Beratung und Support
Technische Plattform
Support-Netz-Portal

paedML® – stabil und zuverlässig vernetzen

Anleitung

Installationsanleitung

Stand 14.02.2023

paedML® Linux

Version: 7.2

paedML® für Grundschulen

Version: 7.2

paedML L

lmz Landesmedienzentrum Baden-Württemberg

Impressum

Herausgeber

Landesmedienzentrum Baden-Württemberg (LMZ)
Support-Netz
Rotenbergstraße 111

70190 Stuttgart

Autoren

der Zentralen Expertengruppe Netze (ZEN),
Support-Netz, LMZ

Michael Salm, Alexander Vötterle

Endredaktion

Kay Höllwarth

Bildnachweis Symbole Titelseite

CC By 3.0 US von Gregor Cresnar, The Noun Project

Weitere Informationen

www.support-netz.de
www.lmz-bw.de

Änderungen und Irrtümer vorbehalten.

Veröffentlicht: 2022

Inhaltsverzeichnis

Einführung

Mit der paedML Linux 7.2 haben Sie sich für eine moderne IT-Lösung entschieden, die mit einem professionellen technischen Unterbau ausgestattet ist. Verlässlichkeit und Stabilität kennzeichnen die neue Version, denn Hardwareunterstützung und die Handhabung wurden deutlich verbessert. Technologisch gesehen ist die paedML Linux 7.2 stärker modular aufgebaut, wodurch die weitere Produktentwicklung in Zukunft flexibler gestaltet werden kann. Wir sind an der Rückmeldung unserer Kunden interessiert und wenn Sie Anregungen oder Wünsche für die Weiterentwicklung der paedML Linux haben, bitten wir Sie um Rückmeldung z. B. über unseren User-Helpdesk.

Die Hotline steht Ihnen mit Rat und Tat zur Seite, um Sie in der Administration Ihres schulischen Netzwerks zu unterstützen. Die Erfahrung hat gezeigt, dass es ratsam ist, lieber einmal zu viel, als einmal zu wenig in der Hotline anzurufen. Wenn Sie Fragen zu Ihrer paedML Linux haben, dann kontaktieren Sie bitte Ihre Supportmitarbeiter.

Linux-Hotline	**Geschäftszeiten:**
0711 – 25 35 83 88	montags - donnerstags 8.00 - 16.00 Uhr
linux-hotline@lmz-bw.de	freitags 8.00 - 14.30 Uhr
Grundschul-Hotline	
0711 - 25 35 83 91	montags - donnerstags 8.00 - 16.00 Uhr
gs-hotline@lmz-bw.de	freitags 8.00 - 14.30 Uhr

Es gibt drei Handbücher für die *paedML Linux*:

- Die hier vorliegende „**Installationsanleitung**“, welche die Einrichtung von VMware, das Aufsetzen der *paedML Linux* Infrastruktur und den technischen Aufbau des *paedML Linux*-Netzwerks behandelt. Diese Anleitung richtet sich an *Dienstleister*, die die *paedML Linux* einrichten.
- Das „**Administrationshandbuch**“ richtet sich an den *Netzwerkberater* als Systembetreuer der Schule und an den *Dienstleister*. In diesem Handbuch werden administrative Aufgaben beschrieben, die im Schulalltag getätigt werden können. Darüber hinaus werden dort auch administrative Aufgaben bei der Einrichtung des Schulnetzes beschrieben, die primäre Aufgabe des Dienstleisters ist, der das Schulnetz einrichtet.
- Das „**Handbuch für Lehrkräfte**“, welches die pädagogischen Funktionen Ihrer *paedML Linux* näher beschreibt, erläutert relevante Module für den Unterricht.

Neben diesen drei Handbüchern gibt es weitere Dokumente, die Sie bei der Planung und dem Aufbau eines *paedML Linux* Netzwerkes unterstützen.

- Der „**Konzeptionsleitfaden**“ ist eine Kurzeinführung in die *paedML Linux*. Dieses Dokument enthält Hinweise zur Planung der Installation des schulischen Netzwerkes.
- Hinweise für die Ausschreibung des schulischen Netzes und bei der Übergabe des Netzwerks von Ihrem Dienstleister an die Schule finden Sie in unserem „**Ausschreibungsleitfaden**“.
- In einem weiteren Dokument haben wir die „**Hardwareanforderungen**“ der paedML Linux zusammengefasst.

Um Doppellungen zu vermeiden haben wir unsere Handreichungen dergestalt gegliedert, dass wir an gegebener Stelle auf die anderen Handbücher verweisen.

Alle hier genannten Handreichungen zur paedML Linux finden Sie unter https://www.lmz-bw.de/netzwerkloesung/produkte-paedml/paedml-linux/downloads/ .

