Empezar

Cloud Volumes ONTAP

NetApp
February 13, 2026

Tabla de contenidos

Empezar

Obtenga más información sobre Cloud Volumes ONTAP

Cloud Volumes ONTAP le permite optimizar los costos y el rendimiento de su almacenamiento en la nube al tiempo que mejora la protección, la seguridad y el cumplimiento de los datos.

Cloud Volumes ONTAP es un dispositivo de almacenamiento de solo software que ejecuta el software de gestión de datos ONTAP en la nube. Proporciona almacenamiento de nivel empresarial con las siguientes características clave:

- Eficiencias de almacenamiento

  Aproveche la deduplicación de datos integrada, la compresión de datos, el aprovisionamiento fino y la clonación para minimizar los costos de almacenamiento.

- Alta disponibilidad

  Garantice la confiabilidad empresarial y las operaciones continuas en caso de fallas en su entorno de nube.

- Protección de datos

  Cloud Volumes ONTAP aprovecha SnapMirror, la tecnología de replicación líder en la industria de NetApp, para replicar datos locales en la nube, de modo que sea fácil tener copias secundarias disponibles para múltiples casos de uso.

  Cloud Volumes ONTAP también se integra con NetApp Backup and Recovery para brindar capacidades de respaldo y restauración para protección y archivo a largo plazo de sus datos en la nube.

  "Obtenga más información sobre copias de seguridad y recuperación"

- Nivelación de datos

  Cambie entre grupos de almacenamiento de alto y bajo rendimiento a pedido sin desconectar las aplicaciones.

- Consistencia de la aplicación

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

  "Obtenga más información sobre SnapCenter"

- Seguridad de datos

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

- Controles de cumplimiento de la privacidad

  La integración con NetApp Data Classification le ayuda a comprender el contexto de los datos e identificar datos confidenciales.

  "Obtenga más información sobre la clasificación de datos"

Las licencias para las funciones de ONTAP están incluidas con Cloud Volumes ONTAP.

"Ver configuraciones compatibles con Cloud Volumes ONTAP"

"Obtenga más información sobre Cloud Volumes ONTAP"

Versiones de ONTAP compatibles con implementaciones de Cloud Volumes ONTAP

La NetApp Console le permite elegir entre varias versiones diferentes de ONTAP cuando agrega un sistema Cloud Volumes ONTAP .

Las versiones de Cloud Volumes ONTAP distintas de las enumeradas aquí no están disponibles para nuevas implementaciones. El parche o la versión genérica (General Availability) en una versión aquí representa la versión base disponible para la implementación. Para detalles sobre los parches disponibles, consulta el "notas de la versión con control de versiones" de cada versión.

Para información sobre la actualización, consulta "Rutas de actualización admitidas".

AWS

Nodo único

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9,8
- 9.7 P5
- 9.5 P6

par HA

- 9.18.1

- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9,8
- 9.7 P5
- 9.5 P6

Azur

Nodo único

- 9.18.1
- 9.17.1 P1
- 9.16.1 P3
- 9.15.1 P10
- 9.14.1 P13
- 9.13.1 P16
- 9.12.1 P18

par HA

- 9.18.1
- 9.17.1 P1
- 9.16.1 P3
- 9.15.1 P10
- 9.14.1 P13
- 9.13.1 P16
- 9.12.1 P18

Google Cloud

Nodo único

- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9,8
- 9.7 P5

par HA

- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9,8

Introducción a Amazon Web Services

Inicio rápido para Cloud Volumes ONTAP en AWS

Comience a utilizar Cloud Volumes ONTAP en AWS en unos pocos pasos.

1 Crear un agente de consola

Si no tienes una "Agente de consola" Aún así, es necesario crear uno. "Aprenda a crear un agente de consola en AWS" .

Tenga en cuenta que si desea implementar Cloud Volumes ONTAP en una subred donde no hay acceso a Internet disponible, deberá instalar manualmente el agente de consola y acceder a la interfaz de usuario de la NetApp Console que se ejecuta en ese agente de consola. "Aprenda a instalar manualmente el agente de consola en una ubicación sin acceso a Internet" .

2 Planifique su configuración

La consola ofrece paquetes preconfigurados que se adaptan a los requisitos de su carga de trabajo, o puede crear su propia configuración. Si elige su propia configuración, debe comprender las opciones disponibles. "Más información" .

3 Configura tu red

1. Asegúrese de que su VPC y sus subredes admitan la conectividad entre el agente de la consola y Cloud Volumes ONTAP.
2. Habilite el acceso a Internet saliente desde la VPC de destino para NetApp AutoSupport.

   Este paso no es necesario si está implementando Cloud Volumes ONTAP en una ubicación donde no hay acceso a Internet disponible.

3. Configura un punto final de VPC para el servicio Amazon Simple Storage Service (Amazon S3).

   Se requiere un punto final de VPC si desea organizar en niveles datos fríos de Cloud Volumes ONTAP en un almacenamiento de objetos de bajo costo.

"Obtenga más información sobre los requisitos de red" .

4 Configurar AWS KMS

Si desea utilizar el cifrado de Amazon con Cloud Volumes ONTAP, deberá asegurarse de que exista una clave maestra del cliente (CMK) activa. También debe modificar la política de claves para cada CMK agregando el rol de IAM que proporciona permisos al agente de la consola como *usuario clave*. "Más información" .

5 Inicie Cloud Volumes ONTAP mediante la consola

Haga clic en **Agregar sistema**, seleccione el tipo de sistema que desea implementar y complete los pasos del asistente. "Lea las instrucciones paso a paso" .

Enlaces relacionados

- "Crear un agente de consola para AWS"
- "Cree un agente de consola desde AWS Marketplace"
- "Instalar y configurar un agente de consola local"
- "Permisos de AWS para el agente de consola"

Planifique su configuración de Cloud Volumes ONTAP en AWS

Cuando implementa Cloud Volumes ONTAP en AWS, puede elegir un sistema preconfigurado que coincida con los requisitos de su carga de trabajo o puede crear su propia configuración. Si elige su propia configuración, debe comprender las opciones disponibles.

Elija una licencia de Cloud Volumes ONTAP

Hay varias opciones de licencia disponibles para Cloud Volumes ONTAP. Cada opción te permite elegir un modelo de consumo que se adapte a tus necesidades.

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

Elija una región compatible

Cloud Volumes ONTAP es compatible con la mayoría de las regiones de AWS. "Ver la lista completa de regiones compatibles" .

Se deben habilitar las regiones de AWS más nuevas antes de poder crear y administrar recursos en esas regiones. "Documentación de AWS: Aprenda a habilitar una región" .

Elija una zona local compatible

La selección de una zona local es opcional. Cloud Volumes ONTAP es compatible con algunas zonas locales de AWS, incluida Singapur. Cloud Volumes ONTAP en AWS solo admite el modo de alta disponibilidad (HA) en una única zona de disponibilidad. No se admiten implementaciones de nodo único.

> Cloud Volumes ONTAP no tiene soporte para niveles de datos ni de nube en AWS Local Zones. Además, no se admiten zonas locales con instancias que no hayan sido calificadas para Cloud Volumes ONTAP . Un ejemplo de esto es Miami, que no está disponible como zona local porque solo tiene instancias Gen6 que no son compatibles ni están calificadas.

"Documentación de AWS: Ver la lista completa de zonas locales" . Las zonas locales deben estar habilitadas antes de poder crear y administrar recursos en esas zonas.

"Documentación de AWS: Introducción a las zonas locales de AWS" .

Elija una instancia compatible

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

"Configuraciones compatibles con Cloud Volumes ONTAP en AWS"

Comprender los límites de almacenamiento

El límite de capacidad bruta para un sistema Cloud Volumes ONTAP está vinculado a la licencia. Límites adicionales impactan el tamaño de los agregados y volúmenes. Debe tener en cuenta estos límites al planificar su configuración.

"Límites de almacenamiento para Cloud Volumes ONTAP en AWS"

Dimensione su sistema en AWS

Dimensionar su sistema Cloud Volumes ONTAP puede ayudarle a cumplir con los requisitos de rendimiento y capacidad. Debe tener en cuenta algunos puntos clave al elegir un tipo de instancia, un tipo de disco y un tamaño de disco:

Tipo de instancia

- Adapte sus requisitos de carga de trabajo al rendimiento máximo y las IOPS para cada tipo de instancia 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 se basa principalmente 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 EBS

A grandes rasgos, las diferencias entre los tipos de discos EBS son las siguientes. Para obtener más información sobre los casos de uso de los discos EBS, consulte "Documentación de AWS: Tipos de volúmenes de EBS" .

- Los discos *SSD de propósito general (gp3)* son los SSD de menor costo que equilibran costo y rendimiento para una amplia gama 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.

  Cuando selecciona un disco gp3, la NetApp Console completa los valores de IOPS y rendimiento predeterminados que brindan un rendimiento equivalente a un disco gp2 según el tamaño de disco seleccionado. Puede aumentar los valores para obtener un mejor rendimiento a un costo mayor, pero no admitimos valores más bajos porque pueden resultar en un rendimiento inferior. En resumen, mantenga los valores predeterminados o auméntelos. No los bajes. "Documentación de AWS: Obtenga 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" .

- Los discos *SSD de propósito general (gp2)* equilibran costo y rendimiento para una amplia gama de cargas de trabajo. El rendimiento se define en términos de IOPS.
- Los discos *SSD con IOPS aprovisionados (io1)* son para aplicaciones críticas que requieren el mayor rendimiento a un mayor costo.

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

- Los discos *HDD de rendimiento optimizado (st1)* están destinados a cargas de trabajo a las que se accede con frecuencia y que requieren un rendimiento rápido y constante a un precio más bajo.

La asignación de niveles de datos a Amazon Simple Storage Service (Amazon S3) no es compatible si tu sistema Cloud Volumes ONTAP está en una AWS Local Zone, porque acceder a los buckets de Amazon S3 fuera de la Local Zone implica mayor latencia y afecta las actividades de Cloud Volumes ONTAP.

Tamaño del disco EBS

Si elige una configuración que no admite el"Función de volúmenes elásticos de Amazon EBS" , entonces deberá elegir un tamaño de disco inicial cuando inicie un sistema Cloud Volumes ONTAP . Después de eso, puedes"Deje que la consola administre la capacidad de un sistema por usted" , pero si quieres"Crea agregados tú mismo" , tenga en cuenta lo siguiente:

- Todos los discos de un agregado deben tener el mismo tamaño.
- El rendimiento de los discos EBS está vinculado al tamaño del disco. El tamaño determina la IOPS de referencia y la duración máxima de ráfaga para los discos SSD, y el rendimiento de referencia y de ráfaga para los discos HDD.
- En última instancia, debes elegir el tamaño de disco que te proporcione el *rendimiento sostenido* que necesitas.
- Incluso si elige discos más grandes (por ejemplo, seis discos de 4 TiB), es posible que no obtenga todas las IOPS porque la instancia EC2 puede alcanzar su límite de ancho de banda.

  Para obtener más detalles sobre el rendimiento del disco EBS, consulte "Documentación de AWS: Tipos de volúmenes de EBS" .

  Como se indicó anteriormente, la elección de un tamaño de disco no es compatible con las configuraciones de Cloud Volumes ONTAP que admiten la función Amazon EBS Elastic Volumes. "Obtenga más información sobre la compatibilidad con Elastic Volumes" .

Ver los discos del sistema predeterminados

Además del almacenamiento para los datos del usuario, la consola también compra almacenamiento en la nube para los datos del sistema Cloud Volumes ONTAP (datos de arranque, datos raíz, datos del núcleo y NVRAM). Para fines de planificación, puede ser útil revisar estos detalles antes de implementar Cloud Volumes ONTAP.

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

El agente de consola también requiere un disco de sistema. "Ver detalles sobre la configuración predeterminada del agente de la consola" .

Prepárese para implementar Cloud Volumes ONTAP en un AWS Outpost

Si tiene un AWS Outpost, puede implementar Cloud Volumes ONTAP en ese Outpost seleccionando la VPC de Outpost durante el proceso de implementación. La experiencia es la misma que la de cualquier otra VPC que resida en AWS. Tenga en cuenta que primero deberá implementar un agente de consola en su AWS Outpost.

Hay algunas limitaciones que conviene señalar:

- En este momento, solo se admiten sistemas Cloud Volumes ONTAP de un solo nodo
- Las instancias EC2 que puede usar con Cloud Volumes ONTAP están limitadas a lo que está disponible en su puesto avanzado

- En este momento solo se admiten SSD de propósito general (gp2)

Recopilar información de redes

Cuando inicia Cloud Volumes ONTAP en AWS, debe especificar detalles sobre su red VPC. Puede utilizar una hoja de trabajo para recopilar la información de su administrador.

Nodo único o par HA en una sola AZ

Información de AWS	Tu valor
Región	
VPC	
Subred	
Grupo de seguridad (si usa el suyo propio)	

Par HA en múltiples AZ

Información de AWS	Tu valor
Región	
VPC	
Grupo de seguridad (si usa el suyo propio)	
Zona de disponibilidad del nodo 1	
Subred del nodo 1	
Zona de disponibilidad del nodo 2	
Subred del nodo 2	
Zona de disponibilidad del mediador	
Subred del mediador	
Par de claves para el mediador	
Dirección IP flotante para el puerto de administración 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

La consola le permite elegir una configuración de velocidad de escritura para Cloud Volumes ONTAP. Antes de elegir una velocidad de escritura, debe comprender las diferencias entre las configuraciones normales y altas, así como los riesgos y recomendaciones al utilizar una velocidad de escritura alta. "Obtenga más información sobre la velocidad de escritura" .

Elija un perfil de uso de volumen

ONTAP incluye varias funciones de eficiencia de almacenamiento que pueden reducir la cantidad total de almacenamiento que necesita. Cuando crea un volumen en la consola, puede elegir un perfil que habilite estas funciones o un perfil que las deshabilite. Debe aprender más sobre estas características para ayudarlo a decidir qué perfil utilizar.

Las características de eficiencia de almacenamiento de NetApp brindan los siguientes beneficios:

Aprovisionamiento fino
: Presenta más almacenamiento lógico a los hosts o usuarios del que realmente tiene en su grupo de almacenamiento físico. En lugar de preasignar espacio de almacenamiento, el espacio de almacenamiento se asigna dinámicamente a cada volumen a medida que se escriben los datos.

Desduplicación
: Mejora la eficiencia al localizar bloques de datos idénticos y reemplazarlos con referencias a un único bloque compartido. Esta técnica reduce los requisitos de capacidad de almacenamiento al eliminar bloques redundantes de datos que residen en el mismo volumen.

Compresión
: Reduce la capacidad física necesaria para almacenar datos al comprimirlos dentro de un volumen en el almacenamiento primario, secundario y de archivo.

Configura tu red

Configurar la red de AWS para Cloud Volumes ONTAP

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

Requisitos generales

Asegúrese de haber cumplido los siguientes requisitos en AWS.

Acceso a Internet saliente para nodos de Cloud Volumes ONTAP

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

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

Puntos finales de Cloud Volumes ONTAP

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

Puntos finales	Aplicable para	Objetivo	Modos de implementación	Impacto si el punto final no está disponible
\ https://netapp-cloud-account.auth0.com	Autenticación	Se utiliza para la autenticación en la consola.	Modos estándar y restringido.	La autenticación del usuario falla y los siguientes servicios permanecen no disponibles: • Servicios de Cloud Volumes ONTAP • Servicios de ONTAP • Protocolos y servicios proxy
\ https://api.bluexp.netapp.com/tenancy	Tenencia	Se utiliza para recuperar recursos de Cloud Volumes ONTAP desde la consola para autorizar recursos y usuarios.	Modos estándar y restringido.	Los recursos de Cloud Volumes ONTAP y los usuarios no están autorizados.
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Se utiliza para enviar datos de telemetría de AutoSupport al soporte de NetApp .	Modos estándar y restringido.	La información de AutoSupport sigue sin entregarse.

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

Acceso a Internet saliente para el mediador de HA

La instancia del mediador de HA debe tener una conexión saliente al servicio AWS EC2 para que pueda ayudar con la conmutación por error del almacenamiento. Para proporcionar la conexión, puede agregar una dirección IP pública, especificar un servidor proxy o utilizar una opción manual.

La opción manual puede ser una puerta de enlace NAT o un punto final de VPC de interfaz desde la subred de destino al servicio AWS EC2. Para obtener detalles sobre los puntos finales de VPC, consulte la

"Documentación de AWS: Puntos de conexión de la VPC de interfaz (AWS PrivateLink)" .

Configuración del proxy de red del agente de la NetApp Console

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

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

Para obtener información sobre cómo configurar servidores proxy, consulte la "Configurar el agente de la consola para utilizar un servidor proxy" .

Direcciones IP privadas

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

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

Direcciones IP para un sistema de nodo único

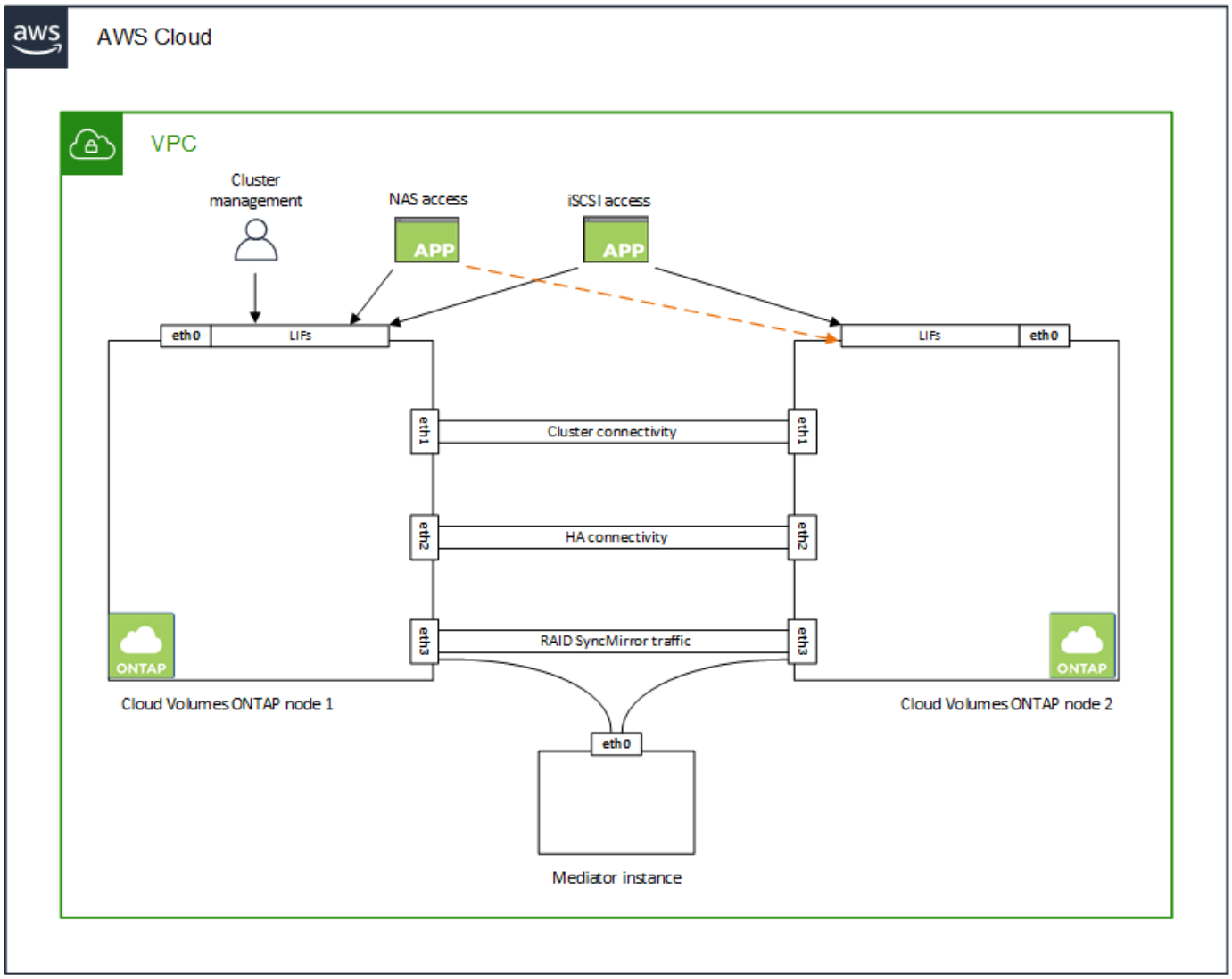
NetApp Console asigna 6 direcciones IP a un sistema de nodo único.

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

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

Direcciones IP para pares HA

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



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

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

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

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

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

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

Grupos de seguridad

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

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

Conexión para la estratificación de datos

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

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

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

Conexiones a sistemas ONTAP

Para replicar datos entre un sistema Cloud Volumes ONTAP en AWS y sistemas ONTAP en otras redes, debe tener una conexión VPN entre AWS VPC y la otra red (por ejemplo, su red corporativa). Para obtener instrucciones, consulte la "Documentación de AWS: Configuración de una conexión VPN de AWS" .

DNS y Active Directory para CIFS

Si desea aprovisionar almacenamiento CIFS, debe configurar DNS y Active Directory en AWS o extender su configuración local a AWS.

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

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

Uso compartido de VPC

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

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

Requisitos para pares de alta disponibilidad en varias zonas de disponibilidad

Se aplican requisitos de red de AWS adicionales a las configuraciones de HA de Cloud Volumes ONTAP que utilizan múltiples zonas de disponibilidad (AZ). Debe revisar estos requisitos antes de lanzar un par de alta

disponibilidad porque debe ingresar los detalles de red en la consola cuando agrega un sistema Cloud Volumes ONTAP .

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

Zonas de disponibilidad

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

Debe haber una subred disponible en cada zona de disponibilidad.

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

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

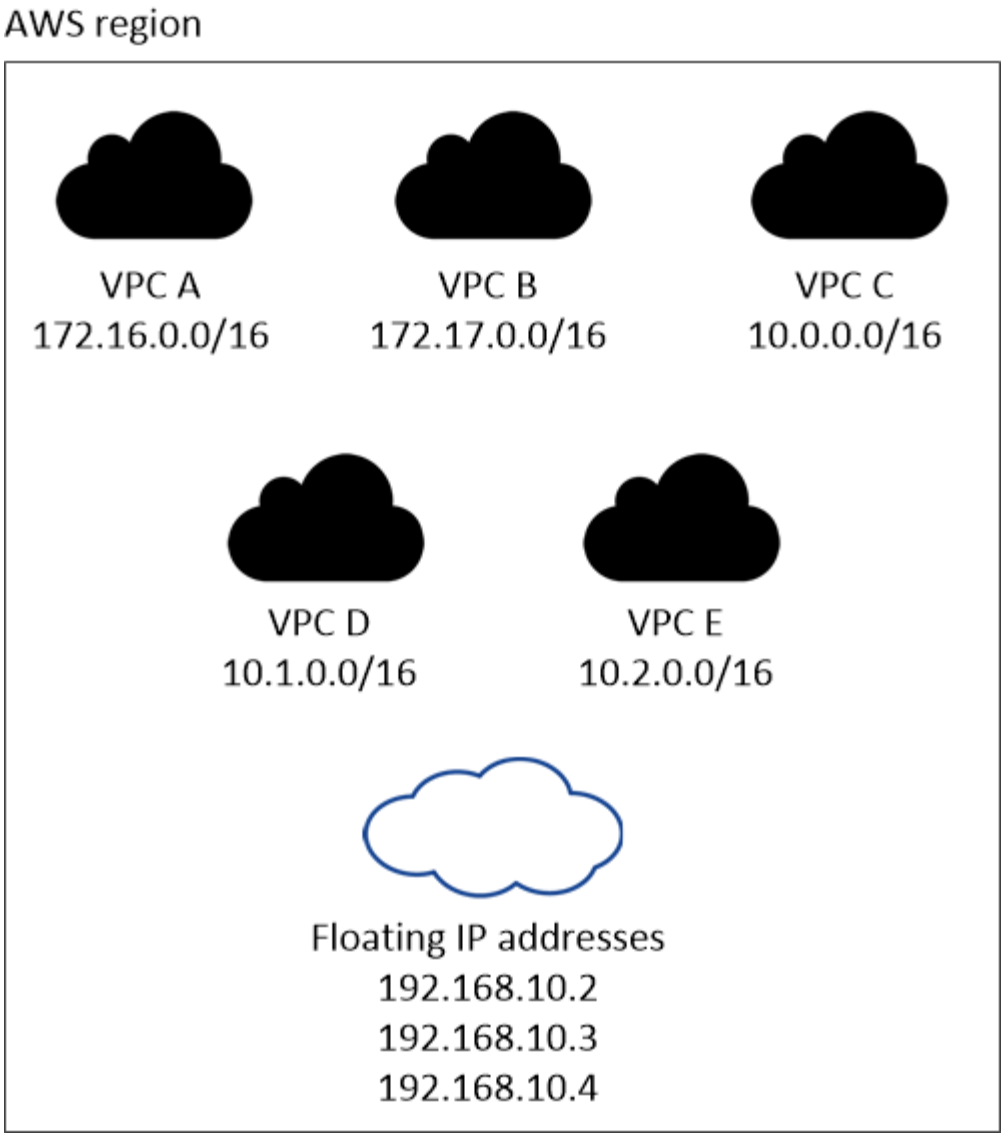
Una dirección IP flotante es para la administración del clúster, otra es para los datos NFS/CIFS en el nodo 1 y otra es para los datos NFS/CIFS en el nodo 2. Una cuarta dirección IP flotante para la gestión de SVM es opcional.

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

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

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

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



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

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

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

Tablas de rutas

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

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

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

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

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

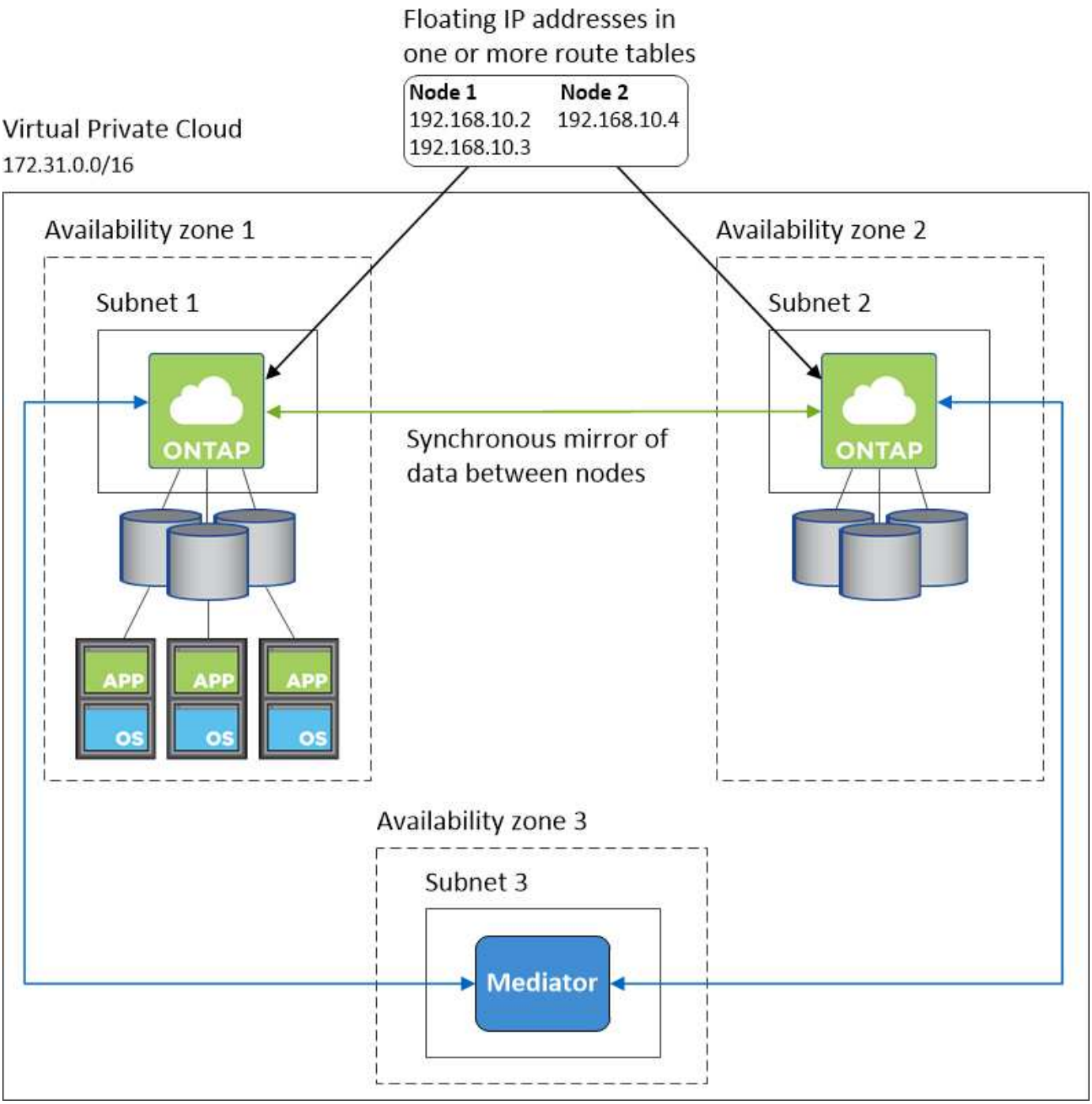
Conexión a las herramientas de gestión de NetApp

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

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

Ejemplo de configuración de alta disponibilidad

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



Requisitos para el agente de consola

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

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

Temas relacionados

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

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

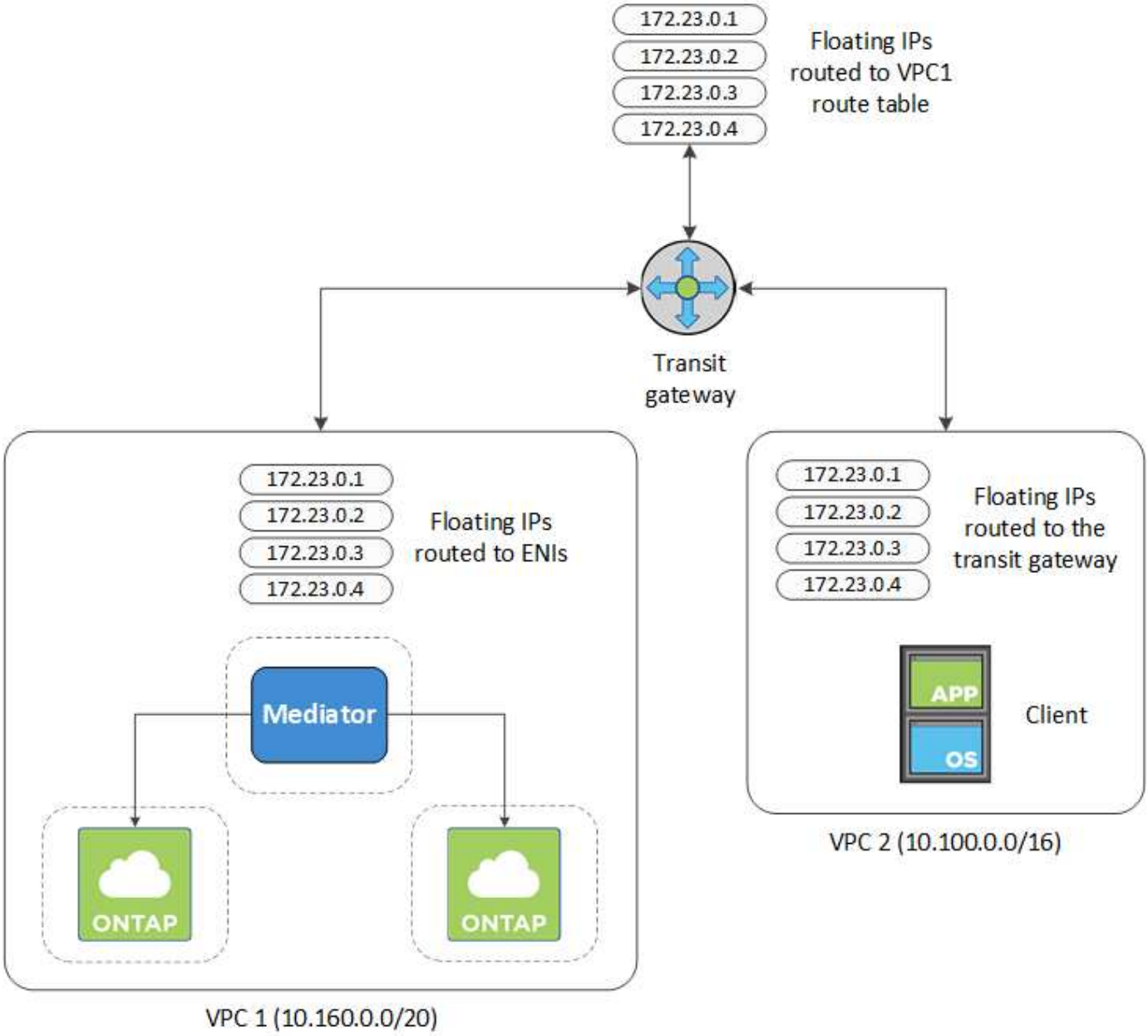
Configurar una puerta de enlace de tránsito de AWS para habilitar el acceso a un par de alta disponibilidad"direcciones IP flotantes" desde fuera de la VPC donde reside el par HA.

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

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

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

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

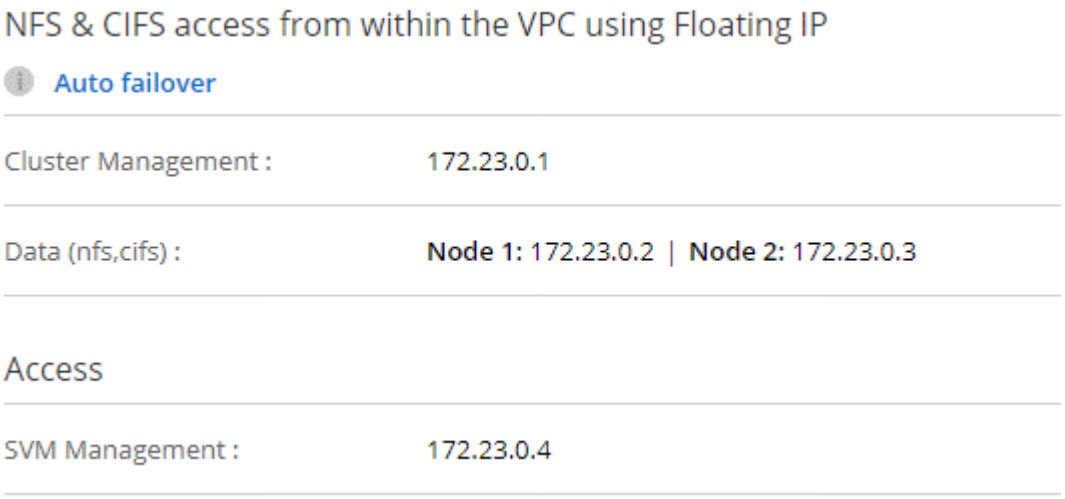


Los siguientes pasos ilustran cómo establecer una configuración similar.

Pasos

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

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



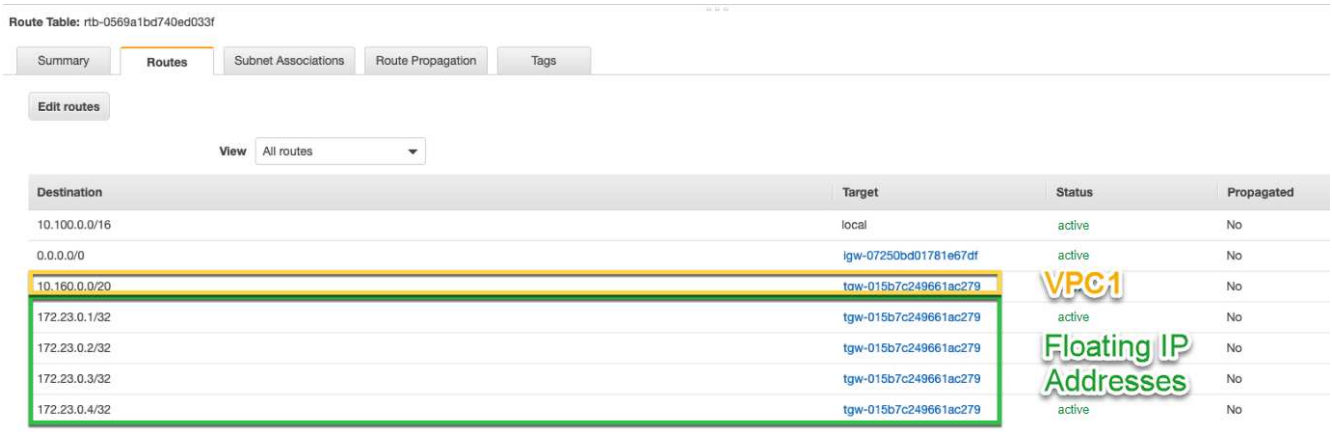
La siguiente imagen de muestra muestra la tabla de rutas para la puerta de enlace de tránsito. Incluye rutas a los bloques CIDR de las dos VPC y cuatro direcciones IP flotantes utilizadas por Cloud Volumes ONTAP.

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

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

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

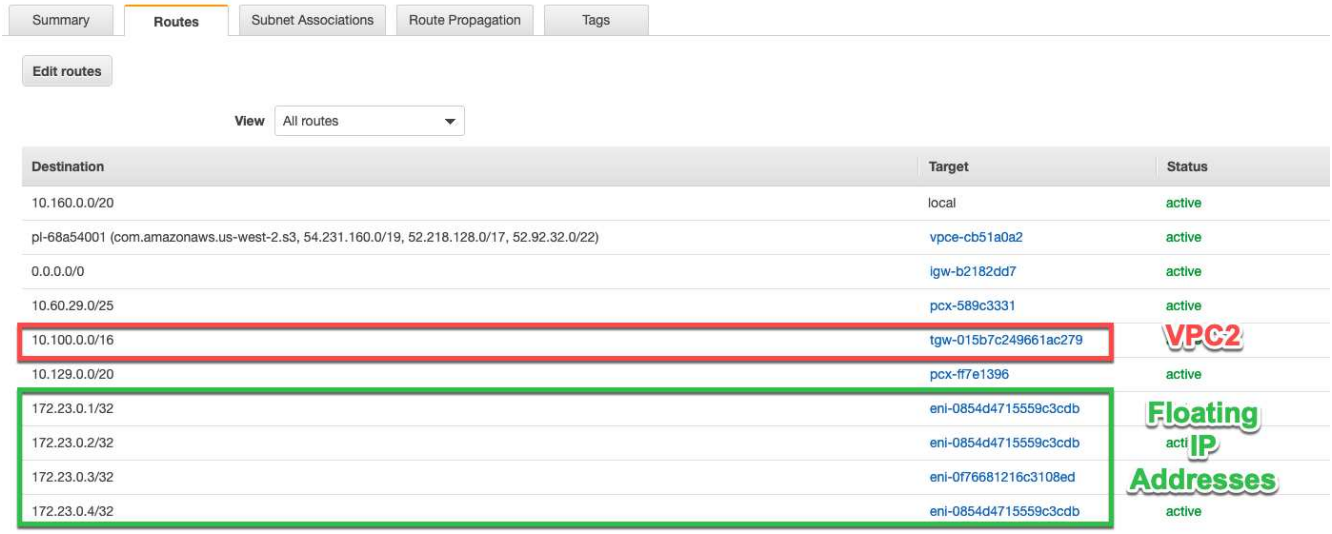
      La siguiente imagen de muestra muestra la tabla de rutas para VPC 2, que incluye rutas a VPC 1 y las direcciones IP flotantes.



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

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

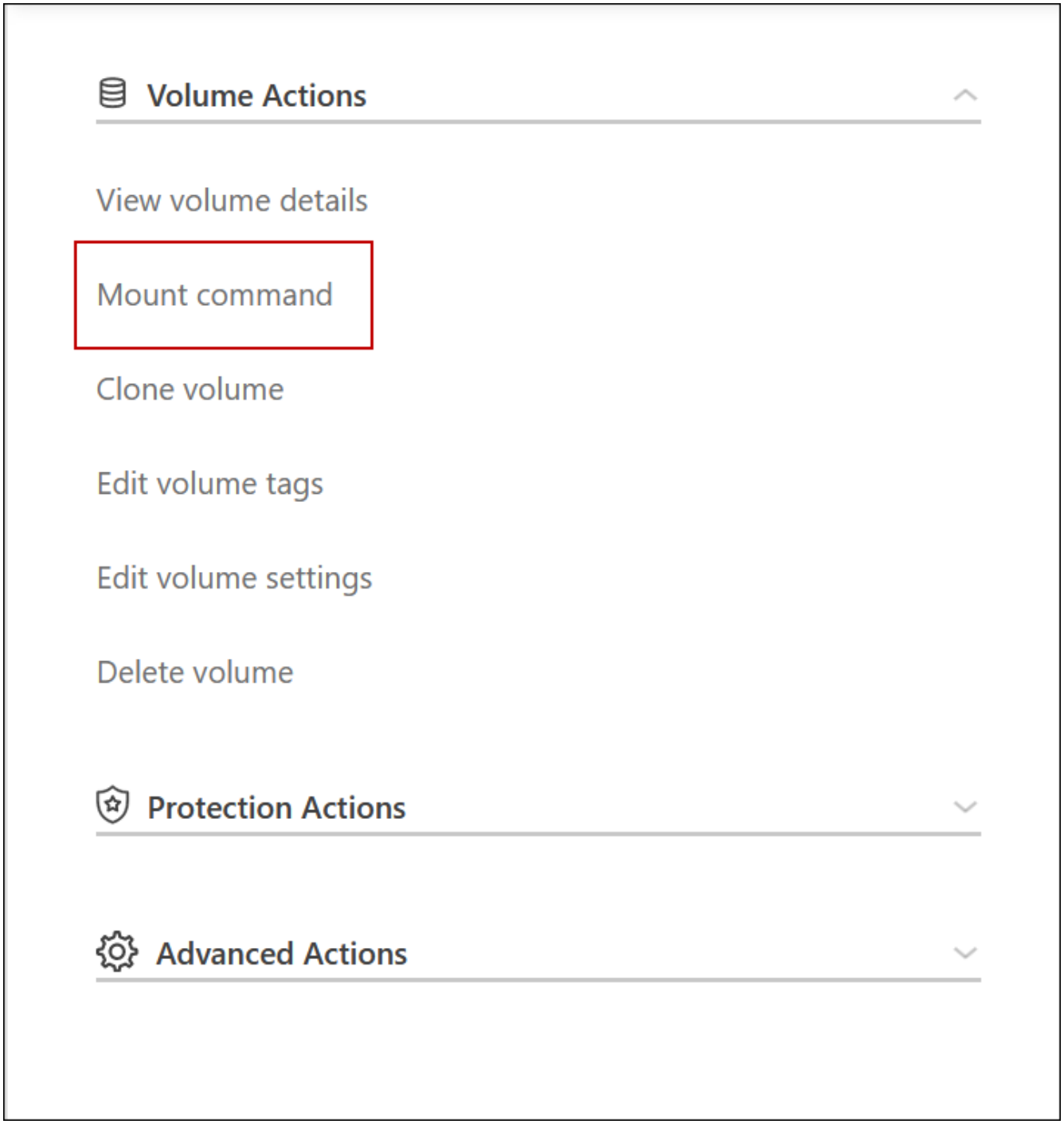
   La siguiente imagen de muestra muestra la tabla de rutas para VPC 1. Incluye una ruta a las direcciones IP flotantes y a VPC 2, que es donde reside un cliente. La consola agregó automáticamente las IP flotantes a la tabla de rutas cuando implementó el par HA.



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

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

panel Administrar volúmenes en la consola.



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

   "Aprenda a editar un volumen" .

Enlaces relacionados

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

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

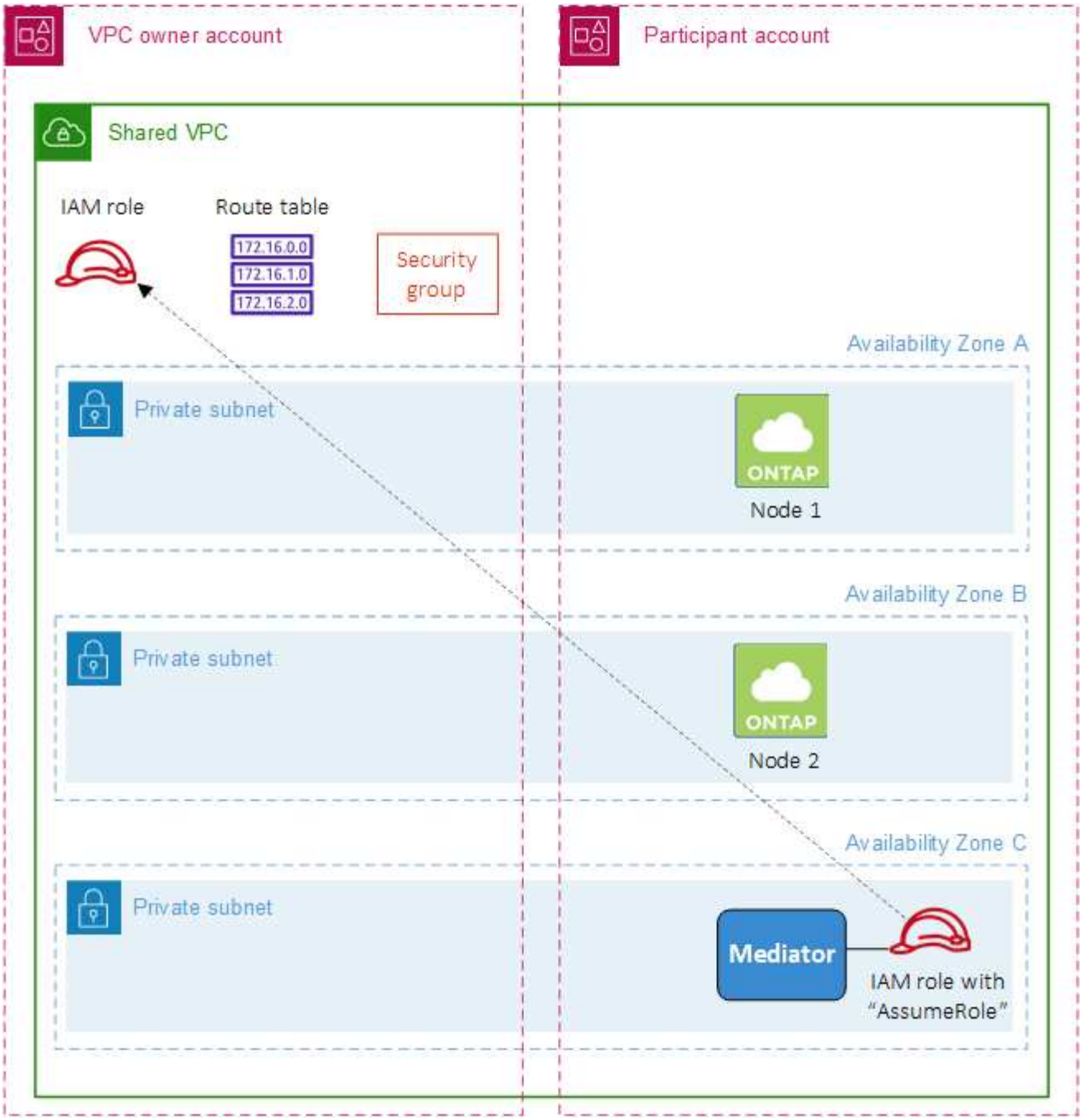
A partir de la versión 9.11.1, los pares de Cloud Volumes ONTAP HA son compatibles con AWS con uso compartido de VPC. El uso compartido de VPC permite que su organización comparta subredes con otras cuentas de AWS. Para utilizar esta configuración, debe configurar su entorno de AWS y luego implementar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

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

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

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

La siguiente imagen muestra los componentes involucrados en esta implementación:



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

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

Pasos

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

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

   "Documentación de AWS: Compartir una subred"

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

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

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

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

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

   Tenga en cuenta que debe especificar los siguientes campos:

   - "ID de grupo de seguridad"

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

   - "assumeRoleArn" en el objeto "haParams"

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

     Por ejemplo:

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

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

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

Las implementaciones de alta disponibilidad (HA) de Cloud Volumes ONTAP en la zona de disponibilidad única (AZ) de AWS pueden fallar y revertirse si falla la creación del grupo de ubicación. La creación del grupo de ubicación también falla y la implementación se revierte si el nodo de Cloud Volumes ONTAP y la instancia del mediador no están

disponibles. Para evitar esto, puede modificar la configuración para permitir que la implementación finalice incluso si falla la creación del grupo de ubicación.

