



SAP HANA mit SUSE KVM und NetApp Storage

NetApp solutions for SAP

NetApp
November 12, 2025

Inhalt

SAP HANA mit SUSE KVM und NetApp Storage	1
SAP HANA auf SUSE KVM mit NetApp -Speicher unter Verwendung von SR-IOV und NFS bereitstellen ..	1
Bereitstellungsanforderungen für SAP HANA auf SUSE KVM mit NetApp -Speicher	1
Infrastrukturanforderungen	2
Wichtige Überlegungen	2
Zusätzliche Ressourcen	2
Wie geht es weiter?	2
Konfigurieren Sie SR-IOV-Netzwerkschnittstellen für SAP HANA auf SUSE KVM	2
Schritt 1: SR-IOV einrichten	3
Schritt 2: Virtuelle Schnittstellen erstellen	5
Schritt 3: VFs beim Systemstart aktivieren	11
Schritt 4: Weisen Sie der VM die virtuellen Schnittstellen zu	12
Schritt 5: Netzwerkschnittstellen innerhalb der VM konfigurieren	18
Wie geht es weiter?	19
Konfigurieren Sie Fibre Channel-Netzwerke für SAP HANA auf SUSE KVM	19
Wie geht es weiter?	25
NetApp Speicher für SAP HANA auf SUSE KVM konfigurieren	25
Konfigurieren Sie NFS-Speicher für SAP HANA	25
FCP-Speicher für SAP HANA konfigurieren	26

SAP HANA mit SUSE KVM und NetApp Storage

SAP HANA auf SUSE KVM mit NetApp -Speicher unter Verwendung von SR-IOV und NFS bereitstellen

Bereitstellung von SAP HANA Single-Host auf SUSE KVM unter Verwendung von NetApp -Speicher mit SR-IOV-Netzwerkschnittstellen und NFS- oder FCP-Speicherzugriff. Folgen Sie diesem Workflow, um virtuelle Schnittstellen zu konfigurieren, sie VMs zuzuweisen und Speicherverbindungen für eine optimale Leistung einzurichten.

Einen Überblick über SAP HANA auf KVM-Virtualisierung finden Sie in der SUSE-Dokumentation: ["SUSE Best Practices für SAP HANA auf KVM"](#) Die

1

"Überprüfen der Konfigurationsanforderungen"

Prüfen Sie die wichtigsten Anforderungen für die Bereitstellung von SAP HANA auf SUSE KVM unter Verwendung von NetApp -Speicher mit SR-IOV und Speicherprotokollen.

2

"Konfigurieren der SR-IOV-Netzwerkschnittstellen"

Richten Sie SR-IOV (Single Root I/O Virtualization) auf dem KVM-Host ein und weisen Sie der VM virtuelle Schnittstellen für die Netzwerkkommunikation und den Speicherzugriff zu.

3

"Fibre Channel-Netzwerk konfigurieren"

Weisen Sie der VM physische FCP HBA-Ports als PCI-Geräte zu, um FCP LUNs mit SAP HANA zu verwenden.

4

"NetApp Speicher für SAP HANA konfigurieren"

Richten Sie NFS- oder FCP-Speicherverbindungen zwischen der VM und den NetApp -Speichersystemen für SAP HANA-Datenbankdateien ein.

Bereitstellungsanforderungen für SAP HANA auf SUSE KVM mit NetApp -Speicher

Prüfen Sie die Anforderungen für die Bereitstellung von SAP HANA Single-Host auf SUSE KVM unter Verwendung von NetApp -Speicher mit SR-IOV-Netzwerkschnittstellen und NFS- oder FCP-Speicherprotokollen.

Für die Implementierung werden zertifizierte SAP HANA-Server, NetApp -Speichersysteme, SR-IOV-fähige Netzwerkadapter und SUSE Linux Enterprise Server für SAP-Anwendungen als KVM-Host benötigt.

Infrastrukturanforderungen

Stellen Sie sicher, dass die folgenden Komponenten und Konfigurationen vorhanden sind:

- Zertifizierte SAP HANA-Server und NetApp Speichersysteme. Siehe die ["SAP HANA Hardwareverzeichnis"](#) für verfügbare Optionen:
- SUSE Linux Enterprise Server für SAP-Anwendungen 15 SP5/SP6 als KVM-Host
- NetApp ONTAP -Speichersystem mit Storage Virtual Machine (SVM), konfiguriert für NFS- und/oder FCP-Datenverkehr
- Logische Schnittstellen (LIFs) wurden auf den entsprechenden Netzwerken für NFS- und FCP-Datenverkehr erstellt.
- SR-IOV-fähige Netzwerkadapter (z. B. Mellanox ConnectX-Serie)
- Fibre Channel HBA-Adapter für FCP-Speicherzugriff
- Netzwerkinfrastruktur zur Unterstützung der erforderlichen VLANs und Netzwerksegmente
- Die VM ist gemäß der ["SUSE Best Practices für SAP HANA auf KVM"](#)

Wichtige Überlegungen

- SR-IOV muss für die SAP HANA-Netzwerkkommunikation und für den Speicherzugriff über NFS verwendet werden. Jede einer VM zugewiesene virtuelle Funktion (VF) benötigt eine Bandbreite von mindestens 10 Gbit/s.
- Physische FCP-HBA-Ports müssen der VM als PCI-Geräte zugewiesen werden, damit FCP-LUNs verwendet werden können. Ein physischer Port kann nur einer VM zugewiesen werden.
- SAP HANA Multi-Host-Systeme werden in dieser Konfiguration nicht unterstützt.

Zusätzliche Ressourcen

- Aktuelle Informationen, einschließlich unterstützter CPU-Architekturen und Einschränkungen, finden Sie im SAP-Hinweis. ["3538596 - SAP HANA auf SUSE KVM-Virtualisierung mit SLES 15 SP5 - SAP für mich"](#) Die
- Informationen zur Konfiguration von ONTAP Speichersystemen finden Sie in der ["ONTAP 9 Dokumentation"](#) Die
- Informationen zur SAP HANA-Speicherkonfiguration mit NetApp -Systemen finden Sie unter ["NetApp SAP-Lösungsdokumentation"](#) Die

Wie geht es weiter?

Nachdem Sie die Bereitstellungsanforderungen geprüft haben, ["SR-IOV-Netzwerkschnittstellen konfigurieren"](#) Die

Konfigurieren Sie SR-IOV-Netzwerkschnittstellen für SAP HANA auf SUSE KVM

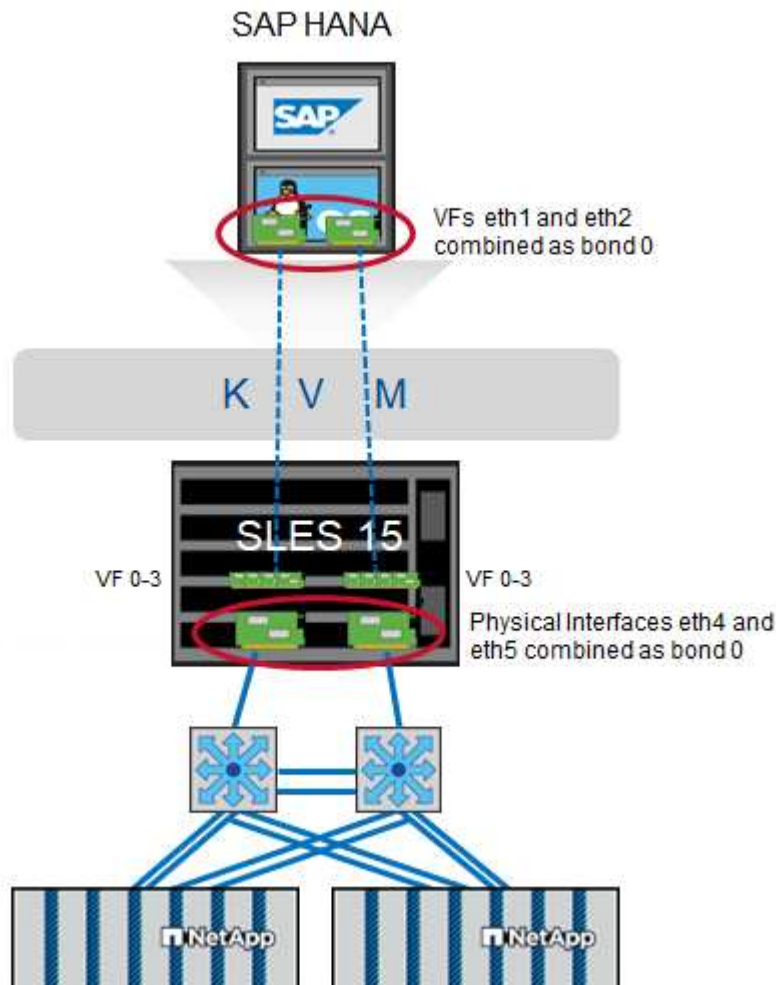
Konfigurieren Sie SR-IOV-Netzwerkschnittstellen auf SUSE KVM für SAP HANA. Richten Sie virtuelle Funktionen (VFs) ein, weisen Sie diese virtuellen Maschinen (VMs) zu und konfigurieren Sie redundante Netzwerkverbindungen für optimale Leistung und optimalen Speicherzugriff.

