Introducción a la NetApp Console

Cloud Volumes ONTAP

NetApp
February 13, 2026

Tabla de contenidos

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.

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 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"

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. Para obtener más información, consulte"Planifique su configuración de Cloud Volumes ONTAP en Azure" .

3 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" .

4 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.

Puntos finales	Aplicable para	Objetivo	Modos de implementación	Impacto si no está disponible
\ 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.
\ 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.

Puntos finales	Aplicable para	Objetivo	Modos de implementación	Impacto si no está disponible
\ 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.
\ 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

Prioridad y nombre	Puerto y protocolo	Origen y destino	Descripción
1006 entrante_161-162 _udp	161-162 UDP	De cualquiera a cualquiera	Protocolo simple de gestión de red
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

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 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

Prioridad y nombre	Puerto y protocolo	Origen y destino	Descripción
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
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

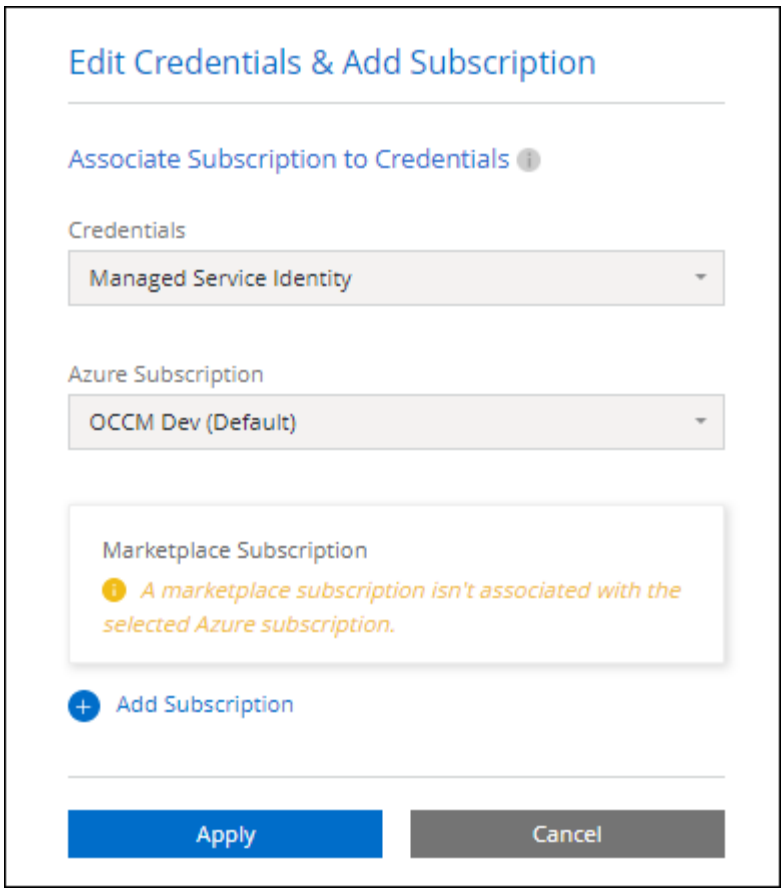
Seleccione la oferta Freemium para utilizar Cloud Volumes ONTAP de forma gratuita con hasta 500 GiB de capacidad aprovisionada. "Obtenga más información sobre la oferta Freemium" .

