud Volumes ONTAP en Google Cloud

Al poner en marcha Cloud Volumes ONTAP en Google Cloud, puede elegir un sistema preconfigurado que se ajuste a los requisitos de la carga de trabajo, o 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 es compatible en la mayoría de las regiones de Google Cloud. "Consulte la lista completa de las regiones admitidas".

Seleccione un tipo de máquina admitido

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

"Configuraciones admitidas para Cloud Volumes ONTAP en GCP"

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 GCP"

Ajuste el tamaño de su sistema en GCP

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

Tipo de máquina

Observe los tipos de máquina admitidos en la "Notas de la versión de Cloud Volumes ONTAP" Y luego revise los detalles de Google sobre cada tipo de máquina compatible. Haga coincidir los requisitos de carga de trabajo con el número de vCPU y memoria para el tipo de máquina. Tenga en cuenta que cada núcleo de CPU aumenta el rendimiento de la red.

Consulte lo siguiente para obtener más información:

- "Documentación de Google Cloud: Tipos de máquina estándar N1"
- "Documentación de Google Cloud: Rendimiento"

Tipo de disco para GCP

Cuando crea volúmenes para Cloud Volumes ONTAP, debe elegir el almacenamiento en cloud subyacente que utiliza Cloud Volumes ONTAP para un disco. El tipo de disco puede ser cualquiera de los siguientes:

- *Zonal SSD persistent disks*: Los discos persistentes de SSD son la mejor opción para cargas de trabajo que requieren altas tasas de IOPS aleatorias.
- *Zonal discos persistentes equilibrados*: Estos SSD equilibran el rendimiento y el coste al proporcionar un menor número de IOPS por GB.
- *Zonal Standard persistent disks* : los discos persistentes estándar son económicos y pueden manejar operaciones secuenciales de lectura y escritura.

  Para obtener información detallada, consulte "Documentación de Google Cloud: Discos persistentes zonal (Standard y SSD)".

Tamaño de discos para GCP

Debe seleccionar un tamaño de disco inicial al poner en marcha un sistema Cloud Volumes ONTAP. Después puede dejar que BlueXP gestione la capacidad de un sistema por usted, pero si desea crear agregados por su cuenta, tenga en cuenta lo siguiente:

- Todos los discos de un agregado deben tener el mismo tamaño.
- Determine el espacio que necesita, teniendo en cuenta el rendimiento.
- El rendimiento de los discos persistentes se amplía automáticamente con el tamaño del disco y el número de vCPU disponibles para el sistema.

  Consulte lo siguiente para obtener más información:

  - "Documentación de Google Cloud: Discos persistentes zonal (Standard y SSD)"
  - "Documentación de Google Cloud: Optimización del rendimiento de discos persistentes y SSD locales"

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.

- "Vea los discos predeterminados para los datos del sistema Cloud Volumes ONTAP en Google Cloud".
- "Documentos de Google Cloud: Cuotas de recursos"

  Google Cloud Compute Engine aplica cuotas al uso de recursos, por lo que debe asegurarse de que no ha alcanzado su límite antes de implementar Cloud Volumes ONTAP.

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

Recopilar información de red

Al implementar Cloud Volumes ONTAP en GCP, debe especificar los detalles de su red virtual. Puede utilizar una hoja de cálculo para recopilar la información del administrador.

Información de red para un sistema de un solo nodo

Información para GCP	Su valor
Región	
Zona	
Red VPC	
Subred	
Política de firewall (si utiliza la suya propia)	

Información de red para un par ha en varias zonas

Información para GCP	Su valor
Región	
Zona para el nodo 1	
Zona para nodo 2	
Zona para el mediador	
VPC-0 y subred	
VPC-1 y subred	
VPC-2 y subred	
VPC-3 y subred	
Política de firewall (si utiliza la suya propia)	

Información de red para un par ha en una sola zona

Información para GCP	Su valor
Región	
Zona	
VPC-0 y subred	
VPC-1 y subred	
VPC-2 y subred	
VPC-3 y subred	
Política de firewall (si utiliza la suya propia)	

Elija una velocidad de escritura

BlueXP le permite elegir una configuración de velocidad de escritura para Cloud Volumes ONTAP, excepto los pares de alta disponibilidad (ha) en Google Cloud. 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.

Requisitos de red para Cloud Volumes ONTAP en Google Cloud

Configure sus redes de Google Cloud para que los sistemas Cloud Volumes ONTAP funcionen correctamente.

Si desea poner en marcha un par de alta disponibilidad, debería hacerlo "Descubra cómo funcionan los pares de alta disponibilidad en Google Cloud".

Requisitos para Cloud Volumes ONTAP

Los siguientes requisitos deben cumplirse en Google Cloud.

Requisitos específicos de los sistemas de un solo nodo

Si desea implementar un sistema de un solo nodo, asegúrese de que la red cumpla los siguientes requisitos.

Un VPC

Se requiere una nube privada virtual (VPC) para un único sistema de nodo.

Direcciones IP privadas

BlueXP asigna direcciones IP privadas 3 o 4 a un sistema de un solo nodo en Google Cloud.

Puede omitir la creación de la LIF de gestión de máquinas virtuales de almacenamiento (SVM) si implementa Cloud Volumes ONTAP mediante la API y especifica el siguiente indicador:

```
skipSvmManagementLif: true
```

> Una LIF es una dirección IP asociada con un puerto físico. Se necesita un LIF de gestión de máquinas virtuales de almacenamiento (SVM) para herramientas de gestión como SnapCenter.

Requisitos específicos de los pares de alta disponibilidad

Si desea implementar un par de alta disponibilidad, asegúrese de que la red cumpla los siguientes requisitos.

Una o varias zonas

Puede garantizar la alta disponibilidad de sus datos mediante la implementación de una configuración de alta disponibilidad en varias o en una sola zona. BlueXP le solicitará que elija varias zonas o una sola zona cuando cree el par ha.

- Varias zonas (recomendado)

  La implementación de una configuración de alta disponibilidad en tres zonas garantiza una disponibilidad continua de los datos en caso de que se produzca un fallo dentro de una zona. Tenga en cuenta que el rendimiento de escritura es ligeramente inferior al de una sola zona, pero es mínimo.

- Una sola zona

  Cuando se implementa en una sola zona, una configuración de alta disponibilidad de Cloud Volumes ONTAP utiliza una política de ubicación distribuida. Esta directiva garantiza que una configuración de alta disponibilidad esté protegida desde un único punto de error dentro de la zona, sin tener que utilizar zonas independientes para lograr el aislamiento de fallos.

  Este modelo de puesta en marcha reduce sus costes, ya que no hay ningún coste por salida de datos entre zonas.

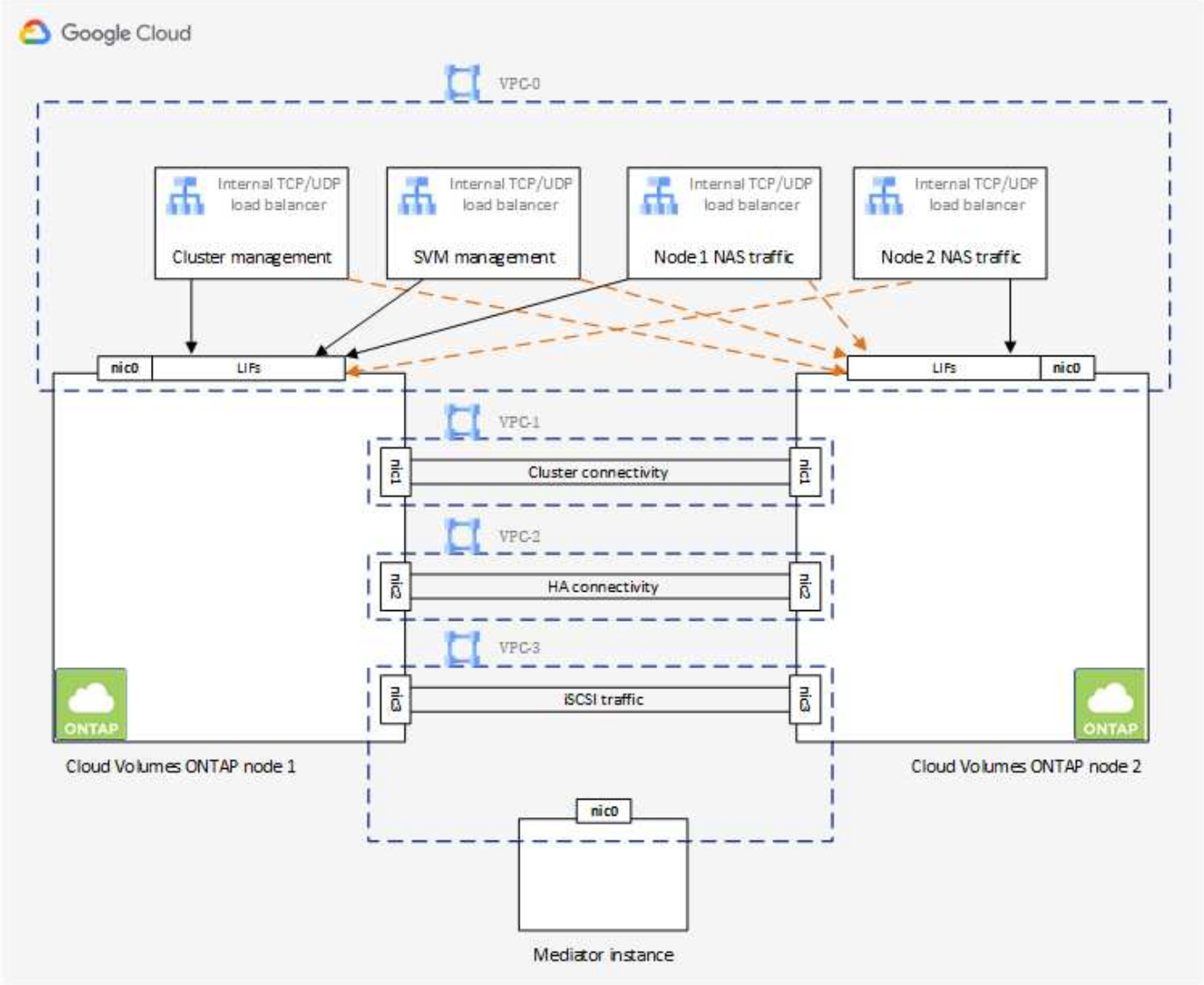
Cuatro clouds privados virtuales

Se necesitan cuatro clouds privados virtuales (VPC) para una configuración de alta disponibilidad. Se necesitan cuatro VPC, ya que Google Cloud requiere que cada interfaz de red resida en una red VPC

independiente.

BlueXP le solicitará que elija cuatro VPC al crear el par ha:

- VPC-0 para conexiones entrantes a los datos y los nodos
- VPC-1, VPC-2 y VPC-3 para la comunicación interna entre los nodos y el mediador de alta disponibilidad



Subredes

Se requiere una subred privada para cada VPC.

Si coloca el conector en VPC-0, deberá habilitar el acceso privado de Google en la subred para acceder a las API y habilitar la organización en niveles de datos.

Las subredes de estas VPC deben tener distintos rangos CIDR. No pueden tener rangos CIDR superpuestos.

Direcciones IP privadas

BlueXP asigna automáticamente el número requerido de direcciones IP privadas a Cloud Volumes ONTAP en Google Cloud. Debe asegurarse de que su red tiene suficientes direcciones 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. Se requiere una LIF de gestión de SVM para herramientas de gestión como SnapCenter.

- **Single Node** BlueXP asigna 4 direcciones IP a un sistema de un solo nodo:
  - LIF de gestión de nodos
  - LIF de gestión de clústeres
  - LIF de datos iSCSI

    Un LIF iSCSI proporciona acceso a los clientes a través del protocolo iSCSI y el sistema lo utiliza para otros flujos de trabajo de red importantes. Estos LIF son necesarios y no deben eliminarse.

  - LIF NAS

    Puede omitir la creación de la LIF de gestión de máquinas virtuales de almacenamiento (SVM) si implementa Cloud Volumes ONTAP mediante la API y especifica el siguiente indicador:

```
skipSvmManagementLif: true
```

- **Par de alta disponibilidad** BlueXP asigna 12-13 direcciones IP a un par de alta disponibilidad:
  - 2 LIF de gestión de nodos (e0a)
  - 1 LIF de administración de clúster (e0a)
  - 2 LIF iSCSI (e0a)

    Un LIF iSCSI proporciona acceso a los clientes a través del protocolo iSCSI y el sistema lo utiliza para otros flujos de trabajo de red importantes. Estos LIF son necesarios y no deben eliminarse.

