



SAP HANA con SUSE KVM y almacenamiento NetApp

NetApp solutions for SAP

NetApp
February 25, 2026

Tabla de contenidos

- SAP HANA con SUSE KVM y almacenamiento NetApp 1
 - Implemente SAP HANA en SUSE KVM con almacenamiento NetApp mediante SR-IOV y NFS. 1
 - Requisitos de implementación de SAP HANA en SUSE KVM con almacenamiento NetApp 1
 - Requisitos de infraestructura 2
 - Consideraciones importantes. 2
 - Recursos adicionales. 2
 - ¿Que sigue? 2
 - Configurar las interfaces de red SR-IOV para SAP HANA en SUSE KVM 2
 - Paso 1: Configurar SR-IOV 3
 - Paso 2: Crear las interfaces virtuales 5
 - Paso 3: Habilitar las VF durante el arranque 11
 - Paso 4: Asignar las interfaces virtuales a la máquina virtual 12
 - Paso 5: Configurar las interfaces de red dentro de la máquina virtual 18
 - ¿Que sigue? 19
 - Configurar la red Fibre Channel para SAP HANA en SUSE KVM 19
 - ¿Que sigue? 25
 - Configurar el almacenamiento NetApp para SAP HANA en SUSE KVM 25
 - Configurar el almacenamiento NFS para SAP HANA 25
 - Configurar el almacenamiento FCP para SAP HANA 26

SAP HANA con SUSE KVM y almacenamiento NetApp

Implemente SAP HANA en SUSE KVM con almacenamiento NetApp mediante SR-IOV y NFS.

Implemente SAP HANA Single-Host en SUSE KVM utilizando almacenamiento NetApp con interfaces de red SR-IOV y acceso a almacenamiento NFS o FCP. Siga este flujo de trabajo para configurar las interfaces virtuales, asignarlas a las máquinas virtuales y configurar las conexiones de almacenamiento para un rendimiento óptimo.

Para obtener una descripción general de SAP HANA en la virtualización KVM, consulte la documentación de SUSE: ["Mejores prácticas de SUSE para SAP HANA en KVM"](#) .

1

"Revisar los requisitos de configuración"

Revisa los requisitos clave para implementar SAP HANA en SUSE KVM utilizando almacenamiento NetApp con SR-IOV y protocolos de almacenamiento.

2

"Configurar interfaces de red SR-IOV"

Configure SR-IOV (Virtualización de E/S de raíz única) en el host KVM y asigne interfaces virtuales a la máquina virtual para la comunicación de red y el acceso al almacenamiento.

3

"Configurar redes Fibre Channel"

Asigne puertos HBA FCP físicos a la máquina virtual como dispositivos PCI para usar LUN FCP con SAP HANA.

4

"Configurar el almacenamiento de NetApp para SAP HANA"

Configure las conexiones de almacenamiento NFS o FCP entre la máquina virtual y los sistemas de almacenamiento NetApp para los archivos de la base de datos SAP HANA.

Requisitos de implementación de SAP HANA en SUSE KVM con almacenamiento NetApp

Revisa los requisitos para implementar SAP HANA Single-Host en SUSE KVM utilizando almacenamiento NetApp con interfaces de red SR-IOV y protocolos de almacenamiento NFS o FCP.

La implementación requiere servidores SAP HANA certificados, sistemas de almacenamiento NetApp , adaptadores de red compatibles con SR-IOV y SUSE Linux Enterprise Server para aplicaciones SAP como

host KVM.

Requisitos de infraestructura

Asegúrese de que los siguientes componentes y configuraciones estén en su lugar:

- Servidores SAP HANA y sistemas de almacenamiento NetApp certificados. Consulte el ["Directorio de hardware de SAP HANA"](#) Para conocer las opciones disponibles:
- SUSE Linux Enterprise Server para aplicaciones SAP 15 SP5/SP6 como host KVM
- Sistema de almacenamiento NetApp ONTAP con máquina virtual de almacenamiento (SVM) configurada para tráfico NFS y/o FCP.
- Interfaces lógicas (LIF) creadas en las redes apropiadas para el tráfico NFS y FCP
- Adaptadores de red compatibles con SR-IOV (por ejemplo, la serie Mellanox ConnectX)
- Adaptadores HBA de canal de fibra para acceso al almacenamiento FCP
- Infraestructura de red que admite las VLAN y los segmentos de red necesarios.
- Máquina virtual configurada según ["Mejores prácticas de SUSE para SAP HANA en KVM"](#)

Consideraciones importantes

- SR-IOV debe utilizarse para la comunicación de red de SAP HANA y para el acceso al almacenamiento mediante NFS. Cada función virtual (VF) asignada a una máquina virtual requiere un ancho de banda de al menos 10 Gbit/s.
- Los puertos físicos FCP HBA deben asignarse a la máquina virtual como dispositivos PCI para utilizar las LUN de FCP. Un puerto físico solo puede asignarse a una máquina virtual.
- Los sistemas SAP HANA de múltiples hosts no son compatibles con esta configuración.

Recursos adicionales

- Para obtener la información más reciente, incluida la arquitectura de CPU compatible y sus limitaciones, consulte la nota SAP. ["3538596 - SAP HANA en virtualización SUSE KVM con SLES 15 SP5 - SAP para mí"](#) .
- Para obtener información sobre la configuración de los sistemas de almacenamiento ONTAP , consulte la ["Documentación de ONTAP 9"](#) .
- Para la configuración del almacenamiento de SAP HANA con sistemas NetApp , consulte la ["Documentación de soluciones SAP de NetApp"](#) .

¿Que sigue?

Una vez que hayas revisado los requisitos de implementación, ["configurar interfaces de red SR-IOV"](#) .

Configurar las interfaces de red SR-IOV para SAP HANA en SUSE KVM

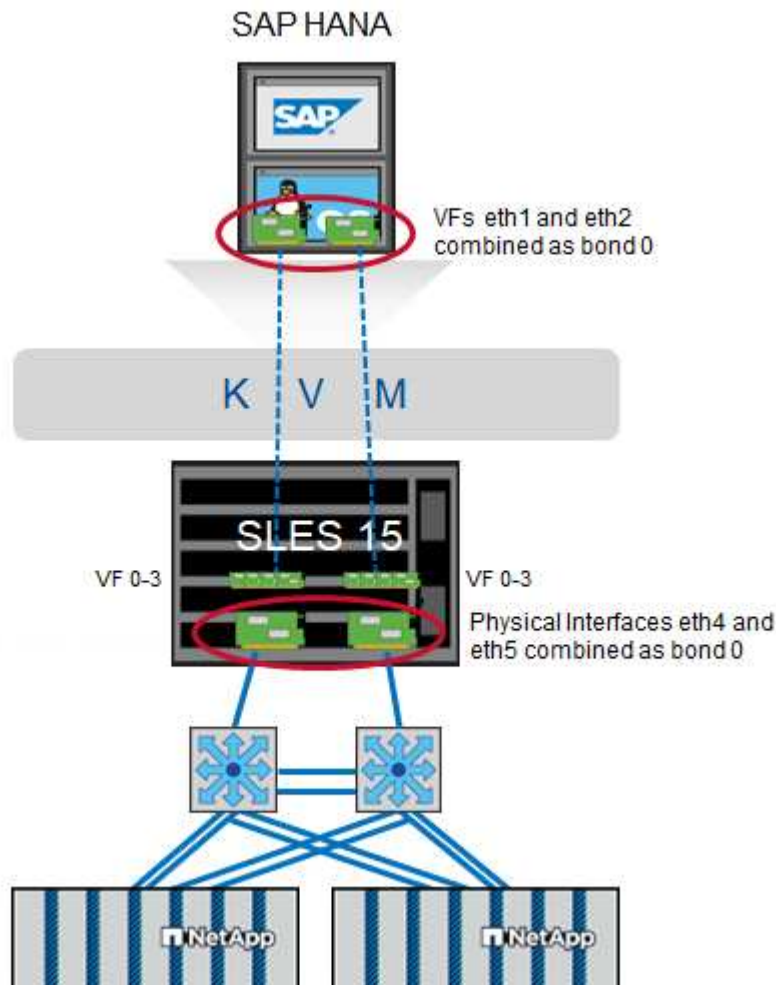
Configure las interfaces de red SR-IOV en SUSE KVM para SAP HANA. Configure las funciones virtuales (VF), asígnelas a las máquinas virtuales y configure conexiones de red redundantes para un rendimiento y acceso al almacenamiento óptimos.

Paso 1: Configurar SR-IOV

Habilite y configure la funcionalidad SR-IOV en el firmware del adaptador para permitir la creación de funciones virtuales.

Este procedimiento se basa en ["Portal de soporte empresarial de NVIDIA | Cómo configurar SR-IOV para ConnectX-4/ConnectX-5/ConnectX-6 con KVM \(Ethernet\)"](#). La guía SUSE SAP HANA KVM describe esto basándose en una NIC INTEL.

Se recomienda utilizar conexiones Ethernet redundantes combinando dos puertos físicos como enlace troncal/enlace. Los puertos virtuales (VF) asignados a la máquina virtual también deben estar configurados como troncales dentro de la máquina virtual.



Antes de empezar

Asegúrese de que se cumplan los siguientes requisitos previos:

- KVM está instalado
- SR-IOV está habilitado en la BIOS del servidor.
- La transferencia directa de PCI se habilita agregando "intel_iommu=on" e "iommu=pt" como opción en el gestor de arranque.
- Los controladores MLNX_OFED más recientes están instalados en los hosts KVM y en la máquina virtual.



