Empiece a usar Azure

Cloud Manager 3.8

NetApp
March 25, 2024

Tabla de contenidos

Empiece a usar Azure

Introducción a Cloud Volumes ONTAP para Azure

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

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".

Al crear el primer entorno de trabajo de Cloud Volumes ONTAP, Cloud Manager le solicitará que implemente un conector si aún no lo tiene.

Planificación de la configuración

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

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 saliente a Internet desde la red virtual de destino para que el conector y Cloud Volumes ONTAP puedan ponerse en contacto con varios puntos finales.

   Este paso es importante porque el conector no puede administrar Cloud Volumes ONTAP sin acceso saliente a Internet. Si necesita limitar la conectividad saliente, consulte la lista de puntos finales para "El conector y Cloud Volumes ONTAP".

"Obtenga más información sobre los requisitos de red".

Inicie Cloud Volumes ONTAP mediante Cloud Manager

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

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

Planificar 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 un tipo de licencia

Cloud Volumes ONTAP está disponible en dos opciones de precios: De pago por uso y con su propia licencia (BYOL). En el modelo de pago por uso, puede elegir entre tres licencias: Explorar, Standard o Premium. Cada licencia proporciona distintas opciones de computación y capacidad.

"Configuraciones compatibles para Cloud Volumes ONTAP 9.7 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 9.7 en Azure"

Ajuste de 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

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

Los sistemas HA utilizan Blobs de página Premium. Mientras tanto, los sistemas de un solo nodo pueden usar dos tipos de discos gestionados de Azure:

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

reducir sus costes.

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

Tamaño de disco de Azure

Al iniciar las instancias de Cloud Volumes ONTAP, debe elegir el tamaño de disco predeterminado para los agregados. Cloud Manager utiliza este tamaño de disco para el agregado inicial y para cualquier agregado adicional que cree cuando utilice la opción de aprovisionamiento simple. Puede crear agregados 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, elegir discos de 1 TB puede proporcionar un mejor rendimiento que los discos de 500 GB a un coste mayor.

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"

Elegir una configuración compatible con Flash Cache

Una configuración de Cloud Volumes ONTAP en Azure incluye almacenamiento NVMe local, que Cloud Volumes ONTAP utiliza como *Flash Cache* para mejorar el rendimiento. "Obtenga más información sobre Flash Cache".

Hoja de trabajo de información de red de Azure

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)	

Elegir una velocidad de escritura

Cloud Manager le permite elegir una configuración de velocidad de escritura para sistemas Cloud Volumes ONTAP de un solo nodo. 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.

Diferencia entre la velocidad de escritura normal y la alta velocidad de escritura

Al elegir la velocidad de escritura normal, los datos se escriben directamente en el disco, lo que reduce la probabilidad de que se pierdan los datos en caso de que se produzca una interrupción del servicio no planificada del sistema.

Al elegir una alta velocidad de escritura, los datos se guardan en búfer en la memoria antes de que se escriban en el disco, lo que proporciona un rendimiento de escritura más rápido. Gracias al almacenamiento en caché, existe la posibilidad de perder datos en caso de que se produzca una interrupción no planificada del sistema.

La cantidad de datos que se pueden perder en caso de una interrupción imprevista del sistema es el plazo de dos últimos puntos de coherencia. Un punto de coherencia es el acto de escribir datos en el búfer en el disco. Un punto de coherencia se produce cuando el registro de escritura está completo o después de 10 segundos (lo que ocurra primero). Sin embargo, el rendimiento del volumen de AWS EBS puede afectar el tiempo de procesamiento del punto de consistencia.

Cuándo utilizar alta velocidad de escritura

La alta velocidad de escritura es una buena opción si es necesario un rendimiento de escritura rápido para su carga de trabajo, y puede resistir el riesgo de pérdida de datos en caso de una interrupción del servicio del sistema no planificada.

Recomendaciones cuando se utiliza una alta velocidad de escritura

Si habilita una alta velocidad de escritura, debe garantizar la protección de escritura en la capa de la aplicación.