Überprüfen Sie diese Seite bitte regelmäßig nach Aktualisierungen!

Typografische Konventionen

Zur besseren Lesbarkeit werden bestimmte Elemente typografisch vom Rest des Textes abgehoben.

- Hervorhebungen in diesem Dokument sind *kursiv*.
- Besondere Hervorhebungen sind **fett** ausgezeichnet.
- Ausgaben oder Abfragen von Programmen sind *„kursiv und erhalten Anführungszeichen“*. Ebenso werden Menüs oder Knöpfe, in Programmen und Bedienoberflächen mit Anführungszeichen hervorgehoben.
- Vom Benutzer auszuführende Tastatureingaben an der Linux-Konsole oder an der *Windows* Eingabeaufforderung (zum Beispiel Systembefehle) sowie Auszüge aus Systemdateien, werden durch die `Courier New` vom Rest des Textes abgesetzt. Das gleiche gilt für Zugangsdaten wie Benutzernamen oder Passwörter.
- Tastenbeschriftungen werden durch Rahmen hervorgehoben.
- Verschachtelte Menüstrukturen werden durch einen senkrechten Strich (|) als Trennzeichen (in der Linux Welt auch *„Pipe“*[1] genannt) voneinander getrennt. So finden Sie zum Beispiel den Zugriff für das Helpdesk-Modul unter *„Schulkonsole: Unterricht | Helpdesk kontaktieren“*.

Unter einigen Kapitelüberschriften finden Sie einen Hinweis, wie Sie den in dem Kapitel beschriebenen Baustein der *paedML Linux* aufrufen können. In der Regel werden konfigurative Änderungen, die in diesem Handbuch beschrieben sind, vom Netzwerkberater ausgeführt. Manche Menüs sind jedoch nur für den Administrator zugänglich. Diese Ausnahmen werden durch Nennung des vom Benutzer *„netzwerkberater“* abweichenden Benutzernamens gekennzeichnet.

Beispiele:

Aufruf über Schulkonsole (Administrator): Unterricht | Computerraum

Adresse: https://server.paedml-linux.lokal/nagios

Der Aufruf aller internen Webseiten der *paedML Linux* muss über den FQDN (voll qualifizierten Domain-Namen) der jeweiligen Seite geschehen.

Es genügt also nicht bspw. https://server/horde einzugeben, um die Startseite des Webmailers aufzurufen.

Nutzen Sie stattdessen https://server.paedml-linux.lokal/horde.

Hinweise und Tipps werden durch besondere Symbole grafisch vom Text abgehoben:

[1] http://de.wikipedia.org/wiki/Pipe_%28Informatik%29

Durch Hinweis-Felder werden Sie auf Sachverhalte hingewiesen, die Sie beachten sollten, um bestimmte Probleme zu vermeiden, die den Betrieb der *paedML Linux* beeinträchtigen könnten.

Das Tipp-Feld gibt Hinweise, die nicht zwingend notwendig, aber hilfreich sind.

Dieses Feld kennzeichnet Inhalte, die nicht von der Hotline unterstützt werden.

Es handelt sich einerseits um Funktionen und Programme, die nicht Bestandteil der Entwicklung der paedML Linux sind. Diese Programme sind in der Regel zu komplex und zu umfangreich, um in Ihrer Tiefe durch die Hotline unterstützt werden zu können.

Andererseits bewirken Änderungen in den beschriebenen Funktionen, Abweichungen von Standardeinstellungen der paedML Linux[2].

Aufgrund der besseren Lesbarkeit wird in diesem Handbuch die männliche Form verwendet.

Die weibliche Form ist selbstverständlich immer miteingeschlossen.

[2] In der Entwicklung unserer Produkte setzen wir Standards, die durch die Hotline unterstützt werden (können). Wir bitten Sie um Verständnis, dass es unseren Mitarbeitern nicht möglich ist auf alle Bedürfnisse en Detail einzugehen. Wir können Ihnen bei manchen Anfragen lediglich Hinweise geben, wie Sie Änderungen am System vornehmen oder wo Sie weitere Dokumentationen zu dem Thema finden können.

1 Grundlagen und Hinweise

Die paedML Linux besteht im Auslieferungszustand aus zwei Servern und einer Firewall. Zusätzlich wird ein Windows-Rechner, die sogenannte W10AdminVM benötigt. Diese Geräte werden virtualisiert installiert.

Im Folgenden soll ein Überblick über den Aufbau und die Nomenklatur der paedML Linux gegeben werden. Weitergehende Ausführungen finden sich im ersten Kapitel des Administrator-Handbuches.

