Administración de Azure

Cloud Volumes ONTAP

NetApp
February 13, 2026

Tabla de contenidos

Administración de Azure

Cambiar el tipo de máquina virtual de Azure para Cloud Volumes ONTAP

Puede elegir entre varios tipos de máquinas virtuales al iniciar Cloud Volumes ONTAP en Microsoft Azure. Puede cambiar el tipo de máquina virtual en cualquier momento si determina que su tamaño es demasiado pequeño o demasiado grande para sus necesidades.

Acerca de esta tarea

- La devolución automática debe estar habilitada en un par de Cloud Volumes ONTAP HA (esta es la configuración predeterminada). Si no es así la operación fallará.

  "Documentación de ONTAP 9: Comandos para configurar la devolución automática"

- Cambiar el tipo de máquina virtual puede afectar los cargos por servicio de Microsoft Azure.
- La operación reinicia Cloud Volumes ONTAP.

  En los sistemas de nodo único, la I/O se interrumpe.

  Para los pares HA, el cambio no es disruptivo. Los pares HA continúan proporcionando datos.

  La NetApp Console cambia un nodo a la vez iniciando la toma de control y esperando la devolución. El equipo de control de calidad de NetApp probó tanto la escritura como la lectura de archivos durante este proceso y no detectó ningún problema en el lado del cliente. A medida que cambiaban las conexiones, se observaron algunos reintentos en el nivel de E/S, pero la capa de aplicación superó el recableado de las conexiones NFS/CIFS.

Pasos

1. En la página **Sistemas**, seleccione el sistema.
2. En la pestaña Descripción general, haga clic en el panel Características y luego haga clic en el ícono de lápiz junto a **Tipo de VM**.

   Si está utilizando una licencia de pago por uso (PAYGO) basada en nodos, puede elegir opcionalmente una licencia y un tipo de VM diferentes haciendo clic en el ícono de lápiz junto a **Tipo de licencia**.

3. Seleccione un tipo de VM, seleccione la casilla de verificación para confirmar que comprende las implicaciones del cambio y luego haga clic en **Cambiar**.

Resultado

Cloud Volumes ONTAP se reinicia con la nueva configuración.

Anular bloqueos CIFS para pares de alta disponibilidad de Cloud Volumes ONTAP en Azure

El administrador de la organización o de la cuenta puede habilitar una configuración en la NetApp Console que evita problemas con la devolución de almacenamiento de Cloud

Volumes ONTAP durante los eventos de mantenimiento de Azure. Cuando habilita esta configuración, Cloud Volumes ONTAP veta los bloqueos CIFS y restablece las sesiones CIFS activas.

Acerca de esta tarea

Microsoft Azure programa eventos de mantenimiento periódicos en sus máquinas virtuales. Cuando ocurre un evento de mantenimiento en un par HA de Cloud Volumes ONTAP , el par HA inicia la toma de control del almacenamiento. Si hay sesiones CIFS activas durante este evento de mantenimiento, los bloqueos en los archivos CIFS pueden impedir la devolución del almacenamiento.

Si habilita esta configuración, Cloud Volumes ONTAP vetará los bloqueos y restablecerá las sesiones CIFS activas. Como resultado, el par HA puede completar la devolución de almacenamiento durante estos eventos de mantenimiento.