  - 1 o 2 LIF NAS (e0a)
  - 2 LIF de clúster (e0b)
  - 2 direcciones IP de interconexión de alta disponibilidad (e0c)
  - 2 direcciones IP iSCSI RSM (e0d)

    Puede omitir la creación de la LIF de gestión de máquinas virtuales de almacenamiento (SVM) si implementa Cloud Volumes ONTAP mediante la API y especifica el siguiente indicador:

```
skipSvmManagementLif: true
```

Equilibradores de carga internos

BlueXP crea automáticamente cuatro equilibradores de carga internos de Google Cloud (TCP/UDP) que gestionan el tráfico entrante para el par de alta disponibilidad de Cloud Volumes ONTAP. No es necesario configurar nada Hemos incluido esto como requisito simplemente para informarle del tráfico de red y para mitigar cualquier problema de seguridad.

Un equilibrador de carga se utiliza para la gestión del clúster, uno para la gestión de máquinas virtuales de almacenamiento (SVM), otro para el tráfico NAS al nodo 1 y, por último, para el tráfico NAS al nodo 2.

La configuración para cada equilibrador de carga es la siguiente:

- Una dirección IP privada compartida
- Una comprobación de estado global

  De manera predeterminada, los puertos que utiliza la comprobación del estado son 63001, 63002 y 63003.

- Un servicio de fondo TCP regional
- Un servicio de backend UDP regional
- Una regla de reenvío TCP
- Una regla de reenvío UDP
- El acceso global está desactivado

  Aunque el acceso global esté deshabilitado de forma predeterminada, se admite la habilitación de la tecnología posterior a la implementación. Lo hemos desactivado porque el tráfico de diferentes regiones tendrá latencias mucho más altas. Queríamos asegurarnos de que no disponías de una experiencia negativa debido a los montajes accidentales en varias regiones. Habilitar esta opción es específica para las necesidades de su negocio.

VPC compartidos

Cloud Volumes ONTAP y el conector son compatibles con un VPC compartido de Google Cloud y también en las VPC independientes.

Para un sistema de un solo nodo, el VPC puede ser un VPC compartido o un VPC independiente.

Para un par de alta disponibilidad, se necesitan cuatro VPC. Cada una de esas VPC puede ser compartida o independiente. Por ejemplo, VPC-0 podría ser un VPC compartido, mientras que VPC-1, VPC-2 y VPC-3 serían equipos virtuales independientes.

Un VPC compartido permite configurar y gestionar de forma centralizada las redes virtuales de varios proyectos. Puede configurar redes VPC compartidas en el *proyecto host* e implementar las instancias de máquina virtual de conector y Cloud Volumes ONTAP en un *proyecto de servicio*. "Documentación de Google Cloud: Información general sobre VPC compartido".

"Revisar los permisos de VPC compartido requeridos que se cubren en la implementación del conector"

Duplicación de paquetes en VPC

"Mirroring de paquetes" Debe desactivarse en la subred de Google Cloud en la que se implementa Cloud Volumes ONTAP. Cloud Volumes ONTAP no puede funcionar correctamente si está habilitado el mirroring de paquetes.

Acceso a Internet de salida

Cloud Volumes ONTAP requiere acceso saliente a Internet para AutoSupport de NetApp, que supervisa proactivamente el estado de su 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 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 firewall del conector permite 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 firewall de 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 utiliza un par de alta disponibilidad, el mediador de alta disponibilidad no requiere acceso saliente a Internet.

Si BlueXP notifica que los mensajes de AutoSupport no se pueden enviar, "Solucione problemas de configuración de AutoSupport".

Reglas del firewall

No necesita crear reglas de firewall porque BlueXP lo hace por usted. Si necesita utilizar el suyo propio, consulte las reglas de firewall que se enumeran a continuación.

Tenga en cuenta que se necesitan dos conjuntos de reglas de firewall para una configuración de alta disponibilidad:

- Un conjunto de reglas para los componentes de alta disponibilidad en VPC-0. Estas reglas permiten el acceso a Cloud Volumes ONTAP a los datos. Leer más.
- Otro conjunto de reglas para los componentes de alta disponibilidad en VPC-1, VPC-2 y VPC-3. Estas reglas están abiertas para la comunicación entrante y saliente entre los componentes ha. Leer más.

Si desea organizar en niveles datos inactivos en un bloque de Google Cloud Storage, debe configurarse la subred en la que resida Cloud Volumes ONTAP para Private Google Access (si utiliza una pareja de alta disponibilidad, esta es la subred en VPC-0). Para obtener instrucciones, consulte "Documentación de Google Cloud: Configuración de Private Google Access".

Para conocer los pasos adicionales necesarios para configurar la organización en niveles de datos en BlueXP, consulte "Organización en niveles de los datos inactivos en almacenamiento de objetos de bajo coste".

Conexiones a sistemas ONTAP en otras redes

Para replicar datos entre un sistema Cloud Volumes ONTAP en Google Cloud y sistemas ONTAP en otras redes, debe tener una conexión VPN entre el VPC y la otra red, por ejemplo, su red corporativa.

Para obtener instrucciones, consulte "Documentación de Google Cloud: Información general sobre Cloud VPN".

Reglas del firewall

BlueXP crea reglas de firewall de Google Cloud que incluyen las reglas entrantes y salientes que Cloud Volumes ONTAP necesita para funcionar correctamente. Puede que desee consultar los puertos para fines de prueba o si prefiere utilizar sus propias reglas de firewall.

Las reglas de firewall para Cloud Volumes ONTAP requieren reglas tanto entrantes como salientes. Si va a implementar una configuración de alta disponibilidad, estas son las reglas del firewall para Cloud Volumes ONTAP en VPC-0.

Tenga en cuenta que se necesitan dos conjuntos de reglas de firewall para una configuración de alta disponibilidad:

- Un conjunto de reglas para los componentes de alta disponibilidad en VPC-0. Estas reglas permiten el acceso a Cloud Volumes ONTAP a los datos.
- Otro conjunto de reglas para los componentes de alta disponibilidad en VPC-1, VPC-2 y VPC-3. Estas reglas están abiertas para la comunicación entrante y saliente entre los componentes ha. Leer más.

¿Busca información sobre el conector? "Ver reglas de firewall para el conector"

Reglas de entrada

Al crear un entorno de trabajo, puede elegir el filtro de origen para la directiva de firewall predefinida durante la implementación:

- **VPC seleccionado sólo**: El filtro de origen para el 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**: El filtro de fuente para el tráfico entrante es el rango IP 0.0.0.0/0.

Si utiliza su propia política de firewall, asegúrese de añadir todas las redes que necesitan comunicarse con Cloud Volumes ONTAP, pero también de agregar ambos rangos de direcciones para permitir que el equilibrador de carga de Google interno funcione correctamente. Estas direcciones son 130.211.0.0/22 y 35.191.0.0/16. Para obtener más información, consulte "Documentación de Google Cloud: Reglas de firewall de equilibrio de carga".

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

Protocolo	Puerto	Específico
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
TCP	63001-63050	Puertos de sonda de equilibrio de carga para determinar qué nodo está en buen estado (Solo para pares de alta disponibilidad)
UDP	111	Llamada a procedimiento remoto para NFS
UDP	161-162	Protocolo simple de gestión de red
UDP	635	Montaje NFS
UDP	2049	Daemon del servidor NFS
UDP	4045	Daemon de bloqueo NFS
UDP	4046	Supervisor de estado de red para NFS
UDP	4049	Protocolo rquotad NFS

Reglas de salida

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

Reglas de salida básicas

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

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

Reglas salientes avanzadas

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

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

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

Servicio	Protocolo	Puerto	Origen	Destino	Específico
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
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)
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
SNMP	TCP	161	LIF de gestión de nodos	Servidor de supervisión	Supervisión mediante capturas SNMP
	UDP	161	LIF de gestión de nodos	Servidor de supervisión	Supervisión mediante capturas SNMP
	TCP	162	LIF de gestión de nodos	Servidor de supervisión	Supervisión mediante capturas SNMP
	UDP	162	LIF de gestión de nodos	Servidor de supervisión	Supervisión mediante capturas SNMP

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

Reglas para VPC-1, VPC-2 y VPC-3

En Google Cloud, se pone en marcha una configuración de alta disponibilidad en cuatro PCs. Las reglas de firewall necesarias para la configuración de alta disponibilidad en VPC-0 son Anteriormente indicado para Cloud Volumes ONTAP.

Mientras tanto, las reglas de firewall predefinidas que BlueXP crea para instancias en VPC-1, VPC-2 y VPC-3 permiten la entrada de comunicación a través de protocolos y puertos *all*. Estas reglas permiten la comunicación entre los nodos de alta disponibilidad.

La comunicación de los nodos de alta disponibilidad al mediador de alta disponibilidad se realiza a través del puerto 3260 (iSCSI).

> Para permitir una alta velocidad de escritura para las nuevas puestas en marcha de parejas de alta disponibilidad de Google Cloud, se requiere una unidad de transmisión máxima (MTU) de al menos 8,896 bytes para VPC-1, VPC-2 y VPC-3. Si decide actualizar VPC-1, VPC-2 y VPC-3 existentes a un MTU de 8,896 bytes, deberá apagar todos los sistemas de alta disponibilidad existentes con estos VPC durante el proceso de configuración.

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 de firewall en Google Cloud"

Planificación de controles de servicio VPC en GCP

A la hora de optar por bloquear su entorno de Google Cloud con controles de servicio VPC, deberá comprender cómo interactúa BlueXP y Cloud Volumes ONTAP con las API de Google Cloud, así como cómo configurar su perímetro de servicios para poner en marcha BlueXP y Cloud Volumes ONTAP.

VPC Service Controls le permite controlar el acceso a servicios gestionados por Google fuera de un perímetro de confianza, para bloquear el acceso a los datos desde ubicaciones que no son de confianza y mitigar los riesgos de transferencia de datos no autorizados. "Más información acerca de los controles de servicio de Google Cloud VPC".

Cómo se comunican los servicios de NetApp con los controles de servicio VPC

BlueXP se comunica directamente con las API de Google Cloud. Esto se activa desde una dirección IP externa fuera de Google Cloud (por ejemplo, desde api.services.cloud.netapp.com) o dentro de Google Cloud desde una dirección interna asignada al conector BlueXP.

Dependiendo del estilo de despliegue del conector, es posible que haya que hacer ciertas excepciones para el perímetro de servicio.

Imágenes

Tanto Cloud Volumes ONTAP como BlueXP usan imágenes de un proyecto dentro de GCP que está gestionado por NetApp. Esto puede afectar la implementación del conector BlueXP y Cloud Volumes ONTAP, si su organización tiene una directiva que bloquea el uso de imágenes que no están alojadas dentro de la organización.

Puede poner en marcha un conector manualmente con el método de instalación manual, pero Cloud Volumes ONTAP también deberá extraer imágenes del proyecto de NetApp. Debe proporcionar una lista de permitidos para desplegar un conector y Cloud Volumes ONTAP.

Despliegue de un conector

El usuario que implementa un conector debe poder hacer referencia a una imagen alojada en el ProjectID *netapp-cloudManager* y el número de proyecto *14190056516*.

Implementar Cloud Volumes ONTAP

- La cuenta de servicio de BlueXP debe hacer referencia a una imagen alojada en el ProjectID *netapp-cloudManager* y al número de proyecto *14190056516* del proyecto de servicio.
- La cuenta de servicio del agente de servicio de API de Google predeterminado debe hacer referencia a una imagen alojada en el ProjectID *netapp-cloudManager* y el número de proyecto *14190056516* del proyecto de servicio.

A continuación se definen ejemplos de las reglas necesarias para extraer estas imágenes con los controles de servicio VPC.

El servicio VPC controla las políticas de perímetro

Las directivas permiten excepciones a los conjuntos de reglas de controles de servicio VPC. Para obtener más información acerca de las políticas, visite la "GCP VPC Service controla la documentación de las políticas".

Para establecer las directivas que requiere BlueXP, desplácese hasta el Perímetro de controles de servicio VPC de su organización y agregue las siguientes directivas. Los campos deben coincidir con las opciones dadas en la página de políticas controles de servicio VPC. Tenga también en cuenta que **todas las reglas** son necesarias y los parámetros **O** deben utilizarse en el conjunto de reglas.