Cada VF asignada a una VM requiere un ancho de banda de al menos 10 Gbit/s. No cree ni asigne más de dos VF para un puerto físico de 25GbE.

Pasos

1. Ejecutar MFT (Herramientas de firmware de Mellanox):

```
# mst start
Starting MST (Mellanox Software Tools) driver set
Loading MST PCI module - Success
Loading MST PCI configuration module - Success
Create devices
Unloading MST PCI module (unused) - Success
```

2. Localice el dispositivo:

```
# mst status
MST modules:
-----
MST PCI module is not loaded
MST PCI configuration module loaded

MST devices:
-----

/dev/mst/mt4125_pciconf0 - PCI configuration cycles access.
domain:bus:dev.fn=0000:ab:00.0 addr.reg=88 data.reg=92
cr_bar.gw_offset=-1

Chip revision is: 00
```

3. Compruebe el estado del dispositivo:

```
mlxconfig -d /dev/mst/mt4125_pciconf0 q |grep -e SRIOV_EN -e NUM_OF_VFS
NUM_OF_VFS 8
SRIOV_EN True(1)_
```

4. Si es necesario, habilite SR-IOV:

```
mlxconfig -d /dev/mst/mt4125_pciconf0 set SRIOV_EN=1
```

5. Establezca la cantidad máxima de VF:

```
mlxconfig -d /dev/mst/mt4125_pciconf0 set NUM_OF_VFS=4
```

6. Reinicie el servidor si fue necesario habilitar la función o si se cambió la cantidad máxima de VF.

Paso 2: Crear las interfaces virtuales

Cree funciones virtuales (VF) en los puertos de red físicos para habilitar la funcionalidad SR-IOV. En este paso, se crean cuatro VF por puerto físico.

Pasos

1. Localiza el dispositivo:

```
# ibstat

CA 'mlx5_0'
CA type: MT4125
Number of ports: 1
Firmware version: 22.36.1010
Hardware version: 0
Node GUID: 0xa088c20300a6f6fc
System image GUID: 0xa088c20300a6f6fc
Port 1:
State: Active
Physical state: LinkUp
Rate: 100
Base lid: 0
LMC: 0
SM lid: 0
Capability mask: 0x00010000
Port GUID: 0xa288c2fffea6f6fd
Link layer: Ethernet
CA 'mlx5_1'
CA type: MT4125
Number of ports: 1
Firmware version: 22.36.1010
Hardware version: 0
Node GUID: 0xa088c20300a6f6fd
System image GUID: 0xa088c20300a6f6fc
Port 1:
State: Active
Physical state: LinkUp
Rate: 100
Base lid: 0
LMC: 0
SM lid: 0
Capability mask: 0x00010000
Port GUID: 0xa288c2fffea6f6fd
Link layer: Ethernet
```

Si se ha creado un vínculo, el resultado sería similar al siguiente:


```

# ibstat
CA 'mlx5_bond_0'
CA type: MT4125
Number of ports: 1
Firmware version: 22.36.1010
Hardware version: 0
Node GUID: 0xa088c20300a6f6fc
System image GUID: 0xa088c20300a6f6fc
Port 1:
State: Active
Physical state: LinkUp
Rate: 100
Base lid: 0
LMC: 0
SM lid: 0
Capability mask: 0x00010000
Port GUID: 0xa288c2fffea6f6fc
Link layer: Ethernet
#:/etc/sysconfig/network # cat /sys/class/infiniband/mlx5_bond_0/device/
aerdevcorrectable iommugroup/ resetmethod
aerdevfatal irq resource
aerdevnonfatal link/ resource0
arienabled localcpulist resource0wc
brokenparitystatus localcpus revision
class maxlinkspeed rom
config maxlinkwidth sriovdriversautoprobe
consistentdmamaskbits mlx5_core.eth.0/ sriovnumvfs
urrentlinkspeed mlx5_core.rdma.0/ sriovoffset
currentlinkwidth modalias sriovstride
d3coldallowed msibus sriovtotalvfs
device msiirqs/ sriovvfdevice
dmamaskbits net/ sriovvftotalmsix
driver/ numanode subsystem/
driveroverride pools subsystemdevice
enable power/ subsystemvendor
firmwarenode/ powerstate uevent
infiniband/ ptp/ vendor
infinibandmad/ remove vpd
infinibandverbs/ rescan
iommu/ reset

```

```
# ibdev2netdev
mlx5_0 port 1 ==> eth4 (Up)
mlx5_1 port 1 ==> eth5 (Up)
```

2. Obtenga el total de VF permitidos y configurados en el firmware:

```
# cat /sys/class/net/eth4/device/sriov_totalvfs
4
# cat /sys/class/net/eth5/device/sriov_totalvfs
4
```

3. Obtenga el número actual de VF en este dispositivo:

```
# cat /sys/class/infiniband/mlx5_0/device/sriov_numvfs
0
# cat /sys/class/infiniband/mlx5_1/device/sriov_numvfs
0
```

4. Establezca el número deseado de VF:

```
# echo 4 > /sys/class/infiniband/mlx5_0/device/sriov_numvfs
# echo 4 > /sys/class/infiniband/mlx5_1/device/sriov_numvfs
```

Si ya ha configurado un enlace utilizando estos dos puertos, el primer comando debe ejecutarse en dicho enlace:

```
# echo 4 > /sys/class/infiniband/mlx5_bond_0/device/sriov_numvfs
```

5. Compruebe el bus PCI:

```
# lspci -D | grep Mellanox
```

```
0000:ab:00.0 Ethernet controller: Mellanox Technologies MT2892 Family  
[ConnectX-6 Dx]
```

```
0000:ab:00.1 Ethernet controller: Mellanox Technologies MT2892 Family  
[ConnectX-6 Dx]
```

```
0000:ab:00.2 Ethernet controller: Mellanox Technologies ConnectX Family  
mlx5Gen Virtual Function
```

```
0000:ab:00.3 Ethernet controller: Mellanox Technologies ConnectX Family  
mlx5Gen Virtual Function
```

```
0000:ab:00.4 Ethernet controller: Mellanox Technologies ConnectX Family  
mlx5Gen Virtual Function
```

```
0000:ab:00.5 Ethernet controller: Mellanox Technologies ConnectX Family  
mlx5Gen Virtual Function
```

```
0000:ab:01.2 Ethernet controller: Mellanox Technologies ConnectX Family  
mlx5Gen Virtual Function
```

```
0000:ab:01.3 Ethernet controller: Mellanox Technologies ConnectX Family  
mlx5Gen Virtual Function
```

```
0000:ab:01.4 Ethernet controller: Mellanox Technologies ConnectX Family  
mlx5Gen Virtual Function
```

```
0000:ab:01.5 Ethernet controller: Mellanox Technologies ConnectX Family  
mlx5Gen Virtual Function
```

```
# ibdev2netdev -v

0000:ab:00.0 mlx5_0 (MT4125 - 51TF3A5000XV3) Mellanox ConnectX-6 Dx
100GbE QSFP56 2-port PCIe 4 Ethernet Adapter fw 22.36.1010 port 1
(ACTIVE) ==> eth4 (Up)
0000:ab:00.1 mlx5_1 (MT4125 - 51TF3A5000XV3) Mellanox ConnectX-6 Dx
100GbE QSFP56 2-port PCIe 4 Ethernet Adapter fw 22.36.1010 port 1
(ACTIVE) ==> eth6 (Up)
0000:ab:00.2 mlx523 (MT4126 - NA) fw 22.36.1010 port 1 (DOWN ) ==> eth6
(Down)
0000:ab:00.3 mlx5_3 (MT4126 - NA) fw 22.36.1010 port 1 (DOWN ) ==> eth7
(Down)
0000:ab:00.4 mlx5_4 (MT4126 - NA) fw 22.36.1010 port 1 (DOWN ) ==> eth8
(Down)
0000:ab:00.5 mlx5_5 (MT4126 - NA) fw 22.36.1010 port 1 (DOWN ) ==> eth9
(Down)
0000:ab:01.2 mlx5_6 (MT4126 - NA) fw 22.36.1010 port 1 (DOWN ) ==> eth10
(Down)
0000:ab:01.3 mlx5_7 (MT4126 - NA) fw 22.36.1010 port 1 (DOWN ) ==> eth11
(Down)
0000:ab:01.4 mlx5_8 (MT4126 - NA) fw 22.36.1010 port 1 (DOWN ) ==> eth12
(Down)
0000:ab:01.5 mlx5_9 (MT4126 - NA) fw 22.36.1010 port 1 (DOWN ) ==> eth13
(Down)
```

6. Compruebe la configuración de las VF mediante la herramienta IP:

```
# ip link show
...
6: eth4: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 9000 qdisc mq
master bond0 state UP mode DEFAULT group default qlen 1000

link/ether a0:88:c2:a6:f6:fd brd ff:ff:ff:ff:ff:ff permaddr
a0:88:c2:a6:f6:fc
vf 0 link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff, spoof checking
off, link-state auto, trust off, query_rss off
vf 1 link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff, spoof checking
off, link-state auto, trust off, query_rss off
vf 2 link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff, spoof checking
off, link-state auto, trust off, query_rss off
vf 3 link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff, spoof checking
off, link-state auto, trust off, query_rss off

altname enp171s0f0np0
altname ens3f0np0

7: eth5: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 9000 qdisc mq
master bond0 state UP mode DEFAULT group default qlen 1000

link/ether a0:88:c2:a6:f6:fd brd ff:ff:ff:ff:ff:ff
vf 0 link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff, spoof checking
off, link-state auto, trust off, query_rss off
vf 1 link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff, spoof checking
off, link-state auto, trust off, query_rss off
vf 2 link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff, spoof checking
off, link-state auto, trust off, query_rss off
vf 3 link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff, spoof checking
off, link-state auto, trust off, query_rss off

altname enp171s0f1np1
altname ens3f1np1
...
```

Paso 3: Habilitar las VF durante el arranque

Configure los ajustes de VF para que persistan tras los reinicios del sistema mediante la creación de servicios systemd y scripts de inicio.