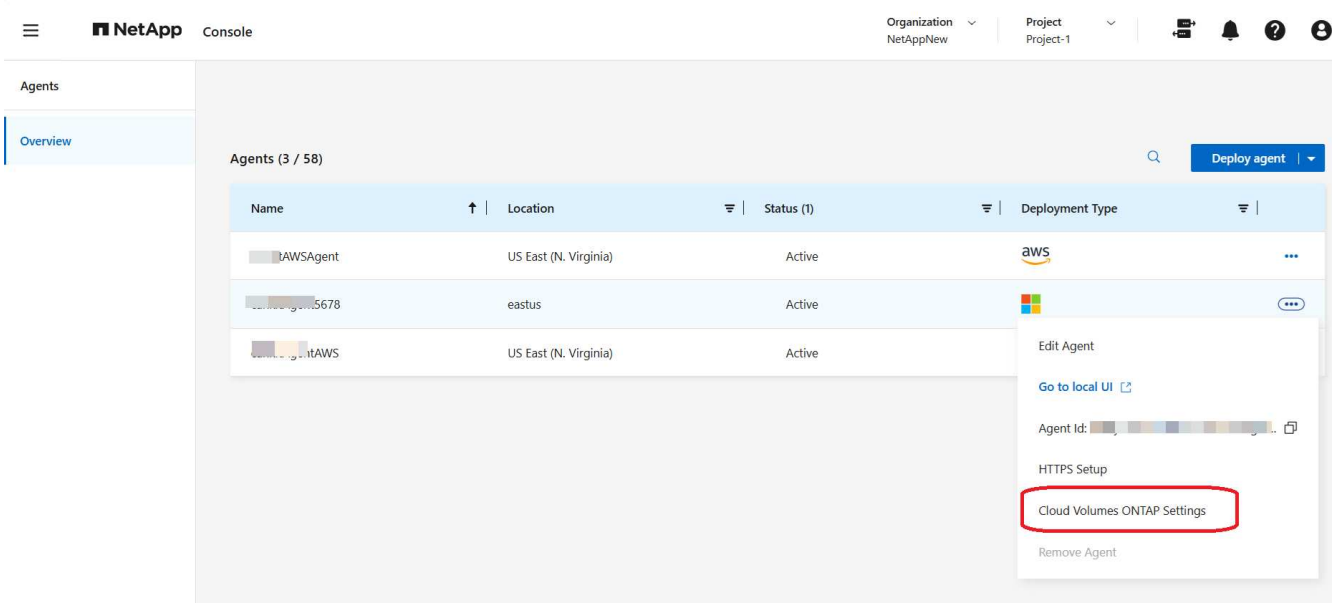
> Este proceso podría resultar perjudicial para los clientes CIFS. Se podrían perder datos que no sean confirmados por los clientes CIFS.

Antes de empezar

Debe crear un agente de consola antes de poder cambiar la configuración de la consola. "Aprende cómo" .

Pasos

1. Desde el panel de navegación izquierdo, vaya a **Administración > Agentes**.
2. Haga clic en el ••• Icono del agente de consola que administra su sistema Cloud Volumes ONTAP .
3. Seleccione *Configuración de Cloud Volumes ONTAP *.



4. En **Azure**, haga clic en **Bloqueos CIFS de Azure para sistemas Azure HA**.
5. Haga clic en la casilla de verificación para habilitar la función y luego haga clic en **Guardar**.

Utilice un enlace privado de Azure o puntos de conexión de servicio para sistemas Cloud Volumes ONTAP

Cloud Volumes ONTAP utiliza un vínculo privado de Azure para las conexiones a sus cuentas de almacenamiento asociadas. Si es necesario, puede deshabilitar Azure Private Links y usar puntos de conexión de servicio en su lugar.

Descripción general

De forma predeterminada, la NetApp Console habilita un vínculo privado de Azure para las conexiones entre Cloud Volumes ONTAP y sus cuentas de almacenamiento asociadas. Un vínculo privado de Azure protege las conexiones entre puntos finales en Azure y proporciona beneficios de rendimiento.

Si es necesario, puede configurar Cloud Volumes ONTAP para usar puntos de conexión de servicio en lugar de un Azure Private Link.

Con cualquiera de las configuraciones, la consola siempre limita el acceso a la red para las conexiones entre Cloud Volumes ONTAP y las cuentas de almacenamiento. El acceso a la red está limitado a la red virtual donde está implementado Cloud Volumes ONTAP y a la red virtual donde está implementado el agente de la consola.