Selección de 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 Cloud Manager, puede seleccionar un perfil que habilite estas funciones o un perfil que las deshabilite. 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 poner en marcha y gestionar Cloud Volumes ONTAP en Azure

Configure sus redes de Azure para que los sistemas Cloud Volumes ONTAP funcionen correctamente. Esto incluye la conexión a redes para el conector y Cloud Volumes ONTAP.

Requisitos para Cloud Volumes ONTAP

Los siguientes requisitos de red deben satisfacerse en Azure.

Acceso saliente a Internet para Cloud Volumes ONTAP

Cloud Volumes ONTAP requiere acceso saliente a Internet para enviar mensajes a NetApp AutoSupport, que supervisa proactivamente el estado del almacenamiento.

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

"Aprenda a configurar AutoSupport".

Grupos de seguridad

No necesita crear grupos de seguridad porque Cloud Manager lo hace por usted. Si necesita utilizar el suyo propio, consulte las reglas de grupo de seguridad que se enumeran a continuación.

Número de direcciones IP

Cloud Manager asigna el siguiente número de direcciones IP a Cloud Volumes ONTAP en Azure:

- Nodo único: Direcciones IP de 5
- Par DE ALTA DISPONIBILIDAD: 16 direcciones IP

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

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.

Conexión de Cloud Volumes ONTAP a Azure Blob Storage para organización en niveles de los datos

Si desea organizar en niveles datos fríos en almacenamiento de Azure Blob, no necesita configurar una conexión entre el nivel de rendimiento y el nivel de capacidad mientras Cloud Manager tenga los permisos necesarios Cloud Manager habilita un extremo de servicio vnet para usted si la política de Cloud Manager tiene estos permisos:

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

Estos permisos se incluyen en el último "Política de Cloud Manager".

Para obtener más información sobre la configuración de la organización en niveles de datos, consulte "Organización en niveles de los datos inactivos en almacenamiento de objetos de bajo coste".

Conexiones a sistemas ONTAP en otras redes

Para replicar datos entre un sistema Cloud Volumes ONTAP en Azure y sistemas ONTAP en otras redes, debe tener una conexión VPN entre el vnet de Azure y la otra red, por ejemplo, un VPC de AWS o una red de su empresa.

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

Requisitos para el conector

Configure su red de modo que el conector pueda gestionar recursos y procesos en su entorno de cloud público. El paso más importante es garantizar el acceso saliente a Internet a varios puntos finales.

Si la red utiliza un servidor proxy para toda la comunicación a Internet, puede especificar el servidor proxy en la página Configuración. Consulte "Configuración del conector para utilizar un servidor proxy".

Conexiones a redes de destino

Un conector requiere una conexión de red a los VPC y VNets en los que desea implementar Cloud Volumes ONTAP.

Por ejemplo, si instala un conector en la red corporativa, debe configurar una conexión VPN al VPC o a vnet en el que inicie Cloud Volumes ONTAP.

Acceso a Internet de salida

El conector requiere acceso saliente a Internet para gestionar recursos y procesos dentro de su entorno de nube pública. Un conector se pone en contacto con los siguientes extremos al gestionar recursos en Azure:

Puntos finales	Específico
https://management.azure.com https://login.microsoftonline.com	Permite que Cloud Manager ponga en marcha y gestione Cloud Volumes ONTAP en la mayoría de las regiones de Azure.
https://management.microsoftazure.de https://login.microsoftonline.de	Permite que Cloud Manager ponga en marcha y gestione Cloud Volumes ONTAP en las regiones de Azure Alemania.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Permite a Cloud Manager implementar y gestionar Cloud Volumes ONTAP en las regiones de Azure US Gov.
https://api.services.cloud.netapp.com:443	Solicitudes de API a Cloud Central de NetApp.