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

Pasos

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

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

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

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

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

Reglas para Cloud Volumes ONTAP

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

Reglas de entrada

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

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

Protocolo	Puerto	Objetivo
Todos los ICMP	Todo	Haciendo ping a la instancia
HTTP	80	Acceso HTTP a la consola web de ONTAP System Manager mediante la dirección IP del LIF de administración del clúster
HTTPS	443	Conectividad con el agente de la consola y acceso HTTPS a la consola web de ONTAP System Manager mediante la dirección IP del LIF de administración del clúster
SSH	22	Acceso SSH a la dirección IP del LIF de administración del clúster o de un LIF de administración de nodos
TCP	111	Llamada a procedimiento remoto para NFS
TCP	139	Sesión de servicio NetBIOS para CIFS
TCP	161-162	Protocolo simple de gestión de red
TCP	445	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
TCP	635	Montaje NFS
TCP	749	Kerberos
TCP	2049	Demonio del servidor NFS
TCP	3260	Acceso iSCSI a través del LIF de datos iSCSI
TCP	4045	Demonio de bloqueo NFS
TCP	4046	Monitor de estado de red para NFS
TCP	10000	Copia de seguridad mediante NDMP
TCP	11104	Gestión de sesiones de comunicación entre clústeres para SnapMirror
TCP	11105	Transferencia de datos de SnapMirror mediante LIF entre clústeres
UDP	111	Llamada a procedimiento remoto para NFS
UDP	161-162	Protocolo simple de gestión de red
UDP	635	Montaje NFS
UDP	2049	Demonio del servidor NFS
UDP	4045	Demonio de bloqueo NFS
UDP	4046	Monitor de estado de red para NFS
UDP	4049	Protocolo rquotad de NFS

Reglas de salida

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

Reglas básicas de salida

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

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

Reglas de salida avanzadas

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

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

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

Servicio	Protocolo	Puerto	Fuente	Destino	Objetivo
AutoSupport	HTTPS	443	LIF de gestión de nodos	mysupport.netapp.com	AutoSupport (HTTPS es el predeterminado)
	HTTP	80	LIF de gestión de nodos	mysupport.netapp.com	AutoSupport (solo si el protocolo de transporte se cambia de HTTPS a HTTP)
	TCP	3128	LIF de gestión de nodos	Agente de consola	Envío de mensajes de AutoSupport a través de un servidor proxy en el agente de la consola, si no hay una conexión a Internet saliente disponible
Copia de seguridad en S3	TCP	5010	LIF entre clústeres	Realizar una copia de seguridad del punto final o restaurarlo	Operaciones de copia de seguridad y restauración para la función Copia de seguridad en S3
Grupo	Todo el tráfico	Todo el tráfico	Todos los LIF en un nodo	Todos los LIF en el otro nodo	Comunicaciones entre clústeres (solo Cloud Volumes ONTAP HA)
	TCP	3000	LIF de gestión de nodos	mediador de HA	Llamadas ZAPI (solo Cloud Volumes ONTAP HA)
	ICMP	1	LIF de gestión de nodos	mediador de HA	Mantener activo (solo Cloud Volumes ONTAP HA)
Copias de seguridad de configuración	HTTP	80	LIF de gestión de nodos	http://<dirección IP del agente de consola>/occm/offboxconfig	Envía copias de seguridad de la configuración al agente de la consola."Documentación de ONTAP"
DHCP	UDP	68	LIF de gestión de nodos	DHCP	Cliente DHCP para la primera configuración
DHCP	UDP	67	LIF de gestión de nodos	DHCP	Servidor DHCP
DNS	UDP	53	LIF de gestión de nodos y LIF de datos (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	LIF de gestión de nodos	Servidores de destino	Copia NDMP
SMTP	TCP	25	LIF de gestión de nodos	Servidor de correo	Alertas SMTP, se pueden utilizar para AutoSupport

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

Reglas para el grupo de seguridad externo del mediador de HA

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

Reglas de entrada

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

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

Reglas de salida

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

Reglas básicas de salida

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

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

Reglas de salida avanzadas

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

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

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

Reglas para el grupo de seguridad interna de configuración de HA

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

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

Reglas de entrada

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

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

Reglas de salida

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

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

Reglas para el agente de consola

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

Configurar Cloud Volumes ONTAP para usar una clave administrada por el cliente en AWS

Si desea utilizar el cifrado de Amazon con Cloud Volumes ONTAP, deberá configurar el Servicio de administración de claves de AWS (KMS).

Pasos

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

   La CMK puede ser una CMK administrada por AWS o una CMK administrada por el cliente. Puede estar en la misma cuenta de AWS que NetApp Console y Cloud Volumes ONTAP o en una cuenta de AWS diferente.

   "Documentación de AWS: Claves maestras del cliente (CMK)"

2. Modifique la política de claves para cada CMK agregando el rol de IAM que proporciona permisos a la consola como *usuario clave*.

   Al agregar el rol de Administración de identidad y acceso (IAM) como usuario clave, se le otorgan a la consola permisos para usar la CMK con Cloud Volumes ONTAP.

   "Documentación de AWS: Edición de claves"

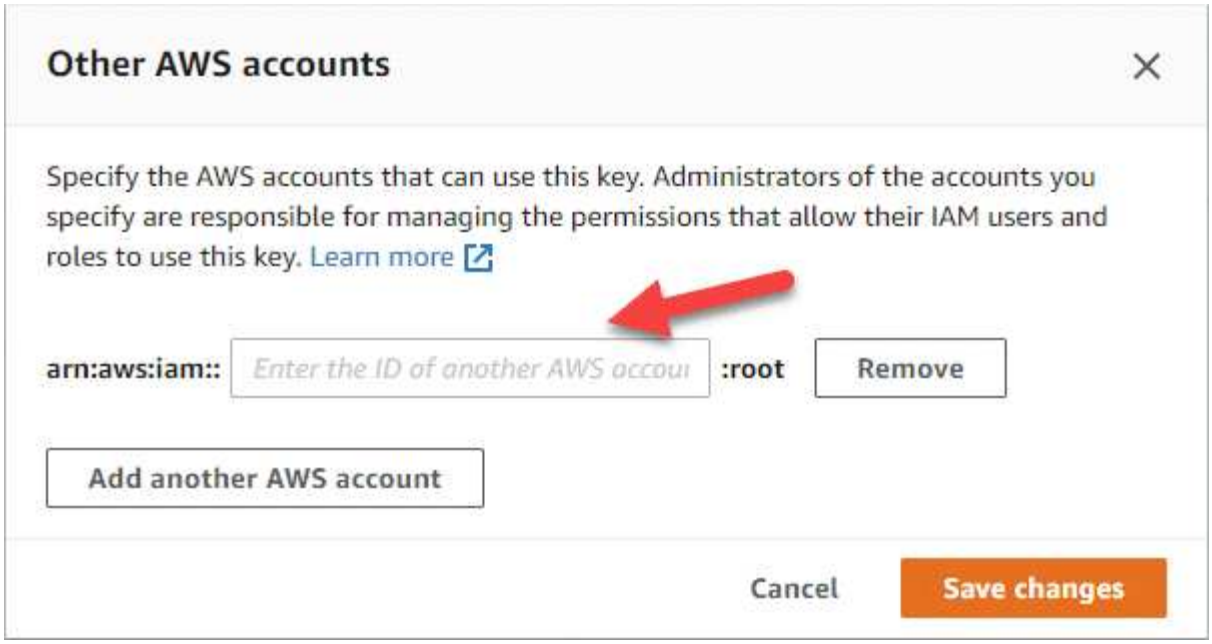
3. Si la CMK está en una cuenta de AWS diferente, complete los siguientes pasos:

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

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

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

      Normalmente, esta es la cuenta donde se implementa la consola. Si la consola no está instalada en AWS, utilice la cuenta para la que proporcionó las claves de acceso de AWS a la consola.



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

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

g. Adjunte la política al rol de IAM o al usuario de IAM que proporciona permisos a la consola.

   La siguiente política proporciona los permisos que la consola necesita para usar la CMK de la cuenta externa de AWS. Asegúrese de modificar la región y el ID de la 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 detalles adicionales sobre este proceso, consulte la "Documentación de AWS: Permitir que los usuarios de otras cuentas utilicen una clave KMS" .

4. Si está utilizando una CMK administrada por el cliente, modifique la política de claves para la CMK agregando el rol IAM de Cloud Volumes ONTAP como *usuario clave*.

Este paso es necesario si habilitaste la organización en niveles de datos en Cloud Volumes ONTAP y quieres cifrar los datos almacenados en el bucket de Amazon Simple Storage Service (Amazon S3).

Deberá realizar este paso *después* de implementar Cloud Volumes ONTAP porque la función de IAM se crea cuando crea un sistema Cloud Volumes ONTAP . (Por supuesto, tienes la opción de usar una función IAM de Cloud Volumes ONTAP existente, por lo que es posible realizar este paso antes).

"Documentación de AWS: Edición de claves"

Configurar roles de AWS IAM para nodos de Cloud Volumes ONTAP

Los roles de administración de identidad y acceso (IAM) de AWS con los permisos necesarios deben estar asociados a cada nodo de Cloud Volumes ONTAP . Lo mismo ocurre con el mediador HA. Lo más fácil es dejar que la NetApp Console cree los roles de IAM para usted, pero puede usar sus propios roles.

Esta tarea es opcional. Cuando crea un sistema Cloud Volumes ONTAP , la opción predeterminada es permitir que la consola cree los roles de IAM por usted. Si las políticas de seguridad de su empresa requieren que usted mismo cree los roles de IAM, siga los pasos a continuación.

Es necesario proporcionar su propio rol de IAM en AWS Secret Cloud. "Aprenda a implementar Cloud Volumes ONTAP en C2S" .

Pasos

1. Vaya a la consola de AWS IAM.
2. Cree políticas de IAM que incluyan los siguientes permisos:
    - Política base para 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 de 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 de alto secreto

```
{
    "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 respaldo para nodos de Cloud Volumes ONTAP

  Si planea utilizar NetApp Backup and Recovery con sus sistemas Cloud Volumes ONTAP , la función 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 de 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 de alto secreto