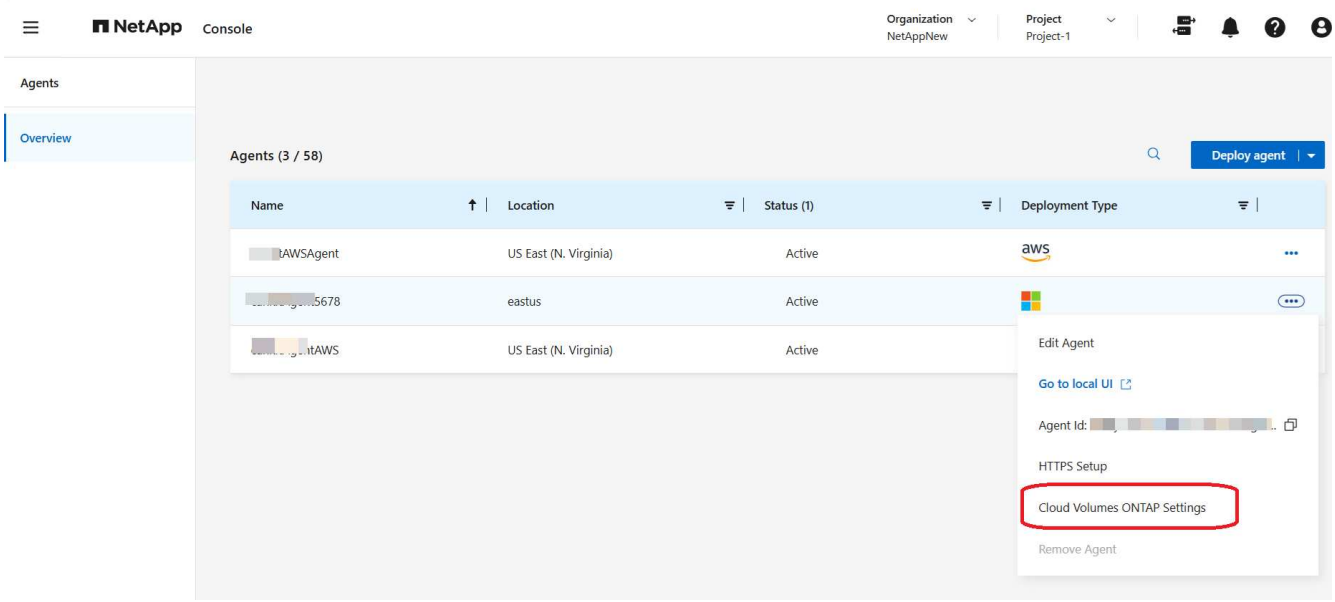
Deshabilite Azure Private Links y utilice puntos de conexión de servicio en su lugar

Si su negocio lo requiere, puede cambiar una configuración en la consola para que configure Cloud Volumes ONTAP para usar puntos de conexión de servicio en lugar de un Azure Private Link. Cambiar esta configuración se aplica a los nuevos sistemas Cloud Volumes ONTAP que usted cree. Los puntos finales de servicio solo se admiten en"Pares de regiones de Azure" entre el agente de consola y las redes virtuales de Cloud Volumes ONTAP .

El agente de consola debe implementarse en la misma región de Azure que los sistemas Cloud Volumes ONTAP que administra, o en la "Par de regiones de Azure" para los sistemas Cloud Volumes ONTAP .

Pasos

1. Desde el panel de navegación izquierdo, vaya a **Administración > Agentes**.
2. Haga clic en el ••• Icono del agente de consola que administra su sistema Cloud Volumes ONTAP .
3. Seleccione *Configuración de Cloud Volumes ONTAP *.



4. En **Azure**, haga clic en **Usar vínculo privado de Azure**.
5. Anule la selección de **Conexión de enlace privado entre Cloud Volumes ONTAP y las cuentas de almacenamiento**.
6. Haga clic en **Guardar**.

Después de terminar

Si deshabilitó Azure Private Links y el agente de consola usa un servidor proxy, debe habilitar el tráfico de API directo.

"Aprenda a habilitar el tráfico API directo en el agente de la consola"

Trabajar con vínculos privados de Azure

En la mayoría de los casos, no es necesario hacer nada para configurar vínculos privados de Azure con Cloud Volumes ONTAP. La consola administra los vínculos privados de Azure por usted. Pero si usa una zona DNS privada de Azure existente, necesitará editar un archivo de configuración.

Requisito de DNS personalizado

De manera opcional, si trabaja con DNS personalizado, deberá crear un reenvío condicional a la zona DNS privada de Azure desde sus servidores DNS personalizados. Para obtener más información, consulte"Documentación de Azure sobre el uso de un reenvío de DNS" .