Puntos finales	Específico
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Proporciona acceso a imágenes, manifiestos y plantillas de software.
https://repo.cloud.support.netapp.com	Se utiliza para descargar las dependencias de Cloud Manager.
http://repo.mysql.com/	Se utiliza para descargar MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Permite a Cloud Manager acceder y descargar manifiestos, plantillas e imágenes de actualización de Cloud Volumes ONTAP.
https://cloudmanagerinfraprod.azurecr.io	Acceso a imágenes de software de componentes de contenedor para una infraestructura que ejecuta Docker y proporciona una solución para las integraciones de servicios con Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Permite a NetApp transmitir datos desde registros de auditoría.
https://cloudmanager.cloud.netapp.com	Comunicación con el servicio Cloud Manager, que incluye cuentas de Cloud Central.
https://netapp-cloud-account.auth0.com	Comunicación con Cloud Central de NetApp para la autenticación de usuario centralizada.
https://mysupport.netapp.com	Comunicación con AutoSupport de NetApp.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Comunicación con NetApp para la licencia del sistema y el registro de soporte.
https://ipa-signer.cloudmanager.netapp.com	Permite que Cloud Manager genere licencias (por ejemplo, una licencia de FlexCache para Cloud Volumes ONTAP).
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Necesario para conectar los sistemas Cloud Volumes ONTAP con un clúster de Kubernetes. Los extremos permiten la instalación de Trident de NetApp.
*.blob.core.windows.net	Necesario para pares de alta disponibilidad cuando se utiliza un proxy.

Puntos finales	Específico
Diversas ubicaciones de terceros, por ejemplo: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org Las ubicaciones de terceros están sujetas a cambios.	Durante las actualizaciones, Cloud Manager descarga los paquetes más recientes para dependencias de terceros.

Aunque debe realizar casi todas las tareas desde la interfaz de usuario de SaaS, todavía hay disponible una interfaz de usuario local en el conector. La máquina que ejecuta el explorador Web debe tener conexiones con los siguientes puntos finales:

Puntos finales	Específico
El host del conector	Debe introducir la dirección IP del host desde un explorador web para cargar la consola de Cloud Manager. Según su conectividad con el proveedor de cloud, puede usar la IP privada o una IP pública asignada al host: • Una IP privada funciona si dispone de una VPN y. acceso directo a la red virtual • Una IP pública funciona en cualquier situación de red En cualquier caso, debe proteger el acceso a la red garantizando que las reglas de grupo de seguridad permiten el acceso sólo desde IP o subredes autorizadas.
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	El explorador web se conecta con estos extremos para conseguir una autenticación de usuario centralizada mediante NetApp Cloud Central.
https://widget.intercom.io	Si busca un chat integrado en los productos que le permita hablar con expertos en cloud de NetApp.

Reglas de grupo de seguridad para Cloud Volumes ONTAP

Cloud Manager crea grupos de seguridad de Azure que incluyen las reglas de entrada y salida 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.

Reglas de entrada para sistemas de un solo nodo

Las reglas que se enumeran a continuación permiten el tráfico, a menos que la descripción indique que

bloquea el tráfico entrante específico.

Prioridad y nombre	Puerto y protocolo	Origen y destino	Descripción
1000 inbound_ssh	22 TCP	De cualquiera a cualquiera	Acceso SSH a la dirección IP de administración del clúster LIF o una LIF de gestión de nodos
1001 inbound_http	80 TCP	De cualquiera a cualquiera	Acceso HTTP a la consola web de System Manager mediante el La dirección IP de la LIF de gestión del clúster
1002 inbound_111_tcp	111 TCP	De cualquiera a cualquiera	Llamada a procedimiento remoto para NFS
1003 inbound_111_udp	111 UDP	De cualquiera a cualquiera	Llamada a procedimiento remoto para NFS
1004 inbound_139	139 TCP	De cualquiera a cualquiera	Sesión de servicio NetBIOS para CIFS
1005 inbound_161-162 _tcp	161-162 TCP	De cualquiera a cualquiera	Protocolo simple de gestión de red
1006 inbound_161-162 _udp	161-162 UDP	De cualquiera a cualquiera	Protocolo simple de gestión de red
1007 inbound_443	443 TCP	De cualquiera a cualquiera	Acceso HTTPS a la consola web de System Manager mediante el 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