Reglas de entrada

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Service Project]
    Services =
        Service name: iam.googleapis.com
          Service methods: All actions
        Service name: compute.googleapis.com
          Service methods:All actions
```

O.

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Host Project]
    Services =
        Service name: compute.googleapis.com
          Service methods: All actions
```

O.

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
    Source > All sources allowed
To:
    Projects =
        [Service Project]
        [Host Project]
    Services =
        Service name: compute.googleapis.com
        Service methods: All actions
```

Reglas de salida

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
To:
    Projects =
        14190056516
    Service =
        Service name: compute.googleapis.com
        Service methods: All actions
```

El número de proyecto descrito anteriormente es el proyecto *netapp-cloudManager* que utiliza NetApp para almacenar imágenes para Connector y Cloud Volumes ONTAP.

Crear una cuenta de servicio para la organización en niveles de datos y los backups

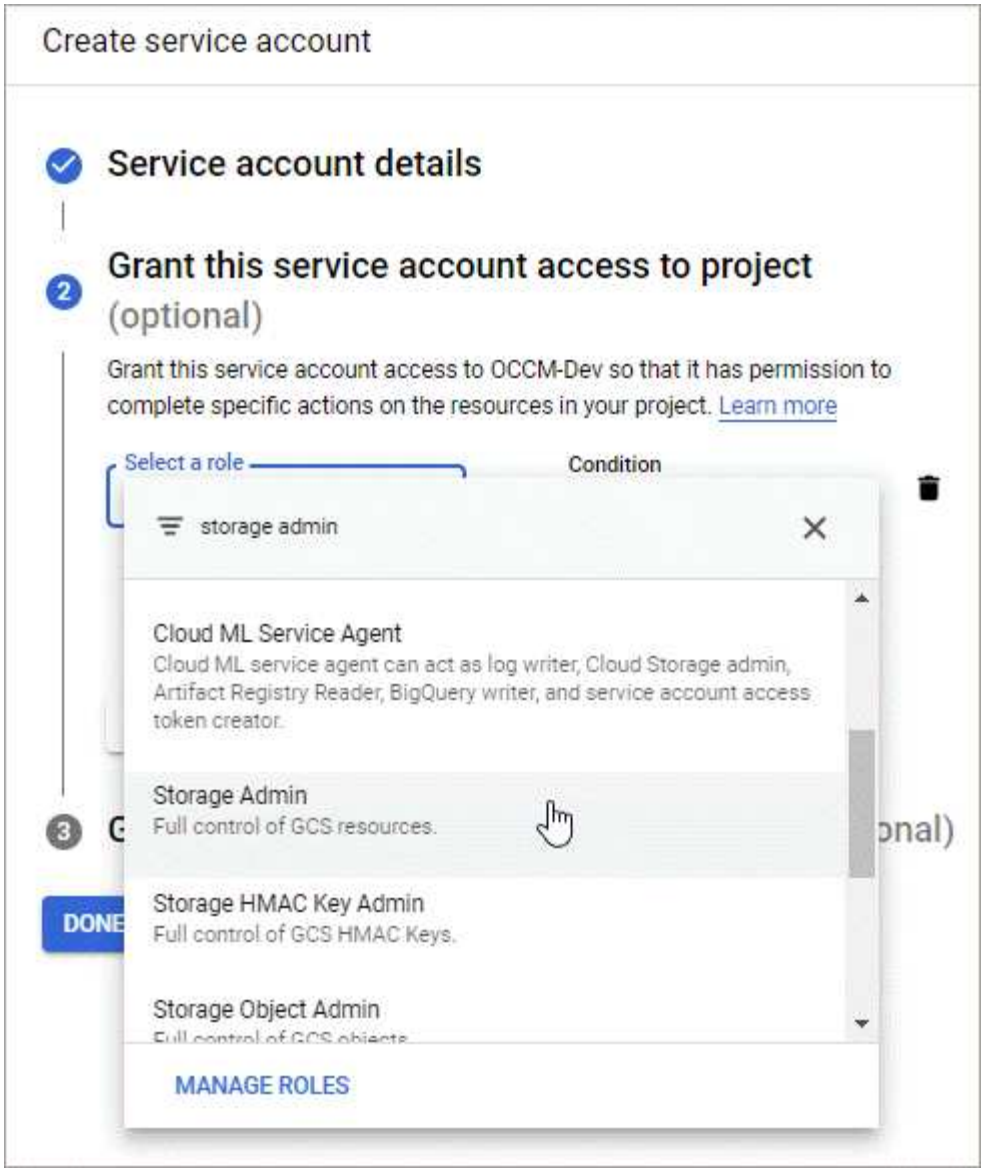
Cloud Volumes ONTAP requiere una cuenta de servicio de Google Cloud para dos finalidades. La primera es cuando se activa "organización en niveles de los datos" Para organizar los datos inactivos en niveles en almacenamiento de objetos de bajo coste en Google Cloud. La segunda es cuando se activa la "Backup y recuperación de BlueXP" para realizar backups de volúmenes en un almacenamiento de objetos de bajo coste.

Cloud Volumes ONTAP utiliza la cuenta de servicio para acceder a un bloque y gestionarlo para datos por niveles y otro bloque para backups.

Puede configurar una cuenta de servicio y utilizarla para ambos fines. La cuenta de servicio debe tener el rol **Administrador de almacenamiento**.

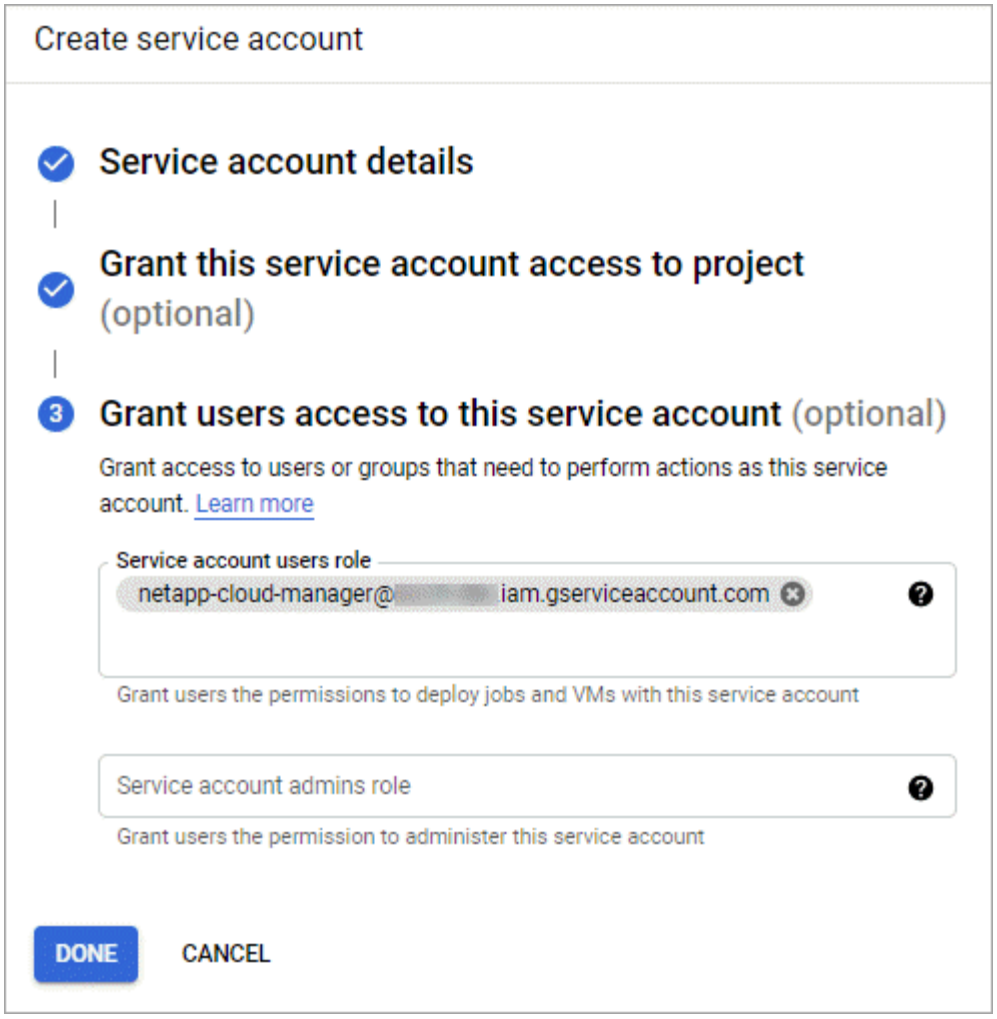
Pasos

1. En la consola de Google Cloud, "Vaya a la página de cuentas de servicio".
2. Seleccione el proyecto.
3. Haga clic en **Crear cuenta de servicio** y proporcione la información necesaria.
    a. **Detalles de la cuenta de servicio**: Introduzca un nombre y una descripción.
    b. **Conceder acceso a esta cuenta de servicio al proyecto**: Seleccione el rol **Administrador de almacenamiento**.



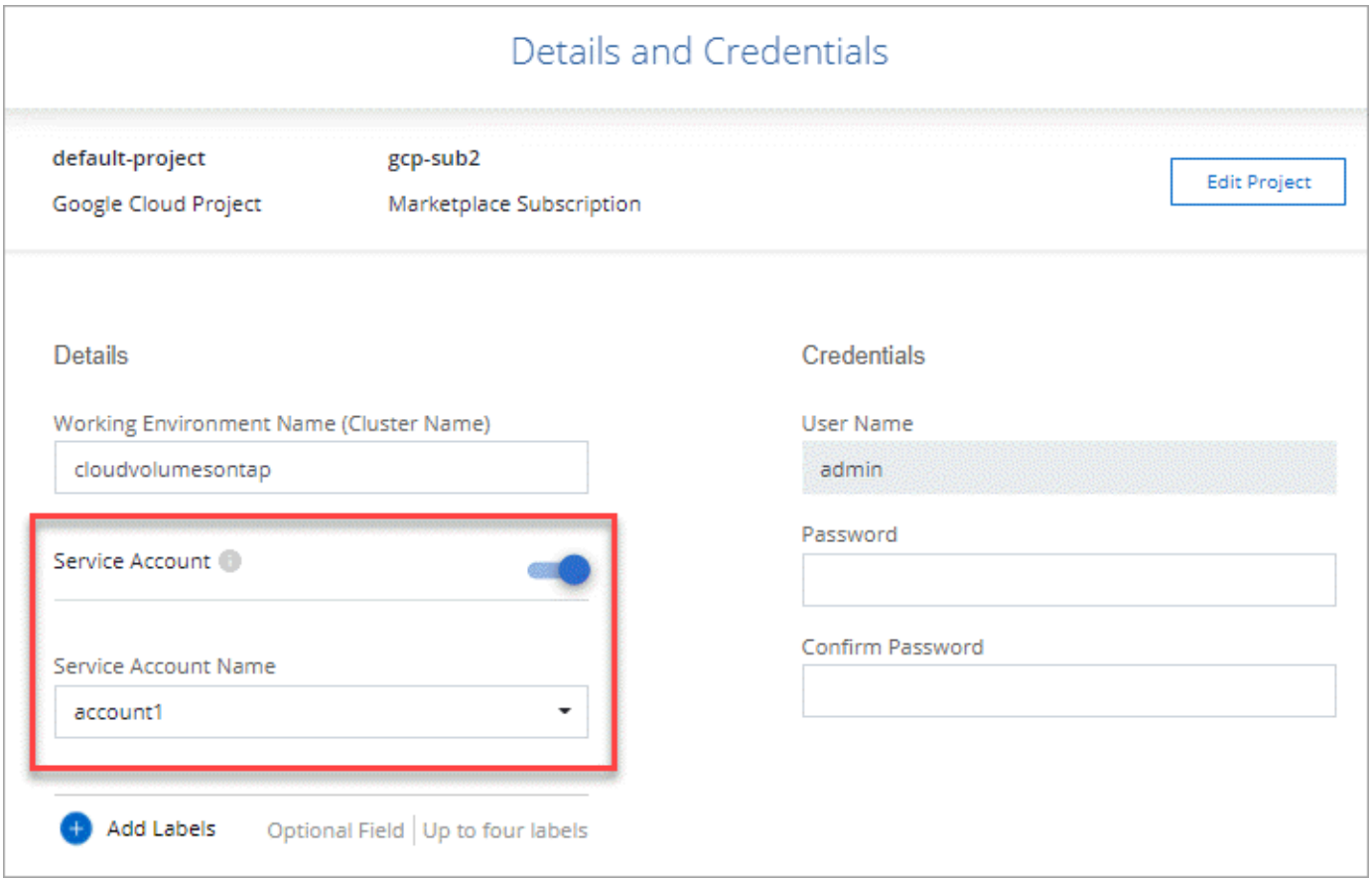
c. **Conceder a los usuarios acceso a esta cuenta de servicio**: Agregue la cuenta de servicio Connector como *Service Account User* a esta nueva cuenta de servicio.