1. Crea un archivo de unidad systemd `/etc/systemd/system/after.local` con el siguiente contenido:

```
[Unit]
Description=/etc/init.d/after.local Compatibility
After=libvirtd.service Requires=libvirtd.service

[Service]
Type=oneshot
ExecStart=/etc/init.d/after.local
RemainAfterExit=true

[Install]
WantedBy=multi-user.target
```

2. Crea el script `/etc/init.d/after.local`:

```
#!/bin/sh
#
#
# ...
echo 4 > /sys/class/infiniband/mlx5_bond_0/device/sriov_numvfs
echo 4 > /sys/class/infiniband/mlx5_1/device/sriov_numvfs
```

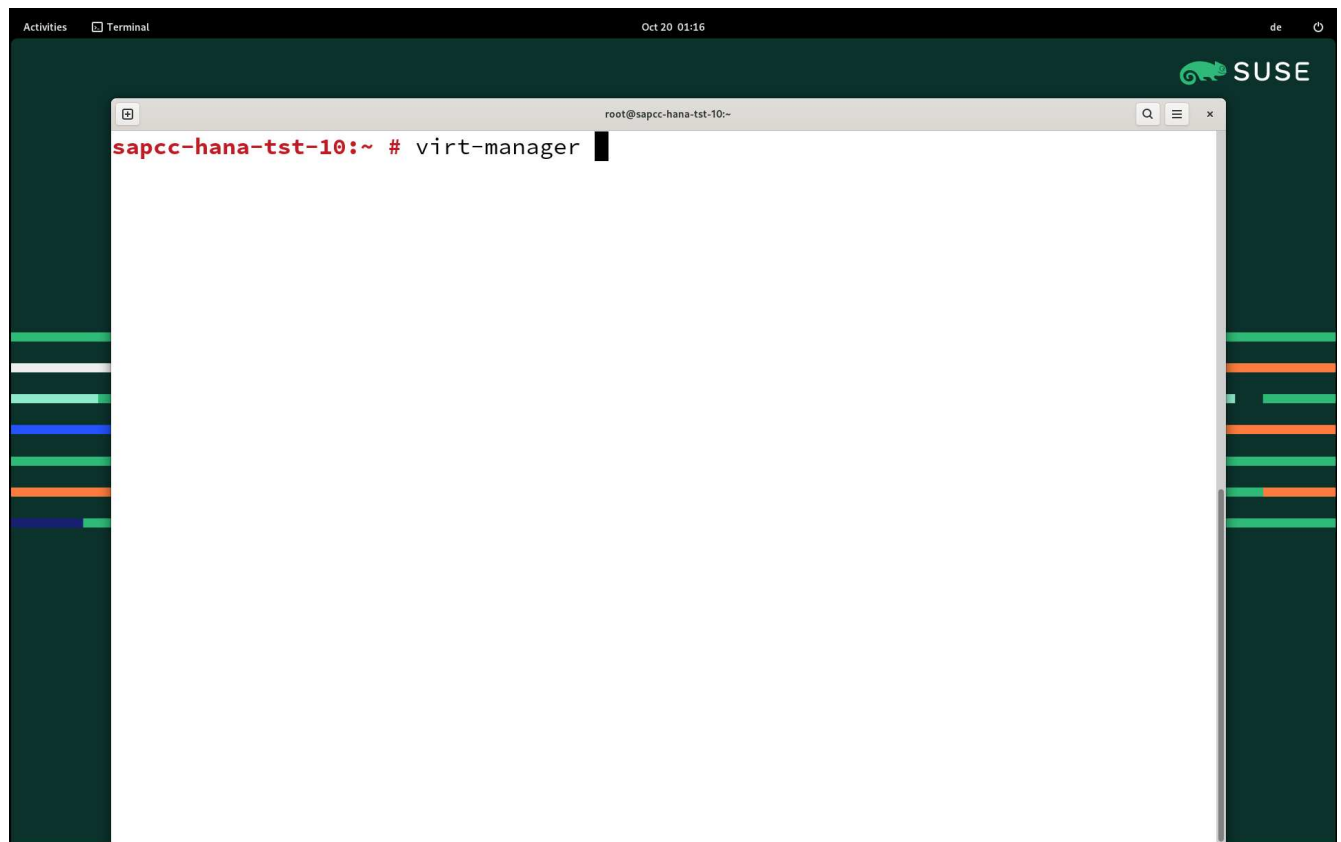
3. Asegúrese de que el archivo se pueda ejecutar:

```
# cd /etc/init.d/
# chmod 750 after.local
```

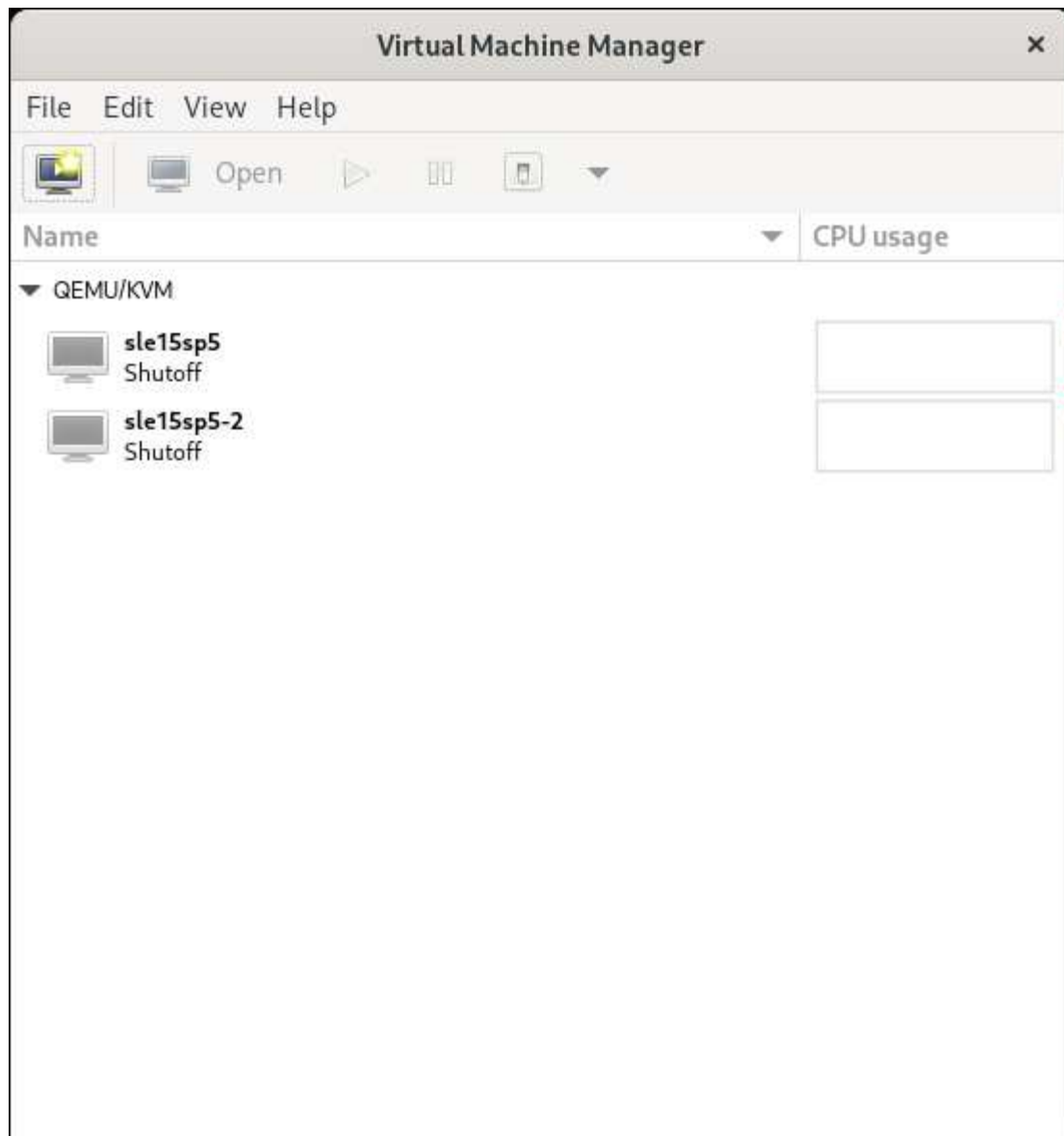
Paso 4: Asignar las interfaces virtuales a la máquina virtual

Asigne las funciones virtuales creadas a la máquina virtual SAP HANA como dispositivos host PCI mediante *virt-manager*.

