Empiece a usar Microsoft Azure

Cloud Volumes ONTAP

NetApp
September 24, 2024

Tabla de contenidos

Empiece a usar Microsoft Azure

Inicio rápido para Cloud Volumes ONTAP en Azure

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

1 Cree un conector

Si usted no tiene un "Conector" Sin embargo, un administrador de cuentas necesita crear uno. "Aprenda a crear un conector en Azure"

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

2 Planificación de la configuración

BlueXP ofrece paquetes preconfigurados que se ajustan a sus necesidades de carga de trabajo, o puede crear su propia configuración. Si elige su propia configuración, debe conocer las opciones disponibles. Para obtener más información, consulte "Planifique la configuración de Cloud Volumes ONTAP en Azure".

3 Configure su red

1. Asegúrese de que vnet y las subredes admitan la conectividad entre el conector y Cloud Volumes ONTAP.
2. Habilite el acceso a Internet de salida desde el VPC de destino para AutoSupport de NetApp.

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

"Obtenga más información sobre los requisitos de red".

4 Inicie Cloud Volumes ONTAP con BlueXP

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

Enlaces relacionados

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

Planifique la configuración de Cloud Volumes ONTAP en Azure

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

Seleccione una licencia de Cloud Volumes ONTAP

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

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

Seleccione una región admitida

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

Seleccione un tipo de máquina virtual admitido

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

"Configuraciones compatibles para Cloud Volumes ONTAP en Azure"

Comprender los límites de almacenamiento

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

"Límites de almacenamiento para Cloud Volumes ONTAP en Azure"

Configure el tamaño de su sistema en Azure

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

Tipo de máquina virtual

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

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

Tipo de disco de Azure con sistemas de nodo único

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

Los sistemas de un solo nodo pueden utilizar los siguientes tipos de discos gestionados de Azure:

- *Premium SSD Managed Disks* proporciona un alto rendimiento para cargas de trabajo con un gran volumen de I/o a un coste más elevado.
- *Premium SSD v2 Managed Disks* Proporciona un mayor rendimiento con menor latencia a un menor costo, en comparación con los discos gestionados SSD Premium.
- *Standard SSD Managed Disks* proporciona un rendimiento constante para cargas de trabajo que requieren un bajo nivel de IOPS.
- *Standard HDD Managed Disks* es una buena opción si no necesita un alto nivel de IOPS y desea reducir sus costes.

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

Tipo de disco de Azure con pares de alta disponibilidad

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

Tamaño de disco de Azure

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

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

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

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

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

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

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

Ver los discos del sistema predeterminados

Además del almacenamiento de los datos de usuario, BlueXP también adquiere almacenamiento en cloud para los datos del sistema Cloud Volumes ONTAP (datos de arranque, datos raíz, datos principales y

NVRAM). Para fines de planificación, es posible que le ayude a revisar estos detalles antes de implementar Cloud Volumes ONTAP.

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

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

Recopilar información de red

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

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

Elija una velocidad de escritura

BlueXP permite elegir una configuración de velocidad de escritura para Cloud Volumes ONTAP. Antes de elegir una velocidad de escritura, debe comprender las diferencias entre la configuración normal y la alta, así como los riesgos y recomendaciones cuando utilice la alta velocidad de escritura. "Más información sobre la velocidad de escritura".

Seleccione un perfil de uso de volumen

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

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

Aprovisionamiento ligero

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

Deduplicación

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

Compresión

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

Requisitos de red para Cloud Volumes ONTAP en Azure

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

Requisitos para Cloud Volumes ONTAP

Los siguientes requisitos de red deben satisfacerse en Azure.

Acceso a Internet de salida

Los nodos Cloud Volumes ONTAP requieren acceso a Internet 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 estrictos requisitos de seguridad.

Puntos finales de Cloud Volumes ONTAP

Cloud Volumes ONTAP requiere acceso a Internet saliente para contactar con varios terminales para las operaciones diarias.

Los siguientes extremos son específicos de Cloud Volumes ONTAP. El conector también contacta con varios puntos finales para las operaciones diarias, así como con la consola basada en web de BlueXP . Consulte "Ver puntos finales contactados desde el conector" y. "Prepare las redes para usar la consola de BlueXP"

Puntos finales	Aplicable para	Específico	Modos de implementación de BlueXP	Impacto si no está disponible
https://netapp-cloud-account.auth0.com	Autenticación	Se utiliza para la autenticación BlueXP .	Modos estándar y restringidos.	La autenticación de usuario falla y los siguientes servicios no están disponibles: • Servicios Cloud Volumes ONTAP • Servicios ONTAP • Protocolos y servicios de proxy

Puntos finales	Aplicable para	Específico	Modos de implementación de BlueXP	Impacto si no está disponible
https://keyvault-production-aks.vault.azure.net	Almacén de claves	Se utiliza para recuperar la clave secreta del cliente del almacén de claves de Azure para comunicarse con los bloques de S3 para gestionar metadatos. El servicio Cloud Volumes ONTAP utiliza este componente internamente.	Modos estándar, restringido y privado.	Los servicios Cloud Volumes ONTAP no están disponibles.
https://cloudmanager.cloud.netapp.com/tenancy	Cliente	Se utiliza para recuperar los recursos de Cloud Volumes ONTAP de la tenencia de BlueXP para autorizar recursos y usuarios.	Modos estándar y restringidos.	Los recursos de Cloud Volumes ONTAP y los usuarios no están autorizados.
https://support.NetApp.com/aods/asupmessage https://support.NetApp.com/asupprod/post/1,0/postAsup	AutoSupport	Se utiliza para enviar datos de telemetría de AutoSupport a soporte técnico de NetApp.	Modos estándar y restringidos.	La información de AutoSupport sigue sin entregarse.
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Regiones públicas	Comunicación con servicios de Azure.	Modos estándar, restringido y privado.	Cloud Volumes ONTAP no se puede comunicar con el servicio de Azure para realizar operaciones específicas de BlueXP en Azure.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Región de China	Comunicación con servicios de Azure.	Modos estándar, restringido y privado.	Cloud Volumes ONTAP no se puede comunicar con el servicio de Azure para realizar operaciones específicas de BlueXP en Azure.

Puntos finales	Aplicable para	Específico	Modos de implementación de BlueXP	Impacto si no está disponible
https://management.microsoftazure.de https://login.microsoftonline.de https://blob.core.cloudapi.de https://core.cloudapi.de	Región de Alemania	Comunicación con servicios de Azure.	Modos estándar, restringido y privado.	Cloud Volumes ONTAP no se puede comunicar con el servicio de Azure para realizar operaciones específicas de BlueXP en Azure.
https://management.usgovcloudapi.net https://login.microsoftonline.us https://blob.core.usgovcloudapi.net https://core.usgovcloudapi.net	Regiones gubernamentales	Comunicación con servicios de Azure.	Modos estándar, restringido y privado.	Cloud Volumes ONTAP no se puede comunicar con el servicio de Azure para realizar operaciones específicas de BlueXP 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 servicios de Azure.	Modos estándar, restringido y privado.	Cloud Volumes ONTAP no se puede comunicar con el servicio de Azure para realizar operaciones específicas de BlueXP en Azure.

Acceso a Internet saliente para NetApp AutoSupport

Los nodos Cloud Volumes ONTAP requieren acceso a Internet de salida para AutoSupport de NetApp, que supervisa de forma proactiva el estado del sistema y envía mensajes al soporte técnico de NetApp.

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

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

Si una conexión a Internet saliente no está disponible para enviar mensajes AutoSupport, BlueXP configura automáticamente sus sistemas Cloud Volumes ONTAP para utilizar el conector como servidor proxy. El único requisito es asegurarse de que el grupo de seguridad del conector permita conexiones *entrante* a través del puerto 3128. Tendrá que abrir este puerto después de desplegar el conector.

Si ha definido reglas de salida estrictas para Cloud Volumes ONTAP, también tendrá que asegurarse de que el grupo de seguridad Cloud Volumes ONTAP permita conexiones *saliente* a través del puerto 3128.

Una vez que haya comprobado que el acceso saliente a Internet está disponible, puede probar AutoSupport para asegurarse de que puede enviar mensajes. Para obtener instrucciones, consulte "Documentos de ONTAP: Configure AutoSupport".

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

Direcciones IP

BlueXP asigna automáticamente el número requerido de direcciones IP privadas a Cloud Volumes ONTAP en Azure. Debe asegurarse de que la red tenga suficientes direcciones IP privadas disponibles.

El número de LIF que BlueXP asigna a Cloud Volumes ONTAP depende de si pone en marcha un sistema de nodo único o un par de alta disponibilidad. Una LIF es una dirección IP asociada con un puerto físico. Se requiere una LIF de gestión de SVM para herramientas de gestión como SnapCenter.