Schritt 1: SR-IOV einrichten

Aktivieren und konfigurieren Sie die SR-IOV-Funktionalität in der Adapter-Firmware, um die Erstellung virtueller Funktionen zu ermöglichen.

Dieses Verfahren basiert auf ["NVIDIA Enterprise Support Portal | Anleitung zur Konfiguration von SR-IOV für ConnectX-4/ConnectX-5/ConnectX-6 mit KVM \(Ethernet\)"](#). Im SUSE SAP HANA KVM-Leitfaden wird dies anhand einer INTEL-Netzwerkkarte beschrieben.

Es wird empfohlen, redundante Ethernet-Verbindungen zu nutzen, indem zwei physische Ports als Trunk/Bond kombiniert werden. Die der VM zugewiesenen virtuellen Ports (VF) müssen auch innerhalb der VM als Trunks konfiguriert werden.



Bevor Sie beginnen

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- KVM ist installiert
- SR-IOV ist im BIOS des Servers aktiviert.
- PCI-Passthrough wird aktiviert, indem „intel_iommu=on“ und „iommu=pt“ als Optionen im Bootloader hinzugefügt werden.
- Auf den KVM-Hosts und VMs sind die neuesten MLNX_OFED-Treiber installiert.



Jede einer VM zugewiesene VF benötigt eine Bandbreite von mindestens 10 Gbit/s. Erstellen und zuweisen Sie nicht mehr als zwei VFs für einen physischen 25GbE-Port.

Schritte

1. Führen Sie MFT (Mellanox Firmware Tools) aus:

```
# 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. Gerät lokalisieren:

```
# 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. Überprüfen Sie den Gerätestatus:

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

4. Aktivieren Sie gegebenenfalls SR-IOV:

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

5. Maximale Anzahl an VFs festlegen:

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

6. Starten Sie den Server neu, falls die Funktion aktiviert werden musste oder die maximale Anzahl virtueller Funktionen geändert wurde.

Schritt 2: Virtuelle Schnittstellen erstellen

Erstellen Sie virtuelle Funktionen (VFs) auf den physischen Netzwerkports, um die SR-IOV-Funktionalität zu aktivieren. In diesem Schritt werden pro physischem Port vier VFs erstellt.

Schritte

1. Gerät finden:

```
# 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
```

Wenn eine Anleihe erstellt wurde, sähe die Ausgabe wie folgt aus:


```
# 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. Ermitteln Sie die Gesamtzahl der in der Firmware zulässigen und konfigurierten VFs:

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

3. Ermitteln Sie die aktuelle Anzahl der VFs auf diesem Gerät:

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

4. Die gewünschte Anzahl an VFs einstellen:

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

Falls Sie bereits eine Verbindung über diese beiden Ports konfiguriert haben, muss der erste Befehl für diese Verbindung ausgeführt werden:

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

5. Überprüfen Sie den PCI-Bus:

```
# 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. Überprüfen Sie die VF-Konfiguration mithilfe des IP-Tools:

```
# 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
...
```

Schritt 3: VFs beim Systemstart aktivieren

Konfigurieren Sie die VF-Einstellungen so, dass sie auch nach Systemneustarts erhalten bleiben, indem Sie systemd-Dienste und Startskripte erstellen.

1. Erstelle eine systemd-Unit-Datei `/etc/systemd/system/after.local` mit folgendem Inhalt:

```
[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. Erstelle das Skript */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
```

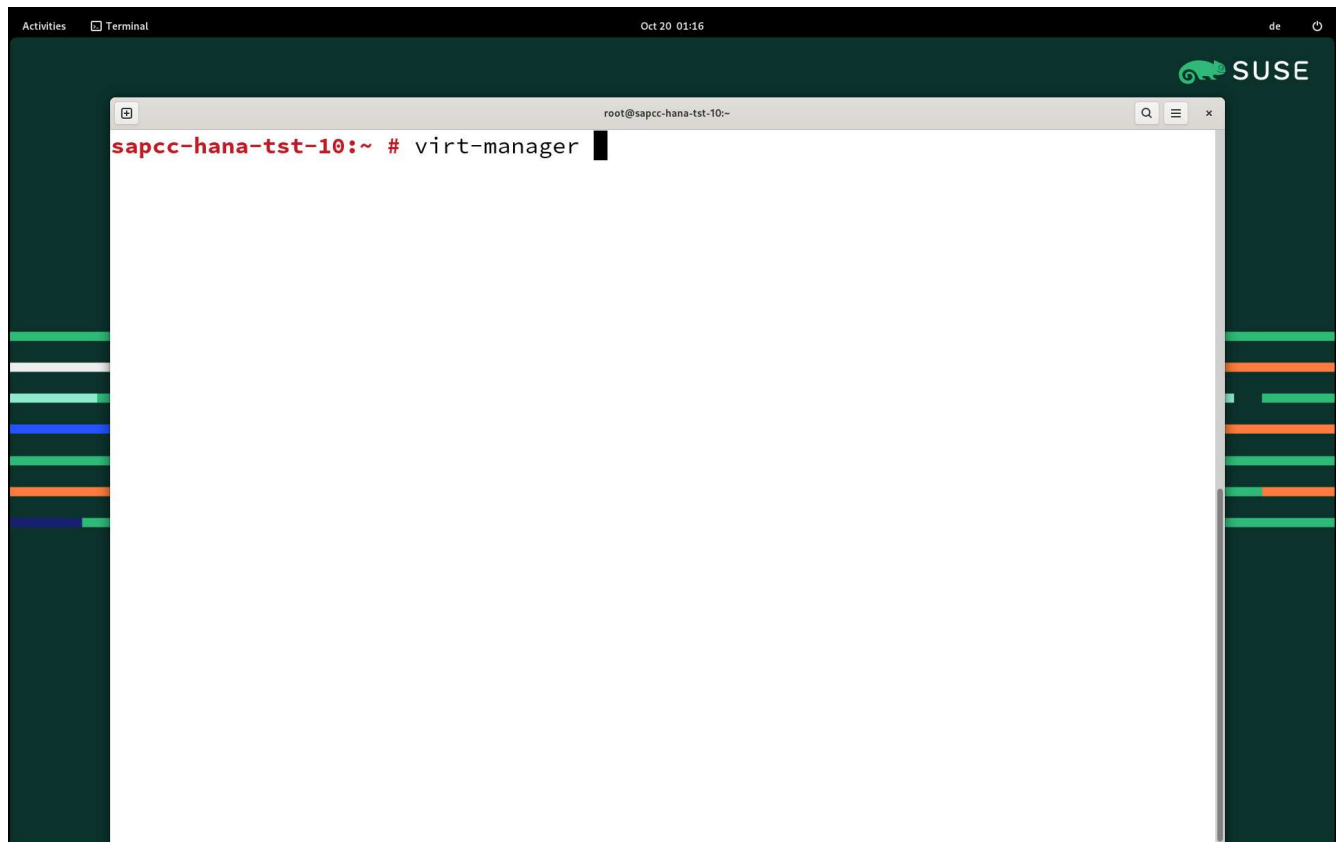
3. Stellen Sie sicher, dass die Datei ausgeführt werden kann:

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

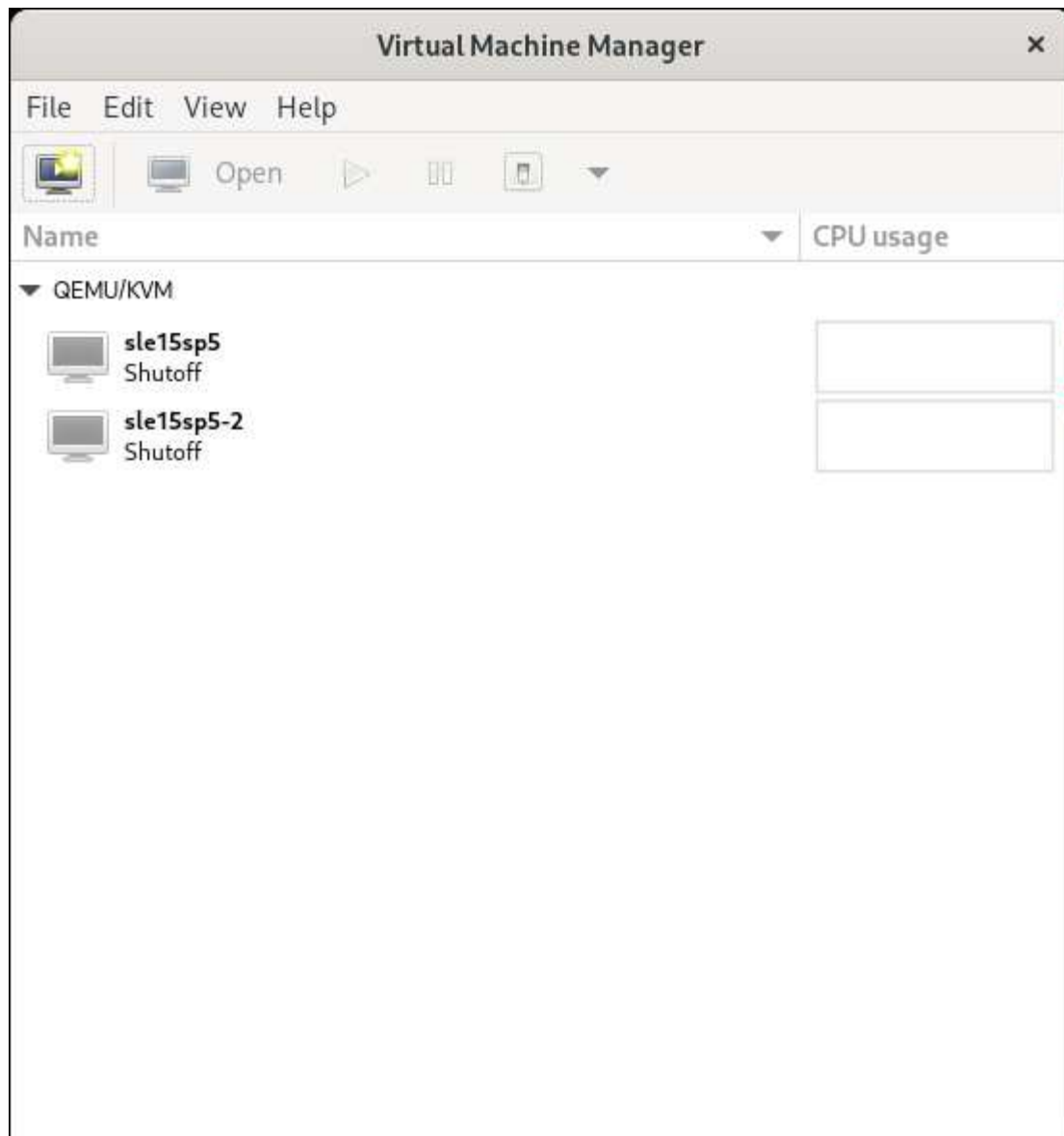
Schritt 4: Weisen Sie der VM die virtuellen Schnittstellen zu.

Weisen Sie die erstellten virtuellen Funktionen der SAP HANA VM als PCI-Hostgeräte mithilfe von *virt-manager* zu.

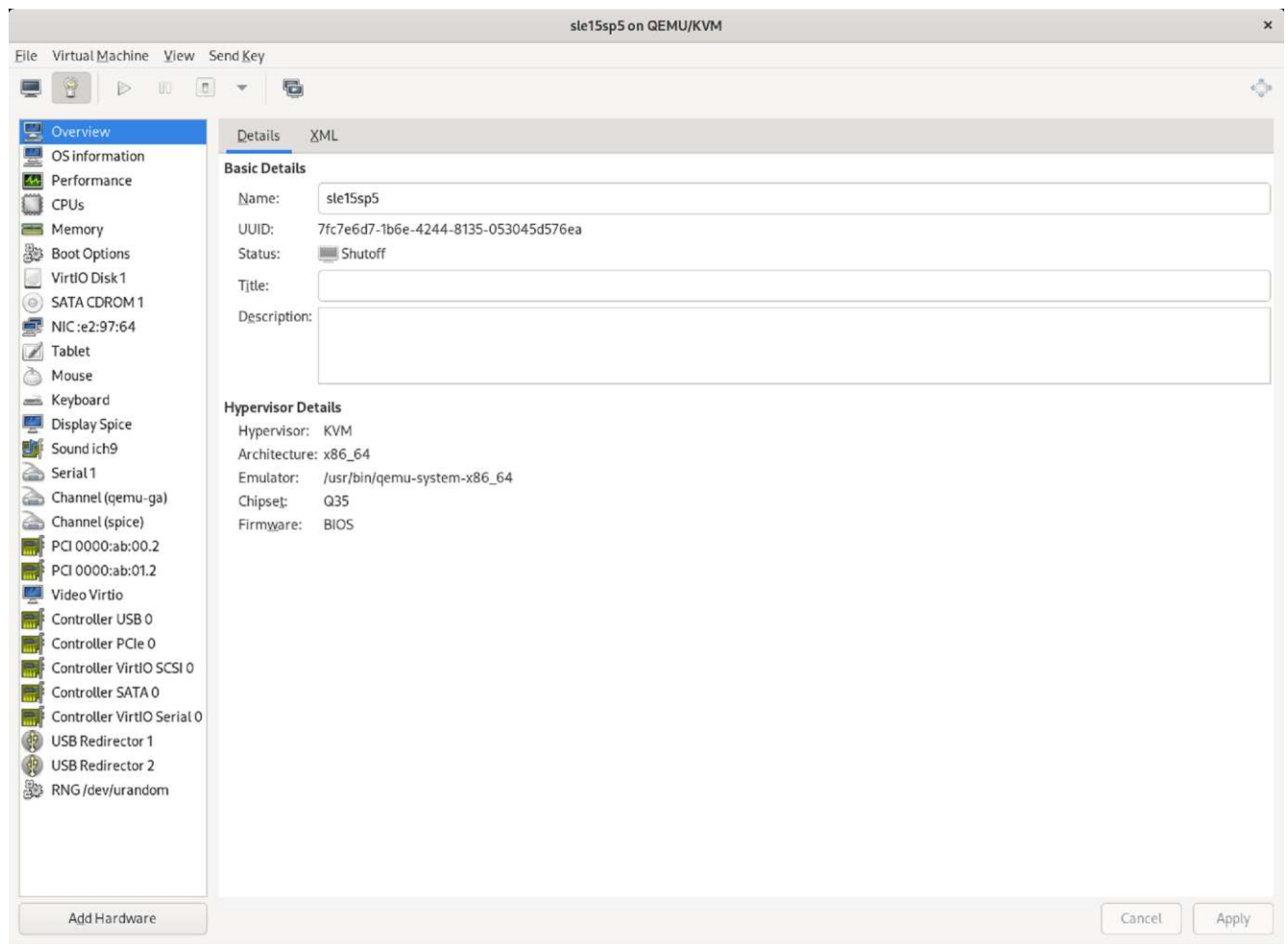
1. Starten Sie virt-manager.



2. Öffnen Sie die gewünschte VM.