```
{
    "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 HA

```
{
    "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. Cree un rol de IAM y adjunte las políticas que creó al rol.

Resultado

Ahora tiene roles de IAM que puede seleccionar cuando crea un nuevo sistema Cloud Volumes ONTAP .

Más información

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

Configurar licencias para Cloud Volumes ONTAP en AWS

Después de decidir qué opción de licencia desea utilizar con Cloud Volumes ONTAP, se requieren algunos pasos antes de poder elegir esa opción de licencia al crear un nuevo sistema.

Freemium

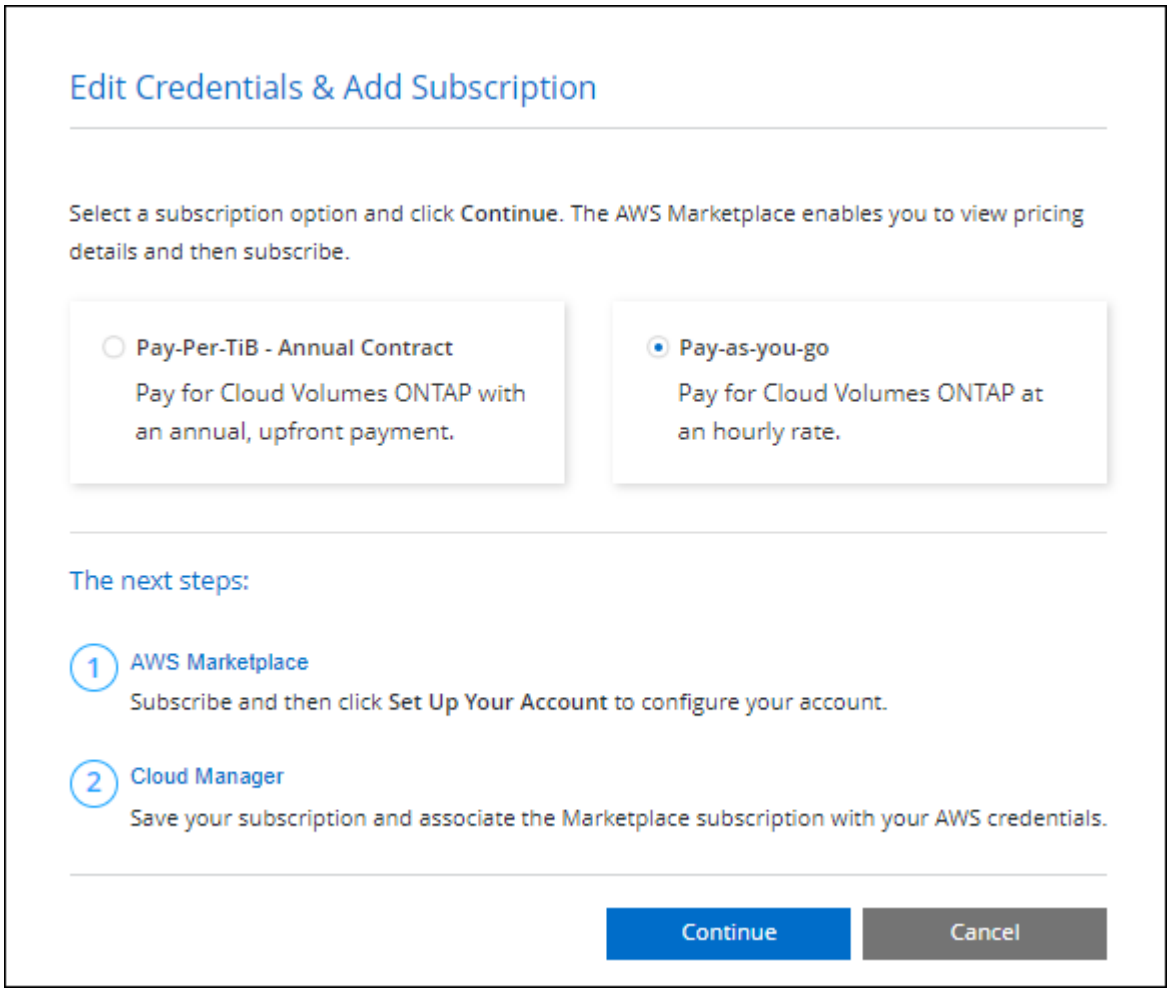
Seleccione la oferta Freemium para utilizar Cloud Volumes ONTAP de forma gratuita con hasta 500 GiB de capacidad aprovisionada. "Obtenga más información sobre la oferta Freemium" .

Pasos

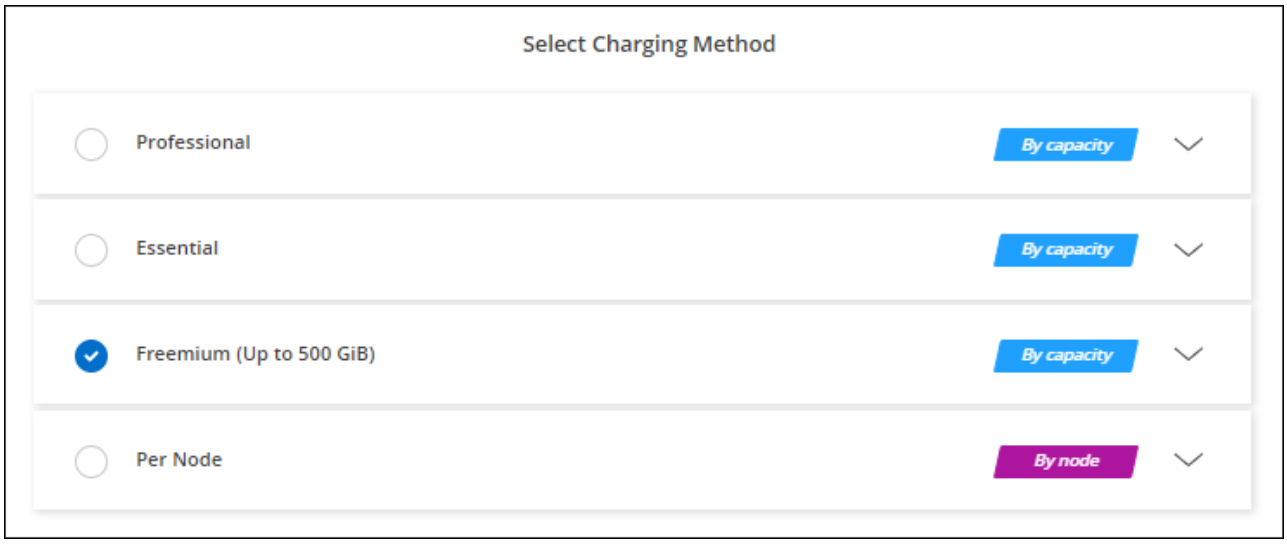
1. Desde el menú de navegación izquierdo de la NetApp Console, seleccione **Almacenamiento > Administración**.
2. En la página **Sistemas**, haga clic en **Agregar sistema** y siga los pasos.

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

   No se le cobrará a través de la suscripción del mercado a menos que exceda los 500 GiB de capacidad aprovisionada, momento en el cual el sistema se convierte automáticamente al"Paquete esencial" .



a. Después de regresar a la consola, seleccione **Freemium** cuando llegue a la página de métodos de cobro.



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

Licencia basada en capacidad

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

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

- Una licencia (traiga su propia licencia (BYOL)) comprada a NetApp
- Una suscripción por hora, de pago por uso (PAYGO) desde AWS Marketplace
- Un contrato anual del AWS Marketplace

"Obtenga más información sobre las licencias basadas en capacidad" .

Las siguientes secciones describen cómo comenzar a utilizar cada uno de estos modelos de consumo.

Trae tu propia bebida

Pague por adelantado comprando una licencia (BYOL) de NetApp para implementar sistemas Cloud Volumes ONTAP en cualquier proveedor de nube.

NetApp ha restringido la compra, extensión y renovación de licencias BYOL. Para más información, consulte "Disponibilidad restringida de licencias BYOL para Cloud Volumes ONTAP" .

Pasos

1. "Comuníquese con el departamento de ventas de NetApp para obtener una licencia"
2. "Agregue su cuenta del sitio de soporte de NetApp a la consola"

   La consola consulta automáticamente el servicio de licencias de NetApp para obtener detalles sobre las licencias asociadas a su cuenta del sitio de soporte de NetApp . Si no hay errores, la Consola agrega automáticamente las licencias a la Consola.

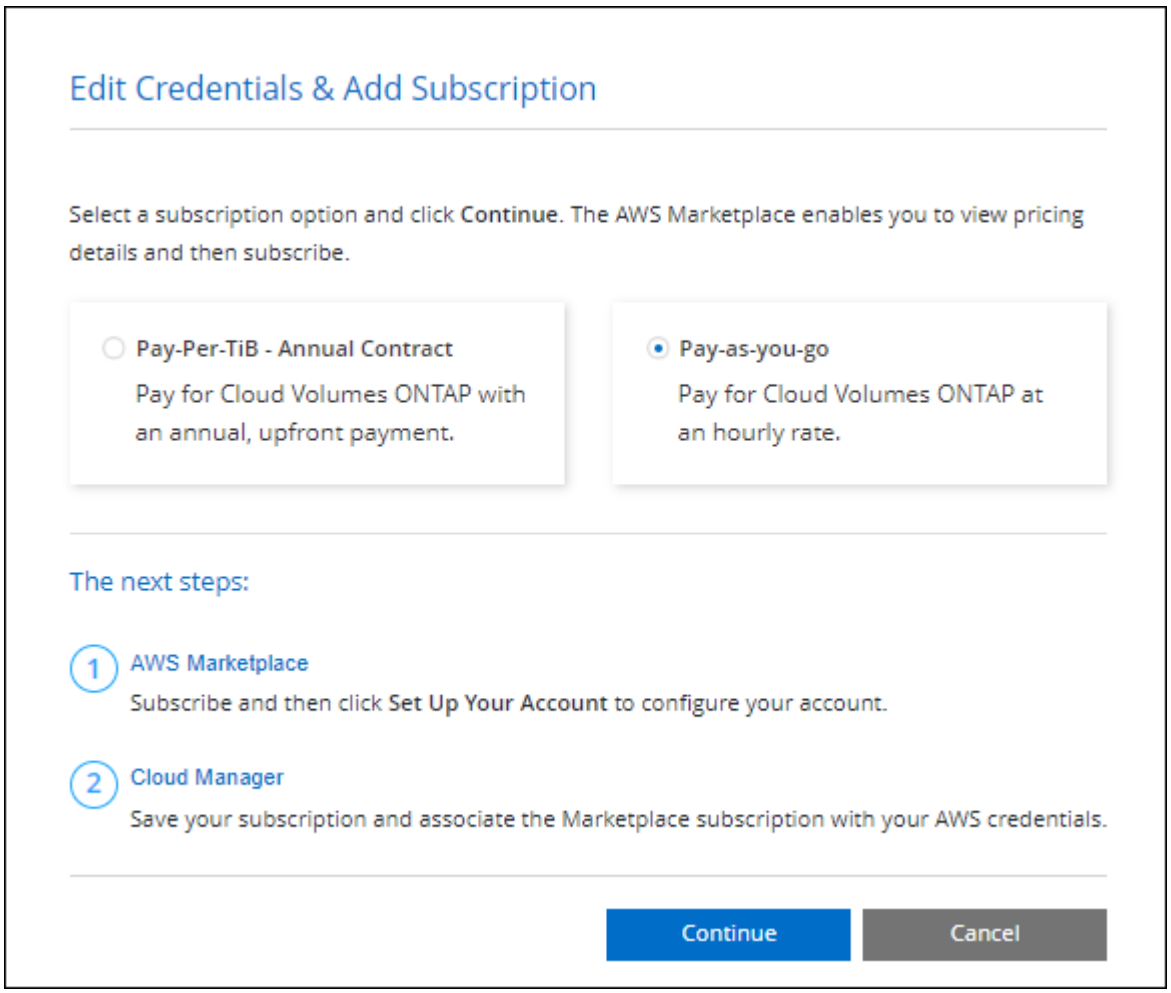
   Su licencia debe estar disponible en la consola antes de poder usarla con Cloud Volumes ONTAP. Si es

necesario, puedes"agregar manualmente la licencia a la consola" .

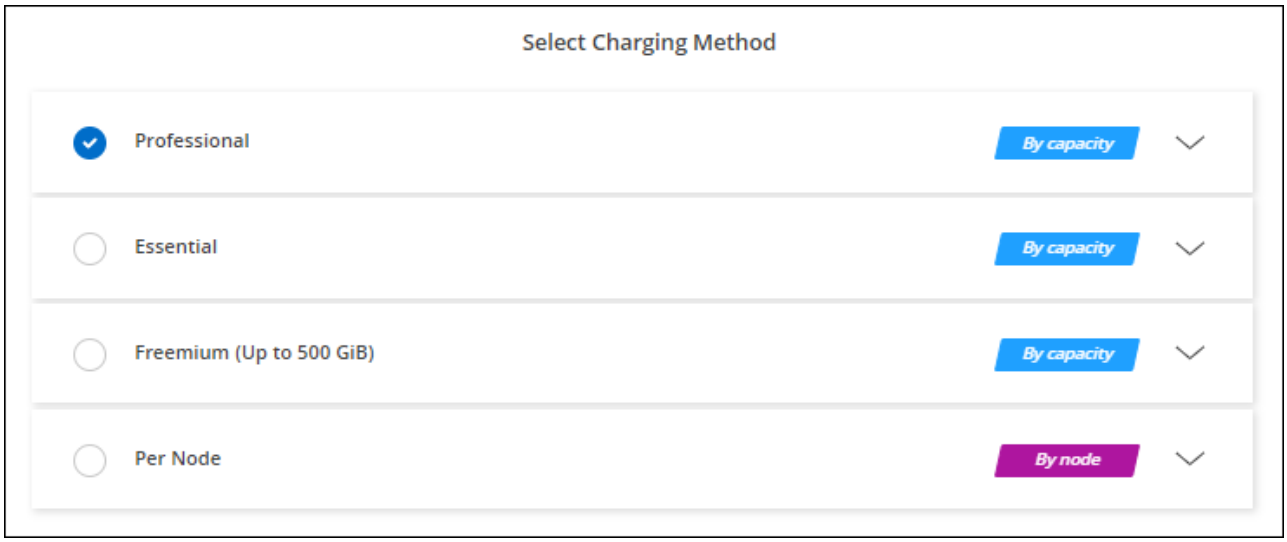
3. En la página **Sistemas** de la Consola, haga clic en **Agregar sistema** y siga los pasos.

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

      La licencia que usted compró de NetApp siempre se cobra primero, pero se le cobrará la tarifa por hora del mercado si excede su capacidad de licencia o si vence el plazo de su licencia.



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



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

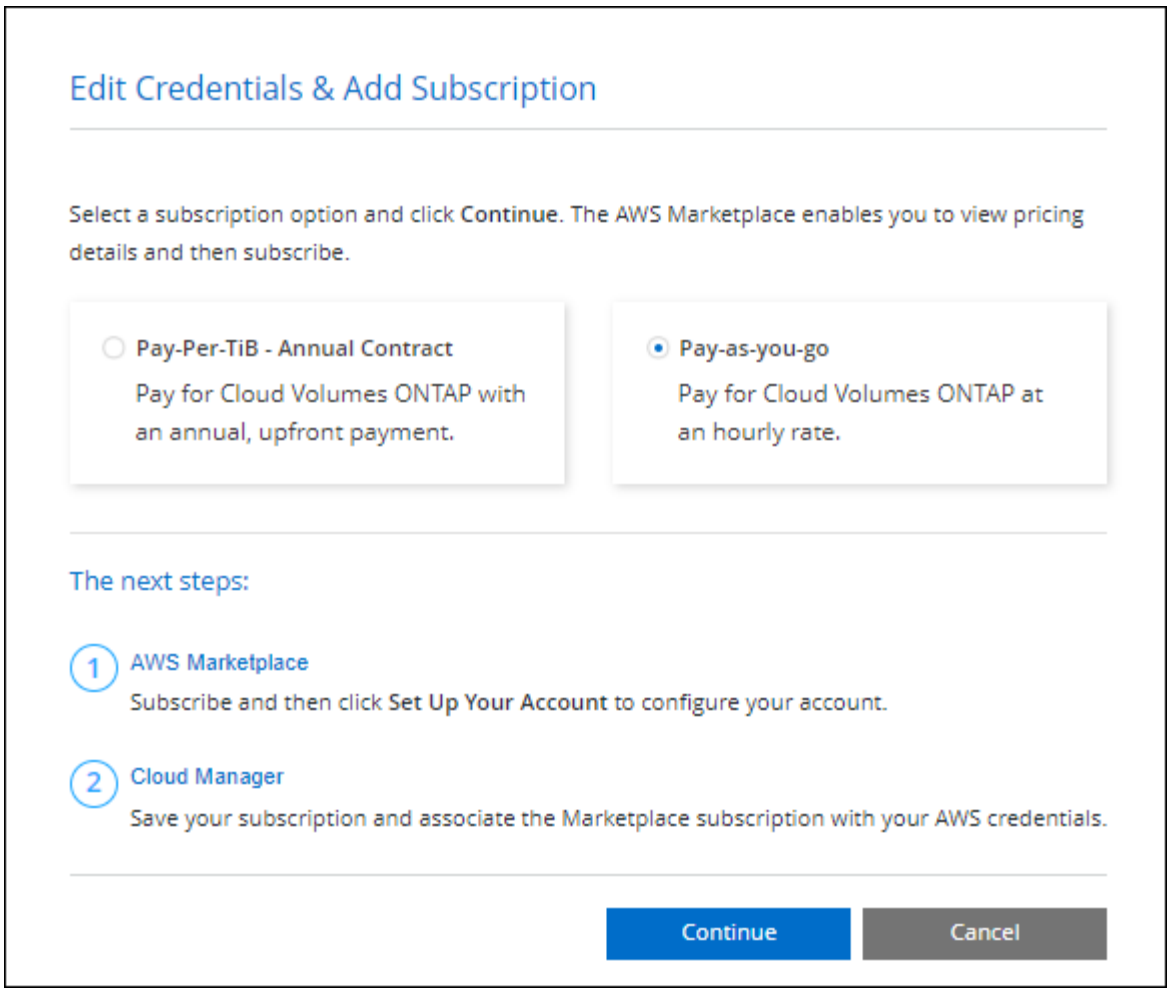
Suscripción PAYGO

Pague por hora suscribiéndose a la oferta del mercado de su proveedor de nube.

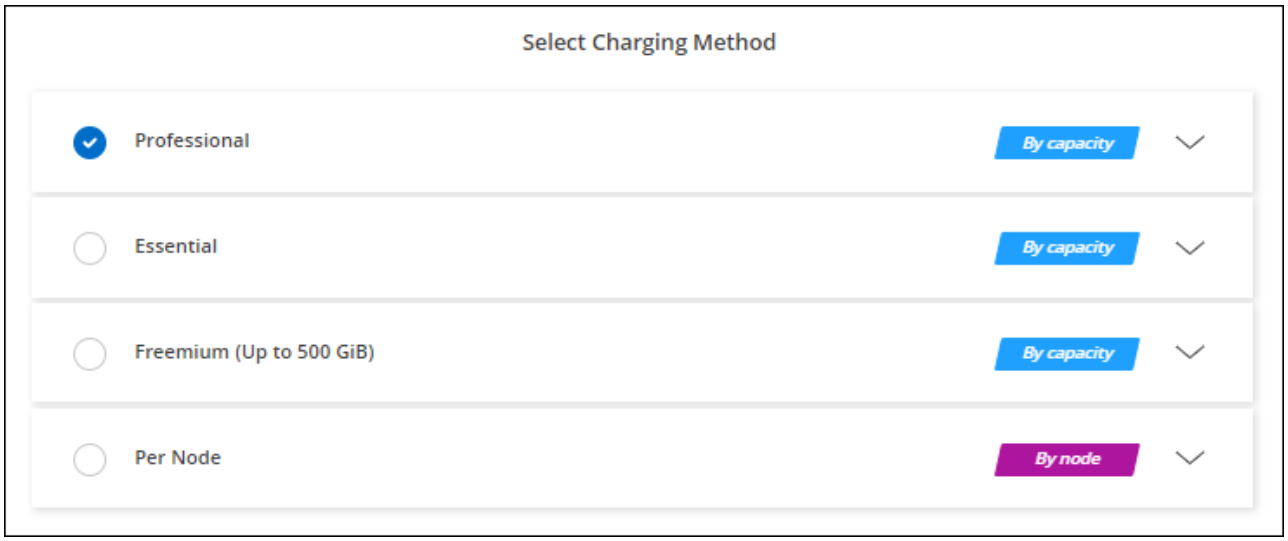
Cuando crea un sistema Cloud Volumes ONTAP , la consola le solicita que se suscriba al acuerdo que está disponible en AWS Marketplace. Esa suscripción se asocia luego al sistema para su cobro. Puede utilizar esa misma suscripción para sistemas Cloud Volumes ONTAP adicionales.

Pasos

1. Desde el menú de navegación de la izquierda, seleccione **Almacenamiento > Administración**.
2. En la página **Sistemas**, haga clic en **Agregar sistema** y siga los pasos.
   a. En la página **Detalles y credenciales**, haga clic en **Editar credenciales > Agregar suscripción** y luego siga las instrucciones para suscribirse a la oferta de pago por uso en AWS Marketplace.



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



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

Puede administrar las suscripciones de AWS Marketplace asociadas con sus cuentas de AWS desde la página Configuración > Credenciales. "Aprenda a administrar sus cuentas y suscripciones de AWS"

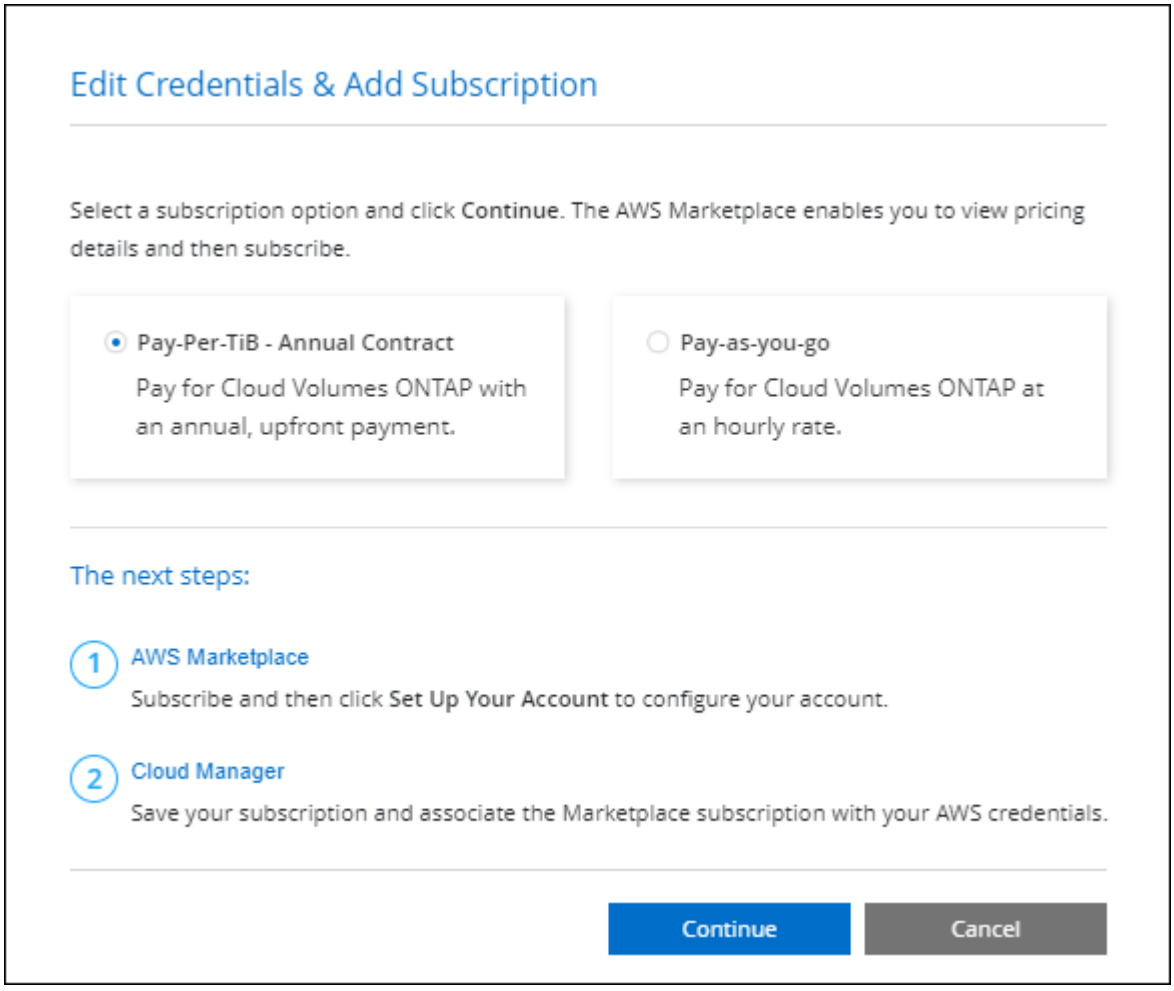
Contrato anual

Pague anualmente comprando un contrato anual en el mercado de su proveedor de nube.

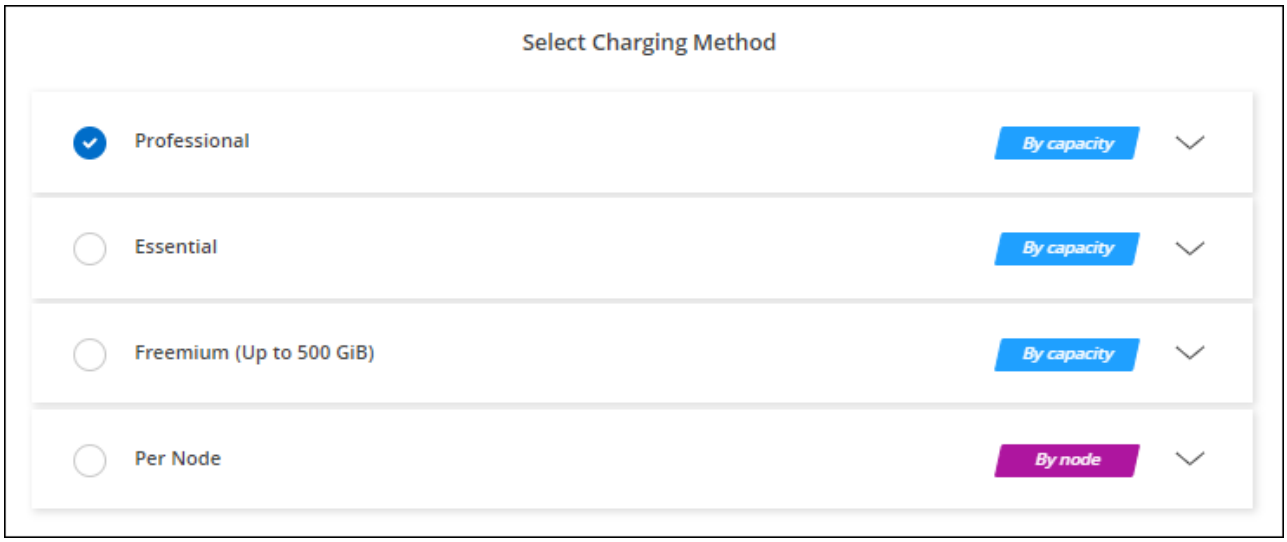
De manera similar a una suscripción por hora, la consola le solicita que se suscriba al contrato anual que está disponible en AWS Marketplace.

Pasos

1. En la página **Sistemas**, haga clic en **Agregar sistema** y siga los pasos.
   a. En la página **Detalles y credenciales**, haga clic en **Editar credenciales > Agregar suscripción** y luego siga las instrucciones para suscribirse al contrato anual en AWS Marketplace.



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



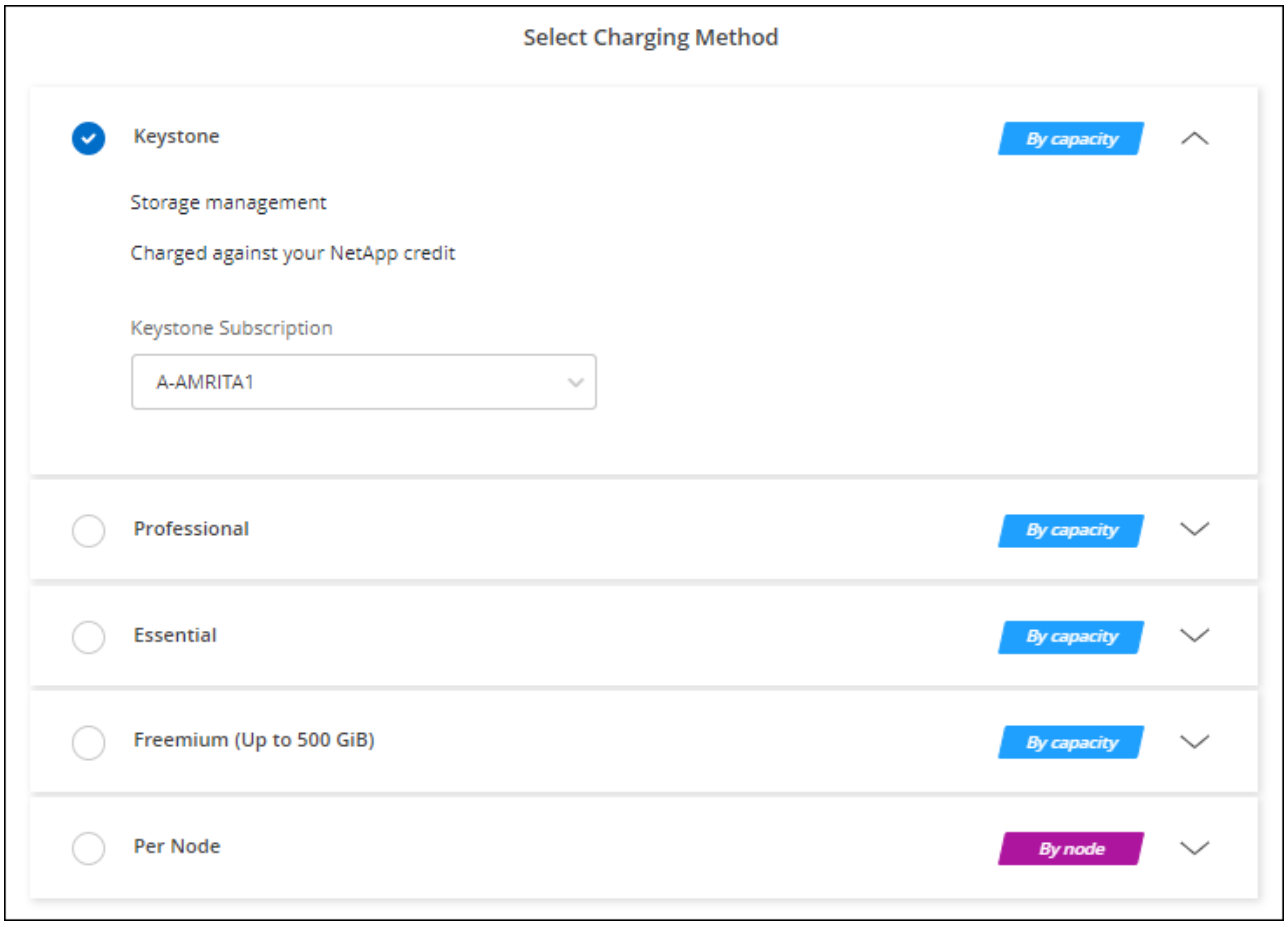
"Vea las instrucciones paso a paso para iniciar Cloud Volumes ONTAP en AWS" .

Suscripción a Keystone

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

Pasos

1. Si aún no tienes una suscripción, "Contactar con NetApp"
2. Contacto NetApp para autorizar su cuenta de usuario con una o más suscripciones de Keystone .
3. Después de que NetApp autorice su cuenta,"Vincula tus suscripciones para usarlas con Cloud Volumes ONTAP" .
4. En la página **Sistemas**, haga clic en **Agregar sistema** y siga los pasos.
    a. Seleccione el método de cobro de suscripción de Keystone cuando se le solicite que elija un método de cobro.



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

Licencia basada en nodos

Una licencia basada en nodos es la licencia de la generación anterior para Cloud Volumes ONTAP. Esta licencia se puede adquirir a través de NetApp (BYOL) y está disponible para renovaciones de licencias, solo en casos específicos. Para obtener información, consulte:

- "Fin de la disponibilidad de las licencias basadas en nodos"
- "Fin de la disponibilidad de las licencias basadas en nodos"
- "Convertir una licencia basada en nodos a una licencia basada en capacidad"

Implemente Cloud Volumes ONTAP en AWS mediante una implementación rápida

Puede implementar Cloud Volumes ONTAP en AWS utilizando un método de implementación rápida tanto para configuraciones de nodo único como de alta disponibilidad (HA). Este proceso simplificado reduce los pasos de implementación en comparación con el método avanzado. También ofrece más claridad en el flujo de trabajo al establecer automáticamente valores predeterminados en una sola página y minimizar la navegación.

Antes de empezar

Necesita lo siguiente para agregar un sistema Cloud Volumes ONTAP en AWS desde la NetApp Console.

- Un agente de consola que está en funcionamiento.
  - Deberías tener una "Agente de consola asociado con su proyecto o espacio de trabajo" .
  - "Debes estar preparado para dejar el agente de consola ejecutándose en todo momento" .
- Una comprensión de la configuración que desea utilizar.

  Debería haberse preparado eligiendo una configuración y obteniendo información de red de AWS de su administrador. Para más detalles, consulte"Planificación de la configuración de Cloud Volumes ONTAP" .
- Una comprensión de lo que se requiere para configurar la licencia para Cloud Volumes ONTAP.

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

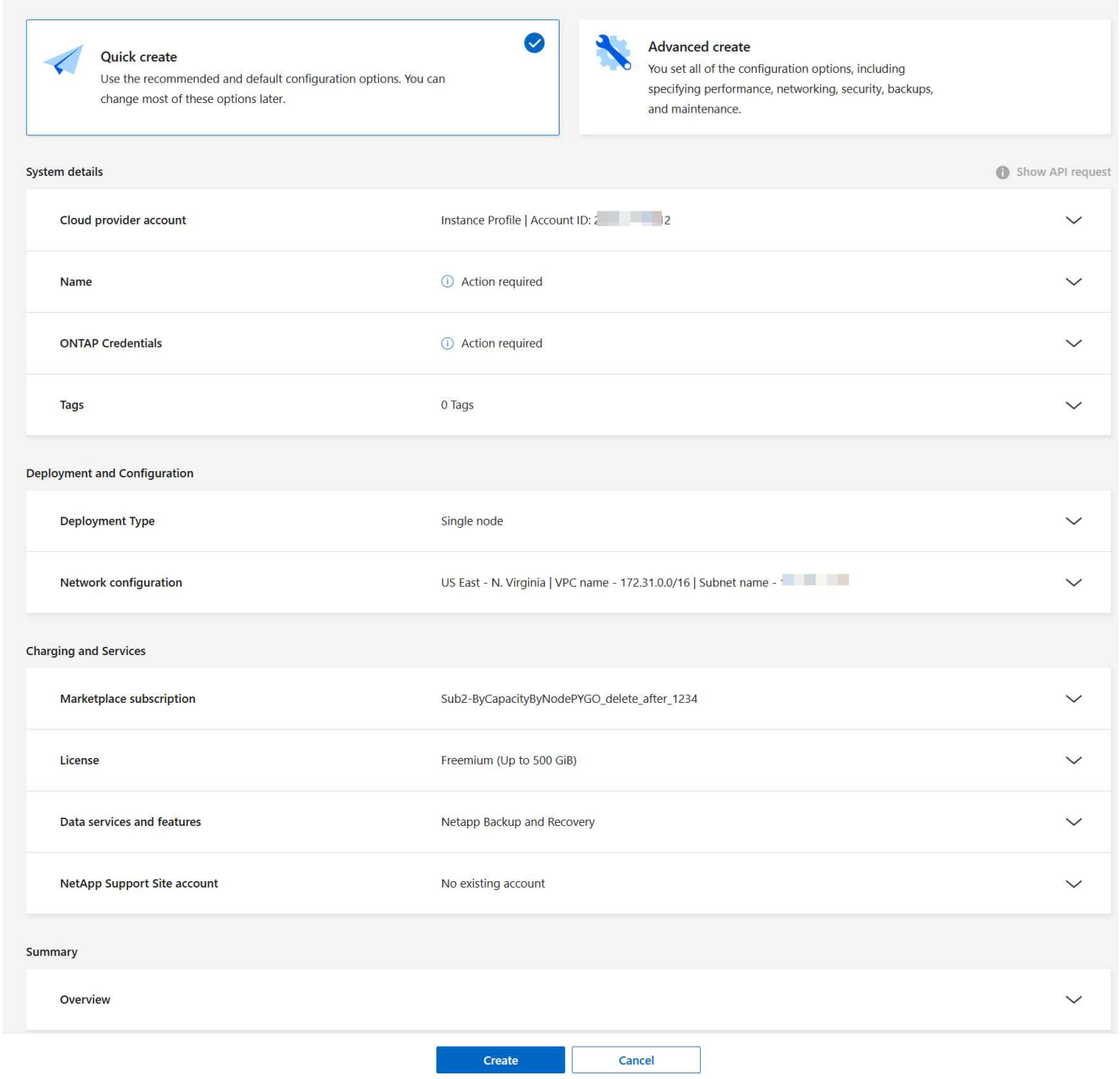
  Para más detalles, consulte"Requisitos de red para Cloud Volumes ONTAP en AWS" .

Acerca de esta tarea

Inmediatamente después de crear el sistema Cloud Volumes ONTAP , la NetApp Console inicia una instancia de prueba en la VPC especificada para verificar la conectividad. Si tiene éxito, la consola finaliza inmediatamente la instancia y luego comienza a implementar el sistema. Si la consola no puede verificar la conectividad, la creación del sistema falla. La instancia de prueba es una `t2.nano` (para tenencia de VPC predeterminada) o una `m3.medium` (para tenencia de VPC dedicada).

Pasos

1. Desde el menú de navegación de la izquierda, seleccione **Almacenamiento > Administración**.
2. En la página Canvas, haga clic en **Agregar sistema** y siga las instrucciones.
3. Seleccione **Amazon Web Services** > * Cloud Volumes ONTAP* > **Agregar nuevo**. La opción **Creación rápida** está seleccionada de forma predeterminada.



detalles del sistema

1. **Cuenta de proveedor de la nube**: los detalles de la cuenta se completan automáticamente en función del agente de consola seleccionado. Si tiene varias cuentas, seleccione la que desea utilizar. Si un agente de consola no está disponible, se le solicitará que "crear un agente de consola" .
2. **Nombre**: El nombre del sistema. La consola usa el nombre del sistema (clúster) para nombrar el sistema Cloud Volumes ONTAP y la instancia de Amazon EC2. También utiliza el nombre como prefijo para el grupo de seguridad predefinido, si selecciona esa opción.
3. * Credenciales de ONTAP * Estas son las credenciales para la cuenta de administrador del clúster Cloud Volumes ONTAP . Puede usar estas credenciales para conectarse a Cloud Volumes ONTAP a través de ONTAP System Manager o la CLI de ONTAP . Puede conservar el nombre de usuario predeterminado *admin* o cambiarlo por un nombre de usuario personalizado.
4. **Etiquetas** Las etiquetas de AWS son metadatos para sus recursos de AWS. La consola agrega las etiquetas a la instancia de Cloud Volumes ONTAP y a cada recurso de AWS asociado con la instancia.

Puede agregar hasta 15 etiquetas desde la interfaz de usuario al crear un sistema Cloud Volumes ONTAP y luego puede agregar más después de su creación. Tenga en cuenta que la API no lo limita a cuatro etiquetas al crear un sistema. Para obtener información sobre las etiquetas, consulte "Documentación de AWS: Cómo etiquetar sus recursos de Amazon EC2" .

Implementación y configuración

1. **Tipo de implementación**: seleccione el tipo de implementación que desea utilizar: nodo único, alta disponibilidad (HA) en una sola zona de disponibilidad (AZ) o HA en varias AZ.
2. **Configuración de red**: Ingrese la información de red que registró en el "Hoja de trabajo de AWS" .
   a. **Región de AWS**: de forma predeterminada, se selecciona la región de la cuenta en la nube asociada que tiene VPC con recursos de subred.
   b. **VPC**: Ingrese una VPC para la región de AWS con una subred. Si no hay subredes, se selecciona el valor predeterminado para la VPC.
   c. **Subred**: puede seleccionar una subred para la VPC solo para una implementación de un solo nodo o una implementación de HA en una sola AZ.

Alta disponibilidad

Si ha seleccionado la configuración HA, ingrese la siguiente información:

HA en una sola AZ

1. **Acceso del mediador**: especifique la información de acceso del mediador. El mediador es una instancia separada que supervisa la salud del par HA y proporciona quórum en caso de falla. Proporcione el nombre del par de claves para permitir que la instancia del mediador se conecte al servicio AWS EC2 y seleccione el método de conexión.

HA en múltiples AZ

1. **Zonas de disponibilidad y mediador**: seleccione las zonas de disponibilidad (AZ) para cada nodo y el mediador y las subredes correspondientes donde desea implementar el par HA de Cloud Volumes ONTAP .
2. **IP flotantes**: si elige varias AZ, especifique las direcciones IP flotantes para los servicios NFS y CIFS y la administración de clústeres y SVM. Las direcciones IP deben estar fuera del bloque CIDR para todas las VPC de la región. Para obtener más detalles, consulte"Requisitos de red de AWS para Cloud Volumes ONTAP HA en varias zonas de disponibilidad" .
3. **Acceso del mediador**: especifique la información de acceso del mediador. El mediador es una instancia separada que supervisa la salud del par HA y proporciona quórum en caso de falla. Proporcione el nombre del par de claves para permitir que la instancia del mediador se conecte al servicio AWS EC2 y seleccione el método de conexión.
4. **Tablas de rutas**: si eligió varias AZ, seleccione las tablas de rutas que incluyan rutas a las direcciones IP flotantes. Si tiene más de una tabla de rutas, es importante seleccionar las tablas de rutas correctas. De lo contrario, es posible que algunos clientes no tengan acceso al par Cloud Volumes ONTAP HA. Para obtener más información sobre las tablas de rutas, consulte la "Documentación de AWS: Tablas de rutas" .

Carga y servicios

1. **Suscripción al mercado**: seleccione la suscripción al mercado de AWS que desea utilizar con este sistema Cloud Volumes ONTAP .
2. **Licencia**: Seleccione el tipo de licencia que desea utilizar con este sistema Cloud Volumes ONTAP . Puede elegir entre licencias Profesional, Esencial y Premium. Para obtener información sobre las

diferentes licencias, consulte"Obtenga más información sobre las licencias de Cloud Volumes ONTAP" .

3. **Servicios y funciones de datos**: Mantenga los servicios habilitados o deshabilite los servicios que no desea utilizar con Cloud Volumes ONTAP.
   - "Obtenga más información sobre la clasificación de NetApp"
   - "Obtenga más información sobre NetApp Backup and Recovery"
   - "Obtenga más información sobre el almacenamiento WORM en Cloud Volumes ONTAP"

     Si desea utilizar WORM y niveles de datos, debe deshabilitar la copia de seguridad y recuperación e implementar un sistema Cloud Volumes ONTAP con la versión 9.8 o superior.

   - *Cuenta del sitio de soporte de NetApp *: si tiene varias cuentas, seleccione la que desee utilizar.

Resumen

Verifique o edite los detalles ingresados y luego haga clic en **Crear**.

Una vez completado el proceso de implementación, no modifique las configuraciones de Cloud Volumes ONTAP generadas por el sistema en el portal de la nube de AWS, especialmente las etiquetas del sistema. Cualquier cambio realizado en estas configuraciones puede provocar un comportamiento inesperado o pérdida de datos.

Enlaces relacionados

- "Planificación de la configuración de Cloud Volumes ONTAP"
- "Implemente Cloud Volumes ONTAP en AWS mediante la implementación avanzada"

Lanzamiento de Cloud Volumes ONTAP en AWS

Puede iniciar Cloud Volumes ONTAP en una configuración de sistema único o como un par de alta disponibilidad en AWS. Este método proporciona una experiencia de implementación avanzada que ofrece más opciones de configuración y flexibilidad que el método de implementación rápida.

Antes de empezar

Necesitará lo siguiente antes de comenzar.

- Un agente de consola que está en funcionamiento.
  - Deberías tener una "Agente de consola asociado con su sistema" .
  - "Debes estar preparado para dejar el agente de consola ejecutándose en todo momento" .
- Una comprensión de la configuración que desea utilizar.

  Debería haberse preparado eligiendo una configuración y obteniendo información de red de AWS de su administrador. Para más detalles, consulte"Planificación de la configuración de Cloud Volumes ONTAP" .

- Una comprensión de lo que se requiere para configurar la licencia para Cloud Volumes ONTAP.

  "Aprenda a configurar las licencias" .

- DNS y Active Directory para configuraciones CIFS.

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

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

Si desea iniciar Cloud Volumes ONTAP en AWS, debe crear un nuevo sistema en la NetApp Console.

Acerca de esta tarea

Inmediatamente después de crear el sistema, la consola lanza una instancia de prueba en la VPC especificada para verificar la conectividad. Si tiene éxito, la consola finaliza inmediatamente la instancia y luego comienza a implementar el sistema Cloud Volumes ONTAP . Si no se puede verificar la conectividad, la creación del sistema falla. La instancia de prueba es una `t2.nano` (para tenencia de VPC predeterminada) o `m3.medium` (para tenencia de VPC dedicada).

Pasos

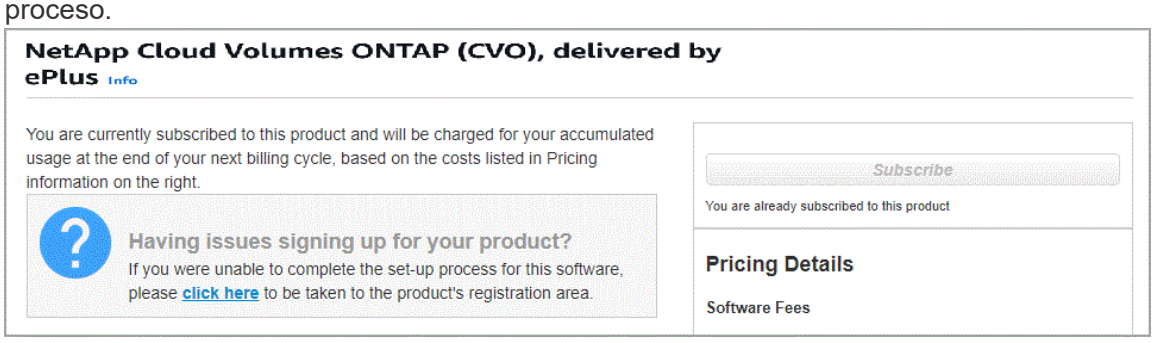
1. Desde el menú de navegación de la izquierda, seleccione **Almacenamiento > Administración**.
2. En la página **Sistemas**, haga clic en **Agregar sistema** y siga las instrucciones.
3. Seleccione **Amazon Web Services** y * Cloud Volumes ONTAP Single Node*.
4. Seleccione **Creación avanzada**. Debido a que el modo **Creación rápida** está seleccionado de manera predeterminada, es posible que vea un mensaje con los valores predeterminados. Haga clic en **Continuar**.
5. Si se le solicita, "crear un agente de consola" .
6. **Detalles y credenciales**: Opcionalmente, cambie las credenciales y la suscripción de AWS, ingrese un nombre de sistema, agregue etiquetas si es necesario y luego ingrese una contraseña.

   Algunos de los campos de esta página se explican por sí solos. La siguiente tabla describe los campos para los que podría necesitar orientación:

Campo	Descripción
Nombre del sistema	La consola usa el nombre del sistema para nombrar tanto el sistema Cloud Volumes ONTAP como 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. La consola agrega las etiquetas a la instancia de Cloud Volumes ONTAP y a cada recurso de AWS asociado con la instancia. Puede agregar hasta cuatro etiquetas desde la interfaz de usuario al crear un sistema y luego puede agregar más una vez creado. Tenga en cuenta que la API no lo limita a cuatro etiquetas al crear un sistema. Para obtener información sobre las etiquetas, consulte "Documentación de AWS: Cómo etiquetar sus recursos de Amazon EC2" .
Nombre de usuario y contraseña	Estas son las credenciales para la cuenta de administrador del clúster de Cloud Volumes ONTAP . Puede usar estas credenciales para conectarse a Cloud Volumes ONTAP a través de ONTAP System Manager o la CLI de ONTAP . Mantenga el nombre de usuario predeterminado *admin* o cámbielo por un nombre de usuario personalizado.

Campo	Descripción
Editar credenciales	Elija las credenciales de AWS asociadas a la cuenta donde desea implementar este sistema. También puede asociar la suscripción al mercado de AWS para usarla con este sistema Cloud Volumes ONTAP . Haga clic en **Añadir suscripción** para asociar las credenciales seleccionadas con una nueva suscripción al marketplace de AWS. La suscripción puede ser anual o por hora. "Descubra cómo agregar credenciales de AWS adicionales a la NetApp Console" .

Si varios usuarios de IAM trabajan en la misma cuenta de AWS, cada usuario debe suscribirse. Una vez que el primer usuario se suscribe, el mercado de AWS informa a los usuarios posteriores que ya están suscritos, como se muestra en la imagen a continuación. Mientras exista una suscripción para la cuenta de AWS, cada usuario de IAM debe asociarse con esa suscripción. Si ve el mensaje que se muestra a continuación, haga clic en el enlace **haga clic aquí** para ir al sitio web de la consola y completar el proceso.



7. **Servicios**: Mantenga los servicios habilitados o deshabilite los servicios individuales que no desea utilizar con Cloud Volumes ONTAP.
   - "Obtenga más información sobre la NetApp Data Classification"
   - "Obtenga más información sobre NetApp Backup and Recovery"

   Si desea utilizar WORM y niveles de datos, debe deshabilitar la función de copia de seguridad y recuperación e implementar un sistema Cloud Volumes ONTAP con la versión 9.8 o superior.

8. **Ubicación y conectividad**: Ingrese la información de red que registró en el "Hoja de trabajo de AWS" .

   La siguiente tabla describe los campos para los que podría necesitar orientación:

Campo	Descripción
VPC	Si tiene un AWS Outpost, puede implementar un sistema Cloud Volumes ONTAP de un solo nodo en ese Outpost seleccionando la VPC de Outpost. La experiencia es la misma que la de cualquier otra VPC que resida en AWS.

Campo	Descripción
Grupo de seguridad generado	Si deja que la consola genere el grupo de seguridad por usted, deberá elegir cómo permitirá el tráfico: • Si elige **Solo VPC seleccionada**, la fuente del tráfico entrante es el rango de subred de la VPC seleccionada y el rango de subred de la VPC donde reside el agente de la consola. Esta es la opción recomendada. • Si elige **Todas las VPC**, la fuente del tráfico entrante es el rango de IP 0.0.0.0/0.
Utilizar el grupo de seguridad existente	Si utiliza una política de firewall existente, asegúrese de que incluya las reglas necesarias. "Obtenga información sobre las reglas de firewall para Cloud Volumes ONTAP" .

9. **Cifrado de datos**: elija sin cifrado de datos o cifrado administrado por AWS.

   Para el cifrado administrado por AWS, puede elegir una clave maestra de cliente (CMK) diferente de su cuenta o de 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 Cloud Volumes ONTAP" .

   "Obtenga más información sobre las tecnologías de cifrado compatibles" .

10. **Métodos de carga y cuenta NSS**: especifique qué opción de carga desea utilizar con este sistema y luego especifique una cuenta del sitio de soporte de NetApp .
    - "Obtenga más información sobre las opciones de licencia para Cloud Volumes ONTAP" .
    - "Aprenda a configurar las licencias" .
11. **Configuración de Cloud Volumes ONTAP * (solo contrato anual del mercado de AWS): 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 necesitará especificar un volumen y luego revisar y aprobar la configuración.

12. **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 elige uno de los paquetes, solo necesita especificar un volumen y luego revisar y aprobar la configuración.

13. **Rol de IAM**: es mejor mantener la opción predeterminada para permitir que la consola cree el rol por usted.

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

14. **Licencia**: cambie la versión de Cloud Volumes ONTAP según sea necesario y seleccione un tipo de instancia y la tenencia de la instancia.

Si hay disponible una versión candidata a lanzamiento, una versión de disponibilidad general o una versión de parche más reciente para la versión seleccionada, la consola actualiza el sistema a esa versión al crear el sistema. Por ejemplo, la actualización se produce si selecciona Cloud Volumes ONTAP 9.13.1 y 9.13.1 P4 está disponible. La actualización no se produce de una versión a otra, por ejemplo, de 9.13 a 9.14.

15. **Recursos de almacenamiento subyacentes**: elija un tipo de disco, configure el almacenamiento subyacente y elija si desea mantener habilitada la clasificación de datos.

    Tenga en cuenta lo siguiente:

    - El tipo de disco es para el volumen inicial (y agregado). Puede elegir un tipo de disco diferente para volúmenes (y agregados) posteriores.
    - Si elige un disco gp3 o io1, la consola utiliza la función Elastic Volumes en AWS para aumentar automáticamente la capacidad del disco de almacenamiento subyacente según sea necesario. Puede elegir la capacidad inicial según sus necesidades de almacenamiento y revisarla después de implementar Cloud Volumes ONTAP . "Obtenga más información sobre la compatibilidad con Elastic Volumes en AWS" .
    - Si elige un disco gp2 o st1, puede seleccionar un tamaño de disco para todos los discos en el agregado inicial y para cualquier agregado adicional que la Consola cree cuando use la opción de aprovisionamiento simple. Puede crear agregados que utilicen un tamaño de disco diferente mediante la opción de asignación avanzada.
    - Puede elegir una política de niveles de volumen específica al crear o editar un volumen.
    - Si deshabilita la clasificación de datos, puede habilitarla en agregados posteriores.

      "Descubra cómo funciona la clasificación de datos" .

16. **Velocidad de escritura y GUSANO**:

    a. Elija velocidad de escritura **Normal** o **Alta**, si lo desea.

       "Obtenga más información sobre la velocidad de escritura" .

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

       No se puede habilitar WORM si la clasificación de datos se habilitó para las versiones 9.7 y anteriores de Cloud Volumes ONTAP . La reversión o degradación a Cloud Volumes ONTAP 9.8 está bloqueada después de habilitar WORM y la clasificación en niveles.

    "Obtenga más información sobre el almacenamiento WORM" .

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

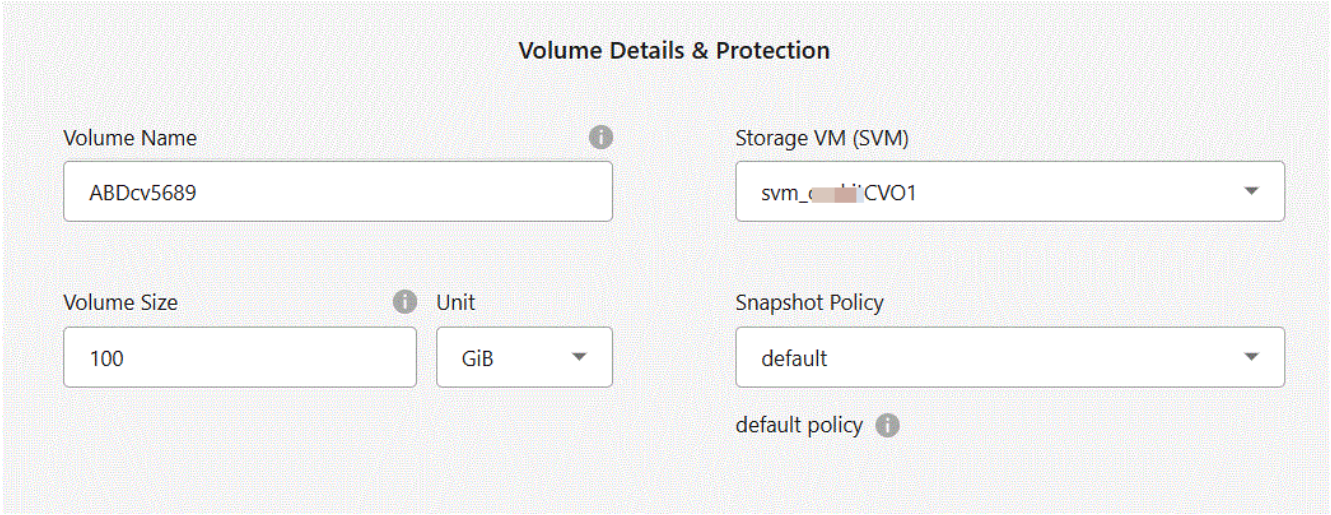
17. **Crear volumen**: Ingrese detalles para el nuevo volumen o haga clic en **Omitir**.

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

    Algunos de los campos de esta página se explican por sí solos. La siguiente tabla describe los campos para los que podría necesitar orientación:

Campo	Descripción
Size	El tamaño máximo que puede ingresar depende en gran medida de si habilita el aprovisionamiento fino, que le permite crear un volumen que sea más grande que el almacenamiento físico actualmente disponible para él.
Control de acceso (solo para NFS)	Una política de exportación define los clientes de la subred que pueden acceder al volumen. De forma predeterminada, la consola ingresa un valor que proporciona acceso a todas las instancias de la subred.
Permisos y usuarios/grupos (solo para CIFS)	Estos campos le permiten controlar el nivel de acceso a un recurso compartido para usuarios y grupos (también llamados listas de control de acceso o ACL). Puede especificar usuarios o grupos de Windows locales o de dominio, o usuarios o grupos de UNIX. Si especifica un nombre de usuario de dominio de Windows, debe incluir el dominio del usuario utilizando el formato dominio\nombre de usuario.
Política de instantáneas	Una política de copia de instantáneas especifica la frecuencia y la cantidad de copias de instantáneas de NetApp creadas automáticamente. Una copia Snapshot de NetApp es una imagen del sistema de archivos en un momento determinado que no tiene impacto en el rendimiento y requiere un almacenamiento mínimo. Puede elegir la política predeterminada o ninguna. Puede elegir ninguno para 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 iniciador e IQN (solo para iSCSI)	Los objetivos de almacenamiento iSCSI se denominan LUN (unidades lógicas) y se presentan a los hosts como dispositivos de bloque estándar. Los grupos de iniciadores son tablas de nombres de nodos de host iSCSI y controlan qué iniciadores tienen acceso a qué LUN. Los objetivos iSCSI se conectan a la red a través de adaptadores de red Ethernet estándar (NIC), tarjetas de motor de descarga TCP (TOE) con iniciadores de software, adaptadores de red convergente (CNA) o adaptadores de bus de host dedicados (HBA) y se identifican mediante nombres calificados iSCSI (IQN). Cuando crea un volumen iSCSI, la consola crea automáticamente un LUN para usted. Lo hemos simplificado creando solo un LUN por volumen, por lo que no es necesario realizar ninguna gestión. Después de crear el volumen,"Utilice el IQN para conectarse al LUN desde sus hosts" .

La siguiente imagen muestra la primera página del asistente de creación de volumen:



18. **Configuración CIFS**: si eligió el protocolo CIFS, configure un servidor CIFS.

Campo	Descripción
Dirección IP primaria y secundaria de DNS	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 ubicar los servidores LDAP de Active Directory y los controladores de dominio para el 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	El nombre y la contraseña de una cuenta de Windows con privilegios suficientes para agregar computadoras a la unidad organizativa (OU) especificada dentro del dominio de AD.
Nombre NetBIOS del servidor CIFS	Un nombre de servidor CIFS que es único en el dominio AD.
Unidad organizativa	La unidad organizativa dentro del dominio AD para asociarse con el servidor CIFS. El valor predeterminado es CN=Computers. Si configura AWS Managed Microsoft AD como servidor AD para Cloud Volumes ONTAP, debe ingresar **OU=Computers,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 utilizando el DNS de Active Directory. Si necesita configurar un servidor NTP utilizando una dirección diferente, debe utilizar la API. Consulte la "Documentación de automatización de la NetApp Console" Para más detalles. Tenga en cuenta que solo puede configurar un servidor NTP al crear un servidor CIFS. No es configurable después de crear el servidor CIFS.

19. **Perfil de uso, tipo de disco y política de niveles**: elija si desea habilitar las funciones de eficiencia de almacenamiento y editar la política de niveles de volumen, si es necesario.

    Para obtener más información, consulte"Comprensión de los perfiles de uso del volumen" ,"Descripción general de la clasificación de datos" , y "KB: ¿Qué funciones de eficiencia de almacenamiento en línea son

compatibles con CVO?"

20. **Revisar y aprobar**: revise y confirme sus selecciones.
    a. Revise los detalles sobre la configuración.
    b. Haga clic en **Más información** para revisar los detalles sobre el soporte y los recursos de AWS que comprará la consola.
    c. Seleccione la casilla de verificación **Entiendo…**.
    d. Haga clic en **Ir**.

Resultado

La consola inicia la instancia de Cloud Volumes ONTAP . Puede seguir el progreso en la página **Auditoría**.

Si tiene algún problema al iniciar la instancia de Cloud Volumes ONTAP , revise el mensaje de error. También puede seleccionar el sistema y hacer clic en **Recrear entorno**.

Para obtener ayuda adicional, visite "Compatibilidad con NetApp Cloud Volumes ONTAP" .

Una vez completado el proceso de implementación, no modifique las configuraciones de Cloud Volumes ONTAP generadas por el sistema en el portal de la nube de AWS, especialmente las etiquetas del sistema. Cualquier cambio realizado en estas configuraciones puede provocar un comportamiento inesperado o pérdida de datos.

Después de terminar

- Si aprovisionó un recurso compartido CIFS, otorgue a los usuarios o grupos permisos para los archivos y carpetas y verifique que esos usuarios puedan acceder al recurso compartido y crear un archivo.
- Si desea aplicar cuotas a los volúmenes, utilice el Administrador del sistema ONTAP o la CLI de ONTAP .

  Las cuotas le permiten restringir o rastrear el espacio en disco y la cantidad de archivos utilizados por un usuario, grupo o qtree.

Lanzar un par de Cloud Volumes ONTAP HA en AWS

Si desea iniciar un par de HA de Cloud Volumes ONTAP en AWS, debe crear un sistema de HA en la consola.

Limitación

En este momento, los pares HA no son compatibles con AWS Outposts.

Acerca de esta tarea

Inmediatamente después de crear el sistema Cloud Volumes ONTAP , la consola inicia una instancia de prueba en la VPC especificada para verificar la conectividad. Si tiene éxito, la consola finaliza inmediatamente la instancia y luego comienza a implementar el sistema Cloud Volumes ONTAP . Si no se puede verificar la conectividad, la creación del sistema falla. La instancia de prueba es una `t2.nano` (para tenencia de VPC predeterminada) o `m3.medium` (para tenencia de VPC dedicada).

Pasos

1. Desde el menú de navegación de la izquierda, seleccione **Almacenamiento > Administración**.
2. En la página **Sistemas**, haga clic en **Agregar sistema** y siga las instrucciones.
3. Seleccione **Amazon Web Services** y * Cloud Volumes ONTAP HA*.

   Algunas zonas locales de AWS están disponibles.

Antes de poder utilizar las Zonas locales de AWS, debe habilitarlas y crear una subred en la Zona local en su cuenta de AWS. Siga los pasos **Inscribirse en una zona local de AWS** y **Ampliar su VPC de Amazon a la zona local** en el"Tutorial de AWS "Comience a implementar aplicaciones de baja latencia con AWS Local Zones"" .

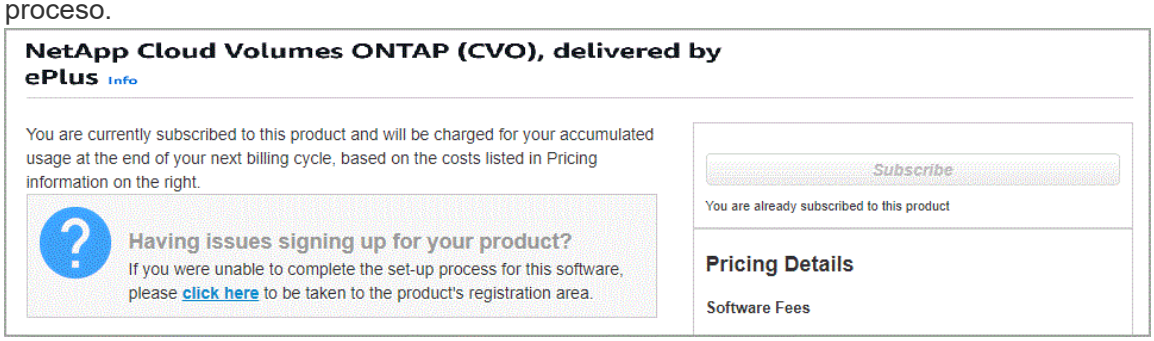
Si está ejecutando el agente de consola 3.9.36 o anterior, debe agregar el `DescribeAvailabilityZones` permiso para el rol de AWS en la consola de AWS EC2.

4. **Detalles y credenciales**: Opcionalmente, cambie las credenciales y la suscripción de AWS, ingrese un nombre de sistema, agregue etiquetas si es necesario y luego ingrese una contraseña.

   Algunos de los campos de esta página se explican por sí solos. La siguiente tabla describe los campos para los que podría necesitar orientación:

Campo	Descripción
Nombre del sistema	La consola usa el nombre del sistema para nombrar tanto el sistema Cloud Volumes ONTAP como 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. La consola agrega las etiquetas a la instancia de Cloud Volumes ONTAP y a cada recurso de AWS asociado con la instancia. Puede agregar hasta cuatro etiquetas desde la interfaz de usuario al crear un sistema y luego puede agregar más una vez creado. Tenga en cuenta que la API no lo limita a cuatro etiquetas al crear un sistema. Para obtener información sobre las etiquetas, consulte "Documentación de AWS: Cómo etiquetar sus recursos de Amazon EC2" .
Nombre de usuario y contraseña	Estas son las credenciales para la cuenta de administrador del clúster de Cloud Volumes ONTAP . Puede usar estas credenciales para conectarse a Cloud Volumes ONTAP a través de ONTAP System Manager o la CLI de ONTAP . Mantenga el nombre de usuario predeterminado *admin* o cámbielo por un nombre de usuario personalizado.
Editar credenciales	Seleccione las credenciales de AWS y la suscripción al marketplace para usar con este sistema Cloud Volumes ONTAP . Haga clic en **Añadir suscripción** para asociar las credenciales seleccionadas con una nueva suscripción al marketplace de AWS. La suscripción puede ser anual o por hora. Si adquirió una licencia directamente de NetApp (traiga su propia licencia [BYOL]), no necesita una suscripción a AWS. NetApp ha restringido la compra, extensión y renovación de licencias BYOL. Para más información, consulte "Disponibilidad restringida de licencias BYOL para Cloud Volumes ONTAP" . "Aprenda a agregar credenciales de AWS adicionales a la consola" .

Si varios usuarios de IAM trabajan en la misma cuenta de AWS, cada usuario debe suscribirse. Una vez que el primer usuario se suscribe, el mercado de AWS informa a los usuarios posteriores que ya están suscritos, como se muestra en la imagen a continuación. Mientras exista una suscripción para la cuenta de AWS, cada usuario de IAM debe asociarse con esa suscripción. Si ve el mensaje que se muestra a continuación, haga clic en el enlace **haga clic aquí** para ir al sitio web de la consola y completar el proceso.



5. **Servicios**: Mantenga los servicios habilitados o deshabilite los servicios individuales que no desea utilizar con este sistema Cloud Volumes ONTAP .
   - "Obtenga más información sobre la NetApp Data Classification"
   - "Obtenga más información sobre copias de seguridad y recuperación"

   Si desea utilizar WORM y niveles de datos, debe deshabilitar la función de copia de seguridad y recuperación e implementar un sistema Cloud Volumes ONTAP con la versión 9.8 o superior.

6. **Modelos de implementación de HA**: elija una configuración de HA.

   Para obtener una descripción general de los modelos de implementación, consulte"Cloud Volumes ONTAP HA para AWS" .

7. **Ubicación y conectividad** (zona de disponibilidad única (AZ)) o **Región y VPC** (múltiples AZ): ingrese la información de red que registró en la hoja de cálculo de AWS.

   La siguiente tabla describe los campos para los que podría necesitar orientación:

Campo	Descripción
Grupo de seguridad generado	Si deja que la consola genere el grupo de seguridad por usted, deberá elegir cómo permitirá el tráfico: • Si elige **Solo VPC seleccionada**, la fuente del tráfico entrante es el rango de subred de la VPC seleccionada y el rango de subred de la VPC donde reside el agente de la consola. Esta es la opción recomendada. • Si elige **Todas las VPC**, la fuente del tráfico entrante es el rango de IP 0.0.0.0/0.
Utilizar el grupo de seguridad existente	Si utiliza una política de firewall existente, asegúrese de que incluya las reglas necesarias. "Obtenga 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 eligió varias AZ, especifique las direcciones IP flotantes.

   Las direcciones IP deben estar fuera del bloque CIDR para todas las VPC de la región. Para obtener más detalles, consulte"Requisitos de red de AWS para Cloud Volumes ONTAP HA en varias zonas de disponibilidad" .

10. **Tablas de rutas**: si eligió varias AZ, 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 Cloud Volumes ONTAP HA. Para obtener más información sobre las tablas de rutas, consulte la "Documentación de AWS: Tablas de rutas" .

11. **Cifrado de datos**: elija sin cifrado de datos o cifrado administrado por AWS.

    Para el cifrado administrado por AWS, puede elegir una clave maestra de cliente (CMK) diferente de su cuenta o de 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 Cloud Volumes ONTAP" .

    "Obtenga más información sobre las tecnologías de cifrado compatibles" .

12. **Métodos de carga y cuenta NSS**: especifique qué opción de carga desea utilizar con este sistema y luego especifique una cuenta del sitio de soporte de NetApp .
    - "Obtenga más información sobre las opciones de licencia para Cloud Volumes ONTAP" .
    - "Aprenda a configurar las licencias" .
13. **Configuración de Cloud Volumes ONTAP * (solo 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 necesitará especificar un volumen y luego revisar y aprobar la configuración.

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

    Si elige uno de los paquetes, solo necesita especificar un volumen y luego revisar y aprobar la configuración.

15. **Rol de IAM**: es mejor mantener la opción predeterminada para permitir que la consola cree el rol por usted.

    Si prefiere utilizar su propia póliza, debe cumplir"Requisitos de política para los nodos de Cloud Volumes ONTAP y el mediador de alta disponibilidad" .

16. **Licencia**: cambie la versión de Cloud Volumes ONTAP según sea necesario y seleccione un tipo de instancia y la tenencia de la instancia.

Si hay disponible una versión candidata a lanzamiento, una versión de disponibilidad general o una versión de parche más reciente para la versión seleccionada, la consola actualiza el sistema a esa versión al crear el sistema. Por ejemplo, la actualización se produce si selecciona Cloud Volumes ONTAP 9.13.1 y 9.13.1 P4 está disponible. La actualización no se produce de una versión a otra, por ejemplo, de 9.13 a 9.14.

17. **Recursos de almacenamiento subyacentes**: elija un tipo de disco, configure el almacenamiento subyacente y elija si desea mantener habilitada la clasificación de datos.

    Tenga en cuenta lo siguiente:

    - El tipo de disco es para el volumen inicial (y agregado). Puede elegir un tipo de disco diferente para volúmenes (y agregados) posteriores.
    - Si elige un disco gp3 o io1, la consola utiliza la función Elastic Volumes en AWS para aumentar automáticamente la capacidad del disco de almacenamiento subyacente según sea necesario. Puede elegir la capacidad inicial según sus necesidades de almacenamiento y revisarla después de implementar Cloud Volumes ONTAP . "Obtenga más información sobre la compatibilidad con Elastic Volumes en AWS" .
    - Si elige un disco gp2 o st1, puede seleccionar un tamaño de disco para todos los discos en el agregado inicial y para cualquier agregado adicional que la Consola cree cuando use la opción de aprovisionamiento simple. Puede crear agregados que utilicen un tamaño de disco diferente mediante la opción de asignación avanzada.
    - Puede elegir una política de niveles de volumen específica al crear o editar un volumen.
    - Si deshabilita la clasificación de datos, puede habilitarla en agregados posteriores.

      "Descubra cómo funciona la clasificación de datos" .

18. **Velocidad de escritura y GUSANO**:

    a. Elija velocidad de escritura **Normal** o **Alta**, si lo desea.

       "Obtenga más información sobre la velocidad de escritura" .

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

       No se puede habilitar WORM si la clasificación de datos se habilitó para las versiones 9.7 y anteriores de Cloud Volumes ONTAP . La reversión o degradación a Cloud Volumes ONTAP 9.8 está bloqueada después de habilitar WORM y la clasificación en niveles.

    "Obtenga más información sobre el almacenamiento WORM" .

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

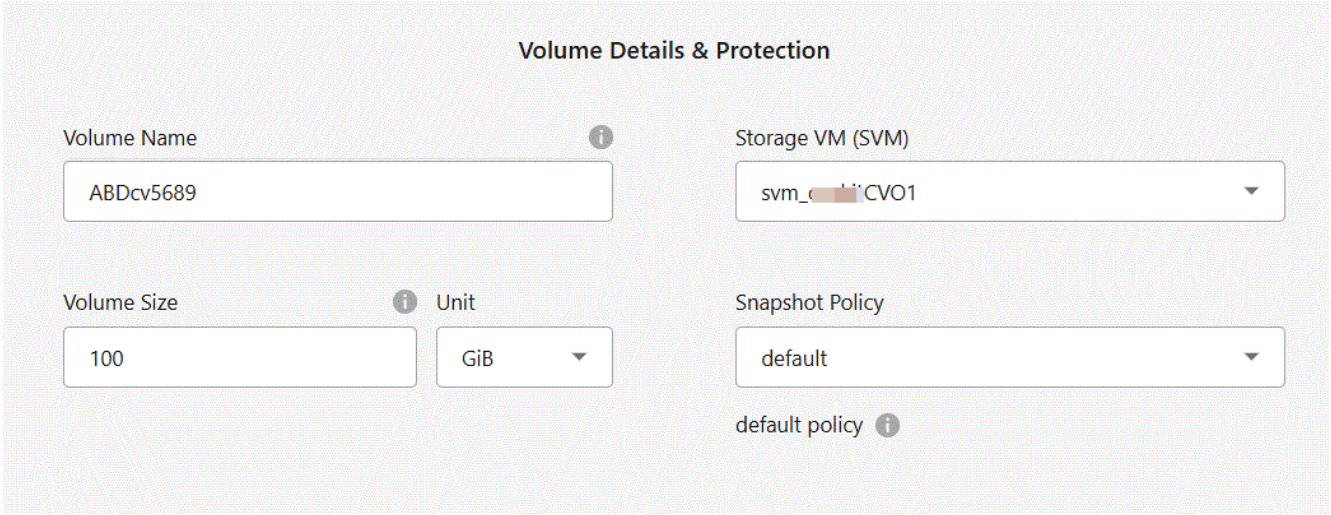
19. **Crear volumen**: Ingrese detalles para el nuevo volumen o haga clic en **Omitir**.

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

    Algunos de los campos de esta página se explican por sí solos. La siguiente tabla describe los campos para los que podría necesitar orientación:

Campo	Descripción
Size	El tamaño máximo que puede ingresar depende en gran medida de si habilita el aprovisionamiento fino, que le permite crear un volumen que sea más grande que el almacenamiento físico actualmente disponible para él.
Control de acceso (solo para NFS)	Una política de exportación define los clientes de la subred que pueden acceder al volumen. De forma predeterminada, la consola ingresa un valor que proporciona acceso a todas las instancias de la subred.
Permisos y usuarios/grupos (solo para CIFS)	Estos campos le permiten controlar el nivel de acceso a un recurso compartido para usuarios y grupos (también llamados listas de control de acceso o ACL). Puede especificar usuarios o grupos de Windows locales o de dominio, o usuarios o grupos de UNIX. Si especifica un nombre de usuario de dominio de Windows, debe incluir el dominio del usuario utilizando el formato dominio\nombre de usuario.
Política de instantáneas	Una política de copia de instantáneas especifica la frecuencia y la cantidad de copias de instantáneas de NetApp creadas automáticamente. Una copia Snapshot de NetApp es una imagen del sistema de archivos en un momento determinado que no tiene impacto en el rendimiento y requiere un almacenamiento mínimo. Puede elegir la política predeterminada o ninguna. Puede elegir ninguno para 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 iniciador e IQN (solo para iSCSI)	Los objetivos de almacenamiento iSCSI se denominan LUN (unidades lógicas) y se presentan a los hosts como dispositivos de bloque estándar. Los grupos de iniciadores son tablas de nombres de nodos de host iSCSI y controlan qué iniciadores tienen acceso a qué LUN. Los objetivos iSCSI se conectan a la red a través de adaptadores de red Ethernet estándar (NIC), tarjetas de motor de descarga TCP (TOE) con iniciadores de software, adaptadores de red convergente (CNA) o adaptadores de bus de host dedicados (HBA) y se identifican mediante nombres calificados iSCSI (IQN). Cuando crea un volumen iSCSI, la consola crea automáticamente un LUN para usted. Lo hemos simplificado creando solo un LUN por volumen, por lo que no es necesario realizar ninguna gestión. Después de crear el volumen,"Utilice el IQN para conectarse al LUN desde sus hosts" .

La siguiente imagen muestra la primera página del asistente de creación de volumen:



20. **Configuración CIFS**: si seleccionó el protocolo CIFS, configure un servidor CIFS.

Campo	Descripción
Dirección IP primaria y secundaria de DNS	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 ubicar los servidores LDAP de Active Directory y los controladores de dominio para el 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	El nombre y la contraseña de una cuenta de Windows con privilegios suficientes para agregar computadoras a la unidad organizativa (OU) especificada dentro del dominio de AD.
Nombre NetBIOS del servidor CIFS	Un nombre de servidor CIFS que es único en el dominio AD.
Unidad organizativa	La unidad organizativa dentro del dominio AD para asociarse con el servidor CIFS. El valor predeterminado es CN=Computers. Si configura AWS Managed Microsoft AD como servidor AD para Cloud Volumes ONTAP, debe ingresar **OU=Computers,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 utilizando el DNS de Active Directory. Si necesita configurar un servidor NTP utilizando una dirección diferente, debe utilizar la API. Consulte la "Documentación de automatización de la NetApp Console" Para más detalles. Tenga en cuenta que solo puede configurar un servidor NTP al crear un servidor CIFS. No es configurable después de crear el servidor CIFS.

21. **Perfil de uso, tipo de disco y política de niveles**: elija si desea habilitar las funciones de eficiencia de almacenamiento y editar la política de niveles de volumen, si es necesario.

    Para obtener más información, consulte"Elija un perfil de uso de volumen" y"Descripción general de la clasificación de datos" .

22. **Revisar y aprobar**: revise y confirme sus selecciones.
    a. Revise los detalles sobre la configuración.
    b. Haga clic en **Más información** para revisar los detalles sobre el soporte y los recursos de AWS que comprará la consola.
    c. Seleccione la casilla de verificación **Entiendo…**.
    d. Haga clic en **Ir**.

Resultado

La consola lanza el par Cloud Volumes ONTAP HA. Puede seguir el progreso en la página **Auditoría**.

Si experimenta algún problema al iniciar el par HA, revise el mensaje de error. También puede seleccionar el sistema y hacer clic en Recrear entorno.

Para obtener ayuda adicional, visite "Compatibilidad con NetApp Cloud Volumes ONTAP" .

Después de terminar

- Si aprovisionó un recurso compartido CIFS, otorgue a los usuarios o grupos permisos para los archivos y carpetas y verifique que esos usuarios puedan acceder al recurso compartido y crear un archivo.
- Si desea aplicar cuotas a los volúmenes, utilice el Administrador del sistema ONTAP o la CLI de ONTAP .

  Las cuotas le permiten restringir o rastrear el espacio en disco y la cantidad de archivos utilizados por un usuario, grupo o qtree.

Una vez completado el proceso de implementación, no modifique las configuraciones de Cloud Volumes ONTAP generadas por el sistema en el portal de la nube de AWS, especialmente las etiquetas del sistema. Cualquier cambio realizado en estas configuraciones puede provocar un comportamiento inesperado o pérdida de datos.

Enlaces relacionados

- "Planificación de la configuración de Cloud Volumes ONTAP"
- "Implemente Cloud Volumes ONTAP en AWS mediante una implementación rápida"

Implementar Cloud Volumes ONTAP en AWS Secret Cloud o AWS Top Secret Cloud

De manera similar a una región estándar de AWS, puede usar la NetApp Console en"Nube secreta de AWS" y en"Nube de alto secreto de AWS" para implementar Cloud Volumes ONTAP, que proporciona funciones de clase empresarial para su almacenamiento en la nube. AWS Secret Cloud y Top Secret Cloud son regiones cerradas específicas de la Comunidad de Inteligencia de EE. UU.; las instrucciones de esta página solo se aplican a los usuarios de las regiones AWS Secret Cloud y Top Secret Cloud.

Antes de empezar

Antes de comenzar, revise las versiones compatibles con AWS Secret Cloud y Top Secret Cloud, y obtenga información sobre el modo privado en la consola.

- Revise las siguientes versiones compatibles con AWS Secret Cloud y Top Secret Cloud:

- Cloud Volumes ONTAP 9.12.1 P2
- Versión 3.9.32 del agente de consola

  El agente de consola es necesario para implementar y administrar Cloud Volumes ONTAP en AWS. Iniciará sesión en la consola desde el software que se instala en la instancia del agente de la consola. El sitio web SaaS para la consola no es compatible con AWS Secret Cloud y Top Secret Cloud.

- Conozca el modo privado

  En AWS Secret Cloud y Top Secret Cloud, la consola funciona en *modo privado*. En el modo privado, no hay conectividad a la capa SaaS desde la consola. Puede acceder a la consola a través de una aplicación web local que pueda acceder al agente de la consola.

  Para obtener más información sobre cómo funciona el modo privado, consulte"el modo de implementación privada en la consola" .

Paso 1: Configura tu red

Configure su red de AWS para que Cloud Volumes ONTAP pueda funcionar correctamente.

Pasos

1. Elija la VPC y las subredes en las que desea iniciar la instancia del agente de consola y las instancias de Cloud Volumes ONTAP .
2. Asegúrese de que su VPC y sus subredes admitan la conectividad entre el agente de la consola y Cloud Volumes ONTAP.
3. Configura un punto final de VPC para el servicio Amazon Simple Storage Service (Amazon S3).

   Se requiere un punto final de VPC si desea organizar en niveles datos fríos de Cloud Volumes ONTAP en un almacenamiento de objetos de bajo costo.

Paso 2: Configurar permisos

Configure políticas y roles de IAM que proporcionen al agente de la consola y a Cloud Volumes ONTAP los permisos que necesitan para realizar acciones en AWS Secret Cloud o Top Secret Cloud.

Necesita una política de IAM y un rol de IAM para cada uno de los siguientes:

- La instancia del agente de consola
- Instancias de Cloud Volumes ONTAP
- Para pares de alta disponibilidad, la instancia del mediador de alta disponibilidad de Cloud Volumes ONTAP (si desea implementar pares de alta disponibilidad)

Pasos

1. Vaya a la consola de AWS IAM y haga clic en **Políticas**.
2. Cree una política para la instancia del agente de consola.

   Crea estas políticas para respaldar los depósitos S3 en tu entorno de AWS. Al crear los depósitos más tarde, asegúrese de que los nombres de los depósitos tengan el prefijo `fabric-pool-` . Este requisito se aplica tanto a las regiones AWS Secret Cloud como a las Top Secret Cloud.

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 de alto secreto