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

Direcciones IP para un sistema de nodo único

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

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

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

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

Direcciones IP para pares de alta disponibilidad

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

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

NIC0

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

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

NIC1

- La IP de red del clúster

NIC2

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

NIC3

- IP de NIC Pageblob (acceso al disco)

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

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

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

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

Conexiones seguras con servicios de Azure

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

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

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

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

Conexiones con otros sistemas ONTAP

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

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

Puerto para la interconexión de alta disponibilidad

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

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

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

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

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

Reglas de grupo de seguridad

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

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

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

Reglas de entrada para sistemas de un solo nodo

Al crear un entorno de trabajo y elegir un grupo de seguridad predefinido, puede optar por permitir el tráfico de una de las siguientes opciones:

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

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

Prioridad y nombre	Puerto y protocolo	Origen y destino	Descripción
1005 inbound_161-162 _tcp	161-162 TCP	De cualquiera a cualquiera	Protocolo simple de gestión de red
1006 inbound_161-162 _udp	161-162 UDP	De cualquiera a cualquiera	Protocolo simple de gestión de red
1007 inbound_443	443 TCP	De cualquiera a cualquiera	Conectividad con el acceso de conector y HTTPS a la consola web de ONTAP System Manager mediante la dirección IP de la LIF de gestión del clúster
1008 inbound_445	445 TCP	De cualquiera a cualquiera	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
1009 inbound_635_tcp	635 TCP	De cualquiera a cualquiera	Montaje NFS
1010 inbound_635_udp	635 UDP	De cualquiera a cualquiera	Montaje NFS
1011 inbound_749	749 TCP	De cualquiera a cualquiera	Kerberos
1012 inbound_2049_tcp	2049 TCP	De cualquiera a cualquiera	Daemon del servidor NFS
1013 inbound_2049_udp	2049 UDP	De cualquiera a cualquiera	Daemon del servidor NFS
1014 inbound_3260	3260 TCP	De cualquiera a cualquiera	Acceso iSCSI mediante la LIF de datos iSCSI
1015 inbound_4045-4046_tcp	4045-4046 TCP	De cualquiera a cualquiera	Daemon de bloqueo NFS y monitor de estado de red
1016 inbound_4045-4046_udp	4045-4046 UDP	De cualquiera a cualquiera	Daemon de bloqueo NFS y monitor de estado de red
1017 inbound_10000	10000 TCP	De cualquiera a cualquiera	Backup con NDMP
1018 inbound_11104-11105	11104-11105 TCP	De cualquiera a cualquiera	Transferencia de datos de SnapMirror
3000 inbound_deny _all_tcp	Cualquier puerto TCP	De cualquiera a cualquiera	Bloquear el resto del tráfico entrante TCP
3001 inbound_deny _all_udp	Cualquier puerto UDP	De cualquiera a cualquiera	Bloquee el resto del tráfico de entrada UDP
65000 AllowVnetInBound	Cualquier protocolo	VirtualNetwork para VirtualNetwork	Tráfico entrante desde dentro del vnet

Prioridad y nombre	Puerto y protocolo	Origen y destino	Descripción
65001 AllowAzureLoad Balance InBound	Cualquier protocolo	AzureLoadBalancer a cualquiera	Tráfico de datos del balanceador de carga estándar de Azure
65500 DenyAllInBound	Cualquier protocolo	De cualquiera a cualquiera	Bloquear el resto del tráfico entrante

Reglas de entrada para sistemas de alta disponibilidad

Al crear un entorno de trabajo y elegir un grupo de seguridad predefinido, puede optar por permitir el tráfico de una de las siguientes opciones:

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

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

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

Reglas de salida

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

Reglas de salida básicas

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

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

Reglas salientes avanzadas

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

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

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

Servicio	Puerto	Protocolo	Origen	Destino	Específico
AutoSupport	HTTPS	443	LIF de gestión de nodos	support.netapp.com	AutoSupport (HTTPS es la predeterminada)
	HTTP	80	LIF de gestión de nodos	support.netapp.com	AutoSupport (solo si el protocolo de transporte cambia de HTTPS a HTTP)
	TCP	3128	LIF de gestión de nodos	Conector	Envío de mensajes AutoSupport a través de un servidor proxy en el conector, si no hay disponible una conexión a Internet saliente
Backups de configuración	HTTP	80	LIF de gestión de nodos	\Http://<connector-IP-address>/occm/offboxconfig	Enviar copias de seguridad de configuración al conector. "Obtener información acerca de los archivos de copia de seguridad de configuración".
DHCP	68	UDP	LIF de gestión de nodos	DHCP	Cliente DHCP para la configuración inicial
DHCPS	67	UDP	LIF de gestión de nodos	DHCP	Servidor DHCP
DNS	53	UDP	LIF de gestión de nodos y LIF de datos (NFS, CIFS)	DNS	DNS
NDMP	18600–18699	TCP	LIF de gestión de nodos	Servidores de destino	Copia NDMP
SMTP	25	TCP	LIF de gestión de nodos	Servidor de correo	Alertas SMTP, que se pueden utilizar para AutoSupport
SNMP	161	TCP	LIF de gestión de nodos	Servidor de supervisión	Supervisión mediante capturas SNMP
	161	UDP	LIF de gestión de nodos	Servidor de supervisión	Supervisión mediante capturas SNMP
	162	TCP	LIF de gestión de nodos	Servidor de supervisión	Supervisión mediante capturas SNMP
	162	UDP	LIF de gestión de nodos	Servidor de supervisión	Supervisión mediante capturas SNMP
SnapMirror	11104	TCP	LIF entre clústeres	LIF de interconexión de clústeres de ONTAP	Gestión de sesiones de comunicación de interconexión de clústeres para SnapMirror
	11105	TCP	LIF entre clústeres	LIF de interconexión de clústeres de ONTAP	Transferencia de datos de SnapMirror
Syslog	514	UDP	LIF de gestión de nodos	Servidor de syslog	Mensajes de syslog Reenviar

Requisitos para el conector

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

- "Ver los requisitos de red del conector"
- "Reglas de grupos de seguridad en Azure"

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

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

Información general de cifrado de datos

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

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

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

Rotación de la clave

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

Cómo se cifran los datos

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

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

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

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

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

Crear una identidad gestionada asignada por el usuario

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

El recurso tiene el siguiente identificador: `userassignedidentity`.

Pasos

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

Cree un almacén de claves y genere una clave

El almacén de claves debe residir en la misma suscripción a Azure y la misma región en la que esté previsto

crear el sistema Cloud Volumes ONTAP.

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

Pasos

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

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

   - El almacén de claves debe residir en la misma región que el sistema Cloud Volumes ONTAP.
   - Deben habilitarse las siguientes opciones:
     - **Borrado suave** (esta opción está activada de forma predeterminada, pero debe *no* estar desactivada)
     - **Protección de purga**
     - * Azure Disk Encryption para cifrado de volúmenes* (para sistemas de un solo nodo, pares de alta disponibilidad en varias zonas e implementaciones de alta disponibilidad en un solo AZ)

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

   - Se debe activar la siguiente opción si ha creado una identidad gestionada asignada por el usuario:
     - **Política de acceso a Vault**
2. Si seleccionó Política de acceso al almacén, haga clic en Crear para crear una política de acceso para el almacén de claves. Si no es así, vaya al paso 3.
   a. Seleccione los siguientes permisos:
      - obtenga
      - lista
      - descifrar
      - cifrar
      - tecla desajustar
      - tecla ajustar
      - verificación
      - firma
   b. Seleccione la identidad administrada (recurso) asignada por el usuario como principal.
   c. Revise y cree la política de acceso.
3. "Genere una clave en el almacén de claves".

   Tenga en cuenta los siguientes requisitos para la clave:

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

Cree un entorno de trabajo que utilice la clave de cifrado

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

Permisos necesarios

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

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

"Consulte la lista más reciente de permisos"

Pasos

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

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

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

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

   "Obtenga más información acerca de esta llamada API".

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

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

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

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

   "Obtenga más información acerca de esta llamada API".

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

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

      `POST /azure/ha/working-environments`

      El cuerpo de la solicitud debe incluir los siguientes campos:

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

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

"Obtenga más información acerca de esta llamada API".

b. Para un sistema de un solo nodo:

`POST /azure/vsa/working-environments`

El cuerpo de la solicitud debe incluir los siguientes campos:

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

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

"Obtenga más información acerca de esta llamada API".