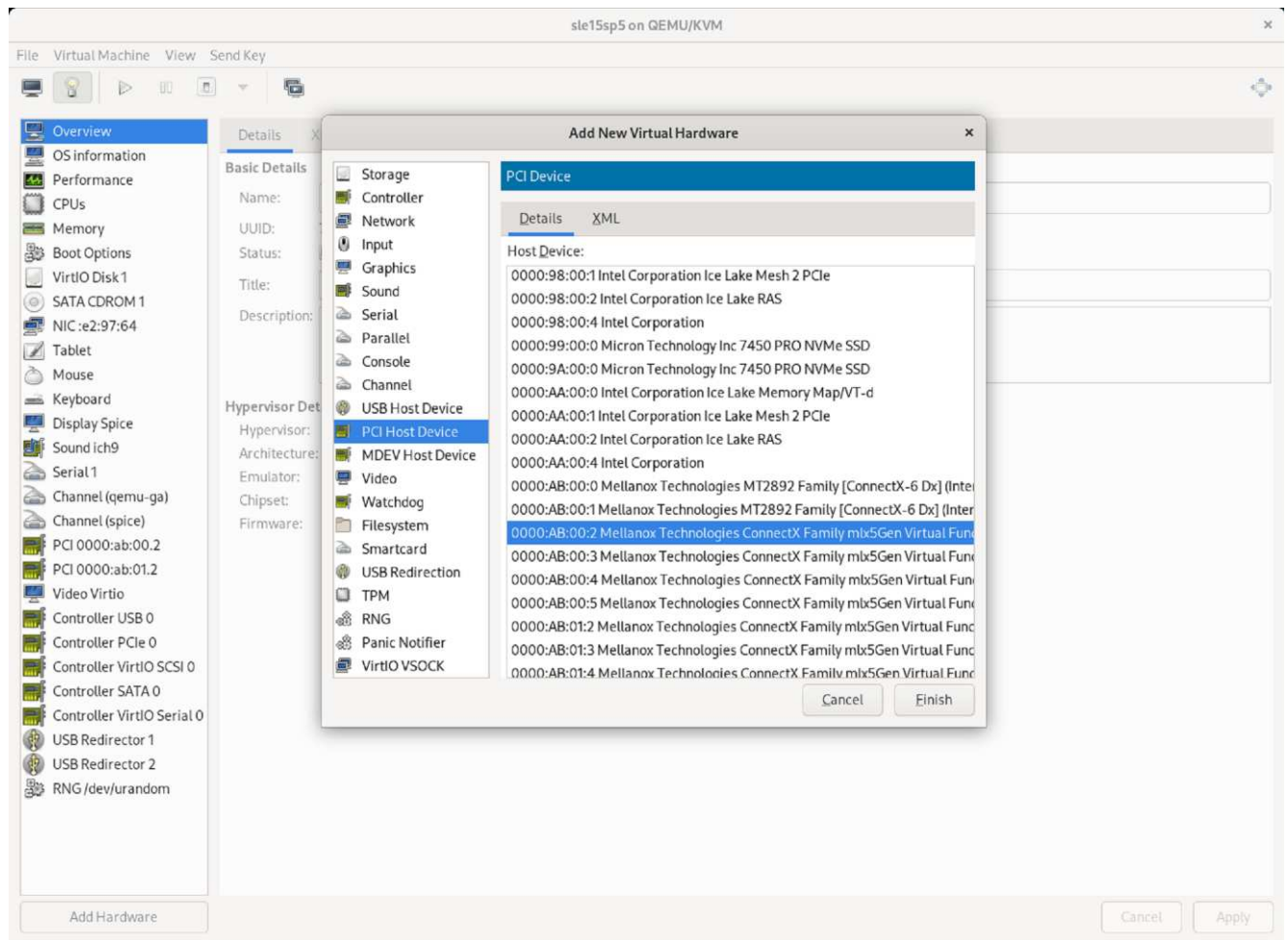


3. Wählen Sie **Hardware hinzufügen.** +

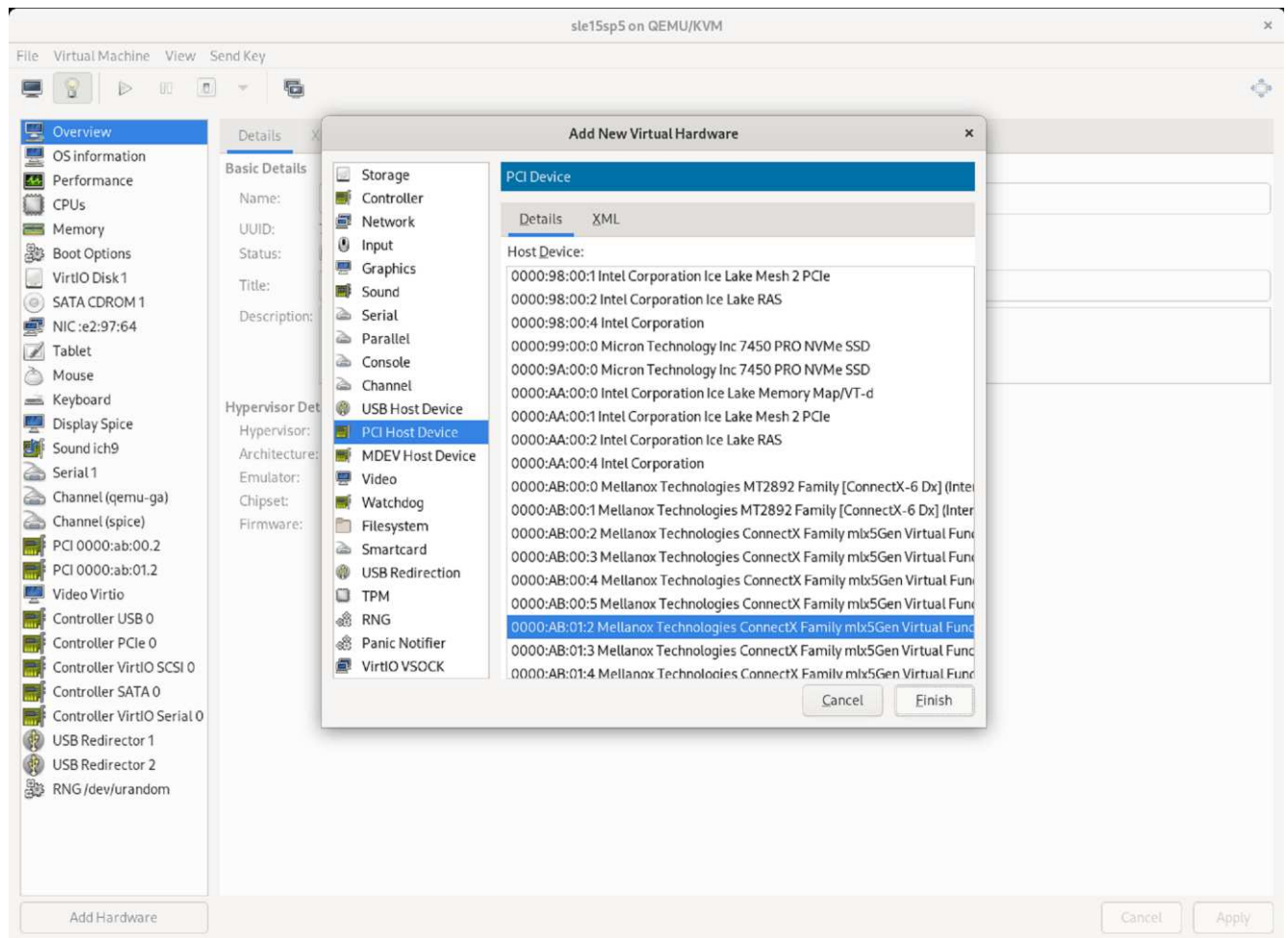


4. Wählen Sie die gewünschte virtuelle Netzwerkkarte aus dem ersten physischen Port in der Liste der PCI-Hostgeräte aus und klicken Sie auf „Fertigstellen“.

In diesem Beispiel gehören 0000.AB:00:2 - 0000.AB:00:4 zum ersten physischen Port und 0000.AB:01:2 - 0000.AB:01:4 zum zweiten physischen Port.