```
{
    "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. Cree 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 de alto secreto

```
{
    "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 los pares de alta disponibilidad, si planea implementar 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 de IAM con el tipo de rol Amazon EC2 y adjunte las políticas que creó en los pasos anteriores.

   Crear el rol:

   De manera similar a las políticas, debe tener un rol de IAM para el agente de consola y uno para los nodos de Cloud Volumes ONTAP . Para pares de alta disponibilidad: de manera similar a las políticas, debe tener un rol de IAM para el agente de consola, uno para los nodos de Cloud Volumes ONTAP y uno para el mediador de alta disponibilidad (si desea implementar pares de alta disponibilidad).

   Seleccione el rol:

   Debe seleccionar la función IAM del agente de consola cuando inicie la instancia del agente de consola. Puede seleccionar los roles de IAM para Cloud Volumes ONTAP cuando crea un sistema Cloud Volumes ONTAP desde la consola. Para los pares de alta disponibilidad, puede seleccionar los roles de IAM para Cloud Volumes ONTAP y el mediador de alta disponibilidad cuando crea un sistema Cloud Volumes ONTAP .

Paso 3: Configurar AWS KMS

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

Pasos

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

   La CMK puede ser una CMK administrada por AWS o una CMK administrada por el cliente.

2. Si la CMK está en una cuenta de AWS separada de la cuenta donde planea implementar Cloud Volumes ONTAP, entonces deberá obtener el ARN de esa clave.

   Debe proporcionar el ARN a la consola cuando crea el sistema Cloud Volumes ONTAP .

3. Agregue la función IAM para la instancia a la lista de usuarios clave para una CMK.

   Esto le otorga a la consola permisos para usar la CMK con Cloud Volumes ONTAP.

Paso 4: Instalar el agente de la consola y configurar la consola

Antes de poder comenzar a usar la consola para implementar Cloud Volumes ONTAP en AWS, debe instalar y configurar el agente de la consola. Permite que la consola administre recursos y procesos dentro de su entorno de nube pública (esto incluye Cloud Volumes ONTAP).

Pasos

1. Obtenga un certificado raíz firmado por una autoridad de certificación (CA) en el formato X.509 codificado en Base-64 de Privacy Enhanced Mail (PEM). 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` certificado, y para Top Secret Cloud, el `Amazon Root CA 4` certificado. Asegúrese de cargar solo estos certificados y no la cadena completa. El archivo de la cadena de certificados es grande y la carga puede fallar. Si tiene certificados adicionales, puede cargarlos más tarde, como se describe en el siguiente paso.

   Debes cargar el certificado durante el proceso de configuración. La consola utiliza el certificado confiable al enviar solicitudes a AWS a través de HTTPS.

2. Inicie la instancia del agente de consola:
   a. Vaya a la página de AWS Intelligence Community Marketplace para obtener la consola.
   b. En la pestaña Lanzamiento personalizado, elija 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.
      - Debes elegir la función de IAM que creaste al configurar los permisos.
      - Debes mantener las opciones de almacenamiento predeterminadas.
      - Los métodos de conexión necesarios para el agente de consola son los siguientes: SSH, HTTP y HTTPS.
3. Configurar la consola desde un host que tenga una conexión a la instancia:
   a. Abra un navegador web e ingrese https://ipaddress donde ipaddress es la dirección IP del host Linux donde instaló el agente de consola.
   b. Especifique un servidor proxy para la conectividad a los servicios de AWS.
   c. Sube el certificado que obtuviste en el paso 1.
   d. Siga las instrucciones para configurar un nuevo sistema.
      - **Detalles del sistema**: Ingrese un nombre para el agente de consola y el nombre de su empresa.
      - **Crear usuario administrador**: crea 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 la consola.

- **Revisar**: Revise los detalles, acepte el acuerdo de licencia y luego seleccione **Configurar**.

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

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

Paso 5: (opcional) Instalar un certificado de modo privado

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

Pasos

1. Enumerar los certificados instalados existentes.
   a. Para recopilar el ID del contenedor occm (nombre identificado “ds-occm-1”), ejecute el siguiente comando:

```
docker ps
```

   b. Para ingresar 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 use la contraseña recopilada en el paso anterior:

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

2. Añadir un certificado.
   a. Para recopilar el ID de Docker del contenedor occm (nombre identificado “ds-occm-1”), ejecute el siguiente comando:

```
docker ps
```

   b. Para ingresar 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 use 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: Agregar una licencia a la consola

Si compró una licencia de NetApp, debe agregarla a la consola para poder seleccionarla cuando cree un nuevo sistema Cloud Volumes ONTAP . Estas licencias permanecerán sin asignar hasta que las asocie con un nuevo sistema Cloud Volumes ONTAP .

Pasos

1. Desde el menú de navegación de la izquierda, seleccione * Licenses and subscriptions*.
2. En el panel * Cloud Volumes ONTAP*, seleccione **Ver**.
3. En la pestaña * Cloud Volumes ONTAP*, seleccione **Licencias > Licencias basadas en nodos**.
4. Haga clic en **Sin asignar**.
5. Haga clic en **Agregar licencias no asignadas**.
6. Ingrese el número de serie de la licencia o cargue el archivo de licencia.

7. Si aún no tiene el archivo de licencia, deberá cargarlo manualmente desde netapp.com.
    a. Ir a la"Generador de archivos de licencia de NetApp" e inicie sesión utilizando sus credenciales del sitio de soporte de NetApp .
    b. Ingrese su contraseña, elija su producto, ingrese el número de serie, confirme que ha leído y aceptado la política de privacidad y luego haga clic en **Enviar**.
    c. Elija si desea recibir el archivo JSON serialnumber.NLF por correo electrónico o descarga directa.
8. Haga clic en **Agregar licencia**.

Resultado

La consola agrega la licencia como no asignada hasta que la asocie con un nuevo sistema Cloud Volumes ONTAP . Puede ver la licencia en el menú de navegación izquierdo en * Licenses and subscriptions > Cloud Volumes ONTAP > Ver > Licencias*.

Paso 7: Inicie Cloud Volumes ONTAP desde la consola

Puede iniciar instancias de Cloud Volumes ONTAP en AWS Secret Cloud y Top Secret Cloud creando nuevos sistemas en la consola.

Antes de empezar

Para los pares de HA, se requiere un par de claves para habilitar la autenticación SSH basada en clave para el mediador de HA.

Pasos

1. En la página **Sistemas**, haga clic en **Agregar sistema**.
2. En **Crear**, seleccione 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 .

> Al realizar selecciones a través del asistente, no seleccione **Data Sense & Compliance** y **Backup to Cloud** en **Servicios**. En **Paquetes preconfigurados**, seleccione solamente **Cambiar configuración** y asegúrese de no haber seleccionado ninguna otra opción. Los paquetes preconfigurados no son compatibles con las regiones AWS Secret Cloud y Top Secret Cloud y, si se seleccionan, su implementación fallará.

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

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

- Debe configurar una puerta de enlace de tránsito cuando implemente Cloud Volumes ONTAP HA en múltiples zonas de disponibilidad (AZ). Para obtener instrucciones, consulte"Configurar una puerta de enlace de tránsito de AWS" .
- Implemente la configuración de la siguiente manera porque solo dos AZ estaban disponibles en AWS Top Secret Cloud 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 la implementación de Cloud Volumes ONTAP en nodos individuales y de alta disponibilidad

Tenga en cuenta lo siguiente a medida que completa 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 necesita utilizar el suyo propio, puede consultar la sección de grupo de seguridad a continuación.

- Debe elegir la función de IAM que creó al preparar su entorno de AWS.
- El tipo de disco AWS subyacente es para el volumen inicial de Cloud Volumes ONTAP .

  Puede elegir un tipo de disco diferente para los volúmenes posteriores.

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

  Debe elegir 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 del disco es el tamaño predeterminado para todos los discos del sistema.

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

Resultado

Se lanza la instancia de Cloud Volumes ONTAP . Puede seguir el progreso en la página **Auditoría**.

Paso 8: Instalar certificados de seguridad para la clasificación de datos

Debe instalar manualmente certificados de seguridad para habilitar la clasificación de datos en las regiones AWS Secret Cloud y Top Secret Cloud.

Antes de empezar

1. Crear depósitos S3.

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

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

Pasos

1. Copie el texto de los certificados raíz que instaló en `step 4` .
2. Conéctese de forma segura al sistema Cloud Volumes ONTAP mediante la CLI.
3. Instalar los certificados raíz. Es posible que tengas que presionar el `ENTER` tecla varias veces:

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

4. Cuando se le solicite, ingrese todo el texto copiado, incluyendo y desde `----- BEGIN CERTIFICATE -----` a `----- END CERTIFICATE -----` .

5. Conserve una copia del certificado digital firmado por la CA para referencia futura.
6. Conserve el nombre de la CA y el número de serie del certificado.
7. Configurar el almacén de objetos para las regiones 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 tener el sufijo `-iso-b` , como `arn:aws-iso-b` . Por ejemplo, si un recurso requiere un ARN con una región, para Top Secret Cloud, utilice la convención de nomenclatura como `us-iso-b` Para el `-server` bandera. Para AWS Secret Cloud, utilice `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. Verifique que el almacén de objetos se haya creado correctamente: `storage aggregate object-store show -instance`
10. Adjunte el almacén de objetos al agregado. Esto debe repetirse para cada nuevo agregado: `storage aggregate object-store attach -aggregate <aggr1> -object-store-name <S3Bucket>`

Introducción a Microsoft Azure

Obtenga información sobre las opciones de implementación de Cloud Volumes ONTAP en Azure

NetApp ofrece dos opciones para implementar Cloud Volumes ONTAP en Azure. Cloud Volumes ONTAP tradicionalmente se basa en la NetApp Console para la implementación y la orquestación. A partir de Cloud Volumes ONTAP 9.16.1, puede aprovechar la implementación directa del mercado de Azure, un proceso optimizado que brinda acceso a un conjunto limitado, pero aún potente, de características y opciones de Cloud Volumes ONTAP .

Cuando implementa Cloud Volumes ONTAP directamente desde Azure Marketplace, no es necesario configurar el agente de la consola ni cumplir con otros criterios de seguridad e incorporación necesarios para implementar Cloud Volumes ONTAP a través de la consola. Desde el mercado de Azure, puede implementar rápidamente Cloud Volumes ONTAP con unos pocos clics y explorar sus características y capacidades principales en su entorno.

Al completar la implementación en Azure Marketplace, podrá descubrir estos sistemas en la consola. Después del descubrimiento, puede administrarlos como sistemas Cloud Volumes ONTAP y aprovechar todas las capacidades de la consola. Consulte "Descubra los sistemas implementados en la consola" .

Aquí está la comparación de características entre las dos opciones. Tenga en cuenta que las características de una instancia independiente implementada a través de Azure Marketplace cambian cuando se detecta en la consola.

	Mercado de Azure	NetApp Console
Incorporación	Más corto y sencillo, se requiere una preparación mínima para la implementación directa	Proceso de incorporación más largo, incluida la instalación del agente de consola
Tipos de máquinas virtuales (VM) compatibles	Tipos de instancia Eds_v5 y Ls_v3	Gama completa de tipos de máquinas virtuales.https://docs.netapp.com/us-en/cloud-volumes-ontap-relnotes/reference-configs-azure.html["Configuraciones admitidas en Azure"^]
Licencia	Licencia libre	Cualquier licencia basada en capacidad."Licencias de Cloud Volumes ONTAP"
* Soporte de NetApp *	No incluido	Disponible, según el tipo de licencia
Capacidad	Hasta 500 GiB	Ampliable por configuración
Modelo de implementación	Implementación en modo de alta disponibilidad (HA) en una única zona de disponibilidad (AZ)	Todas las configuraciones compatibles, incluidos los modos de nodo único y alta disponibilidad, implementaciones de zona de disponibilidad única y múltiple
Tipo de disco compatible	Discos administrados SSD v2 Premium	Apoyo más amplio."Configuración predeterminada para Cloud Volumes ONTAP"
Velocidad de escritura (modo de escritura rápida)	No compatible	Compatible, según su configuración. "Obtenga información sobre las velocidades de escritura en Cloud Volumes ONTAP" .
Capacidades de orquestación	No disponible	Disponible a través de la NetApp Console, según el tipo de licencia
Número de máquinas virtuales de almacenamiento compatibles	Uno por implementación	Varias máquinas virtuales de almacenamiento, según su configuración."Número de máquinas virtuales de almacenamiento admitidas"
Cambiar el tipo de instancia	No compatible	Apoyado
*Niveles de FabricPool *	No compatible	Apoyado

Enlaces relacionados

- Implementación directa de Azure Marketplace:"Implementar Cloud Volumes ONTAP desde Azure Marketplace"
- Implementación a través de la consola:"Inicio rápido de Cloud Volumes ONTAP en Azure"
- "Documentación de la NetApp Console"

Introducción a la NetApp Console

Inicio rápido de Cloud Volumes ONTAP en Azure

Comience a utilizar Cloud Volumes ONTAP para Azure en unos pocos pasos.

Crear un agente de consola

Si no tienes una "Agente de consola" Aún así, es necesario crear uno. "Aprenda a crear un agente de consola en Azure"

Tenga en cuenta que si desea implementar Cloud Volumes ONTAP en una subred donde no hay acceso a Internet disponible, deberá instalar manualmente el agente de consola y acceder a la NetApp Console que se ejecuta en ese agente de consola. "Aprenda a instalar manualmente el agente de consola en una ubicación sin acceso a Internet"

Planifique su configuración

La consola ofrece paquetes preconfigurados que se adaptan a los requisitos de su carga de trabajo, o puede crear su propia configuración. Si elige su propia configuración, debe comprender las opciones disponibles. Para obtener más información, consulte"Planifique su configuración de Cloud Volumes ONTAP en Azure" .

Configura tu red

1. Asegúrese de que su VNet y sus subredes admitan la conectividad entre el agente de la consola y Cloud Volumes ONTAP.
2. Habilite el acceso a Internet saliente desde la VPC de destino para NetApp AutoSupport.

   Este paso no es necesario si está implementando Cloud Volumes ONTAP en una ubicación donde no hay acceso a Internet disponible.

"Obtenga más información sobre los requisitos de red" .

Lanzamiento de Cloud Volumes ONTAP

Haga clic en **Agregar sistema**, 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 agente de consola desde la consola"
- "Creación de un agente de consola desde Azure Marketplace"
- "Instalación del software del agente de consola en un host Linux"
- "Qué hace la consola con los permisos"

Planifique su configuración de Cloud Volumes ONTAP en Azure

Al implementar Cloud Volumes ONTAP en Azure, puede elegir un sistema preconfigurado que coincida con los requisitos de su carga de trabajo o puede crear su

propia configuración. Si elige su propia configuración, debe comprender las opciones disponibles.

Elija una licencia de Cloud Volumes ONTAP

Hay varias opciones de licencia disponibles para Cloud Volumes ONTAP. Cada opción te permite elegir un modelo de consumo que se adapte a tus necesidades.

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

Elija una región compatible

Cloud Volumes ONTAP es compatible con la mayoría de las regiones de Microsoft Azure. "Ver la lista completa de regiones compatibles" .

Elija un tipo de máquina virtual compatible

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

"Configuraciones compatibles con Cloud Volumes ONTAP en Azure"

Comprender los límites de almacenamiento

El límite de capacidad bruta para un sistema Cloud Volumes ONTAP está vinculado a la licencia. Límites adicionales impactan el tamaño de los agregados y volúmenes. Debe tener en cuenta estos límites al planificar su configuración.

"Límites de almacenamiento para Cloud Volumes ONTAP en Azure"

Dimensione su sistema en Azure

Dimensionar su sistema Cloud Volumes ONTAP puede ayudarle a cumplir con los requisitos de rendimiento y capacidad. Debe tener en cuenta algunos puntos clave al elegir un tipo de máquina virtual, un tipo de disco y un tamaño de disco:

Tipo de máquina virtual

Mire los tipos de máquinas virtuales compatibles en el "Notas de la versión de Cloud Volumes ONTAP" y luego revise los detalles sobre cada tipo de VM compatible. Tenga en cuenta que cada tipo de VM admite una cantidad específica de discos de datos.

- "Documentación de Azure: Tamaños de máquinas virtuales de propósito general"
- "Documentación de Azure: Tamaños de máquinas virtuales optimizados para memoria"

Tipo de disco Azure con sistemas de nodo único

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

Los sistemas de nodo único pueden usar estos tipos de Azure Managed Disks:

- Los *discos administrados SSD Premium* brindan un alto rendimiento para cargas de trabajo intensivas en E/S a un costo mayor.
- Los discos administrados SSD v2 Premium brindan un mayor rendimiento con menor latencia a un

menor costo, en comparación con los discos administrados SSD Premium.

- Los *discos administrados SSD estándar* brindan un rendimiento constante para cargas de trabajo que requieren IOPS bajos.
- Los *discos administrados HDD estándar* son una buena opción si no necesita IOPS altos y desea reducir sus costos.

Para obtener detalles adicionales 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 HA utilizan discos administrados compartidos SSD Premium que brindan un alto rendimiento para cargas de trabajo intensivas en E/S a un costo mayor. Las implementaciones de HA creadas antes de la versión 9.12.1 utilizan blobs de página Premium.

Tamaño del disco de Azure

Al iniciar instancias de Cloud Volumes ONTAP , debe elegir el tamaño de disco predeterminado para los agregados. La NetApp Console utiliza 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 que utilicen un tamaño de disco diferente del predeterminado"utilizando la opción de asignación avanzada" .

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

Al elegir un tamaño de disco, debes tener en cuenta varios factores. El tamaño del disco afecta el precio que paga por el almacenamiento, el tamaño de los volúmenes que puede crear en conjunto, la capacidad total disponible para Cloud Volumes ONTAP y el rendimiento del almacenamiento.

El rendimiento de Azure Premium Storage está vinculado al tamaño del disco. Los discos más grandes proporcionan mayor IOPS y rendimiento. Por ejemplo, elegir discos de 1 TiB puede proporcionar un mejor rendimiento que discos de 500 GiB, a un costo mayor.

No hay diferencias de rendimiento entre los tamaños de disco para el almacenamiento estándar. Debe elegir el tamaño del disco en función de la capacidad que necesite.

Consulte Azure para obtener información sobre IOPS y rendimiento según el tamaño del disco:

- "Microsoft Azure: precios de discos administrados"
- "Microsoft Azure: precios de Page Blobs"

Ver los discos del sistema predeterminados

Además del almacenamiento para los datos del usuario, la consola también compra almacenamiento en la nube para los datos del sistema Cloud Volumes ONTAP (datos de arranque, datos raíz, datos del núcleo y NVRAM). Para fines de planificación, puede ser útil revisar estos detalles antes de implementar Cloud Volumes ONTAP.

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

El agente de consola también requiere un disco de sistema. "Ver detalles sobre la configuración predeterminada del agente de la consola" .

Recopilar información de redes

Cuando implementa Cloud Volumes ONTAP en Azure, debe especificar detalles sobre su red virtual. Puede utilizar una hoja de trabajo para recopilar la información de su administrador.

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

Elija una velocidad de escritura

La consola le permite elegir una configuración de velocidad de escritura para Cloud Volumes ONTAP. Antes de elegir una velocidad de escritura, debe comprender las diferencias entre las configuraciones normales y altas, así como los riesgos y recomendaciones al utilizar una velocidad de escritura alta. "Obtenga más información sobre la velocidad de escritura" .

Elija un perfil de uso de volumen

ONTAP incluye varias funciones de eficiencia de almacenamiento que pueden reducir la cantidad total de almacenamiento que necesita. Cuando crea un volumen en la consola, puede elegir un perfil que habilite estas funciones o un perfil que las deshabilite. Debe aprender más sobre estas características para ayudarlo a decidir qué perfil utilizar.

Las características de eficiencia de almacenamiento de NetApp brindan los siguientes beneficios:

Aprovisionamiento fino

Presenta más almacenamiento lógico a los hosts o usuarios del que realmente tiene en su grupo de almacenamiento físico. En lugar de preasignar espacio de almacenamiento, el espacio de almacenamiento se asigna dinámicamente a cada volumen a medida que se escriben los datos.

Desduplicación

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

Compresión

Reduce la capacidad física necesaria para almacenar datos al comprimirlos dentro de un volumen en el almacenamiento primario, secundario y de archivo.

Configurar la red de Azure para Cloud Volumes ONTAP

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

Requisitos para Cloud Volumes ONTAP

Se deben cumplir los siguientes requisitos de red en Azure.

Acceso a Internet de salida

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

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

Puntos finales de Cloud Volumes ONTAP

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

Puntos finales	Aplicable para	Objetivo	Modos de implementación	Impacto si no está disponible
\ https://netapp-cloud-account.auth0.com	Autenticación	Se utiliza para la autenticación en la consola.	Modos estándar y restringido.	La autenticación del usuario falla y los siguientes servicios permanecen no disponibles: • Servicios de Cloud Volumes ONTAP • Servicios de ONTAP • Protocolos y servicios proxy
https://vault.azure.net	Bóveda de claves	Se utiliza para recuperar claves secretas de cliente de Azure Key Vault cuando se utilizan claves administradas por el cliente (CMK).	Modos estándar, restringido y privado.	Los servicios de Cloud Volumes ONTAP no están disponibles.
\ https://api.bluexp.netapp.com/tenancy	Tenencia	Se utiliza para recuperar los recursos de Cloud Volumes ONTAP de la consola para autorizar recursos y usuarios.	Modos estándar y restringido.	Los recursos de Cloud Volumes ONTAP y los usuarios no están autorizados.

Puntos finales	Aplicable para	Objetivo	Modos de implementación	Impacto si no está disponible
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Se utiliza para enviar datos de telemetría de AutoSupport al soporte de NetApp .	Modos estándar y restringido.	La información de AutoSupport sigue sin entregarse.
\ https://management.azure.com \ https://login.microsoftonline.com \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://core.windows.net	regiones públicas	Comunicación con los servicios de Azure.	Modos estándar, restringido y privado.	Cloud Volumes ONTAP no puede comunicarse con el servicio de Azure para realizar operaciones específicas para la consola en Azure.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Región de China	Comunicación con los servicios de Azure.	Modos estándar, restringido y privado.	Cloud Volumes ONTAP no puede comunicarse con el servicio de Azure para realizar operaciones específicas para la consola en Azure.
\ https://management.microsoftazure.de \ https://login.microsoftonline.de \ https://blob.core.cloudapi.de \ https://core.cloudapi.de	Región de Alemania	Comunicación con los servicios de Azure.	Modos estándar, restringido y privado.	Cloud Volumes ONTAP no puede comunicarse con el servicio de Azure para realizar operaciones específicas para la consola en Azure.
\ https://management.usgovcloudapi.net \ https://login.microsoftonline.us \ https://blob.core.usgovcloudapi.net \ https://core.usgovcloudapi.net	Regiones gubernamentales	Comunicación con los servicios de Azure.	Modos estándar, restringido y privado.	Cloud Volumes ONTAP no puede comunicarse con el servicio de Azure para realizar operaciones específicas para la consola en Azure.

Puntos finales	Aplicable para	Objetivo	Modos de implementación	Impacto si no está disponible
\ https://management.azure.microsoft.scloud \ https://login.microsoftonline.microsoft.scloud \ https://blob.core.microsoft.scloud \ https://core.microsoft.scloud	Regiones gubernamentales del Departamento de Defensa	Comunicación con los servicios de Azure.	Modos estándar, restringido y privado.	Cloud Volumes ONTAP no puede comunicarse con el servicio de Azure para realizar operaciones específicas para la consola en Azure.

Configuración del proxy de red del agente de la NetApp Console

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

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

Para obtener información sobre cómo configurar servidores proxy, consulte la "Configurar el agente de la consola para utilizar un servidor proxy" .

Direcciones IP

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

El número de LIF asignados para Cloud Volumes ONTAP depende de si despliegas un sistema de nodo único o un par HA. Un LIF es una dirección IP asociada con un puerto físico. Se requiere un LIF de gestión de SVM para herramientas de gestión como SnapCenter.

Un LIF iSCSI proporciona acceso de cliente 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

La NetApp Console asigna 5 o 6 direcciones IP a un sistema de nodo único:

- IP de gestión de clúster

- IP de gestión de nodos
- IP entre clústeres para SnapMirror
- IP NFS/CIFS
- IP iSCSI

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

- Gestión de SVM (opcional, no configurada de forma predeterminada)

Direcciones IP para pares HA

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

Ten en cuenta que la Console crea un LIF de gestión de SVM en pares HA, pero no en sistemas de nodo único en Azure.

NIC0

- IP de gestión de nodos
- IP entre clústeres
- IP iSCSI

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

NIC1

- IP de red de clúster

NIC2

- IP de interconexión de clúster (HA IC)

NIC3

- IP de NIC de Pageblob (acceso al disco)

> NIC3 solo se aplica a implementaciones de alta disponibilidad que utilizan almacenamiento de blobs de páginas.

Las direcciones IP anteriores no migran en eventos de conmutación por error.

Además, se configuran 4 IP frontend (FIP) para migrar en eventos de conmutación por error. Estas IP de interfaz residen en el balanceador de carga.

- IP de gestión de clúster
- IP de datos del Nodo A (NFS/CIFS)

- IP de datos del Nodo B (NFS/CIFS)
- IP de gestión de SVM

Conexiones seguras a los servicios de Azure

De forma predeterminada, la consola habilita un vínculo privado de Azure para las conexiones entre Cloud Volumes ONTAP y las cuentas de almacenamiento de blobs en páginas de Azure.

En la mayoría de los casos, no es necesario hacer nada: la consola administra Azure Private Link por usted. Pero si usa DNS privado de Azure, necesitará editar un archivo de configuración. También debe tener en cuenta un requisito para la ubicación del agente de consola en Azure.

También puede desactivar la conexión de enlace privado, si así lo requieren las necesidades de su negocio. Si deshabilita el enlace, la consola configura Cloud Volumes ONTAP para utilizar un punto final de servicio en su lugar.

"Obtenga más información sobre el uso de Azure Private Links o puntos de conexión 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, su red corporativa).

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

Puerto para la interconexión HA

Un par HA de Cloud Volumes ONTAP incluye una interconexión HA, que permite que cada nodo verifique continuamente si su socio está funcionando y refleje los datos de registro en la memoria no volátil del otro. La interconexión HA utiliza el puerto TCP 10006 para la comunicación.

De forma predeterminada, la comunicación entre los LIF de interconexión HA está abierta y no hay reglas de grupo de seguridad para este puerto. Pero si crea un firewall entre los LIF de interconexión de HA, entonces debe asegurarse de que el tráfico TCP esté abierto para el puerto 10006 para que el par de HA 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 Cloud Volumes ONTAP HA que implemente en Azure. Solo se admite un par HA en un grupo de recursos.

La consola experimenta problemas de conexión si intenta implementar un segundo par de Cloud Volumes ONTAP HA en un grupo de recursos de Azure.

Reglas del grupo de seguridad

La consola crea grupos de seguridad de Azure que incluyen las reglas de entrada y salida para que Cloud Volumes ONTAP funcione correctamente. "Ver las reglas del grupo de seguridad para el agente de la consola" .

Los grupos de seguridad de Azure para Cloud Volumes ONTAP requieren que los puertos adecuados estén abiertos para la comunicación interna entre los nodos. "Obtenga más información sobre los puertos internos

de ONTAP" .

No recomendamos modificar los grupos de seguridad predefinidos ni utilizar grupos de seguridad personalizados. Sin embargo, si debe hacerlo, tenga en cuenta que el proceso de implementación requiere que el sistema Cloud Volumes ONTAP tenga acceso completo dentro de su propia subred. Una vez completada la implementación, si decide modificar el grupo de seguridad de red, asegúrese de mantener abiertos los puertos del clúster y los puertos de red HA. Esto garantiza una comunicación fluida dentro del clúster Cloud Volumes ONTAP (comunicación de cualquier tipo entre los nodos).

Reglas de entrada para sistemas de nodo único

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

- **Solo VNet seleccionado**: la fuente del tráfico entrante es el rango de subred de la VNet para el sistema Cloud Volumes ONTAP y el rango de subred de la VNet donde reside el agente de la consola. Esta es la opción recomendada.
- **Todas las redes virtuales**: la fuente del tráfico entrante es el rango de IP 0.0.0.0/0.
- **Deshabilitado**: esta opción restringe el acceso de la red pública a su cuenta de almacenamiento y deshabilita la organización en niveles de datos para los sistemas Cloud Volumes ONTAP . Esta es una opción recomendada si sus direcciones IP privadas no deben quedar expuestas incluso dentro de la misma VNet debido a regulaciones y políticas de seguridad.

Prioridad y nombre	Puerto y protocolo	Origen y destino	Descripción
1000 entrantes_ssh	22 TCP	De cualquiera a cualquiera	Acceso SSH a la dirección IP del LIF de administración del clúster o de un LIF de administración de nodos
1001 entrante_http	80 TCP	De cualquiera a cualquiera	Acceso HTTP a la consola web de ONTAP System Manager mediante la dirección IP del LIF de administración del clúster
1002 entrante_111_tcp	111 TCP	De cualquiera a cualquiera	Llamada a procedimiento remoto para NFS
1003 entrante_111_udp	111 UDP	De cualquiera a cualquiera	Llamada a procedimiento remoto para NFS
1004 entrante_139	139 TCP	De cualquiera a cualquiera	Sesión de servicio NetBIOS para CIFS
1005 entrante_161-162 _tcp	161-162 TCP	De cualquiera a cualquiera	Protocolo simple de gestión de red
1006 entrante_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 entrante_443	443 TCP	De cualquiera a cualquiera	Conectividad con el agente de la consola y acceso HTTPS a la consola web de ONTAP System Manager mediante la dirección IP del LIF de administración del clúster
1008 entrante_445	445 TCP	De cualquiera a cualquiera	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
1009 entrante_635_tcp	635 TCP	De cualquiera a cualquiera	Montaje NFS
1010 entrante_635_udp	635 UDP	De cualquiera a cualquiera	Montaje NFS
1011 entrante_749	749 TCP	De cualquiera a cualquiera	Kerberos
1012 entrante_2049_tcp	2049 TCP	De cualquiera a cualquiera	Demonio del servidor NFS
1013 entrante_2049_udp	2049 UDP	De cualquiera a cualquiera	Demonio del servidor NFS
1014 entrante_3260	3260 TCP	De cualquiera a cualquiera	Acceso iSCSI a través del LIF de datos iSCSI
1015 entrante_4045-4046_tcp	4045-4046 TCP	De cualquiera a cualquiera	Demonio de bloqueo NFS y monitor de estado de red
1016 entrante_4045-4046_udp	4045-4046 UDP	De cualquiera a cualquiera	Demonio de bloqueo NFS y monitor de estado de red
1017 entrante_10000	10000 TCP	De cualquiera a cualquiera	Copia de seguridad mediante NDMP
1018 entrante_11104-11105	11104-11105 TCP	De cualquiera a cualquiera	Transferencia de datos de SnapMirror
3000 denegación de entrada _all_tcp	Cualquier puerto TCP	De cualquiera a cualquiera	Bloquear todo el resto del tráfico entrante TCP
3001 entrada_denegación_todos_udp	Cualquier puerto UDP	De cualquiera a cualquiera	Bloquear todo el resto del tráfico entrante UDP
65000 PermitirVnetInBound	Cualquier puerto Cualquier protocolo	Red virtual a red virtual	Tráfico entrante desde dentro de la red virtual
65001 Permitir entrada del balanceador de carga de Azure	Cualquier puerto Cualquier protocolo	AzureLoadBalancer a cualquier	Tráfico de datos desde Azure Standard Load Balancer

Prioridad y nombre	Puerto y protocolo	Origen y destino	Descripción
65500 DenyAllInBound	Cualquier puerto Cualquier protocolo	De cualquiera a cualquiera	Bloquear todo el resto del tráfico entrante

Reglas de entrada para sistemas HA

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

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

> Los sistemas de HA tienen menos reglas de entrada que los sistemas de nodo único porque el tráfico de datos de entrada pasa por el Azure Standard Load Balancer. Por esto, el tráfico del Load Balancer debe estar abierto, como se muestra en la regla "AllowAzureLoadBalancerInBound".

- **Deshabilitado**: esta opción restringe el acceso de la red pública a su cuenta de almacenamiento y deshabilita la organización en niveles de datos para los sistemas Cloud Volumes ONTAP . Esta es una opción recomendada si sus direcciones IP privadas no deben quedar expuestas incluso dentro de la misma VNet debido a regulaciones y políticas de seguridad.

Prioridad y nombre	Puerto y protocolo	Origen y destino	Descripción
100 entrantes_443	443 Cualquier protocolo	De cualquiera a cualquiera	Conectividad con el agente de la consola y acceso HTTPS a la consola web de ONTAP System Manager mediante la dirección IP del LIF de administración del clúster
101 entrante_111_tcp	111 Cualquier protocolo	De cualquiera a cualquiera	Llamada a procedimiento remoto para NFS
102 entrante_2049_tcp	2049 Cualquier protocolo	De cualquiera a cualquiera	Demonio del servidor NFS
111 entrada_ssh	22 Cualquier protocolo	De cualquiera a cualquiera	Acceso SSH a la dirección IP del LIF de administración del clúster o de un LIF de administración de nodos
121 entrante_53	53 Cualquier protocolo	De cualquiera a cualquiera	DNS y CIFS
65000 PermitirVnetInBound	Cualquier puerto Cualquier protocolo	Red virtual a red virtual	Tráfico entrante desde dentro de la red virtual

Prioridad y nombre	Puerto y protocolo	Origen y destino	Descripción
65001 Permitir entrada del balanceador de carga de Azure	Cualquier puerto Cualquier protocolo	AzureLoadBalancer a cualquier	Tráfico de datos desde Azure Standard Load Balancer
65500 DenyAllInBound	Cualquier puerto Cualquier protocolo	De cualquiera a cualquiera	Bloquear todo 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 salida. Si necesita reglas más rígidas, utilice las reglas de salida avanzadas.

Reglas básicas de salida

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

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

Reglas de salida avanzadas

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

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

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

Servicio	Puerto	Protocolo	Fuente	Destino	Objetivo
AutoSupport	HTTPS	443	LIF de gestión de nodos	mysupport.netapp.com	AutoSupport (HTTPS es el predeterminado)
	HTTP	80	LIF de gestión de nodos	mysupport.netapp.com	AutoSupport (solo si el protocolo de transporte se cambia de HTTPS a HTTP)
	TCP	3128	LIF de gestión de nodos	Agente de consola	Envío de mensajes de AutoSupport a través de un servidor proxy en el agente de la consola, si no hay una conexión a Internet saliente disponible
Copias de seguridad de configuración	HTTP	80	LIF de gestión de nodos	http://<dirección IP del agente de consola>/occm/offboxconfig	Envía copias de seguridad de la configuración al agente de la consola. "Documentación de ONTAP" .
DHCP	68	UDP	LIF de gestión de nodos	DHCP	Cliente DHCP para la primera configuración
DHCP	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, se pueden utilizar para AutoSupport
SNMP	161	TCP	LIF de gestión de nodos	Servidor de monitorización	Monitoreo mediante trampas SNMP
	161	UDP	LIF de gestión de nodos	Servidor de monitorización	Monitoreo mediante trampas SNMP
	162	TCP	LIF de gestión de nodos	Servidor de monitorización	Monitoreo mediante trampas SNMP
	162	UDP	LIF de gestión de nodos	Servidor de monitorización	Monitoreo mediante trampas SNMP
SnapMirror	11104	TCP	LIF entre clústeres	LIF entre clústeres de ONTAP	Gestión de sesiones de comunicación entre clústeres para SnapMirror
	11105	TCP	LIF entre clústeres	LIF entre clústeres de ONTAP	Transferencia de datos de SnapMirror

Servicio	Puerto	Protocolo	Fuente	Destino	Objetivo
Registro del sistema	514	UDP	LIF de gestión de nodos	Servidor de syslog	Mensajes de reenvío de syslog

Requisitos para el agente de consola

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

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

Temas relacionados

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

Configurar Cloud Volumes ONTAP para usar una clave administrada por el cliente en Azure

Los datos se cifran automáticamente en Cloud Volumes ONTAP en Azure mediante Azure Storage Service Encryption con una clave administrada por Microsoft. Pero puedes utilizar tu propia clave de cifrado siguiendo los pasos de esta página.

Descripción general del 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 administrada por el cliente con Cloud Volumes ONTAP, deberá completar los siguientes pasos:

1. Desde Azure, cree un almacén de claves y luego genere una clave en ese almacén.
2. Desde la NetApp Console, use la API para crear un sistema Cloud Volumes ONTAP que use la clave.

Cómo se cifran los datos

La consola utiliza un conjunto de cifrado de disco, que permite la administración de claves de cifrado con discos administrados, no con blobs de página. Cualquier disco de datos nuevo también utiliza el mismo conjunto de cifrado de disco. Las versiones inferiores utilizarán la clave administrada por Microsoft, en lugar de la clave administrada por el cliente.

Después de crear un sistema Cloud Volumes ONTAP configurado para usar una clave administrada 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
Nodo único	• Bota • Centro • NVRAM	• Raíz • Datos
Zona de disponibilidad única de Azure HA con blobs de página	• Bota • Centro • NVRAM	Ninguno
Zona de disponibilidad única de Azure HA con discos administrados compartidos	• Bota • Centro • NVRAM	• Raíz • Datos
Zonas de disponibilidad múltiple de Azure HA con discos administrados compartidos	• Bota • Centro • NVRAM	• Raíz • Datos

Todas las cuentas de almacenamiento de Azure para Cloud Volumes ONTAP están cifradas mediante una clave administrada por el cliente. Si desea cifrar sus cuentas de almacenamiento durante su creación, debe crear y proporcionar el ID del recurso en la solicitud de creación de Cloud Volumes ONTAP . Esto se aplica a todo tipo de implementaciones. Si no lo proporciona, las cuentas de almacenamiento se cifrarán de todos modos, pero la consola primero crea las cuentas de almacenamiento con el cifrado de clave administrado por Microsoft y luego actualiza las cuentas de almacenamiento para usar la clave administrada por el cliente.

Rotación de claves en Cloud Volumes ONTAP

Al configurar sus claves de cifrado, debe usar el portal de Azure para configurar y habilitar la rotación automática de claves. La creación y habilitación de una nueva versión de claves de cifrado garantiza que Cloud Volumes ONTAP pueda detectar y usar automáticamente la última versión de clave para el cifrado, lo que garantiza que sus datos permanezcan seguros sin necesidad de intervención manual.

Para obtener información sobre cómo configurar sus claves y configurar la rotación de claves, consulte los siguientes temas de la documentación de Microsoft Azure:

- "Configurar la rotación automática de claves criptográficas en Azure Key Vault"
- "Azure PowerShell: Habilitar claves administradas por el cliente"

> Después de configurar las claves, asegúrese de haber seleccionado "*Habilitar rotación automática*" , para que Cloud Volumes ONTAP pueda usar las nuevas claves cuando caduquen las claves anteriores. Si no habilita esta opción en el portal de Azure, Cloud Volumes ONTAP no podrá detectar automáticamente las nuevas claves, lo que podría causar problemas con el aprovisionamiento de almacenamiento.

Crear una identidad administrada asignada por el usuario

Tiene la opción de crear un recurso llamado identidad administrada asignada por el usuario. Al hacerlo, podrá cifrar sus cuentas de almacenamiento cuando cree un sistema Cloud Volumes ONTAP . Recomendamos crear este recurso antes de crear un almacén de claves y generar una clave.

El recurso tiene el siguiente ID: `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 del agente de consola.
   - **Grupo de recursos**: utilice un grupo de recursos existente o cree uno nuevo.
   - **Región**: Opcionalmente, seleccione la misma región que el agente de consola.
   - **Nombre**: Ingrese un nombre para el recurso.
4. Opcionalmente, agregue etiquetas.
5. Haga clic en **Crear**.

Crear un almacén de claves y generar una clave

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

Si ustedcreó una identidad administrada 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 de Azure" .

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

   - La bóveda de claves debe residir en la misma región que el sistema Cloud Volumes ONTAP .
   - Se deben habilitar las siguientes opciones:
     - **Eliminación suave** (esta opción está habilitada de manera predeterminada, pero no debe deshabilitarse)
     - **Protección de purga**
     - **Azure Disk Encryption para el cifrado de volúmenes** (para sistemas de nodo único, pares HA en varias zonas y implementaciones HA de una sola AZ)

       El uso de claves de cifrado administradas por el cliente de Azure depende de que el cifrado de disco de Azure esté habilitado para el almacén de claves.

   - La siguiente opción debe estar habilitada si creó una identidad administrada asignada por el usuario:
     - **Política de acceso a la bóveda**
2. Si seleccionó la Política de acceso a la bóveda, haga clic en Crear para crear una política de acceso para la bóveda de claves. En caso contrario, salte al paso 3.

a. Seleccione los siguientes permisos:
   - conseguir
   - lista
   - descifrar
   - cifrar
   - desenvolver clave
   - llave de envoltura
   - verificar
   - firmar

b. Seleccione la identidad administrada asignada por el usuario (recurso) como principal.

c. Revisar y crear la política de acceso.

3. "Generar 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.

Crear un sistema 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 que esté configurado para usar la clave. Estos pasos se respaldan mediante el uso de la API.

Permisos necesarios

Si desea utilizar una clave administrada por el cliente con un sistema Cloud Volumes ONTAP de un solo nodo, asegúrese de que el agente de la consola tenga 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"
```

"Ver la lista más reciente de permisos"

Pasos

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

   Para un par HA: `GET /azure/ha/metadata/vaults`

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

   Tome nota del **nombre** y del **grupo de recursos**. Necesitarás especificar esos valores en el siguiente

paso.

"Obtenga más información sobre esta llamada API" .

2. Obtenga la lista de claves dentro de la bóveda utilizando la siguiente llamada API.

   Para un par HA: `GET /azure/ha/metadata/keys-vault`

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

   Tome nota del **keyName**. Necesitará especificar ese valor (junto con el nombre de la bóveda) en el siguiente paso.

   "Obtenga más información sobre esta llamada API" .

3. Cree un sistema Cloud Volumes ONTAP utilizando la siguiente llamada API.

   a. Para un par HA:

      `POST /azure/ha/working-environments`

      El cuerpo de la solicitud debe incluir los siguientes campos:

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

      Incluir el `"userAssignedIdentity": " userAssignedIdentityId"` campo si creó este recurso para usarlo para el cifrado de la cuenta de almacenamiento.

      "Obtenga más información sobre 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"
      }
      ```

      Incluir el `"userAssignedIdentity": " userAssignedIdentityId"` campo si creó este recurso para usarlo para el cifrado de la cuenta de almacenamiento.

   "Obtenga más información sobre esta llamada API" .

Resultado

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

Configurar licencias para Cloud Volumes ONTAP en Azure

Después de decidir qué opción de licencia desea utilizar con Cloud Volumes ONTAP, se requieren algunos pasos antes de poder elegir esa opción de licencia al crear un nuevo sistema.

Freemium

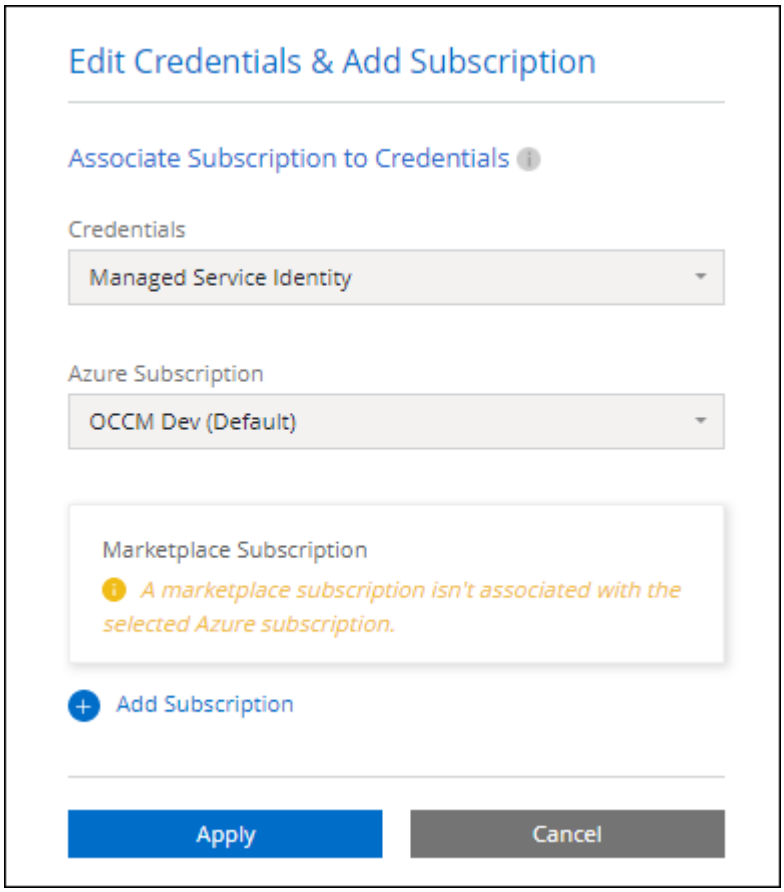
Seleccione la oferta Freemium para utilizar Cloud Volumes ONTAP de forma gratuita con hasta 500 GiB de capacidad aprovisionada. "Obtenga más información sobre la oferta Freemium" .