Resultado

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

Configure las licencias para Cloud Volumes ONTAP en Azure

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

Freemium

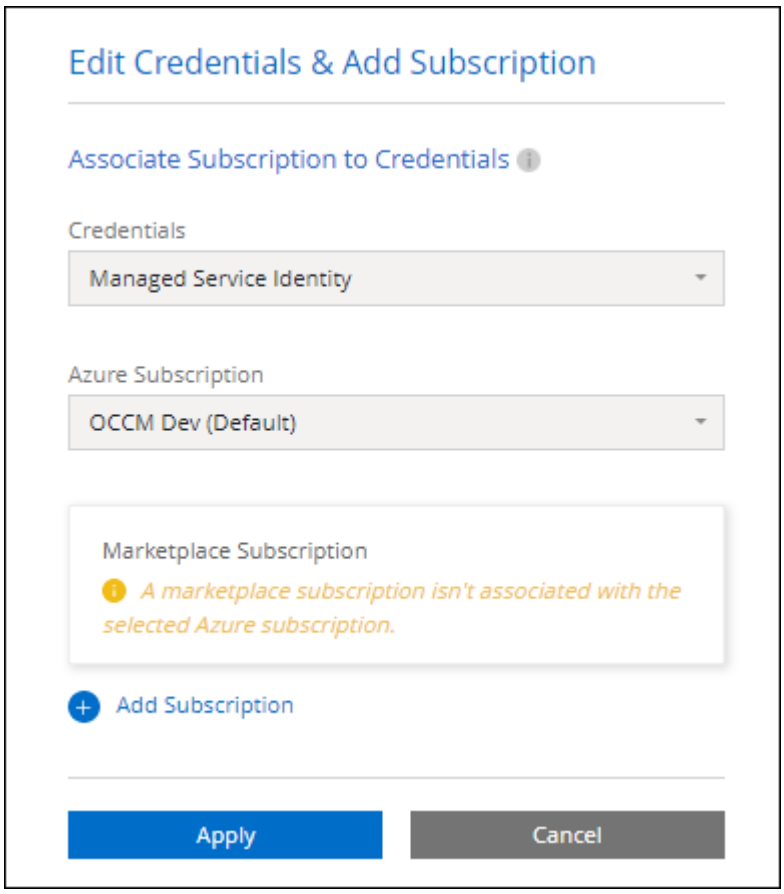
Seleccione la oferta freemium para utilizar Cloud Volumes ONTAP de forma gratuita con hasta 500 GIB de capacidad aprovisionada. "Obtenga más información sobre la oferta de Freemium".

Pasos

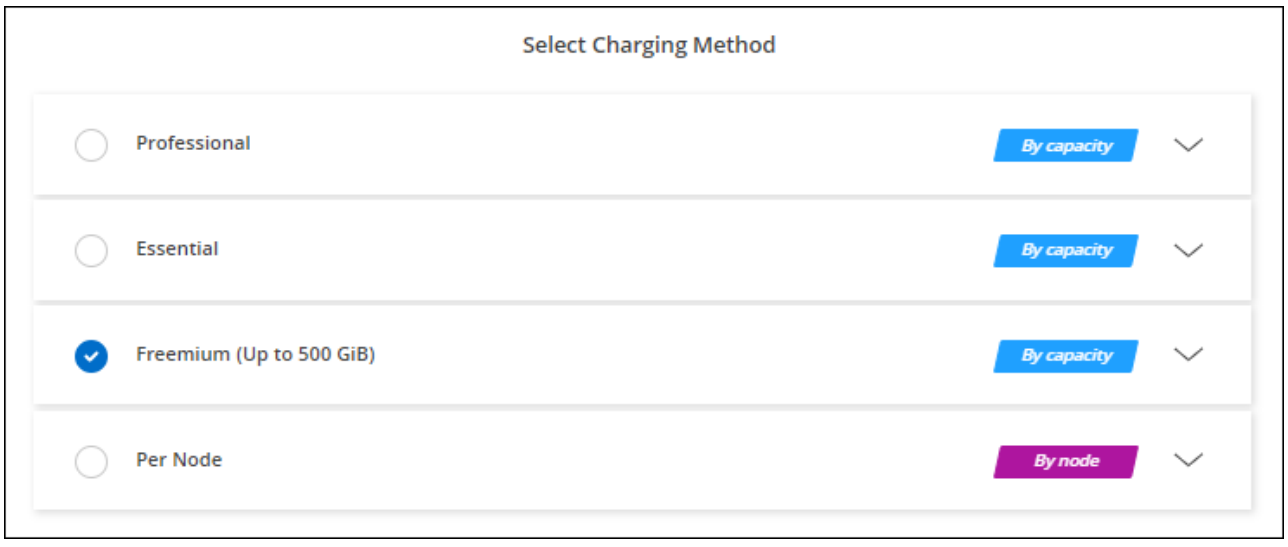
1. En el menú de navegación de la izquierda, selecciona **almacenamiento > Canvas**.
2. En la página Canvas, haga clic en **Agregar entorno de trabajo** y siga los pasos de BlueXP.

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

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



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



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

Licencia basada en capacidad

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

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

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

"Más información sobre las licencias basadas en capacidad".

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

BYOL

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

Pasos

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

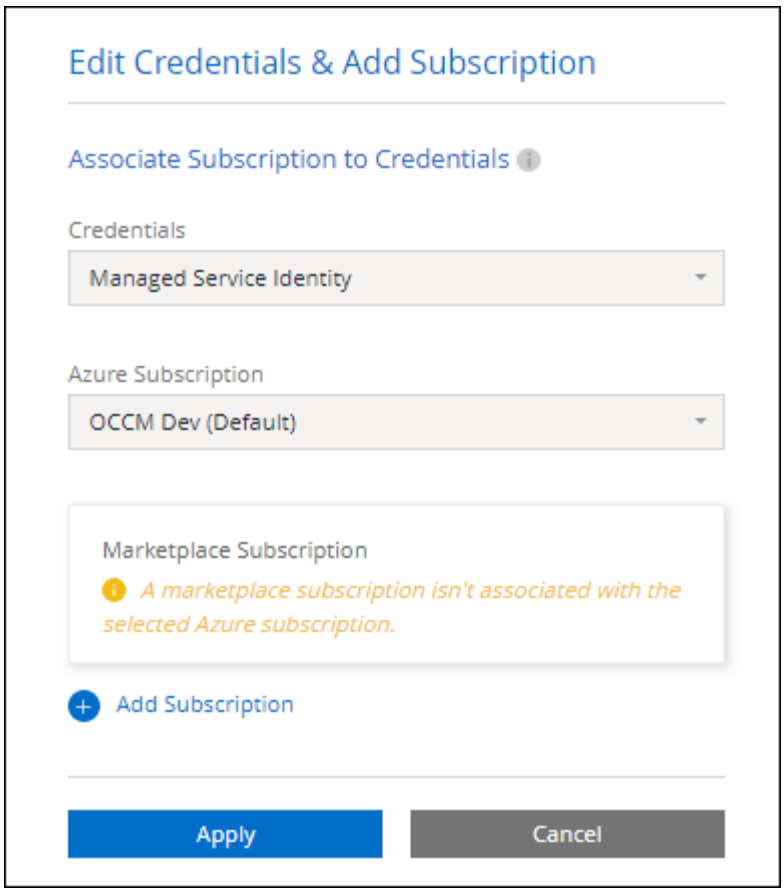
   BlueXP consulta automáticamente al servicio de licencias de NetApp para obtener detalles sobre las licencias asociadas a su cuenta del sitio de soporte de NetApp. Si no se producen errores, BlueXP añade automáticamente las licencias a la cartera digital.

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

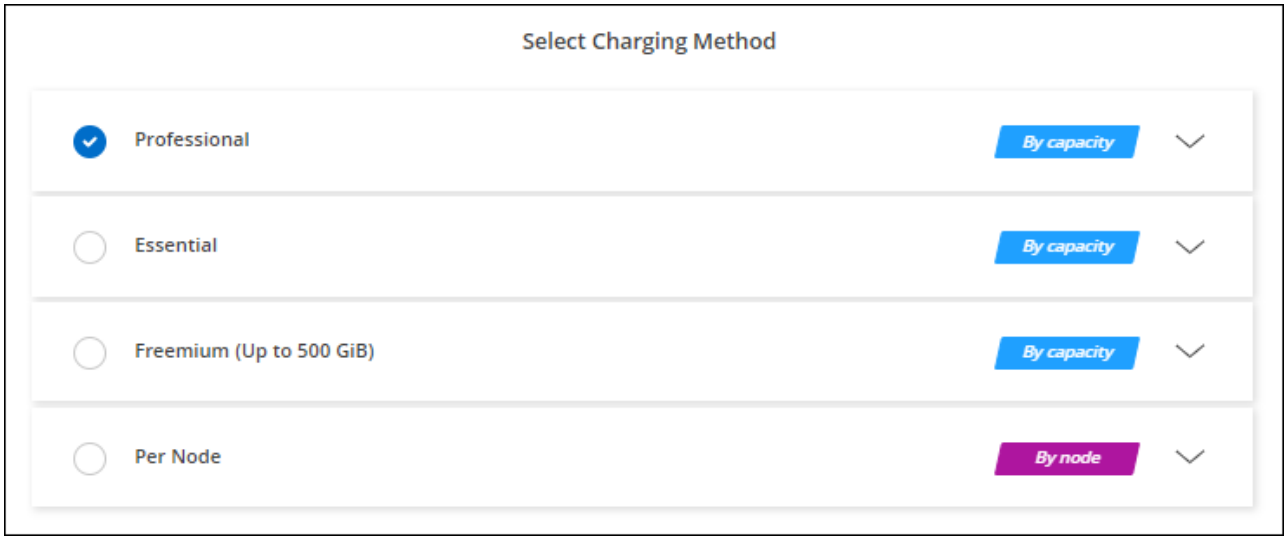
3. En la página Canvas, haga clic en **Agregar entorno de trabajo** y siga los pasos de BlueXP.