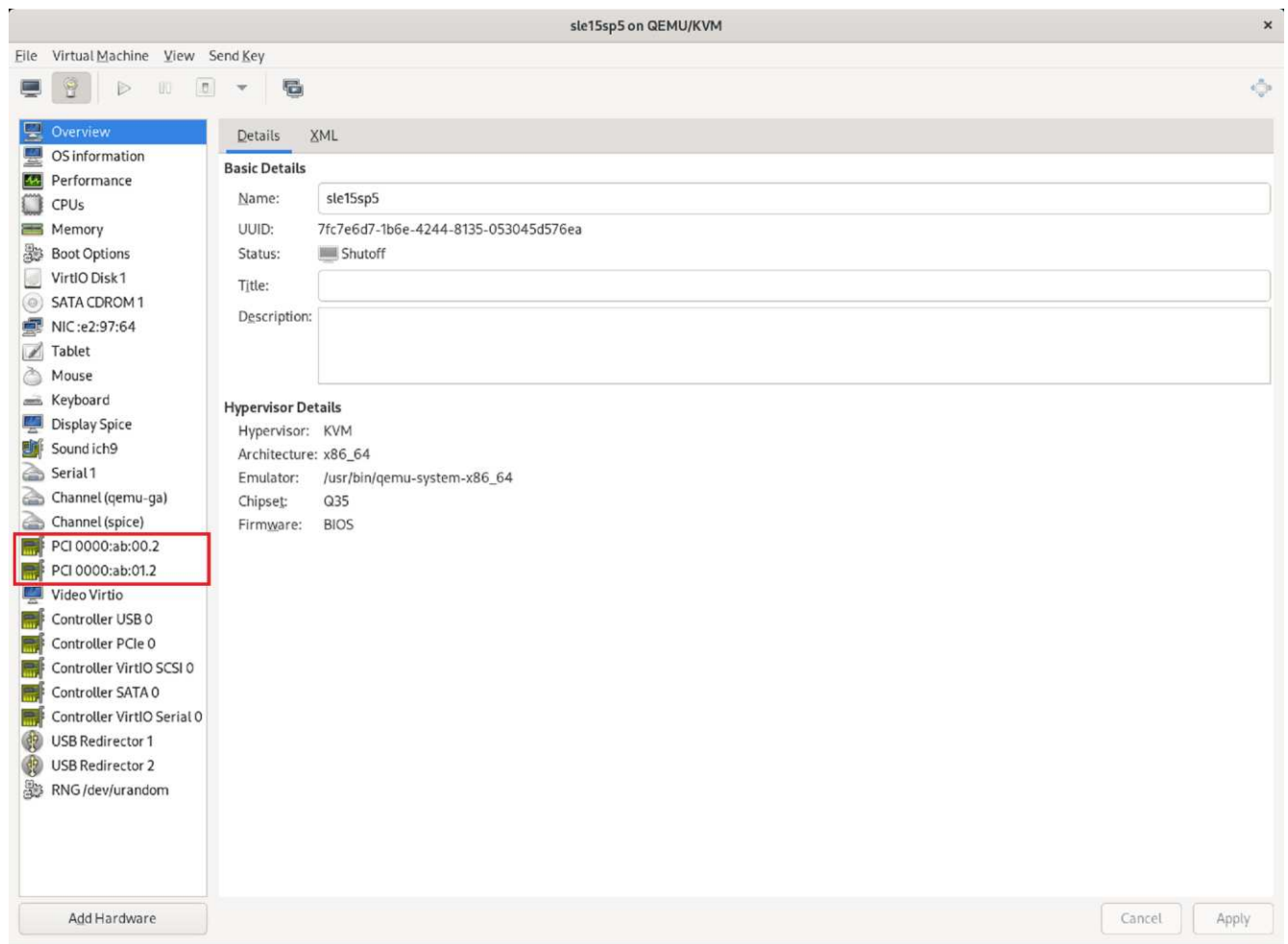


5. Wählen Sie den nächsten virtuellen NIC-Port aus der Liste der PCI-Hostgeräte, verwenden Sie einen virtuellen Port vom zweiten physischen Port und wählen Sie **Fertigstellen**.



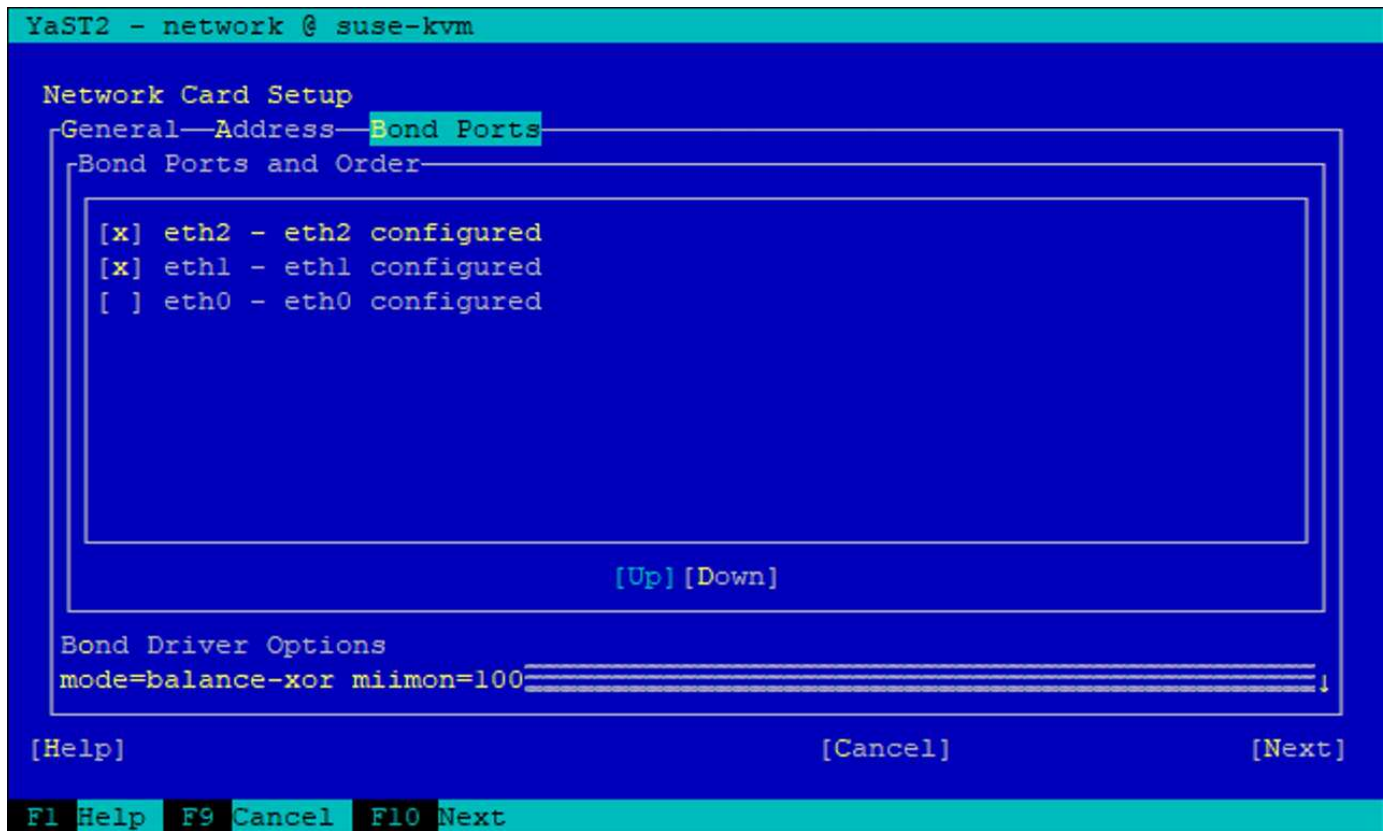
6. Anschließend werden die virtuellen Schnittstellen der VM zugewiesen und die VM kann gestartet werden.

+



Schritt 5: Netzwerkschnittstellen innerhalb der VM konfigurieren

Melden Sie sich in der VM an und konfigurieren Sie die beiden VFs als Bond. Wählen Sie entweder Modus 0 oder Modus 2. Verwenden Sie LACP nicht, da LACP nur an physischen Ports verwendet werden kann. Die folgende Abbildung zeigt eine Modus-2-Konfiguration mit YAST.



Wie geht es weiter?

Nachdem Sie die SR-IOV-Netzwerkschnittstellen konfiguriert haben, "[Fibre Channel-Netzwerk konfigurieren](#)" wenn FCP als Speicherprotokoll verwendet werden soll.

Konfigurieren Sie Fibre Channel-Netzwerke für SAP HANA auf SUSE KVM

Konfigurieren Sie Fibre Channel-Netzwerke für SAP HANA auf SUSE KVM, indem Sie VMs physische HBA-Ports als PCI-Geräte zuweisen. Richten Sie redundante FCP-Verbindungen ein, indem Sie zwei physische Ports verwenden, die an verschiedene Fabric-Switches angeschlossen sind.



Die folgenden Schritte sind nur erforderlich, wenn FCP als Speicherprotokoll verwendet wird. Bei Verwendung von NFS sind diese Schritte nicht erforderlich.

