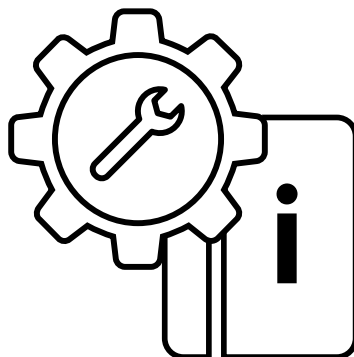


Installation Guide

LANCOM R&S[®] UF Command Center



Copyright

© 2022 LANCOM Systems GmbH, Würselen (Germany). Alle Rechte vorbehalten.

Alle Angaben in dieser Dokumentation sind nach sorgfältiger Prüfung zusammengestellt worden, gelten jedoch nicht als Zusicherung von Produkteigenschaften. LANCOM Systems haftet ausschließlich in dem Umfang, der in den Verkaufs- und Lieferbedingungen festgelegt ist. Weitergabe und Vervielfältigung der zu diesem Produkt gehörenden Dokumentation und Software und die Verwendung ihres Inhalts sind nur mit schriftlicher Erlaubnis von LANCOM Systems gestattet. Änderungen, die dem technischen Fortschritt dienen, bleiben vorbehalten.

Windows® und Microsoft® sind eingetragene Marken von Microsoft, Corp. LANCOM, LANCOM Systems, LCOS, LANcommunity und Hyper Integration sind eingetragene Marken. Alle anderen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein. Dieses Dokument enthält zukunftsbezogene Aussagen zu Produkten und Produkteigenschaften. LANCOM Systems behält sich vor, diese jederzeit ohne Angaben von Gründen zu ändern. Keine Gewähr für technische Ungenauigkeiten und / oder Auslassungen.

Produkte von LANCOM Systems enthalten Software, die vom „OpenSSL Project“ für die Verwendung im „OpenSSL Toolkit“ entwickelt wurde (<http://www.openssl.org/>).

Produkte von LANCOM Systems enthalten kryptographische Software, die von Eric Young (eay@cryptsoft.com) geschrieben wurde.

Produkte von LANCOM Systems enthalten Software, die von der NetBSD Foundation, Inc. und ihren Mitarbeitern entwickelt wurde.

Produkte von LANCOM Systems enthalten das LZMA SDK, das von Igor Pavlov entwickelt wurde.

Das Produkt enthält separate Komponenten, die als sogenannte Open Source Software eigenen Lizenzen, insbesondere der General Public License (GPL), unterliegen. Sofern die jeweilige Lizenz dies verlangt, werden Quelldateien zu den betroffenen Software-Komponenten auf Anfrage bereitgestellt. Wenden Sie sich hierzu via E-Mail an gpl@lancom.de.

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Würselen
Deutschland

www.lancom-systems.de
Würselen, 11/2022

Einleitung

Vielen Dank für den Erwerb eines LANCOM R&S®UF Command Centers. Das LANCOM R&S®UF Command Center ist die ideale Lösung für Managed-Security-Service-Anbieter und Unternehmen, die eine Vielzahl LANCOM R&S®Unified Firewalls zentral verwalten, konfigurieren und überwachen müssen. Ein intuitives Dashboard erlaubt das vollständige Management und Monitoring, zentrales Backup-Management und Archivierung sowie Lizenzmonitoring aller verwalteten LANCOM R&S®Unified Firewalls. In diesem Installation Guide wird die Inbetriebnahme des LANCOM R&S®UF Command Centers unter VMware ESXi-Server, Oracle Virtual Box sowie Microsoft Hyper-V-Server beschrieben.

Installation auf einem VMware ESXi-Server

Im Folgenden werden die Voraussetzungen und einzelnen Schritte zur erfolgreichen Installation des LANCOM R&S®UF Command Centers in einem VMware ESXi-Server erläutert.

Dateien

Die folgenden Dateien sind für das LANCOM R&S®UF Command Center im LANcommunity Partnerportal erhältlich:

→ ISO-Image-Datei

Voraussetzungen

Folgende Voraussetzungen müssen für die erfolgreiche Installation des LANCOM R&S®UF Command Centers in einem VMware ESXi-Server gegeben sein

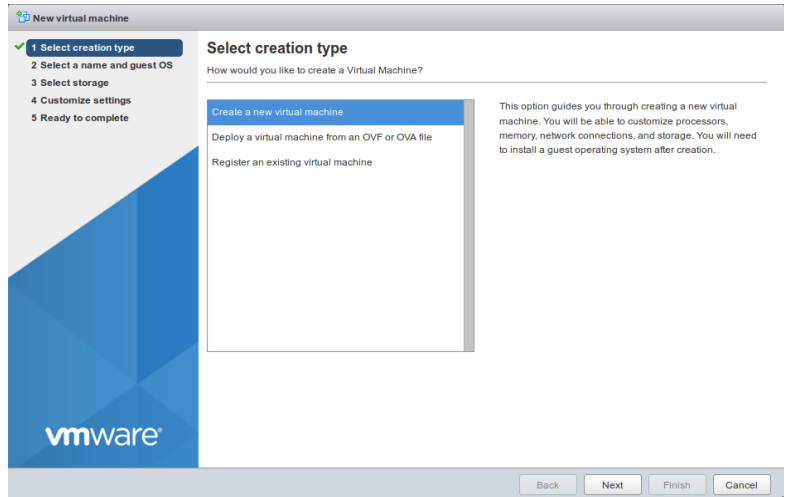
- Die Software des LANCOM R&S®UF Command Centers muss als ISO-Image-Datei vorliegen
- Die VMware ESXi version ESXi 6.0.0 (VM version 11) oder höher muss auf einem Server mit x86-kompatiblen 64 Bit-Prozessor installiert sein
- Die virtuelle Maschine muss folgende Minimalvoraussetzungen erfüllen:
 - 1 x86 CPU (64 bit) Prozessor
 - 2 GB RAM
 - 16 GB freier Festplattenspeicher
 - 1 Netzwerkschnittstelle

Erstellen und konfigurieren

Im Folgenden werden die verschiedenen Schritte beschrieben, die notwendig sind, um das LANCOM R&S®UF Command Center auf einem VMware ESXi-Server in Betrieb zu nehmen.

Starten Sie VMware ESXi, melden Sie sich an und erstellen Sie eine neue virtuelle Maschine.

→ Select creation type - Create a new virtual machine



Vergeben Sie einen Namen für die virtuelle Maschine

→ Select a name and guest OS

The screenshot shows the 'New virtual machine - Command Center (ESXI 6.0 virtual machine)' wizard. The left sidebar indicates the current step is '2. Select a name and guest OS'. The main area is titled 'Select a name and guest OS' and contains the following fields and options:

- Name:** A text input field containing 'Command Center'. Below it, a note states: 'Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.'
- Compatibility:** A dropdown menu set to 'ESXI 6.0 virtual machine'.
- Guest OS family:** A dropdown menu set to 'Linux'.
- Guest OS version:** A dropdown menu set to 'Debian GNU/Linux 8 (64-bit)'.

At the bottom right, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

Im gezeigten Beispiel wurde der Name „Command Center“ gewählt.

Darüber hinaus konfigurieren Sie

→ **Compability:** ESXI 6.0 virtual machine

→ **Guest OS family:** Linux

→ **Guest OS version:** Debian Linux 8 (64 bit)

Wählen Sie den Speicherort für die virtuelle Maschine aus.

→ Select storage

Select storage

Select the datastore in which to store the configuration and disk files.

The following datastores are accessible from the destination resource that you selected. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
BAREOS	10.83 TB	2.75 TB	NFS	Supported	Single
DATA	5.46 TB	1.12 TB	VMFS5	Supported	Single
OS	110.75 GB	109.34 GB	VMFS6	Supported	Single

3 items

Back Next Finish Cancel

Passen Sie die Einstellungen an.