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

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



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



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

Suscripción a PAYGO

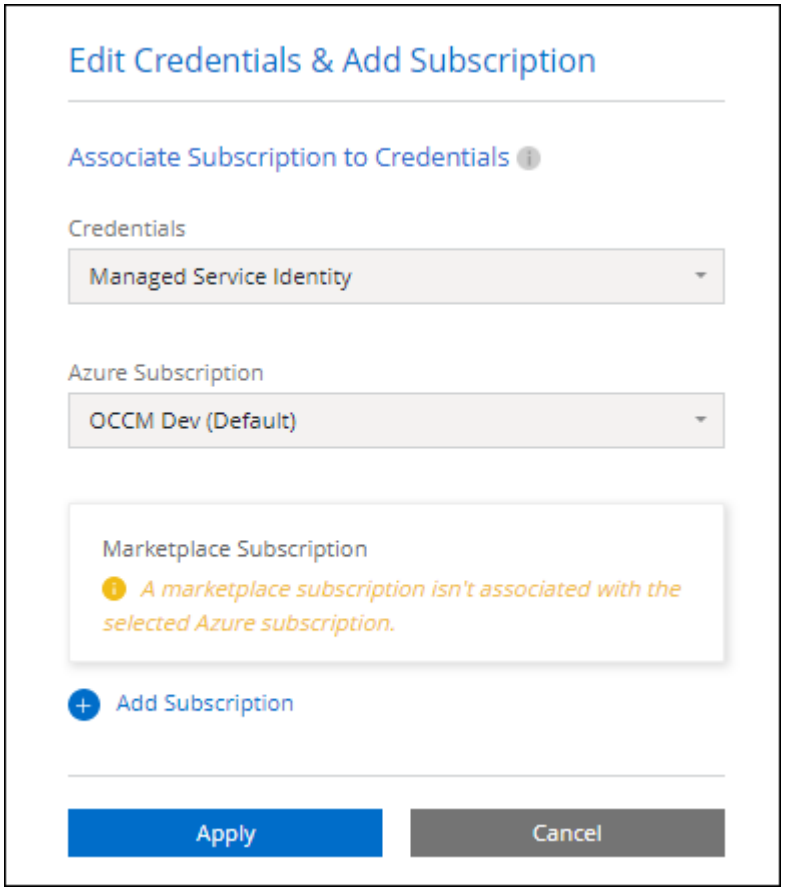
Pague por horas suscribiendo la oferta del mercado de su proveedor de cloud.

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

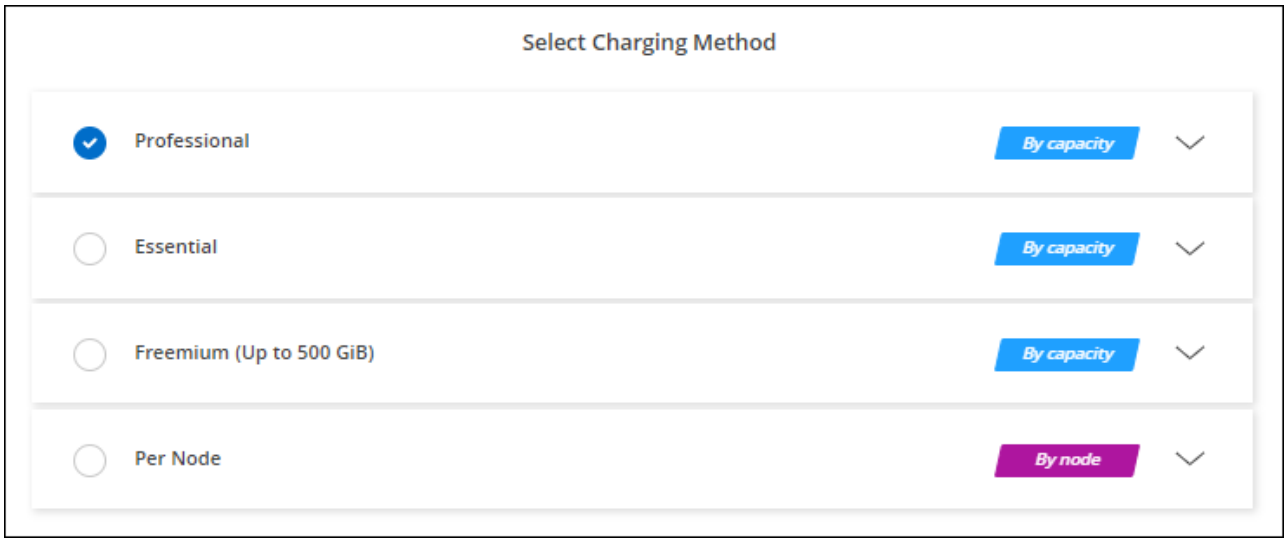
carga. Puede utilizar la misma suscripción para entornos de trabajo adicionales.

Pasos

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



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



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

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

Contrato anual

Pague anualmente por Cloud Volumes ONTAP comprando un contrato anual.

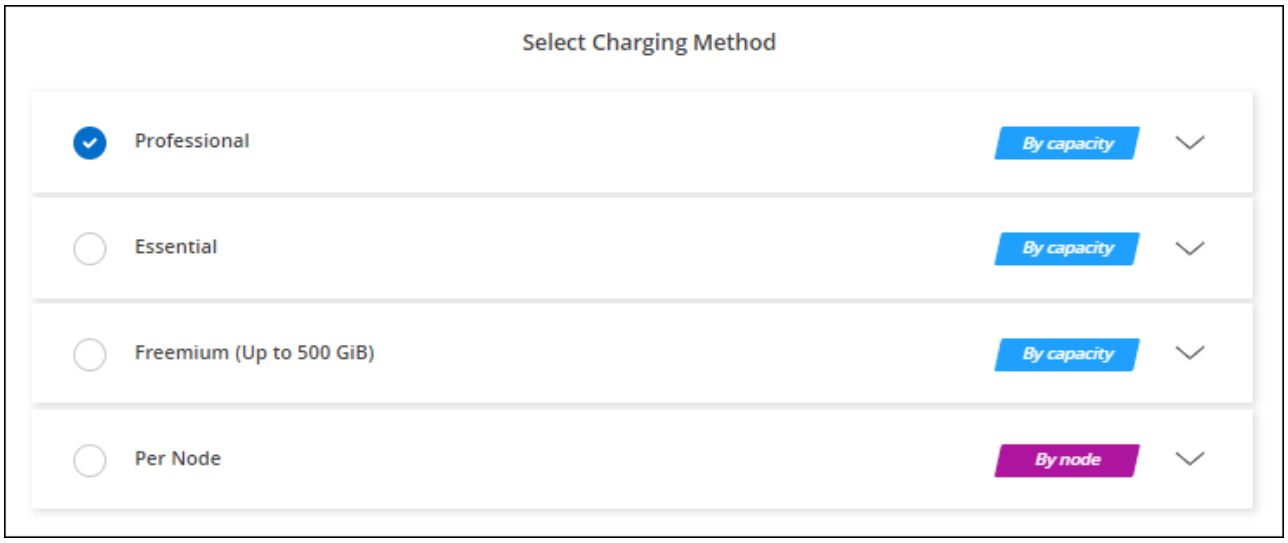
Pasos

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

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

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

2. En la página Canvas, haga clic en **Agregar entorno de trabajo** y siga los pasos de BlueXP.
   a. En la página **Detalles y credenciales**, haga clic en **Editar credenciales > Agregar suscripción > continuar**.
   b. En el portal de Azure, seleccione el plan anual que compartió con su cuenta de Azure y, a continuación, haga clic en **Suscribirse**.
   c. Después de volver a BlueXP, seleccione un paquete basado en la capacidad cuando llegue a la página de métodos de carga.