   Este paso solo es necesario para la organización en niveles de datos. No es obligatorio para el backup y recuperación de BlueXP.



El futuro

Deberá seleccionar la cuenta de servicio más adelante al crear un entorno de trabajo de Cloud Volumes ONTAP.



Utiliza claves de cifrado gestionadas por el cliente con Cloud Volumes ONTAP

Mientras Google Cloud Storage siempre cifra sus datos antes de que se escriban en el disco, puede utilizar la API de BlueXP para crear un sistema Cloud Volumes ONTAP que utilice *claves de cifrado gestionadas por el cliente*. Estas son claves que genera y gestiona en GCP mediante el servicio Cloud Key Management Service.

Pasos

1. Asegúrese de que la cuenta de servicio de BlueXP Connector tiene los permisos correctos en el nivel de proyecto, en el proyecto en el que se almacena la clave.

   Los permisos se proporcionan en la "Permisos de cuenta de servicio de conector de forma predeterminada", Pero no se puede aplicar si utiliza un proyecto alternativo para el Servicio de administración de claves en la nube.

   Los permisos son los siguientes:

   ```
   - cloudkms.cryptoKeyVersions.useToEncrypt
   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.list
   ```

2. Asegúrese de que la cuenta de servicio de "Agente de servicio de Google Compute Engine" Tiene permisos cifrado/descifrado de Cloud KMS en la clave.

El nombre de la cuenta de servicio utiliza el siguiente formato: "Service-[Service_Project_Number]@compute-system.iam.gserviceaccount.com".

"Documentación de Google Cloud: Uso de IAM con Cloud KMS: Concesión de roles en un recurso"

3. Obtenga el "id" de la clave invocando el comando get para `/gcp/vsa/metadata/gcp-encryption-keys` Llame a la API o elija "Copy Resource Name" en la clave de la consola de GCP.
4. Si se utilizan claves de cifrado gestionadas por el cliente y los datos organizados en niveles en el almacenamiento de objetos, BlueXP intenta utilizar las mismas claves que se utilizan para cifrar los discos persistentes. Pero en primer lugar tendrá que habilitar las buckets de Google Cloud Storage para usar las claves:

   a. Busque el agente del servicio Google Cloud Storage en la siguiente "Documentación de Google Cloud: Obtener el agente del servicio de almacenamiento en cloud".

   b. Desplácese hasta la clave de cifrado y asigne el agente del servicio Google Cloud Storage con permisos cifrado/descifrado de Cloud KMS.

   Para obtener más información, consulte "Documentación de Google Cloud: Uso de claves de cifrado gestionadas por el cliente"

5. Utilice el parámetro "GcpEncryption" con la solicitud de API al crear un entorno de trabajo.

   ejemplo

```
"gcpEncryptionParameters": {
    "key": "projects/project-1/locations/us-east4/keyRings/keyring-1/cryptoKeys/generatedkey1"
  }
```

Consulte la "Documentos de automatización de BlueXP" Para obtener más detalles sobre el uso del parámetro "GcpEncryption".

Configure las licencias para Cloud Volumes ONTAP en Google Cloud

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

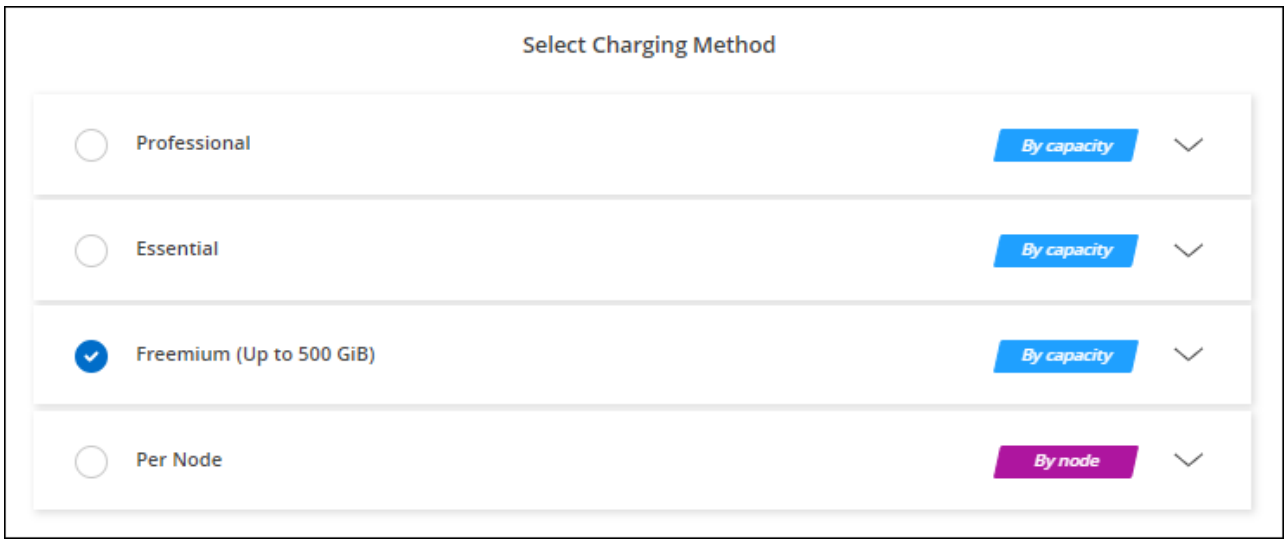
Seleccione la oferta freemium para utilizar Cloud Volumes ONTAP de forma gratuita con hasta 500 GIB de capacidad aprovisionada. "Obtenga más información sobre la oferta de Freemium".

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 Google Cloud Marketplace.

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".

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



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

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 Google Cloud Marketplace
- Un contrato anual

"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.

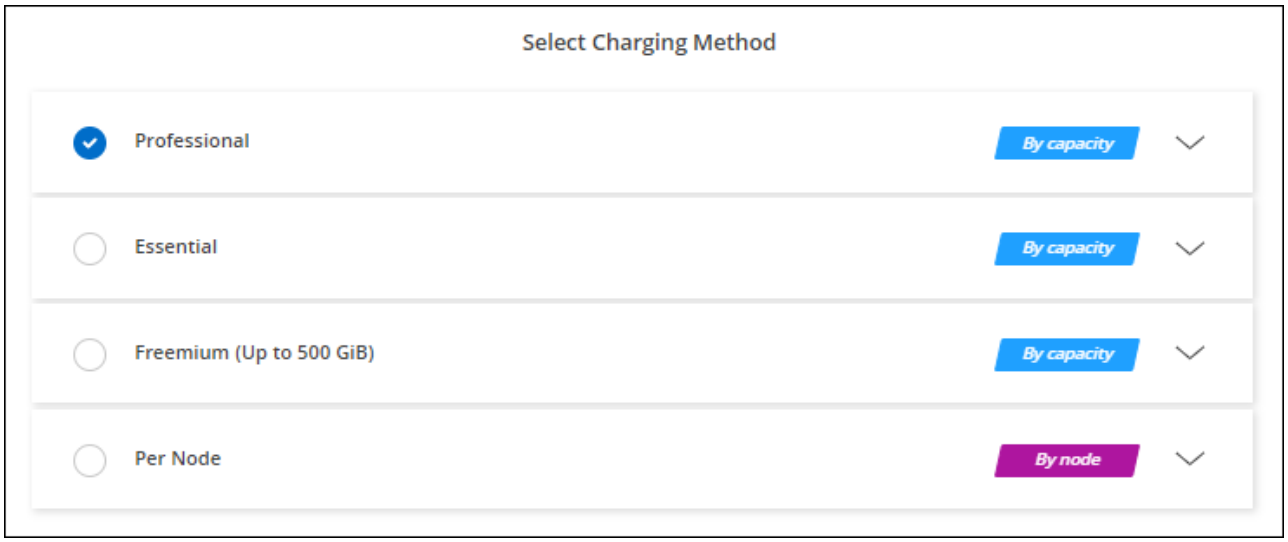
   Tu licencia debe estar disponible en la cartera digital de BlueXP para poder utilizarla con Cloud Volumes

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 Google Cloud Marketplace.

      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.

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



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

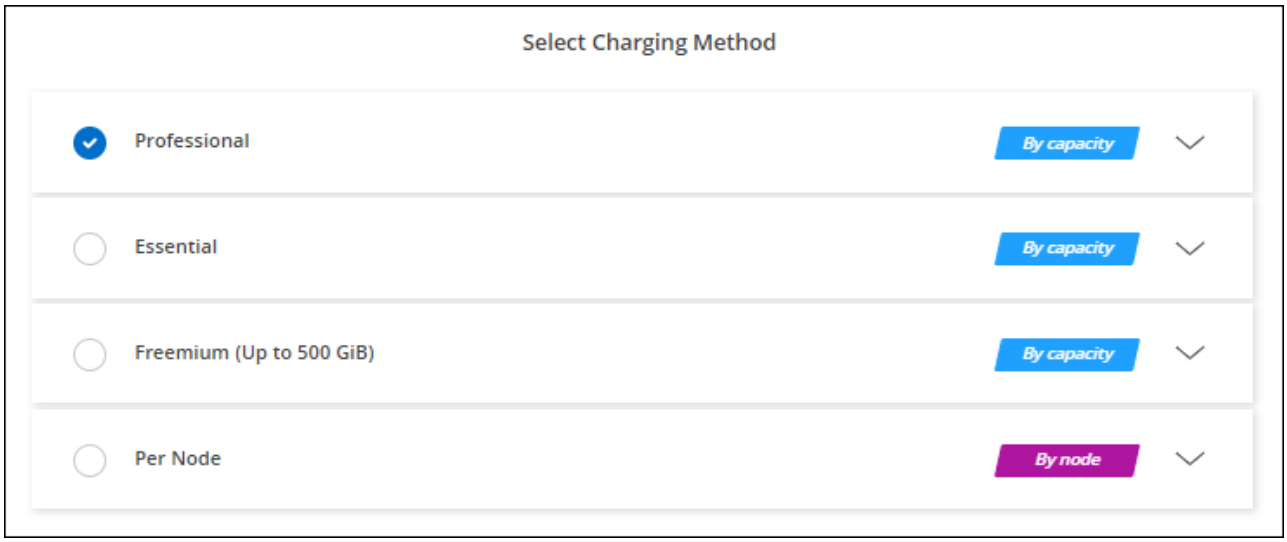
Suscripción a PAYGO

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 pide que se suscriba al acuerdo que está disponible en Google Cloud 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 Google Cloud Marketplace.
   b. Después de volver a BlueXP, seleccione un paquete basado en la capacidad cuando llegue a la página de métodos de carga.



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

Puede gestionar las suscripciones de Google Cloud Marketplace asociadas con sus cuentas en la página Configuración > credenciales. "Descubra cómo administrar sus credenciales y suscripciones a Google Cloud"

Contrato anual

Pague anualmente por Cloud Volumes ONTAP comprando un contrato anual.