→ Customize settings

Customize settings

Configure the virtual machine hardware and virtual machine additional options

Virtual Hardware VM Options

Add hard disk Add network adapter Add other device

CPU 1

Memory 2048 MB

Hard disk 1 16 GB

SCSI Controller 0 VMware Paravirtual

SATA Controller 0

Network Adapter 1 Testnet

Status Connect at power on

Adapter Type VMXNET 3

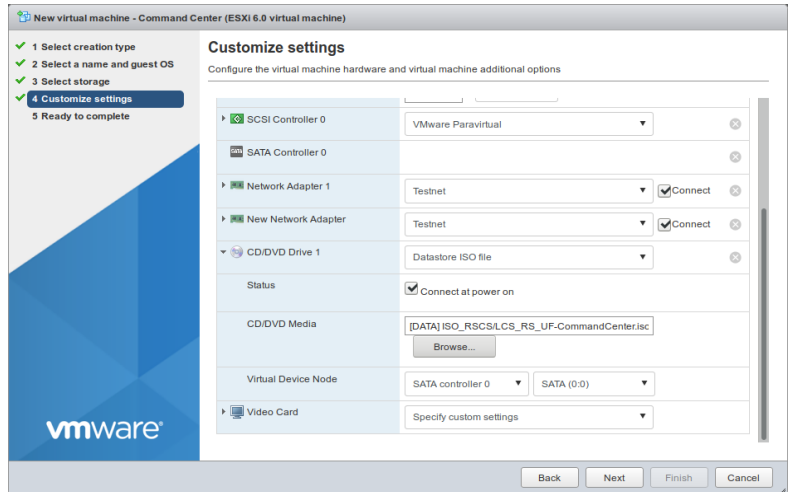
MAC Address Automatic 00:00:00:00:00:00

Back Next Finish Cancel

Konfigurieren Sie nun wie folgt:

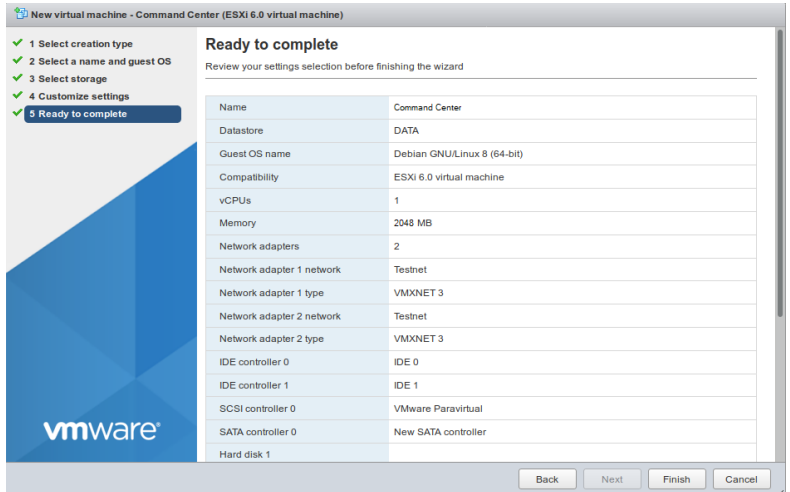
- **CPU:** mindestens 1
- **Memory:** mindestens 2048 MB
- **Hard disk 1:** mindestens 16 GB
- **Adapter Type:** VMXNET 3

Wählen Sie die ISO-Image-Datei über die **Browse**-Schaltfläche.



Überprüfen Sie Ihre Konfiguration.

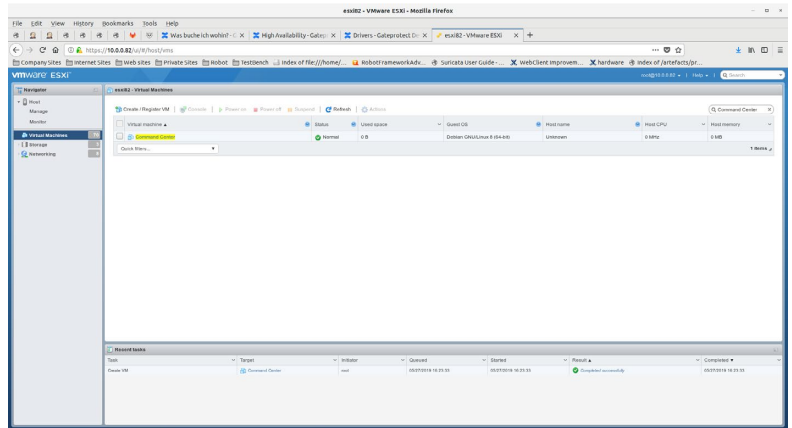
→ Ready to complete



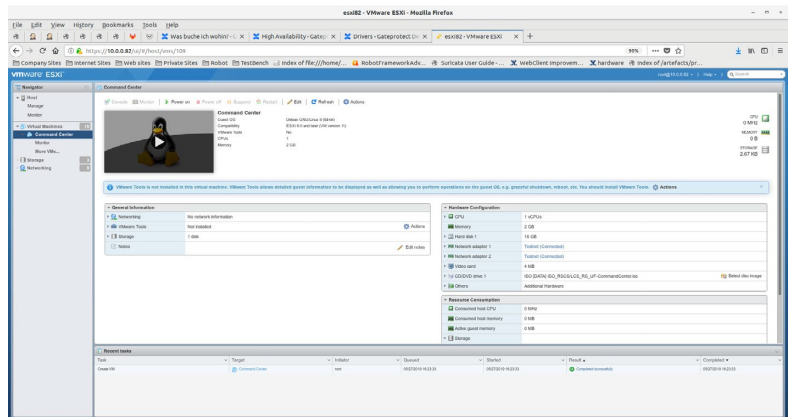
Bestätigen Sie die überprüfte Konfiguration mit der **Finish**-Schaltfläche. Anschließend sehen Sie Ihre virtuellen Maschinen.

Start des LANCOM R&S®UF Command Centers

Geben Sie im Suchfeld den Namen, beispielsweise „Command Center“, ein.

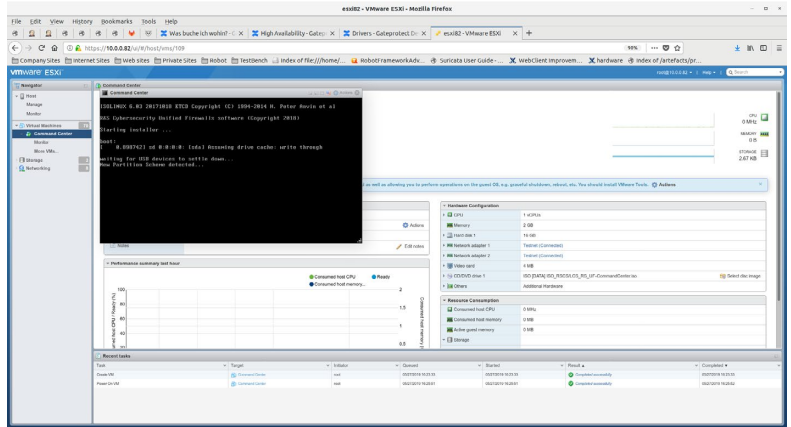


Nach der Auswahl von „Command Center“ sehen Sie die folgende Übersicht:



Wählen Sie **Power on** in der oberen Menüleiste.

Wählen Sie **Console** in der oberen Menüleiste und im dann erscheinenden Fenster **Open browser console**.



Die weiterführende Konfiguration des LANCOM R&S®UF Command Centers über die Konsole wird im Kapitel „Abschließende Installation auf der Konsole“ auf Seite 37 beschrieben.

Installation in Oracle VirtualBox

Dateien

Die folgenden Dateien sind für das LANCOM R&S®UF Command Center erhältlich:

- ISO-Image-Datei

Voraussetzungen

Folgende Voraussetzungen müssen für die erfolgreiche Installation des LANCOM R&S®UF Command Centers in einem Oracle VM VirtualBox Manager gegeben sein:

- Die Software des LANCOM R&S®UF Command Centers muss als ISO-Image-Datei vorliegen
- Oracle VM VirtualBox Manager 5.0 oder höher muss auf einem Server mit x86-kompatiblen 64 Bit-Prozessor installiert sein

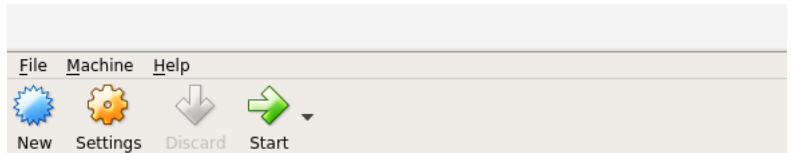
Die virtuelle Maschine muss folgende Minimalvoraussetzungen erfüllen:

- 1 x86 CPU (64 bit) Prozessor
- 2 GB RAM
- 16 GB freier Festplattenspeicher
- 1 Netzwerkschnittstelle

Erstellen und konfigurieren

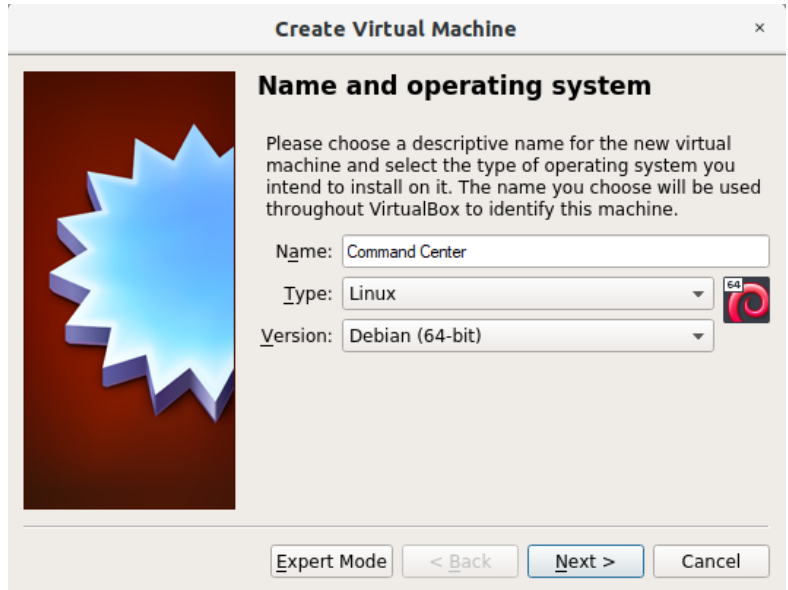
Im Folgenden werden die verschiedenen Schritte beschrieben, die notwendig sind, um das LANCOM R&S®UF Command Center im Oracle Virtual Box Manager in Betrieb zu nehmen.