Pasos

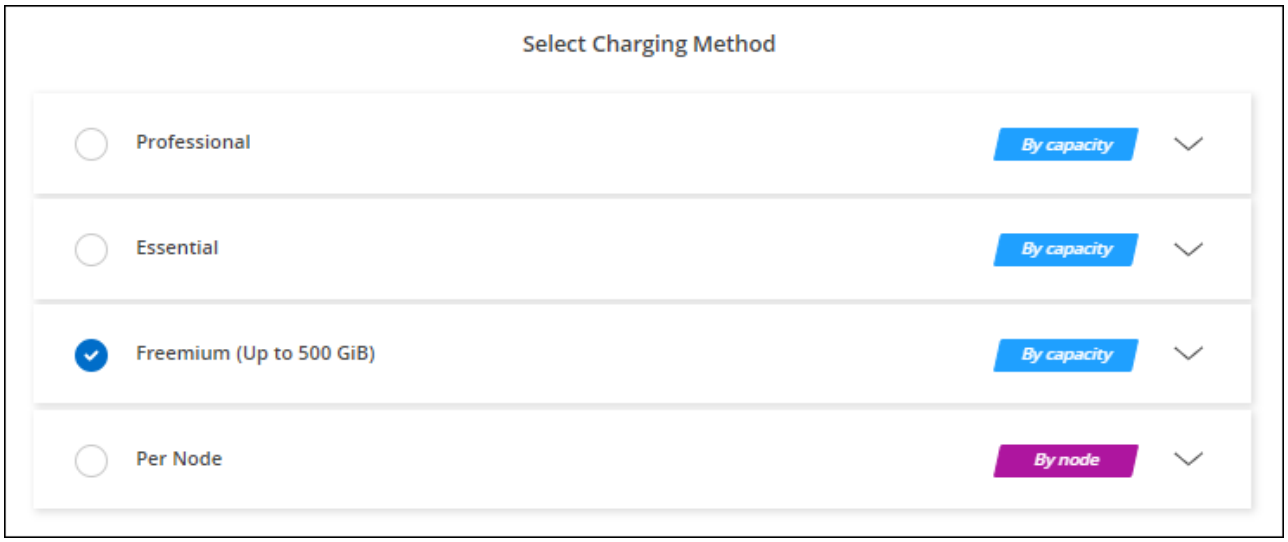
1. Desde el menú de navegación izquierdo de la NetApp Console, seleccione **Almacenamiento > Administración**.
2. En la página **Sistemas**, haga clic en **Agregar sistema** y siga los pasos.

    a. En la página **Detalles y credenciales**, haga clic en **Editar credenciales > Agregar suscripción** y luego siga las instrucciones para suscribirse a la oferta de pago por uso en Azure Marketplace.

    No se le cobrará a través de la suscripción del mercado a menos que exceda los 500 GiB de capacidad aprovisionada, momento en el cual el sistema se convierte automáticamente al"Paquete esencial" .



a. Después de regresar a la consola, seleccione **Freemium** cuando llegue a la página de métodos de cobro.



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

Licencia basada en capacidad

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

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

- Una licencia (traiga su propia licencia (BYOL)) comprada a NetApp
- Una suscripción por hora, de pago por uso (PAYGO) desde Azure Marketplace
- Un contrato anual

"Obtenga más información sobre las licencias basadas en capacidad" .

Las siguientes secciones describen cómo comenzar a utilizar cada uno de estos modelos de consumo.

Trae tu propia bebida

Pague por adelantado comprando una licencia (BYOL) de NetApp para implementar sistemas Cloud Volumes ONTAP en cualquier proveedor de nube.

NetApp ha restringido la compra, extensión y renovación de licencias BYOL. Para más información, consulte "Disponibilidad restringida de licencias BYOL para Cloud Volumes ONTAP" .

Pasos

1. "Comuníquese con el departamento de ventas de NetApp para obtener una licencia"
2. "Agregue su cuenta del sitio de soporte de NetApp a la consola"

   La consola consulta automáticamente el servicio de licencias de NetApp para obtener detalles sobre las

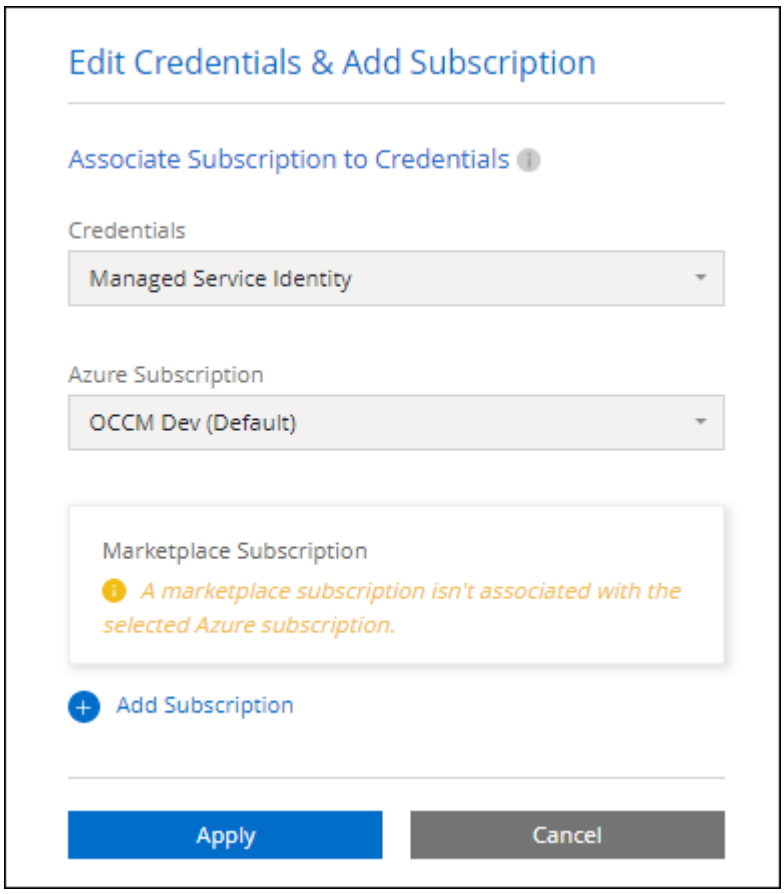
licencias asociadas a su cuenta del sitio de soporte de NetApp . Si no hay errores, la Consola agrega automáticamente las licencias a la Consola.

Su licencia debe estar disponible en la consola antes de poder usarla con Cloud Volumes ONTAP. Si es necesario, puedes"agregar manualmente la licencia a la consola" .

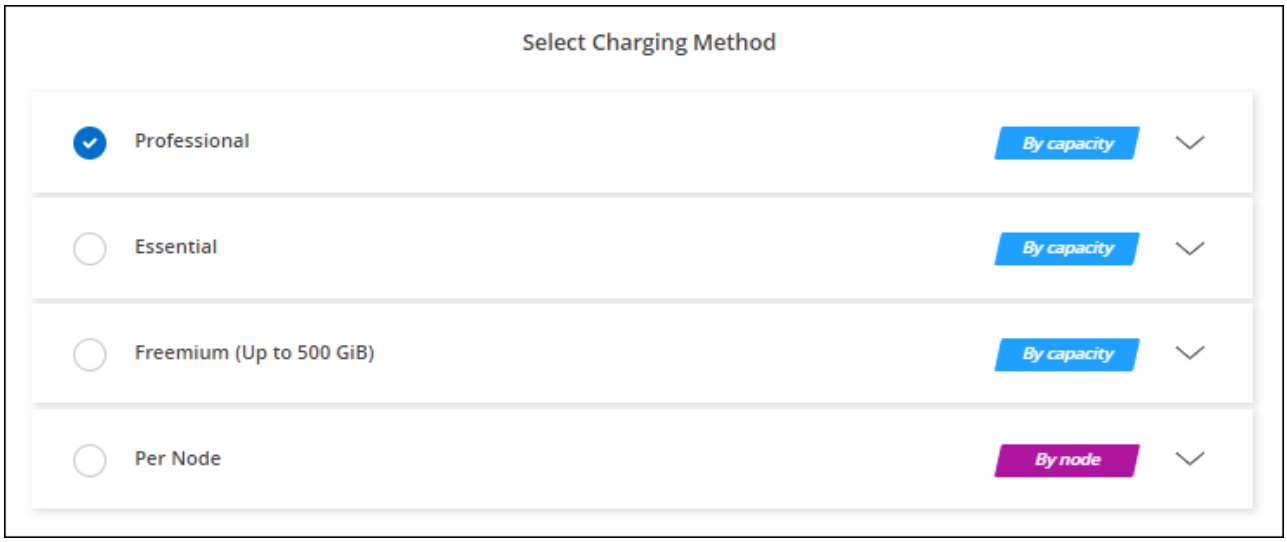
3. En la página **Sistemas**, haga clic en **Agregar sistema** y siga los pasos.

   a. En la página **Detalles y credenciales**, haga clic en **Editar credenciales > Agregar suscripción** y luego siga las instrucciones para suscribirse a la oferta de pago por uso en Azure Marketplace.

      La licencia que usted compró de NetApp siempre se cobra primero, pero se le cobrará la tarifa por hora del mercado si excede su capacidad de licencia o si vence el plazo de su licencia.



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



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

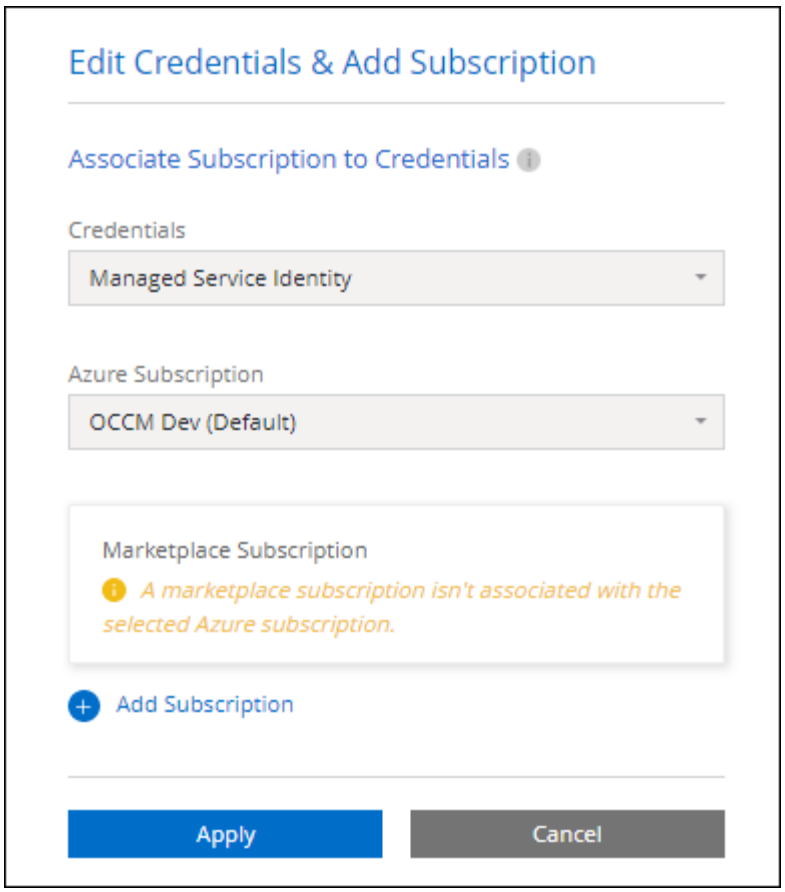
Suscripción PAYGO

Pague por hora suscribiéndose a la oferta del mercado de su proveedor de nube.

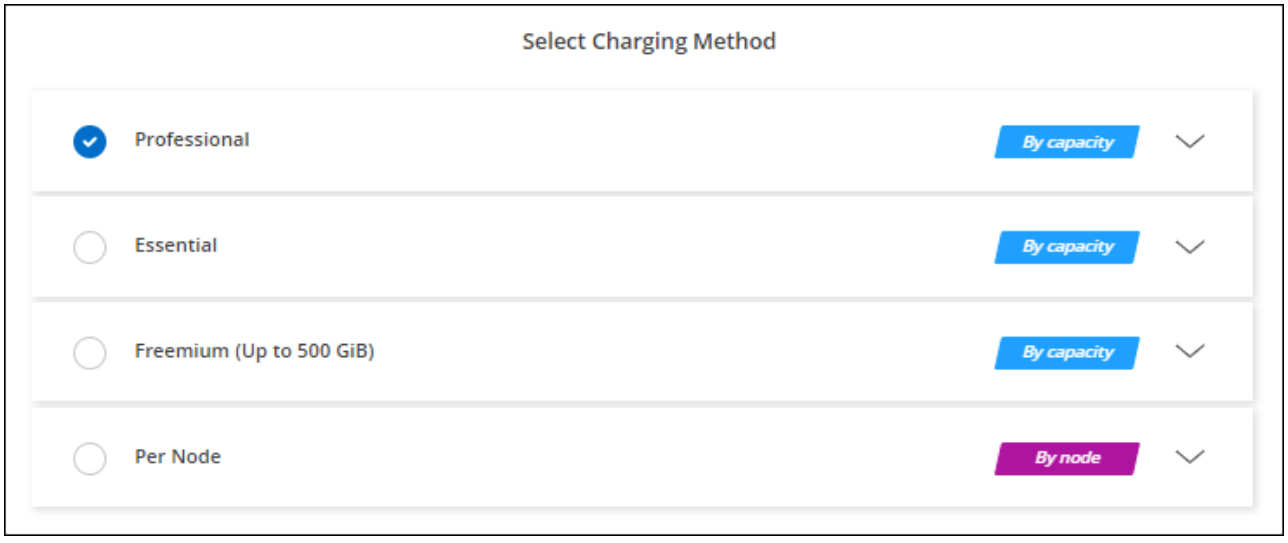
Cuando crea un sistema Cloud Volumes ONTAP , la consola le solicita que se suscriba al contrato que está disponible en Azure Marketplace. Esa suscripción se asocia luego al sistema para su cobro. Puede utilizar esa misma suscripción para sistemas adicionales.

Pasos

1. Desde el menú de navegación de la izquierda, seleccione **Almacenamiento > Administración**.
2. En la página **Sistemas**, haga clic en **Agregar sistema** y siga los pasos.
   a. En la página **Detalles y credenciales**, haga clic en **Editar credenciales > Agregar suscripción** y luego siga las instrucciones para suscribirse a la oferta de pago por uso en Azure Marketplace.



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



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

Puede administrar las suscripciones de Azure Marketplace asociadas a sus cuentas de Azure desde la página Configuración > Credenciales. "Aprenda a administrar sus cuentas y suscripciones de Azure"

Contrato anual

Pague Cloud Volumes ONTAP anualmente comprando un contrato anual.

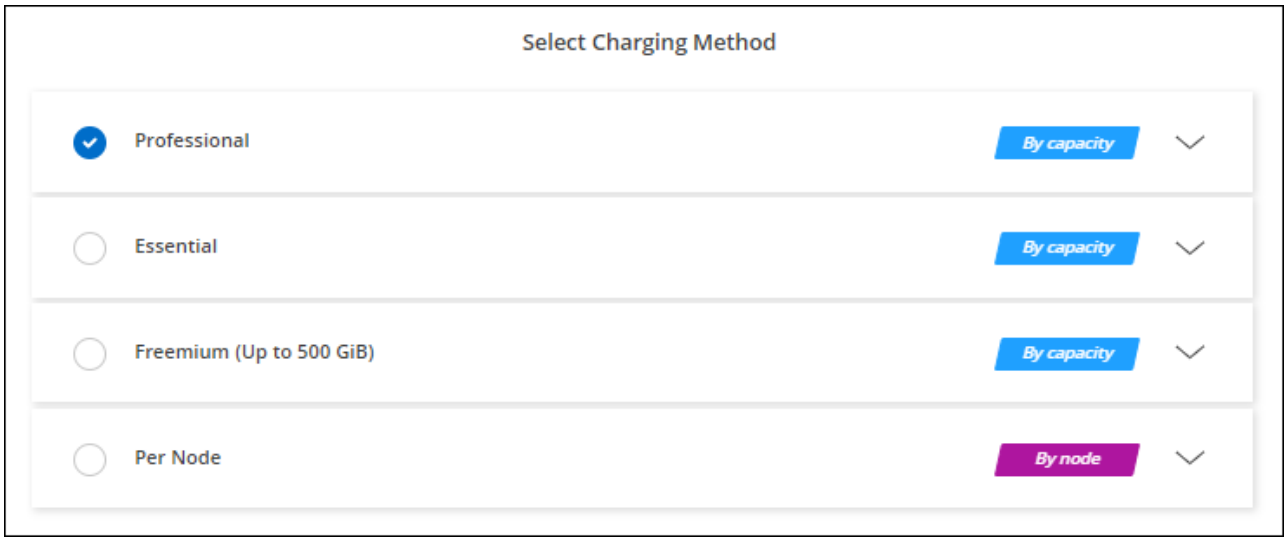
Pasos

1. Comuníquese con su representante de ventas de NetApp para comprar un contrato anual.

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

   Después de que NetApp comparta la oferta privada con usted, puede seleccionar el plan anual cuando se suscriba desde Azure Marketplace durante la creación del sistema.

2. En la página **Sistemas**, haga clic en **Agregar sistema** y siga los pasos.
   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 se compartió con su cuenta de Azure y luego haga clic en **Suscribirse**.
   c. Después de regresar a la consola, seleccione un paquete basado en capacidad cuando llegue a la página de métodos de carga.



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

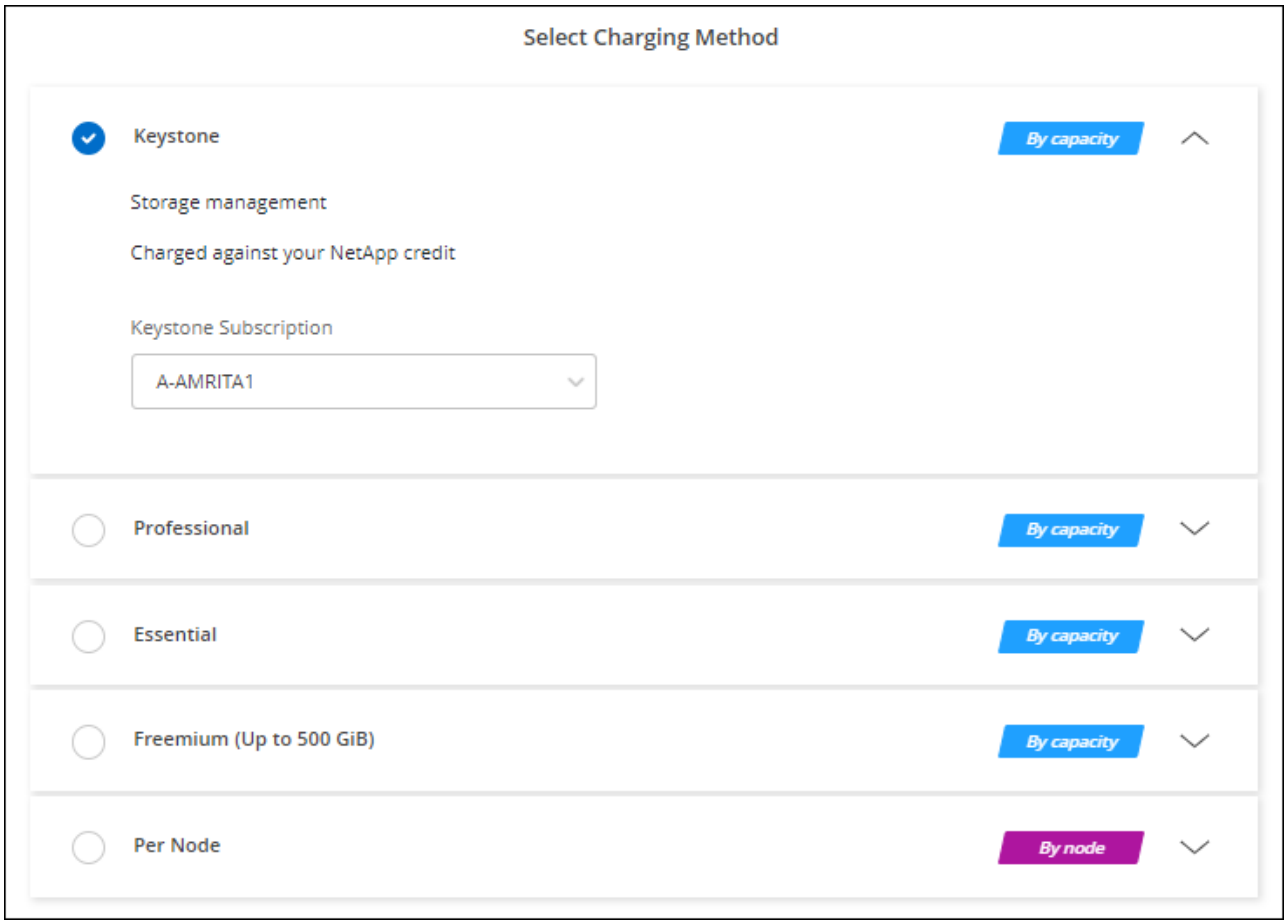
Suscripción a Keystone

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

Pasos

1. Si aún no tienes una suscripción, "Contactar con NetApp"
2. Contacto NetApp para autorizar su cuenta de usuario en la Consola con una o más suscripciones de Keystone .
3. Después de que NetApp autorice su cuenta,"Vincula tus suscripciones para usarlas con Cloud Volumes ONTAP" .
4. En la página **Sistemas**, haga clic en **Agregar sistema** y siga los pasos.

a. Seleccione el método de cobro de suscripción de Keystone cuando se le solicite que elija un método de cobro.



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

Licencia basada en nodos

Una licencia basada en nodos es la licencia de la generación anterior para Cloud Volumes ONTAP. Esta licencia se puede adquirir a través de NetApp (BYOL) y está disponible para renovaciones de licencias, solo en casos específicos. Para obtener información, consulte:

- "Fin de la disponibilidad de las licencias basadas en nodos"
- "Fin de la disponibilidad de las licencias basadas en nodos"
- "Convertir una licencia basada en nodos a una licencia basada en capacidad"

Habilitar el modo de alta disponibilidad para Cloud Volumes ONTAP en Azure

El modo de alta disponibilidad (HA) de Microsoft Azure debe estar habilitado para reducir los tiempos de conmutación por error no planificados y para habilitar la compatibilidad de NFSv4 con Cloud Volumes ONTAP. En este modo, sus nodos de Cloud Volumes ONTAP HA pueden alcanzar un objetivo de tiempo de recuperación (RTO) bajo (60 segundos) durante conmutaciones por error no planificadas en clientes CIFS y NFSv4.

A partir de Cloud Volumes ONTAP 9.10.1, redujimos el tiempo de conmutación por error no planificado para

los pares de Cloud Volumes ONTAP HA que se ejecutan en Microsoft Azure y agregamos compatibilidad con NFSv4. Para que estas mejoras estén disponibles para Cloud Volumes ONTAP, debe habilitar la función de alta disponibilidad en su suscripción de Azure.

La NetApp Console le solicita estos detalles cuando es necesario habilitar la función en una suscripción de Azure.

Tenga en cuenta lo siguiente:

- No hay problemas con la alta disponibilidad de su par Cloud Volumes ONTAP HA. Esta característica de Azure funciona en conjunto con ONTAP para reducir el tiempo de interrupción de la aplicación observado por el cliente para los protocolos NFS que resultan de eventos de conmutación por error no planificados.
- Habilitar esta función no interrumpe los pares HA de Cloud Volumes ONTAP .
- Habilitar esta función en su suscripción de Azure no causa problemas a otras máquinas virtuales.
- Cloud Volumes ONTAP utiliza un Azure Load Balancer interno durante las conmutaciones por error de los LIF de administración de clústeres y SVM en clientes CIFS y NFS.
- Cuando el modo HA está habilitado, la consola escanea el sistema cada 12 horas para actualizar las reglas internas de Azure Load Balancer.

Un usuario de Azure que tenga 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. Registrar la función de 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. Opcionalmente, verifique que la función ahora esté registrada:

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

   La CLI de Azure debería devolver un resultado similar al 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"
}
```

Habilitar VMOrchestratorZonalMultiFD para Cloud Volumes ONTAP en Azure

Para implementar instancias de VM en zonas de disponibilidad única (AZ) de almacenamiento con redundancia local (LRS), debe activar Microsoft `Microsoft.Compute/VMOrchestratorZonalMultiFD` función para sus suscripciones. En un modo de alta disponibilidad (HA), esta característica facilita la implementación de nodos en dominios de falla separados en la misma zona de disponibilidad.

A menos que active esta función, la implementación zonal no se produce y la implementación no zonal de LRS anterior se vuelve efectiva.

Para obtener información sobre la implementación de máquinas virtuales en una única zona de disponibilidad, consulte"Pares de alta disponibilidad en Azure" .

Realice estos pasos como usuario con privilegios de "Propietario":

Pasos

1. Acceda a Azure Cloud Shell desde el portal de Azure. Para obtener información, consulte la "Documentación de Microsoft Azure: Introducción a Azure Cloud Shell" .
2. Regístrate para el `Microsoft.Compute/VMOrchestratorZonalMultiFD` función ejecutando este comando:

   conjunto de cuentas az -s *<nombre_o_ID_de_suscripción_de_Azure>* registro de características az --name VMOrchestratorZonalMultiFD --namespace Microsoft.Compute

3. Verificar el estado del registro y la muestra de salida:

   az feature show -n VMOrchestratorZonalMultiFD --namespace Microsoft.Compute { "id": "/subscriptions/*<ID>*/providers/Microsoft.Features/providers/Microsoft.Compute/features/VMOrchestratorZonalMultiFD", "name": "Microsoft.Compute/VMOrchestratorZonalMultiFD", "properties": { "state": "Registrado" }, "type": "Microsoft.Features/providers/features" }

Lanzamiento de Cloud Volumes ONTAP en Azure

Puedes lanzar un sistema de nodo único o un par de alta disponibilidad en Azure creando un sistema Cloud Volumes ONTAP en NetApp Console.

Antes de empezar

Necesitará lo siguiente antes de comenzar.

- Un agente de consola que está en funcionamiento.
  - Deberías tener una "Agente de consola asociado con su sistema" .
  - "Debes estar preparado para dejar el agente de consola ejecutándose en todo momento" .
- Una comprensión de la configuración que desea utilizar.

  Debe tener una configuración planificada y los detalles de red de Azure necesarios de su administrador. Para obtener más información, consulte "Planificación de la configuración de Cloud Volumes ONTAP" .
- Una comprensión de lo que se requiere para configurar la licencia para Cloud Volumes ONTAP.

  "Aprenda a configurar las licencias" .

Acerca de esta tarea

Cuando la consola 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 Cloud Volumes ONTAP .
>
> No se recomienda implementar Cloud Volumes ONTAP en un grupo de recursos compartido existente debido al riesgo de pérdida de datos. Si bien la consola puede eliminar recursos de Cloud Volumes ONTAP de un grupo de recursos compartidos en caso de una falla o eliminación en la implementación, un usuario de Azure podría eliminar accidentalmente recursos de Cloud Volumes ONTAP de un grupo de recursos compartidos.

Lanzar un sistema Cloud Volumes ONTAP de un solo nodo en Azure

Si quieres lanzar un sistema Cloud Volumes ONTAP de un solo nodo en Azure, necesitas crear un sistema de un solo nodo en la NetApp Console.

Pasos

1. Desde el menú de navegación de la izquierda, seleccione **Almacenamiento > Administración**.
2. En la página **Sistemas**, haga clic en **Agregar sistema** y siga las instrucciones.
3. **Elija una ubicación**: seleccione **Microsoft Azure** y * Cloud Volumes ONTAP Single Node*.
4. Si se le solicita, "crear un agente de consola" .
5. **Detalles y credenciales**: Opcionalmente, cambie las credenciales y la suscripción de Azure, especifique un nombre de clúster, agregue etiquetas si es necesario y luego especifique las credenciales.

   La siguiente tabla describe los campos para los que podría necesitar orientación:

Campo	Descripción
Nombre del sistema	La consola usa el nombre del sistema 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 de grupos de recursos	Las etiquetas son metadatos para sus recursos de Azure. Cuando ingresa etiquetas en este campo, la consola las agrega al grupo de recursos asociado con el sistema Cloud Volumes ONTAP . Puede agregar hasta cuatro etiquetas desde la interfaz de usuario al crear un sistema y luego puede agregar más una vez creado. Tenga en cuenta que la API no lo limita a cuatro etiquetas al crear un sistema. Para obtener información sobre las etiquetas, consulte la "Documentación de Microsoft Azure: Uso de etiquetas para organizar los recursos de Azure" .
Nombre de usuario y contraseña	Estas son las credenciales para la cuenta de administrador del clúster de Cloud Volumes ONTAP . Puede usar estas credenciales para conectarse a Cloud Volumes ONTAP a través de ONTAP System Manager o la CLI de ONTAP . 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 usar con este sistema Cloud Volumes ONTAP . Debe asociar una suscripción de Azure Marketplace con la suscripción de Azure seleccionada para implementar un sistema Cloud Volumes ONTAP de pago por uso. "Aprenda cómo agregar credenciales" .

6. **Servicios**: habilite o deshabilite los servicios individuales que desea o no desea utilizar con Cloud Volumes ONTAP.
   - "Obtenga más información sobre la NetApp Data Classification"
   - "Obtenga más información sobre NetApp Backup and Recovery"

   Si desea utilizar WORM y niveles de datos, debe deshabilitar la función de copia de seguridad y recuperación e implementar un sistema Cloud Volumes ONTAP con la versión 9.8 o superior.

7. **Ubicación**: seleccione una región, una zona de disponibilidad, una red virtual y una subred, y luego seleccione la casilla de verificación para confirmar la conectividad de red entre el agente de la consola y la ubicación de destino.

   Para las regiones de China, las implementaciones de nodo único solo se admiten en Cloud Volumes ONTAP 9.12.1 GA y 9.13.0 GA. Puede actualizar estas versiones a parches y lanzamientos posteriores de Cloud Volumes ONTAP como"compatible con Azure" . Si desea implementar versiones posteriores de Cloud Volumes ONTAP en las regiones de China, comuníquese con el soporte de NetApp . En las regiones de China solo se admiten las licencias compradas directamente a NetApp ; las suscripciones al mercado no están disponibles.

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

   La siguiente tabla describe los campos para los que podría necesitar orientación:

Campo	Descripción
Grupo de recursos	Cree un nuevo grupo de recursos para Cloud Volumes ONTAP o utilice un grupo de recursos existente. La mejor práctica es utilizar un nuevo grupo de recursos dedicado para Cloud Volumes ONTAP. Si bien es posible implementar Cloud Volumes ONTAP en un grupo de recursos compartido 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 la "permisos requeridos" La consola elimina los recursos de Cloud Volumes ONTAP de un grupo de recursos en caso de falla o eliminación de la implementación.
Grupo de seguridad generado	Si deja que la consola genere el grupo de seguridad por usted, deberá elegir cómo permitirá el tráfico: • Si elige **Solo VNet seleccionado**, la fuente del tráfico entrante es el rango de subred de la VNet seleccionada y el rango de subred de la VNet donde reside el agente de la consola. Esta es la opción recomendada. • Si elige **Todas las redes virtuales**, la fuente del tráfico entrante es el rango de IP 0.0.0.0/0.
Utilizar los existentes	Si elige un grupo de seguridad existente, debe cumplir con los requisitos de Cloud Volumes ONTAP . "Ver el grupo de seguridad predeterminado" .

9. **Métodos de carga y cuenta NSS**: especifique qué opción de carga desea utilizar con este sistema y luego especifique una cuenta del sitio de soporte de NetApp .
   - "Obtenga más 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 elige uno de los paquetes, solo necesita especificar un volumen y luego revisar y aprobar la configuración.

11. **Licencia**: cambie la versión de Cloud Volumes ONTAP si es necesario y seleccione un tipo de máquina virtual.

    Si hay disponible una versión más nueva de Candidato de lanzamiento, Disponibilidad general o versión de parche 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 9.16.1 P3 y 9.16.1 P4 está disponible. La actualización no se produce de una versión a otra, por ejemplo, de 9.15 a 9.16.

12. **Suscribirse desde Azure Marketplace**: verá esta página si la consola no pudo habilitar las implementaciones programáticas de Cloud Volumes ONTAP. Siga los pasos que aparecen en la pantalla. Consulte "Implementación programática de productos del Marketplace" Para más información.
13. **Recursos de almacenamiento subyacentes**: elija configuraciones para el agregado inicial: un tipo de disco, un tamaño para cada disco y si se debe habilitar la organización en niveles de datos en el

almacenamiento de blobs.

Tenga en cuenta lo siguiente:

- Si el acceso público a su cuenta de almacenamiento está deshabilitado dentro de la VNet, no podrá habilitar la organización en niveles de datos en su sistema Cloud Volumes ONTAP . Para obtener más información, consulte"Reglas del grupo de seguridad" .
- El tipo de disco es para el volumen inicial. Puede elegir un tipo de disco diferente para los volúmenes posteriores.
- El tamaño del disco es para todos los discos en el agregado inicial y para cualquier agregado adicional que la Consola crea cuando 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 para elegir un tipo y tamaño de disco, consulte"Dimensionar su sistema en Azure" .

- Puede elegir una política de niveles de volumen específica al crear o editar un volumen.
- Si deshabilita la clasificación de datos, puede habilitarla en agregados posteriores.

  "Obtenga más información sobre la clasificación de datos" .

14. **Velocidad de escritura y GUSANO**:

    a. Elija velocidad de escritura **Normal** o **Alta**, si lo desea.

       "Obtenga más información sobre la velocidad de escritura" .

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

       Esta opción sólo está disponible para ciertos tipos de máquinas virtuales. Para saber qué tipos de máquinas virtuales son compatibles, consulte"Configuraciones admitidas por licencia para pares HA" .

       No se puede habilitar WORM si la clasificación de datos se habilitó para las versiones 9.7 y anteriores de Cloud Volumes ONTAP . La reversión o degradación a Cloud Volumes ONTAP 9.8 está bloqueada después de habilitar WORM y la clasificación en niveles.

    "Obtenga más información sobre el almacenamiento WORM" .

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

15. **Crear volumen**: Ingrese detalles para el nuevo volumen o haga clic en **Omitir**.

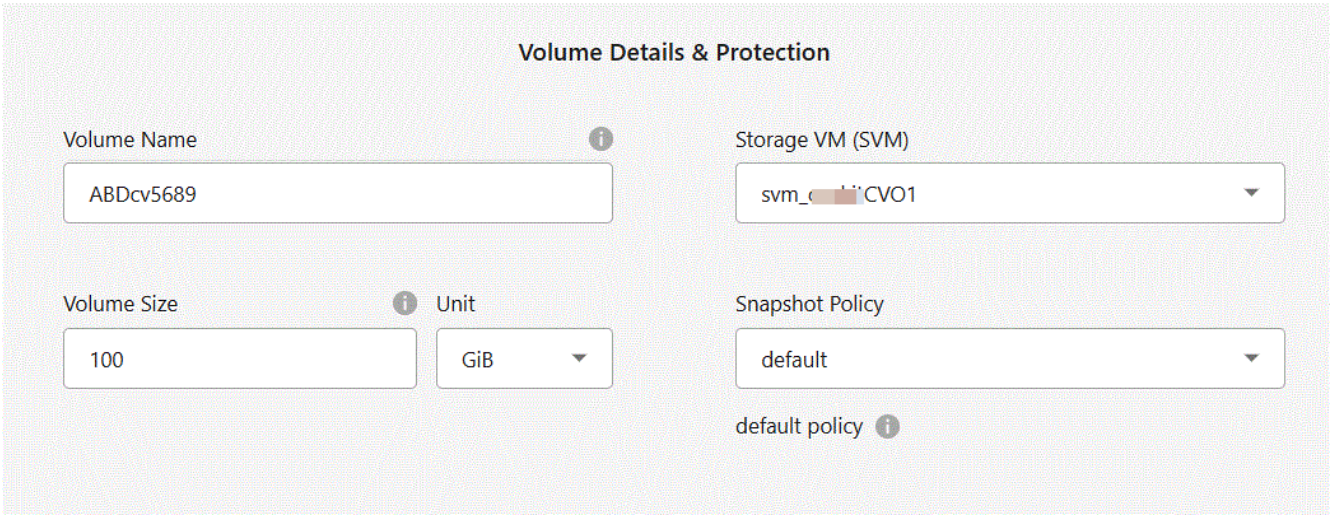
    "Obtenga información sobre los protocolos y versiones de cliente compatibles" .

    Algunos de los campos de esta página se explican por sí solos. La siguiente tabla describe los campos para los que podría necesitar orientación:

Campo	Descripción
Size	El tamaño máximo que puede ingresar depende en gran medida de si habilita el aprovisionamiento fino, que le permite crear un volumen que sea más grande que el almacenamiento físico actualmente disponible para él.

Campo	Descripción
Control de acceso (solo para NFS)	Una política de exportación define los clientes de la subred que pueden acceder al volumen. De forma predeterminada, la consola ingresa un valor que proporciona acceso a todas las instancias de la subred.
Permisos y usuarios/grupos (solo para CIFS)	Estos campos le permiten controlar el nivel de acceso a un recurso compartido para usuarios y grupos (también llamados listas de control de acceso o ACL). Puede especificar usuarios o grupos de Windows locales o de dominio, o usuarios o grupos de UNIX. Si especifica un nombre de usuario de dominio de Windows, debe incluir el dominio del usuario utilizando el formato dominio\nombre de usuario.
Política de instantáneas	Una política de copia de instantáneas especifica la frecuencia y la cantidad de copias de instantáneas de NetApp creadas automáticamente. Una copia Snapshot de NetApp es una imagen del sistema de archivos en un momento determinado que no tiene impacto en el rendimiento y requiere un almacenamiento mínimo. Puede elegir la política predeterminada o ninguna. Puede elegir ninguno para 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 iniciador e IQN (solo para iSCSI)	Los objetivos de almacenamiento iSCSI se denominan LUN (unidades lógicas) y se presentan a los hosts como dispositivos de bloque estándar. Los grupos de iniciadores son tablas de nombres de nodos de host iSCSI y controlan qué iniciadores tienen acceso a qué LUN. Los objetivos iSCSI se conectan a la red a través de adaptadores de red Ethernet estándar (NIC), tarjetas de motor de descarga TCP (TOE) con iniciadores de software, adaptadores de red convergente (CNA) o adaptadores de bus de host dedicados (HBA) y se identifican mediante nombres calificados iSCSI (IQN). Cuando crea un volumen iSCSI, la consola crea automáticamente un LUN para usted. Lo hemos simplificado creando solo un LUN por volumen, por lo que no es necesario realizar ninguna gestión. Después de crear el volumen,"Utilice el IQN para conectarse al LUN desde sus hosts" .

La siguiente imagen muestra la primera página del asistente de creación de volumen:



16. **Configuración CIFS**: si eligió el protocolo CIFS, configure un servidor CIFS.

Campo	Descripción
Dirección IP primaria y secundaria de DNS	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 ubicar los servidores LDAP de Active Directory y los controladores de dominio para el 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	El nombre y la contraseña de una cuenta de Windows con privilegios suficientes para agregar computadoras a la unidad organizativa (OU) especificada dentro del dominio de AD.
Nombre NetBIOS del servidor CIFS	Un nombre de servidor CIFS que es único en el dominio AD.
Unidad organizativa	La unidad organizativa dentro del dominio AD para asociarse con el servidor CIFS. El valor predeterminado es CN=Computers. Para configurar Azure AD Domain Services como servidor de AD para Cloud Volumes ONTAP, debe ingresar **OU=AADDC Computers** o **OU=AADDC Users** en este campo.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Documentación de Azure: Crear una unidad organizativa (OU) en un dominio administrado 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 utilizando el DNS de Active Directory. Si necesita configurar un servidor NTP utilizando una dirección diferente, debe utilizar la API. Consulte la "Documentación de automatización de la NetApp Console" Para más detalles. Tenga en cuenta que solo puede configurar un servidor NTP al crear un servidor CIFS. No es configurable después de crear el servidor CIFS.

17. **Perfil de uso, tipo de disco y política de niveles**: elija si desea habilitar las funciones de eficiencia de almacenamiento y cambiar la política de niveles de volumen, si es necesario.

    Para obtener más información, consulte"Comprensión de los perfiles de uso del volumen" y"Descripción general de la clasificación de datos" .

18. **Revisar y aprobar**: revise y confirme sus selecciones.
    a. Revise los detalles sobre la configuración.
    b. Haga clic en **Más información** para revisar los detalles sobre el soporte y los recursos de Azure que comprará la consola.
    c. Seleccione la casilla de verificación **Entiendo…**.
    d. Haga clic en **Ir**.

Resultado

La consola implementa el sistema Cloud Volumes ONTAP . Puede seguir el progreso en la página Auditoría.

Si experimenta algún problema al implementar el sistema Cloud Volumes ONTAP , revise el mensaje de error. También puede seleccionar el sistema y hacer clic en **Recrear entorno**.

Para obtener ayuda adicional, visite "Compatibilidad con NetApp Cloud Volumes ONTAP" .

> Una vez completado el proceso de implementación, no modifique las configuraciones de Cloud Volumes ONTAP generadas por el sistema en el portal de Azure, especialmente las etiquetas del sistema. Cualquier cambio realizado en estas configuraciones puede provocar un comportamiento inesperado o pérdida de datos.

Después de terminar

- Si aprovisionó un recurso compartido CIFS, otorgue a los usuarios o grupos permisos para los archivos y carpetas y verifique que esos usuarios puedan acceder al recurso compartido y crear un archivo.
- Si desea aplicar cuotas a los volúmenes, utilice el Administrador del sistema ONTAP o la CLI de ONTAP .

  Las cuotas le permiten restringir o rastrear el espacio en disco y la cantidad de archivos utilizados por un usuario, grupo o qtree.

Lanzar un par de Cloud Volumes ONTAP HA en Azure

Si desea iniciar un par de HA de Cloud Volumes ONTAP en Azure, debe crear un sistema de HA en la consola.

Pasos

1. Desde el menú de navegación de la izquierda, seleccione **Almacenamiento > Administración**.
2. En la página **Sistemas**, haga clic en **Agregar sistema** y siga las instrucciones.
3. Si se le solicita, "crear un agente de consola" .
4. **Detalles y credenciales**: Opcionalmente, cambie las credenciales y la suscripción de Azure, especifique un nombre de clúster, agregue etiquetas si es necesario y luego especifique las credenciales.

   La siguiente tabla describe los campos para los que podría necesitar orientación:

Campo	Descripción
Nombre del sistema	La consola usa el nombre del sistema 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 de grupos de recursos	Las etiquetas son metadatos para sus recursos de Azure. Cuando ingresa etiquetas en este campo, la consola las agrega al grupo de recursos asociado con el sistema Cloud Volumes ONTAP . Puede agregar hasta cuatro etiquetas desde la interfaz de usuario al crear un sistema y luego puede agregar más una vez creado. Tenga en cuenta que la API no lo limita a cuatro etiquetas al crear un sistema. Para obtener información sobre las etiquetas, consulte la "Documentación de Microsoft Azure: Uso de etiquetas para organizar los recursos de Azure" .
Nombre de usuario y contraseña	Estas son las credenciales para la cuenta de administrador del clúster de Cloud Volumes ONTAP . Puede usar estas credenciales para conectarse a Cloud Volumes ONTAP a través de ONTAP System Manager o la CLI de ONTAP . 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 usar con este sistema Cloud Volumes ONTAP . Debe asociar una suscripción de Azure Marketplace con la suscripción de Azure seleccionada para implementar un sistema Cloud Volumes ONTAP de pago por uso. "Aprenda cómo agregar credenciales" .

5. **Servicios**: habilite o deshabilite los servicios individuales según si desea usarlos con Cloud Volumes ONTAP.
   - "Obtenga más información sobre la NetApp Data Classification"
   - "Obtenga más información sobre NetApp Backup and Recovery"

   Si desea utilizar WORM y niveles de datos, debe deshabilitar la función de copia de seguridad y recuperación e implementar un sistema Cloud Volumes ONTAP con la versión 9.8 o superior.

6. **Modelos de implementación de HA**:
   a. Seleccione **Zona de disponibilidad única** o **Zona de disponibilidad múltiple**.
      - Para zonas de disponibilidad individuales, seleccione una región de Azure, una zona de disponibilidad, una red virtual y una subred.

        A partir de Cloud Volumes ONTAP 9.15.1, puede implementar instancias de máquinas virtuales (VM) en modo HA en zonas de disponibilidad (AZ) únicas en Azure. Debe seleccionar una zona y una región que admitan esta implementación. Si la zona o región no admite la implementación zonal, se sigue el modo de implementación no zonal anterior para LRS. Para comprender las configuraciones compatibles con los discos administrados compartidos, consulte"Configuración de zona de disponibilidad única de HA con discos administrados compartidos" .

      - Para múltiples zonas de disponibilidad, seleccione una región, una red virtual, una subred, una zona para el nodo 1 y una zona para el nodo 2.

   b. Seleccione la casilla de verificación **He verificado la conectividad de red…**.

7. **Conectividad**: Elija un grupo de recursos nuevo o existente y luego elija si desea utilizar el grupo de seguridad predefinido o utilizar el suyo propio.

   La siguiente tabla describe los campos para los que podría necesitar orientación:

Campo	Descripción
Grupo de recursos	Cree un nuevo grupo de recursos para Cloud Volumes ONTAP o utilice un grupo de recursos existente. La mejor práctica es utilizar un nuevo grupo de recursos dedicado para Cloud Volumes ONTAP. Si bien es posible implementar Cloud Volumes ONTAP en un grupo de recursos compartido existente, no se recomienda debido al riesgo de pérdida de datos. Consulte la advertencia anterior para obtener más detalles. Debe utilizar un grupo de recursos dedicado para cada par de Cloud Volumes ONTAP HA que implemente en Azure. Solo se admite un par HA en un grupo de recursos. La consola experimenta problemas de conexión si intenta implementar un segundo par de Cloud Volumes ONTAP HA en un grupo de recursos de Azure. Si la cuenta de Azure que está utilizando tiene la "permisos requeridos" La consola elimina los recursos de Cloud Volumes ONTAP de un grupo de recursos en caso de falla o eliminación de la implementación.
Grupo de seguridad generado	Si deja que la consola genere el grupo de seguridad por usted, deberá elegir cómo permitirá el tráfico: • Si elige **Solo VNet seleccionado**, la fuente del tráfico entrante es el rango de subred de la VNet seleccionada y el rango de subred de la VNet donde reside el agente de la consola. Esta es la opción recomendada. • Si elige **Todas las redes virtuales**, la fuente del tráfico entrante es el rango de IP 0.0.0.0/0.
Utilizar los existentes	Si elige un grupo de seguridad existente, debe cumplir con los requisitos de Cloud Volumes ONTAP . "Ver el grupo de seguridad predeterminado" .

8. **Métodos de carga y cuenta NSS**: especifique qué opción de carga desea utilizar con este sistema y luego especifique una cuenta del sitio de soporte de NetApp .
   - "Obtenga más 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 elige uno de los paquetes, solo necesita especificar un volumen y luego 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 candidata a lanzamiento, una versión de disponibilidad general o una versión de parche más reciente para la versión seleccionada, la consola actualiza el sistema a esa versión al crearla. Por ejemplo, la actualización se produce si selecciona Cloud Volumes ONTAP 9.13.1 y 9.13.1 P4 está disponible. La actualización no se produce de una versión a otra, por ejemplo, de 9.13 a 9.14.

11. **Suscribirse desde Azure Marketplace**: siga los pasos si la consola no pudo habilitar las implementaciones programáticas de Cloud Volumes ONTAP.
12. **Recursos de almacenamiento subyacentes**: elija configuraciones para el agregado inicial: un tipo de disco, un tamaño para cada disco y si se debe habilitar la organización en niveles de datos en el almacenamiento de blobs.

    Tenga en cuenta lo siguiente:

    - El tamaño del disco es para todos los discos en el agregado inicial y para cualquier agregado adicional que la Consola crea cuando 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 para elegir un tamaño de disco, consulte"Dimensione su sistema en Azure" .

    - Si el acceso público a su cuenta de almacenamiento está deshabilitado dentro de la VNet, no podrá habilitar la organización en niveles de datos en su sistema Cloud Volumes ONTAP . Para obtener más información, consulte"Reglas del grupo de seguridad" .
    - Puede elegir una política de niveles de volumen específica al crear o editar un volumen.
    - Si deshabilita la clasificación de datos, puede habilitarla en agregados posteriores.

      "Obtenga más información sobre la clasificación de datos" .

    - A partir de Cloud Volumes ONTAP 9.15.0P1, los blobs en páginas de Azure ya no son compatibles con las nuevas implementaciones de pares de alta disponibilidad. Si actualmente usa blobs de páginas de Azure en implementaciones de pares de alta disponibilidad existentes, puede migrar a tipos de instancias de VM más nuevos en las VM de las series Edsv4 y Edsv5.

      "Obtenga más información sobre las configuraciones compatibles en Azure" .

13. **Velocidad de escritura y GUSANO**:

    a. Elija velocidad de escritura **Normal** o **Alta**, si lo desea.

       "Obtenga más información sobre la velocidad de escritura" .

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

       Esta opción sólo está disponible para ciertos tipos de máquinas virtuales. Para saber qué tipos de máquinas virtuales son compatibles, consulte"Configuraciones admitidas por licencia para pares HA" .

       No se puede habilitar WORM si la clasificación de datos se habilitó para las versiones 9.7 y anteriores de Cloud Volumes ONTAP . La reversión o degradación a Cloud Volumes ONTAP 9.8 está bloqueada después de habilitar WORM y la clasificación en niveles.

    "Obtenga más información sobre el almacenamiento WORM" .

    a. Si activa el almacenamiento WORM, seleccione el período de retención.
14. **Comunicación segura con almacenamiento y WORM**: elija si desea habilitar una conexión HTTPS a las cuentas de almacenamiento de Azure y activar el almacenamiento de escritura única, lectura múltiple (WORM), si lo desea.

    La conexión HTTPS es de un par de Cloud Volumes ONTAP 9.7 HA a cuentas de almacenamiento de blobs en páginas de Azure. Tenga en cuenta que habilitar esta opción puede afectar el rendimiento de escritura. No puedes cambiar la configuración después de crear el sistema.

"Obtenga más información sobre el almacenamiento WORM" .

No se puede habilitar WORM si se habilitó la clasificación de datos.

"Obtenga más información sobre el almacenamiento WORM" .

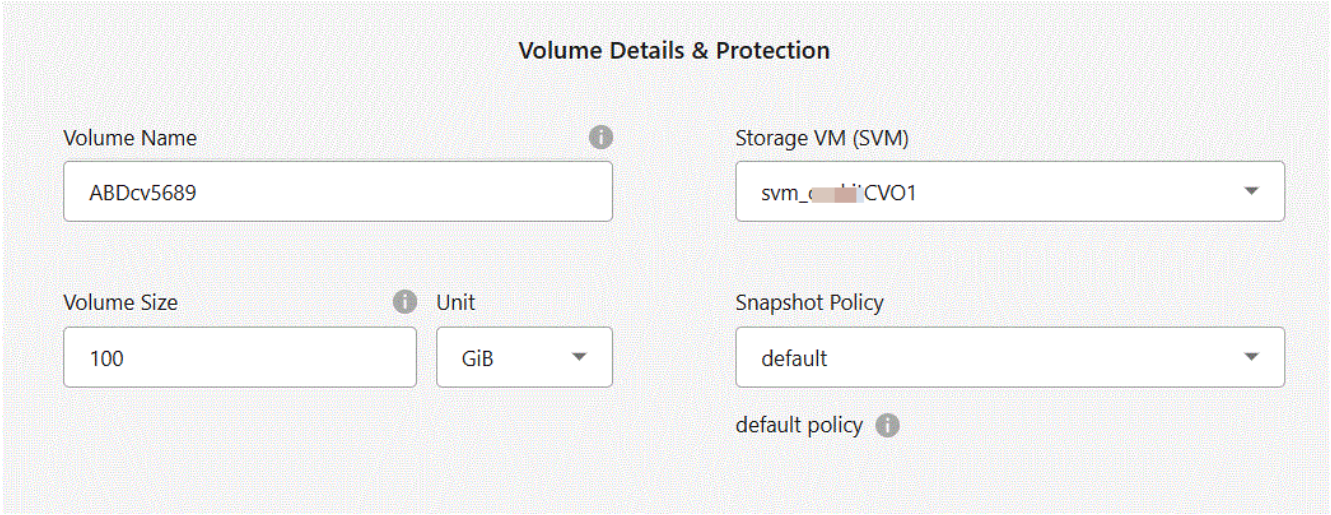
15. **Crear volumen**: Ingrese detalles para el nuevo volumen o haga clic en **Omitir**.

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

    Algunos de los campos de esta página se explican por sí solos. La siguiente tabla describe los campos para los que podría necesitar orientación:

Campo	Descripción
Size	El tamaño máximo que puede ingresar depende en gran medida de si habilita el aprovisionamiento fino, que le permite crear un volumen que sea más grande que el almacenamiento físico actualmente disponible para él.
Control de acceso (solo para NFS)	Una política de exportación define los clientes de la subred que pueden acceder al volumen. De forma predeterminada, la consola ingresa un valor que proporciona acceso a todas las instancias de la subred.
Permisos y usuarios/grupos (solo para CIFS)	Estos campos le permiten controlar el nivel de acceso a un recurso compartido para usuarios y grupos (también llamados listas de control de acceso o ACL). Puede especificar usuarios o grupos de Windows locales o de dominio, o usuarios o grupos de UNIX. Si especifica un nombre de usuario de dominio de Windows, debe incluir el dominio del usuario utilizando el formato dominio\nombre de usuario.
Política de instantáneas	Una política de copia de instantáneas especifica la frecuencia y la cantidad de copias de instantáneas de NetApp creadas automáticamente. Una copia Snapshot de NetApp es una imagen del sistema de archivos en un momento determinado que no tiene impacto en el rendimiento y requiere un almacenamiento mínimo. Puede elegir la política predeterminada o ninguna. Puede elegir ninguno para 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 iniciador e IQN (solo para iSCSI)	Los objetivos de almacenamiento iSCSI se denominan LUN (unidades lógicas) y se presentan a los hosts como dispositivos de bloque estándar. Los grupos de iniciadores son tablas de nombres de nodos de host iSCSI y controlan qué iniciadores tienen acceso a qué LUN. Los objetivos iSCSI se conectan a la red a través de adaptadores de red Ethernet estándar (NIC), tarjetas de motor de descarga TCP (TOE) con iniciadores de software, adaptadores de red convergente (CNA) o adaptadores de bus de host dedicados (HBA) y se identifican mediante nombres calificados iSCSI (IQN). Cuando crea un volumen iSCSI, la consola crea automáticamente un LUN para usted. Lo hemos simplificado creando solo un LUN por volumen, por lo que no es necesario realizar ninguna gestión. Después de crear el volumen,"Utilice el IQN para conectarse al LUN desde sus hosts" .

    La siguiente imagen muestra la primera página del asistente de creación de volumen:



16. **Configuración CIFS**: si eligió el protocolo CIFS, configure un servidor CIFS.

Campo	Descripción
Dirección IP primaria y secundaria de DNS	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 ubicar los servidores LDAP de Active Directory y los controladores de dominio para el 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	El nombre y la contraseña de una cuenta de Windows con privilegios suficientes para agregar computadoras a la unidad organizativa (OU) especificada dentro del dominio de AD.
Nombre NetBIOS del servidor CIFS	Un nombre de servidor CIFS que es único en el dominio AD.
Unidad organizativa	La unidad organizativa dentro del dominio AD para asociarse con el servidor CIFS. El valor predeterminado es CN=Computers. Para configurar Azure AD Domain Services como servidor de AD para Cloud Volumes ONTAP, debe ingresar **OU=AADDC Computers** o **OU=AADDC Users** en este campo.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Documentación de Azure: Crear una unidad organizativa (OU) en un dominio administrado 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 utilizando el DNS de Active Directory. Si necesita configurar un servidor NTP utilizando una dirección diferente, debe utilizar la API. Consulte la "Documentación de automatización de la NetApp Console" Para más detalles. Tenga en cuenta que solo puede configurar un servidor NTP al crear un servidor CIFS. No es configurable después de crear el servidor CIFS.

17. **Perfil de uso, tipo de disco y política de niveles**: elija si desea habilitar las funciones de eficiencia de almacenamiento y cambiar la política de niveles de volumen, si es necesario.

Para obtener más información, consulte"Elija un perfil de uso de volumen" ,"Descripción general de la clasificación de datos" , y "KB: ¿Qué funciones de eficiencia de almacenamiento en línea son compatibles con CVO?"

18. **Revisar y aprobar**: revise y confirme sus selecciones.
    a. Revise los detalles sobre la configuración.
    b. Haga clic en **Más información** para revisar los detalles sobre el soporte y los recursos de Azure que comprará la consola.
    c. Seleccione la casilla de verificación **Entiendo…**.
    d. Haga clic en **Ir**.

Resultado

La consola implementa el sistema Cloud Volumes ONTAP . Puede seguir el progreso en la página Auditoría.

Si experimenta algún problema al implementar el sistema Cloud Volumes ONTAP , revise el mensaje de error. También puede seleccionar el sistema y hacer clic en **Recrear entorno**.

Para obtener ayuda adicional, visite "Compatibilidad con NetApp Cloud Volumes ONTAP" .

Después de terminar

- Si aprovisionó un recurso compartido CIFS, otorgue a los usuarios o grupos permisos para los archivos y carpetas y verifique que esos usuarios puedan acceder al recurso compartido y crear un archivo.
- Si desea aplicar cuotas a los volúmenes, utilice el Administrador del sistema ONTAP o la CLI de ONTAP .

  Las cuotas le permiten restringir o rastrear el espacio en disco y la cantidad de archivos utilizados por un usuario, grupo o qtree.

Una vez completado el proceso de implementación, no modifique las configuraciones de Cloud Volumes ONTAP generadas por el sistema en el portal de Azure, especialmente las etiquetas del sistema. Cualquier cambio realizado en estas configuraciones puede provocar un comportamiento inesperado o pérdida de datos.

Enlaces relacionados

*"Planificación de la configuración de Cloud Volumes ONTAP en Azure" *"Implementar Cloud Volumes ONTAP en Azure desde Azure Marketplace"

Verificar la imagen de la plataforma Azure

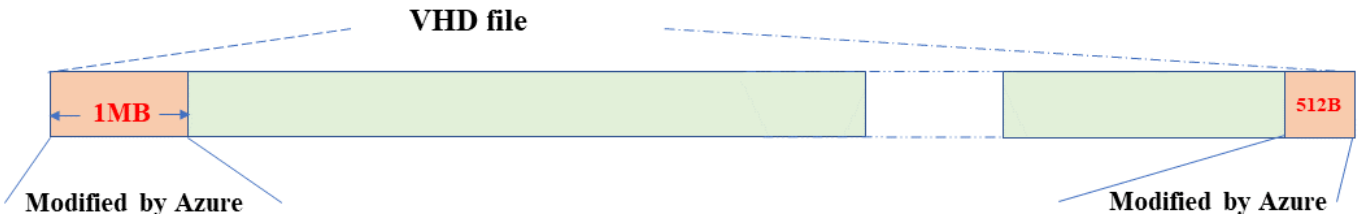
Verificación de imágenes de Azure Marketplace para Cloud Volumes ONTAP

La verificación de imágenes de Azure cumple con los requisitos de seguridad mejorados de NetApp . Verificar un archivo de imagen es un proceso sencillo. Sin embargo, la verificación de la firma de la imagen de Azure requiere consideraciones específicas para el archivo de imagen VHD de Azure porque se modifica en Azure Marketplace.

La verificación de imágenes de Azure es compatible con Cloud Volumes ONTAP 9.15.0 y versiones posteriores.

Alteración de archivos VHD publicados por parte de Azure

Azure modifica los 1 MB (1048576 bytes) al principio y los 512 bytes al final del archivo VHD. NetApp firma el archivo VHD restante.



En el ejemplo, el archivo VHD es de 10 GB. La parte que firmó NetApp está marcada en verde (10 GB - 1 MB - 512 bytes).

Enlaces relacionados

- "Blog de errores de página: Cómo firmar y verificar usando OpenSSL"
- "Usar la imagen de Azure Marketplace para crear una imagen de máquina virtual para su GPU de Azure Stack Edge Pro | Microsoft Learn"
- "Exportar o copiar un disco administrado a una cuenta de almacenamiento mediante la CLI de Azure | Microsoft Learn"
- "Guía de inicio rápido de Azure Cloud Shell: Bash | Microsoft Learn"
- "Cómo instalar la CLI de Azure | Microsoft Learn"
- "Copia de blobs de almacenamiento de Az | Microsoft Learn"
- "Sign in con la CLI de Azure: Inicio de sesión y autenticación | Microsoft Learn"

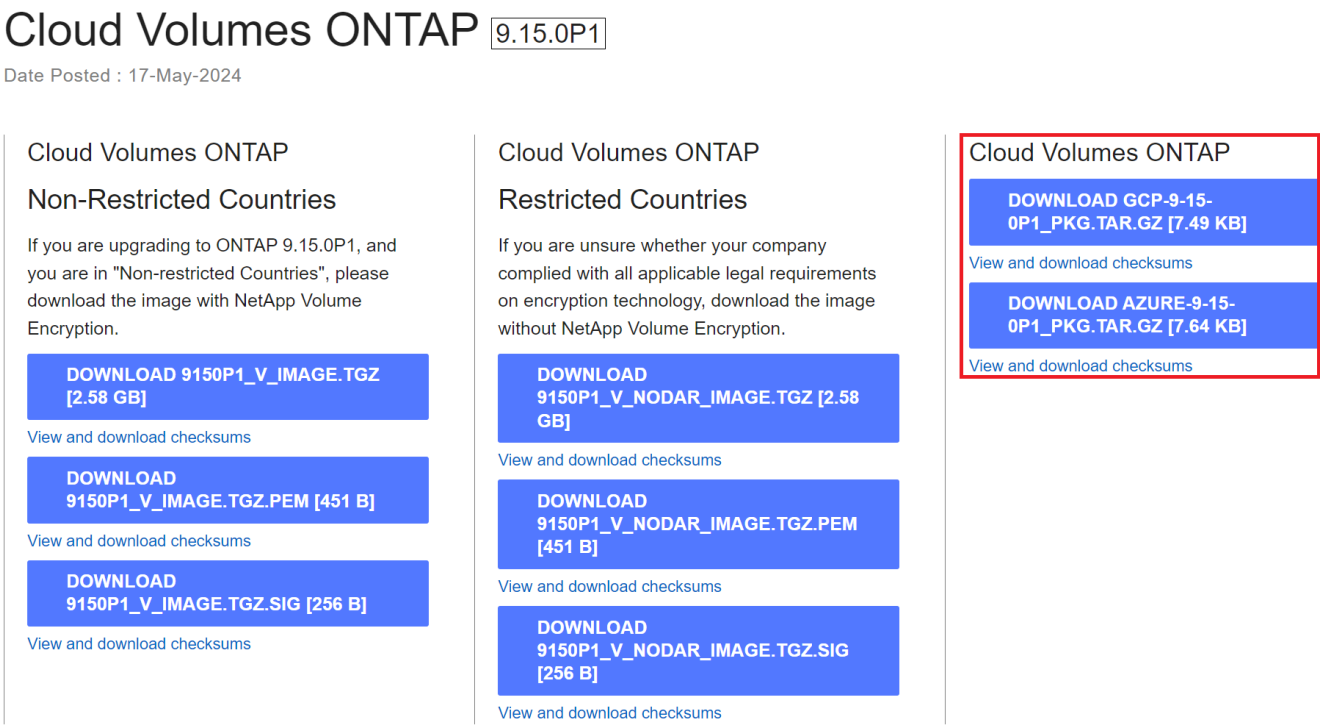
Descargue el archivo de imagen de Azure para Cloud Volumes ONTAP

Puede descargar el archivo de imagen de Azure desde "Sitio de soporte de NetApp" .

El archivo *tar.gz* contiene los archivos necesarios para la verificación de la firma de la imagen. Junto con el archivo *tar.gz*, también debe descargar el archivo *checksum* de la imagen. El archivo de suma de comprobación contiene la `md5` y `sha256` sumas de comprobación del archivo *tar.gz*.

Pasos

1. Ir a la "Página del producto Cloud Volumes ONTAP en el sitio de soporte de NetApp" y descargue la versión de software requerida desde la sección **Descargas**.
2. En la página de descarga de Cloud Volumes ONTAP , haga clic en el archivo descargable de la imagen de Azure y descargue el archivo *tar.gz*.



3. En Linux, ejecute `md5sum AZURE-<version>_PKG.TAR.GZ .`

   En macOS, ejecute `sha256sum AZURE-<version>_PKG.TAR.GZ .`

4. Verificar que el `md5sum` y `sha256sum` Los valores coinciden con los de la imagen de Azure descargada.
5. En Linux y macOS, extraiga el archivo *tar.gz* usando el `tar -xzf` dominio.

   El archivo *tar.gz* extraído contiene el archivo de resumen (*.sig*), el archivo de certificado de clave pública (*.pem*) y el archivo de certificado de cadena (*.pem*).

   Ejemplo de salida después de extraer el archivo tar.gz:

```
$ 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
```

Exportar imágenes VHD para Cloud Volumes ONTAP desde Azure Marketplace

Una vez que la imagen VHD se publica en la nube de Azure, NetApp ya no la administra. En su lugar, la imagen publicada se coloca en el mercado de Azure. Cuando la imagen se prepara y se publica en Azure Marketplace, Azure modifica 1 MB al principio y 512 bytes al final del VHD. Para verificar la firma del archivo VHD, debe exportar la imagen VHD modificada por Azure desde Azure Marketplace.

Antes de empezar

Asegúrese de que la CLI de Azure esté instalada en su sistema o que Azure Cloud Shell esté disponible a través del portal de Azure. Para obtener más información sobre cómo instalar la CLI de Azure, consulte "Documentación de Microsoft: Cómo instalar la CLI de Azure" .

Pasos

1. Asigne la versión de Cloud Volumes ONTAP en su sistema a la versión de la imagen de Azure Marketplace usando el contenido del archivo *version_readme*. La versión de Cloud Volumes ONTAP está representada por `buildname` y la versión de la imagen de Azure Marketplace está representada por `version` en las asignaciones de versiones.

   En el siguiente ejemplo, la versión de Cloud Volumes ONTAP `9.15.0P1` se asigna a la versión de la imagen de Azure Marketplace `9150.01000024.05090105` . Esta versión de la imagen de Azure Marketplace se utiliza posteriormente para establecer la URN de la imagen.

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

   ]
   ```

2. Identifique la región donde desea crear las máquinas virtuales. El nombre de la región se utiliza como valor para el `locName` variable al configurar la URN de la imagen del marketplace. Para enumerar las regiones disponibles, ejecute este comando:

   ```
   az account list-locations -o table
   ```

   En esta tabla, el nombre de la región aparece en el `Name` campo.

   ```
   $ 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 los nombres de SKU para las versiones de Cloud Volumes ONTAP y los tipos de implementación de VM correspondientes en la siguiente tabla. El nombre del SKU se utiliza como valor para el `skuName` variable al configurar la URN de la imagen del marketplace.

   Por ejemplo, todas las implementaciones de un solo nodo con Cloud Volumes ONTAP 9.15.0 deben usar `ontap_cloud_byol` como el nombre del SKU.

*Versión de Cloud Volumes ONTAP *	**Implementación de VM a través de**	**Nombre del SKU**
9.17.1 y posteriores	El mercado de Azure	ontap_cloud_direct_gen2
9.17.1 y posteriores	La NetApp Console	ontap_cloud_gen2
9.16.1	El mercado de Azure	ontap_cloud_direct
9.16.1	La consola	ontap_cloud
9.15.1	La consola	ontap_cloud
9.15.0	La consola, implementaciones de nodo único	ontap_cloud_byol
9.15.0	La consola, implementaciones de alta disponibilidad (HA)	ontap_cloud_byol_ha

4. Después de asignar la versión de ONTAP y la imagen de Azure Marketplace, exporte el archivo VHD desde Azure Marketplace mediante Azure Cloud Shell o la CLI de Azure.

Exportar archivo VHD mediante Azure Cloud Shell en Linux

Desde Azure Cloud Shell, exporte la imagen de Marketplace al archivo VHD (por ejemplo, *9150.01000024.05090105.vhd*) y descárguelo en su sistema Linux local. Realice estos pasos para obtener la imagen VHD del mercado de Azure.

Pasos

1. Establezca la URN y otros parámetros de la imagen del mercado. El formato URN es `<publisher>:<offer>:<sku>:<version>` . Opcionalmente, puede enumerar las imágenes del mercado de NetApp para confirmar la versión correcta de la imagen.

```
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
...
```

2. Cree un nuevo disco administrado a partir de la imagen de Marketplace con la versión de imagen correspondiente:

```
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
```

3. Exporte el archivo VHD desde el disco administrado a Azure Storage. Cree un contenedor con el nivel de acceso adecuado. En este ejemplo, hemos utilizado un contenedor llamado `vm-images` con `Container` nivel de acceso. Obtenga la clave de acceso de la cuenta de almacenamiento desde el portal de Azure: **Cuentas de almacenamiento > *examplesaname* > Clave de acceso > *key1* > *key* > Mostrar > <*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
```

4. Descargue la imagen generada a su sistema Linux. Utilice el `wget` Comando para descargar el archivo VHD:

```
wget <URL of filename/Containers/vm-images/9150.01000024.05090105.vhd>
```

   La URL sigue un formato estándar. Para la automatización, puede derivar la cadena URL como se muestra a continuación. Alternativamente, puede utilizar la CLI de Azure `az` Comando para obtener la URL. URL de ejemplo:https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

5. Limpiar el disco administrado

```
PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG -DiskName
$diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName
$diskName
```

Exportar archivo VHD mediante la CLI de Azure en Linux

Exporte la imagen del mercado a un archivo VHD mediante la CLI de Azure desde un sistema Linux local.

Pasos

1. Inicie sesión en la CLI de Azure y enumere las imágenes del Marketplace:

```
% az login --use-device-code
```

2. Para iniciar sesión, utilice un navegador web para abrir la página. https://microsoft.com/devicelogin e ingrese el código de autenticación.

```
% 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"
},
...
```

3. Cree un nuevo disco administrado a partir de la imagen del mercado con la versión de imagen correspondiente.

```
% 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.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxxx"
}
% export diskAccessSAS="https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxx"
```

Para automatizar el proceso, es necesario extraer el SAS de la salida estándar. Consulte los documentos apropiados para obtener orientación.

4. Exportar el archivo VHD desde el disco administrado.

   a. Cree un contenedor con el nivel de acceso adecuado. En este ejemplo, un contenedor llamado `vm-images` con `Container` Se utiliza el nivel de acceso.

   b. Obtenga la clave de acceso de la cuenta de almacenamiento desde el portal de Azure: **Cuentas de almacenamiento > *examplesaname* > Clave de acceso > *key1* > *key* > Mostrar > <*copy*>**

      También puedes utilizar el `az` Comando para este paso.

```
% 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
}
```

5. Verifique el estado de la copia del blob.

```
% 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.bluexpinfraprod.eastus2.data.azurecr.io/xxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
      "status": "success",
      "statusDescription": null
    },
....
```

6. Descargue la imagen generada a su servidor Linux.

```
wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>
```

La URL sigue un formato estándar. Para la automatización, puede derivar la cadena URL como se muestra a continuación. Alternativamente, puede utilizar la CLI de Azure `az` Comando para obtener la URL. URL de ejemplo:https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

7. Limpiar el disco administrado

```
az disk revoke-access --name $diskName --resource-group $diskRG
az disk delete --name $diskName --resource-group $diskRG --yes
```

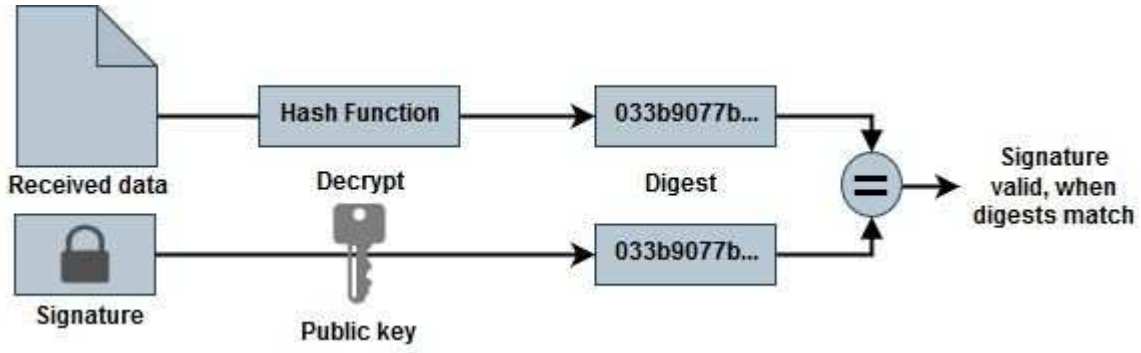
Verificar la firma del archivo

Verificación de la firma de imágenes de Azure Marketplace para Cloud Volumes ONTAP

El proceso de verificación de imágenes de Azure genera un archivo de resumen a partir del archivo VHD quitando 1 MB al principio y 512 bytes al final, y luego aplicando una función hash. Para que coincida con el procedimiento de firma, se utiliza *sha256* para el hash.

Resumen del flujo de trabajo de verificación de firmas de archivos

A continuación se presenta una descripción general del proceso de flujo de trabajo de verificación de firma de archivo.



- Descargar la imagen de Azure desde el "Sitio de soporte de NetApp" y extraer el archivo de resumen (.sig), el archivo de certificado de clave pública (.pem) y el archivo de certificado de cadena (.pem). Consulte "Descargar el archivo de resumen de imagen de Azure" Para más información.
- Verificación de la cadena de confianza.
- Extraer la clave pública (.pub) del certificado de clave pública (.pem).
- Descifrar el archivo de resumen utilizando la clave pública extraída.
- Comparando el resultado con un resumen recién generado de un archivo temporal creado a partir del archivo de imagen después de eliminar 1 MB al principio y 512 bytes al final. Este paso se realiza mediante la herramienta de línea de comandos OpenSSL. La herramienta CLI de OpenSSL muestra mensajes apropiados en caso de éxito o fracaso en la coincidencia de los archivos.

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

Verificar la firma de la imagen de Azure Marketplace para Cloud Volumes ONTAP en Linux

La verificación de la firma de un archivo VHD exportado en Linux incluye validar la cadena de confianza, editar el archivo y verificar la firma.

Pasos

1. Descargue el archivo de imagen de Azure desde "Sitio de soporte de NetApp" y extraiga el archivo de resumen (.sig), el archivo de certificado de clave pública (.pem) y el archivo de certificado de cadena (.pem).

   Referirse a "Descargar el archivo de resumen de imagen de Azure" Para más información.

2. Verificar 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 1 MB (1.048.576 bytes) al principio y 512 bytes al final del archivo VHD. Al utilizar `tail` , el `-c +K` La opción genera bytes a partir del byte K del archivo. Por lo tanto, pasa 1048577 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 eliminado (sign.tmp) con el archivo de firma y la clave pública.

   El símbolo del sistema muestra mensajes que indican el éxito o el fracaso según la 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. Limpiar el espacio de trabajo.

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

Verificar la firma de la imagen de Azure Marketplace para Cloud Volumes ONTAP en macOS

La verificación de la firma de un archivo VHD exportado en Linux incluye validar la cadena de confianza, editar el archivo y verificar la firma.

Pasos

1. Descargue el archivo de imagen de Azure desde "Sitio de soporte de NetApp" y extraiga el archivo de resumen (.sig), el archivo de certificado de clave pública (.pem) y el archivo de certificado de cadena (.pem).

   Referirse a "Descargar el archivo de resumen de imagen de Azure" Para más información.

2. Verificar 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 1 MB (1.048.576 bytes) al principio y 512 bytes al final del archivo VHD. Al utilizar `tail` , el `-c +K` La opción genera bytes a partir del byte K del archivo. Por lo tanto, pasa 1048577 a `tail -c` . Tenga en cuenta que en macOS, el comando tail puede tardar unos diez minutos en completarse.

```
% 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 eliminado (sign.tmp) con el archivo de firma y la clave pública. El símbolo del sistema muestra mensajes que indican el éxito o el fracaso según la 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. Limpiar el espacio de trabajo.

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

Implementar Cloud Volumes ONTAP desde Azure Marketplace

Puede utilizar la implementación directa de Azure Marketplace para implementar Cloud Volumes ONTAP de manera rápida y sencilla. Desde el mercado de Azure, puede implementar rápidamente Cloud Volumes ONTAP con unos pocos clics y explorar sus características y capacidades principales en su entorno.

Para obtener más información sobre esta oferta, consulte"Obtenga más información sobre las ofertas de Cloud Volumes ONTAP en la NetApp Console y el mercado." .

Acerca de esta tarea

El sistema Cloud Volumes ONTAP implementado mediante la implementación directa de Azure Marketplace tiene estas propiedades. Tenga en cuenta que las características de una instancia independiente implementada a través de Azure Marketplace cambian cuando se detecta en la NetApp Console.

- La última versión de Cloud Volumes ONTAP (9.16.1 o posterior).
- Una licencia gratuita para Cloud Volumes ONTAP que está limitada a 500 GiB de capacidad aprovisionada. Esta licencia no incluye soporte de NetApp y no tiene fecha de vencimiento.
- Dos nodos configurados en modo de alta disponibilidad (HA) en una única zona de disponibilidad (AZ), aprovisionados con números de serie predeterminados. Las máquinas virtuales de almacenamiento (VM de almacenamiento) se implementan en un"modo de orquestación flexible" .
- Un agregado para la instancia creada de forma predeterminada.
- Un disco administrado SSD v2 Premium con capacidad aprovisionada de 500 GiB, un disco raíz y un disco de datos.
- Se implementó una máquina virtual de almacenamiento de datos, con servicios de datos NFS, CIFS, iSCSI y NVMe/TCP. No es posible agregar ninguna máquina virtual de almacenamiento de datos adicional.
- Licencias instaladas para NFS, CIFS (SMB), iSCSI, Autonomous Ransomware Protection (ARP), SnapLock y SnapMirror.
- "Eficiencia de almacenamiento sensible a la temperatura (TSSE) de ONTAP", cifrado de volumen y administración de claves externas habilitadas de forma predeterminada.
- Estas funciones no son compatibles:
  - Nivelación de FabricPool
  - Cambiar el tipo de máquina virtual de almacenamiento
  - Modo de escritura rápida

Antes de empezar

- Asegúrese de tener una suscripción válida al mercado de Azure.
- Asegúrese de cumplir con los requisitos de red para un"Implementación de alta disponibilidad en una única zona de disponibilidad" en Azure. Consulte "Configurar la red de Azure para Cloud Volumes ONTAP" .
- Se le debe asignar uno de estos roles de Azure para implementar Cloud Volumes ONTAP:
  - El `contributor` rol con los permisos predeterminados. Para obtener más información, consulte la "Documentación de Microsoft Azure: Roles integrados de Azure" .
  - Un rol RBAC personalizado con los siguientes permisos. Para obtener más información, consulte la "Documentación de Azure: Roles personalizados de Azure" .

"permisos": [{ "acciones": ["Microsoft.AAD/registrar/acción",
"Microsoft.Recursos/suscripciones/gruposderecursos/escritura",
"Microsoft.Red/balanceadoresdecarga/escritura",
"Microsoft.ClassicCompute/máquinasvirtuales/escritura",
"Microsoft.Compute/gruposdereservacióndecapacidad/implementar/acción",
"Microsoft.ClassicCompute/máquinasvirtuales/interfacesdered/gruposdeseguridadderedasociados
/escritura", "Microsoft.Red/interfacesdered/escritura",
"Microsoft.Compute/máquinasvirtuales/escritura",
"Microsoft.Compute/máquinasvirtuales/extensiones/escritura",
"Microsoft.Recursos/implementaciones/validar/acción",
"Microsoft.Recursos/suscripciones/gruposderecursos/lectura",
"Microsoft.Red/redesvirtuales/escritura", "Microsoft.Network/virtualNetworks/lectura",
"Microsoft.Network/networkSecurityGroups/escritura",
"Microsoft.Network/networkSecurityGroups/lectura", "Microsoft.Compute/discos/escritura",
"Microsoft.Compute/virtualMachineScaleSets/escritura",
"Microsoft.Recursos/implementaciones/escritura",
"Microsoft.Network/virtualNetworks/subredes/lectura",
"Microsoft.Network/virtualNetworks/subredes/escritura"], "notActions": [], "dataActions": [],
"notDataActions": [] }]

Si ha registrado el proveedor de recursos "Microsoft.storage" en su suscripción, entonces no necesita el `Microsoft.AAD/register/action` permiso. Para obtener más información, consulte la "Documentación de Azure: Permisos de Azure para almacenamiento" .

Pasos

1. Desde el sitio de Azure Marketplace, busque productos NetApp .
2. Seleccione * NetApp Cloud Volumes ONTAP directo*.
3. Haga clic en **Crear** para iniciar el asistente de implementación.
4. Seleccione un plan. La lista **Plan** generalmente muestra las últimas versiones de Cloud Volumes ONTAP.
5. En la pestaña **Información básica**, proporcione estos detalles:
   - **Suscripción**: Seleccione una suscripción. La implementación estará vinculada al número de suscripción.
   - **Grupo de recursos**: utilice un grupo de recursos existente o cree uno nuevo. Los grupos de recursos ayudan a asignar todos los recursos, como discos y máquinas virtuales de almacenamiento, dentro de un solo grupo para un sistema Cloud Volumes ONTAP .
   - **Región**: seleccione una región que admita la implementación de Azure HA en una sola zona de disponibilidad. Solo verás las regiones disponibles en la lista.
   - **Tamaño**: seleccione un tamaño de VM de almacenamiento para el disco administrado SSD v2 Premium compatible.
   - **Zona**: Seleccione una zona para la región que seleccionó.
   - **Contraseña de administrador**: Establezca una contraseña. Utilice esta contraseña de administrador para iniciar sesión en el sistema después de la implementación.
   - **Confirmar contraseña**: Vuelva a ingresar la misma contraseña para confirmarla.
     - En la pestaña **Red**, agregue una red virtual y una subred, o selecciónelas de las listas.

Para cumplir con las restricciones de Microsoft Azure, debe crear una nueva subred al configurar una nueva red virtual. Del mismo modo, si elige una red existente, deberá seleccionar una subred existente.

- Para seleccionar un grupo de seguridad de red predefinido, seleccione **Sí**. Seleccione **No** para asignar un grupo de seguridad de red de Azure predefinido con las reglas de tráfico necesarias. Para obtener más información, consulte "Reglas de grupo de seguridad para Azure" .
- En la pestaña **Avanzado**, confirme si se han configurado las dos características de Azure necesarias para esta implementación. Referirse a"Habilitar una función de Azure para implementaciones de zona de disponibilidad única de Cloud Volumes ONTAP" y"Habilitar el modo de alta disponibilidad para Cloud Volumes ONTAP en Azure" .
- Puede definir pares de nombre y valor para los recursos o grupos de recursos en la pestaña **Etiquetas**.
- En la pestaña **Revisar + crear**, revise los detalles e inicie la implementación.

Después de terminar

Seleccione el icono de notificación para ver el progreso de su implementación. Una vez implementado Cloud Volumes ONTAP , puede ver las máquinas virtuales de almacenamiento enumeradas para las operaciones.

Una vez accesible, use ONTAP System Manager o la CLI de ONTAP para iniciar sesión en la máquina virtual de almacenamiento con las credenciales de administrador que configuró. Posteriormente, puede crear volúmenes, LUN o recursos compartidos y comenzar a utilizar las capacidades de almacenamiento de Cloud Volumes ONTAP.

Solucionar problemas de implementación

Los sistemas Cloud Volumes ONTAP implementados directamente a través del mercado de Azure no incluyen soporte de NetApp. Si surge algún problema durante la implementación, puede solucionarlo y resolverlo de forma independiente.

Pasos

1. En el sitio de Azure Marketplace, vaya a **Diagnóstico de arranque > Registro de serie**.
2. Descargue e investigue los registros seriales.
3. Consulte la documentación del producto y los artículos de la base de conocimientos (KB) para solucionar problemas.
   - "Documentación de Azure Marketplace"
   - "Documentación de NetApp"
   - "Artículos de la base de conocimientos de NetApp"

Descubra los sistemas implementados en la consola

Puede descubrir los sistemas Cloud Volumes ONTAP que implementó mediante la implementación directa de Azure Marketplace y administrarlos en la página **Sistemas** de la Consola. El agente de la consola descubre los sistemas, los agrega, aplica las licencias necesarias y desbloquea todas las capacidades de la consola para estos sistemas. Se conserva la configuración de alta disponibilidad original en una única zona de disponibilidad con discos administrados PSSD v2, y el sistema se registra en la misma suscripción de Azure y el mismo grupo de recursos que la implementación original.

Acerca de esta tarea

Al descubrir los sistemas Cloud Volumes ONTAP implementados mediante la implementación directa de Azure

Marketplace, el agente de consola realiza estas tareas:

- Reemplaza las licencias gratuitas de los sistemas descubiertos como licencias regulares basadas en capacidad."Licencias freemium" .
- Conserva las capacidades existentes de los sistemas implementados y agrega las capacidades adicionales de la consola, como protección de datos, administración de datos y funciones de seguridad.
- Reemplaza las licencias instaladas en los nodos con nuevas licencias ONTAP para NFS, CIFS (SMB), iSCSI, ARP, SnapLock y SnapMirror.
- Convierte los números de serie de nodo genéricos en números de serie únicos.
- Asigna nuevas etiquetas de sistema a los recursos según sea necesario.
- Convierte las direcciones IP dinámicas de la instancia en direcciones IP estáticas.
- Habilita las funcionalidades de"Nivelación de FabricPool" ,"AutoSupport" , y"escribir una vez, leer muchas veces" (WORM) almacenamiento en los sistemas implementados. Puedes activar estas funciones desde la consola cuando las necesites.
- Registra las instancias en las cuentas NSS utilizadas para descubrirlas.
- Habilita funciones de gestión de capacidad en"modos automático y manual" para los sistemas descubiertos.

Antes de empezar

Asegúrese de que la implementación esté completa en Azure Marketplace. El agente de la consola puede descubrir los sistemas solo cuando se completa la implementación y están disponibles para el descubrimiento.

Pasos

En la consola, siga el procedimiento estándar para descubrir sistemas existentes. Consulte "Agregue un sistema Cloud Volumes ONTAP existente a la consola" .

> Durante el descubrimiento, es posible que veas mensajes de error, pero puedes ignorarlos hasta que se complete el proceso de descubrimiento. No modifique las configuraciones de Cloud Volumes ONTAP generadas por el sistema en el portal de Azure Marketplace durante la detección, especialmente las etiquetas del sistema. Cualquier cambio realizado en estas configuraciones puede provocar un comportamiento inesperado del sistema.

Después de terminar

Una vez finalizado el descubrimiento, podrá ver los sistemas enumerados en la página **Sistemas** en la Consola. Puede realizar diversas tareas de gestión, como:"expandiendo el agregado" ,"adición de volúmenes" ,"aprovisionamiento de máquinas virtuales de almacenamiento adicionales" , y"cambiando los tipos de instancia" .

Enlaces relacionados

Consulte la documentación de ONTAP para obtener más información sobre la creación de almacenamiento:

- "Crear volúmenes para NFS"
- "Crear LUN para iSCSI"
- "Crear recursos compartidos para CIFS"

Comience a usar Google Cloud

Inicio rápido de Cloud Volumes ONTAP en Google Cloud

Comience a utilizar Cloud Volumes ONTAP en Google Cloud en unos pocos pasos.

1 Crear un agente de consola

Si no tienes una "Agente de consola" Aún así, es necesario crear uno. "Aprenda a crear un agente de consola en Google Cloud"

Tenga en cuenta que si desea implementar Cloud Volumes ONTAP en una subred donde no hay acceso a Internet disponible, deberá instalar manualmente el agente de consola y acceder a la NetApp Console que se ejecuta en ese agente de consola. "Aprenda a instalar manualmente el agente de consola en una ubicación sin acceso a Internet"

2 Planifique su configuración

La consola ofrece paquetes preconfigurados que se adaptan a los requisitos de su carga de trabajo, o puede crear su propia configuración. Si elige su propia configuración, debe comprender las opciones disponibles.

"Obtenga más información sobre cómo planificar su configuración" .

3 Configura tu red

1. Asegúrese de que su VPC y sus subredes admitan la conectividad entre el agente de la consola y Cloud Volumes ONTAP.
2. Si planea habilitar la clasificación de datos, "Configurar la subred de Cloud Volumes ONTAP para el acceso privado de Google" .
3. Si está implementando un par de alta disponibilidad, asegúrese de tener cuatro VPC, cada una con su propia subred.
4. Si está utilizando una VPC compartida, proporcione el rol *Usuario de red de cómputo* a la cuenta de servicio del agente de consola.
5. Habilite el acceso a Internet saliente desde la VPC de destino para NetApp AutoSupport.

   Este paso no es necesario si está implementando Cloud Volumes ONTAP en una ubicación donde no hay acceso a Internet disponible.

"Obtenga más información sobre los requisitos de red" .

4 Configurar una cuenta de servicio

Cloud Volumes ONTAP requiere una cuenta de servicio de Google Cloud para dos propósitos. El primero es cuando habilitas"niveles de datos" para clasificar datos fríos en almacenamiento de objetos de bajo costo en Google Cloud. El segundo es cuando habilitas el "NetApp Backup and Recovery" para realizar copias de seguridad de volúmenes en un almacenamiento de objetos de bajo costo.

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

"Lea las instrucciones paso a paso" .

5 Habilitar las API de Google Cloud

"Habilite las siguientes API de Google Cloud en su proyecto" . Estas API son necesarias para implementar el agente de consola y Cloud Volumes ONTAP.

- API de Cloud Deployment Manager V2
- API de registro en la nube
- API del administrador de recursos en la nube
- API de Compute Engine
- API de gestión de identidad y acceso (IAM)

6 Inicie Cloud Volumes ONTAP mediante la consola

Haga clic en **Agregar sistema**, 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 agente de consola"
- "Instalación del software del agente de consola en un host Linux"
- "Permisos de Google Cloud para el agente de la consola"

Planifique su configuración de Cloud Volumes ONTAP en Google Cloud

Cuando implementa Cloud Volumes ONTAP en Google Cloud, puede elegir un sistema preconfigurado que coincida con sus requisitos de carga de trabajo o puede crear su propia configuración. Si elige su propia configuración, debe comprender las opciones disponibles.

Elija una licencia de Cloud Volumes ONTAP

Hay varias opciones de licencia disponibles para Cloud Volumes ONTAP. Cada opción te permite elegir un modelo de consumo que se adapte a tus necesidades.

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

Elija una región compatible

Cloud Volumes ONTAP es compatible con la mayoría de las regiones de Google Cloud. "Ver la lista completa de regiones compatibles" .

Elija un tipo de máquina compatible

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

"Configuraciones compatibles para Cloud Volumes ONTAP en Google Cloud"

Comprender los límites de almacenamiento

El límite de capacidad bruta para un sistema Cloud Volumes ONTAP está vinculado a la licencia. Límites adicionales impactan el tamaño de los agregados y volúmenes. Debe tener en cuenta estos límites al planificar su configuración.

"Límites de almacenamiento para Cloud Volumes ONTAP en Google Cloud"

Dimensiona tu sistema en Google Cloud

Dimensionar su sistema Cloud Volumes ONTAP puede ayudarle a cumplir con los requisitos de rendimiento y capacidad. Debe tener en cuenta algunos puntos clave al elegir un tipo de máquina, un tipo de disco y un tamaño de disco:

Tipo de máquina

Mire los tipos de máquinas compatibles en el "Notas de la versión de Cloud Volumes ONTAP" y luego revise los detalles de Google sobre cada tipo de máquina compatible. Adapte los requisitos de su carga de trabajo a la cantidad 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 detalles:

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

Tipos de disco

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

- *Discos persistentes SSD zonales*: Los discos persistentes SSD son mejores para cargas de trabajo que requieren altas tasas de IOPS aleatorias.
- *Discos persistentes zonales equilibrados*: estos SSD equilibran el rendimiento y el costo al proporcionar menores IOPS por GB.
- *Discos persistentes estándar zonales*: Los discos persistentes estándar son económicos y pueden manejar operaciones secuenciales de lectura/escritura.

  Para más detalles, consulte la "Documentación de Google Cloud: Discos persistentes zonales (estándar y SSD)" .

Tamaño del disco

Debe elegir un tamaño de disco inicial cuando implemente un sistema Cloud Volumes ONTAP . Después de eso, puede dejar que la NetApp Console administre la capacidad de un sistema por usted, pero si desea crear agregados usted mismo, tenga en cuenta lo siguiente:

- Todos los discos de un agregado deben tener el mismo tamaño.
- Determina el espacio que necesitas, teniendo en cuenta el rendimiento.
- El rendimiento de los discos persistentes se escala automáticamente con el tamaño del disco y la cantidad de vCPU disponibles para el sistema.

  Consulte lo siguiente para obtener más detalles:

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

Ver los discos del sistema predeterminados

Además del almacenamiento para los datos del usuario, la consola también compra almacenamiento en la nube para los datos del sistema Cloud Volumes ONTAP (datos de arranque, datos raíz, datos del núcleo y NVRAM). Para fines de planificación, puede ser útil revisar estos detalles antes de implementar Cloud Volumes ONTAP.

- "Ver los discos predeterminados para los datos del sistema Cloud Volumes ONTAP en Google Cloud" .
- "Documentación de Google Cloud: Descripción general de las cuotas de nube"

  Google Cloud Compute Engine aplica cuotas en el uso de recursos, por lo que debes asegurarte de no haber alcanzado el límite antes de implementar Cloud Volumes ONTAP.

El agente de consola también requiere un disco de sistema. "Ver detalles sobre la configuración predeterminada del agente de la consola" .

Recopilar información de redes

Cuando despliegues Cloud Volumes ONTAP en Google Cloud, necesitas especificar detalles sobre tu red virtual. Puedes usar una hoja de trabajo para recopilar la información de tu administrador.

Información de red para un sistema de un solo nodo

Información de Google Cloud	Tu valor
Región	
Zona	
Red VPC	
Subred	
Política de firewall (si utiliza la suya propia)	

Información de red para un par HA en múltiples zonas

Información de Google Cloud	Tu valor
Región	
Zona para el Nodo 1	
Zona para el Nodo 2	
Zona para el mediador	
VPC-0 y subred	
VPC-1 y subred	
VPC-2 y subred	

Información de Google Cloud	Tu valor
VPC-3 y subred	
Política de firewall (si utiliza la suya propia)	

Información de red para un par HA en una sola zona

Información de Google Cloud	Tu 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

La consola le permite elegir una configuración de velocidad de escritura para Cloud Volumes ONTAP, excepto para los pares de alta disponibilidad (HA) en Google Cloud. Antes de elegir una velocidad de escritura, debe comprender las diferencias entre las configuraciones normales y altas, así como los riesgos y recomendaciones al utilizar una velocidad de escritura alta. "Obtenga más información sobre la velocidad de escritura" .

Elija un perfil de uso de volumen

ONTAP incluye varias funciones de eficiencia de almacenamiento que pueden reducir la cantidad total de almacenamiento que necesita. Cuando crea un volumen en la consola, puede elegir un perfil que habilite estas funciones o un perfil que las deshabilite. Debe aprender más sobre estas características para ayudarlo a decidir qué perfil utilizar.

Las características de eficiencia de almacenamiento de NetApp brindan los siguientes beneficios:

Aprovisionamiento fino

Presenta más almacenamiento lógico a los hosts o usuarios del que realmente tiene en su grupo de almacenamiento físico. En lugar de preasignar espacio de almacenamiento, el espacio de almacenamiento se asigna dinámicamente a cada volumen a medida que se escriben los datos.

Desduplicación

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

Compresión

Reduce la capacidad física necesaria para almacenar datos al comprimirlos dentro de un volumen en el almacenamiento primario, secundario y de archivo.

Configurar la red de Google Cloud para Cloud Volumes ONTAP

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

Si desea implementar un par HA, debe"Descubra cómo funcionan los pares HA en Google Cloud" .

Requisitos para Cloud Volumes ONTAP

Se deben cumplir los siguientes requisitos en Google Cloud.

Requisitos específicos de los sistemas de nodo único

Si quieres implementar un sistema de un solo nodo, asegúrate de que tu red cumpla con los siguientes requisitos.

Una VPC

Se requiere una Virtual Private Cloud (VPC) para un sistema de un solo nodo.

Direcciones IP privadas

Para un sistema de nodo único en Google Cloud, la NetApp Console asigna direcciones IP privadas a lo siguiente:

- Node
- Grupo
- Máquina virtual de almacenamiento
- LIF de NAS de datos
- Datos iSCSI LIF

Puede omitir la creación del LIF de administración de la máquina virtual 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 a un puerto físico. Se requiere un LIF de administración de máquinas virtuales de almacenamiento (SVM) para herramientas de administración como SnapCenter.

Requisitos específicos para pares HA

Si desea implementar un par HA, asegúrese de que su red cumpla con los siguientes requisitos.

Una o varias zonas

Puede garantizar la alta disponibilidad de sus datos implementando una configuración de alta disponibilidad en varias zonas o en una sola. La consola le solicita que elija varias zonas o una sola zona cuando crea el par HA.

- Varias zonas (recomendado)

  La implementación de una configuración de alta disponibilidad en tres zonas garantiza la disponibilidad continua de los datos si ocurre una falla dentro de una zona. Tenga en cuenta que el rendimiento de escritura es ligeramente inferior en comparación con el uso de una sola zona, pero es mínimo.

- Zona única

  Cuando se implementa en una sola zona, una configuración de Cloud Volumes ONTAP HA utiliza una política de ubicación distribuida. Esta política garantiza que una configuración de HA esté protegida contra un único punto de falla dentro de la zona, sin tener que usar zonas separadas para lograr el aislamiento de fallas.

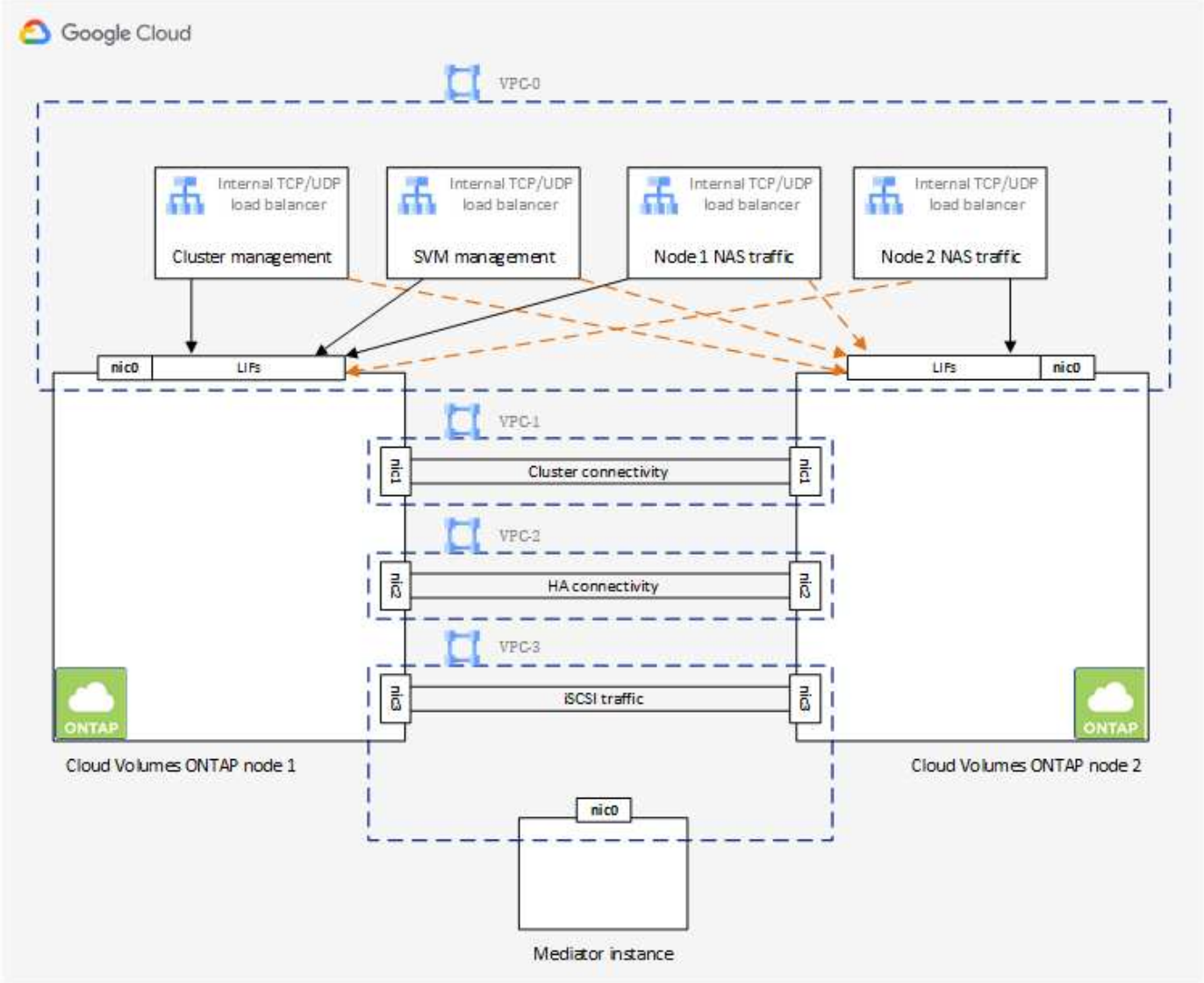
  Este modelo de implementación reduce sus costos porque no hay cargos por salida de datos entre zonas.

Cuatro nubes privadas virtuales

Se requieren cuatro nubes privadas virtuales (VPC) para una configuración de alta disponibilidad. Se requieren cuatro VPC porque Google Cloud requiere que cada interfaz de red resida en una red de VPC independiente.

La consola le solicita que elija cuatro VPC cuando crea el par HA:

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



Subredes

Se requiere una subred privada para cada VPC.

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

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

Direcciones IP privadas

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

El número de LIF asignados para Cloud Volumes ONTAP depende de si despliegas un sistema de nodo único o un par HA. Un LIF es una dirección IP asociada con un puerto físico. Se requiere un LIF de gestión de SVM para herramientas de gestión como SnapCenter.

- **Nodo único** NetApp Console asigna 4 direcciones IP a un sistema de nodo único:
  - LIF de gestión de nodos

- Gestión de clústeres LIF
- LIF de datos iSCSI

> Un LIF iSCSI proporciona acceso de cliente 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.

- NAS LIF

Puede omitir la creación del LIF de administración de la máquina virtual de almacenamiento (SVM) si implementa Cloud Volumes ONTAP mediante la API y especifica el siguiente indicador:

```
skipSvmManagementLif: true
```

- **Par HA** La consola asigna entre 12 y 13 direcciones IP a un par HA:
  - 2 LIF de gestión de nodos (e0a)
  - 1 LIF de gestión de clústeres (e0a)
  - 2 LIF iSCSI (e0a)

> Un LIF iSCSI proporciona acceso de cliente 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 HA (e0c)
  - 2 direcciones IP iSCSI RSM (e0d)

Puede omitir la creación del LIF de administración de la máquina virtual de almacenamiento (SVM) si implementa Cloud Volumes ONTAP mediante la API y especifica el siguiente indicador:

```
skipSvmManagementLif: true
```

Balanceadores de carga internos

La consola crea cuatro balanceadores de carga internos de Google Cloud (TCP/UDP) que administran el tráfico entrante al par Cloud Volumes ONTAP HA. No se requiere ninguna configuración por su parte. Hemos incluido esto como un requisito simplemente para informarle sobre el tráfico de la red y mitigar cualquier problema de seguridad.

Un balanceador de carga es para la administración del clúster, uno es para la administración de máquinas virtuales de almacenamiento (SVM), uno es para el tráfico NAS al nodo 1 y el último es para el tráfico NAS al nodo 2.

La configuración para cada balanceador de carga es la siguiente:

- Una dirección IP privada compartida
- Un chequeo de salud global

De forma predeterminada, los puertos utilizados por la comprobación de estado son 63001, 63002 y 63003.

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

  Aunque el acceso global está deshabilitado de forma predeterminada, se admite su habilitación después de la implementación. Lo desactivamos porque el tráfico entre regiones tendrá latencias significativamente más altas. Queríamos asegurarnos de que no tuvieras una experiencia negativa debido a montajes accidentales entre regiones. Habilitar esta opción depende de las necesidades específicas de su negocio.

VPC compartidas

Cloud Volumes ONTAP y el agente de consola son compatibles con una VPC compartida de Google Cloud y también con VPC independientes.

Para un sistema de nodo único, la VPC puede ser una VPC compartida o una VPC independiente.

Para un par HA, se requieren cuatro VPC. Cada una de esas VPC puede ser compartida o independiente. Por ejemplo, VPC-0 podría ser una VPC compartida, mientras que VPC-1, VPC-2 y VPC-3 podrían ser VPC independientes.

Una VPC compartida le permite configurar y administrar de forma centralizada redes virtuales en múltiples proyectos. Puede configurar redes VPC compartidas en el *proyecto de host* e implementar el agente de consola y las instancias de máquina virtual de Cloud Volumes ONTAP en un *proyecto de servicio*.

"Documentación de Google Cloud: Descripción general de VPC compartida" .

"Revise los permisos de VPC compartidos necesarios que se tratan en la implementación del agente de consola"

Duplicación de paquetes en VPC

"Duplicación de paquetes"debe estar deshabilitado en la subred de Google Cloud en la que implementa Cloud Volumes ONTAP.

Acceso a Internet de salida

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

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

Puntos finales de Cloud Volumes ONTAP

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

Puntos finales	Aplicable para	Objetivo	Modo de implementación	Impacto si el punto final no está disponible
\ https://netapp-cloud-account.auth0.com	Autenticación	Se utiliza para la autenticación en la consola.	Modos estándar y restringido.	La autenticación del usuario falla y los siguientes servicios permanecen no disponibles: • Servicios de Cloud Volumes ONTAP • Servicios de ONTAP • Protocolos y servicios proxy
\ https://api.bluexp.netapp.com/tenancy	Tenencia	Se utiliza para recuperar recursos de Cloud Volumes ONTAP desde la consola para autorizar recursos y usuarios.	Modos estándar y restringido.	Los recursos de Cloud Volumes ONTAP y los usuarios no están autorizados.
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Se utiliza para enviar datos de telemetría de AutoSupport al soporte de NetApp .	Modos estándar y restringido.	La información de AutoSupport sigue sin entregarse.

Puntos finales	Aplicable para	Objetivo	Modo de implementación	Impacto si el punto final no está disponible
https://cloudbuild.googleapis.com/v1 (solo para despliegues en modo privado) https://cloudkms.googleapis.com/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://compute.googleapis.com/compute/v1 https://www.googleapis.com/compute/beta https://www.googleapis.com/compute/v1/projects/ https://www.googleapis.com/deploymentmanager/v2/projects https://www.googleapis.com/storage/v1 https://www.googleapis.com/upload/storage/v1 https://config.googleapis.com/v1 https://iam.googleapis.com/v1 https://storage.googleapis.com/storage/v1	Google Cloud (uso comercial).	Comunicación con los servicios de Google Cloud.	Modos estándar, restringido y privado.	Cloud Volumes ONTAP no puede comunicarse con el servicio Google Cloud para realizar operaciones específicas para la consola en Google Cloud.

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 la VPC y la otra red (por ejemplo, su red corporativa).

"Documentación de Google Cloud: Descripción general de Cloud VPN" .

Reglas del firewall

La consola crea reglas de firewall de Google Cloud que incluyen las reglas de entrada y salida que Cloud Volumes ONTAP necesita para funcionar correctamente. Es posible que desees consultar los puertos para fines de prueba o si prefieres utilizar tus propias reglas de firewall.

Las reglas de firewall para Cloud Volumes ONTAP requieren reglas tanto entrantes como salientes. Si está implementando una configuración de alta disponibilidad, estas son las reglas de firewall para Cloud Volumes

ONTAP en VPC-0.

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

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

¿Buscas información sobre el agente de consola? "Ver las reglas de firewall para el agente de la consola"

Reglas de entrada

Cuando agrega un sistema Cloud Volumes ONTAP , puede elegir el filtro de origen para la política de firewall predefinida durante la implementación:

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

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

Protocolo	Puerto	Objetivo
Todos los ICMP	Todo	Haciendo ping a la instancia
HTTP	80	Acceso HTTP a la consola web de ONTAP System Manager mediante la dirección IP del LIF de administración del clúster
HTTPS	443	Conectividad con el agente de la consola y acceso HTTPS a la consola web de ONTAP System Manager mediante la dirección IP del LIF de administración del clúster
SSH	22	Acceso SSH a la dirección IP del LIF de administración del clúster o de un LIF de administración de nodos
TCP	111	Llamada a procedimiento remoto para NFS
TCP	139	Sesión de servicio NetBIOS para CIFS
TCP	161-162	Protocolo simple de gestión de red
TCP	445	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
TCP	635	Montaje NFS
TCP	749	Kerberos
TCP	2049	Demonio del servidor NFS

Protocolo	Puerto	Objetivo
TCP	3260	Acceso iSCSI a través del LIF de datos iSCSI
TCP	4045	Demonio de bloqueo NFS
TCP	4046	Monitor de estado de red para NFS
TCP	10000	Copia de seguridad mediante NDMP
TCP	11104	Gestión de sesiones de comunicación entre clústeres para SnapMirror
TCP	11105	Transferencia de datos de SnapMirror mediante LIF entre clústeres
TCP	63001-63050	Puertos de sonda de equilibrio de carga para determinar qué nodo está en buen estado (requerido 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	Demonio del servidor NFS
UDP	4045	Demonio de bloqueo NFS
UDP	4046	Monitor de estado de red para NFS
UDP	4049	Protocolo rquotad de NFS

Reglas de salida

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

Reglas básicas de salida

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

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

Reglas de salida avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede usar la siguiente información para abrir solo aquellos puertos que Cloud Volumes ONTAP requiere para la comunicación saliente. Los clústeres de Cloud Volumes ONTAP utilizan los siguientes puertos para regular el tráfico de los nodos.

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

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

Servicio	Protocolo	Puerto	Fuente	Destino	Objetivo
AutoSupport	HTTPS	443	LIF de gestión de nodos	mysupport.netapp.com	AutoSupport (HTTPS es el predeterminado)
	HTTP	80	LIF de gestión de nodos	mysupport.netapp.com	AutoSupport (solo si el protocolo de transporte se cambia de HTTPS a HTTP)
	TCP	3128	LIF de gestión de nodos	Agente de consola	Envío de mensajes de AutoSupport a través de un servidor proxy en el agente de la consola, si no hay una conexión a Internet saliente disponible
Copias de seguridad de configuración	HTTP	80	LIF de gestión de nodos	http://<dirección IP del agente de consola>/occm/offboxconfig	Envía copias de seguridad de la configuración al agente de la consola."Documentación de ONTAP"
DHCP	UDP	68	LIF de gestión de nodos	DHCP	Cliente DHCP para la primera configuración
DHCP	UDP	67	LIF de gestión de nodos	DHCP	Servidor DHCP
DNS	UDP	53	LIF de gestión de nodos y LIF de datos (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	LIF de gestión de nodos	Servidores de destino	Copia NDMP
SMTP	TCP	25	LIF de gestión de nodos	Servidor de correo	Alertas SMTP, se pueden utilizar para AutoSupport
SNMP	TCP	161	LIF de gestión de nodos	Servidor de monitorización	Monitoreo mediante trampas SNMP
	UDP	161	LIF de gestión de nodos	Servidor de monitorización	Monitoreo mediante trampas SNMP
	TCP	162	LIF de gestión de nodos	Servidor de monitorización	Monitoreo mediante trampas SNMP
	UDP	162	LIF de gestión de nodos	Servidor de monitorización	Monitoreo mediante trampas SNMP
SnapMirror	TCP	11104	LIF entre clústeres	LIF entre clústeres de ONTAP	Gestión de sesiones de comunicación entre clústeres para SnapMirror
	TCP	11105	LIF entre clústeres	LIF entre clústeres de ONTAP	Transferencia de datos de SnapMirror

Servicio	Protocolo	Puerto	Fuente	Destino	Objetivo
Registro del sistema	UDP	514	LIF de gestión de nodos	Servidor de syslog	Mensajes de reenvío de syslog

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

En Google Cloud, una configuración de alta disponibilidad se implementa en cuatro VPC. Las reglas de firewall necesarias para la configuración de HA en VPC-0 sonenumerados anteriormente para Cloud Volumes ONTAP .

Mientras tanto, las reglas de firewall predefinidas creadas para las instancias en VPC-1, VPC-2 y VPC-3 permiten la comunicación de ingreso a través de *todos* los protocolos y puertos. Estas reglas permiten la comunicación entre nodos HA.

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

> Para permitir una alta velocidad de escritura para las nuevas implementaciones de pares de Google Cloud HA, se requiere una unidad de transmisión máxima (MTU) de al menos 8896 bytes para VPC-1, VPC-2 y VPC-3. Si elige actualizar VPC-1, VPC-2 y VPC-3 existentes a una MTU de 8896 bytes, debe apagar todos los sistemas HA existentes que utilicen estas VPC durante el proceso de configuración.

Requisitos para el agente de consola

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

- "Ver los requisitos de red para el agente de consola"
- "Reglas de firewall en Google Cloud"

Configuraciones de red para soportar el proxy del agente de consola

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

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

Para obtener información sobre cómo configurar servidores proxy para el agente de consola, consulte la "Configurar un agente de consola para utilizar un servidor proxy" .

Configurar etiquetas de red para Cloud Volumes ONTAP en Google Cloud

Durante la configuración del proxy transparente del agente de la consola, el administrador agrega una etiqueta de red para Google Cloud. Debe obtener y agregar manualmente la misma etiqueta de red para su configuración de Cloud Volumes ONTAP . Esta etiqueta es necesaria para que el servidor proxy funcione correctamente.

1. En Google Cloud Console, localiza tu sistema Cloud Volumes ONTAP.
2. Vaya a **Detalles > Redes > Etiquetas de red**.
3. Agregue la etiqueta utilizada para el agente de consola y guarde la configuración.

Temas relacionados

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

Configurar controles de servicio de VPC para implementar Cloud Volumes ONTAP en Google Cloud

Al elegir bloquear su entorno de Google Cloud con controles de servicio de VPC, debe comprender cómo interactúan NetApp Console y Cloud Volumes ONTAP con las API de Google Cloud, así como también cómo configurar su perímetro de servicio para implementar Console y Cloud Volumes ONTAP.

Los controles de servicio de VPC le permiten controlar el acceso a los servicios administrados por Google fuera de un perímetro confiable, bloquear el acceso a datos desde ubicaciones no confiables y mitigar los riesgos de transferencia de datos no autorizada. "Obtenga más información sobre los controles de servicio de Google Cloud VPC" .

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

La consola 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 agente de la consola.

Según el estilo de implementación del agente de consola, es posible que se deban realizar ciertas excepciones para el perímetro de su servicio.

Imágenes

Tanto Cloud Volumes ONTAP como la Console utilizan imágenes de un proyecto dentro de Google Cloud que está gestionado por NetApp. Esto puede afectar el despliegue del agente de la Console y de Cloud Volumes ONTAP, si tu organización tiene una política que bloquea el uso de imágenes que no están alojadas dentro de la organización.

Puede implementar un agente de consola manualmente mediante el método de instalación manual, pero Cloud Volumes ONTAP también necesitará extraer imágenes del proyecto de NetApp . Debe proporcionar una lista permitida para implementar un agente de consola y Cloud Volumes ONTAP.

Implementación de un agente de consola

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

Implementación de Cloud Volumes ONTAP

- La cuenta de servicio de la consola debe hacer referencia a una imagen alojada en el proyecto *netapp-cloudmanager* y al número de proyecto *14190056516* del proyecto de servicio.
- La cuenta de servicio del agente de servicio de las API de Google predeterminado debe hacer referencia a una imagen alojada en el proyecto Id. *netapp-cloudmanager* y al 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 de VPC.

Políticas perimetrales de controles de servicio de VPC

Las políticas permiten excepciones a los conjuntos de reglas de VPC Service Controls. Para obtener más información sobre las políticas, por favor visita "Documentación de la política de Service Controls de Google Cloud VPC".

Para configurar las políticas que requiere la consola, navegue al perímetro de controles de servicio de VPC dentro de su organización y agregue las siguientes políticas. Los campos deben coincidir con las opciones proporcionadas en la página de políticas de Controles de servicio de VPC. Tenga en cuenta también que **todas** las reglas son obligatorias y que los parámetros **OR** deben utilizarse en el conjunto de reglas.

Reglas de ingreso

```
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* utilizado por NetApp para almacenar imágenes para el agente de consola y para Cloud Volumes ONTAP.

Cree una cuenta de servicio de Google Cloud para Cloud Volumes ONTAP

Cloud Volumes ONTAP requiere una cuenta de servicio de Google Cloud para dos

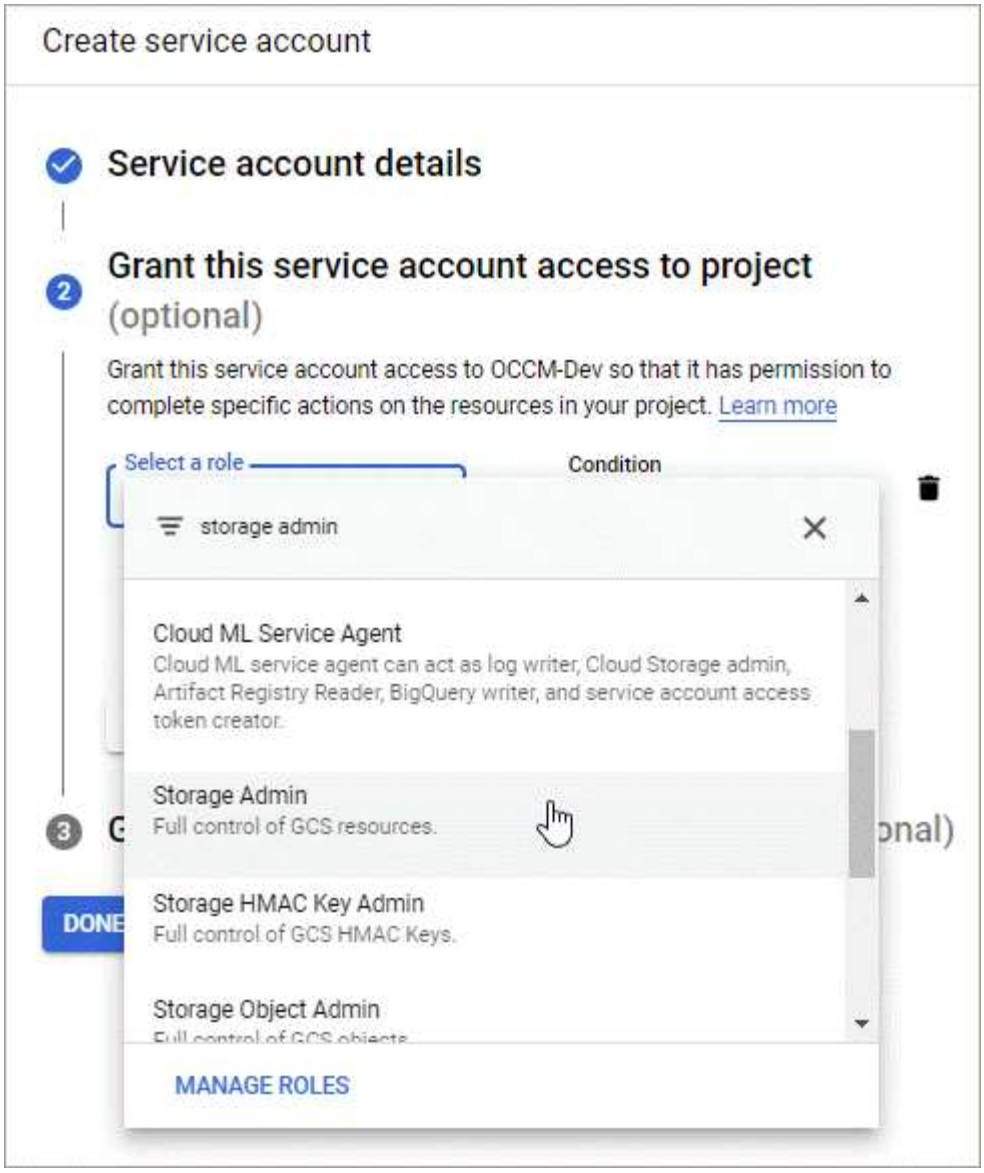
propósitos. El primero es cuando habilitas"niveles de datos" para clasificar datos fríos en almacenamiento de objetos de bajo costo en Google Cloud. El segundo es cuando habilitas el "NetApp Backup and Recovery" para realizar copias de seguridad de volúmenes en un almacenamiento de objetos de bajo costo.

Cloud Volumes ONTAP utiliza la cuenta de servicio para acceder y administrar un depósito para datos escalonados y otro depósito para copias de seguridad.

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

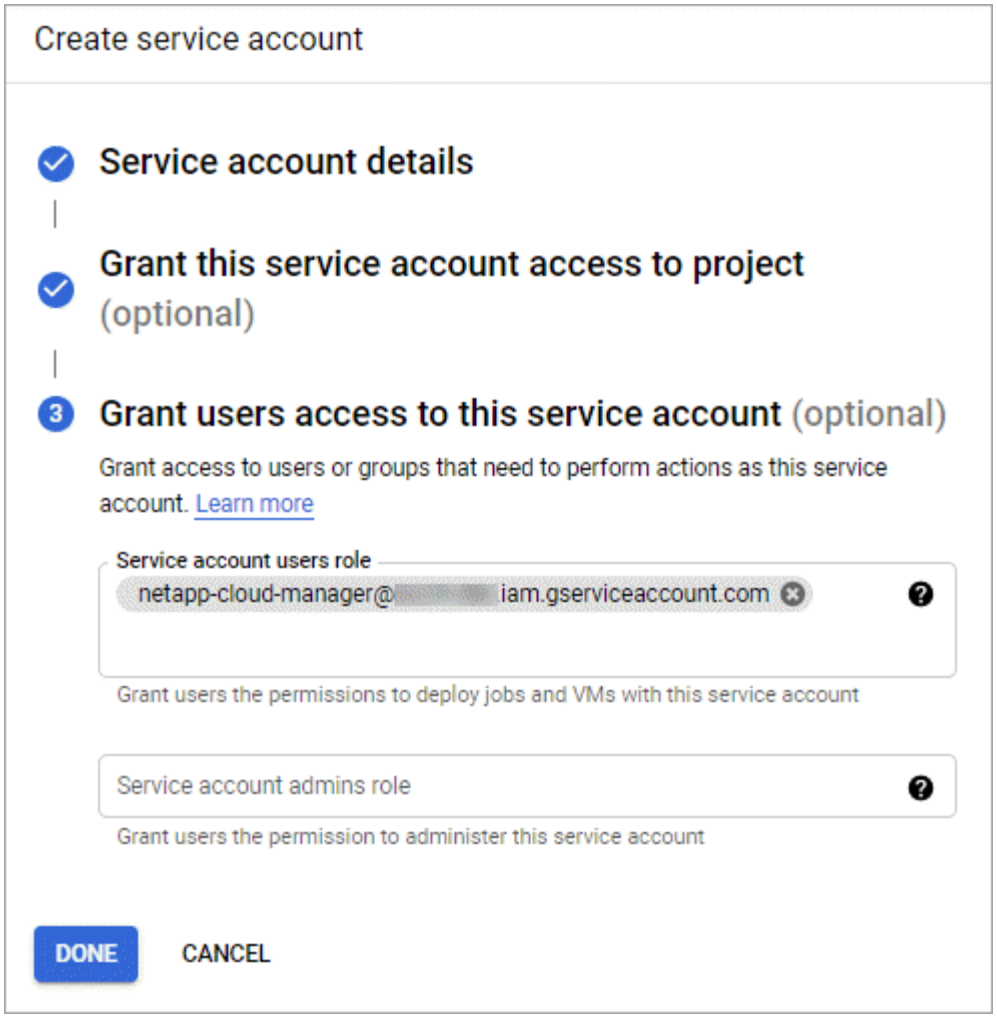
Pasos

1. En la Google Cloud Console, "Vaya a la página de Cuentas de servicio".
2. Seleccione su proyecto
3. Haga clic en **Crear cuenta de servicio** y proporcione la información requerida.
    a. **Detalles de la cuenta de servicio**: Ingrese un nombre y una descripción.
    b. **Otorgar a esta cuenta de servicio acceso al proyecto**: seleccione el rol de **Administrador de almacenamiento**.



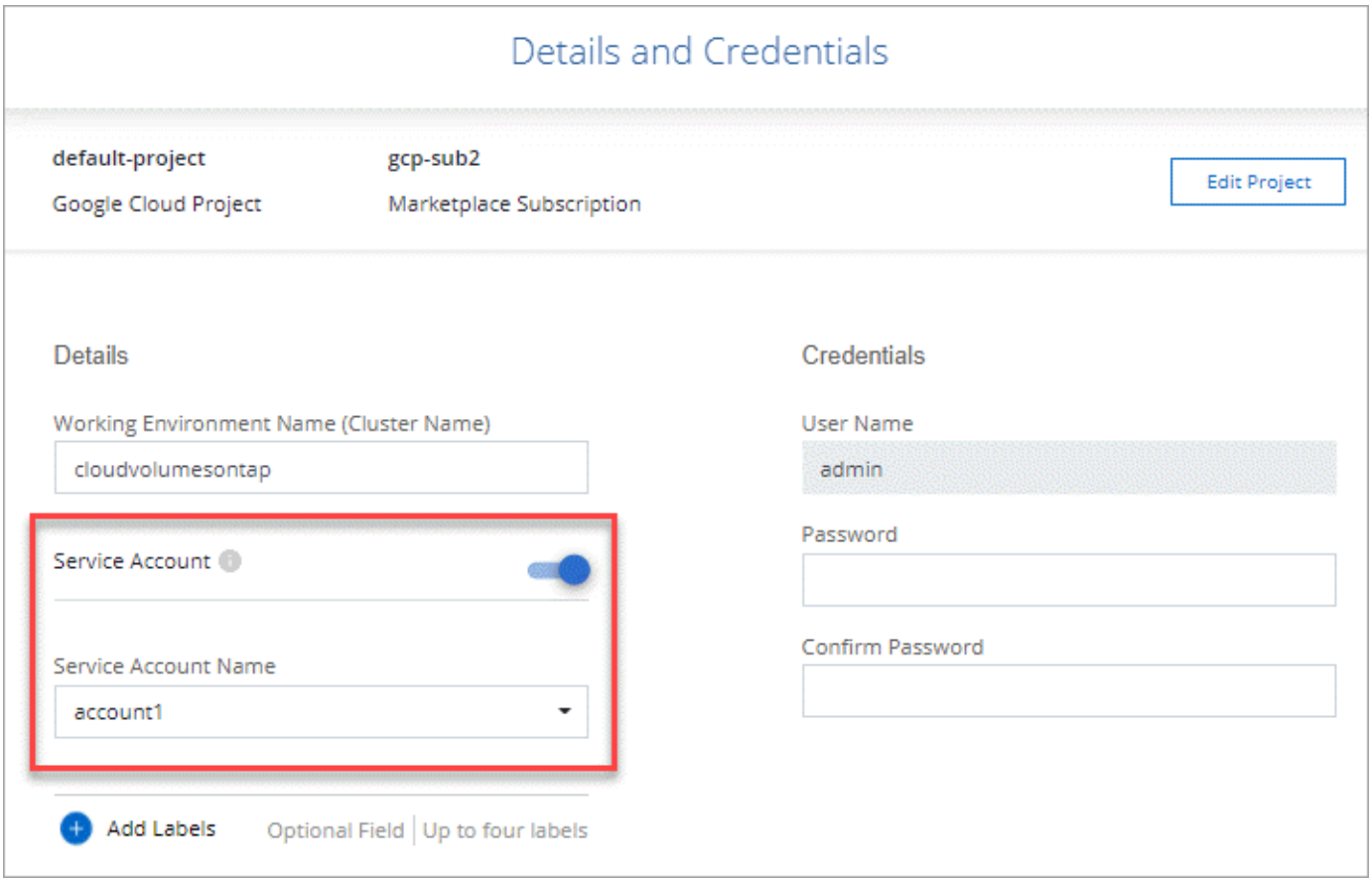
c. **Otorgar a los usuarios acceso a esta cuenta de servicio**: agregue la cuenta de servicio del agente de consola como un *Usuario de cuenta de servicio* a esta nueva cuenta de servicio.

   Este paso es necesario únicamente para la clasificación de datos. No es necesario para realizar copias de seguridad y recuperación.



¿Que sigue?

Deberá seleccionar la cuenta de servicio más adelante cuando cree un sistema Cloud Volumes ONTAP .



Uso de claves de cifrado administradas por el cliente con Cloud Volumes ONTAP

Si bien Google Cloud Storage siempre cifra sus datos antes de escribirlos en el disco, puede usar las API para crear un sistema Cloud Volumes ONTAP que utilice *claves de cifrado administradas por el cliente*. Se trata de claves que usted genera y administra en GCP mediante el Servicio de administración de claves en la nube.

Pasos

1. Asegúrese de que la cuenta de servicio del agente de consola tenga los permisos correctos en el nivel del proyecto, en el proyecto donde está almacenada la clave.

   Los permisos se proporcionan en el "Los permisos de la cuenta de servicio por defecto" , pero es posible que no se aplique 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 para el "Agente de servicio de Google Compute Engine" Tiene permisos de 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 la `/gcp/vsa/metadata/gcp-encryption-keys` Llamada API o eligiendo "Copiar nombre de recurso" en la clave en la consola de GCP.
4. Si se utilizan claves de cifrado administradas por el cliente y se organizan los datos en niveles para el almacenamiento de objetos, la NetApp Console intenta utilizar las mismas claves que se usan para cifrar los discos persistentes. Pero primero deberás habilitar los depósitos de Google Cloud Storage para usar las claves:

   a. Encuentre el agente del servicio Google Cloud Storage siguiendo las instrucciones "Documentación de Google Cloud: Cómo obtener el agente del servicio Cloud Storage" .

   b. Navegue hasta la clave de cifrado y asigne al agente del servicio Google Cloud Storage permisos de cifrado/descifrado de Cloud KMS.

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

5. Usa el parámetro "gcpEncryption" con tu solicitud de API al crear un sistema.

   Ejemplo

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

Consulte la "Documentación de automatización de la NetApp Console" para obtener más detalles sobre el uso del parámetro "GcpEncryption".

Configurar licencias para Cloud Volumes ONTAP en Google Cloud

Después de decidir qué opción de licencia desea utilizar con Cloud Volumes ONTAP, se requieren algunos pasos antes de poder elegir esa opción de licencia al crear un nuevo sistema.

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 Freemium" .

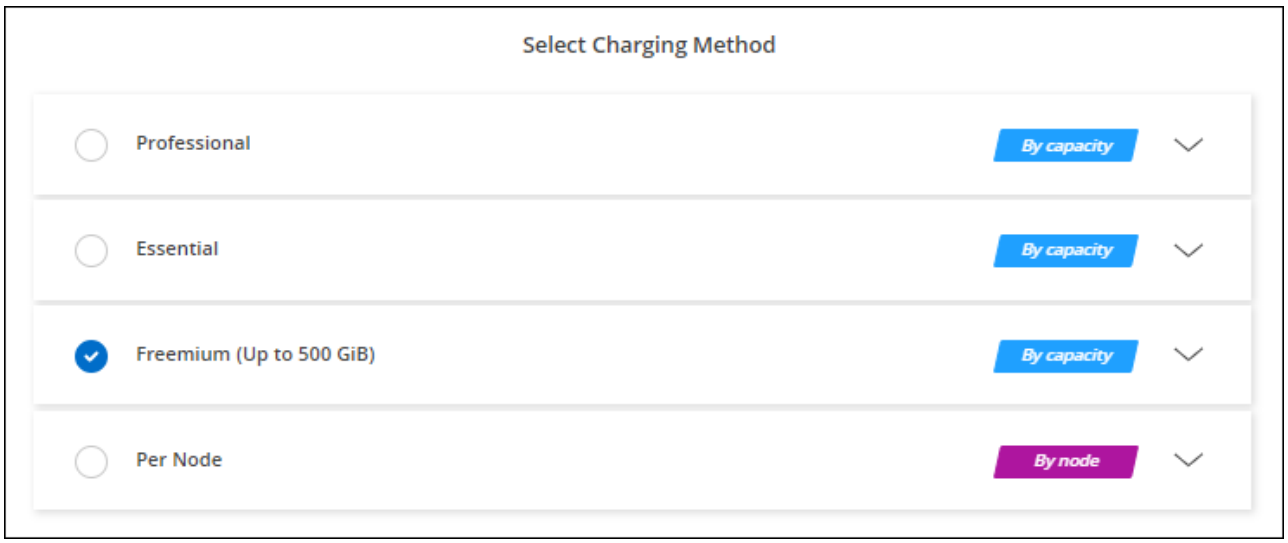
Pasos

1. Desde el menú de navegación de la izquierda, seleccione **Almacenamiento > Administración**.
2. En la página **Sistemas**, haga clic en **Agregar sistema** y siga los pasos en la NetApp Console.
   a. En la página **Detalles y credenciales**, haga clic en **Editar credenciales > Agregar suscripción** y luego siga las instrucciones para suscribirse a la oferta de pago por uso en Google Cloud Marketplace.

      No se le cobrará a través de la suscripción del mercado a menos que exceda los 500 GiB de

capacidad aprovisionada, momento en el cual el sistema se convierte automáticamente al"Paquete esencial" .

b. Después de regresar a la consola, seleccione **Freemium** cuando llegue a la página de métodos de cobro.



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

Licencia basada en capacidad

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

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

- Una licencia (traiga su propia licencia (BYOL)) comprada a NetApp
- Una suscripción por hora, de pago por uso (PAYGO) de Google Cloud Marketplace
- Un contrato anual

"Obtenga más información sobre las licencias basadas en capacidad" .

Las siguientes secciones describen cómo comenzar a utilizar cada uno de estos modelos de consumo.

Trae tu propia bebida

Pague por adelantado comprando una licencia (BYOL) de NetApp para implementar sistemas Cloud Volumes ONTAP en cualquier proveedor de nube.

NetApp ha restringido la compra, extensión y renovación de licencias BYOL. Para más información, consulte "Disponibilidad restringida de licencias BYOL para Cloud Volumes ONTAP" .

Pasos

1. "Comuníquese con el departamento de ventas de NetApp para obtener una licencia"
2. "Agregue su cuenta del sitio de soporte de NetApp a la NetApp Console"

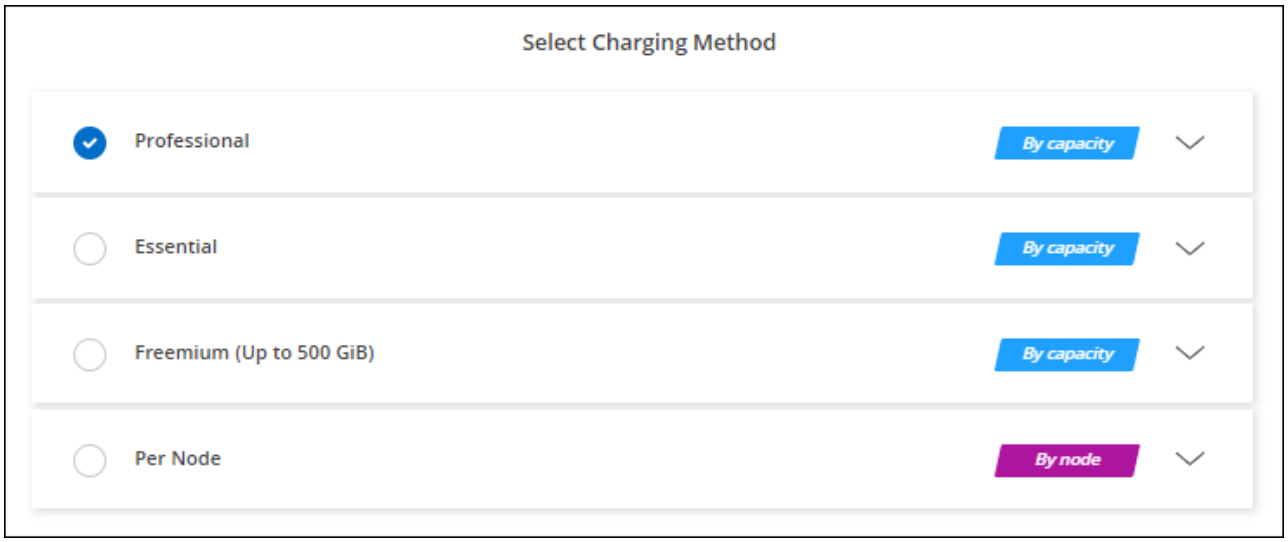
La consola consulta automáticamente el servicio de licencias de NetApp para obtener detalles sobre las licencias asociadas a su cuenta del sitio de soporte de NetApp . Si no hay errores, la Consola agrega las licencias.

Su licencia debe estar disponible en la consola antes de poder usarla con Cloud Volumes ONTAP. Si es necesario, puedes"agregar manualmente la licencia a la consola" .

3. En la página **Sistemas**, haga clic en **Agregar sistema** y siga los pasos.
   a. En la página **Detalles y credenciales**, haga clic en **Editar credenciales > Agregar suscripción** y luego siga las instrucciones para suscribirse a la oferta de pago por uso en Google Cloud Marketplace.

      La licencia que usted compró de NetApp siempre se cobra primero, pero se le cobrará la tarifa por hora del mercado si excede su capacidad de licencia o si vence el plazo de su licencia.

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



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

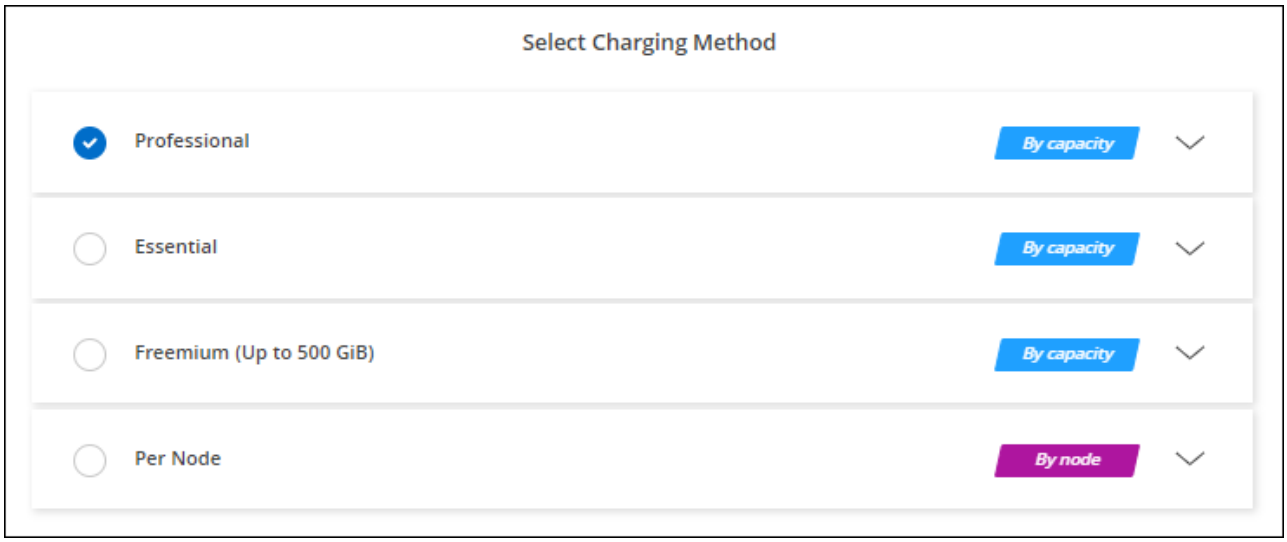
Suscripción PAYGO

Pague por hora suscribiéndose a la oferta del mercado de su proveedor de nube.

Cuando crea un sistema Cloud Volumes ONTAP , la consola le solicita que se suscriba al acuerdo que está disponible en Google Cloud Marketplace. Esa suscripción se asocia luego al sistema para su cobro. Puede utilizar esa misma suscripción para sistemas adicionales.

Pasos

1. Desde el menú de navegación de la izquierda, seleccione **Almacenamiento > Administración**.
2. En la página **Sistemas**, haga clic en **Agregar sistema** y siga los pasos.
   a. En la página **Detalles y credenciales**, haga clic en **Editar credenciales > Agregar suscripción** y luego siga las instrucciones para suscribirse a la oferta de pago por uso en Google Cloud Marketplace.
   b. Después de regresar a la consola, seleccione un paquete basado en capacidad cuando llegue a la página de métodos de carga.



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

Puede administrar las suscripciones de Google Cloud Marketplace asociadas a sus cuentas desde la página Configuración > Credenciales. "Aprenda a administrar sus credenciales y suscripciones de Google Cloud"

Contrato anual

Pague Cloud Volumes ONTAP anualmente comprando un contrato anual.