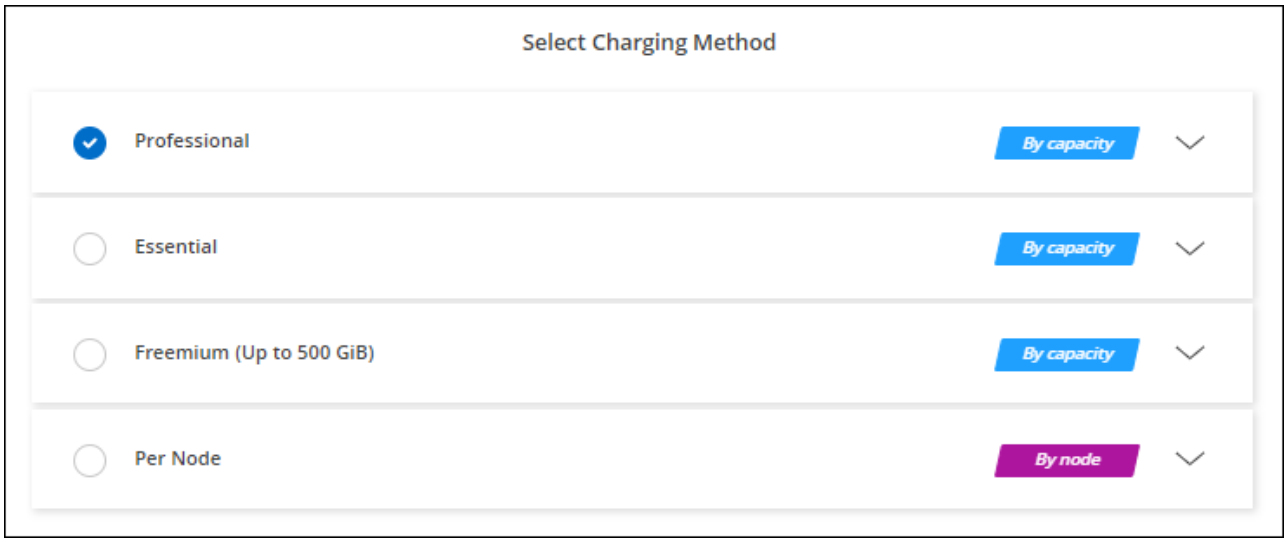
Pasos

1. Póngase en contacto con su representante de ventas de NetApp para adquirir un contrato anual.

   El contrato está disponible como una oferta *private* en Google Cloud Marketplace.

   Una vez que NetApp comparta la oferta privada con usted, podrá seleccionar el plan anual al suscribirse desde Google Cloud Marketplace durante la creación del entorno de trabajo.

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 al plan anual en Google Cloud Marketplace.
   b. En Google Cloud, seleccione el plan anual que se compartió con su cuenta y, a continuación, haga clic en **Suscribirse**.
   c. Después de volver a BlueXP, seleccione un paquete basado en la capacidad cuando llegue a la página de métodos de carga.



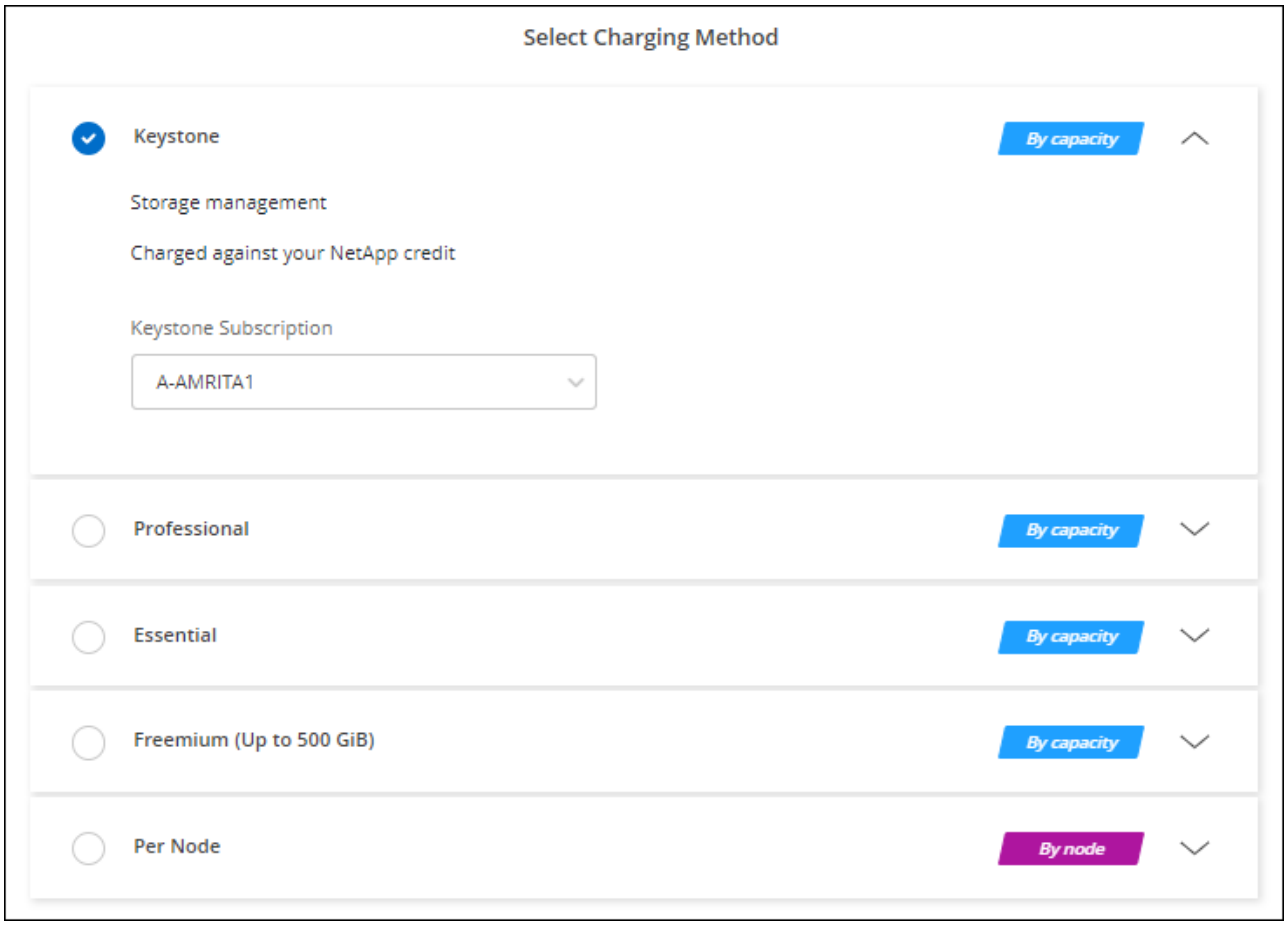
"Consulte las instrucciones paso a paso para iniciar Cloud Volumes ONTAP en Google Cloud".

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 las instrucciones paso a paso para iniciar Cloud Volumes ONTAP en Google Cloud".

Lanzamiento de Cloud Volumes ONTAP en Google Cloud

Puede iniciar Cloud Volumes ONTAP en una configuración de un solo nodo o como par de alta disponibilidad en Google Cloud.

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".
  - La cuenta de servicio asociada con el conector "debe tener los permisos necesarios"
- Descripción de la configuración que desea usar.

  Debe haberse preparado eligiendo una configuración y obteniendo de su administrador información de red de Google Cloud. 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".

- Deberían tener las API de Google Cloud "habilitado en el proyecto":
  - API de Cloud Deployment Manager V2
  - API de registro en la nube
  - API de Cloud Resource Manager
  - API del motor de computación
  - API de gestión de acceso e identidad (IAM)

Iniciar un sistema de un único nodo en Google Cloud

Cree un entorno de trabajo en BlueXP para ejecutar Cloud Volumes ONTAP en Google Cloud.

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 **Google Cloud** y **Cloud Volumes ONTAP**.
4. Si se le solicita, "Cree un conector".
5. **Detalles y credenciales**: Seleccione un proyecto, especifique un nombre de clúster, seleccione opcionalmente una cuenta de servicio, agregue etiquetas y especifique las credenciales.

   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 nombrar tanto al sistema Cloud Volumes ONTAP como a la instancia de Google Cloud VM. También utiliza el nombre como prefijo para el grupo de seguridad predefinido si selecciona esa opción.
Nombre de cuenta de servicio	Si tiene previsto utilizar "organización en niveles de los datos" o. "Backup y recuperación de BlueXP" Con Cloud Volumes ONTAP, tendrá que activar **cuenta de servicio** y seleccionar una cuenta de servicio que tenga la función de administrador de almacenamiento predefinido. "Aprenda a crear una cuenta de servicio".
Agregar etiquetas	Las etiquetas son metadatos para sus recursos de Google Cloud. BlueXP añade las etiquetas al sistema Cloud Volumes ONTAP y a los recursos de Google Cloud asociados al sistema. Puede añadir hasta cuatro etiquetas desde la interfaz de usuario al crear un entorno de trabajo y, después, puede agregar más. Tenga en cuenta que la API no le limita a cuatro etiquetas al crear un entorno de trabajo. Para obtener más información sobre las etiquetas, consulte "Documentación de Google Cloud: Etiquetado de recursos".
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.

Campo	Descripción
Editar proyecto	Seleccione el proyecto en el que desea que resida Cloud Volumes ONTAP. El proyecto predeterminado es el proyecto en el que reside BlueXP. Si no ve ningún proyecto adicional en la lista desplegable, aún no ha asociado la cuenta de servicio de BlueXP a otros proyectos. Vaya a la consola de Google Cloud, abra el servicio IAM y seleccione el proyecto. Agregue la cuenta de servicio con la función BlueXP a ese proyecto. Deberá repetir este paso con cada proyecto. Esta es la cuenta de servicio que configuró para BlueXP, "como se describe en esta página". Haga clic en **Agregar suscripción** para asociar las credenciales seleccionadas a una suscripción. Para crear un sistema de pago por uso Cloud Volumes ONTAP, debe seleccionar un proyecto de Google Cloud asociado con una suscripción a Cloud Volumes ONTAP desde Google Cloud Marketplace.

En el siguiente vídeo se muestra cómo asociar una suscripción a un mercado de pago por uso a su proyecto de Google Cloud. Como alternativa, siga los pasos para suscribirse ubicados en el "Asociación de una suscripción a Marketplace con credenciales de Google Cloud" sección.

Suscríbete a BlueXP desde Google Cloud Marketplace

6. **Servicios**: Seleccione los servicios que desea utilizar en este sistema. Para seleccionar el backup y la recuperación de datos de BlueXP o para utilizar la organización en niveles de BlueXP, debes haber especificado la cuenta de servicio en el paso 3.

   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**: Seleccione una ubicación, elija una política de firewall y confirme la conectividad de red al almacenamiento de Google Cloud para la organización en niveles de datos.

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

Campo	Descripción
Verificación de conectividad	Para organizar los datos inactivos en niveles en un bloque de Google Cloud Storage, la subred en la que resida Cloud Volumes ONTAP debe estar configurada para acceso privado a Google. Para obtener instrucciones, consulte "Documentación de Google Cloud: Configuración de Private Google Access".

Campo	Descripción
Política de firewall generada	Si deja que BlueXP genere la política de firewall para usted, debe elegir cómo permitirá el tráfico: • Si elige **VPC seleccionado sólo**, el filtro de origen para el 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 **todos los VPC**, el filtro de origen para el tráfico entrante es el intervalo IP 0.0.0.0/0.
Usar la política de firewall existente	Si utiliza una directiva de firewall existente, asegúrese de que incluye las reglas requeridas. Enlace: Learn acerca de las reglas de firewall para Cloud Volumes ONTAP.

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

   Si selecciona uno de los paquetes, solo tiene que especificar un volumen y, a continuación, revisar y aprobar la configuración.
10. **Licencia**: Cambie la versión de Cloud Volumes ONTAP según sea necesario y seleccione un tipo de máquina.

    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.
11. **Recursos de almacenamiento subyacentes**: Elija la configuración del agregado inicial: Un tipo de disco y el tamaño de cada disco.

    El tipo de disco es para el volumen inicial. Es posible seleccionar un tipo de disco diferente para volúmenes posteriores.

    El tamaño del disco es para todos los discos de la agrupación inicial y para cualquier agregado adicional que BlueXP cree cuando se utiliza la opción de aprovisionamiento simple. Puede crear agregados que utilicen un tamaño de disco diferente mediante la opción de asignación avanzada.

    Para obtener ayuda a elegir el tipo y el tamaño de disco, consulte "Ajusta el tamaño de tu sistema en Google Cloud".
12. **Flash Cache, velocidad de escritura y WORM**:

    a. Active **Flash Cache**, si lo desea.

A partir de Cloud Volumes ONTAP 9.13.1, *Flash Cache* se admite en los tipos de instancias n2-standard-16, n2-standard-32, n2-standard-48 y n2-standard-64. No es posible deshabilitar Flash Cache después de la implementación.

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

"Más información sobre la velocidad de escritura".