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

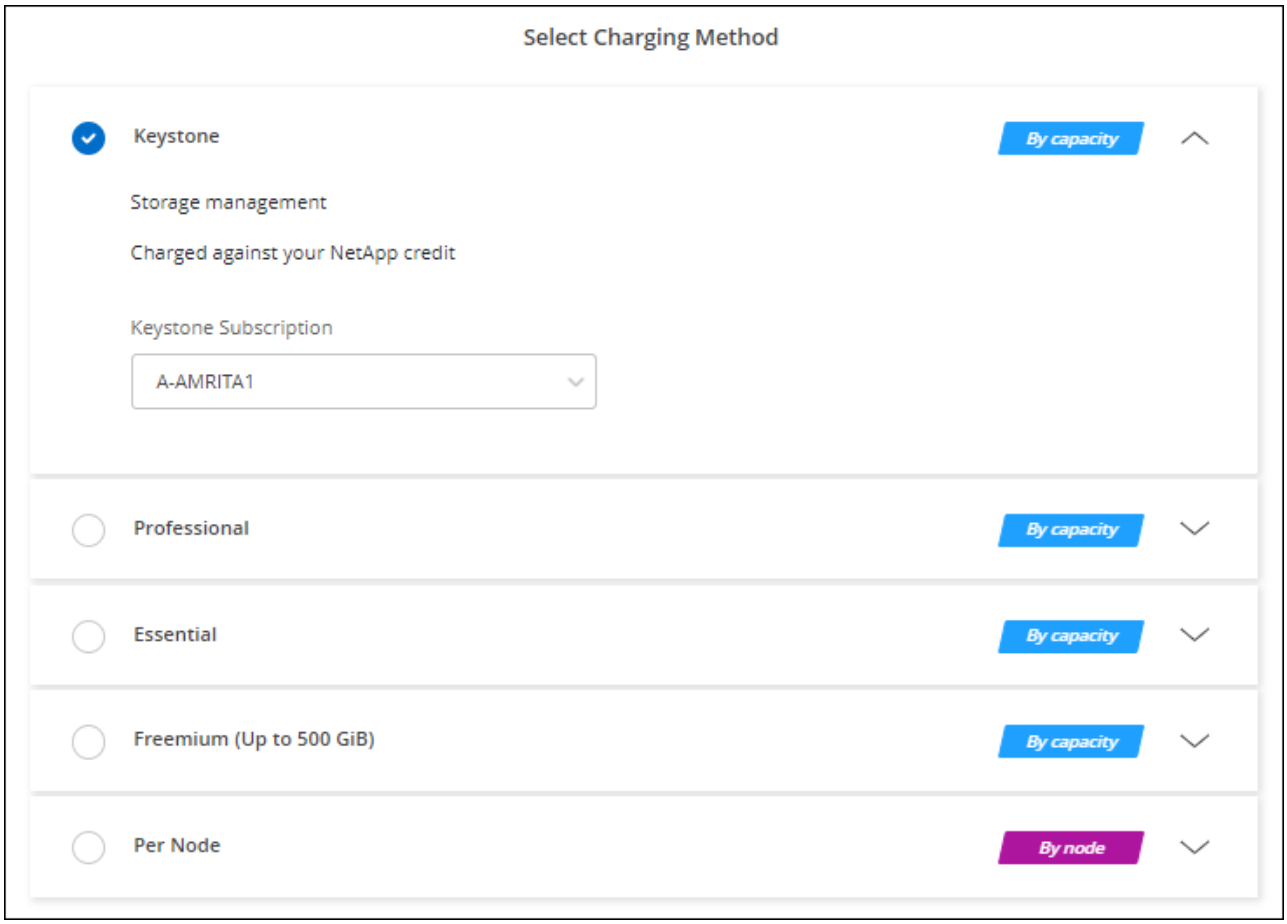
Suscripción a Keystone

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

Pasos

1. Si aún no tiene una suscripción, "Póngase en contacto con NetApp"

2. Mailto:ng-keystone-success@netapp.com[Contactar con NetApp] para autorizar tu cuenta de usuario de BlueXP con una o más suscripciones de Keystone.
3. Una vez que NetApp le autorice a su cuenta, "Vincule sus suscripciones para su uso con Cloud Volumes ONTAP".
4. En la página Canvas, haga clic en **Agregar entorno de trabajo** y siga los pasos de BlueXP.
    a. Seleccione el método de carga de Keystone Subscription cuando se le solicite que elija un método de carga.



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

Habilitar el modo de alta disponibilidad en Azure

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

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

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

Tenga en cuenta lo siguiente:

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

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

Pasos

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

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

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

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

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

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

Activar VMOrchestratorZonalMultiFD para zonas de disponibilidad únicas

Para implementar instancias de VM en zonas de disponibilidad únicas de

almacenamiento redundante local (LRS), debe activar `Microsoft.Compute/VMOrchestratorZonalMultiFD` la función Microsoft para sus suscripciones. En un modo de alta disponibilidad, esta función facilita la puesta en marcha de nodos en dominios de fallo independientes en la misma zona de disponibilidad.

A menos que active esta función, no se producirá el despliegue zonal y se hará efectivo el despliegue no zonal anterior de LRS.

Para obtener más información sobre la puesta en marcha de VM en una zona de disponibilidad única, consulte "Pares de alta disponibilidad en Azure".

Realice estos pasos como usuario con Privileges de propietario:

Pasos

1. Acceda a Azure Cloud Shell desde el portal de Azure. Para obtener más información, consulte "Documentación de Microsoft Azure: Comience a usar Azure Cloud Shell".
2. Regístrese para la `Microsoft.Compute/VMOrchestratorZonalMultiFD` función mediante la ejecución de este comando:

   ```
   az account set -s <Azure_subscription_name_or_ID> az feature register --name VMOrchestratorZonalMultiFD --namespace Microsoft.Compute
   ```