Informationen zu diesem Vorgang

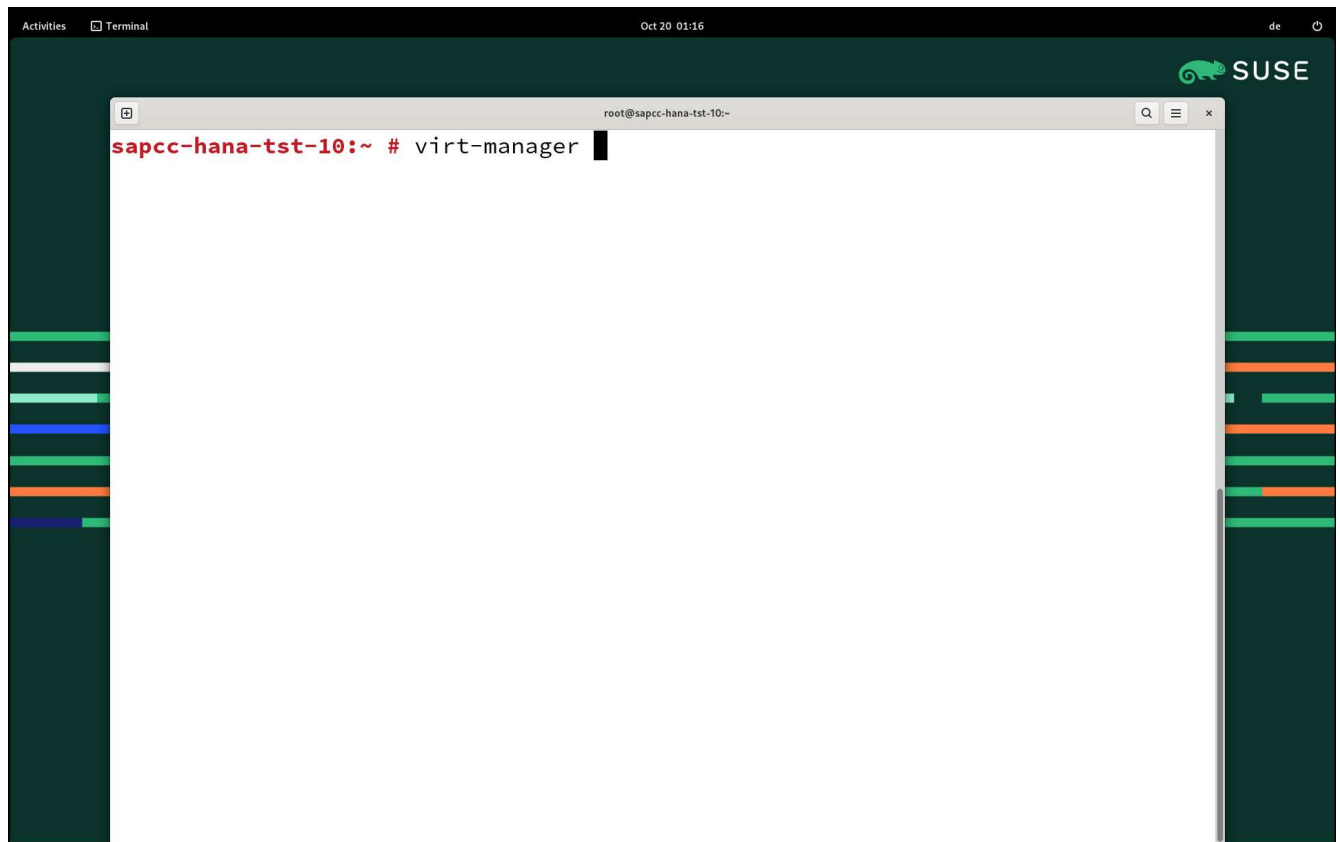
Da es für FCP keine SR-IOV-äquivalente Funktion gibt, weisen Sie die physischen HBA-Ports direkt der VM zu. Verwenden Sie zwei physische Anschlüsse, die an unterschiedlichen Textilien befestigt sind, um Redundanz zu gewährleisten.



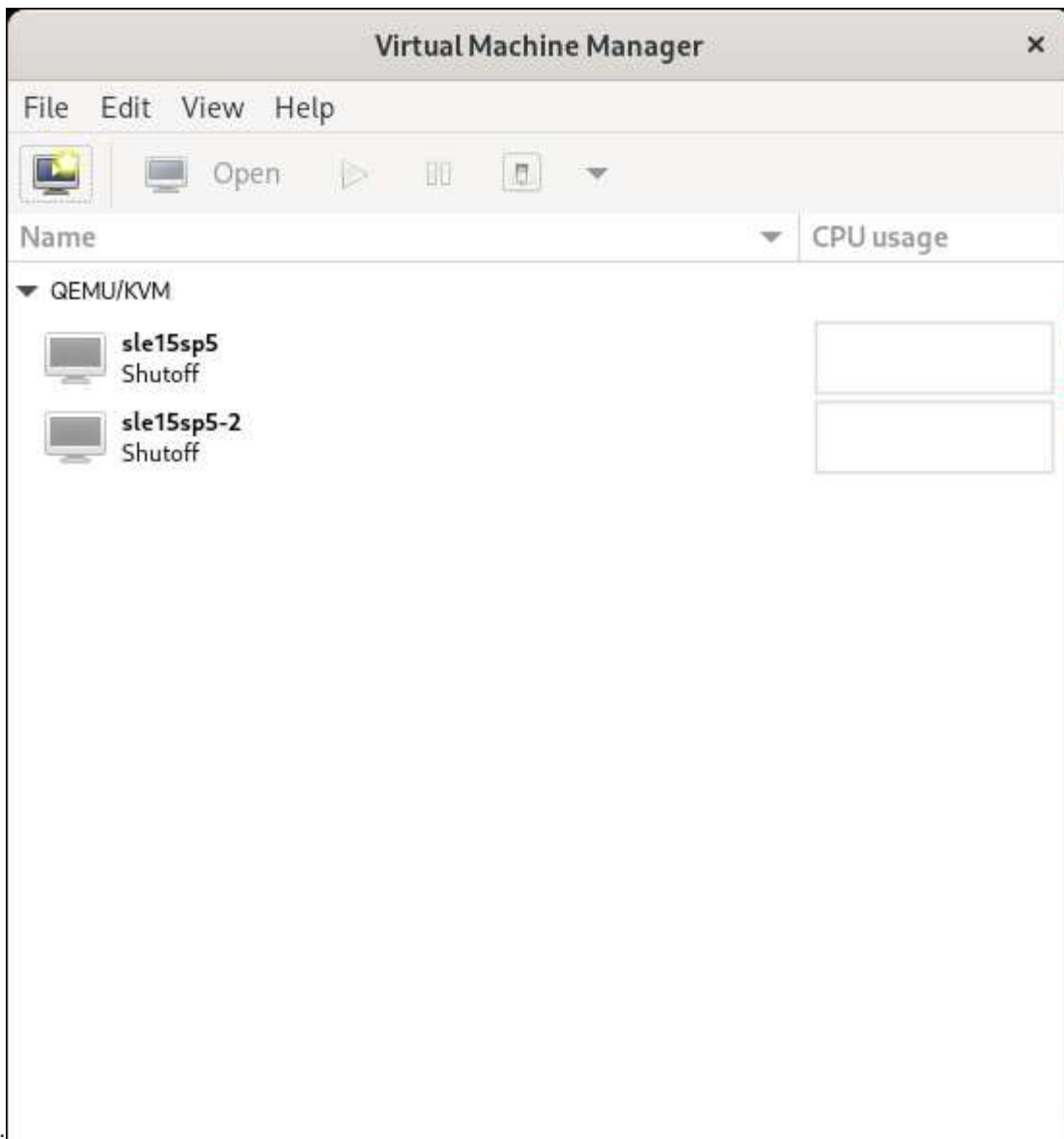
Ein physischer Port kann nur einer VM zugewiesen werden.