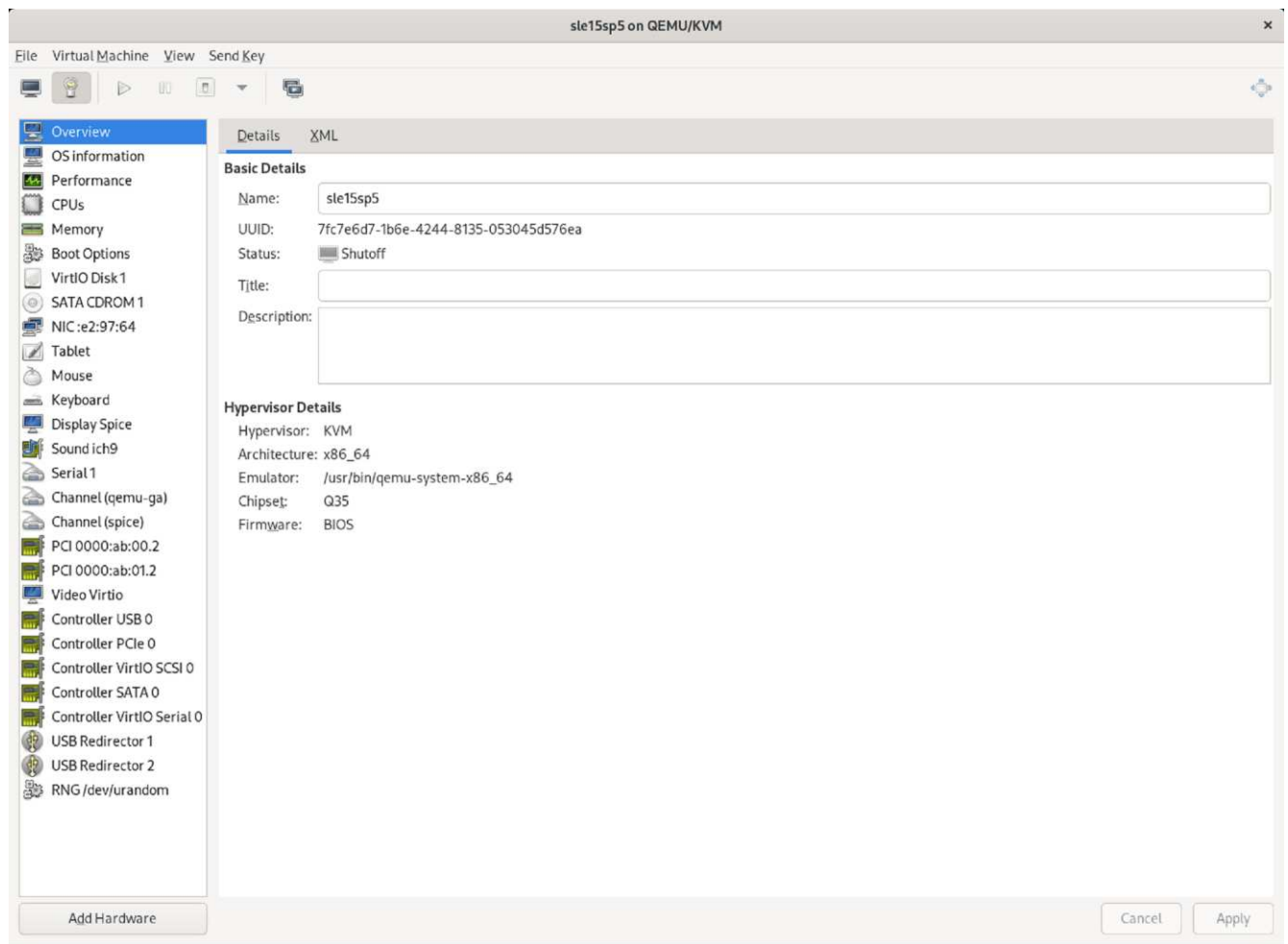
1. Inicie virt-manager.