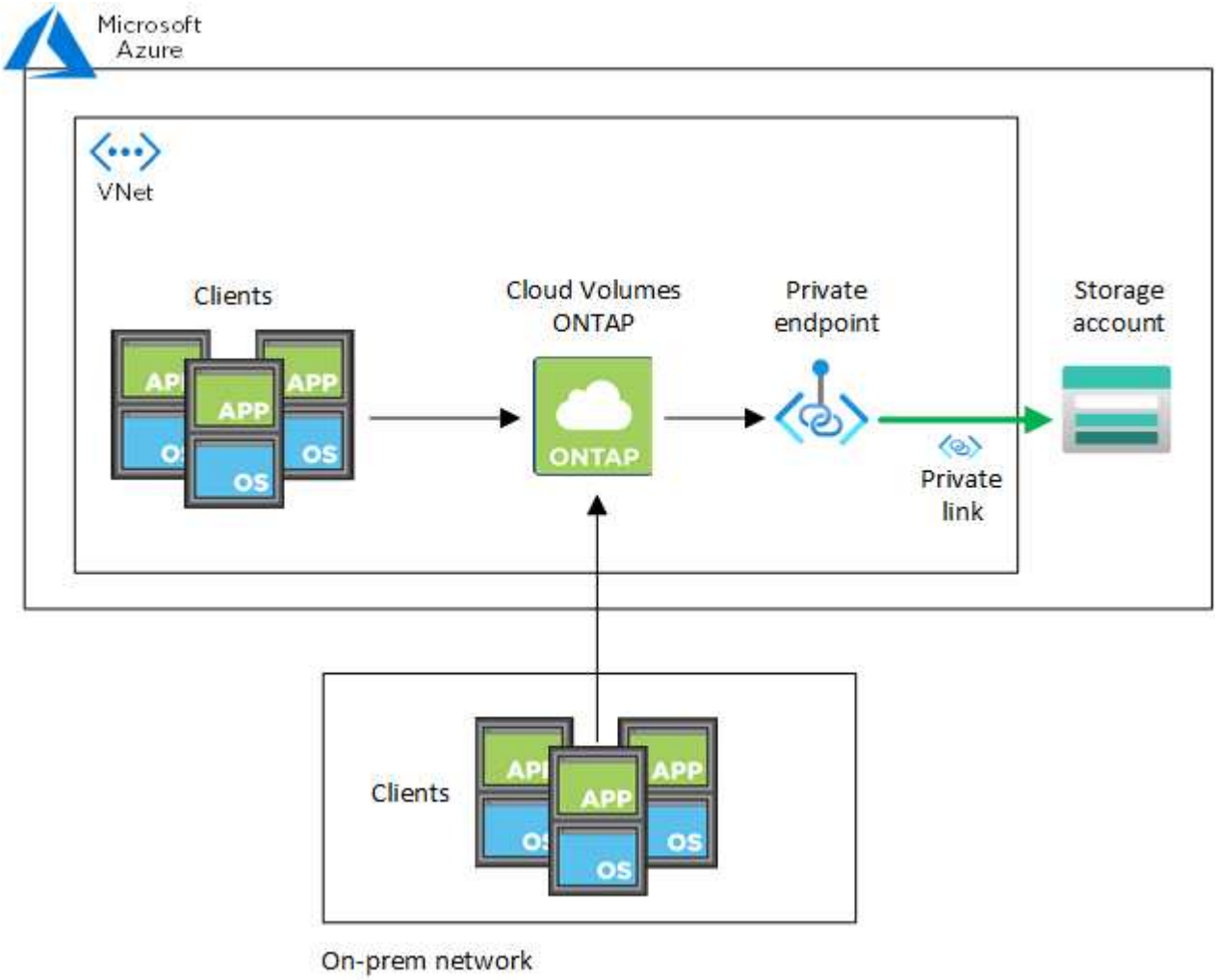
Cómo funcionan las conexiones de Private Link

Cuando la consola implementa Cloud Volumes ONTAP en Azure, crea un punto final privado en el grupo de recursos. El punto final privado está asociado con cuentas de almacenamiento para Cloud Volumes ONTAP. Como resultado, el acceso al almacenamiento de Cloud Volumes ONTAP viaja a través de la red troncal de Microsoft.

El acceso del cliente se realiza a través del enlace privado cuando los clientes están dentro de la misma red virtual que Cloud Volumes ONTAP, dentro de redes virtuales emparejadas o en su red local cuando usan una conexión VPN privada o ExpressRoute a la red virtual.

A continuación se muestra un ejemplo que muestra el acceso del cliente a través de un enlace privado desde

dentro de la misma VNet y desde una red local que tiene una conexión VPN privada o ExpressRoute.



Si el agente de la consola y los sistemas Cloud Volumes ONTAP están implementados en diferentes redes virtuales, debe configurar el emparejamiento de redes virtuales entre la red virtual donde está implementado el agente de la consola y la red virtual donde están implementados los sistemas Cloud Volumes ONTAP .