Alta velocidad de escritura y una unidad de transmisión máxima (MTU) más alta de 8.896 bytes están disponibles a través de la opción de velocidad de escritura * Alta *. Además, el MTU superior de 8,896 requiere la selección de VPC-1, VPC-2 y VPC-3 para la puesta en marcha. Para obtener más información sobre VPC-1, VPC-2 y VPC-3, consulte "Reglas para VPC-1, VPC-2 y VPC-3".

c. 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.

13. **Segmentación de datos en Google Cloud Platform**: Elija si desea activar la organización en niveles de datos en el agregado inicial, elija una clase de almacenamiento para los datos organizados por niveles y, a continuación, seleccione una cuenta de servicio con la función de administración de almacenamiento predefinida (necesaria para Cloud Volumes ONTAP 9.7 o posterior), O seleccione una cuenta de Google Cloud (necesaria para Cloud Volumes ONTAP 9.6).

Tenga en cuenta lo siguiente:

- BlueXP establece la cuenta de servicio en la instancia de Cloud Volumes ONTAP. Esta cuenta de servicio proporciona permisos para organizar los datos en niveles en un bloque de Google Cloud Storage. Asegúrese de agregar la cuenta de servicio Connector como usuario de la cuenta de servicio de organización en niveles; de lo contrario, no podrá seleccionarla en BlueXP
- Para obtener ayuda con la adición de una cuenta de Google Cloud, consulte "Configuración y adición de cuentas de Google Cloud para la organización en niveles de datos con 9.6".
- 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 los datos, puede habilitarla en agregados posteriores, pero tendrá que apagar el sistema y agregar una cuenta de servicio desde la consola de Google Cloud.

"Más información acerca de la organización en niveles de los datos".

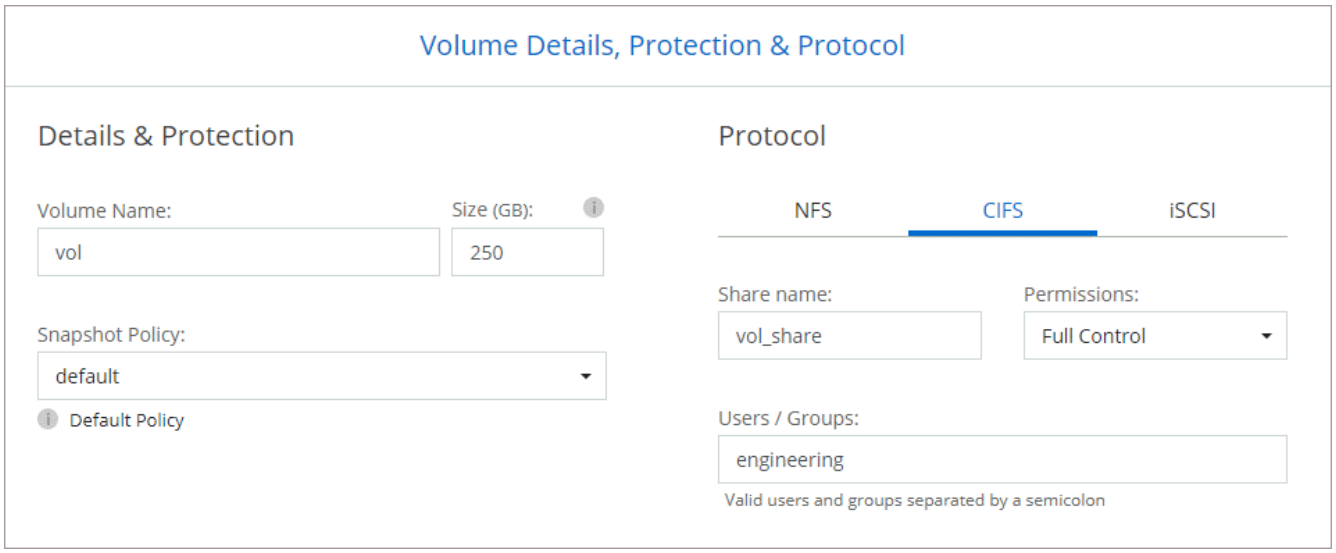
14. **Crear volumen**: Introduzca los detalles del nuevo volumen o haga clic en **Omitir**.

"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:



15. **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. Si está configurando Google Managed Active Directory, se puede acceder a AD de forma predeterminada con la dirección IP 169.254.169.254.
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. Para configurar Google Managed Microsoft AD como servidor AD para Cloud Volumes ONTAP, introduzca **OU=equipos,OU=Cloud** en este campo.https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Documentación de Google Cloud: Unidades organizativas de Google Managed Microsoft AD"^]
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.

Campo	Descripción
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.

16. **Perfil de uso, Tipo de disco y Directiva de organización en niveles**: Elija si desea activar las funciones de eficiencia del almacenamiento y cambiar 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".

17. **revisar y aprobar**: Revise y confirme sus selecciones.
    a. Consulte los detalles de la configuración.
    b. Haga clic en **más información** para revisar los detalles sobre el soporte técnico y los recursos de Google Cloud que BlueXP comprará.
    c. Active las casillas de verificación **comprendo…**.
    d. Haga clic en **Ir**.

Resultado

BlueXP despliega el sistema Cloud Volumes ONTAP. Puede realizar un seguimiento del progreso en la línea de tiempo.

Si tiene algún problema con la implementación del sistema 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.

Lanzamiento de una pareja de alta disponibilidad en Google Cloud

Cree un entorno de trabajo en BlueXP para ejecutar Cloud Volumes ONTAP en Google Cloud.

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 **Google Cloud** y **Cloud Volumes ONTAP ha**.
4. **Detalles y credenciales**: Seleccione un proyecto, especifique un nombre de clúster, seleccione

opcionalmente una cuenta de servicio, agregue etiquetas y especifique las credenciales.

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 nombrar tanto al sistema Cloud Volumes ONTAP como a la instancia de Google Cloud VM. También utiliza el nombre como prefijo para el grupo de seguridad predefinido si selecciona esa opción.
Nombre de cuenta de servicio	Si tiene pensado utilizar el "Organización en niveles de BlueXP" o. "Backup y recuperación de BlueXP" Servicios, debe activar el conmutador **cuenta de servicio** y, a continuación, seleccionar la cuenta de servicio que tenga la función Administrador de almacenamiento predefinida.
Agregar etiquetas	Las etiquetas son metadatos para sus recursos de Google Cloud. BlueXP añade las etiquetas al sistema Cloud Volumes ONTAP y a los recursos de Google Cloud asociados al sistema. Puede añadir hasta cuatro etiquetas desde la interfaz de usuario al crear un entorno de trabajo y, después, puede agregar más. Tenga en cuenta que la API no le limita a cuatro etiquetas al crear un entorno de trabajo. Para obtener más información sobre las etiquetas, consulte "Documentación de Google Cloud: Etiquetado de recursos".
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 proyecto	Seleccione el proyecto en el que desea que resida Cloud Volumes ONTAP. El proyecto predeterminado es el proyecto en el que reside BlueXP. Si no ve ningún proyecto adicional en la lista desplegable, aún no ha asociado la cuenta de servicio de BlueXP a otros proyectos. Vaya a la consola de Google Cloud, abra el servicio IAM y seleccione el proyecto. Agregue la cuenta de servicio con la función BlueXP a ese proyecto. Deberá repetir este paso con cada proyecto. Esta es la cuenta de servicio que configuró para BlueXP, "como se describe en esta página". Haga clic en **Agregar suscripción** para asociar las credenciales seleccionadas a una suscripción. Para crear un sistema de pago por uso Cloud Volumes ONTAP, debe seleccionar un proyecto de Google Cloud asociado con una suscripción a Cloud Volumes ONTAP desde Google Cloud Marketplace.

En el siguiente vídeo se muestra cómo asociar una suscripción a un mercado de pago por uso a su proyecto de Google Cloud. Como alternativa, siga los pasos para suscribirse ubicados en el "Asociación de una suscripción a Marketplace con credenciales de Google Cloud" sección.

Suscríbete a BlueXP desde Google Cloud Marketplace

5. **Servicios**: Seleccione los servicios que desea utilizar en este sistema. Para seleccionar el backup y la recuperación de datos de BlueXP o para utilizar BlueXP Tiering, debes haber especificado la cuenta de servicio en el paso 3.

   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 varias zonas (recomendado) o una sola zona para la configuración de alta disponibilidad. A continuación, seleccione una región y zonas.

   "Obtenga más información sobre los modelos de puesta en marcha de alta disponibilidad".

7. **conectividad**: Seleccione cuatro VPC diferentes para la configuración ha, una subred en cada VPC y, a continuación, elija una directiva de firewall.

   "Obtenga más información sobre los requisitos de red".

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

Campo	Descripción
Política generada	Si deja que BlueXP genere la política de firewall para usted, debe elegir cómo permitirá el tráfico: • Si elige **VPC seleccionado sólo**, el filtro de origen para el 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 **todos los VPC**, el filtro de origen para el tráfico entrante es el intervalo IP 0.0.0.0/0.
Utilice la 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. **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".
9. **Paquetes preconfigurados**: Seleccione uno de los paquetes para implementar rápidamente un sistema Cloud Volumes ONTAP, o haga clic en **Crear mi propia configuración**.

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

10. **Licencia**: Cambie la versión de Cloud Volumes ONTAP según sea necesario y seleccione un tipo de máquina.

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.

11. **Recursos de almacenamiento subyacentes**: Elija la configuración del agregado inicial: Un tipo de disco y el tamaño de cada disco.

    El tipo de disco es para el volumen inicial. Es posible seleccionar un tipo de disco diferente para volúmenes posteriores.

    El tamaño del disco es para todos los discos de la agrupación inicial y para cualquier agregado adicional que BlueXP cree cuando se utiliza la opción de aprovisionamiento simple. Puede crear agregados que utilicen un tamaño de disco diferente mediante la opción de asignación avanzada.

    Para obtener ayuda a elegir el tipo y el tamaño de disco, consulte "Ajusta el tamaño de tu sistema en Google Cloud".

12. **Flash Cache, velocidad de escritura y WORM**:

    a. Active **Flash Cache**, si lo desea.

    A partir de Cloud Volumes ONTAP 9.13.1, *Flash Cache* se admite en los tipos de instancias n2-standard-16, n2-standard-32, n2-standard-48 y n2-standard-64. No es posible deshabilitar Flash Cache después de la implementación.

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

    "Más información sobre la velocidad de escritura".

    Alta velocidad de escritura y una unidad de transmisión máxima (MTU) más alta de 8.896 bytes están disponibles a través de la opción de velocidad de escritura **Alta** con los tipos de instancia n2-standard-16, n2-standard-32, n2-standard-48 y n2-standard-64. Además, el MTU superior de 8,896 requiere la selección de VPC-1, VPC-2 y VPC-3 para la puesta en marcha. La alta velocidad de escritura y una MTU de 8.896 dependen de la función y no se pueden desactivar individualmente en una instancia configurada. Para obtener más información sobre VPC-1, VPC-2 y VPC-3, consulte "Reglas para VPC-1, VPC-2 y VPC-3".

    c. 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.

13. **Segmentación de datos en Google Cloud**: Elija si desea activar la organización en niveles de datos en el agregado inicial, elija una clase de almacenamiento para los datos organizados por niveles y, a continuación, seleccione una cuenta de servicio que tenga la función de administración de almacenamiento predefinida.

Tenga en cuenta lo siguiente:

- BlueXP establece la cuenta de servicio en la instancia de Cloud Volumes ONTAP. Esta cuenta de servicio proporciona permisos para organizar los datos en niveles en un bloque de Google Cloud Storage. Asegúrese de agregar la cuenta de servicio Connector como usuario de la cuenta de servicio de organización en niveles; de lo contrario, no podrá seleccionarla en BlueXP.
- 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 los datos, puede habilitarla en agregados posteriores, pero tendrá que apagar el sistema y agregar una cuenta de servicio desde la consola de Google Cloud.

  "Más información acerca de la organización en niveles de los datos".