2. Abra la máquina virtual deseada.

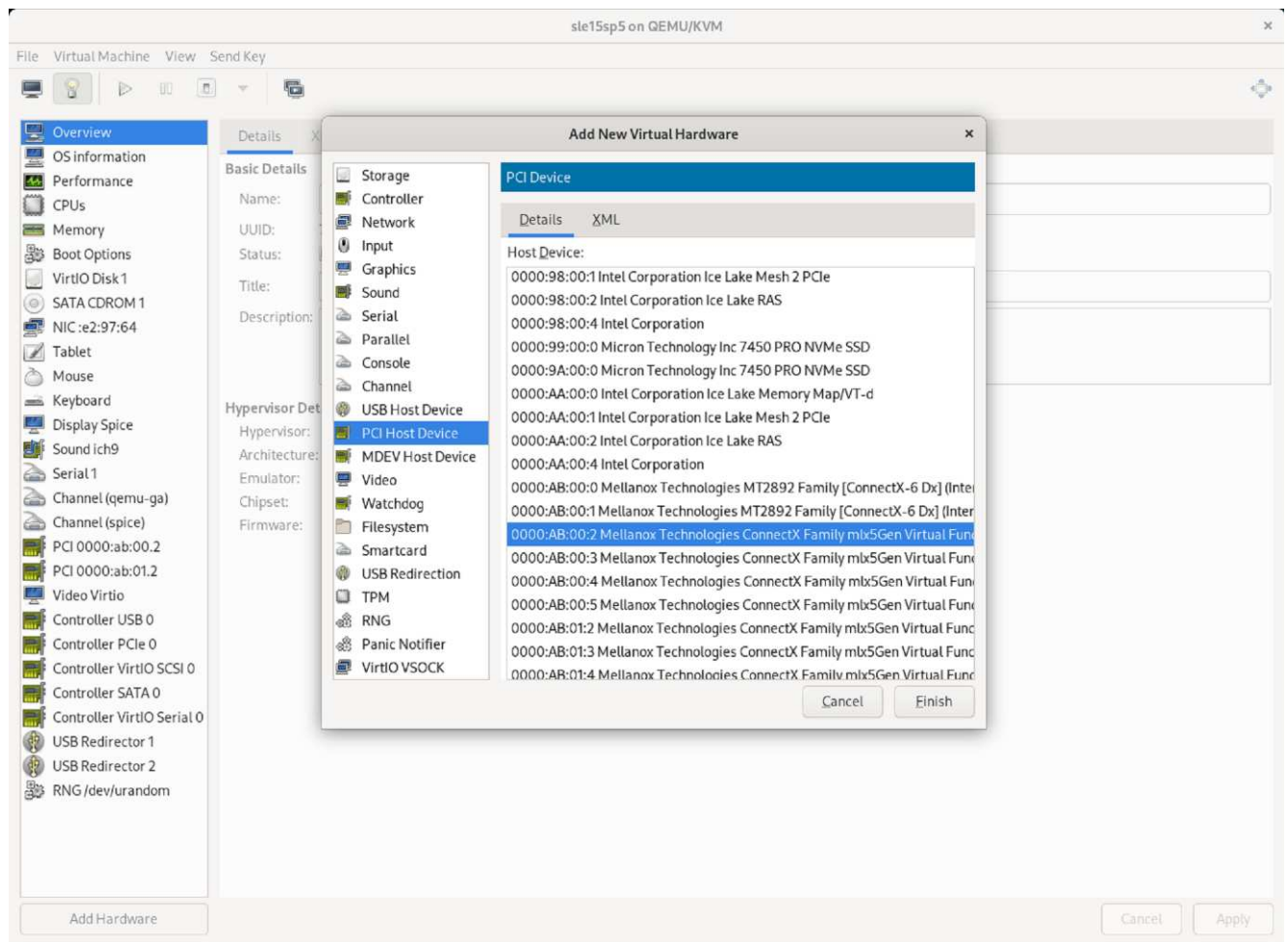


3. Seleccione **Agregar hardware.** +

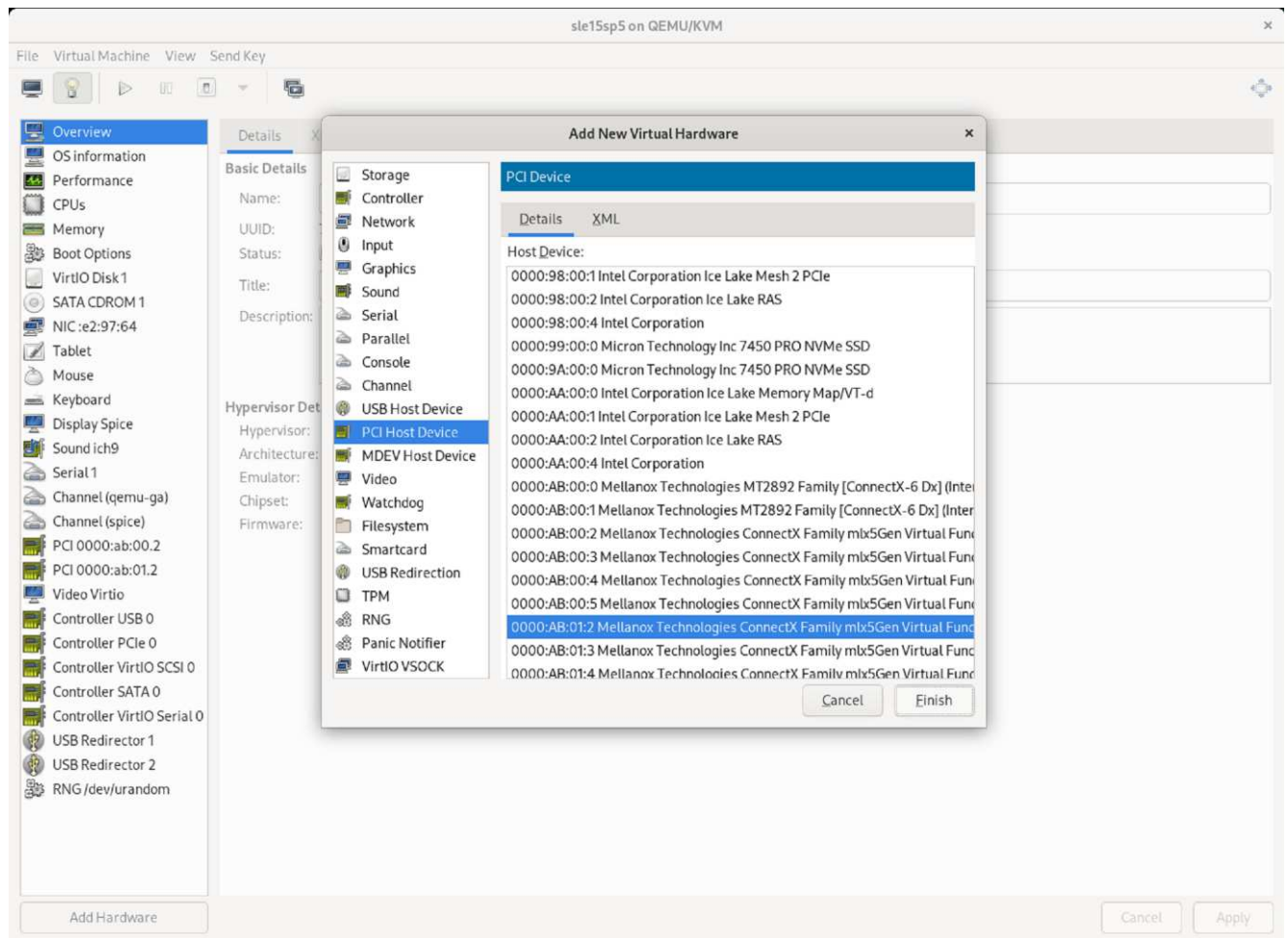


4. Elija la NIC virtual deseada del primer puerto físico de la lista de dispositivos host PCI y pulse Finalizar.

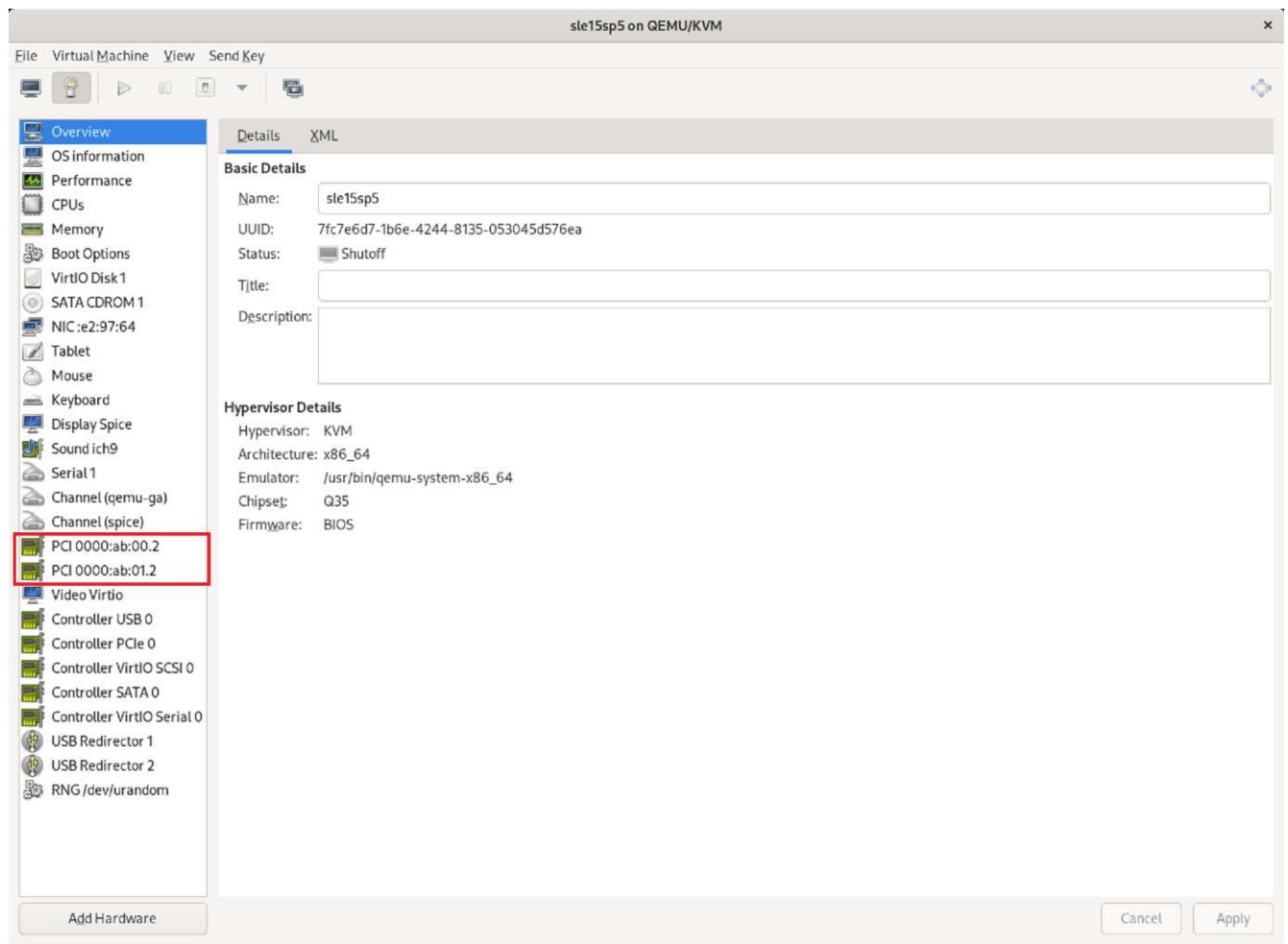
En este ejemplo, 0000.AB:00:2 - 0000.AB:00:4 pertenecen al primer puerto físico y 0000.AB:01:2 - 0000.AB:01:4 pertenecen al segundo puerto físico.



5. Elija el siguiente puerto NIC virtual de la lista de dispositivos host PCI, utilice un puerto virtual del segundo puerto físico y seleccione **Finalizar**.

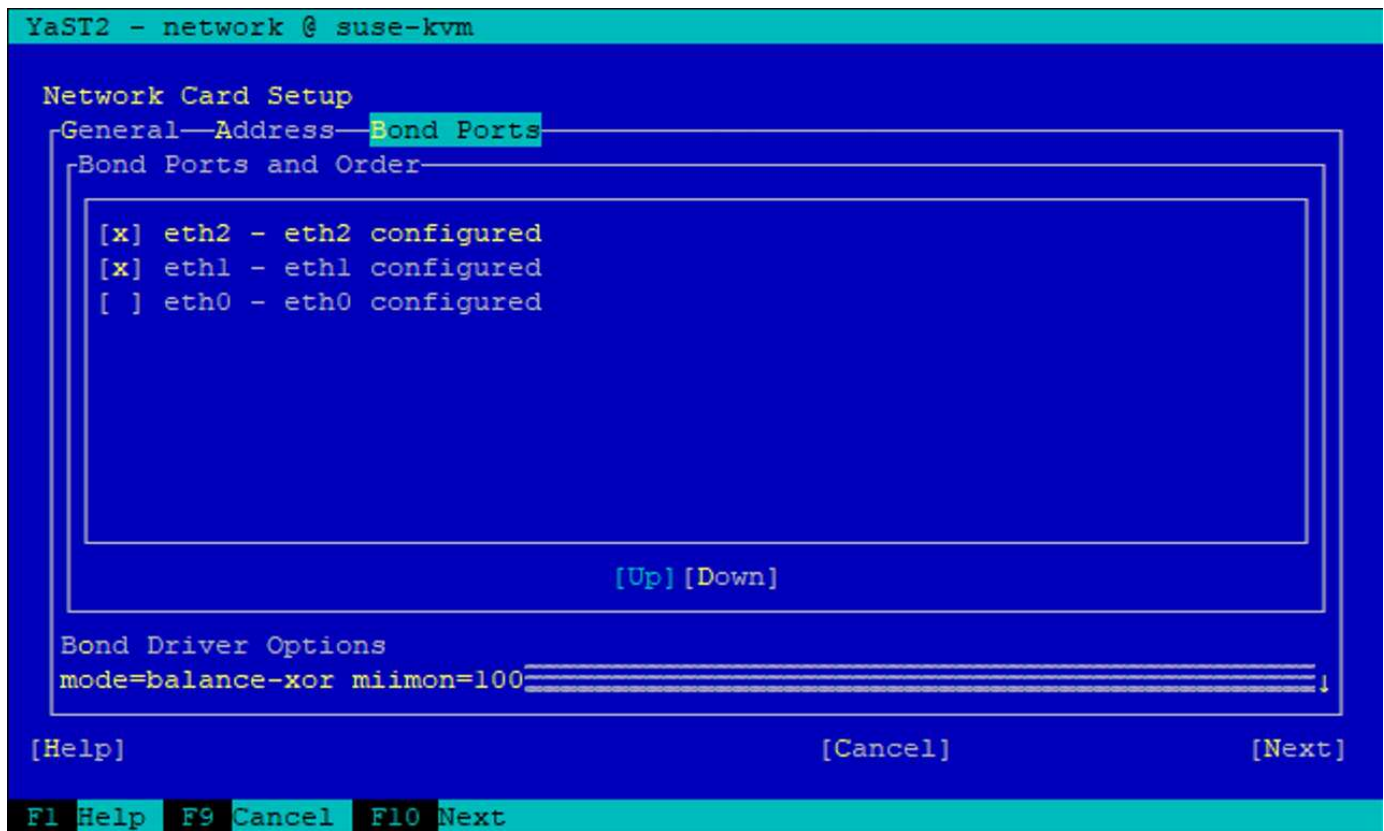


6. Posteriormente, las interfaces virtuales se asignan a la máquina virtual y esta puede iniciarse. +



Paso 5: Configurar las interfaces de red dentro de la máquina virtual

Inicie sesión en la máquina virtual y configure las dos VF como enlace. Elija el modo 0 o el modo 2. No utilice LACP, ya que LACP solo se puede usar en puertos físicos. La figura siguiente muestra una configuración de modo 2 utilizando YAST.