Bitte installieren Sie immer die aktuelle Version der *paedML Linux*. Sollten Sie eine ältere Version installieren, müssen Sie die Update Anleitungen berücksichtigen:

https://www.lmz-bw.de/nc/netzwerkloesung/produkte-paedml/paedml-linux/#updates

Bitte halten Sie Ihren ESXi-Virtualisierungshost und alle seine Komponenten stets aktuell (Updates z.B. quartalsweise durchführen). Geben Sie den Zugriff auf den ESXi-Virtualisierungshost und seine Managementfunktionen nicht für das Internet frei. Der Fernzugriff im Rahmen des Supports durch das LMZ erfolgt ausschließlich über die Software „TeamViewer“.

1.1 Server, Firewall, AdminVM und Nextcloud

Die *paedML Linux* basiert in der Standardkonfiguration auf den folgenden vier virtuellen Maschinen mit unterschiedlichen Funktionen:

virtuelle Maschine	Funktionen (auszugsweise)
VM „*Server*“	Benutzerauthentifizierung File-Server (Benutzerverzeichnisse) Administration des Systems (Schulkonsole) Proxy-Server Steuerung des Internetzugriffs
VM „*opsi-Server*“	Client-Management (Ausrollen der Betriebssysteme, Softwareverteilung). Aus Gründen, die dem Unterbau auf *Univention Corporate Server* geschuldet sind, lautet die Bezeichnung an manchen Stellen auch „*backup*“.
VM „*Firewall*“	Die Firewall trennt die internen Netze (pädagogisches Netz, Lehrernetz, Gäste-Netz) und stellt den Internetzugang für diese Netze bereit. Die Firewall bietet eine Reihe von Filtermöglichkeiten.
VM „W10*AdminVM*“	Virtuelle Maschine, die unter *Windows 10* (64 bit) läuft. Sie wird für diverse Hilfsdienste (z.B. Gruppenrichtlinien, *Windows*-Aktivierung) benötigt, die zwingend unter *Windows* laufen müssen. Für diese VM wird eine *Windows 10* (64 bit)-Lizenz benötigt.
VM Nextcloud	Eine virtuelle Maschine mit einem UCS-Server, auf dem die App Nextcloud installiert ist. Die Verwendung ist optional.

Tabelle 1: Die virtuellen Maschinen der paedML Linux

1.2 Virtualisierung

Virtualisierungs-Host

Grundlage der Virtualisierung bildet der physische Server, der sogenannte „*Virtualisierungs-Host*“. Dieser muss über genügend Prozessorleistung, Hauptspeicher und Plattenplatz verfügen. Hinweise zur Ausstattung des Virtualisierungs-Hosts finden Sie in unseren Hardwareanforderungs-Dokument unter https://www.lmz-bw.de/nc/netzwerkloesung/produkte-paedml/paedml-linux/#manuals.

Hypervisor

Als *Hypervisor* bezeichnet man die Software, die auf dem Virtualisierungs-Host die eigentliche Virtualisierung vornimmt und eine Umgebung für virtuelle Gastsysteme zur Verfügung stellt. Die *paedML Linux* basiert auf *VMware vSphere ESXi*, einem nativen Hypervisor, der ohne ein zusätzliches Wirts-Betriebssystem direkt auf der Hardware des Servers läuft.

Virtuelle Maschinen

In der virtuellen Umgebung des Hypervisors werden mehrere virtuelle Maschinen (VM) betrieben. Diese virtuellen Maschinen laufen auf „virtueller Hardware“ und teilen sich die Ressourcen des Virtualisierungs-Hosts.

Konsolenzugriff auf den Hypervisor

Per angeschlossener Tastatur und Monitor kann auf den Hypervisor nur über eine Textoberfläche zugegriffen werden, die ausschließlich zur Basiskonfiguration des Hypervisors selbst dient. Eine Verwaltung oder ein Zugriff auf die virtuellen Maschinen ist darüber nicht möglich.
Sollte es später bei einer versehentlichen Fehlkonfiguration der Netze über die grafische Schnittstelle (s. nächster Abschnitt) zu einem sog. „Lockout“ kommen, d.h. der Zugriff über die grafische Schnittstelle dadurch auf den Hypervisor abgeschnitten sein, so kann über die Textkonsole der Netzzugriff wieder hergestellt werden.

Grafischer Zugriff auf die virtuellen Maschinen

Die Verwaltung der virtuellen Maschinen und der grafische Zugriff erfolgt über das Webinterface (Host-Client oder *vSphere Client*). Diese Anleitung bezieht sich auf den Host-Client.

Für den Installationsvorgang der *paedML Linux* kann der *vmware-Host-Client* auch temporär auf einem beliebigen PC (z.B. auf dem Notebook eines IT-Dienstleisters) verwendet werden, der per Netzwerk mit dem Virtualisierungs-Host verbunden ist.