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

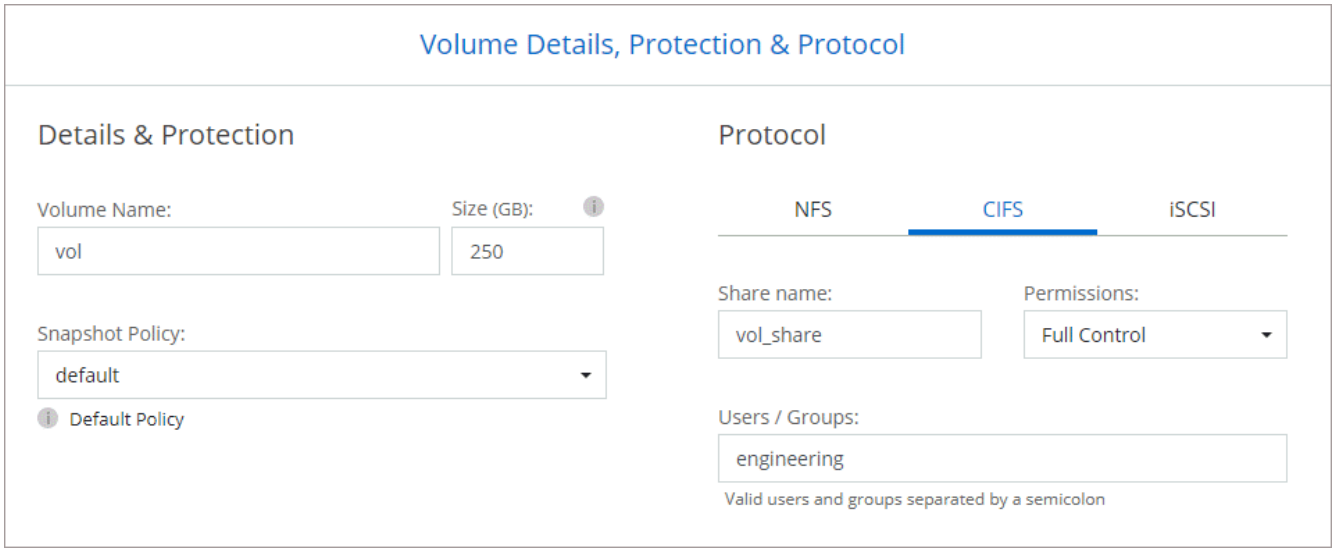
    "Obtenga información sobre las versiones y los protocolos de cliente compatibles".

    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.

Campo	Descripción
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:



15. **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. Si está configurando Google Managed Active Directory, se puede acceder a AD de forma predeterminada con la dirección IP 169.254.169.254.
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.

Campo	Descripción
Unidad organizacional	La unidad organizativa del dominio AD para asociarla con el servidor CIFS. El valor predeterminado es CN=Computers. Para configurar Google Managed Microsoft AD como servidor AD para Cloud Volumes ONTAP, introduzca **OU=equipos,OU=Cloud** en este campo.https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Documentación de Google Cloud: Unidades organizativas de Google Managed Microsoft AD"^]
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.

16. **Perfil de uso, Tipo de disco y Directiva de organización en niveles**: Elija si desea activar las funciones de eficiencia del almacenamiento y cambiar 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".

17. **revisar y aprobar**: Revise y confirme sus selecciones.
    a. Consulte los detalles de la configuración.
    b. Haga clic en **más información** para revisar los detalles sobre el soporte técnico y los recursos de Google Cloud que BlueXP comprará.
    c. Active las casillas de verificación **comprendo…**.
    d. Haga clic en **Ir**.

Resultado

BlueXP despliega el sistema Cloud Volumes ONTAP. Puede realizar un seguimiento del progreso en la línea de tiempo.

Si tiene algún problema con la implementación del sistema 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.

Verificación de imágenes de Google Cloud Platform

Información general de verificación de imágenes de Google Cloud

La verificación de imágenes de Google Cloud cumple con los requisitos de seguridad mejorados de NetApp. Se han realizado cambios en la secuencia de comandos que generan las imágenes para firmar la imagen en la forma en que se utilizan claves privadas generadas específicamente para esta tarea. Puede verificar la integridad de la imagen de GCP utilizando el resumen firmado y el certificado público de Google Cloud, que se puede descargar a través de "NSS" para una versión específica.

La verificación de Google Cloud Image es compatible con la versión 9.13.0 o posterior del software Cloud Volumes ONTAP.

Convierta la imagen al formato sin formato en Google Cloud

La imagen que se utilizará para implementar nuevas instancias, actualizaciones o utilizarse en imágenes existentes se compartirá con los clientes a través de "El sitio de soporte de NetApp (NSS)". El resumen firmado y los certificados se podrán descargar a través del portal de NSS. Asegúrese de descargar el resumen y los certificados de la versión correcta que corresponde a la imagen compartida por el soporte de NetApp. Por ejemplo, 9.13.0 imágenes tendrán un resumen firmado de 9.13.0 y certificados disponibles en NSS.

¿Por qué es necesario este paso?

Las imágenes de Google Cloud no se pueden descargar directamente. Para verificar la imagen frente al resumen firmado y los certificados, es necesario contar con un mecanismo para comparar los dos archivos y descargar la imagen. Para ello, debe exportar o convertir la imagen en un formato disk.raw y guardar los resultados en un bloque de almacenamiento en Google Cloud. El archivo disk.raw es tarred y gzip en el proceso.

El usuario/cuenta de servicio necesitará privilegios para realizar lo siguiente:

- Acceso a bucket de almacenamiento de Google
- Escribir en Google Storage bucket
- Creación de trabajos de creación de cloud (que se usan durante el proceso de exportación)
- Acceso a la imagen deseada
- Cree tareas de exportación de imágenes

Para verificar la imagen, debe convertirse a un formato disk.RAW y, a continuación, descargarse.

Utilice la línea de comandos de Google Cloud para exportar imagen de Google Cloud

La forma preferida de exportar una imagen al almacenamiento en cloud es utilizar la "comando de exportación de imágenes de computación gcloud". Este comando toma la imagen proporcionada y la convierte en un archivo disk.raw que se consigue tarred y gzip. El archivo generado se guarda en la URL de destino y puede descargarse para su verificación.

El usuario/cuenta debe tener privilegios para acceder y escribir en el bloque deseado, exportar la imagen y crear la nube (utilizados por Google para exportar la imagen) para ejecutar esta operación.

Exportar imagen de Google Cloud mediante gcloud

Haga clic para mostrar

```
$ gcloud compute images export \
    --destination-uri DESTINATION_URI \
    --image IMAGE_NAME

# For our example:
$ gcloud compute images export \
    --destination-uri gs://vsa-dev-bucket1/example-user-exportimage-
gcp-demo \
    --image example-user-20230120115139


## DEMO ##
# Step 1 - Optional: Checking access and listing objects in the
destination bucket
$ gsutil ls gs://example-user-export-image-bucket/

# Step 2 - Exporting the desired image to the bucket
$ gcloud compute images export --image example-user-export-image-demo
--destination-uri gs://example-user-export-image-bucket/export-
demo.tar.gz
Created [https://cloudbuild.googleapis.com/v1/projects/example-demo-
project/locations/us-central1/builds/xxxxxxxxxxxx].
Logs are available at [https://console.cloud.google.com/cloud-
build/builds;region=us-central1/xxxxxxxxxxxx?project=xxxxxxxxxxxx].
[image-export]: 2023-01-25T18:13:48Z Fetching image "example-user-
export-image-demo" from project "example-demo-project".
[image-export]: 2023-01-25T18:13:49Z Validating workflow
[image-export]: 2023-01-25T18:13:49Z Validating step "setup-disks"
[image-export]: 2023-01-25T18:13:49Z Validating step "image-export-
export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "setup-disks"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "run-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "wait-for-inst-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "copy-image-object"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "delete-inst"
[image-export]: 2023-01-25T18:13:51Z Validation Complete
[image-export]: 2023-01-25T18:13:51Z Workflow Project: example-demo-
project
[image-export]: 2023-01-25T18:13:51Z Workflow Zone: us-central1-c
```

```
[image-export]: 2023-01-25T18:13:51Z Workflow GCSPath: gs://example-
demo-project-example-bkt-us/
[image-export]: 2023-01-25T18:13:51Z Example scratch path:
https://console.cloud.google.com/storage/browser/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px
[image-export]: 2023-01-25T18:13:51Z Uploading sources
[image-export]: 2023-01-25T18:13:51Z Running workflow
[image-export]: 2023-01-25T18:13:51Z Running step "setup-disks"
(CreateDisks)
[image-export.setup-disks]: 2023-01-25T18:13:51Z CreateDisks: Creating
disk "disk-image-export-image-export-r88px".
[image-export]: 2023-01-25T18:14:02Z Step "setup-disks" (CreateDisks)
successfully finished.
[image-export]: 2023-01-25T18:14:02Z Running step "image-export-export-
disk" (IncludeWorkflow)
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "setup-disks" (CreateDisks)
[image-export.image-export-export-disk.setup-disks]: 2023-01-
25T18:14:02Z CreateDisks: Creating disk "disk-image-export-export-disk-
image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Step
"setup-disks" (CreateDisks) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "run-image-export-export-disk" (CreateInstances)
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:02Z CreateInstances: Creating instance "inst-image-
export-export-disk-image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Step
"run-image-export-export-disk" (CreateInstances) successfully finished.
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:08Z CreateInstances: Streaming instance "inst-image-
export-export-disk-image-export-image-export--r88px" serial port 1
output to https://storage.cloud.google.com/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px/logs/inst-
image-export-export-disk-image-export-image-export--r88px-serial-
port1.log
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Running
step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:08Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
watching serial port 1, SuccessMatch: "ExportSuccess", FailureMatch:
["ExportFailed:"] (this is not an error), StatusMatch: "GCEExport:".
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
```

```
StatusMatch found: "GCEExport: <serial-output key:'source-size-gb'
value:'10'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Running export tool."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Disk /dev/sdb is 10 GiB, compressed size
will most likely be much smaller."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Beginning export process..."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Copying \"/dev/sdb\" to gs://example-
demo-project-example-bkt-us/example-image-export-20230125-18:13:49-
r88px/outs/image-export-export-disk.tar.gz."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Using \"/root/upload\" as the buffer
prefix, 1.0 GiB as the buffer size, and 4 as the number of workers."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Creating gzipped image of \"/dev/sdb\"."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 1.0 GiB of 10 GiB (212 MiB/sec),
total written size: 992 MiB (198 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:59Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 8.0 GiB of 10 GiB (237 MiB/sec),
total written size: 1.5 GiB (17 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished creating gzipped image of
\"/dev/sdb\" in 48.956433327s [213 MiB/s] with a compression ratio of
6."
```

```
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished export in  48.957347731s"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: <serial-output key:'target-size-gb'
value:'2'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
SuccessMatch found "ExportSuccess"
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "copy-image-object" (CopyGCSObjects)
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "delete-inst" (DeleteResources)
[image-export.image-export-export-disk.delete-inst]: 2023-01-
25T18:15:19Z DeleteResources: Deleting instance "inst-image-export-
export-disk".
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"copy-image-object" (CopyGCSObjects) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:34Z Step
"delete-inst" (DeleteResources) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Step "image-export-export-disk"
(IncludeWorkflow) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> source-
size-gb:10
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> target-
size-gb:2
[image-export]: 2023-01-25T18:15:34Z Workflow "image-export" cleaning
up (this may take up to 2 minutes).
[image-export]: 2023-01-25T18:15:35Z Workflow "image-export" finished
cleanup.

# Step 3 - Validating the image was successfully exported
$ gsutil ls gs://example-user-export-image-bucket/
gs://example-user-export-image-bucket/export-demo.tar.gz


# Step 4 - Download the exported image
$ gcloud storage cp gs://BUCKET_NAME/OBJECT_NAME SAVE_TO_LOCATION
```

```
$ gcloud storage cp gs://example-user-export-image-bucket/export-
demo.tar.gz CVO_GCP_Signed_Digest.tar.gz
Copying gs://example-user-export-image-bucket/export-demo.tar.gz to
file://CVO_GCP_Signed_Digest.tar.gz
  Completed files 1/1 | 1.5GiB/1.5GiB | 185.0MiB/s

Average throughput: 213.3MiB/s
$ ls -l
total 1565036
-rw-r--r-- 1 example-user example-user 1602589949 Jan 25 18:44
CVO_GCP_Signed_Digest.tar.gz
```

Extraer archivos comprimidos

```
# Extracting files from the digest
$ tar -xf CVO_GCP_Signed_Digest.tar.gz
```

Consulte "Documento de Google Cloud sobre la exportación de una imagen" Para obtener más información sobre cómo exportar una imagen a través de Google Cloud.