¿Que sigue?

Una vez configuradas las interfaces de red SR-IOV, "[Configurar redes Fibre Channel](#)" si se va a utilizar FCP como protocolo de almacenamiento.

Configurar la red Fibre Channel para SAP HANA en SUSE KVM

Configure la red Fibre Channel para SAP HANA en SUSE KVM asignando puertos HBA físicos a las máquinas virtuales como dispositivos PCI. Configure conexiones FCP redundantes utilizando dos puertos físicos conectados a diferentes conmutadores de estructura.



Los siguientes pasos solo son necesarios si se utiliza FCP como protocolo de almacenamiento. Si se utiliza NFS, estos pasos no son necesarios.

Acerca de esta tarea

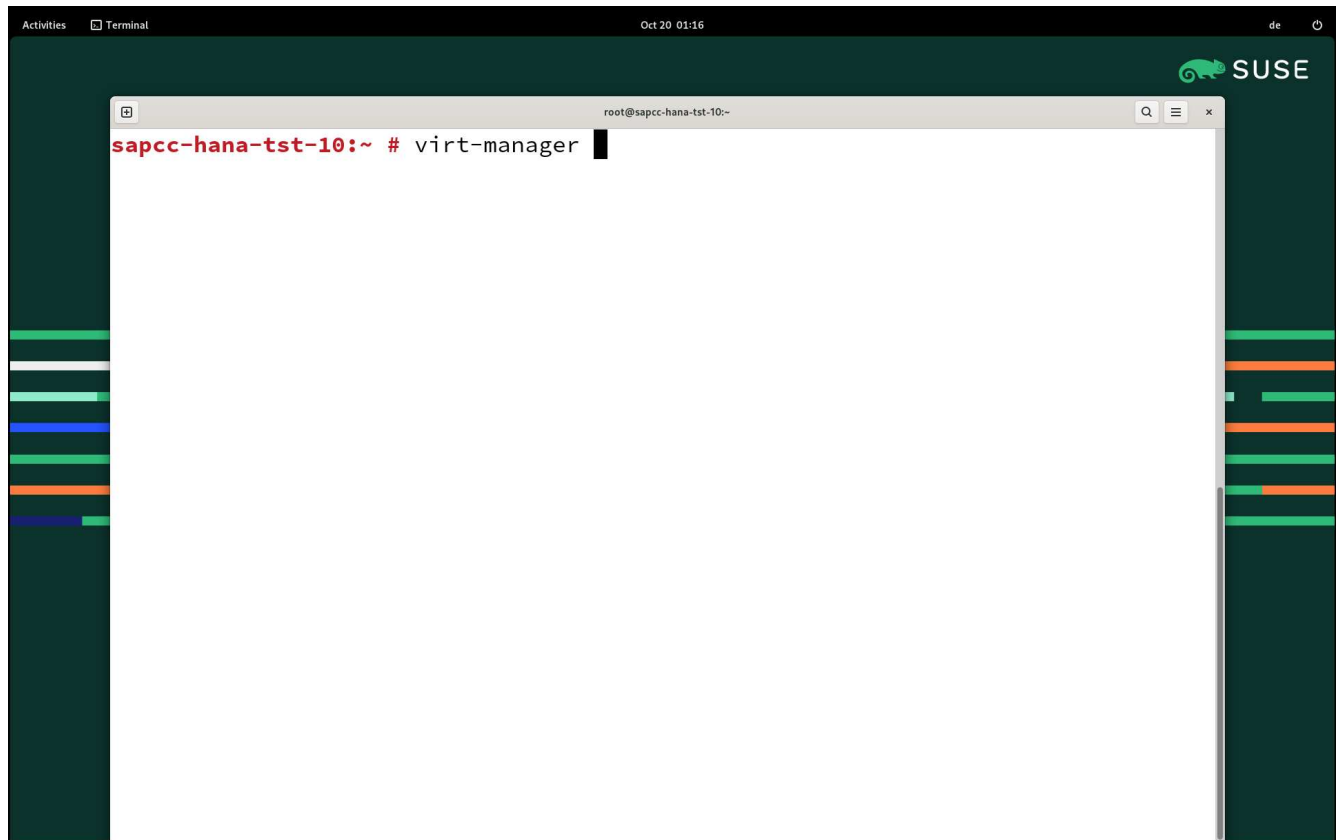
Como no existe ninguna función equivalente a SR-IOV para FCP, asigne los puertos HBA físicos directamente a la máquina virtual. Utilice dos puertos físicos conectados a diferentes tejidos para redundancia.



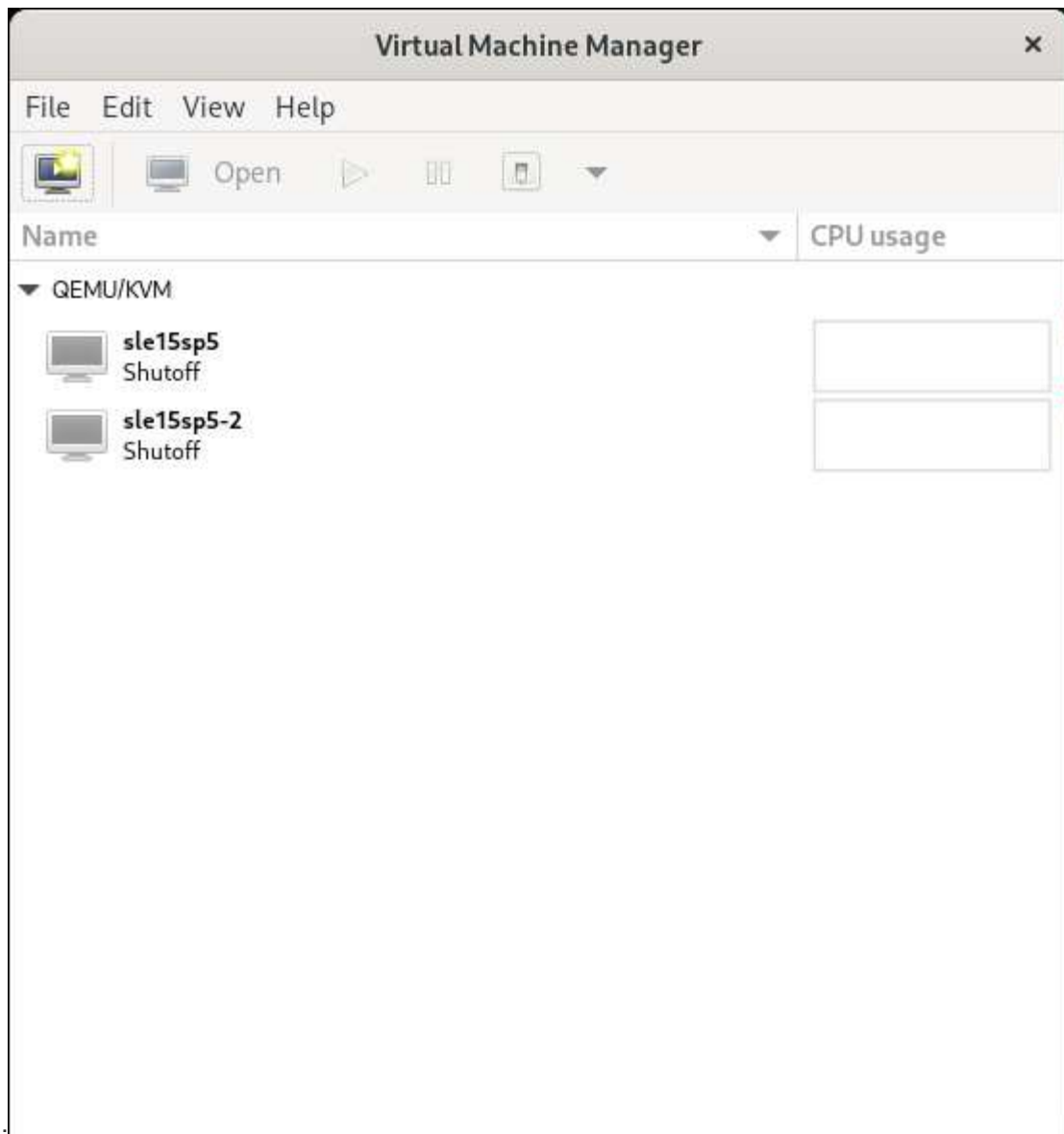
Un puerto físico solo puede asignarse a una máquina virtual.