Im laufenden Betrieb ist es ebenfalls notwendig, per *vmware-Host-Client* auf die virtuellen Maschinen zuzugreifen. Hierzu könnte auf den *vmware-Host-Client* über einen beliebigen PC oder Notebook zugegriffen werden. Dieses Gerät muss über das Netzwerk mit dem Virtualisierungs-Host verbunden sein.

1.3 Management-PC

In der vorliegenden Installationsanleitung wird unter dem Begriff *Management-PC* ein physischer PC verstanden, über den auf den *vmware-Host-Client* zugegriffen wird. Dieser Rechner ist über das Netzwerk mit dem Virtualisierungs-Host verbunden. Bei der Einrichtung des schulischen Netzes kann ein Rechner des Dienstleisters diese Aufgabe übernehmen.

Vorgehensweise nach der Installation

Wenn die Installation der paedML Linux abgeschlossen ist, wird der Management-PC nur noch sporadisch benötigt. Über den vmware-Host-Client werden virtuelle Maschinen und/oder der Hypervisor gestartet oder heruntergefahren. Konfigurative Änderungen an der Virtualisierung werden ebenfalls über den vmware-Host-Client durchgeführt.

Obwohl aus „Kostengründen“ auch ein Client-PC temporär als Management-PC zweckentfremdet werden könnte, empfehlen wir, für Administrationsaufgaben der paedML Linux einen dedizierten PC als Management-PC zu verwenden.

Der Vorteil beim Einsatz eines dedizierten Management-PCs im Netzsegment „Internet“ (vgl. folgender Abschnitt) ist, dass Dienstleister oder die Hotline immer auf das System zugreifen können. Dies gilt auch, wenn der Virtualisierungs-Server Probleme macht, da der Zugriff direkt nach dem Router erfolgt. Wenn das Gerät nicht in Benutzung ist, kann es ausgeschaltet werden.

Bei *„Management-PC“* und *„AdminVM“* handelt es sich um völlig verschiedene Maschinen, die nicht verwechselt werden sollten.

1.4 Netzübersicht

Innerhalb der *paedML Linux* sind fünf Netze definiert:

- „*PAEDAGOGIK*“: Hier befinden sich die Client-Rechner und die Server der *paedML Linux*.
- „*GAESTE*“: Das Gäste-Netz ist für den sicheren Betrieb von nicht zum Schul-Netz gehörigen Rechnern wie Notebooks von Schülern oder Lehrern (Stichwort: „*Bring Your Own Device*“) vorgesehen. Sollen keine schulfremden Geräte an das Schulnetz angeschlossen werden, so kann auf das Gäste-Netz verzichtet werden.
- „*INTERNET*“: Netz für die Internetanbindung und den Management-PC, über den auf den Hypervisor zugegriffen werden kann. In der Nomenklatur des Hypervisors ist dies das sogenannte „*Management-Netz*“.
- „*MDM*“ – Netz für Geräte, die mit einem MDM verwaltet werden, z.B. iPads. Sollten keine MDM-verwalteten Geräte verwendet werden, kann auf dieses Netz verzichtet werden.
- „*DMZ*“ – Netz, welches für den sicheren Betrieb der Nextcloud benötigt wird. Sollte keine Nextcloud zum Einsatz kommen, können Sie auf dieses Netz verzichten.

Die Netze können sowohl mit drei physikalisch getrennten Switchen, als auch per VLAN über einen management-fähigen Switch betrieben werden. Dies ist von der vorhandenen Netzinfrastruktur der Schule abhängig.

Jedes Netz existiert sowohl außerhalb des Virtualisierungs-Hosts als auch innerhalb der virtualisierten Umgebung (außer das Netz DMZ). Dort existiert für jedes Netz ein „virtueller Switch“ (in der VMware-Nomenklatur „*vSwitch*“).

Innerhalb der virtualisierten Umgebung werden die virtualisierten Netzwerkkarten der VMs „per Mausklick“ mit einem *vSwitch* verbunden und so an das Netz angebunden.

Die physischen Netzwerkkarten des Virtualisierungs-Hosts verbinden den physischen mit dem virtualisierten Teil eines jeden Netzes. Aus Sicht der Netzwerkgeräte (Client-PCs und auch virtualisierte Server) geschieht dies jedoch völlig transparent.

Die Einrichtung und Wartung einer funktionierenden Netzwerk-Infrastruktur ist Aufgabe des Dienstleisters.

Die Mitarbeiter der Hotline können hierbei nur unterstützend wirken.