Pasos

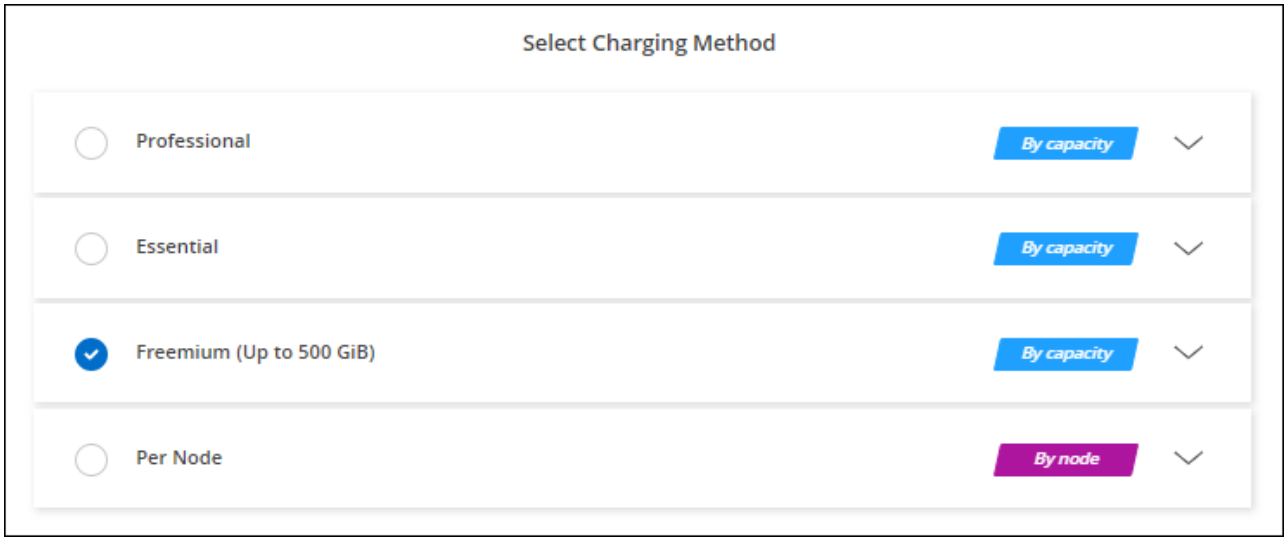
1. Desde el menú de navegación izquierdo de la NetApp Console, seleccione **Almacenamiento > Administración**.
2. En la página **Sistemas**, haga clic en **Agregar sistema** y siga los pasos.

    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"

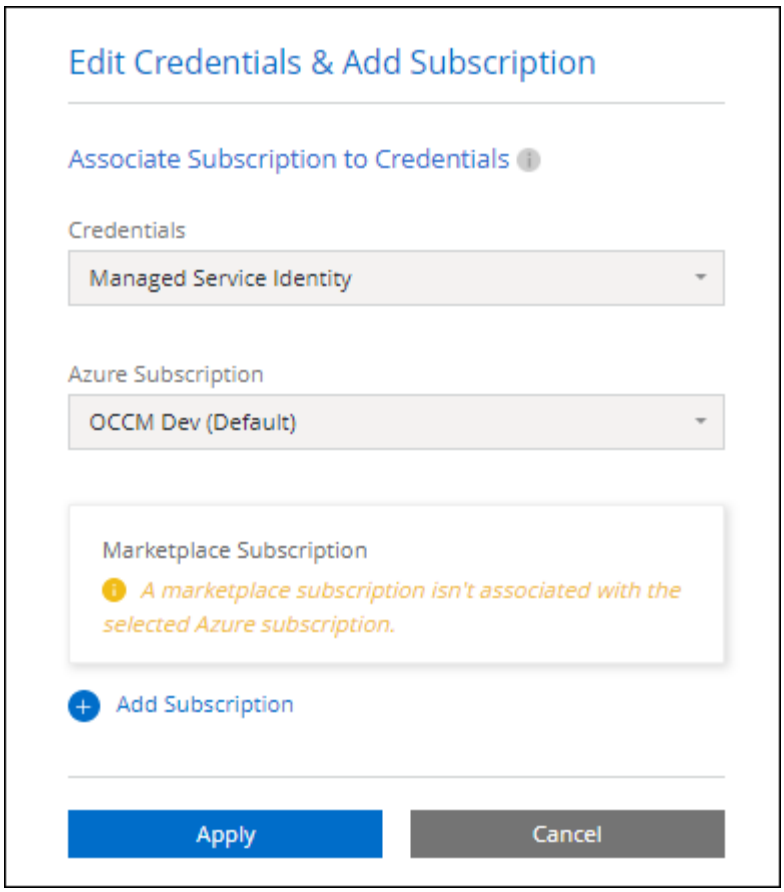
   La consola consulta automáticamente el servicio de licencias de NetApp para obtener detalles sobre las licencias asociadas a su cuenta del sitio de soporte de NetApp . Si no hay errores, la Consola agrega automáticamente las licencias a la Consola.