Pasos

1. Inicie virt-manager:

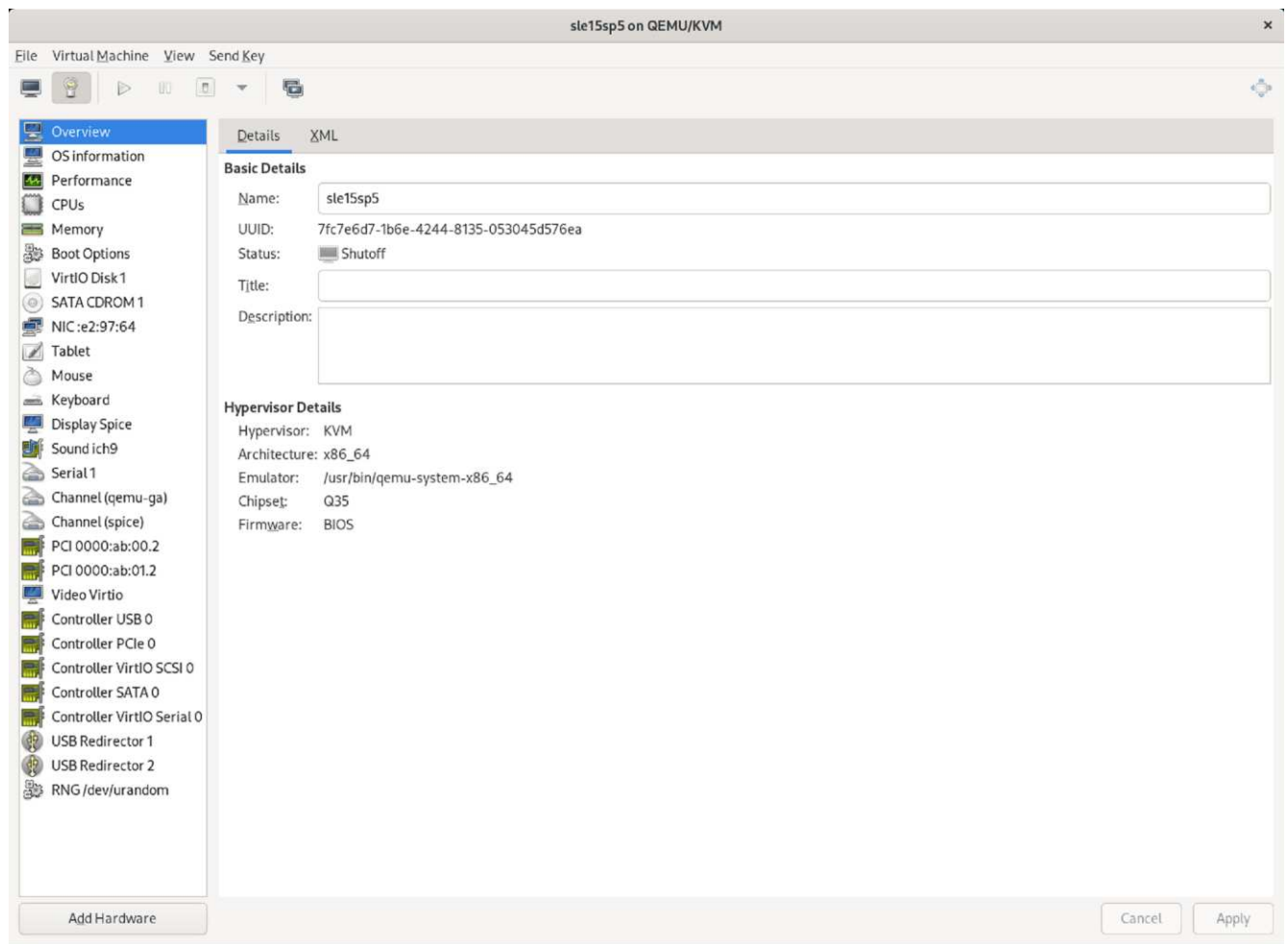


2. Abra la máquina virtual



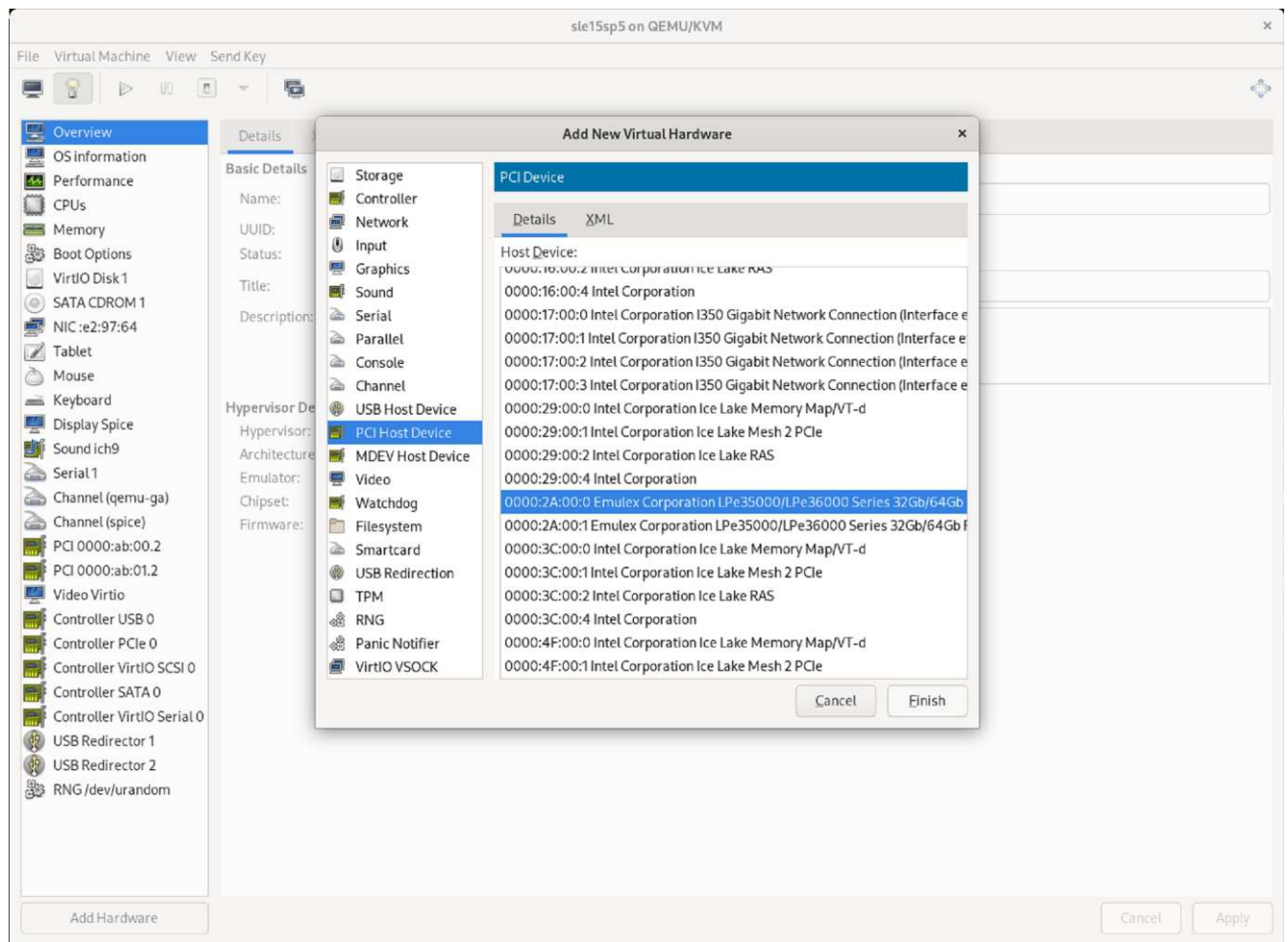
deseada.