Proporcione detalles sobre su DNS privado de Azure

Si utilizas "DNS privado de Azure" , entonces necesitará modificar un archivo de configuración en cada agente de consola. De lo contrario, la consola no puede establecer la conexión de Azure Private Link entre Cloud Volumes ONTAP y sus cuentas de almacenamiento asociadas.

Tenga en cuenta que el nombre DNS debe coincidir con los requisitos de nombres de DNS de Azure. "como se muestra en la documentación de Azure" .

Pasos

1. Acceda por SSH al host del agente de la consola e inicie sesión.
2. Navegar hasta el `/opt/application/netapp/cloudmanager/docker_occm/data` directorio.
3. Editar `app.conf` añadiendo el `user-private-dns-zone-settings` parámetro con los siguientes pares palabra clave-valor:

```
"user-private-dns-zone-settings" : {
   "resource-group" : "<resource group name of the DNS zone>",
   "subscription" : "<subscription ID>",
   "use-existing" : true,
   "create-private-dns-zone-link" : true
}
```

El `subscription` La palabra clave solo es necesaria si la zona DNS privada está en una suscripción diferente a la del agente de la consola.

4. Guarde el archivo y cierre la sesión del agente de la consola.

   No es necesario reiniciar.

Habilitar reversión en caso de fallos

Si la consola no logra crear un Azure Private Link como parte de acciones específicas, completa la acción sin la conexión de Azure Private Link. Esto puede suceder al crear un nuevo sistema (nodo único o par HA) o cuando ocurren las siguientes acciones en un par HA: crear un nuevo agregado, agregar discos a un agregado existente o crear una nueva cuenta de almacenamiento al superar los 32 TiB.

Puede cambiar este comportamiento predeterminado habilitando la reversión si la consola no logra crear el vínculo privado de Azure. Esto puede ayudar a garantizar que cumple plenamente con las normas de seguridad de su empresa.

Si habilita la reversión, la consola detiene la acción y revierte todos los recursos que se crearon como parte de la acción.

Puede habilitar la reversión a través de la API o actualizando el archivo app.conf.

Habilitar la reversión a través de la API

Paso

1. Utilice el `PUT /occm/config` Llamada API con el siguiente cuerpo de solicitud:

```
{ "rollbackOnAzurePrivateLinkFailure": true }
```

Habilitar la reversión actualizando app.conf

Pasos

1. Acceda por SSH al host del agente de consola e inicie sesión.
2. Navegue al siguiente directorio: /opt/application/netapp/cloudmanager/docker_occm/data
3. Edite app.conf agregando el siguiente parámetro y valor:

```
 "rollback-on-private-link-failure": true
. Guarde el archivo y cierre la sesión del agente de la consola.
```

No es necesario reiniciar.

Mover un grupo de recursos de Azure para Cloud Volumes ONTAP en la consola de Azure

Cloud Volumes ONTAP admite movimientos de grupos de recursos de Azure, pero el flujo de trabajo se realiza únicamente en la consola de Azure.

Puede mover un sistema Cloud Volumes ONTAP de un grupo de recursos a otro en Azure dentro de la misma suscripción de Azure. No se admite mover grupos de recursos entre diferentes suscripciones de Azure.

Pasos

1. Eliminar el sistema Cloud Volumes ONTAP . Consulte "Eliminación de sistemas Cloud Volumes ONTAP" .
2. Ejecute el movimiento del grupo de recursos en la consola de Azure.

   Para completar el movimiento, consulte"Mover recursos a un nuevo grupo de recursos o suscripción en la documentación de Microsoft Azure" .

3. En la página **Sistemas**, descubre el sistema.
4. Busque el nuevo grupo de recursos en la información del sistema.

Resultado

El sistema y sus recursos (máquinas virtuales, discos, cuentas de almacenamiento, interfaces de red, instantáneas) están en el nuevo grupo de recursos.