   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" .

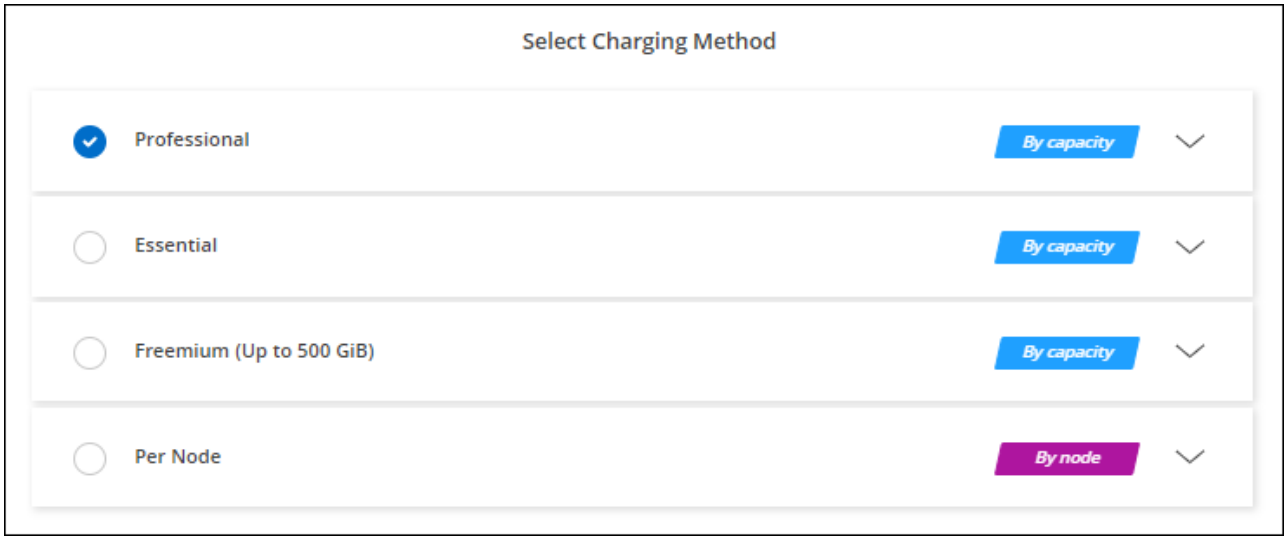
3. En la página **Sistemas**, haga clic en **Agregar sistema** y siga los pasos.

   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

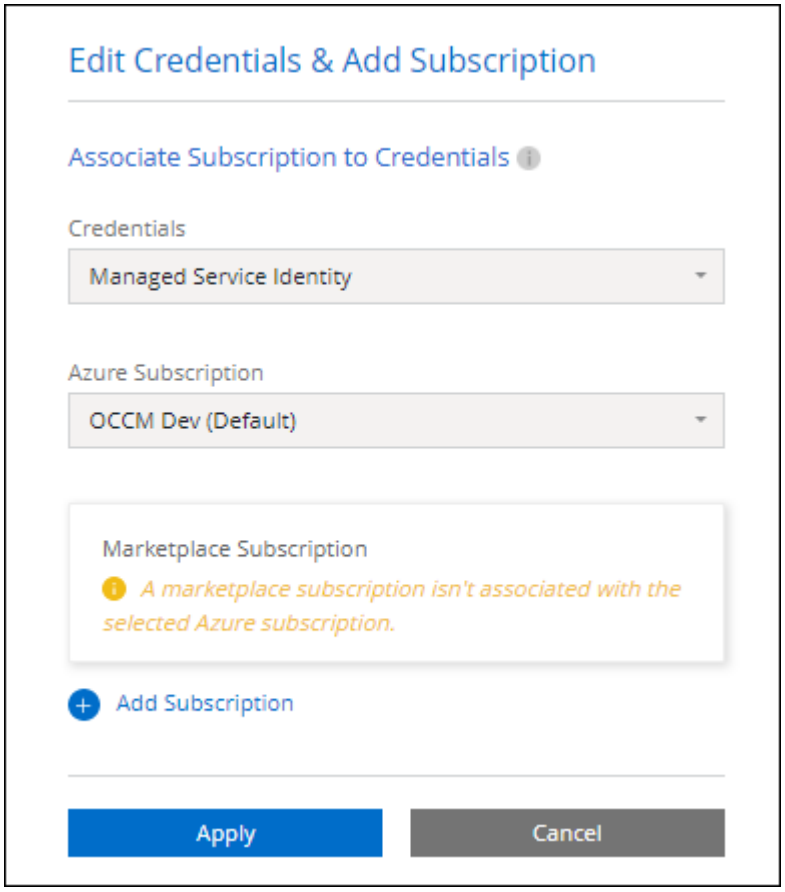
Pague por hora suscribiéndose a la oferta del mercado de su proveedor de nube.