3. Compruebe 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»: «Registered» }, «type»: «Microsoft.features/providers/features» }
   ```

Inicio de Cloud Volumes ONTAP en Azure

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

Lo que necesitará

Necesita lo siguiente para crear un entorno de trabajo.

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

  Debe haber elegido una configuración y obtener información de redes de Azure de su administrador. Para obtener más información, consulte "Planificación de la configuración de Cloud Volumes ONTAP".

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

  "Aprenda a configurar las licencias".

Acerca de esta tarea

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

Potencial de pérdida de datos

La mejor práctica es utilizar un nuevo grupo de recursos dedicado para cada sistema de Cloud Volumes ONTAP.

No se recomienda la implementación de Cloud Volumes ONTAP en un grupo de recursos compartidos existente debido al riesgo de pérdida de datos. Si bien BlueXP puede eliminar recursos de Cloud Volumes ONTAP de un grupo de recursos compartidos en caso de error o eliminación de la implementación, es posible que un usuario de Azure elimine accidentalmente los recursos de Cloud Volumes ONTAP de un grupo de recursos compartidos.

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

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

Pasos

1. En el menú de navegación de la izquierda, selecciona **almacenamiento > Canvas**.
2. en la página Canvas, haga clic en **Agregar entorno de trabajo** y siga las indicaciones.
3. **Elija una ubicación**: Seleccione **Microsoft Azure** y **Cloud Volumes ONTAP Single Node**.
4. Si se le solicita, "Cree un conector".
5. **Detalles y credenciales**: De forma opcional, cambie las credenciales y la suscripción de Azure, especifique un nombre de clúster, añada etiquetas si es necesario y, a continuación, especifique credenciales.

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

Campo	Descripción
Nombre del entorno de trabajo	BlueXP usa el nombre de entorno de trabajo para nombrar tanto el sistema Cloud Volumes ONTAP como la máquina virtual de Azure. También utiliza el nombre como prefijo para el grupo de seguridad predefinido si selecciona esa opción.
Etiquetas del grupo de recursos	Las etiquetas son metadatos para sus recursos de Azure. Cuando introduce etiquetas en este campo, BlueXP las añade al grupo de recursos asociado al sistema Cloud Volumes ONTAP. Puede agregar hasta cuatro etiquetas desde la interfaz de usuario al crear un entorno de trabajo y, a continuación, puede agregar más después de crear. Tenga en cuenta que la API no le limita a cuatro etiquetas al crear un entorno de trabajo. Para obtener información sobre las etiquetas, consulte la "Documentación de Microsoft Azure: Uso de etiquetas para organizar los recursos de Azure".

Campo	Descripción
Nombre de usuario y contraseña	Estas son las credenciales de la cuenta de administrador del clúster de Cloud Volumes ONTAP. Puede usar estas credenciales para conectarse a Cloud Volumes ONTAP a través de ONTAP System Manager o la interfaz de línea de comandos 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 utilizarlo con este sistema de Cloud Volumes ONTAP. Tiene que asociar una suscripción a Azure Marketplace con la suscripción de Azure seleccionada para poner en marcha un sistema Cloud Volumes ONTAP de pago por uso. "Aprenda a añadir credenciales".

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

Suscríbete a BlueXP desde Azure Marketplace

6. **Servicios**: Habilita o deshabilita los servicios individuales que quieres o no quieres usar con Cloud Volumes ONTAP.
   - "Más información sobre la clasificación de BlueXP"
   - "Más información sobre el backup y la recuperación de datos de BlueXP"

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

7. **Ubicación**: Seleccione una región, zona de disponibilidad, vnet y subred y, a continuación, active la casilla de verificación para confirmar la conectividad de red entre el conector y la ubicación de destino.
8. **Conectividad**: Elija un grupo de recursos nuevo o existente y, a continuación, elija si desea utilizar el grupo de seguridad predefinido o si desea utilizar el suyo.

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

Campo	Descripción
Grupo de recursos	Crear un nuevo grupo de recursos para Cloud Volumes ONTAP o utilizar un grupo de recursos existente. La mejor práctica es utilizar un nuevo grupo de recursos dedicado para Cloud Volumes ONTAP. Aunque es posible implementar Cloud Volumes ONTAP en un grupo de recursos compartidos existente, no se recomienda debido al riesgo de pérdida de datos. Consulte la advertencia anterior para obtener más detalles. Si la cuenta de Azure que está utilizando tiene el "permisos necesarios", BlueXP quita los recursos de Cloud Volumes ONTAP de un grupo de recursos, en caso de error o eliminación de la implementación.

Campo	Descripción
Grupo de seguridad generado	Si deja que BlueXP genere el grupo de seguridad para usted, debe elegir cómo permitirá el tráfico: • Si selecciona **sólo vnet seleccionado**, el origen del tráfico entrante es el intervalo de subred del vnet seleccionado y el rango de subred del vnet donde reside el conector. Esta es la opción recomendada. • Si elige **All VNets**, el origen del tráfico entrante es el intervalo IP 0.0.0.0/0.
Utilice la existente	Si elige un grupo de seguridad existente, este debe cumplir con los requisitos de Cloud Volumes ONTAP. "Consulte el grupo de seguridad predeterminado".

9. **Métodos de carga y cuenta de NSS**: Especifique la opción de carga que desea utilizar con este sistema y, a continuación, especifique una cuenta en la página de soporte de NetApp.
   - "Obtenga información sobre las opciones de licencia para Cloud Volumes ONTAP".
   - "Aprenda a configurar las licencias".
10. **Paquetes preconfigurados**: Seleccione uno de los paquetes para implementar rápidamente un sistema Cloud Volumes ONTAP, o haga clic en **Crear mi propia configuración**.

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

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

    Si hay disponible una versión más reciente de Release Candidate, General Availability o Patch para la versión seleccionada, BlueXP actualiza el sistema a esa versión al crear el entorno de trabajo. Por ejemplo, la actualización se produce si selecciona Cloud Volumes ONTAP 9.13.1 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.

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

    Tenga en cuenta lo siguiente:

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

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

    - Se puede elegir una política de organización en niveles de volumen específica cuando se crea o se

edita un volumen.

- Si deshabilita la organización en niveles de datos, puede habilitarla en agregados posteriores.

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

14. **Escribir velocidad y GUSANO**:

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

       "Más información sobre la velocidad de escritura".

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

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

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

    "Más información acerca del almacenamiento WORM".

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

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

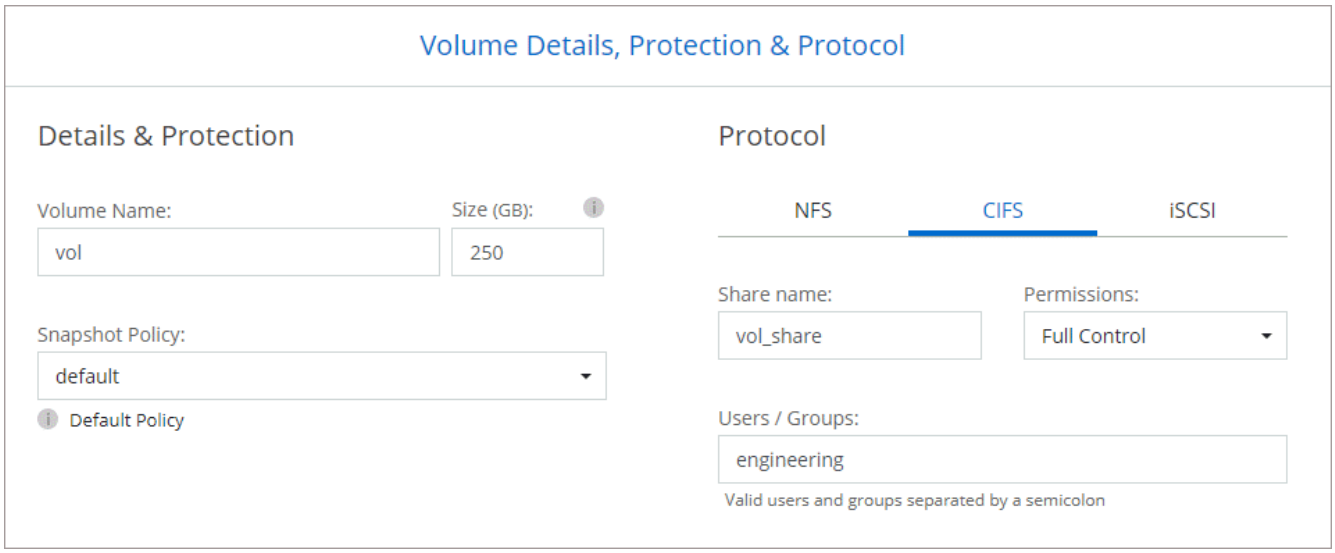
    "Obtenga información sobre las versiones y los protocolos de cliente compatibles".

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

Campo	Descripción
Tamaño	El tamaño máximo que puede introducir depende en gran medida de si habilita thin provisioning, lo que le permite crear un volumen que sea mayor que el almacenamiento físico que hay disponible actualmente.
Control de acceso (solo para NFS)	Una política de exportación define los clientes de la subred que pueden acceder al volumen. De forma predeterminada, BlueXP introduce un valor que proporciona acceso a todas las instancias de la subred.
Permisos y usuarios/grupos (solo para CIFS)	Estos campos permiten controlar el nivel de acceso a un recurso compartido para usuarios y grupos (también denominados listas de control de acceso o ACL). Es posible especificar usuarios o grupos de Windows locales o de dominio, o usuarios o grupos de UNIX. Si especifica un nombre de usuario de Windows de dominio, debe incluir el dominio del usuario con el formato domain\username.
Política de Snapshot	Una política de copia de Snapshot especifica la frecuencia y el número de copias de Snapshot de NetApp creadas automáticamente. Una copia snapshot de NetApp es una imagen del sistema de archivos puntual que no afecta al rendimiento y requiere un almacenamiento mínimo. Puede elegir la directiva predeterminada o ninguna. Es posible que no elija ninguno para los datos transitorios: Por ejemplo, tempdb para Microsoft SQL Server.

Campo	Descripción
Opciones avanzadas (solo para NFS)	Seleccione una versión de NFS para el volumen: NFSv3 o NFSv4.
Grupo del iniciador y IQN (solo para iSCSI)	Los destinos de almacenamiento iSCSI se denominan LUN (unidades lógicas) y se presentan a los hosts como dispositivos de bloque estándar. Los iGroups son tablas de los nombres de los nodos de host iSCSI y controlan qué iniciadores tienen acceso a qué LUN. Los destinos iSCSI se conectan a la red a través de adaptadores de red Ethernet (NIC) estándar, tarjetas DEL motor de descarga TCP (TOE) con iniciadores de software, adaptadores de red convergente (CNA) o adaptadores de host de salida dedicados (HBA) y se identifican mediante nombres cualificados de iSCSI (IQN). Cuando se crea un volumen iSCSI, BlueXP crea automáticamente una LUN para usted. Lo hemos hecho sencillo creando sólo una LUN por volumen, por lo que no hay que realizar ninguna gestión. Después de crear el volumen, "Utilice el IQN para conectarse con la LUN del hosts".

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



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

Campo	Descripción
DNS Dirección IP principal y secundaria	Las direcciones IP de los servidores DNS que proporcionan resolución de nombres para el servidor CIFS. Los servidores DNS enumerados deben contener los registros de ubicación de servicio (SRV) necesarios para localizar los servidores LDAP de Active Directory y los controladores de dominio del dominio al que se unirá el servidor CIFS.
Dominio de Active Directory al que unirse	El FQDN del dominio de Active Directory (AD) al que desea que se una el servidor CIFS.
Credenciales autorizadas para unirse al dominio	Nombre y contraseña de una cuenta de Windows con privilegios suficientes para agregar equipos a la unidad organizativa (OU) especificada dentro del dominio AD.
Nombre NetBIOS del servidor CIFS	Nombre de servidor CIFS que es único en el dominio de AD.

Campo	Descripción
Unidad organizacional	La unidad organizativa del dominio AD para asociarla con el servidor CIFS. El valor predeterminado es CN=Computers. Para configurar los Servicios de dominio de Azure AD como servidor AD para Cloud Volumes ONTAP, debe introducir **OU=equipos ADDC** o **OU=usuarios ADDC** en este campo.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Documentación de Azure: Cree una unidad organizativa (OU) en un dominio gestionado de Azure AD Domain Services"^]
Dominio DNS	El dominio DNS para la máquina virtual de almacenamiento (SVM) de Cloud Volumes ONTAP. En la mayoría de los casos, el dominio es el mismo que el dominio de AD.
Servidor NTP	Seleccione **usar dominio de Active Directory** para configurar un servidor NTP mediante el DNS de Active Directory. Si necesita configurar un servidor NTP con una dirección diferente, debe usar la API. Consulte la "Documentos de automatización de BlueXP" para obtener más información. Tenga en cuenta que solo puede configurar un servidor NTP cuando cree un servidor CIFS. No se puede configurar después de crear el servidor CIFS.

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

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

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

Resultado

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

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

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

Después de terminar

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

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

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

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

Pasos

1. En el menú de navegación de la izquierda, selecciona **almacenamiento > Canvas**.
2. en la página Canvas, haga clic en **Agregar entorno de trabajo** y siga las indicaciones.