Segregar el tráfico de SnapMirror en Azure

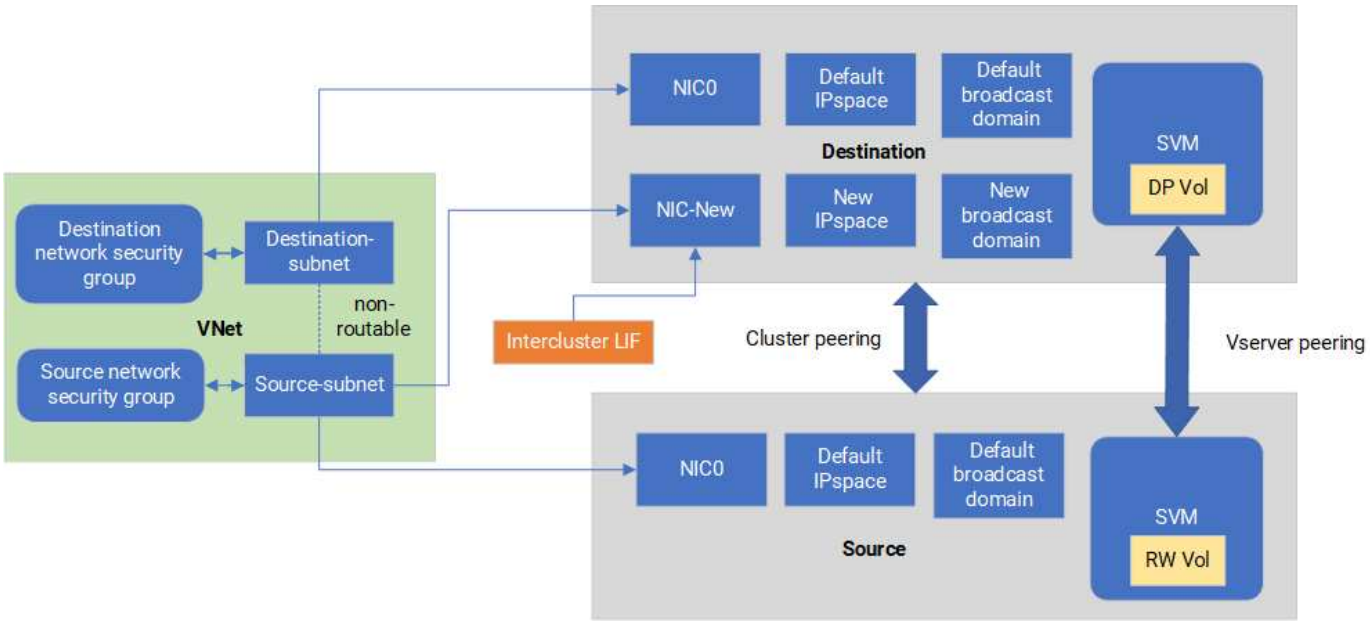
Con Cloud Volumes ONTAP en Azure, puede segregar el tráfico de replicación de SnapMirror del tráfico de datos y administración. Para segregar el tráfico de replicación de SnapMirror de su tráfico de datos, deberá agregar una nueva tarjeta de interfaz de red (NIC), un LIF entre clústeres asociado y una subred no enrutable.

Acerca de la segregación de tráfico de SnapMirror en Azure

De forma predeterminada, la NetApp Console configura todas las NIC y LIF en una implementación de Cloud Volumes ONTAP en la misma subred. En tales configuraciones, el tráfico de replicación de SnapMirror y el tráfico de datos y administración utilizan la misma subred. La segregación del tráfico de SnapMirror aprovecha una subred adicional que no se puede enrutar a la subred existente utilizada para el tráfico de datos y administración.

Figura 1

Los siguientes diagramas muestran la segregación del tráfico de replicación de SnapMirror con una NIC adicional, un LIF entre clústeres asociado y una subred no enrutable en una implementación de un solo nodo. La implementación de un par HA difiere ligeramente.



Antes de empezar

Revise las siguientes consideraciones:

- Solo puede agregar una única NIC a una implementación de un solo nodo o par HA de Cloud Volumes ONTAP (instancia de VM) para la segregación de tráfico de SnapMirror .
- Para agregar una nueva NIC, el tipo de instancia de VM que implemente debe tener una NIC sin usar.
- Los clústeres de origen y destino deben tener acceso a la misma red virtual (VNet). El clúster de destino es un sistema Cloud Volumes ONTAP en Azure. El clúster de origen puede ser un sistema Cloud Volumes ONTAP en Azure o un sistema ONTAP .

Paso 1: Cree una NIC adicional y conéctela a la máquina virtual de destino

Esta sección proporciona instrucciones sobre cómo crear una NIC adicional y conectarla a la máquina virtual de destino. La VM de destino es el nodo único o el sistema de par HA en Cloud Volumes ONTAP en Azure donde desea configurar su NIC adicional.