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

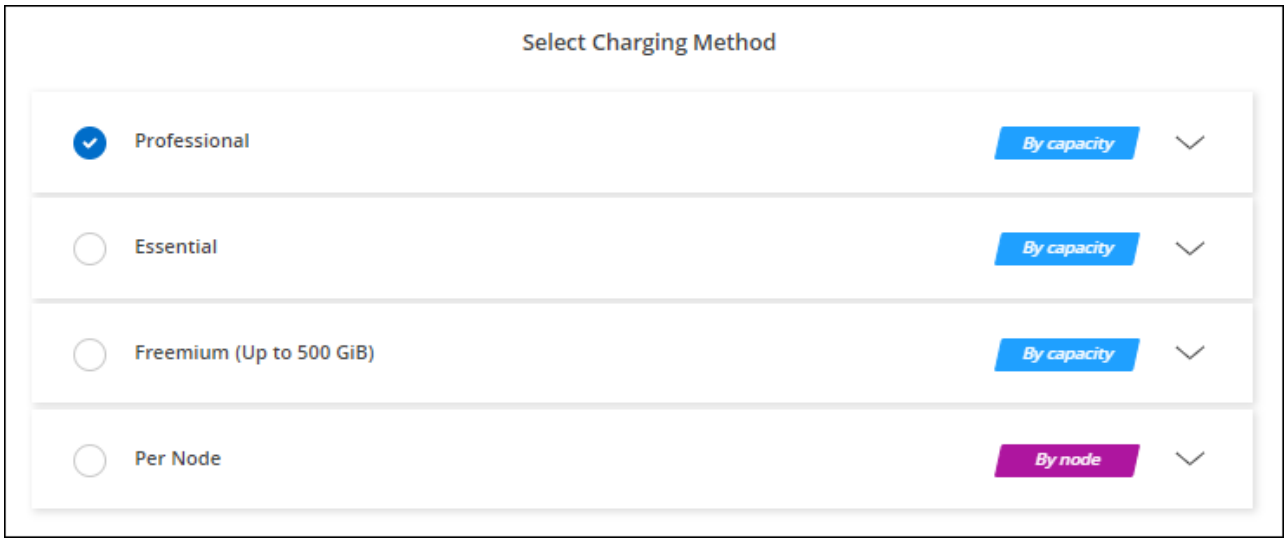
misma suscripción para sistemas adicionales.

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.