Starten Sie den Oracle VM Virtual Box Manager und wählen Sie die **New**-Schaltfläche in der oberen Menüleiste, um eine neue virtuelle Maschine zu erzeugen.



Im nun erscheinenden Fenster **Name and operating system** vergeben Sie einen Namen für die virtuelle Maschine.

Im gezeigten Beispiel wurde der Name „Command Center“ gewählt.



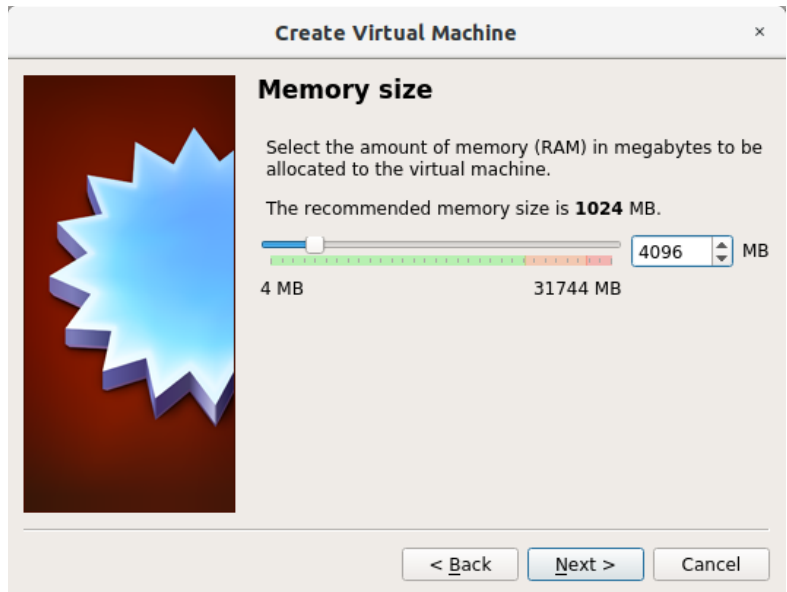
Darüber hinaus konfigurieren Sie

→ **Type:** Linux

→ **Version:** Debian (64-bit)

Klicken Sie auf **Next**.

Im Fenster **Memory size** konfigurieren Sie den zu reservierenden Speicher für die virtuelle Maschine.



Wählen Sie hier 2048 MB als **Minimum** und bestätigen Sie mit **Next**.

Im Fenster **Hard disk** konfigurieren Sie die virtuelle Festplatte.



Wählen Sie **Create a virtual hard disk now** und bestätigen Sie mit **Create**.

Im nächsten Schritt **Hard disk file type** legen Sie den Dateityp der virtuellen Festplatte fest.



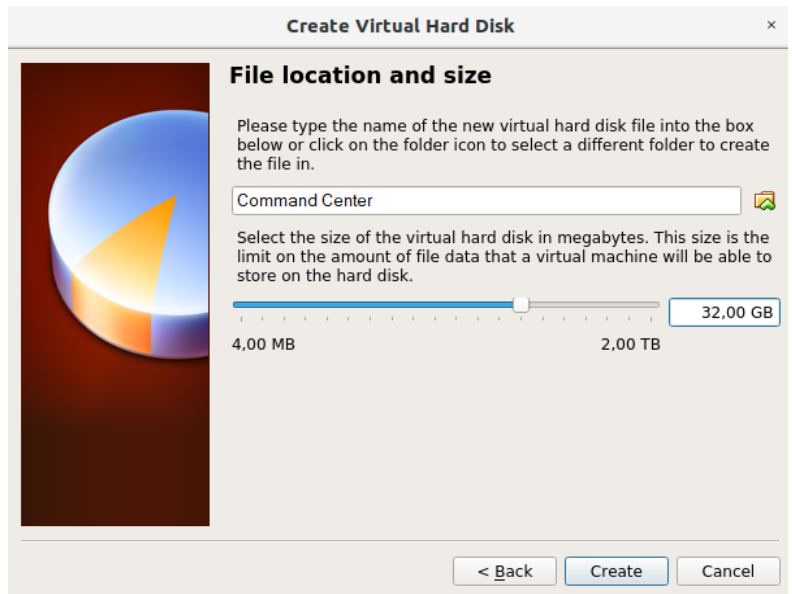
Wählen Sie **VDI (Virtual Box Disk Image)** und bestätigen Sie mit **Next**.

Legen Sie im nächsten Fenster **Storage on physical hard disk** fest, dass der Speicherplatz der virtuellen Festplatte bei Bedarf dynamisch angepasst werden soll.



Wählen Sie **Dynamically allocated** und bestätigen Sie mit **Next**.

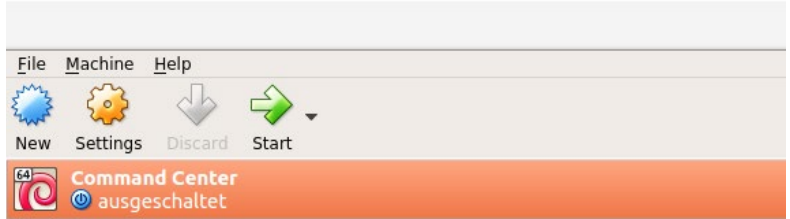
Im nächsten Schritt **File location and size** konfigurieren Sie den Namen der virtuellen Festplatte, deren Ablageort und die minimale Größe.



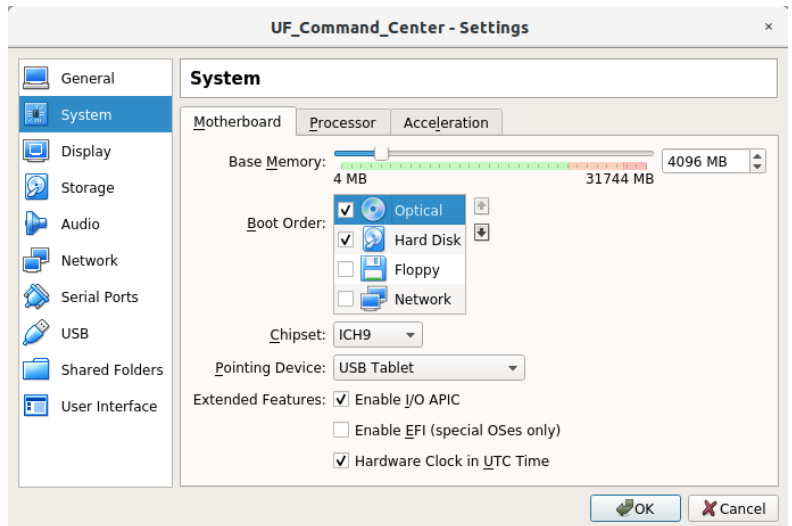
Wählen Sie eine minimale Größe von 16 GB und klicken Sie auf **Create**.

Im Hauptfenster des Oracle VM Virtual Box Managers erscheint daraufhin der Eintrag für Ihre soeben erstellte virtuelle Maschine.

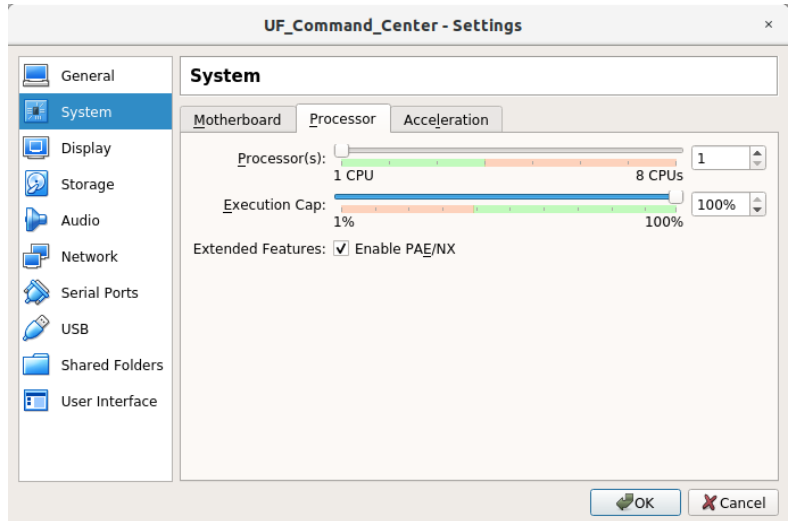
Selektieren Sie die virtuelle Maschine durch einfachen Klick und wählen Sie **Settings** in der oberen Menüleiste.