Schritte

1. Starten Sie virt-manager:

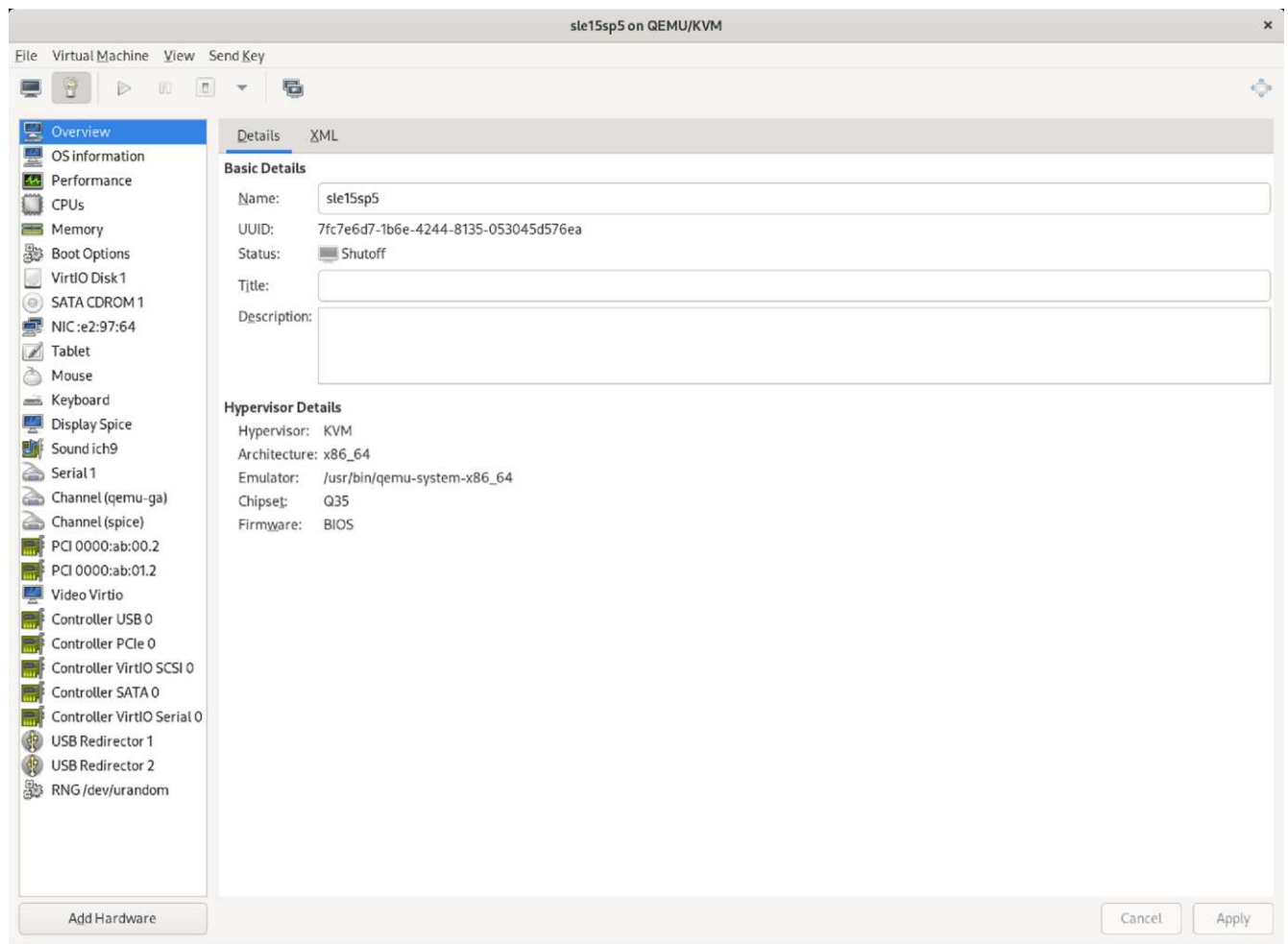


2. Öffnen Sie die gewünschte



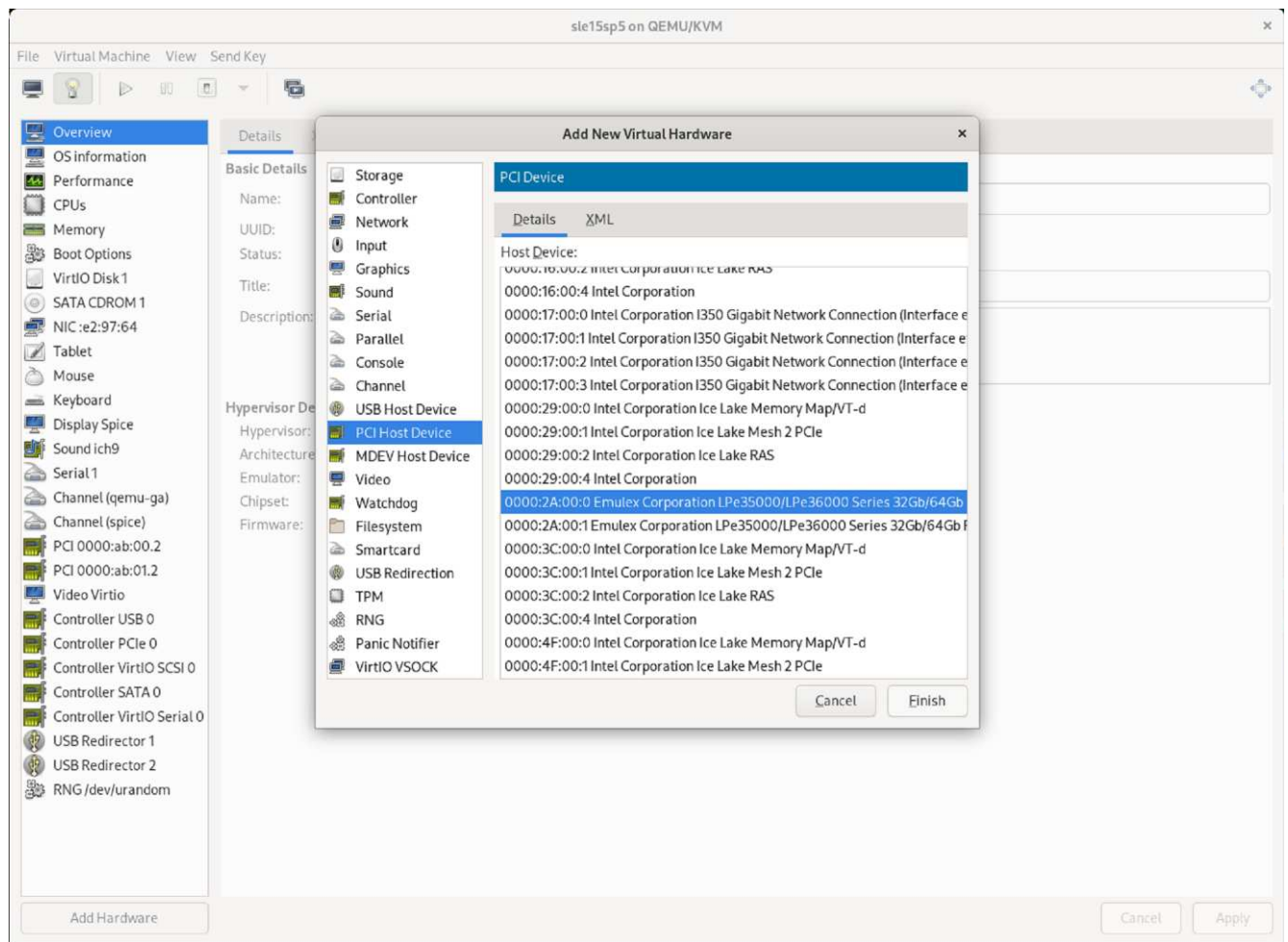
VM.