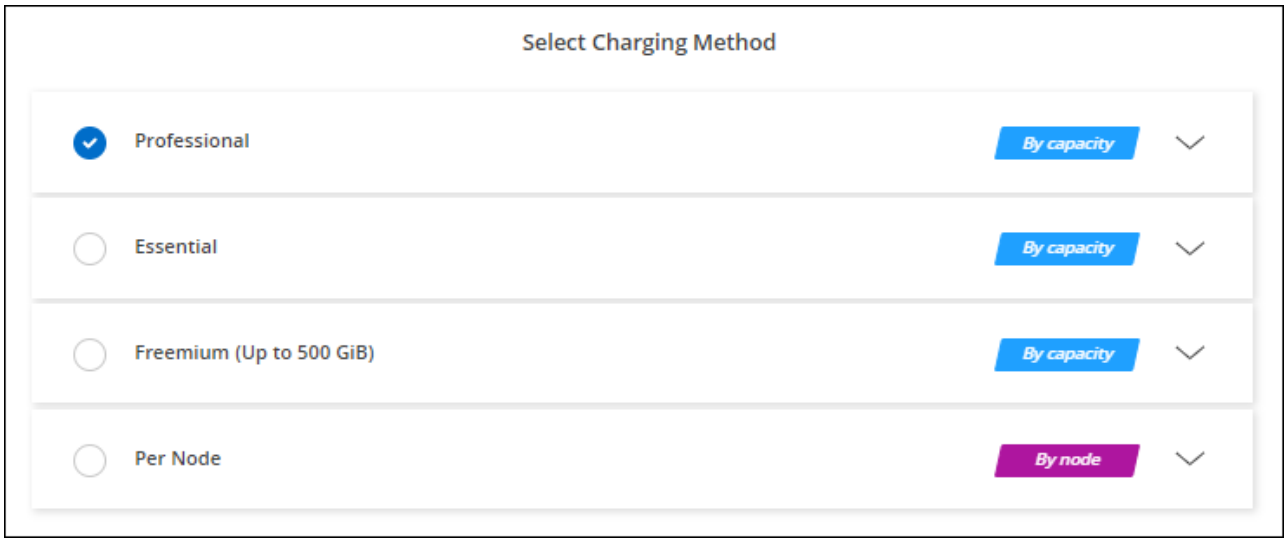
Pasos

1. Comuníquese con su representante de ventas de NetApp para comprar un contrato anual.

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

   Después de que NetApp comparta contigo la oferta privada, podrás seleccionar el plan anual cuando te suscribas desde Google Cloud Marketplace durante la creación del sistema.

2. En la página **Sistemas**, haga clic en **Agregar sistema** y siga los pasos.
   a. En la página **Detalles y credenciales**, haga clic en **Editar credenciales > Agregar suscripción** y luego siga las instrucciones para suscribirse al plan anual en Google Cloud Marketplace.
   b. En Google Cloud, seleccione el plan anual que se compartió con su cuenta y luego haga clic en **Suscribirse**.
   c. Después de regresar a la consola, seleccione un paquete basado en capacidad cuando llegue a la página de métodos de carga.



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

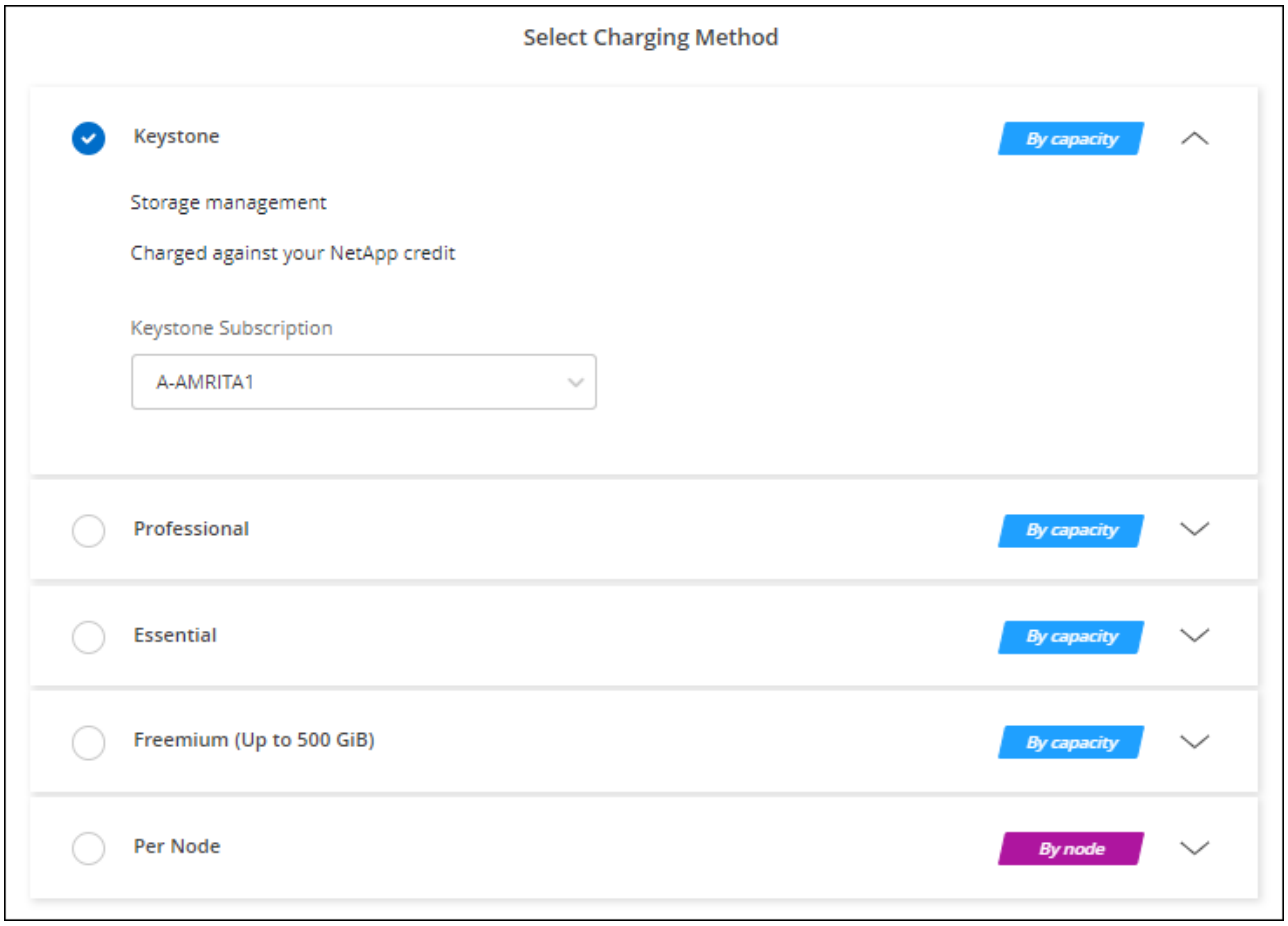
Suscripción a Keystone

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

Pasos

1. Si aún no tienes una suscripción, "Contactar con NetApp"
2. Contacto NetApp para autorizar su cuenta de usuario de la consola con una o más suscripciones de Keystone .
3. Después de que NetApp autorice su cuenta,"Vincula tus suscripciones para usarlas con Cloud Volumes ONTAP" .
4. En la página **Sistemas**, haga clic en **Agregar sistema** y siga los pasos.

    a. Seleccione el método de cobro de suscripción de Keystone cuando se le solicite que elija un método de cobro.



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

Licencia basada en nodos

Una licencia basada en nodos es la licencia de la generación anterior para Cloud Volumes ONTAP. Esta licencia se puede adquirir a través de NetApp (BYOL) y está disponible para renovaciones de licencias, solo en casos específicos. Para obtener información, consulte:

- "Fin de la disponibilidad de las licencias basadas en nodos"
- "Fin de la disponibilidad de las licencias basadas en nodos"
- "Convertir una licencia basada en nodos a una licencia basada en capacidad"

Lanzamiento de Cloud Volumes ONTAP en Google Cloud

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

Antes de empezar

Necesitará lo siguiente antes de comenzar.

- Un agente de NetApp Console que está en funcionamiento.
  - Deberías tener una "Agente de consola asociado con su sistema" .
  - "Debes estar preparado para dejar el agente de consola ejecutándose en todo momento" .

- La cuenta de servicio asociada con el agente de consola "debe tener los permisos requeridos"

- Una comprensión de la configuración que desea utilizar.

  Deberías haberte preparado eligiendo una configuración y obteniendo información de red de Google Cloud de tu administrador. Para más detalles, consulte"Planificación de la configuración de Cloud Volumes ONTAP" .

- Una comprensión de lo que se requiere para configurar la licencia para Cloud Volumes ONTAP.

  "Aprenda a configurar las licencias" .

- Las API de Google Cloud deberían ser "habilitado en su proyecto" :
  - API de Cloud Deployment Manager V2
  - API de registro en la nube
  - API del administrador de recursos en la nube
  - API de Compute Engine
  - API de gestión de identidad y acceso (IAM)

Lanzar un sistema de un solo nodo en Google Cloud

Cree un sistema en la NetApp Console para iniciar Cloud Volumes ONTAP en Google Cloud.

Pasos

1. Desde el menú de navegación de la izquierda, seleccione **Almacenamiento > Administración**.
2. En la página **Sistemas**, haga clic en **Agregar sistema** y siga las instrucciones.
3. **Elija una ubicación**: seleccione **Google Cloud** y * Cloud Volumes ONTAP*.
4. Si se le solicita, "crear un agente de consola" .
5. **Detalles y credenciales**: seleccione un proyecto, especifique un nombre de clúster, seleccione opcionalmente una cuenta de servicio, agregue etiquetas opcionalmente y luego especifique las credenciales.

   La siguiente tabla describe los campos para los que podría necesitar orientación:

Campo	Descripción
Nombre del sistema	La consola usa el nombre del sistema para nombrar tanto el sistema Cloud Volumes ONTAP como la instancia de Google Cloud VM. También utiliza el nombre como prefijo para el grupo de seguridad predefinido, si selecciona esa opción.
Nombre de la cuenta de servicio	Si planea utilizar"niveles de datos" o "NetApp Backup and Recovery" con Cloud Volumes ONTAP, debe habilitar **Cuenta de servicio** y seleccionar una cuenta de servicio que tenga el rol de administrador de almacenamiento predefinido. "Aprenda a crear una cuenta de servicio" .

Campo	Descripción
Agregar etiquetas	Las etiquetas son metadatos para sus recursos de Google Cloud. La consola agrega las etiquetas al sistema Cloud Volumes ONTAP y a los recursos de Google Cloud asociados con el sistema. Puede agregar hasta cuatro etiquetas desde la interfaz de usuario al crear un sistema y luego puede agregar más una vez creado. Tenga en cuenta que la API no lo limita a cuatro etiquetas al crear un sistema. Para obtener información sobre las etiquetas, consulte la "Documentación de Google Cloud: Recursos de etiquetado" .
Nombre de usuario y contraseña	Estas son las credenciales para la cuenta de administrador del clúster de Cloud Volumes ONTAP . Puede usar estas credenciales para conectarse a Cloud Volumes ONTAP a través de ONTAP System Manager o la CLI de ONTAP . Mantenga el nombre de usuario predeterminado *admin* o cámbielo por un nombre de usuario personalizado.
Editar proyecto	Seleccione el proyecto donde desea que resida Cloud Volumes ONTAP . El proyecto predeterminado es el proyecto donde se encuentra la Consola. Si no ves ningún proyecto adicional en la lista desplegable, entonces aún no has asociado la cuenta de servicio con otros proyectos. Ve a Google Cloud Console, abre el servicio IAM y selecciona el proyecto. Agrega la cuenta de servicio con el rol que usas para la Console a ese proyecto. Tendrás que repetir este paso para cada proyecto. Esta es la cuenta de servicio que configuraste para la consola."como se describe en esta página" . Haga clic en **Agregar suscripción** para asociar las credenciales seleccionadas con una suscripción. Para crear un sistema Cloud Volumes ONTAP de pago por uso, debe seleccionar un proyecto de Google Cloud que esté asociado con una suscripción a Cloud Volumes ONTAP desde el mercado de Google Cloud. Referirse a "Cómo asociar una suscripción de Marketplace con las credenciales de Google Cloud" .

6. **Servicios**: Seleccione los servicios que desea utilizar en este sistema. Para seleccionar Copia de seguridad y recuperación, o para utilizar NetApp Cloud Tiering, debe haber especificado la cuenta de servicio en el paso 3.

   Si desea utilizar WORM y niveles de datos, debe deshabilitar la función de copia de seguridad y recuperación e implementar un sistema Cloud Volumes ONTAP con la versión 9.8 o superior.

7. **Ubicación y conectividad**: selecciona la región y la zona de Google Cloud para tu sistema, elige una política de cortafuegos y confirma la conectividad de red con Google Cloud storage para la organización de datos por niveles.

   La siguiente tabla describe los campos para los que podría necesitar orientación:

Campo	Descripción
Verificación de conectividad	Para agrupar datos fríos en un depósito de Google Cloud Storage, la subred en la que reside Cloud Volumes ONTAP debe estar configurada para el acceso privado de Google. Para obtener instrucciones, consulte "Documentación de Google Cloud: Configuración del acceso privado a Google" .
Política de firewall generada	Si deja que la consola genere la política de firewall por usted, deberá elegir cómo permitirá el tráfico: • Si elige **Solo VPC seleccionada**, el filtro de origen para el tráfico entrante es el rango de subred de la VPC seleccionada y el rango de subred de la VPC donde reside el agente de la consola. Esta es la opción recomendada. • Si elige **Todas las VPC**, el filtro de origen para el tráfico entrante es el rango de IP 0.0.0.0/0.
Utilizar la política de firewall existente	Si utiliza una política de firewall existente, asegúrese de que incluya las reglas necesarias:"Obtenga información sobre las reglas de firewall para Cloud Volumes ONTAP"

8. **Métodos de cobro y cuenta NSS**: especifique qué opción de cobro desea utilizar con este sistema y luego especifique una cuenta del sitio de soporte de NetApp :
   - "Obtenga más 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 elige uno de los paquetes, solo necesita especificar un volumen y luego 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 candidata a lanzamiento, una versión de disponibilidad general o una versión de parche más reciente para una versión seleccionada, la consola actualiza el sistema a esa versión al crearla. Por ejemplo, la actualización se produce si selecciona Cloud Volumes ONTAP 9.13.1 y 9.13.1 P4 está disponible. La actualización no se produce de una versión a otra, por ejemplo, de 9.13 a 9.14.
11. **Recursos de almacenamiento subyacentes**: elija configuraciones para el agregado inicial: un tipo de disco y el tamaño de cada disco.

    El tipo de disco es para el volumen inicial. Puede elegir un tipo de disco diferente para los volúmenes posteriores.

    El tamaño del disco es para todos los discos en el agregado inicial y para cualquier agregado adicional que la Consola crea cuando 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 para elegir un tipo y tamaño de disco, consulte"Dimensiona tu sistema en Google Cloud" .

12. **Caché Flash, Velocidad de Escritura y WORM**:

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

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

    b. Elija velocidad de escritura **Normal** o **Alta**, si lo desea.

    "Obtenga más información sobre la velocidad de escritura" .

    > La opción de velocidad de escritura **Alta** permite obtener una alta velocidad de escritura y una unidad de transmisión máxima (MTU) más alta de 8,896 bytes. Además, la MTU más alta de 8.896 requiere la selección de VPC-1, VPC-2 y VPC-3 para la implementación. Para obtener más información sobre VPC-1, VPC-2 y VPC-3, consulte "Reglas para VPC-1, VPC-2 y VPC-3" .

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

    No se puede habilitar WORM si la clasificación de datos se habilitó para las versiones 9.7 y anteriores de Cloud Volumes ONTAP . La reversión o degradación a Cloud Volumes ONTAP 9.8 está bloqueada después de habilitar WORM y la clasificación en niveles.

    "Obtenga más información sobre el almacenamiento WORM" .

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

13. **Niveles de datos en Google Cloud Platform**: elija si desea habilitar los niveles de datos en el agregado inicial, elija una clase de almacenamiento para los datos en niveles y luego seleccione una cuenta de servicio que tenga la función de administrador de almacenamiento predefinida (requerida para Cloud Volumes ONTAP 9.7 o posterior) o seleccione una cuenta de Google Cloud (requerida para Cloud Volumes ONTAP 9.6).

    Tenga en cuenta lo siguiente:

    - La consola configura la cuenta de servicio en la instancia de Cloud Volumes ONTAP . Esta cuenta de servicio proporciona permisos para la organización de datos en niveles en un depósito de Google Cloud Storage. Asegúrese de agregar la cuenta de servicio del agente de la consola como usuario de la cuenta de servicio de niveles; de lo contrario, no podrá seleccionarla desde la consola.
    - Para obtener ayuda para agregar una cuenta de Google Cloud, consulte "Configuración y adición de cuentas de Google Cloud para la organización de datos en niveles con 9.6" .
    - Puede elegir una política de niveles de volumen específica al crear o editar un volumen.
    - Si desactivas la asignación de niveles de datos, puedes activarla en los agregados posteriores, pero tendrás que apagar el sistema y añadir una cuenta de servicio desde Google Cloud Console.

    "Obtenga más información sobre la clasificación de datos" .

14. **Crear volumen**: Ingrese detalles para el nuevo volumen o haga clic en **Omitir**.

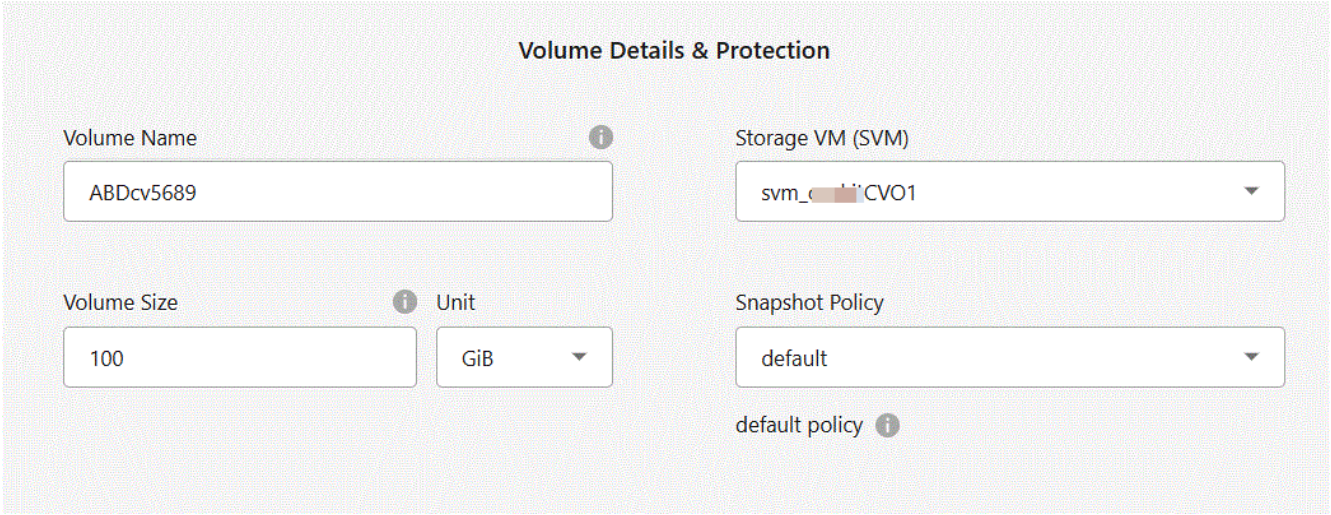
    "Obtenga información sobre los protocolos y versiones de cliente compatibles" .

    Algunos de los campos de esta página se explican por sí solos. La siguiente tabla describe los campos

para los que podría necesitar orientación:

Campo	Descripción
Size	El tamaño máximo que puede ingresar depende en gran medida de si habilita el aprovisionamiento fino, que le permite crear un volumen que sea más grande que el almacenamiento físico actualmente disponible para él.
Control de acceso (solo para NFS)	Una política de exportación define los clientes de la subred que pueden acceder al volumen. De forma predeterminada, la consola ingresa un valor que proporciona acceso a todas las instancias de la subred.
Permisos y usuarios/grupos (solo para CIFS)	Estos campos le permiten controlar el nivel de acceso a un recurso compartido para usuarios y grupos (también llamados listas de control de acceso o ACL). Puede especificar usuarios o grupos de Windows locales o de dominio, o usuarios o grupos de UNIX. Si especifica un nombre de usuario de dominio de Windows, debe incluir el dominio del usuario utilizando el formato dominio\nombre de usuario.
Política de instantáneas	Una política de copia de instantáneas especifica la frecuencia y la cantidad de copias de instantáneas de NetApp creadas automáticamente. Una copia Snapshot de NetApp es una imagen del sistema de archivos en un momento determinado que no tiene impacto en el rendimiento y requiere un almacenamiento mínimo. Puede elegir la política predeterminada o ninguna. Puede elegir ninguno para 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 iniciador e IQN (solo para iSCSI)	Los objetivos de almacenamiento iSCSI se denominan LUN (unidades lógicas) y se presentan a los hosts como dispositivos de bloque estándar. Los grupos de iniciadores son tablas de nombres de nodos de host iSCSI y controlan qué iniciadores tienen acceso a qué LUN. Los objetivos iSCSI se conectan a la red a través de adaptadores de red Ethernet estándar (NIC), tarjetas de motor de descarga TCP (TOE) con iniciadores de software, adaptadores de red convergente (CNA) o adaptadores de bus de host dedicados (HBA) y se identifican mediante nombres calificados iSCSI (IQN). Cuando crea un volumen iSCSI, la consola crea automáticamente un LUN para usted. Lo hemos simplificado creando solo un LUN por volumen, por lo que no es necesario realizar ninguna gestión. Después de crear el volumen,"Utilice el IQN para conectarse al LUN desde sus hosts" .

La siguiente imagen muestra la primera página del asistente de creación de volumen:



15. **Configuración CIFS**: si eligió el protocolo CIFS, configure un servidor CIFS.

Campo	Descripción
Dirección IP primaria y secundaria de DNS	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 ubicar los servidores LDAP de Active Directory y los controladores de dominio para el 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	El nombre y la contraseña de una cuenta de Windows con privilegios suficientes para agregar computadoras a la unidad organizativa (OU) especificada dentro del dominio de AD.
Nombre NetBIOS del servidor CIFS	Un nombre de servidor CIFS que es único en el dominio AD.
Unidad organizativa	La unidad organizativa dentro del dominio AD para asociarse con el servidor CIFS. El valor predeterminado es CN=Computers. Para configurar Google Managed Microsoft AD como servidor AD para Cloud Volumes ONTAP, ingrese **OU=Computers,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 en 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 utilizando el DNS de Active Directory. Si necesita configurar un servidor NTP utilizando una dirección diferente, debe utilizar la API. Para obtener información, consulte la "Documentación de automatización de la NetApp Console" Para más detalles. Tenga en cuenta que solo puede configurar un servidor NTP al crear un servidor CIFS. No es configurable después de crear el servidor CIFS.

16. **Perfil de uso, tipo de disco y política de niveles**: elija si desea habilitar las funciones de eficiencia de almacenamiento y cambiar la política de niveles de volumen, si es necesario.

    Para obtener más información, consulte"Elija un perfil de uso de volumen" ,"Descripción general de la clasificación de datos" , y "KB: ¿Qué funciones de eficiencia de almacenamiento en línea son compatibles con CVO?"

17. **Revisar y aprobar**: revise y confirme sus selecciones.
    a. Revise los detalles sobre la configuración.
    b. Haga clic en **Más información** para revisar los detalles sobre el soporte y los recursos de Google Cloud que comprará la consola.
    c. Seleccione la casilla de verificación **Entiendo…**.
    d. Haga clic en **Ir**.

Resultado

La consola implementa el sistema Cloud Volumes ONTAP . Puede seguir el progreso en la página **Auditoría**.

Si experimenta algún problema al implementar el sistema Cloud Volumes ONTAP , revise el mensaje de error. También puede seleccionar el sistema y hacer clic en **Recrear entorno**.

Para obtener ayuda adicional, visite "Compatibilidad con NetApp Cloud Volumes ONTAP" .

Después de terminar

- Si aprovisionó un recurso compartido CIFS, otorgue a los usuarios o grupos permisos para los archivos y carpetas y verifique que esos usuarios puedan acceder al recurso compartido y crear un archivo.
- Si desea aplicar cuotas a los volúmenes, utilice el Administrador del sistema ONTAP o la CLI de ONTAP .

  Las cuotas le permiten restringir o rastrear el espacio en disco y la cantidad de archivos utilizados por un usuario, grupo o qtree.

> Después de que se complete el proceso de despliegue, no modifiques las configuraciones de Cloud Volumes ONTAP generadas por el sistema en el portal de Google Cloud, como las etiquetas del sistema y las etiquetas establecidas en los recursos de Google Cloud. Cualquier cambio hecho en estas configuraciones puede causar un comportamiento inesperado o pérdida de datos.

Lanzar un par HA en Google Cloud

Cree un sistema en la consola para iniciar Cloud Volumes ONTAP en Google Cloud.

Pasos

1. Desde el menú de navegación de la izquierda, seleccione **Almacenamiento > Administración**.
2. En la página **Sistemas**, haga clic en **Almacenamiento > Sistema** y siga las instrucciones.
3. **Elija una ubicación**: seleccione **Google Cloud** y * Cloud Volumes ONTAP HA*.
4. **Detalles y credenciales**: seleccione un proyecto, especifique un nombre de clúster, opcionalmente seleccione una cuenta de servicio, opcionalmente agregue etiquetas y luego especifique las credenciales.

   La siguiente tabla describe los campos para los que podría necesitar orientación:

Campo	Descripción
Nombre del sistema	La consola usa el nombre del sistema para nombrar tanto el sistema Cloud Volumes ONTAP como la instancia de Google Cloud VM. También utiliza el nombre como prefijo para el grupo de seguridad predefinido, si selecciona esa opción.
Nombre de la cuenta de servicio	Si planea utilizar el"NetApp Cloud Tiering" o "Copia de seguridad y recuperación" servicios, debe habilitar el interruptor **Cuenta de servicio** y luego seleccionar la Cuenta de servicio que tenga el rol de Administrador de almacenamiento predefinido.
Agregar etiquetas	Las etiquetas son metadatos para sus recursos de Google Cloud. La consola agrega las etiquetas al sistema Cloud Volumes ONTAP y a los recursos de Google Cloud asociados con el sistema. Puede agregar hasta cuatro etiquetas desde la interfaz de usuario al crear un sistema y luego puede agregar más una vez creado. Tenga en cuenta que la API no lo limita a cuatro etiquetas al crear un sistema. Para obtener información sobre las etiquetas, consulte "Documentación de Google Cloud: Recursos de etiquetado" .
Nombre de usuario y contraseña	Estas son las credenciales para la cuenta de administrador del clúster de Cloud Volumes ONTAP . Puede usar estas credenciales para conectarse a Cloud Volumes ONTAP a través de ONTAP System Manager o la CLI de ONTAP . Mantenga el nombre de usuario predeterminado *admin* o cámbielo por un nombre de usuario personalizado.
Editar proyecto	Seleccione el proyecto donde desea que resida Cloud Volumes ONTAP . El proyecto predeterminado es el proyecto de la Consola. Si no ves ningún proyecto adicional en la lista desplegable, entonces aún no has asociado la cuenta de servicio con otros proyectos. Ve a Google Cloud Console, abre el servicio IAM y selecciona el proyecto. Agrega la cuenta de servicio con el rol que usas para la Console a ese proyecto. Tendrás que repetir este paso para cada proyecto. Esta es la cuenta de servicio que configuraste para la consola."como se describe en esta página" . Haga clic en **Agregar suscripción** para asociar las credenciales seleccionadas con una suscripción. Para crear un sistema Cloud Volumes ONTAP de pago por uso, debe seleccionar un proyecto de Google Cloud que esté asociado con una suscripción a Cloud Volumes ONTAP desde Google Cloud Marketplace. Referirse a "Cómo asociar una suscripción de Marketplace con las credenciales de Google Cloud" .

5. **Servicios**: Seleccione los servicios que desea utilizar en este sistema. Para seleccionar Copia de seguridad y recuperación, o para utilizar NetApp Cloud Tiering, debe haber especificado la cuenta de servicio en el paso 3.

Si desea utilizar WORM y niveles de datos, debe deshabilitar la función de copia de seguridad y recuperación e implementar un sistema Cloud Volumes ONTAP con la versión 9.8 o superior.

6. **Modelos de implementación de HA**: elige varias zonas (recomendado) o una sola zona para la configuración de HA. Luego selecciona una región y una zona.

   "Obtenga más información sobre los modelos de implementación de HA" .

7. **Conectividad**: seleccione cuatro VPC diferentes para la configuración de HA, una subred en cada VPC y luego elija una política de firewall.

   "Obtenga más información sobre los requisitos de red" .

   La siguiente tabla describe los campos para los que podría necesitar orientación:

Campo	Descripción
Política generada	Si deja que la consola genere la política de firewall por usted, deberá elegir cómo permitirá el tráfico: • Si elige **Solo VPC seleccionada**, el filtro de origen para el tráfico entrante es el rango de subred de la VPC seleccionada y el rango de subred de la VPC donde reside el agente de la consola. Esta es la opción recomendada. • Si elige **Todas las VPC**, el filtro de origen para el tráfico entrante es el rango de IP 0.0.0.0/0.
Utilizar los existentes	Si utiliza una política de firewall existente, asegúrese de que incluya las reglas necesarias. "Obtenga información sobre las reglas de firewall para Cloud Volumes ONTAP" .

8. **Métodos de carga y cuenta NSS**: especifique qué opción de carga desea utilizar con este sistema y luego especifique una cuenta del sitio de soporte de NetApp .
   - "Obtenga más 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 elige uno de los paquetes, solo necesita especificar un volumen y luego 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 candidata a lanzamiento, una versión de disponibilidad general o una versión de parche más reciente para la versión seleccionada, la consola actualiza el sistema a esa versión al crearla. Por ejemplo, la actualización se produce si selecciona Cloud Volumes ONTAP 9.13.1 y 9.13.1 P4 está disponible. La actualización no se produce de una versión a otra, por ejemplo, de 9.13 a 9.14.

11. **Recursos de almacenamiento subyacentes**: elija configuraciones para el agregado inicial: un tipo de disco y el tamaño de cada disco.

    El tipo de disco es para el volumen inicial. Puede elegir un tipo de disco diferente para los volúmenes posteriores.

El tamaño del disco es para todos los discos en el agregado inicial y para cualquier agregado adicional que la Consola crea cuando 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 para elegir un tipo y tamaño de disco, consulte"Dimensiona tu sistema en Google Cloud" .

12. **Caché Flash, Velocidad de Escritura y WORM**:

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

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

    b. Elija velocidad de escritura **Normal** o **Alta**, si lo desea.

    "Obtenga más información sobre la velocidad de escritura" .

    > La opción de velocidad de escritura **Alta** ofrece una alta velocidad de escritura y una unidad de transmisión máxima (MTU) más alta de 8896 bytes con los tipos de instancia n2-standard-16, n2-standard-32, n2-standard-48 y n2-standard-64. Además, la MTU más alta de 8.896 requiere la selección de VPC-1, VPC-2 y VPC-3 para la implementación. La alta velocidad de escritura y una MTU de 8,896 dependen de la función y no se pueden desactivar individualmente dentro de 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. Active el almacenamiento de escritura única y lectura múltiple (WORM), si lo desea.

    No se puede habilitar WORM si la clasificación de datos se habilitó para las versiones 9.7 y anteriores de Cloud Volumes ONTAP . La reversión o degradación a Cloud Volumes ONTAP 9.8 está bloqueada después de habilitar WORM y la clasificación en niveles.

"Obtenga más información sobre el almacenamiento WORM" .

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

13. **Niveles de datos en Google Cloud**: elija si desea habilitar los niveles de datos en el agregado inicial, elija una clase de almacenamiento para los datos estratificados y, luego, seleccione una cuenta de servicio que tenga la función de administrador de almacenamiento predefinida.

    Tenga en cuenta lo siguiente:

    - La consola configura la cuenta de servicio en la instancia de Cloud Volumes ONTAP . Esta cuenta de servicio proporciona permisos para la organización de datos en niveles en un depósito de Google Cloud Storage. Asegúrese de agregar la cuenta de servicio del agente de la consola como usuario de la cuenta de servicio de niveles; de lo contrario, no podrá seleccionarla desde la consola.
    - Puede elegir una política de niveles de volumen específica al crear o editar un volumen.
    - Si desactivas la asignación de niveles de datos, puedes activarla en los agregados posteriores, pero tendrás que apagar el sistema y añadir una cuenta de servicio desde Google Cloud Console.

    "Obtenga más información sobre la clasificación de datos" .

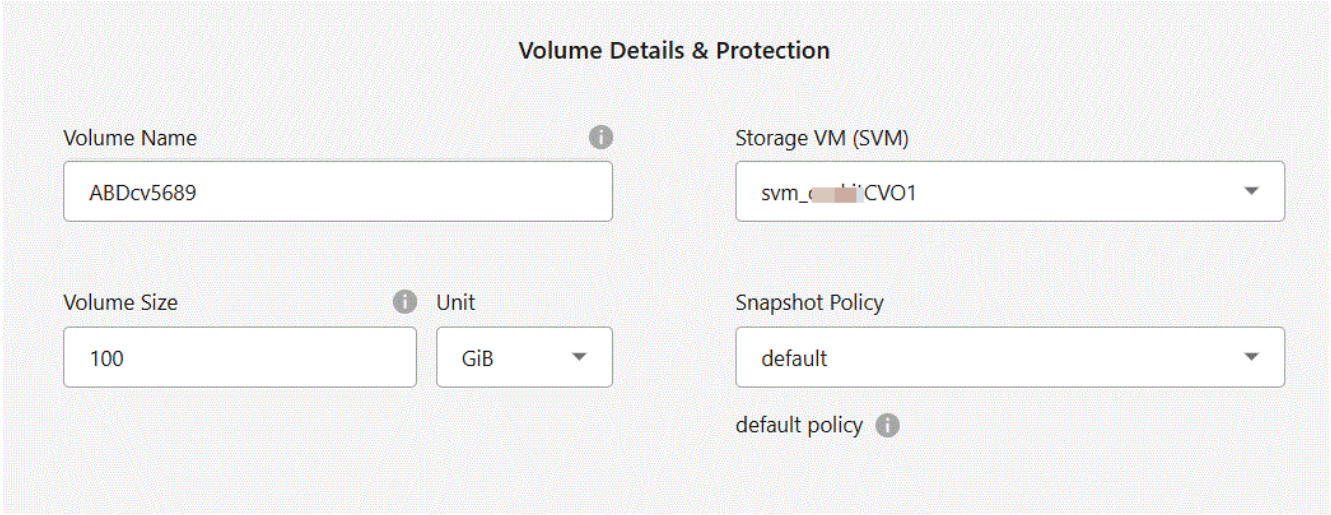
14. **Crear volumen**: Ingrese detalles para el nuevo volumen o haga clic en **Omitir**.

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

    Algunos de los campos de esta página se explican por sí solos. La siguiente tabla describe los campos para los que podría necesitar orientación:

Campo	Descripción
Size	El tamaño máximo que puede ingresar depende en gran medida de si habilita el aprovisionamiento fino, que le permite crear un volumen que sea más grande que el almacenamiento físico actualmente disponible para él.
Control de acceso (solo para NFS)	Una política de exportación define los clientes de la subred que pueden acceder al volumen. De forma predeterminada, la consola ingresa un valor que proporciona acceso a todas las instancias de la subred.
Permisos y usuarios/grupos (solo para CIFS)	Estos campos le permiten controlar el nivel de acceso a un recurso compartido para usuarios y grupos (también llamados listas de control de acceso o ACL). Puede especificar usuarios o grupos de Windows locales o de dominio, o usuarios o grupos de UNIX. Si especifica un nombre de usuario de dominio de Windows, debe incluir el dominio del usuario utilizando el formato dominio\nombre de usuario.
Política de instantáneas	Una política de copia de instantáneas especifica la frecuencia y la cantidad de copias de instantáneas de NetApp creadas automáticamente. Una copia Snapshot de NetApp es una imagen del sistema de archivos en un momento determinado que no tiene impacto en el rendimiento y requiere un almacenamiento mínimo. Puede elegir la política predeterminada o ninguna. Puede elegir ninguno para 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 iniciador e IQN (solo para iSCSI)	Los objetivos de almacenamiento iSCSI se denominan LUN (unidades lógicas) y se presentan a los hosts como dispositivos de bloque estándar. Los grupos de iniciadores son tablas de nombres de nodos de host iSCSI y controlan qué iniciadores tienen acceso a qué LUN. Los objetivos iSCSI se conectan a la red a través de adaptadores de red Ethernet estándar (NIC), tarjetas de motor de descarga TCP (TOE) con iniciadores de software, adaptadores de red convergente (CNA) o adaptadores de bus de host dedicados (HBA) y se identifican mediante nombres calificados iSCSI (IQN). Cuando crea un volumen iSCSI, la consola crea automáticamente un LUN para usted. Lo hemos simplificado creando solo un LUN por volumen, por lo que no es necesario realizar ninguna gestión. Después de crear el volumen,"Utilice el IQN para conectarse al LUN desde sus hosts" .

    La siguiente imagen muestra la primera página del asistente de creación de volumen:



15. **Configuración CIFS**: si eligió el protocolo CIFS, configure un servidor CIFS.

Campo	Descripción
Dirección IP primaria y secundaria de DNS	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 ubicar los servidores LDAP de Active Directory y los controladores de dominio para el 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	El nombre y la contraseña de una cuenta de Windows con privilegios suficientes para agregar computadoras a la unidad organizativa (OU) especificada dentro del dominio de AD.
Nombre NetBIOS del servidor CIFS	Un nombre de servidor CIFS que es único en el dominio AD.
Unidad organizativa	La unidad organizativa dentro del dominio AD para asociarse con el servidor CIFS. El valor predeterminado es CN=Computers. Para configurar Google Managed Microsoft AD como servidor AD para Cloud Volumes ONTAP, ingrese **OU=Computers,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 en 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 utilizando el DNS de Active Directory. Si necesita configurar un servidor NTP utilizando una dirección diferente, debe utilizar la API. Consulte la "Documentación de automatización de la NetApp Console" Para más detalles. Tenga en cuenta que solo puede configurar un servidor NTP al crear un servidor CIFS. No es configurable después de crear el servidor CIFS.

16. **Perfil de uso, tipo de disco y política de niveles**: elija si desea habilitar las funciones de eficiencia de almacenamiento y cambiar la política de niveles de volumen, si es necesario.

    Para obtener más información, consulte"Elija un perfil de uso de volumen" ,"Descripción general de la clasificación de datos" , y "KB: ¿Qué funciones de eficiencia de almacenamiento en línea son compatibles con CVO?"

17. **Revisar y aprobar**: revise y confirme sus selecciones.
    a. Revise los detalles sobre la configuración.
    b. Haga clic en **Más información** para revisar los detalles sobre el soporte y los recursos de Google Cloud que comprará la consola.
    c. Seleccione la casilla de verificación **Entiendo…**.
    d. Haga clic en **Ir**.

Resultado

La consola implementa el sistema Cloud Volumes ONTAP . Puede seguir el progreso en la página **Auditoría**.

Si experimenta algún problema al implementar el sistema Cloud Volumes ONTAP , revise el mensaje de error. También puede seleccionar el sistema y hacer clic en **Recrear entorno**.

Para obtener ayuda adicional, visite "Compatibilidad con NetApp Cloud Volumes ONTAP" .

Después de terminar

- Si aprovisionó un recurso compartido CIFS, otorgue a los usuarios o grupos permisos para los archivos y carpetas y verifique que esos usuarios puedan acceder al recurso compartido y crear un archivo.
- Si desea aplicar cuotas a los volúmenes, utilice el Administrador del sistema ONTAP o la CLI de ONTAP .

  Las cuotas le permiten restringir o rastrear el espacio en disco y la cantidad de archivos utilizados por un usuario, grupo o qtree.

> Después de que se complete el proceso de despliegue, no modifiques las configuraciones de Cloud Volumes ONTAP generadas por el sistema en el portal de Google Cloud, como las etiquetas del sistema y las etiquetas establecidas en los recursos de Google Cloud. Cualquier cambio hecho en estas configuraciones puede causar un comportamiento inesperado o pérdida de datos.

Enlaces relacionados

- "Planificación de la configuración de Cloud Volumes ONTAP en Google Cloud"

Verificación de imágenes de Google Cloud Platform

Descubra cómo se verifica la imagen de Google Cloud en Cloud Volumes ONTAP

La verificación de imágenes de Google Cloud cumple con los requisitos de seguridad mejorados de NetApp . Se han realizado cambios en el script que genera las imágenes para firmar la imagen a lo largo del camino utilizando claves privadas generadas específicamente para esta tarea. Puede verificar la integridad de la imagen de Google Cloud mediante el resumen firmado y el certificado público de Google Cloud, que se pueden descargar a través de "Sistema Nacional de Seguridad" para un lanzamiento

específico.

La verificación de imágenes de Google Cloud es compatible con el software Cloud Volumes ONTAP versión 9.13.0 o superior.

Convertir imágenes de Google Cloud a formato RAW para Cloud Volumes ONTAP

La imagen que se utiliza para implementar nuevas instancias, actualizaciones o que se utiliza en imágenes existentes se compartirá con los clientes a través de "el sitio de soporte de NetApp (NSS)" . El resumen firmado y los certificados estarán disponibles para descargar a través del portal NSS. Asegúrese de estar descargando el resumen y los certificados de la versión correcta correspondiente a la imagen compartida por el soporte de NetApp . Por ejemplo, las imágenes 9.13.0 tendrán un resumen firmado 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 con el resumen firmado y los certificados, necesita tener un mecanismo para comparar los dos archivos y descargar la imagen. Para ello, debes exportar/convertir la imagen a un formato disk.raw y guardar los resultados en un depósito de almacenamiento en Google Cloud. El archivo disk.raw se procesa en formato tar y gzip durante el proceso.

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

- Acceso al depósito de almacenamiento de Google
- Escribir en el depósito de Google Storage
- Crear trabajos de compilación en la nube (utilizados durante el proceso de exportación)
- Acceso a la imagen deseada
- Crear tareas de exportación de imágenes

Para verificar la imagen, debe convertirse a formato disk.raw y luego descargarse.

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

La forma preferida de exportar una imagen a Cloud Storage es usar el "Comando de exportación de imágenes de gcloud compute" . Este comando toma la imagen proporcionada y la convierte en un archivo disk.raw que se comprime y se empaqueta en gzip. El archivo generado se guarda en la URL de destino y luego se puede descargar para su verificación.

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

Exportar imagen de Google Cloud usando 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
```

Para obtener más información sobre cómo exportar una imagen a través de Google Cloud, consulte "Documento de Google Cloud sobre cómo exportar una imagen" .

Verificación de firma de imagen

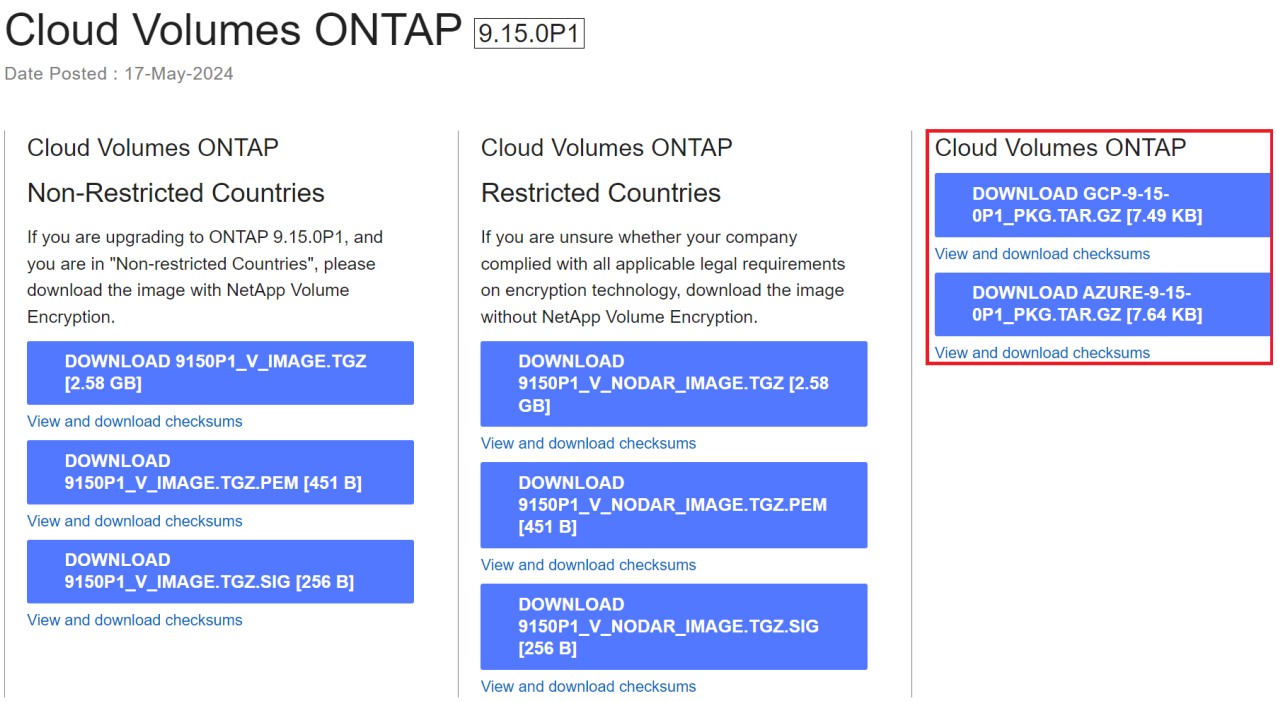
Verificación de firma de imágenes de Google Cloud para Cloud Volumes ONTAP

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

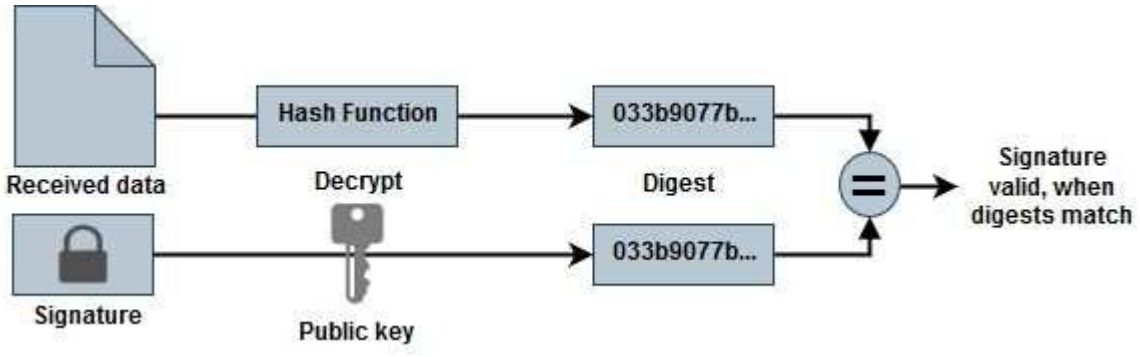
Resumen del flujo de trabajo de verificación de imágenes firmadas

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

- Desde "Sistema Nacional de Seguridad" , descargue el archivo de Google Cloud que contiene los siguientes archivos:
  - Compendio firmado (.sig)
  - Certificado que contiene la clave pública (.pem)
  - Cadena de certificados (.pem)



- Descargue el archivo disk.raw convertido
- Validar el certificado utilizando la cadena de certificados
- Validar el resumen firmado utilizando el certificado que contiene la clave pública
  - Descifrar el resumen firmado utilizando la clave pública para extraer el resumen del archivo de imagen
  - Crear un resumen del archivo disk.raw descargado
  - Compare los dos archivos de resumen para su validación



Verifique el archivo disk.raw de la imagen de Google Cloud para Cloud Volumes ONTAP mediante OpenSSL

Puede verificar el archivo disk.raw descargado de Google Cloud con el contenido del archivo de resumen disponible a través de "Sistema Nacional de Seguridad" utilizando OpenSSL.

Los comandos OpenSSL para validar la imagen son compatibles con máquinas Linux, macOS y Windows.

Pasos

1. Verificar el certificado usando 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 utilizando la clave pública extraída y verifique 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
```