3. Si se le solicita, "Cree un conector".
4. **Detalles y credenciales**: De forma opcional, cambie las credenciales y la suscripción de Azure, especifique un nombre de clúster, añada etiquetas si es necesario y, a continuación, especifique credenciales.

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

Campo	Descripción
Nombre del entorno de trabajo	BlueXP usa el nombre de entorno de trabajo para nombrar tanto el sistema Cloud Volumes ONTAP como la máquina virtual de Azure. También utiliza el nombre como prefijo para el grupo de seguridad predefinido si selecciona esa opción.
Etiquetas del grupo de recursos	Las etiquetas son metadatos para sus recursos de Azure. Cuando introduce etiquetas en este campo, BlueXP las añade al grupo de recursos asociado al sistema Cloud Volumes ONTAP. Puede agregar hasta cuatro etiquetas desde la interfaz de usuario al crear un entorno de trabajo y, a continuación, puede agregar más después de crear. Tenga en cuenta que la API no le limita a cuatro etiquetas al crear un entorno de trabajo. Para obtener información sobre 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 de 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 interfaz de línea de comandos 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 utilizarlo con este sistema de Cloud Volumes ONTAP. Tiene que asociar una suscripción a Azure Marketplace con la suscripción de Azure seleccionada para poner en marcha un sistema Cloud Volumes ONTAP de pago por uso. "Aprenda a añadir credenciales".

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

   Suscríbete a BlueXP desde Azure Marketplace

5. **Servicios**: Habilita o deshabilita los servicios individuales en función de si quieres usarlos con Cloud Volumes ONTAP.
   - "Más información sobre la clasificación de BlueXP"
   - "Más información sobre el backup y la recuperación de datos de BlueXP"

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

6. **Modelos de despliegue de alta disponibilidad**:
   a. Seleccione **Zona de disponibilidad única** o **Zona de disponibilidad múltiple**.
      - Para zonas de disponibilidad únicas, seleccione una región de Azure, una zona de disponibilidad, vnet y una subred.

        A partir de Cloud Volumes ONTAP 9.15.1, puede poner en marcha instancias de máquinas virtuales (VM) en modo HA en zonas de disponibilidad única (AZs) en Azure. Debe seleccionar una zona y una región que soporten este despliegue. Si la zona o la región no admiten el despliegue zonal, se sigue el modo de despliegue no zonal anterior para LRS. Para conocer las configuraciones compatibles para discos gestionados compartidos, consulte "Configuración DE zona de disponibilidad única DE ALTA DISPONIBILIDAD con discos gestionados compartidos".

      - Para varias zonas de disponibilidad, seleccione una región, vnet, subred, zona para el nodo 1 y zona para el nodo 2.
   b. Active la casilla de verificación **he verificado la conectividad de red…**.
7. **Conectividad**: Elija un grupo de recursos nuevo o existente y, a continuación, elija si desea utilizar el grupo de seguridad predefinido o si desea utilizar el suyo.

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

Campo	Descripción
Grupo de recursos	Crear un nuevo grupo de recursos para Cloud Volumes ONTAP o utilizar un grupo de recursos existente. La mejor práctica es utilizar un nuevo grupo de recursos dedicado para Cloud Volumes ONTAP. Aunque es posible implementar Cloud Volumes ONTAP en un grupo de recursos compartidos existente, no se recomienda debido al riesgo de pérdida de datos. Consulte la advertencia anterior para obtener más detalles. Tiene que utilizar un grupo de recursos dedicado para cada par de alta disponibilidad de Cloud Volumes ONTAP que implemente en Azure. Solo se admite un par de alta disponibilidad en un grupo de recursos. BlueXP experimenta problemas de conexión si intenta implementar un segundo par de alta disponibilidad de Cloud Volumes ONTAP en un grupo de recursos de Azure. Si la cuenta de Azure que está utilizando tiene el "permisos necesarios", BlueXP quita los recursos de Cloud Volumes ONTAP de un grupo de recursos, en caso de error o eliminación de la implementación.

Campo	Descripción
Grupo de seguridad generado	Si deja que BlueXP genere el grupo de seguridad para usted, debe elegir cómo permitirá el tráfico: • Si selecciona **sólo vnet seleccionado**, el origen del tráfico entrante es el intervalo de subred del vnet seleccionado y el rango de subred del vnet donde reside el conector. Esta es la opción recomendada. • Si elige **All VNets**, el origen del tráfico entrante es el intervalo IP 0.0.0.0/0.
Utilice la existente	Si elige un grupo de seguridad existente, este debe cumplir con los requisitos de Cloud Volumes ONTAP. "Consulte el grupo de seguridad predeterminado".

8. **Métodos de carga y cuenta de NSS**: Especifique la opción de carga que desea utilizar con este sistema y, a continuación, especifique una cuenta en la página de soporte de NetApp.
   - "Obtenga información sobre las opciones de licencia para Cloud Volumes ONTAP".
   - "Aprenda a configurar las licencias".
9. **Paquetes preconfigurados**: Seleccione uno de los paquetes para implementar rápidamente un sistema Cloud Volumes ONTAP, o haga clic en **Cambiar configuración**.

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

    Si hay disponible una versión más reciente de Release Candidate, General Availability o Patch para la versión seleccionada, BlueXP actualiza el sistema a esa versión al crear el entorno de trabajo. Por ejemplo, la actualización se produce si selecciona Cloud Volumes ONTAP 9.13.1 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 al mercado de Azure**: Siga los pasos si BlueXP no pudo permitir la implementación programática de Cloud Volumes ONTAP.
12. **Recursos de almacenamiento subyacentes**: Elija la configuración para el agregado inicial: Un tipo de disco, un tamaño para cada disco y si se debe habilitar la organización en niveles de datos para el almacenamiento BLOB.

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

      Para obtener ayuda para elegir un tamaño de disco, consulte "Configure el tamaño de su sistema en Azure".
    - Se puede elegir una política de organización en niveles de volumen específica cuando se crea o se edita un volumen.
    - Si deshabilita la organización en niveles de datos, puede habilitarla en agregados posteriores.

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

13. **Escribir velocidad y GUSANO**:

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

       "Más información sobre la velocidad de escritura".

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

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

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

    "Más información acerca del almacenamiento WORM".

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

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

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

    "Más información acerca del almacenamiento WORM".

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

    "Más información acerca del almacenamiento WORM".

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

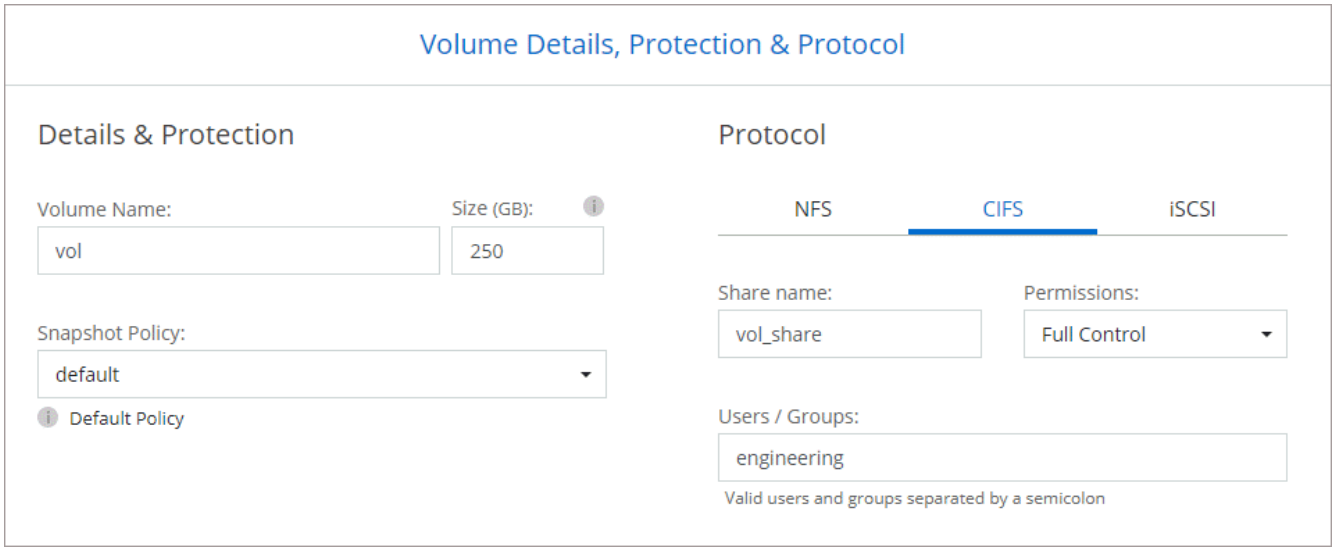
    "Obtenga información sobre las versiones y los protocolos de cliente compatibles".

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

Campo	Descripción
Tamaño	El tamaño máximo que puede introducir depende en gran medida de si habilita thin provisioning, lo que le permite crear un volumen que sea mayor que el almacenamiento físico que hay disponible actualmente.
Control de acceso (solo para NFS)	Una política de exportación define los clientes de la subred que pueden acceder al volumen. De forma predeterminada, BlueXP introduce un valor que proporciona acceso a todas las instancias de la subred.

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

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



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

Campo	Descripción
DNS Dirección IP principal y secundaria	Las direcciones IP de los servidores DNS que proporcionan resolución de nombres para el servidor CIFS. Los servidores DNS enumerados deben contener los registros de ubicación de servicio (SRV) necesarios para localizar los servidores LDAP de Active Directory y los controladores de dominio del dominio al que se unirá el servidor CIFS.
Dominio de Active Directory al que unirse	El FQDN del dominio de Active Directory (AD) al que desea que se una el servidor CIFS.
Credenciales autorizadas para unirse al dominio	Nombre y contraseña de una cuenta de Windows con privilegios suficientes para agregar equipos a la unidad organizativa (OU) especificada dentro del dominio AD.
Nombre NetBIOS del servidor CIFS	Nombre de servidor CIFS que es único en el dominio de AD.
Unidad organizacional	La unidad organizativa del dominio AD para asociarla con el servidor CIFS. El valor predeterminado es CN=Computers. Para configurar los Servicios de dominio de Azure AD como servidor AD para Cloud Volumes ONTAP, debe introducir **OU=equipos ADDC** o **OU=usuarios ADDC** en este campo.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Documentación de Azure: Cree una unidad organizativa (OU) en un dominio gestionado de Azure AD Domain Services"^]
Dominio DNS	El dominio DNS para la máquina virtual de almacenamiento (SVM) de Cloud Volumes ONTAP. En la mayoría de los casos, el dominio es el mismo que el dominio de AD.
Servidor NTP	Seleccione **usar dominio de Active Directory** para configurar un servidor NTP mediante el DNS de Active Directory. Si necesita configurar un servidor NTP con una dirección diferente, debe usar la API. Consulte la "Documentos de automatización de BlueXP" para obtener más información. Tenga en cuenta que solo puede configurar un servidor NTP cuando cree un servidor CIFS. No se puede configurar después de crear el servidor CIFS.

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

    Para obtener más información, consulte "Seleccione un perfil de uso de volumen" y. "Información general sobre organización en niveles de datos"

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

Resultado

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

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

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

Después de terminar

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

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

Verificación de imagen de la plataforma Azure

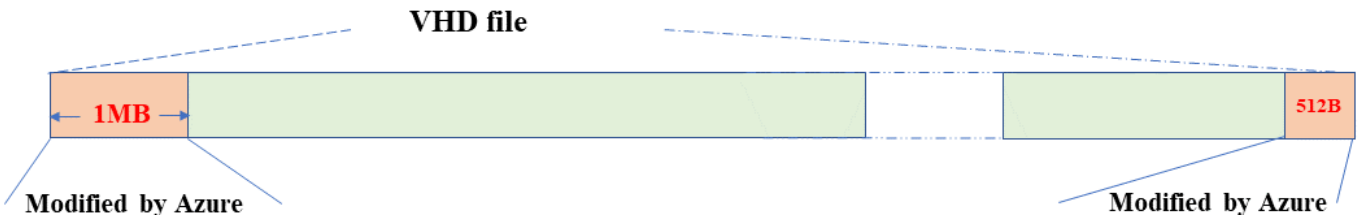
Información general sobre la verificación de imágenes de Azure

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

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

Modificación de Azure de los archivos VHD publicados

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



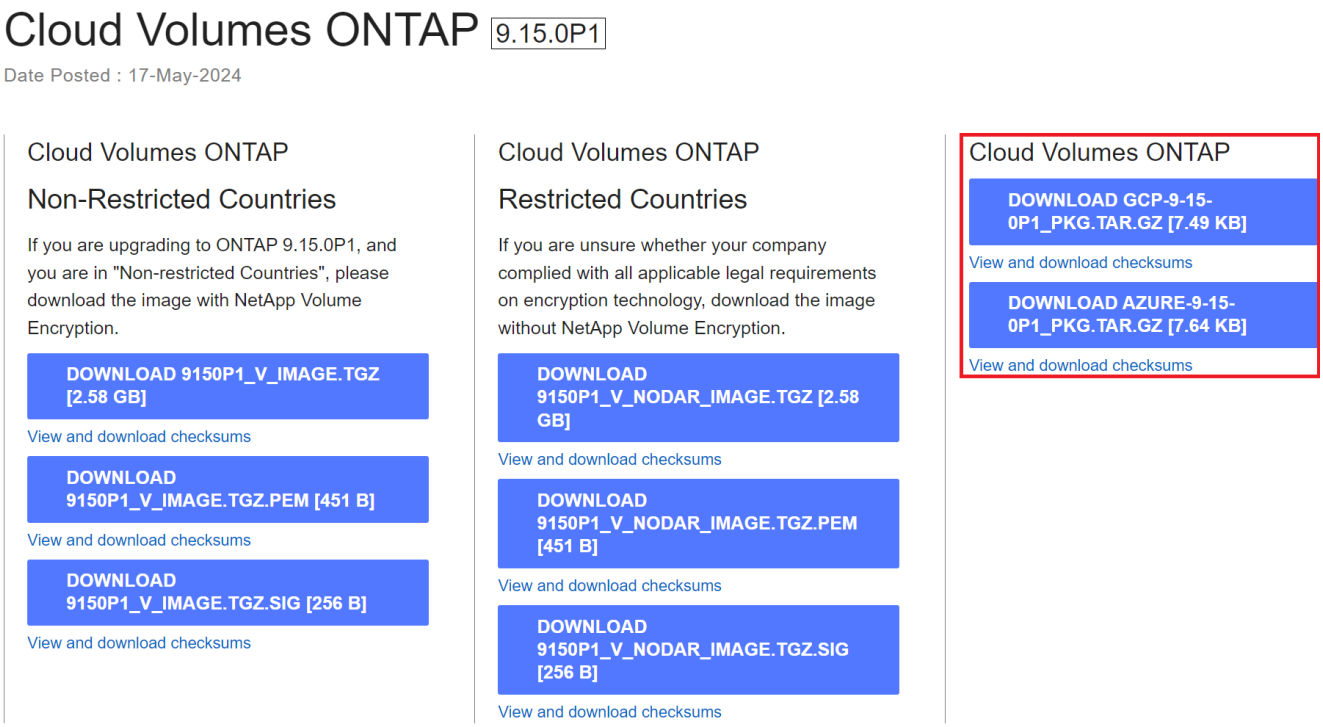
Como ejemplo, el diagrama anterior muestra un archivo VHD con un tamaño de 10GB MB. Pero la porción firmada de NetApp está marcada en verde con un tamaño de 10GB - 1MB - 512B.

Descargue Azure Image Digest File

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

Pasos

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



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

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

Lista de resultados de untar tar.gz archivo

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

Exportación de imágenes desde Azure Marketplace

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

Lo que necesitará

Debe instalar los programas necesarios en su sistema.

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

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

Pasos

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Haga clic para mostrar

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

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

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

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

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

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

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

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

Haga clic para mostrar

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

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

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

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

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

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

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

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

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