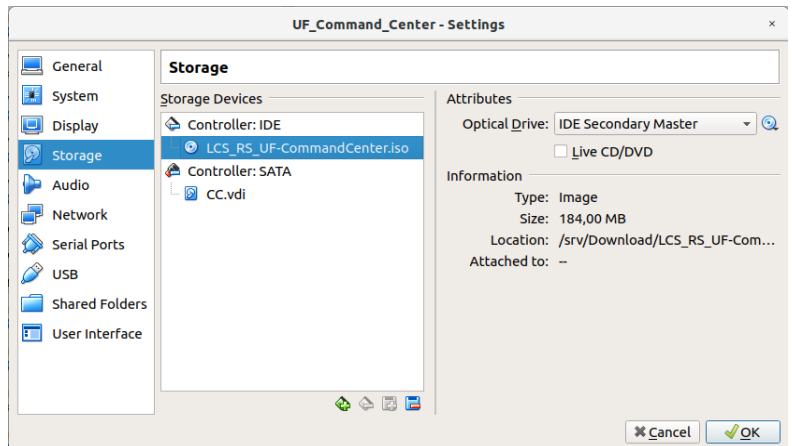
Kontrollieren Sie im Abschnitt **System** die Einstellungen im Reiter **Motherboard** und passen Sie diese ggf. wie im folgenden Screenshot dargestellt an.



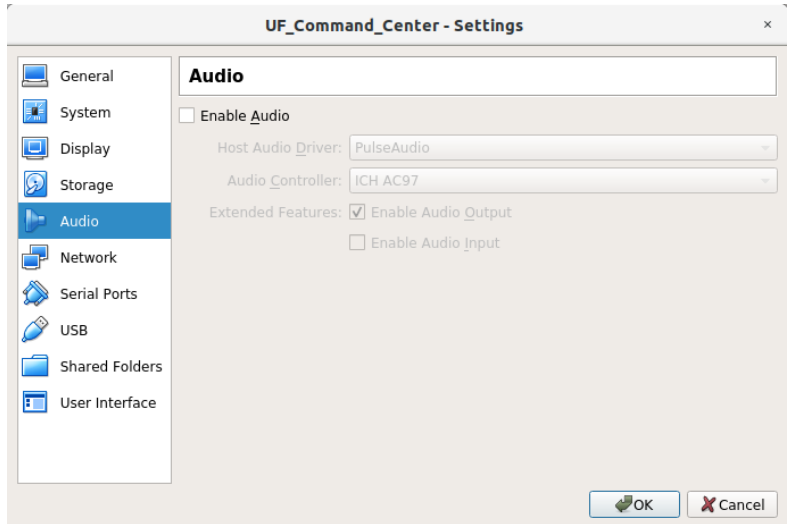
Aktivieren Sie im Reiter **Processor** die Option **Enable PAE/NX**.



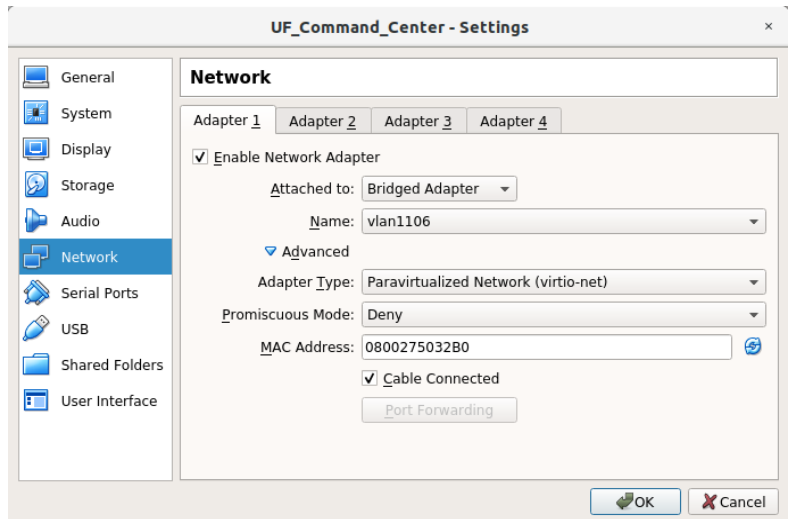
Wechseln Sie links im Menü zum Eintrag **Storage** und wählen Sie unter **Attributes** mit einem Klick auf das Disk-Symbol **Virtual optical disk file**.



Im Menü **Audio** entfernen Sie den Haken bei **Enable Audio**.



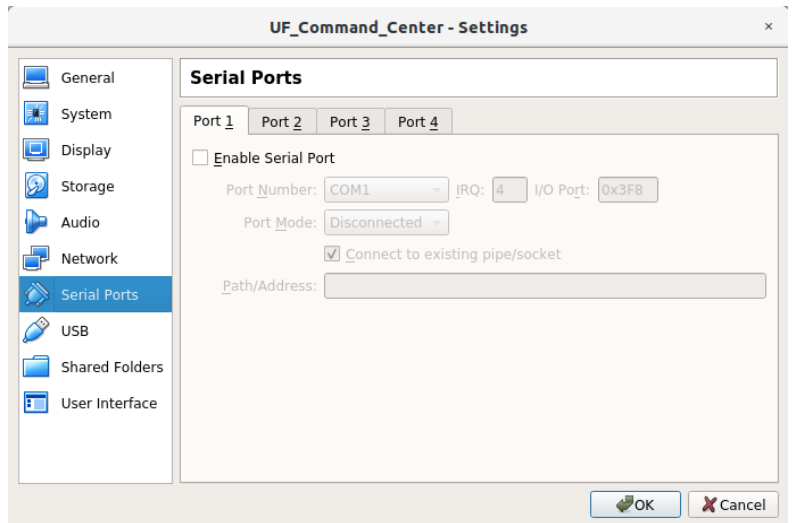
Im Menü **Network** aktivieren Sie **Enable Network Adapter** und konfigurieren wie folgt:



- **Attached to:** Benutzerspezifisch, z.B. **Bridged Adapter**
- **Name:** Benutzerspezifisch; falls **Bridged Adapter** ausgewählt wurde, wählen Sie hier das entsprechende Interface.
- **Adapter Type:** Paravirtualized Network (virtio-net)
- **Promiscuous Mode:** Deny
- **Cable Connected:** enabled

Die MAC-Adresse wird automatisch ermittelt und eingetragen.

Im Menü **Serial Ports** deaktivieren Sie sämtliche seriellen Schnittstellen.

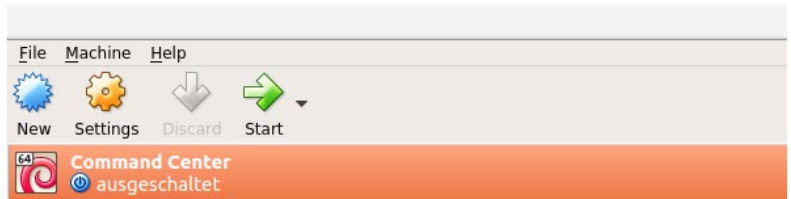


In den Menüs **USB**, **Shared Folders** und **User Interface** verwenden Sie die voreingestellten Standard-Werte.

Klicken Sie zum Abschluss der Konfiguration **OK**, um die angepassten Einstellungen zu übernehmen.

Start des LANCOM R&S®UF Command Centers

Starten Sie im Oracle VM Virtual Box Manager die virtuelle Maschine mit einem Klick auf den grünen **Start**-Pfeil.



Die weiterführende Konfiguration des LANCOM R&S®UF Command Centers über die Konsole wird im Kapitel „Abschließende Installation auf der Konsole“ auf Seite 37 beschrieben.

Installation in Microsoft Hyper-V

Im Folgenden werden die Voraussetzungen und einzelnen Schritte zur erfolgreichen Installation des LANCOM R&S®UF Command Centers in Microsoft Hyper-V erläutert.

Dateien

Die folgenden Dateien sind für das LANCOM R&S®UF Command Center erhältlich:

- ISO-Image-Datei

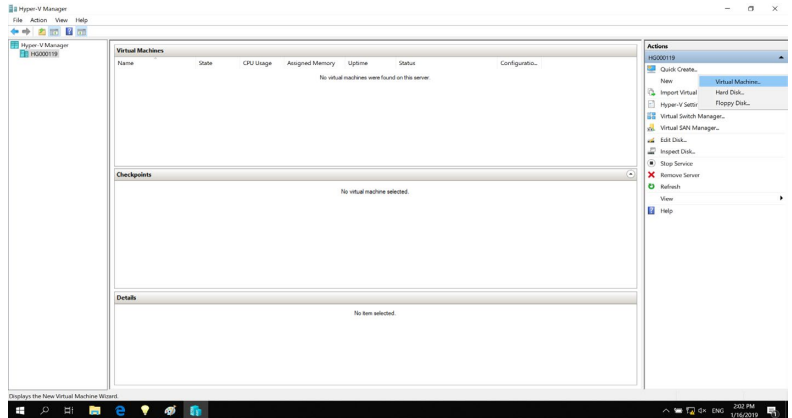
Voraussetzungen

Folgende Voraussetzungen müssen für die erfolgreiche Installation des LANCOM R&S®UF Command Centers in Microsoft Hyper-V gegeben sein:

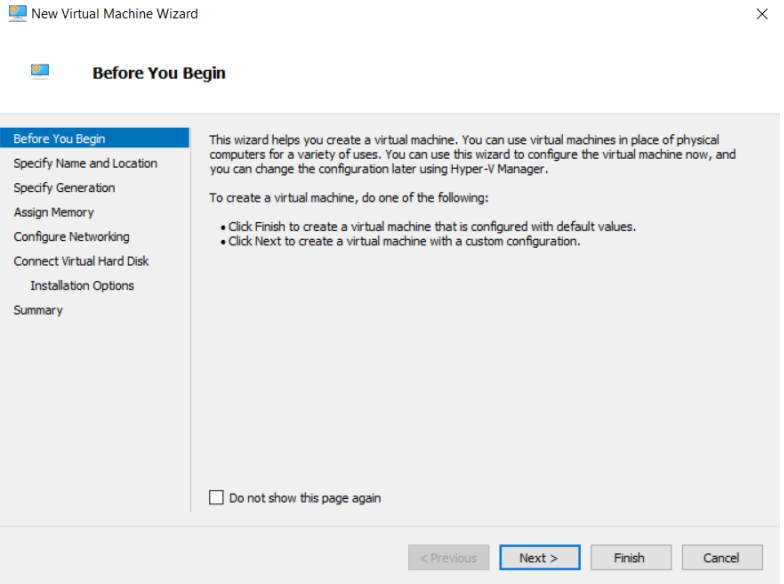
- Die Software des LANCOM R&S®UF Command Center muss als ISO-Image-Datei vorliegen
- Microsoft Hyper-V Manager 10.0 oder höher muss auf einem Server mit x86-kompatiblen 64 Bit-Prozessor installiert sein
- Die virtuelle Maschine muss folgende Minimalvoraussetzungen erfüllen:
 - 1 x86 CPU (64 bit) Prozessor
 - 2 GB RAM
 - 16 GB freier Festplattenspeicher
 - 1 Netzwerkschnittstelle

Erstellen und konfigurieren

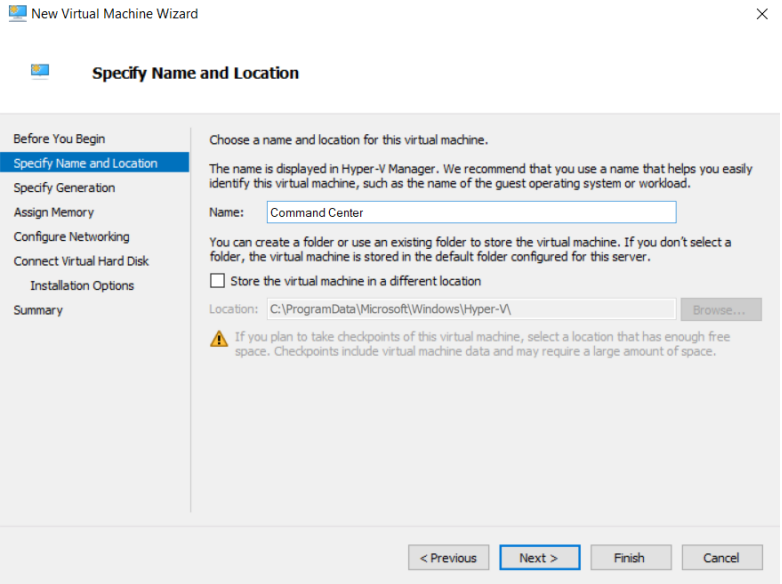
Starten Sie den Microsoft Hyper-V Manager und klicken Sie auf der rechten Seite der Oberfläche im **Actions**-Bereich zunächst auf **New**, dann auf **Virtual Machine**.



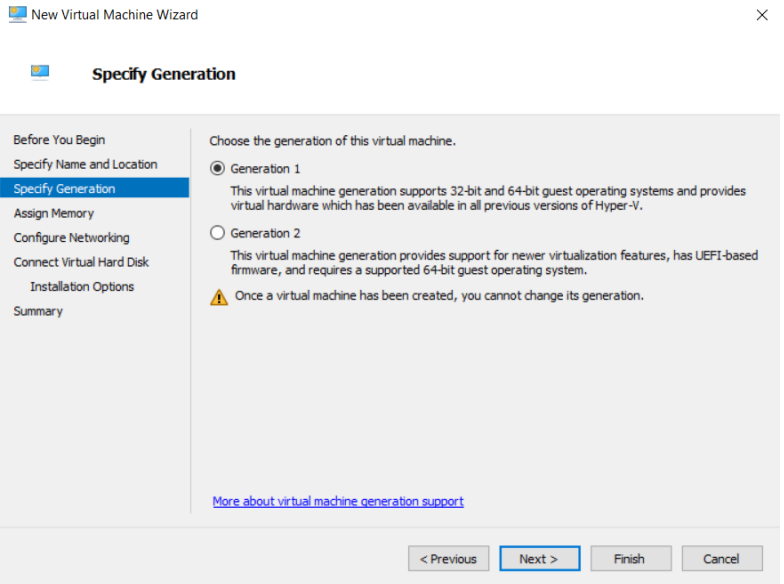
Der **New Virtual Machine Wizard** wird gestartet. Es öffnet sich das neue Fenster **Before You Begin**.



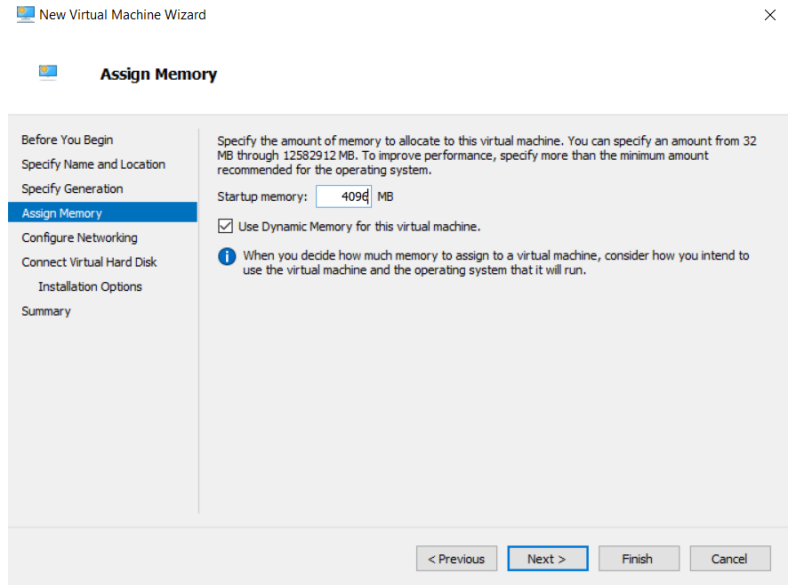
Klicken Sie **Next** und vergeben Sie im nächsten Fenster einen Namen für die virtuelle Maschine, z.B. „Command Center“. Bestätigen Sie mit **Next**.



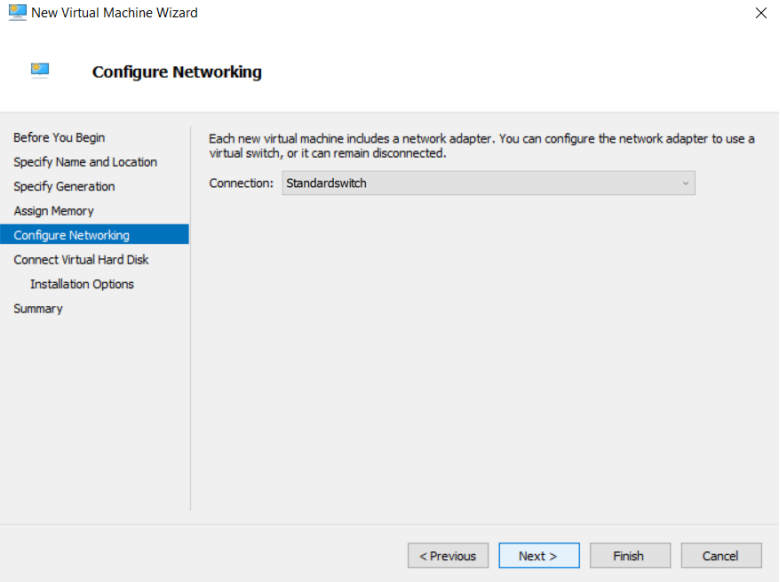
Im nächsten Schritt wählen Sie **Generation 1** und bestätigen mit **Next**.



Im Fenster **Assign Memory** stellen Sie für **Startup Memory** mindestens den Wert 2048 MB ein und aktivieren **Use Dynamic Memory for this virtual machine**. Bestätigen Sie mit **Next**.



Im Schritt **Configure Networking** vergeben Sie für **Connection** den Wert **Standardswitch**. Bestätigen Sie mit **Next**.



Unter **Connect Virtual Hard Disk** wählen Sie die Option **Create a virtual hard disk** und eine minimale Grösse von 16 GB. Bestätigen Sie mit **Next**.

New Virtual Machine Wizard ×

Connect Virtual Hard Disk

Before You Begin
Specify Name and Location
Specify Generation
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Installation Options
Summary

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

Create a virtual hard disk
Use this option to create a VHDX dynamically expanding virtual hard disk.