1.5 Schematische Übersicht über die paedML Linux

Die folgende Grafik gibt einen Überblick über den Aufbau der *paedML Linux*:

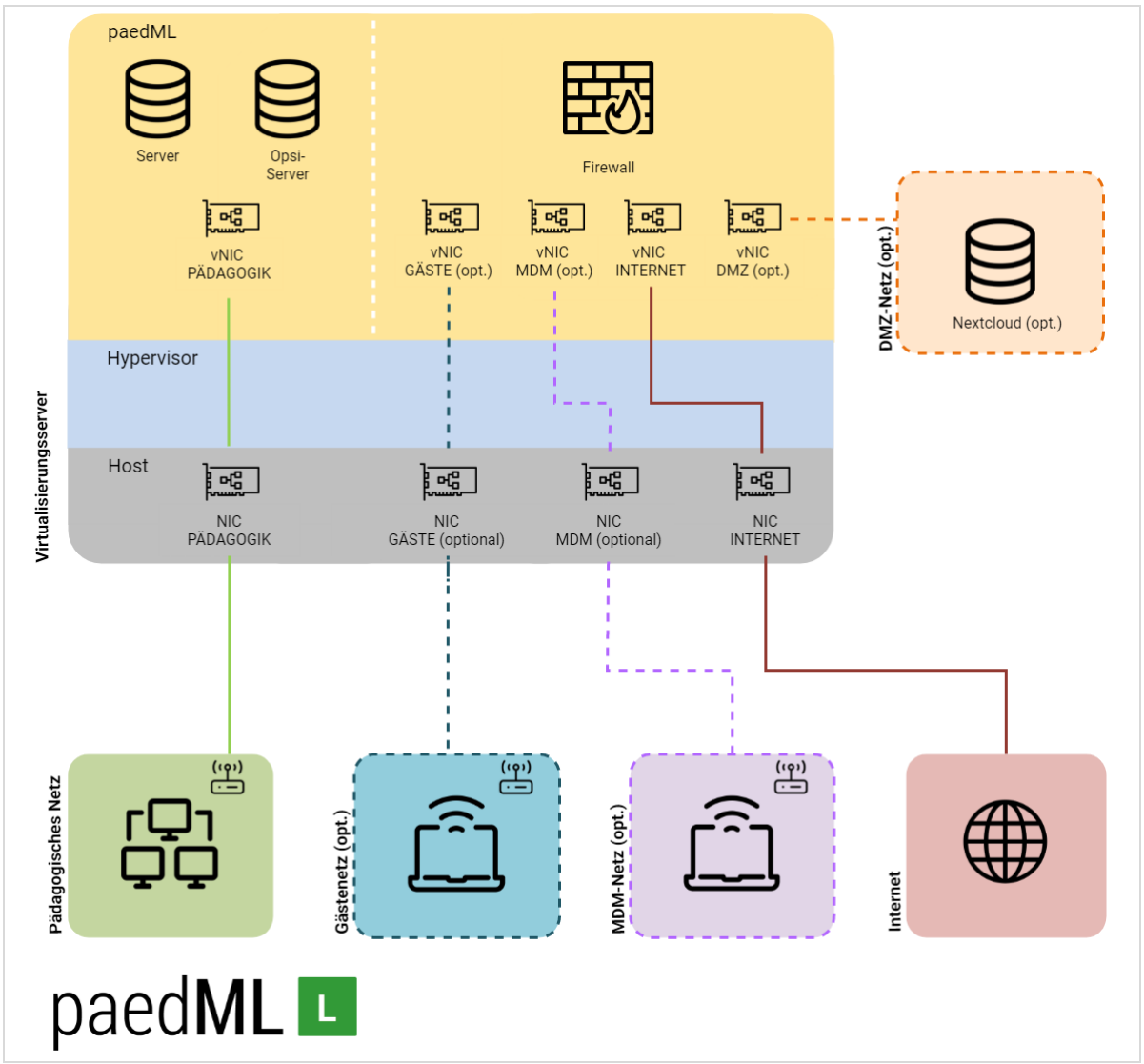

Abb. 1: Schematischer Aufbau der paedML Linux.

2 Vorbereitung des Virtualisierungs-Hosts

Bitte beachten Sie folgende Schritt-für Schritt-Ableitung zur Installation des Virtualisierungs-Hosts: https://masteringvmware.com/how-to-install-esxi-6-7-step-by-step/ .

Auf dem Virtualisierungs-Host muss zunächst der Hypervisor (Virtualisierungs-Software) installiert werden. In der *paedMLLinux* kommt das Produkt „*VMware vSphere Hypervisor (ESXi)*“ zum Einsatz.

In den folgenden Schritten werden Download, Installation und Basiskonfiguration des Hypervisors beschrieben.