Pasos

1. En la CLI de ONTAP , detenga el nodo.

```
dest::> halt -node <dest_node-vm>
```

2. En el portal de Azure, verifique que el estado de la máquina virtual (nodo) esté detenido.

```
az vm get-instance-view --resource-group <dest-rg> --name <dest-vm>
--query instanceView.statuses[1].displayStatus
```

3. Utilice el entorno Bash en Azure Cloud Shell para detener el nodo.
   a. Detener el nodo.

```
az vm stop --resource-group <dest_node-rg> --name <dest_node-vm>
```

b. Desasignar el nodo.

```
az vm deallocate --resource-group <dest_node-rg> --name <dest_node-vm>
```

4. Configure las reglas del grupo de seguridad de red para que las dos subredes (subred del clúster de origen y subred del clúster de destino) no sean enrutables entre sí.
   a. Cree la nueva NIC en la máquina virtual de destino.
   b. Busque el ID de subred para la subred del clúster de origen.

```
az network vnet subnet show -g <src_vnet-rg> -n <src_subnet> --vnet -name <vnet> --query id
```

   c. Cree la nueva NIC en la máquina virtual de destino con el ID de subred para la subred del clúster de origen. Aquí ingresa el nombre de la nueva NIC.

```
az network nic create -g <dest_node-rg> -n <dest_node-vm-nic-new> --subnet <id_from_prev_command> --accelerated-networking true
```

   d. Guarde la dirección IP privada. Esta dirección IP, <new_added_nic_primary_addr>, se utiliza para crear un LIF entre clústeres enDominio de difusión, LIF entre clústeres para la nueva NIC .
5. Conecte la nueva NIC a la máquina virtual.

```
az vm nic add -g <dest_node-rg> --vm-name <dest_node-vm> --nics <dest_node-vm-nic-new>
```

6. Inicie la máquina virtual (nodo).

```
az vm start --resource-group <dest_node-rg>  --name <dest_node-vm>
```

7. En el portal de Azure, vaya a **Redes** y confirme que la nueva NIC, por ejemplo nic-new, existe y que la red acelerada está habilitada.

```
az network nic list --resource-group azure-59806175-60147103-azure-rg --query "[].{NIC: name, VM: virtualMachine.id}"
```

Para las implementaciones de pares HA, repita los pasos para el nodo asociado.

Paso 2: Cree un nuevo espacio IP, dominio de difusión y LIF entre clústeres para la nueva NIC

Un espacio IP separado para LIF entre clústeres proporciona una separación lógica entre la funcionalidad de red para la replicación entre clústeres.

Utilice la CLI de ONTAP para los siguientes pasos.

Pasos

1. Crea el nuevo espacio IP (new_ipspace).

```
dest::> network ipspace create -ipspace <new_ipspace>
```

2. Cree un dominio de transmisión en el nuevo espacio IP (new_ipspace) y agregue el puerto nic-new.

```
dest::> network port show
```

3. Para los sistemas de nodo único, el puerto recién añadido es *e0b*. Para las implementaciones de HA-pair con discos gestionados, el puerto recién añadido es *e0d*. Para las implementaciones de HA-pair con page blobs, el puerto recién añadido es *e0e*. Usa el nombre de nodo, no el nombre de la VM. Encuentra el nombre de nodo ejecutando `node show`.

```
dest::> broadcast-domain create -broadcast-domain <new_bd> -mtu 1500
-ipspace <new_ipspace> -ports <dest_node-cot-vm:e0b>
```

4. Cree un LIF entre clústeres en el nuevo dominio de transmisión (new_bd) y en la nueva NIC (nic-new).

```
dest::> net int create -vserver <new_ipspace> -lif <new_dest_node-ic-
lif> -service-policy default-intercluster -address
<new_added_nic_primary_addr> -home-port <e0b> -home-node <node> -netmask
<new_netmask_ip> -broadcast-domain <new_bd>
```

5. Verificar la creación del nuevo LIF entre clústeres.

```
dest::> net int show
```

Para las implementaciones de pares HA, repita los pasos para el nodo asociado.

Paso 3: Verificar el peering del clúster entre los sistemas de origen y destino

Esta sección proporciona instrucciones sobre cómo verificar el peering entre los sistemas de origen y destino.

Utilice la CLI de ONTAP para los siguientes pasos.