Name:

Location:

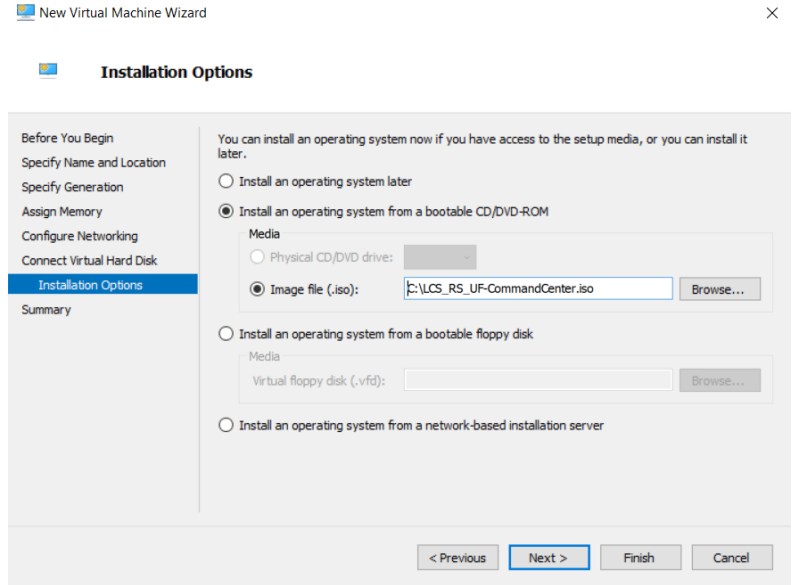
Size: GB (Maximum: 64 TB)

Use an existing virtual hard disk
Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

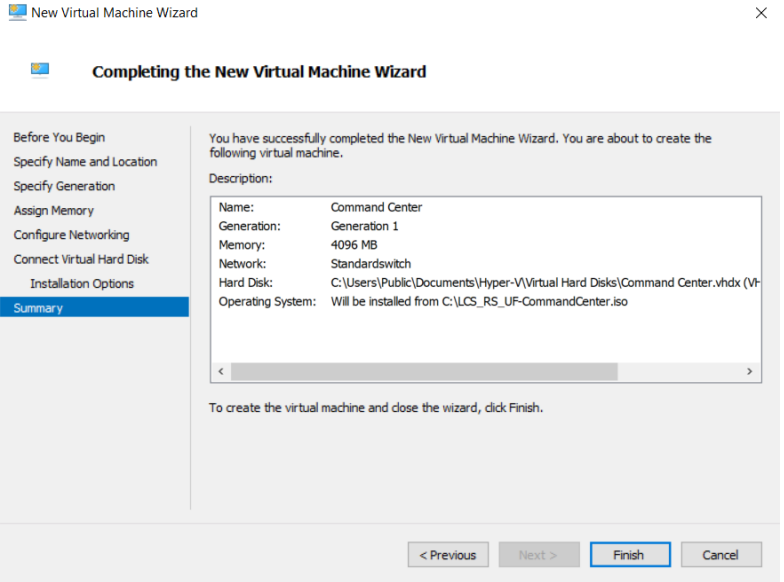
Location:

Attach a virtual hard disk later
Use this option to skip this step now and attach an existing virtual hard disk later.

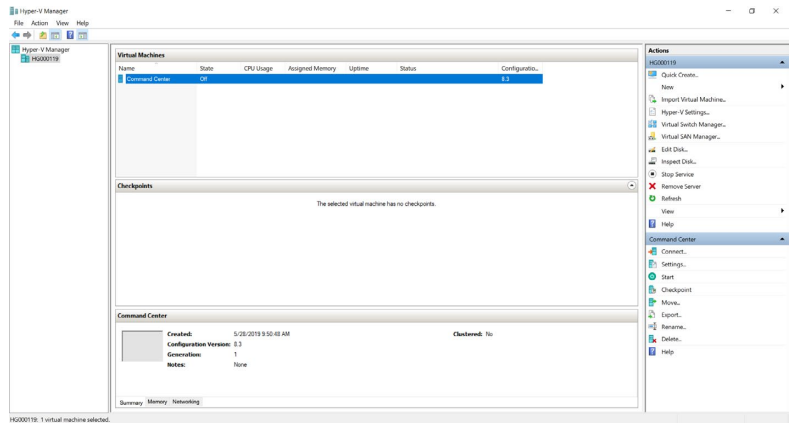
Im Fenster **Installation Options** aktivieren Sie die Option **Install an operating system from a bootable CD /DVD-ROM** sowie die Option **Image file (.iso)**. Wählen bzw. bestätigen Sie den Pfad zur LANCOM R&S®UF Command Center Image-Datei und bestätigen Sie mit **Next**.



Zum Abschluss des Wizards wird eine Übersichtsseite mit den bisher konfigurierten Parametern angezeigt. Bestätigen Sie nun mit **Finish**.

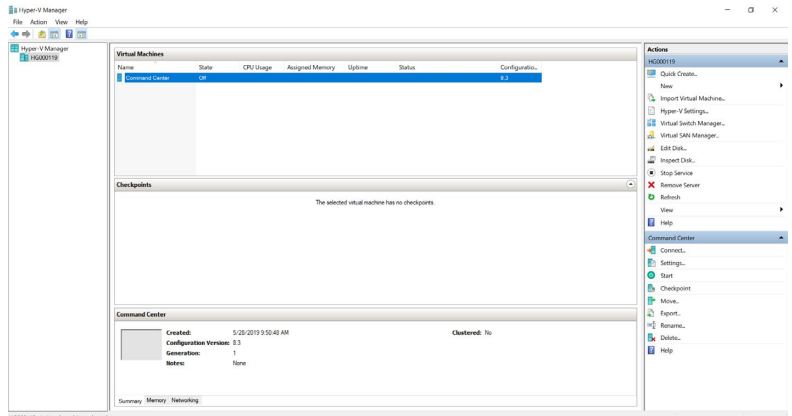


Die virtuelle Maschine ist nun angelegt.



Start des LANCOM R&S®UF Command Centers

Wählen Sie im Hauptfenster des Microsoft Hyper-V Managers unter **Actions / Command Center** den Eintrag **Start** und dann **Connect**.



Es erscheint ein separates Konsolen-Fenster. Fahren Sie nun mit der Installation des LANCOM R&S®UF Command Centers auf der Konsole fort, wie im nächsten Kapitel beschrieben.

Abschließende Installation auf der Konsole

Die folgende Menüführung auf der Konsole gilt grundsätzlich für alle in diesem Installation Guide beschriebenen virtuellen Umgebungen. Bei Abweichungen zwischen den Systemen wird dies durch separate Screenshots kenntlich gemacht.

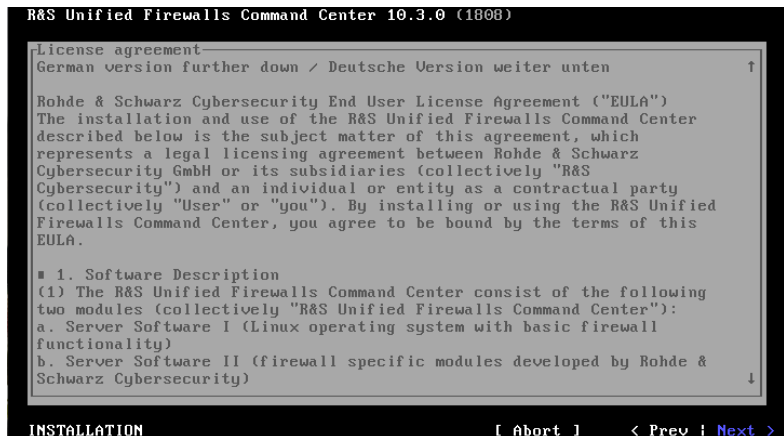
Nach dem Start der Konsole erscheint folgendes Fenster:

Auswahl der Sprache

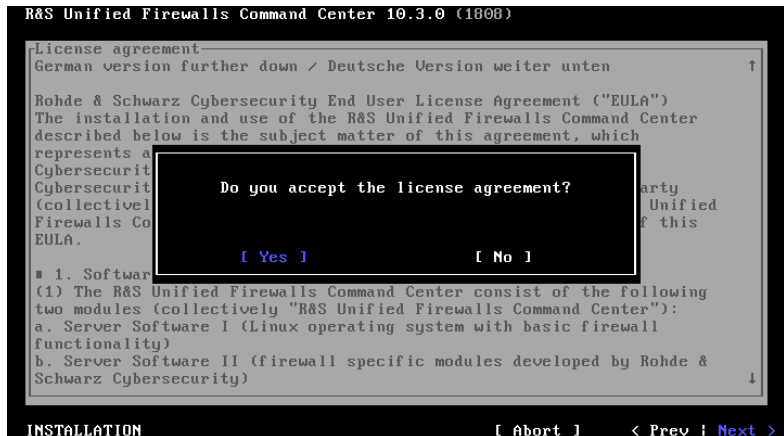


Wählen Sie Ihre Sprache und bestätigen Sie mit **Next**.