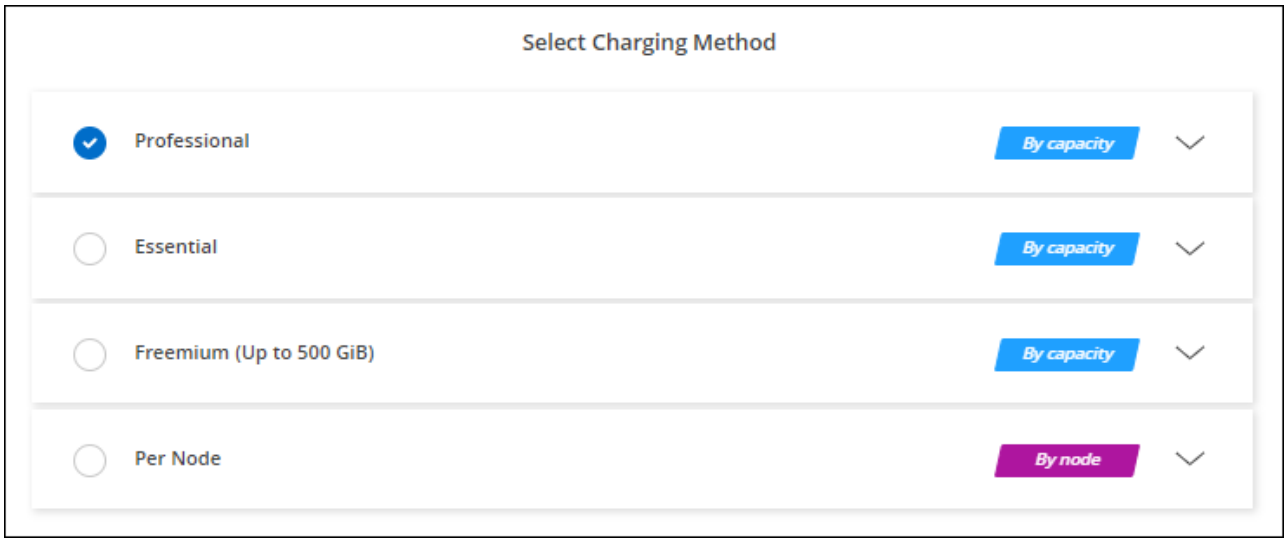
Pasos

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" .