Prioridad y nombre	Puerto y protocolo	Origen y destino	Descripción
1016 inbound_4045-4046_udp	4045-4046 UDP	De cualquiera a cualquiera	Daemon de bloqueo NFS y monitor de estado de red
1017 inbound_10000	10000 TCP	De cualquiera a cualquiera	Backup con NDMP
1018 inbound_11104-11105	11104-11105 TCP	De cualquiera a cualquiera	Transferencia de datos de SnapMirror
3000 inbound_deny _all_tcp	Cualquier puerto TCP	De cualquiera a cualquiera	Bloquear el resto del tráfico entrante TCP
3001 inbound_deny _all_udp	Cualquier puerto UDP	De cualquiera a cualquiera	Bloquee el resto del tráfico de entrada UDP
65000 AllowVnetInBound	Cualquier protocolo	VirtualNetwork para VirtualNetwork	Tráfico entrante desde dentro del vnet
65001 AllowAzureLoad Balance InBound	Cualquier protocolo	AzureLoadBalancer a cualquiera	Tráfico de datos del balanceador de carga estándar de Azure
65500 DenyAllInBound	Cualquier protocolo	De cualquiera a cualquiera	Bloquear el resto del tráfico entrante

Reglas de entrada para sistemas de alta disponibilidad

Las reglas que se enumeran a continuación permiten el tráfico, a menos que la descripción indique que bloquea el tráfico entrante específico.

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	Acceso HTTPS a la consola web de System Manager mediante el 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

Prioridad y nombre	Puerto y protocolo	Origen y destino	Descripción
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)
DHCP	68	UDP	LIF de gestión de nodos	DHCP	Cliente DHCP para la configuración inicial

Servicio	Puerto	Protocolo	Origen	Destino	Específico
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

Reglas de grupo de seguridad para el conector

El grupo de seguridad del conector requiere reglas entrantes y salientes.

Reglas de entrada

El origen de las reglas entrantes en el grupo de seguridad predefinido es 0.0.0.0/0.

Puerto	Protocolo	Específico
22	SSH	Proporciona acceso SSH al host de Connector
80	HTTP	Proporciona acceso HTTP desde navegadores web de cliente al local interfaz de usuario

Puerto	Protocolo	Específico
443	HTTPS	Proporciona acceso HTTPS desde exploradores web de cliente al local interfaz de usuario

Reglas de salida

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

Reglas de salida básicas

El grupo de seguridad predefinido para el conector 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 parte del conector.

La dirección IP de origen es el host del conector.

Servicio	Puerto	Protocolo	Destino	Específico
Active Directory	88	TCP	Bosque de Active Directory	Autenticación Kerberos V.
	139	TCP	Bosque de Active Directory	Sesión de servicio NetBIOS
	389	TCP	Bosque de Active Directory	LDAP
	445	TCP	Bosque de Active Directory	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
	464	TCP	Bosque de Active Directory	Kerberos V cambiar y establecer contraseña (SET_CHANGE)
	749	TCP	Bosque de Active Directory	Contraseña de modificación y definición de Kerberos V de Active Directory (RPCSEC_GSS)
	137	UDP	Bosque de Active Directory	Servicio de nombres NetBIOS
	138	UDP	Bosque de Active Directory	Servicio de datagramas NetBIOS
	464	UDP	Bosque de Active Directory	Administración de claves Kerberos
Llamadas API y AutoSupport	443	HTTPS	LIF de gestión de clústeres de ONTAP y Internet saliente	API llama a AWS y ONTAP y envía mensajes de AutoSupport a NetApp
Llamadas API	3000	TCP	LIF de gestión de clústeres de ONTAP	Llamadas API a ONTAP
DNS	53	UDP	DNS	Utilizado para resolver DNS por Cloud Manager

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 Cloud Manager.

Antes de empezar

- Usted debe tener un "Conector asociado al área de trabajo".

> Debe ser un administrador de cuentas para crear un conector. Al crear el primer entorno de trabajo de Cloud Volumes ONTAP, Cloud Manager le solicita que cree un conector si todavía no lo tiene.

- "Debe estar preparado para dejar el conector funcionando en en todo momento".
- 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".
- Para poner en marcha un sistema BYOL, necesita el número de serie (clave de licencia) de 20 dígitos para cada nodo.