```
    },
....

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

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

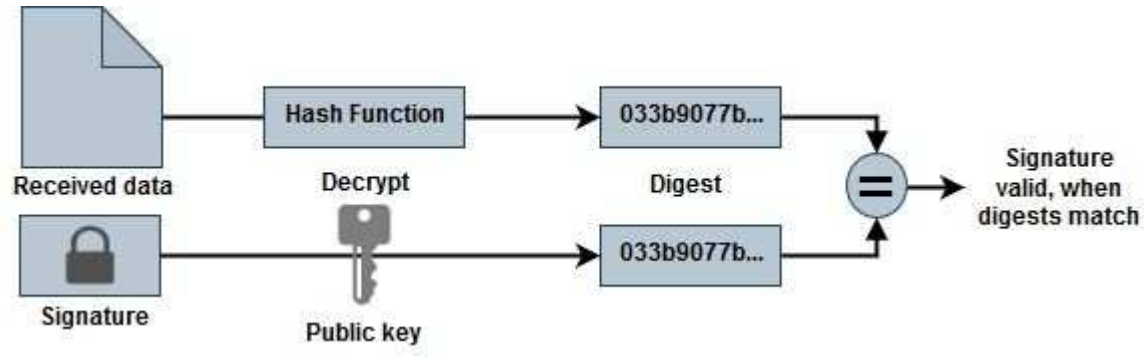
Verificación de firma de archivo

Verificación de firma de archivo

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

Resumen del flujo de trabajo de verificación de firmas de archivos

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



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

  Consulte "Descargue Azure Image Digest File" si desea obtener más información.

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

  Este paso se logra a través del siguiente comando openssl.

  - La sentencia CLI general aparece de la siguiente manera:

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

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

Verificación de firma de archivo en Linux

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

Pasos

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

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

2. Verifique la cadena de confianza.

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

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

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

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

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

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

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

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

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

5. Limpie el espacio de trabajo.

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

Verificación de firma de archivo en Mac OS

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

Pasos

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

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

2. Verifique la cadena de confianza.

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

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

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

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

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

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

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

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

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

5. Limpie el espacio de trabajo.

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

Dónde encontrar información adicional sobre la verificación de imágenes de Azure

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

Referencias

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

Información de copyright

Información de la marca comercial