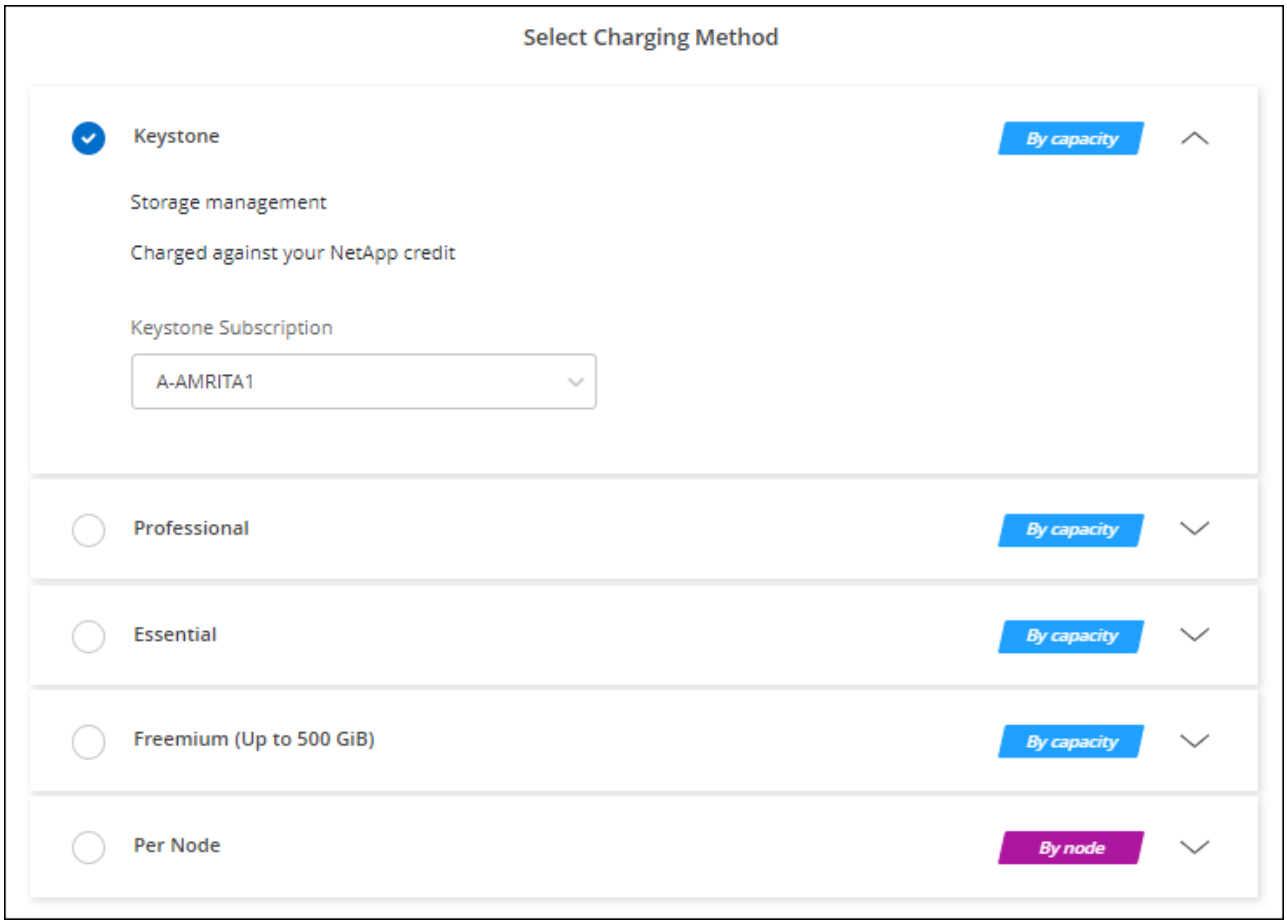
Suscripción a Keystone

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**.

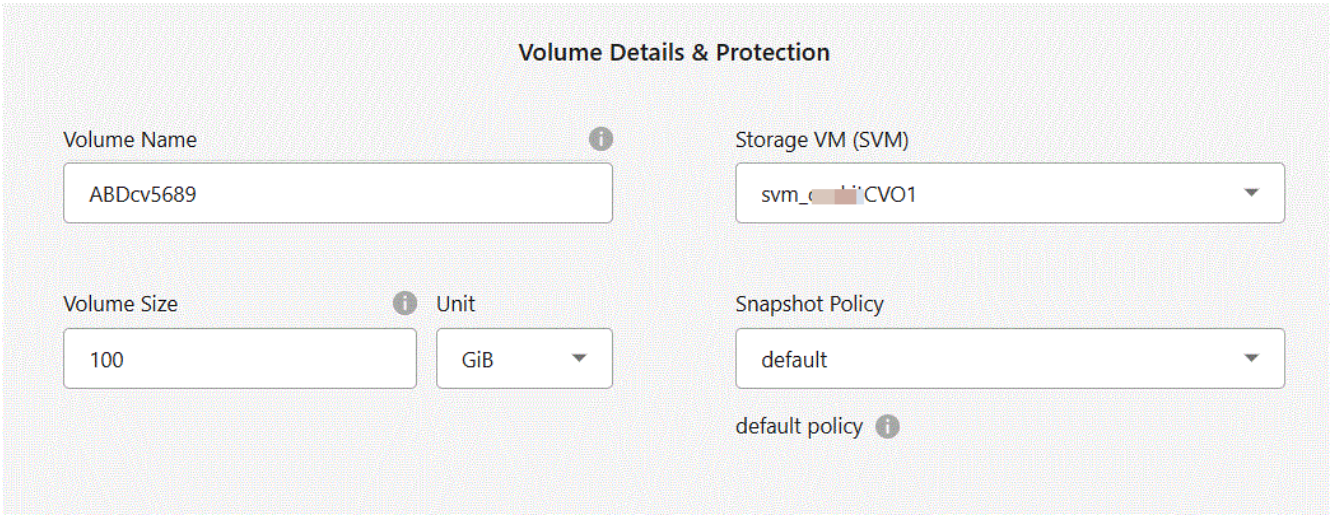
    "Obtenga información sobre los protocolos y versiones de cliente compatibles" .

    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" .