Lizenzvereinbarung



Bestätigen Sie die Lizenzvereinbarung mit **Next** und quittieren Sie den nachfolgenden Dialog mit **Yes**.



Übersicht der erkannten Hardware

→ VMware ESXi:

```

R&S Unified Firewalls Command Center 10.3.0 (1000)

Detected hardware
    Hard disks   SCSI: Virtual disk (16384 MB)
                CD-ROM   SCSI: NECUMar!UMware SATA CDB0
    Network interface cards  eth0: UMware VMXNET3 Ethernet Controller
                            eth1: UMware VMXNET3 Ethernet Controller

INSTALLATION [ Abort ] < Prev | Next >
  
```

→ Oracle VirtualBox

```

R&S Unified Firewalls Command Center 10.3.0 (1000)

Detected hardware
    Hard disks   SCSI: VBox HARDISK (10432 MB)
                CD-ROM   SCSI: VBoxICD-ROM
    Network interface cards  eth0: Red Hat, Inc
                            eth1: Red Hat, Inc

INSTALLATION [ Abort ] < Prev | Next >
  
```

→ Microsoft Hyper-V

```

R&S Unified Firewalls Command Center 10.3.0 (1000)

Detected hardware
    Hard disks   SCSI: Virtual Disk (32768 MB)
                CD-ROM   SCSI: MsftiVirtual CD-ROM
    Network interface cards  eth0: Microsoft Corporation
                            eth1: Microsoft Corporation

INSTALLATION [ Abort ] < Prev | Next >
  
```

Bestätigen Sie jeweils mit **Next**.

Konfiguration der Netzwerkschnittstellen

Die Default-IP-Adressen werden durch Drücken von F12 den Netzwerkschnittstellen zugewiesen. Es erscheint folgender Screenshot:

→ VMware ESXi

```
R&S Unified Firewalls Command Center 10.3.0 (1088)

Network interface configuration

- eth0 (VMware VMXNET3 Etherae)
- eth1 (VMware VMXNET3 Etherae)

Hint: Leave input fields blank to
deactivate an interface. Press F12 for
default IP addresses.
IP: 192.168.0.254 / 255.255.255.0
IP: 192.168.1.254 / 255.255.255.0

INSTALLATION [ Abort ] < Prev | Next >
```

→ Oracle VirtualBox

```
R&S Unified Firewalls Command Center 10.3.0 (1088)

Network interface configuration

- eth0 (Red Hat, Inc )
- eth1 (Red Hat, Inc )

Hint: Leave input fields blank to
deactivate an interface. Press F12 for
default IP addresses.
IP: 192.168.0.254 / 255.255.255.0
IP: 192.168.1.254 / 255.255.255.0

INSTALLATION [ Abort ] < Prev | Next >
```

→ Microsoft Hyper-V

```
R&S Unified Firewalls Command Center 10.3.0 (1088)

Network interface configuration

- eth0 (Microsoft Corporation )
- eth1 (Microsoft Corporation )

Hint: Leave input fields blank to
deactivate an interface. Press F12 for
default IP addresses.
IP: 192.168.0.254 / 255.255.255.0
IP: 192.168.1.254 / 255.255.255.0

INSTALLATION [ Abort ] < Prev | Next >
```

Bestätigen Sie jeweils mit **Next**.

Eingabedialog für Host- und Domain-Name

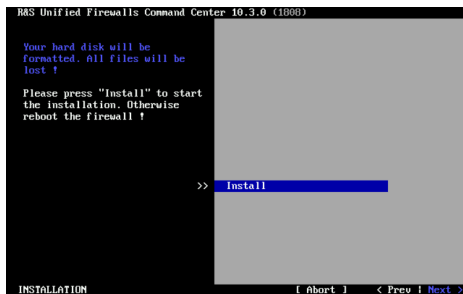
Konfigurieren Sie wie folgt:

- **Hostname:** UF100
- **Domain name:** lancom
- **Password:** frei wählbar

Bestätigen Sie Ihre Eingaben mit **Next**.

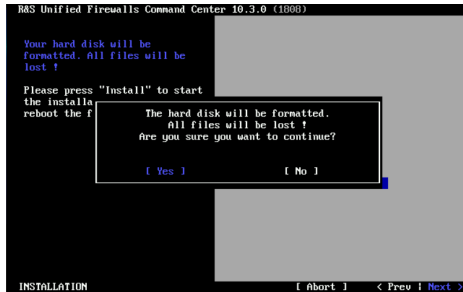


Start der Installation



Bestätigen Sie mit **Next**.

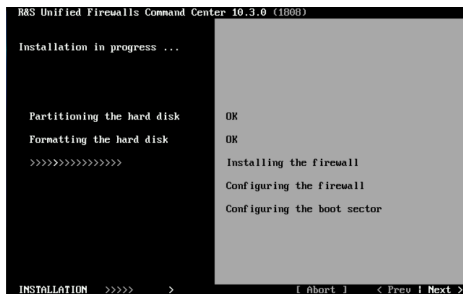
Bestätigung der Formatierung der virtuellen Festplatte



Bestätigen Sie die Frage nach der Formatierung der virtuellen Festplatte mit **Yes**.

Durchführung der Installation

Die Installation wird nun durchgeführt und dauert einige Minuten (bis zu 10 Minuten), typischerweise nur wenige Minuten.



Abschluss der LANCOM R&S®UF Command Center-Installation

Nach dem Neustart erscheint folgender Bildschirm:



Die Installation ist nun abgeschlossen. Ein Login auf der Konsole ist nicht erforderlich. Folgen Sie den Informationen bzgl. der Benutzer-Anmeldung im Browser über die vordefinierten Interfaces, wie im Screenshot dargestellt.

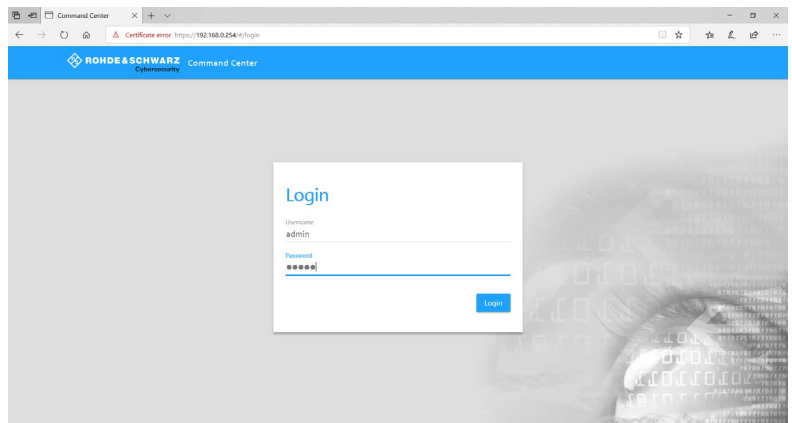
Einloggen über das Web-Interface

Starten Sie einen Web-Browser auf einem Rechner, der sich im gleichen Subnetz wie das LANCOM R&S®UF Command Center befindetet und rufen Sie die Web-Oberfläche des LANCOM R&S®UF Command Centers wie folgt auf:
Zum Erreichen der Netzwerkschnittstelle eth0 geben Sie folgendes ein:
`https://192.168.0.254`

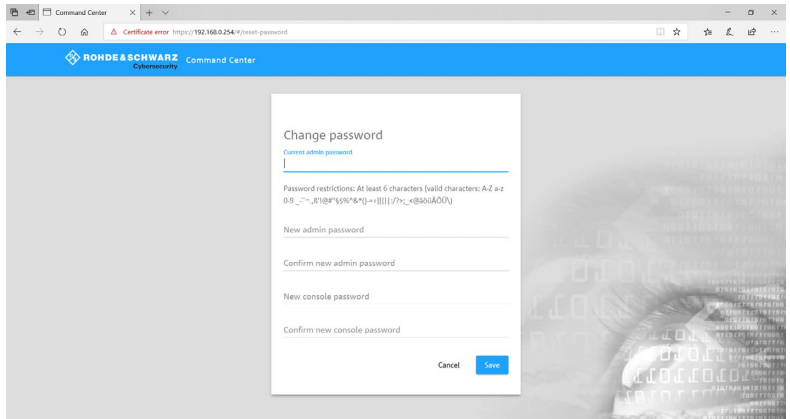
oder für die Netzwerkschnittstelle eth1:

`https://192.168.1.254`

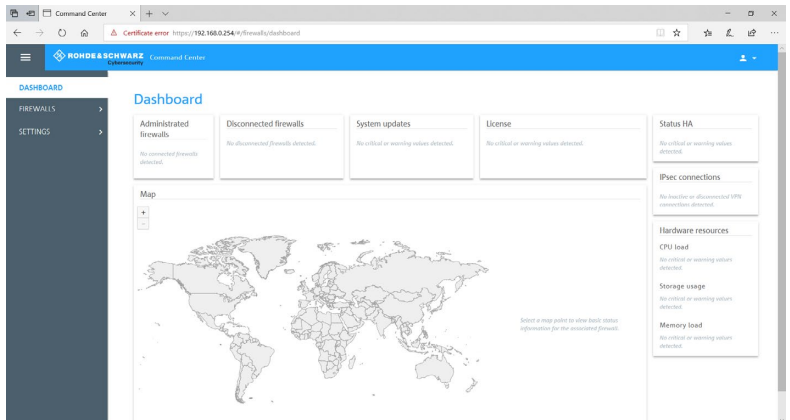
Es erscheint das Anmeldefenster Ihres LANCOM R&S®UF Command Centers.
Geben Sie als Benutzernamen und Passwort jeweils **admin** ein.