Verificación de la firma de la imagen

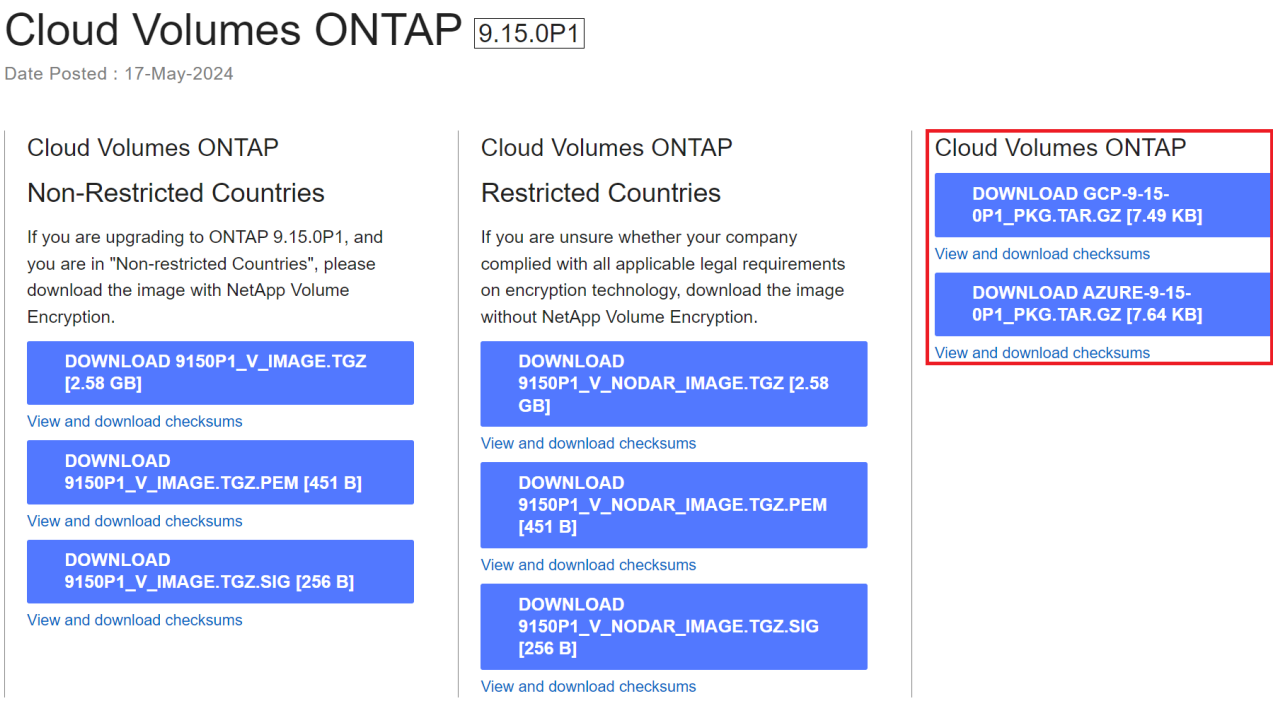
Compruebe las imágenes firmadas de Google Cloud

Para verificar la imagen firmada de Google Cloud exportada, debe descargar el archivo de resumen de imágenes del NSS para validar el archivo disk.raw y el contenido del archivo de resumen.

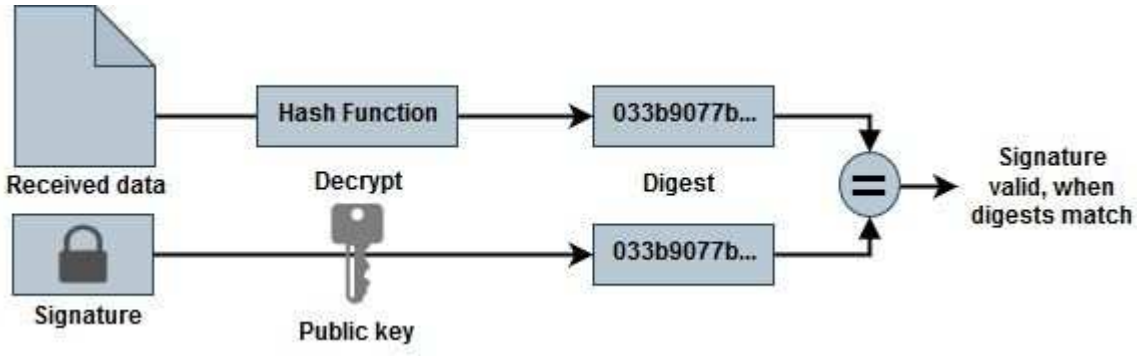
Resumen del flujo de trabajo de verificación de imagen firmada

A continuación se ofrece una descripción general del proceso de flujo de trabajo de verificación de imágenes firmadas de Google Cloud.

- Desde la "NSS", Descargue el archivo de Google Cloud que contiene los siguientes archivos:
  - Resumen firmado (.sig)
  - Certificado que contiene la clave pública (.pem)
  - Cadena de certificados (.pem)



- Descargue el archivo disk.raw convertido
- Validar el certificado mediante la cadena de certificados
- Validar el resumen firmado con el certificado que contiene la clave pública
  - Descifre el resumen firmado con la clave pública para extraer el resumen del archivo de imagen
  - Cree un resumen del archivo disk.raw descargado
  - Compare el archivo de dos resúmenes para su validación



Verificación del archivo disk.raw y digiere el contenido de los archivos con OpenSSL

Puede verificar el archivo disk.RAW descargado de Google Cloud con el contenido del archivo digest disponible en la "NSS" Uso de OpenSSL.

Los comandos OpenSSL para validar la imagen son compatibles con equipos Linux, Mac OS y Windows.

Pasos

1. Verifique el certificado con OpenSSL.

Haga clic para mostrar

```
# Step 1 - Optional, but recommended: Verify the certificate using
OpenSSL

# Step 1.1 - Copy the Certificate and certificate chain to a
directory
$ openssl version
LibreSSL 3.3.6
$ ls -l
total 48
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem

# Step 1.2 - Get the OSCP URL
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in <Certificate-
Chain.pem>)
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem)
$ echo $oscp_url
http://ocsp.entrust.net

# Step 1.3 - Generate an OCSP request for the certificate
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -reqout <request.der>
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem -reqout req.der

# Step 1.4 - Optional: Check the new file "req.der" has been
generated
$ ls -l
total 56
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der

# Step 1.5 - Connect to the OCSP Manager using openssl to send the
OCSP request
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -url ${ocsp_url} -resp_text
-respout <response.der>
```

```
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem  -url ${ocsp_url} -resp_text
-respout resp.der
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2
    Produced At: Jan 19 15:14:00 2023 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A
      Issuer Key Hash: CE894F8251AA15A28462CA312361D261FBF8FE78
      Serial Number: 5994B3D01D26D594BD1D0FA7098C6FF5
    Cert Status: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

    Signature Algorithm: sha512WithRSAEncryption
         0b:b6:61:e4:03:5f:98:6f:10:1c:9a:f7:5f:6f:c7:e3:f4:72:
         f2:30:f4:86:88:9a:b9:ba:1e:d6:f6:47:af:dc:ea:e4:cd:31:
         af:e3:7a:20:35:9e:60:db:28:9c:7f:2e:17:7b:a5:11:40:4f:
         1e:72:f7:f8:ef:e3:23:43:1b:bb:28:1a:6f:c6:9c:c5:0c:14:
         d3:5d:bd:9b:6b:28:fb:94:5e:8a:ef:40:20:72:a4:41:df:55:
         cf:f3:db:1b:39:e0:30:63:c9:c7:1f:38:7e:7f:ec:f4:25:7b:
         1e:95:4c:70:6c:83:17:c3:db:b2:47:e1:38:53:ee:0a:55:c0:
         15:6a:82:20:b2:ea:59:eb:9c:ea:7e:97:aa:50:d7:bc:28:60:
         8c:d4:21:92:1c:13:19:b4:e0:66:cb:59:ed:2e:f8:dc:7b:49:
         e3:40:f2:b6:dc:d7:2d:2e:dd:21:82:07:bb:3a:55:99:f7:59:
         5d:4a:4d:ca:e7:8f:1c:d3:9a:3f:17:7b:7a:c4:57:b2:57:a8:
         b4:c0:a5:02:bd:59:9c:50:32:ff:16:b1:65:3a:9c:8c:70:3b:
         9e:be:bc:4f:f9:86:97:b1:62:3c:b2:a9:46:08:be:6b:1b:3c:
         24:14:59:28:c6:ae:e8:d5:64:b2:f8:cc:28:24:5c:b2:c8:d8:
         5a:af:9d:55:48:96:f6:3e:c6:bf:a6:0c:a4:c0:ab:d6:57:03:
         2b:72:43:b0:6a:9f:52:ef:43:bb:14:6a:ce:66:cc:6c:4e:66:
         17:20:a3:64:e0:c6:d1:82:0a:d7:41:8a:cc:17:fd:21:b5:c6:
         d2:3a:af:55:2e:2a:b8:c7:21:41:69:e1:44:ab:a1:dd:df:6d:
         15:99:90:cc:a0:74:1e:e5:2e:07:3f:50:e6:72:a6:b9:ae:fc:
         44:15:eb:81:3d:1a:f8:17:b6:0b:ff:05:76:9d:30:06:40:72:
         cf:d5:c4:6f:8b:c9:14:76:09:6b:3d:6a:70:2c:5a:c4:51:92:
         e5:cd:84:b6:f9:d9:d5:bc:8d:72:b7:7c:13:9c:41:89:a8:97:
         6f:4a:11:5f:8f:b6:c9:b5:df:00:7e:97:20:e7:29:2e:2b:12:
         77:dc:e2:63:48:87:42:49:1d:fc:d0:94:a8:8d:18:f9:07:85:
```

```
         e4:d0:3e:9a:4a:d7:d5:d0:02:51:c3:51:1c:73:12:96:2d:75:
         22:83:a6:70:5a:4a:2b:f2:98:d9:ae:1b:57:53:3d:3b:58:82:
         38:fc:fa:cb:57:43:3f:3e:7e:e0:6d:5b:d6:fc:67:7e:07:7e:
         fb:a3:76:43:26:8f:d1:42:d6:a6:33:4e:9e:e0:a0:51:b4:c4:
         bc:e3:10:0d:bf:23:6c:4b
WARNING: no nonce in response
Response Verify OK
Certificate-GCP-CVO-20230119-0XXXXX.pem: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

# Step 1.5 - Optional: Check the response file "response.der" has
been generated. Verify its contents.
$ ls -l
total 64
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der
-rw-r--r--  1 example-user  engr   806 Jan 19 16:51 resp.der

# Step 1.6 - Verify the chain of trust and expiration dates against
the local host
$ openssl version -d
OPENSSLDIR: "/private/etc/ssl"
$ OPENSSLDIR=$(openssl version -d | cut -d '"' -f2)
$ echo $OPENSSLDIR
/private/etc/ssl

$ openssl verify -untrusted <Certificate-Chain.pem> -CApath <OpenSSL
dir> <Certificate.pem>
$ openssl verify -untrusted Certificate-Chain-GCP-CVO-20230119-
0XXXXX.pem -CApath ${OPENSSLDIR} Certificate-GCP-CVO-20230119-
0XXXXX.pem
Certificate-GCP-CVO-20230119-0XXXXX.pem: OK
```

2. Coloque el archivo disk.raw descargado, la firma y los certificados en un directorio.
3. Extraiga la clave pública del certificado utilizando OpenSSL.
4. Descifre la firma con la clave pública extraída y compruebe el contenido del archivo disk.raw descargado.

Haga clic para mostrar

```
# Step 1 - Place the downloaded disk.raw, the signature and the
certificates in a directory
$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 2 - Extract the public key from the certificate
$ openssl x509 -pubkey -noout -in (certificate.pem) >
(public_key.pem)
$ openssl x509 -pubkey -noout -in Certificate-GCP-CVO-20230119-
0XXXXX.pem > CVO-GCP-pubkey.pem

$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 17:02 CVO-GCP-pubkey.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 3 - Decrypt the signature using the extracted public key and
verify the contents of the downloaded disk.raw
$ openssl dgst -verify (public_key) -keyform PEM -sha256 -signature
(signed digest) -binary (downloaded or obtained disk.raw)
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary disk.raw
Verified OK

# A failed response would look like this
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary
../sample_file.txt
Verification Failure
```