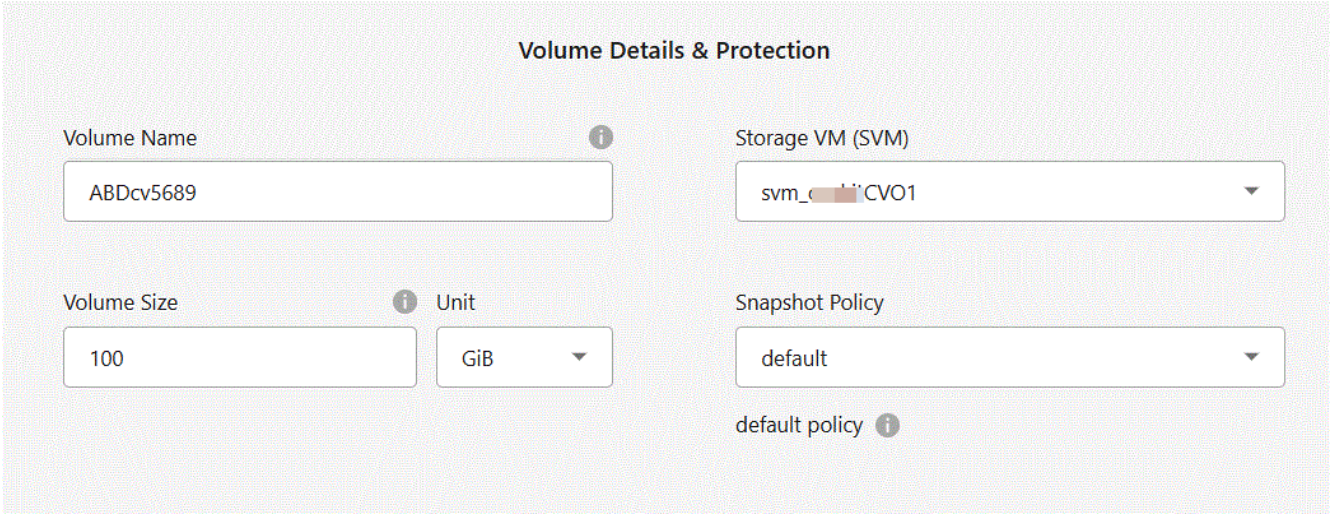
15. **Crear volumen**: Ingrese detalles para el nuevo volumen o haga clic en **Omitir**.

    "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

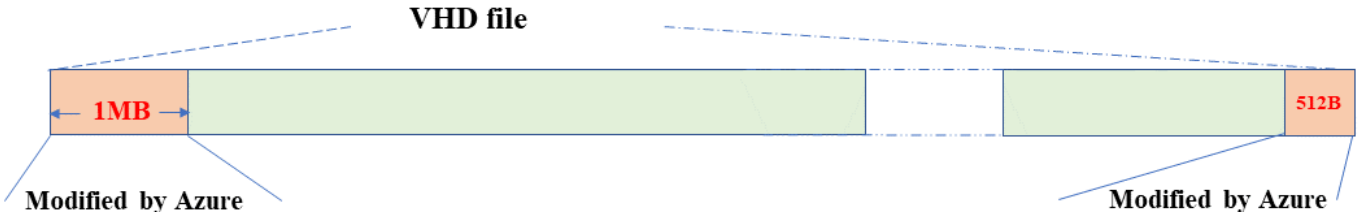
Verificación de imágenes de Azure Marketplace para Cloud Volumes ONTAP

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"