Pasos

1. Verifique que el LIF entre clústeres del clúster de destino pueda hacer ping al LIF entre clústeres del clúster de origen. Debido a que el clúster de destino ejecuta este comando, la dirección IP de destino es la dirección IP LIF entre clústeres en el origen.

```
dest::> ping -lif <new_dest_node-ic-lif> -vserver <new_ipspace>
-destination <10.161.189.6>
```

2. Verifique que el LIF entre clústeres del clúster de origen pueda hacer ping al LIF entre clústeres del clúster de destino. El destino es la dirección IP de la nueva NIC creada en el destino.

```
src::> ping -lif <src_node-ic-lif> -vserver <src_svm> -destination
<10.161.189.18>
```

Para las implementaciones de pares HA, repita los pasos para el nodo asociado.

Paso 4: Crear peering SVM entre el sistema de origen y el de destino

Esta sección proporciona instrucciones sobre cómo crear un peering SVM entre el sistema de origen y el de destino.

Utilice la CLI de ONTAP para los siguientes pasos.

Pasos

1. Cree un intercambio de clústeres en el destino utilizando la dirección IP LIF entre clústeres de origen como `-peer-addrs` . Para los pares de alta disponibilidad, indique la dirección IP LIF entre clústeres de origen para ambos nodos como `-peer-addrs` .

```
dest::> cluster peer create -peer-addrs <10.161.189.6> -ipspace
<new_ipspace>
```

2. Ingrese y confirme la contraseña.
3. Cree un clúster de intercambio de tráfico en el origen utilizando la dirección IP LIF del clúster de destino como `peer-addrs` . Para los pares de alta disponibilidad, indique la dirección IP LIF de destino entre clústeres para ambos nodos como `-peer-addrs` .

```
src::> cluster peer create -peer-addrs <10.161.189.18>
```

4. Ingrese y confirme la contraseña.
5. Verifique que el clúster esté emparejado.

```
src::> cluster peer show
```

El emparejamiento exitoso muestra **Disponible** en el campo de disponibilidad.

6. Cree un peering SVM en el destino. Tanto las SVM de origen como las de destino deben ser SVM de datos.

```
dest::> vserver peer create -vserver <dest_svm> -peer-vserver <src_svm>
-peer-cluster <src_cluster> -applications snapmirror``
```

7. Aceptar peering SVM.

```
src::> vserver peer accept -vserver <src_svm> -peer-vserver <dest_svm>
```

8. Verifique que el SVM esté emparejado.

```
dest::> vserver peer show
```

Los estados pares muestran*`peered` * y aplicaciones de peering muestran*`snapmirror` *.

Paso 5: Cree una relación de replicación de SnapMirror entre el sistema de origen y el de destino

Esta sección proporciona instrucciones sobre cómo crear una relación de replicación SnapMirror entre el sistema de origen y el de destino.

Para mover una relación de replicación de SnapMirror existente, primero debe romper la relación de replicación de SnapMirror existente antes de crear una nueva relación de replicación de SnapMirror .

Utilice la CLI de ONTAP para los siguientes pasos.

Pasos

1. Cree un volumen protegido de datos en el SVM de destino.

```
dest::> vol create -volume <new_dest_vol> -vserver <dest_svm> -type DP
-size <10GB> -aggregate <aggr1>
```

2. Cree la relación de replicación de SnapMirror en el destino que incluye la política y la programación de SnapMirror para la replicación.

```
dest::> snapmirror create -source-path src_svm:src_vol  -destination
-path  dest_svm:new_dest_vol -vserver dest_svm -policy
MirrorAllSnapshots -schedule 5min
```

3. Inicialice la relación de replicación de SnapMirror en el destino.

```
dest::> snapmirror initialize -destination-path  <dest_svm:new_dest_vol>
```

4. En la CLI de ONTAP , valide el estado de la relación de SnapMirror ejecutando el siguiente comando:

   ```
   dest::> snapmirror show
   ```

   El estado civil es `Snapmirrored` y la salud de la relación es `true` .

5. Opcional: en la CLI de ONTAP , ejecute el siguiente comando para ver el historial de acciones de la relación SnapMirror .

   ```
   dest::> snapmirror show-history
   ```

Opcionalmente, puede montar los volúmenes de origen y destino, escribir un archivo en el origen y verificar que el volumen se esté replicando en el destino.

Información de copyright

Información de la marca comercial