3. Wählen Sie **Hardware hinzufügen**.

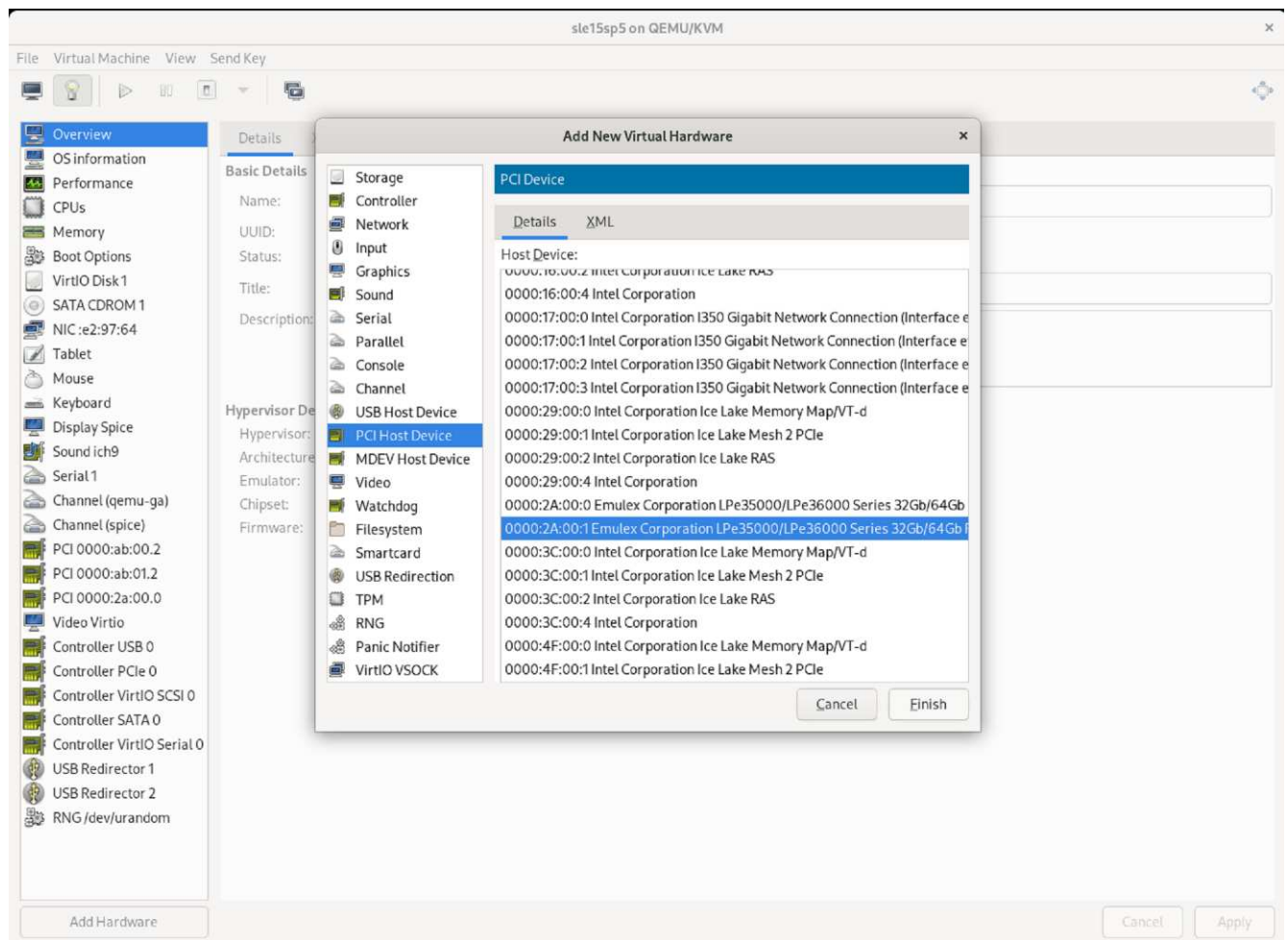


4. Wählen Sie den gewünschten HBA-Port aus der Liste der PCI-Hostgeräte aus und klicken Sie auf Fertigstellen.

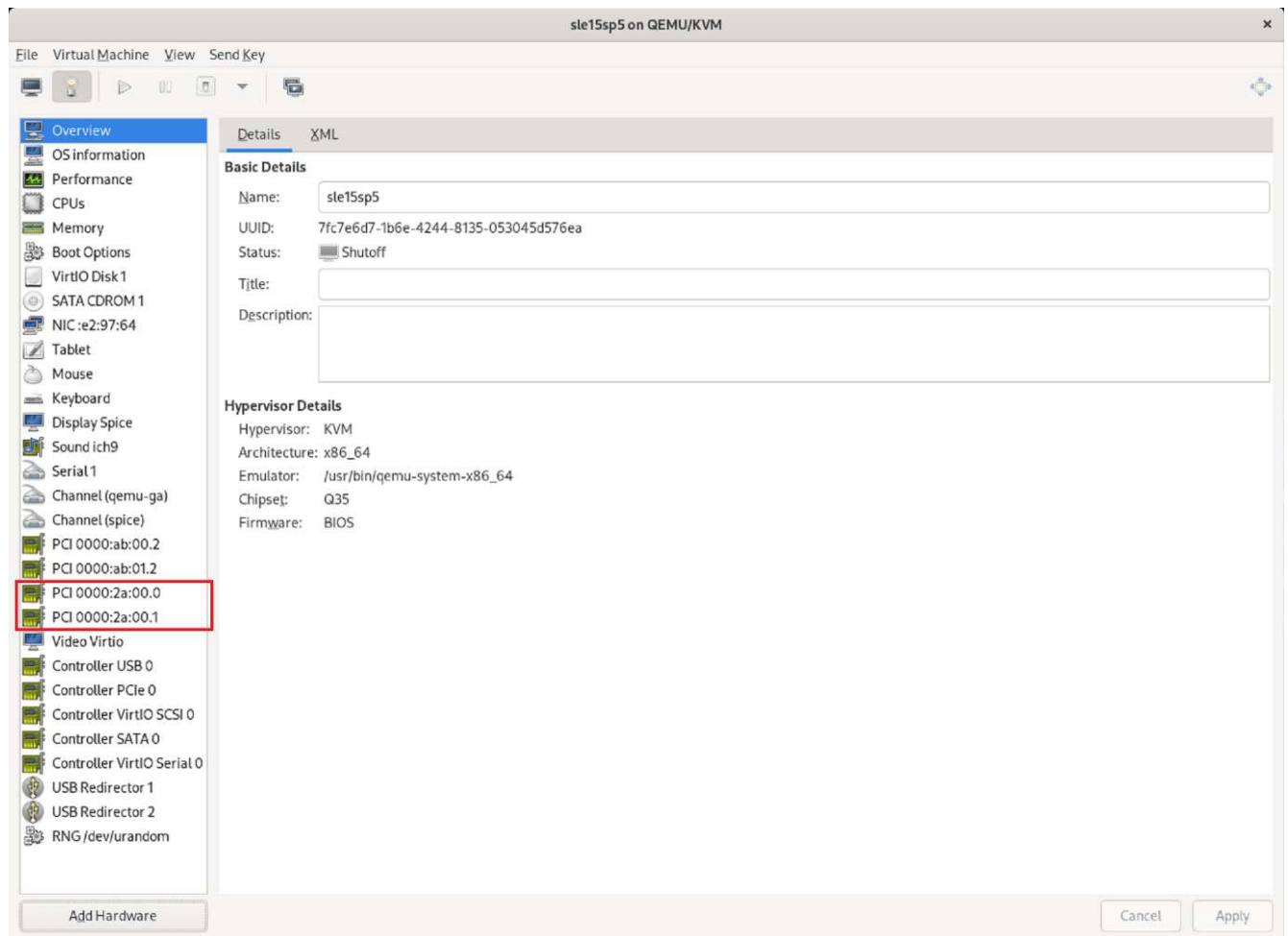
In diesem Beispiel 0000.A2:00:0.



5. Wählen Sie den gewünschten HBA-Port aus der Liste der PCI-Hostgeräte des zweiten Fabric aus und drücken Sie auf Fertigstellen. In diesem Beispiel 0000.A2:00:1.



6. Anschließend werden die physischen HBA-Ports der VM zugewiesen und die VM kann gestartet werden.



Die physischen Ports werden an die VM durchgereicht, sodass innerhalb der VM keine zusätzliche Vorbereitung erforderlich ist.

Wie geht es weiter?

Nachdem Sie das Fibre Channel-Netzwerk konfiguriert haben, "[NetApp Speicher für SAP HANA konfigurieren](#)". Die

NetApp Speicher für SAP HANA auf SUSE KVM konfigurieren

Konfigurieren Sie NetApp -Speicher für SAP HANA auf SUSE KVM unter Verwendung der NFS- oder FCP-Protokolle. Richten Sie Speicherverbindungen zwischen der VM und den NetApp ONTAP Systemen ein, um eine optimale Datenbankleistung zu erzielen.

Nachdem die VM mit SR-IOV-Netzwerkschnittstellen oder FCP-HBA-Ports konfiguriert wurde, konfigurieren Sie den Speicherzugriff innerhalb der VM. Verwenden Sie den passenden NetApp SAP HANA-Konfigurationsleitfaden, der auf dem von Ihnen gewählten Speicherprotokoll basiert.

Konfigurieren Sie NFS-Speicher für SAP HANA

Verwenden Sie die zuvor erstellten SR-IOV-Netzwerkschnittstellen, wenn das NFS-Protokoll für den SAP

HANA-Speicher verwendet werden soll.

Folgen Sie den ausführlichen Konfigurationsschritten in der ["SAP HANA on NetApp AFF Systems with NFS - Konfigurationsleitfaden"](#) Die

Wichtige Konfigurationsüberlegungen für KVM-Umgebungen:

- Verwenden Sie die zuvor für den Netzwerkverkehr konfigurierten virtuellen SR-IOV-Funktionen (VFs).
- Konfigurieren Sie Netzwerk-Bonding innerhalb der VM für Redundanz.
- Stellen Sie eine ordnungsgemäße Netzwerkumschaltung zwischen der VM und den NetApp -Speicher -SVMs sicher.
- Konfigurieren Sie Speichercontroller und VMs gemäß dem SAP HANA Konfigurationsleitfaden.

FCP-Speicher für SAP HANA konfigurieren

Verwenden Sie die der VM zugewiesenen physischen HBA-Ports als PCI-Geräte, wenn das FCP-Protokoll für den SAP HANA-Speicher verwendet werden soll.

Wählen Sie die passende Konfigurationsanleitung für Ihr NetApp Speichersystem aus:

- Für NetApp AFF -Systeme: ["Technischer Bericht: SAP HANA on NetApp AFF Systems with Fibre Channel Protocol"](#)
- Für NetApp ASA -Systeme: ["Technischer Bericht: SAP HANA on NetApp ASA Systems with Fibre Channel Protocol"](#)

Wichtige Konfigurationsüberlegungen für KVM-Umgebungen:

- Verwenden Sie die physischen HBA-Ports, die der VM über PCI-Passthrough zugewiesen wurden.
- Konfigurieren Sie Multipathing innerhalb der VM für Redundanz über Fabric-Switches hinweg.
- Konfigurieren Sie Speichercontroller und VMs gemäß dem SAP HANA-Konfigurationsleitfaden.

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.