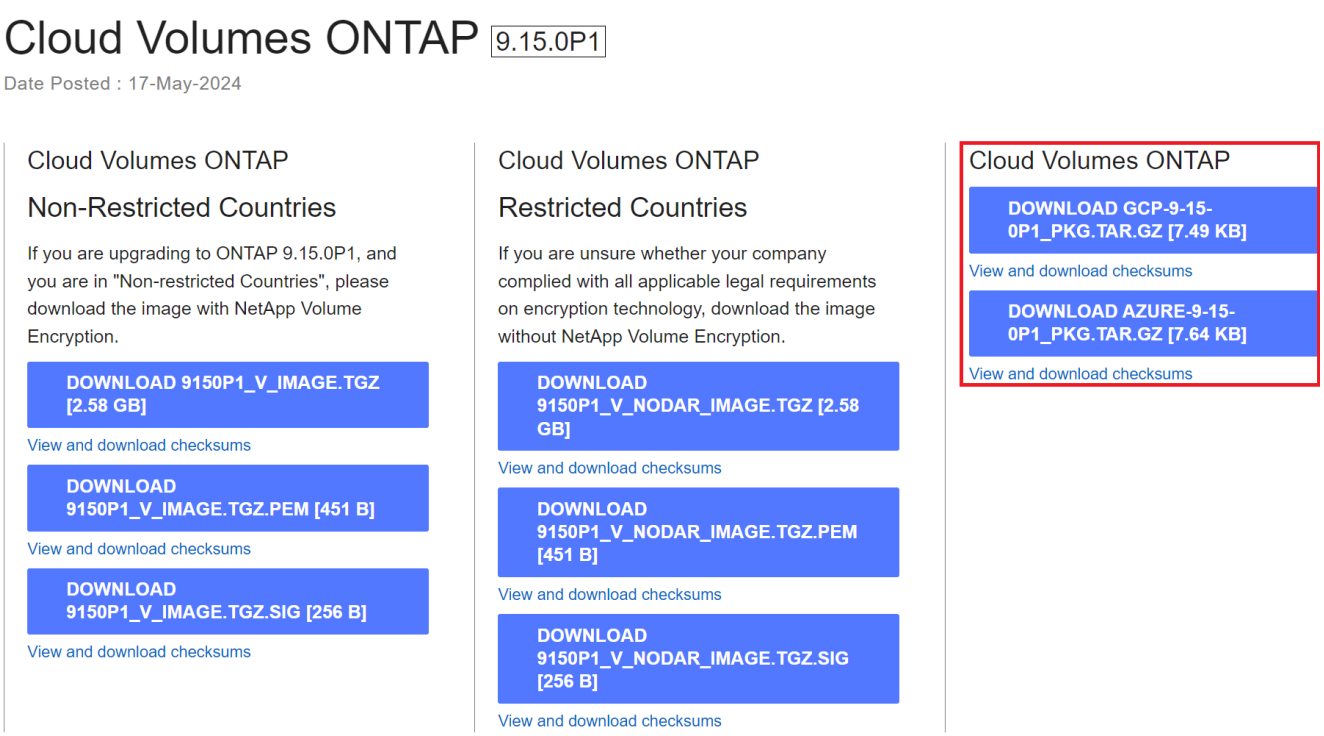
Descargue el archivo de imagen de Azure para Cloud Volumes ONTAP

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&sigxxxxxxxxxxxxxxxxxxxxxxxx"
```

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
```

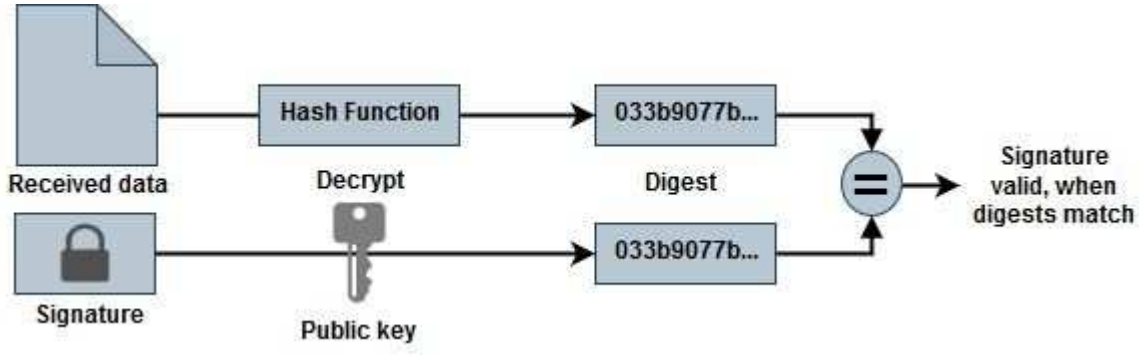
Verificar la firma del archivo

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
```