Acerca de esta tarea

Cuando Cloud Manager 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**
>
> No se recomienda la implementación de Cloud Volumes ONTAP en un grupo de recursos compartidos existente debido al riesgo de pérdida de datos. Mientras que la reversión está deshabilitada de forma predeterminada cuando se usa la API para implementar en un grupo de recursos existente, la eliminación de Cloud Volumes ONTAP potencialmente elimina otros recursos de ese grupo compartido.
>
> La mejor práctica es utilizar un nuevo grupo de recursos dedicado para Cloud Volumes ONTAP. Esta es la opción predeterminada y solo recomendada cuando implemente Cloud Volumes ONTAP en Azure desde Cloud Manager.

Pasos

1. En la página entornos de trabajo, haga clic en **Agregar entorno de trabajo** y siga las indicaciones.
2. **Elija una ubicación**: Seleccione **Microsoft Azure** y **Cloud Volumes ONTAP Single Node** o **Cloud Volumes ONTAP High Availability**.
3. **Detalles y credenciales**: De forma opcional, cambie las credenciales y la suscripción de Azure, especifique un nombre de clúster y un nombre de grupo de recursos, 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	Cloud Manager utiliza 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.

Campo	Descripción
Nombre del grupo de recursos	Conserve el nombre predeterminado para el nuevo grupo de recursos o desactive **Use Default** e introduzca su propio nombre para el nuevo grupo de recursos. 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 mediante la API, no se recomienda debido al riesgo de pérdida de datos. Consulte la advertencia anterior para obtener más detalles.
Etiquetas	Las etiquetas son metadatos para sus recursos de Azure. Cuando introduce etiquetas en este campo, Cloud Manager las añade al grupo de recursos asociado con el sistema Cloud Volumes ONTAP. Puede agregar hasta cuatro etiquetas desde la interfaz de usuario al crear un entorno de trabajo y, a continuación, puede agregar más después de crear. Tenga en cuenta que la API no le limita a cuatro etiquetas al crear un entorno de trabajo. Para obtener información sobre etiquetas, consulte "Documentación de Microsoft Azure: Uso de etiquetas para organizar los recursos de Azure".
Nombre de usuario y contraseña	Estas son las credenciales de la cuenta de administrador del clúster de Cloud Volumes ONTAP. Puede usar estas credenciales para conectarse a Cloud Volumes ONTAP a través de OnCommand System Manager o de su CLI.
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:

► https://docs.netapp.com/es-es/occm38//media/video_subscribing_azure.mp4 *(video)*

4. **Servicios**: Mantenga activados los servicios o desactive los servicios individuales que no desea utilizar con Cloud Volumes ONTAP.
   - "Más información sobre Cloud Compliance".
   - "Más información sobre el backup en el cloud".
5. **Ubicación y conectividad**: Seleccione una ubicación y un grupo de seguridad y active la casilla de verificación para confirmar la conectividad de red entre Cloud Manager y la ubicación de destino.
6. **cuenta del sitio de soporte y licencia**: Indique si desea usar el modelo de pago por uso o con su licencia y, a continuación, especifique una cuenta del sitio de soporte de NetApp.