2.1 Download des Installationsmediums

Den freien Hypervisor „*VMware vSphere Hypervisor (ESXi)*“ können Sie sich auf der Website des Herstellers unter http://www.vmware.com/de/products/vsphere-hypervisor.html herunterladen. Hierzu ist lediglich eine Registrierung per Emailadresse („*Create an Account*“, bzw. „*Konto erstellen*“) auf der vorgenannten Website erforderlich. Empfohlen wird mindestens die Version 6.7 oder höher.

Brennen Sie abschließend das zuvor heruntergeladene ISO-Image des Hypervisors auf CD. Sie benötigen diese im Rahmen des folgenden Installationsprozesses.

2.2 Beschaffung eines schulspezifischen Lizenzschlüssels

Der *vSphere Hypervisor* befindet sich direkt nach der Installation in einem 60 Tage andauernden Testmodus, in welchem er auch im Hinblick auf die teuerste Kaufvariante des vorgenannten Hypervisors zunächst funktional uneingeschränkt ist.

Bitte beachten Sie, dass Sie nur mit der Kaufvariante des vSphere Hypervisors die Sicherung des Systems (virtuelle Maschinen und Daten) durchführen können. Weitere Informationen zur Sicherung und Wiederherstellung der paedML Linux finden Sie hier: https://www.lmz-bw.de/nc/netzwerkloesung/produkte-paedml/paedml-linux/#howtos

Es wird empfohlen, die schulische Hypervisor-Installation vor Ort umgehend auf eine zeitlich unbefristete Nutzungsdauer umzustellen, indem Sie den Lizenzschlüssel eingeben.

Der individuelle Lizenzschlüssel für die Schule lässt sich nach Login auf der Herstellerseite mit dem oben erzeugten Benutzerkonto unter der Rubrik „*License & Download*“ abrufen. Am besten speichern Sie diesen Lizenzschlüssel auf einem externen Datenträger (z.B. USB-Stick) ab, da er später noch für die kostenlose Lizensierung des Virtualisierungs-Hosts benötigt wird.

Für spätere Verwendungszwecke (z.B. Neuinstallation des Hypervisors) ist es ratsam den Lizenzschlüssel aufzubewahren.

2.3 Installation des Hypervisors auf dem Virtualisierungs-Host

Die eingesetzte Serverhardware sollte grundsätzlich VMware-zertifiziert sein (vgl. https://www.vmware.com/guides.html) und darüber hinaus dem Hardware-Anforderungspapier zur

paedML Linux (vgl. https://www.lmz-bw.de/nc/netzwerkloesung/produkte-paedml/paedml-linux/#manuals) entsprechen.

Legen Sie nun die gebrannte Installations-CD in das optische Laufwerk des Servers ein und booten Sie diesen von CD-ROM.

Wenn Ihr Server auf Booten vom optischen Laufwerk eingestellt ist, erscheint zunächst das folgende Auswahlmenü:

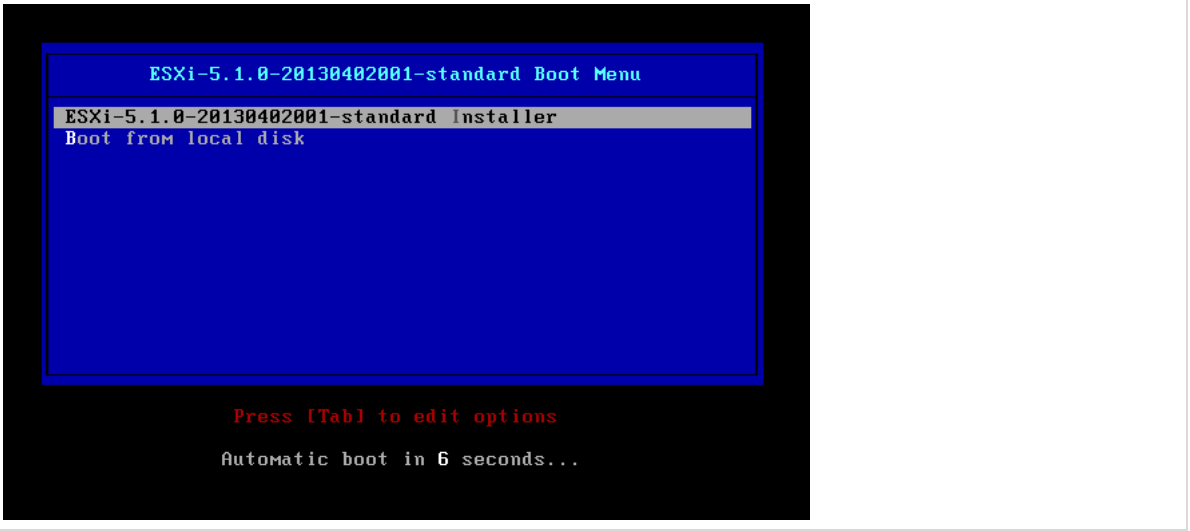

Abb. 2: Auswahl des Bootmediums

Bestätigen Sie den Bootvorgang von der Installer-CD mit Enter. Daraufhin wird das Installer-System von CD gebootet:

Beim Installationsvorgang werden sämtliche Daten auf der Festplatte unwiederbringlich gelöscht!