Sie werden daraufhin aufgefordert, ein neues Passwort zu vergeben.



Nach der Vergabe des neuen Passworts werden Sie angemeldet und die Web-Oberfläche Ihres LANCOM R&S®UF Command Center erscheint.



Verbinden der ersten Firewall

Für die sichere Kommunikation zwischen den LANCOM R&S®Unified Firewalls und dem LANCOM R&S®UF Command Center baut die Firewall eine spezielle SSL-VPN-Verbindung zum LANCOM R&S®UF Command Center auf. Diese Verbindung ist durch Zertifikate abgesichert. Daher ist es notwendig, für die Verbindung entsprechende Zertifikate und Vertrauensstellungen einzurichten. Dazu gehen Sie in folgenden Schritten vor:

1. Auf einer beliebigen LANCOM R&S®Unified Firewall für das LANCOM R&S®UF Command Center eine **Certificate Authority (CA)** und ein **VPN-Zertifikat** erstellen und als **PKCS12** exportieren:

a) Certificate Management > Certificates > New

- **Type** auf **CA for VPN/ Webserver Certificates**
- **Private Key Password** wählen
- **Common Name (CN)** wählen, zum Beispiel „CommandCenterCA“
- Klicken Sie auf **Create**

CommandCenterCA Certificate

★ New - changes will be preserved until you cancel this dialog or log out.

Type: CA for VPN/Webserver Certificates

Validity: 06/04/2019 - 06/04/2020

Private Key Encryption: RSA

Private Key Password: *****

Private Key Size: 2048 Bit

Distinguished Name (DN)

Fill from Template: []

Common Name (CN): CommandCenterCA

Country (C): optional

City (L): optional

Organization (O): optional

State (ST): optional

Organizational Unit (OU): optional

Subject Alternative Name (SAN)

Name: [] Type: E-Mail

Certificate Authority Services

OCSP:

CRL:

Addresses for OCSP Responder/CRL Download: []

Cancel Create

b) Certificate Management > Certificates > New

- **Typ** auf **VPN Certificate**
- **Signing CA** auf CA aus 1a)
- **CA Password** aus 1a) eingeben
- **Private-Key Password** wählen
- **Common Name (CN)** wählen, zum Beispiel „CommandCenterCert“

- Klicken Sie auf **Create**

★ New - changes will be preserved until you cancel this dialog or log out.

Type	VPN Certificate	Validity	06/04/2019 - 06/04/2020
Signing CA	CommandCenterCA	CA Password	***** <input type="checkbox"/> Show CA Password
Private Key Encryption	RSA	Private Key Password	***** <input type="checkbox"/> Show Private Key Password
Private Key Size	2048 Bit		

Distinguished Name (DN)

Fill from Template		City (L)	optional
Common Name (CN)	CommandCenterCert	Organization (O)	optional
Country (C)	optional	Organizational Unit (OU)	optional
State (ST)	optional		

Subject Alternative Name (SAN)

Name	Type	
	E-Mail	<input type="text"/>

- c) Erstelltes Zertifikat „CommandCenterCert“ exportieren
 - Expandieren Sie die Listbar
 - In der Zertifikatsliste bei „CommandCenterCert“ auf **exportieren** klicken
 - **PKCS12** wählen
 - **Password** ist das Private Key Password aus Schritt 1b)
 - **Transport Password** wählen
2. Auf dem LANCOM R&S®UF Command Center unter **Settings > Device Connection** die p12-Datei als **Command Center Certificate** auswählen und importieren.
3. Auf der hinzuzufügenden LANCOM R&S®Unified Firewall eine CA und ein VPN-Zertifikat für die Firewall erstellen und die CA als PEM exportieren:
 - a) **Certificate Management > Certificates > New**
 - **Type** auf **CA for VPN / Webserver Certificates**
 - **Private Key Password** wählen
 - **Common Name (CN)** wählen, zum Beispiel „FirewallCA“
 - Klicken Sie auf **Create**

FirewallCA Certificate ✕

★ New - changes will be preserved until you cancel this dialog or log out.

Type: Validity:

Private Key Encryption: Private Key Password: Show Private Key Password

Private Key Size:

Distinguished Name (DN)

Fill from Template:

Common Name (CN): City (L):

Country (C): Organization (O):

State (ST): Organizational Unit (OU):

Subject Alternative Name (SAN)

Name	Type	
<input type="text"/>	<input type="text" value="E-Mail"/>	

Certificate Authority Services

OCSRP

CRL

Addresses for OCSRP Responder/CRL Download

b) **Certificate Management > Certificates > New**

- **Type** auf **VPN Certificate**
- **Signing CA** auf CA aus 3a)
- **CA Password** aus 3a) eingeben
- **Private Key Password** wählen
- **Common Name (CN)** wählen, zum Beispiel „FirewallA“
- Klicken Sie auf **Create**

FirewallA Certificate ✕

★ New - changes will be preserved until you cancel this dialog or log out.

Type	VPN Certificate	Validity	06/04/2019 - 06/04/2020
Signing CA	FirewallCA	CA Password	***** <input type="checkbox"/> Show CA Password
Private Key Encryption	RSA	Private Key Password	***** <input type="checkbox"/> Show Private Key Password
Private Key Size	2048 Bit		

Distinguished Name (DN)

Fill from Template		City (L)	optional
Common Name (CN)	FirewallA	Organization (O)	optional
Country (C)	optional	Organizational Unit (OU)	optional
State (ST)	optional		

Subject Alternative Name (SAN)


Name	Type	
	E-Mail	<input type="button" value="+"/>

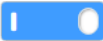
c) Firewall-CA exportieren

- Expandieren Sie die Listbar
 - In der Zertifikatsliste bei FirewallCA auf **exportieren** klicken
 - **PEM** wählen
 - Auf dem LANCOM R&S®UF Command Center unter **Settings > Device Connection** die PEM-Datei zu den **Accepted Remote CAs** hinzufügen
4. Auf der LANCOM R&S®Unified Firewall unter **Firewall Command Center** die Verbindung zum LANCOM R&S®UF Command Center konfigurieren:
- a) Die IP-Adresse (**Host**), unter der die LANCOM R&S®Unified Firewall das LANCOM R&S®UF Command Center erreicht:
- Falls die LANCOM R&S®Unified Firewall und das LANCOM R&S®UF Command Center im selben Netz stehen, dann ist dies die IP-Adresse des LANCOM R&S®UF Command Centers.

- Falls die LANCOM R&S®Unified Firewall und das LANCOM R&S®UF Command Center in unterschiedlichen Netzen stehen, dann ist dies die IP -Adresse des Gateways vor dem LANCOM R&S®UF Command Center. Außerdem wird dann ein Port Forwarding auf dem Gateway benötigt.
- b) Der **Port**, auf dem die LANCOM R&S®Unified Firewall das LANCOM R&S®UF Command Center erreicht:
- Falls die LANCOM R&S®Unified Firewall und das LANCOM R&S®UF Command Center im selben Netz stehen, dann bleibt es beim Standard-Port (11940).
 - Falls die LANCOM R&S®Unified Firewall und das LANCOM R&S®UF Command Center in unterschiedlichen Netzen stehen, dann ist dies der Port auf dem Gateway, der zum Command Center weitergeleitet wird.
- c) Verwenden Sie das neue VPN-Zertifikat aus Schritt 4 als **Firewall Certificate**.
- d) Die CA des Command Center-Zertifikats aus Schritt 1 als **Command Center CA**.
- e) Optional die GPS-Koordinaten des LANCOM R&S®Unified Firewall-Standorts, damit die LANCOM R&S®Unified Firewall auf der Karte im Dashboard korrekt angezeigt wird.
- f) Schalten Sie oben links die Verbindung zum LANCOM R&S®UF Command Center ein

Command Center ✕

 Modified version - changes will be preserved until you reset or log out.




Host

Port

Command Center CA ▾

Firewall Certificate ▾

Firewall Location

 Enter the coordinates of the firewall location here. Use a pure decimal degrees notation, e.g. Latitude 53.555483 and Longitude 9.984625.

Latitude °

Longitude °

5. Im LANCOM R&S®UF Command Center unter **Firewalls > Device Selection** erscheint die verbundene LANCOM R&S®Unified Firewall.
6. Die neue LANCOM R&S®Unified Firewall auf **Administrated** setzen.
7. Die neue LANCOM R&S®Unified Firewall erscheint im Dashboard.

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Würselen | Deutschland
info@lancom.de
www.lancom-systems.de