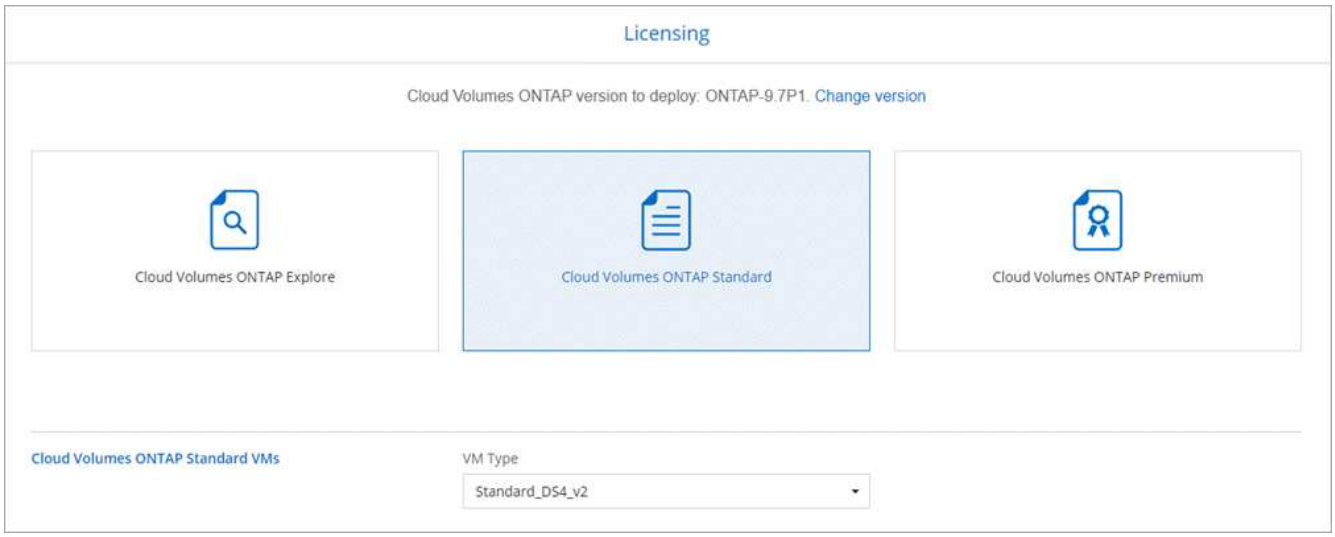
   Para comprender cómo funcionan las licencias, consulte "Licencia".

   Una cuenta del sitio de soporte de NetApp es opcional para el pago por uso, pero obligatoria para los sistemas BYOL. "Aprenda a añadir cuentas del sitio de soporte de NetApp".

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

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

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



Si sus necesidades cambian después de iniciar el sistema, puede modificar la licencia o el tipo de máquina virtual más adelante.

> Si hay disponible un candidato de versión, disponibilidad general o versión de revisión más reciente para la versión seleccionada, Cloud Manager actualiza el sistema a esa versión al crear el entorno de trabajo. Por ejemplo, la actualización se produce si selecciona Cloud Volumes ONTAP 9.6 RC1 y 9.6 GA está disponible. La actualización no se produce de una versión a otra; por ejemplo, de 9.6 a 9.7.

9. **Suscribirse desde el mercado de Azure**: Siga los pasos si Cloud Manager no pudo permitir implementaciones programáticas de Cloud Volumes ONTAP.
10. **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 de disco es para todos los discos del agregado inicial y para cualquier agregado adicional que Cloud Manager cree cuando utilice la opción de aprovisionamiento simple. Puede crear agregados que utilicen un tamaño de disco diferente mediante la opción de asignación avanzada.

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

    - Se puede elegir una política de organización en niveles de volumen específica cuando se crea o se edita un volumen.
    - Si deshabilita la organización en niveles de datos, puede habilitarla en agregados posteriores.

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

11. **escribir velocidad y GUSANO** (sólo sistemas de un solo nodo): Elija **velocidad de escritura normal** o **Alta** y active el almacenamiento de escritura única, lectura múltiple (WORM), si lo desea.

Además, es posible seleccionar una velocidad de escritura con sistemas de un solo nodo.

"Más información sobre la velocidad de escritura".

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

"Más información acerca del almacenamiento WORM".

12. **Secure Communication to Storage & WORM** (sólo ha): Si desea activar una conexión HTTPS a cuentas de almacenamiento de Azure y activar el almacenamiento de escritura única y lectura múltiple (WORM).

    La conexión HTTPS es de un par de alta disponibilidad de Cloud Volumes ONTAP 9.7 a las cuentas de almacenamiento 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".