3. Seleccione **Agregar hardware**.

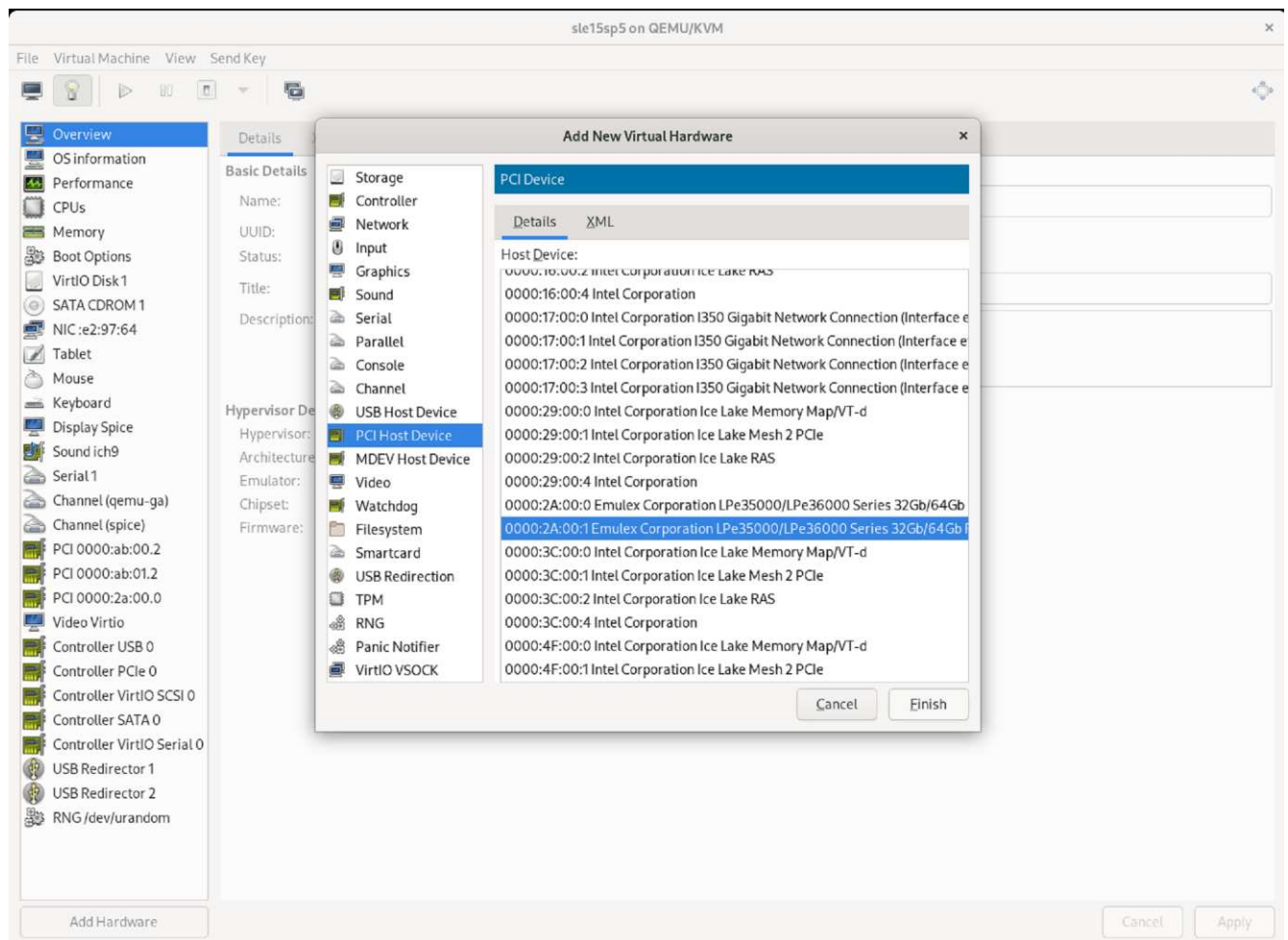


4. Seleccione el puerto HBA deseado de la lista de dispositivos host PCI y pulse Finalizar.

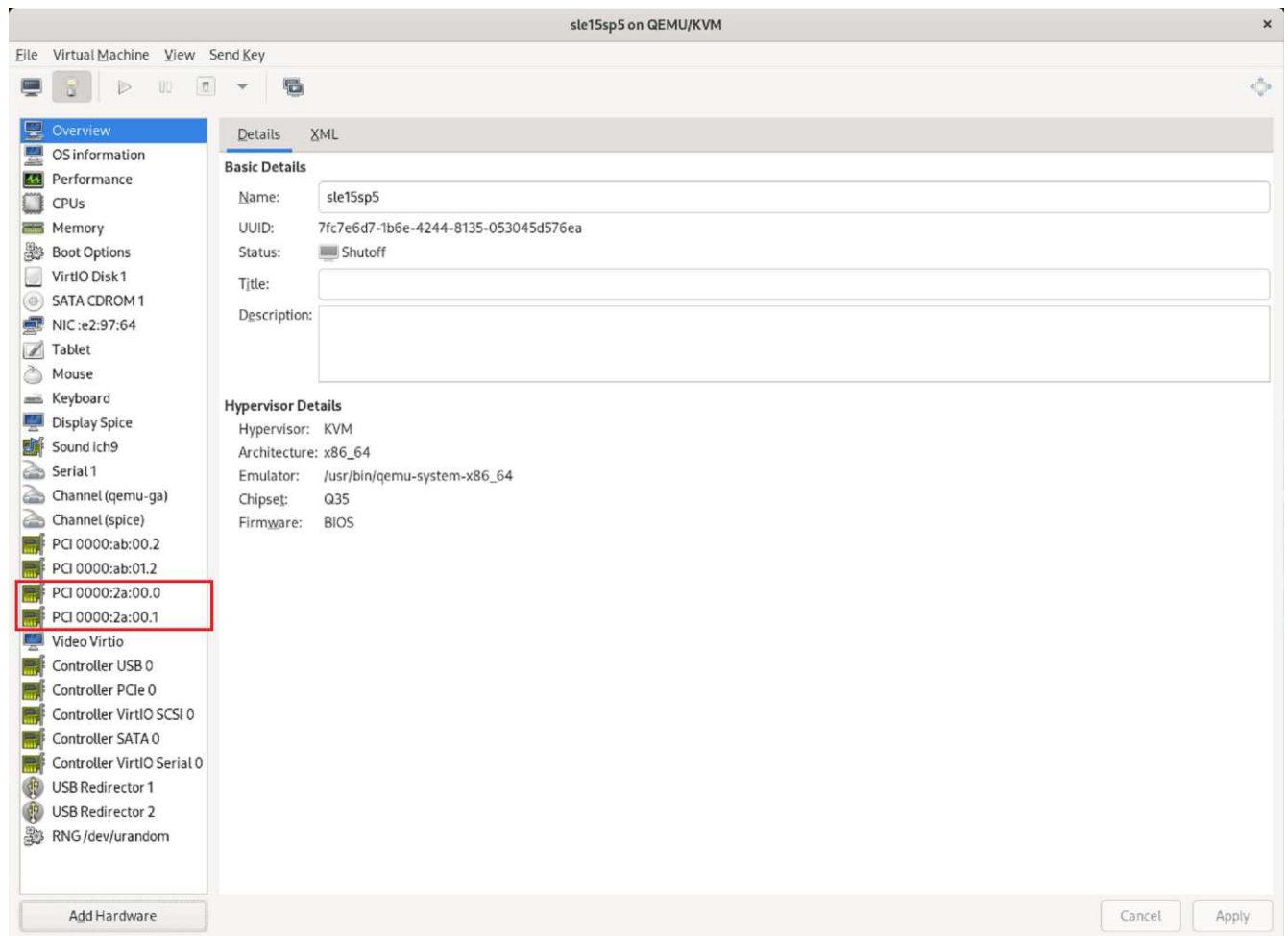
En este ejemplo 0000.A2:00:0.



5. Seleccione el puerto HBA deseado de la lista de dispositivos host PCI pertenecientes al segundo tejido y pulse Finalizar. En este ejemplo 0000.A2:00:1.



6. Posteriormente, los puertos HBA físicos se asignan a la máquina virtual y esta puede iniciarse.



Los puertos físicos se transfieren a la máquina virtual, por lo que no se requiere ninguna preparación adicional dentro de la misma.

¿Que sigue?

Una vez que hayas configurado la red Fibre Channel, "[Configurar el almacenamiento NetApp para SAP HANA](#)".

Configurar el almacenamiento NetApp para SAP HANA en SUSE KVM

Configure el almacenamiento NetApp para SAP HANA en SUSE KVM utilizando los protocolos NFS o FCP. Configure las conexiones de almacenamiento entre la máquina virtual y los sistemas NetApp ONTAP para un rendimiento óptimo de la base de datos.

Después de configurar la máquina virtual con interfaces de red SR-IOV o puertos HBA FCP, configure el acceso al almacenamiento desde dentro de la máquina virtual. Utilice la guía de configuración de NetApp SAP HANA adecuada según el protocolo de almacenamiento elegido.

Configurar el almacenamiento NFS para SAP HANA

Utilice las interfaces de red SR-IOV creadas previamente si se va a utilizar el protocolo NFS para el

almacenamiento de SAP HANA.

Siga los pasos de configuración detallados en el ["SAP HANA en sistemas NetApp AFF con NFS: Guía de configuración de"](#) .

Consideraciones clave de configuración para entornos KVM:

- Utilice las funciones virtuales (VF) SR-IOV configuradas anteriormente para el tráfico de red.
- Configure la agregación de enlaces de red dentro de la máquina virtual para redundancia.
- Asegúrese de que la conmutación de red entre la máquina virtual y los SVM de almacenamiento NetApp sea la correcta.
- Configure los controladores de almacenamiento y la máquina virtual de acuerdo con la Guía de configuración de SAP HANA.

Configurar el almacenamiento FCP para SAP HANA

Utilice los puertos HBA físicos asignados a la máquina virtual como dispositivos PCI si se va a utilizar el protocolo FCP para el almacenamiento de SAP HANA.

Elija la guía de configuración adecuada según su sistema de almacenamiento NetApp :

- Para sistemas NetApp AFF : ["SAP HANA en sistemas AFF de NetApp con el protocolo Fibre Channel"](#)
- Para sistemas NetApp ASA : ["SAP HANA en sistemas ASA de NetApp con el protocolo Fibre Channel"](#)

Consideraciones clave de configuración para entornos KVM:

- Utilice los puertos HBA físicos que se asignaron a la máquina virtual mediante PCI passthrough.
- Configure el enrutamiento de múltiples rutas dentro de la máquina virtual para lograr redundancia entre los conmutadores de la estructura.
- Configure los controladores de almacenamiento y las máquinas virtuales de acuerdo con la Guía de configuración de SAP HANA.

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.