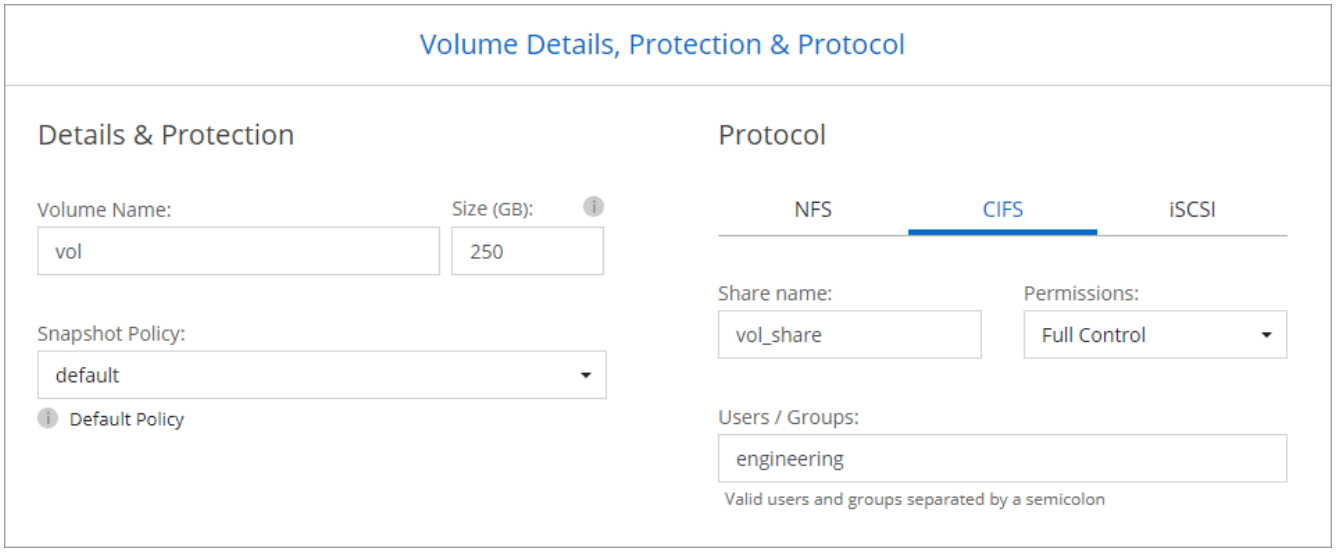
13. **Crear volumen**: Introduzca los detalles del nuevo volumen o haga clic en **Omitir**.

    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, Cloud Manager introduce un valor que proporciona acceso a todas las instancias de la subred.
Permisos y usuarios/grupos (solo para CIFS)	Estos campos permiten controlar el nivel de acceso a un recurso compartido para usuarios y grupos (también denominados listas de control de acceso o ACL). Es posible especificar usuarios o grupos de Windows locales o de dominio, o usuarios o grupos de UNIX. Si especifica un nombre de usuario de Windows de dominio, debe incluir el dominio del usuario con el formato domain\username.
Política de Snapshot	Una política de copia de Snapshot especifica la frecuencia y el número de copias de Snapshot de NetApp creadas automáticamente. Una copia snapshot de NetApp es una imagen del sistema de archivos puntual que no afecta al rendimiento y requiere un almacenamiento mínimo. Puede elegir la directiva predeterminada o ninguna. Es posible que no elija ninguno para los datos transitorios: Por ejemplo, tempdb para Microsoft SQL Server.
Opciones avanzadas (solo para NFS)	Seleccione una versión de NFS para el volumen: NFSv3 o NFSv4.

Campo	Descripción
Grupo del iniciador y IQN (solo para iSCSI)	Los destinos de almacenamiento iSCSI se denominan LUN (unidades lógicas) y se presentan a los hosts como dispositivos de bloque estándar. Los iGroups son tablas de los nombres de los nodos de host iSCSI y controlan qué iniciadores tienen acceso a qué LUN. Los destinos iSCSI se conectan a la red a través de adaptadores de red Ethernet (NIC) estándar, tarjetas DEL motor de descarga TCP (TOE) con iniciadores de software, adaptadores de red convergente (CNA) o adaptadores de host de salida dedicados (HBA) y se identifican mediante nombres cualificados de iSCSI (IQN). Cuando se crea un volumen iSCSI, Cloud Manager crea automáticamente un LUN. 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:



14. **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 "Guía para desarrolladores de API de Cloud Manager" para obtener más detalles.

15. **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".

16. **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 adquirirá Cloud Manager.
    c. Active las casillas de verificación **comprendo…**.
    d. Haga clic en **Ir**.

Resultado

Cloud Manager pone en marcha el sistema Cloud Volumes ONTAP. Puede realizar un seguimiento del progreso en la línea de tiempo.

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

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

Después de terminar

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

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

Información de copyright

Información de la marca comercial