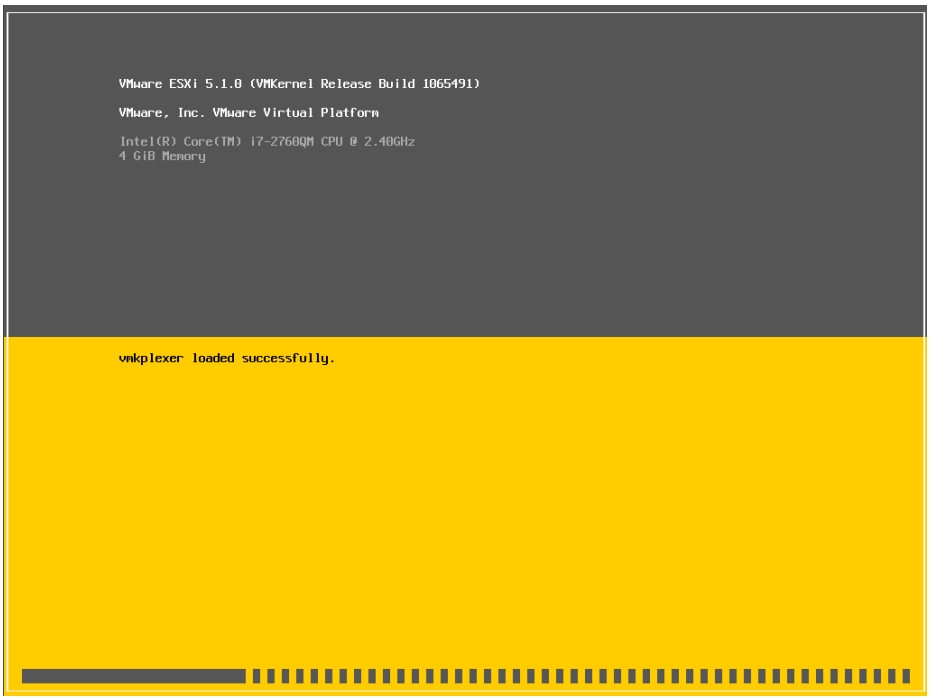

Abb. 3: Bootvorgang des Installer-Systems

Nach kurzer Wartezeit wird der Startschirm der Installationsroutine angezeigt. Bestätigen Sie den Start des Installationsvorgangs mit ENTER.

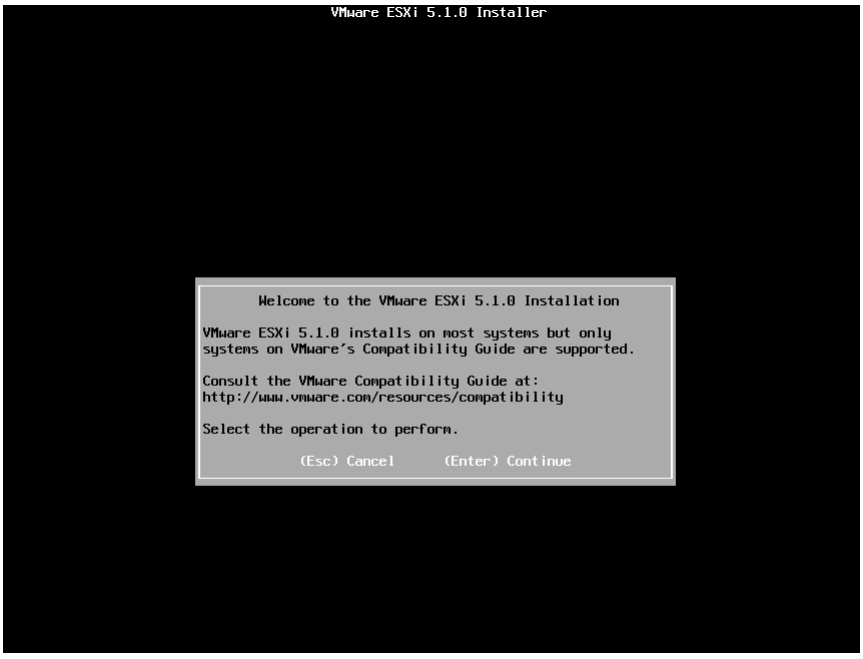

Abb. 4: Start der Installation des Hypervisors

Im nächsten Bildschirm werden die Lizenzbedingungen (*End User License Agreement*, kurz *EULA*) angezeigt:

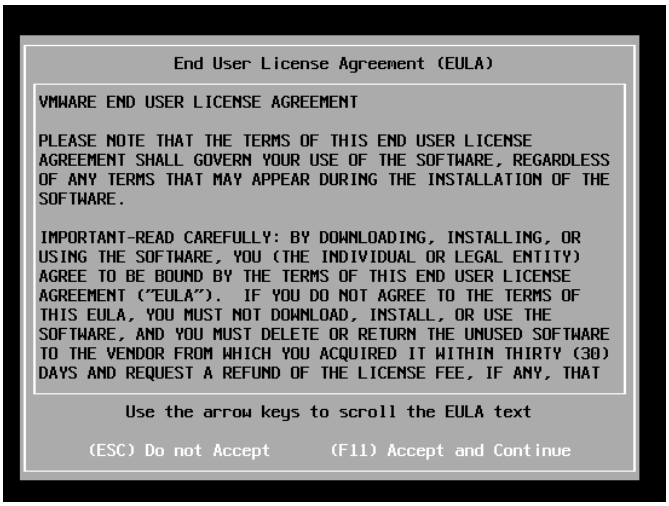

Abb. 5: Bestätigung der Lizenzbedingungen des Hypervisors

Bestätigen Sie mit F11. Der Installer beginnt mit dem Scannen der Hardware.

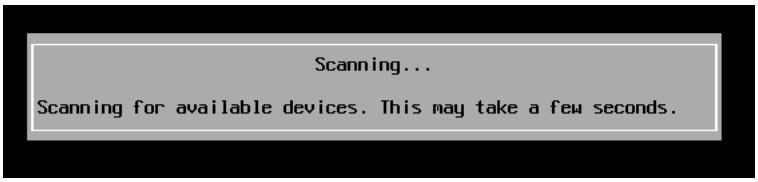

Abb. 6: Scan der Hardware des Virtualisierungs-Hosts

Im nächsten Bildschirm muss die Festplatte für die Installation des Hypervisors ausgewählt werden:

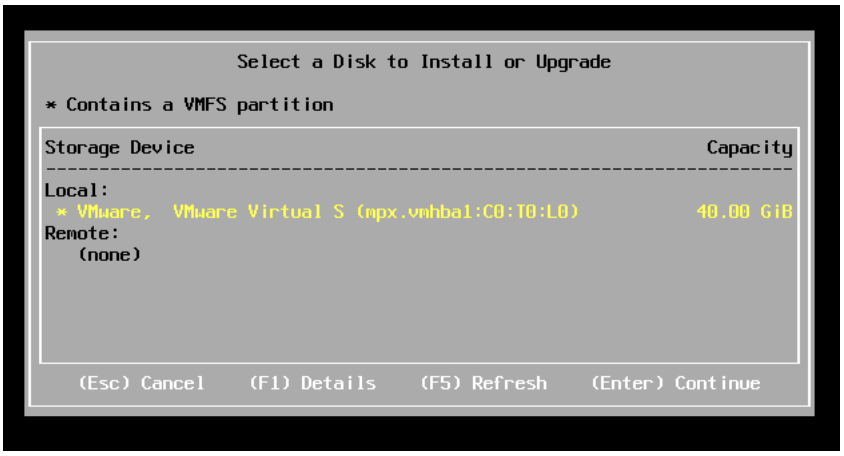

Abb. 7: Auswahl der Festplatte, auf der der Hypervisor installiert wird.

Wählen Sie die Festplatte aus, auf der der Hypervisor installiert werden soll und bestätigen Sie Ihre Wahl mit ENTER.

Im nächsten Bildschirm muss die Tastaturbelegung ausgewählt werden:

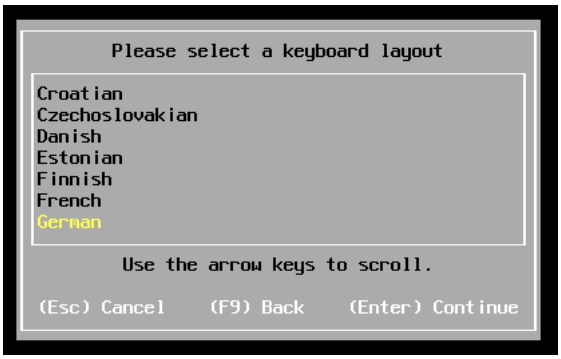

Abb. 8: Auswahl der Tastaturbelegung

Wählen Sie mit den Pfeiltasten Hoch/Runter die gewünschte Tastaturbelegung aus (typischerweise „*German*“) und bestätigen Sie mit ENTER.

Im nächsten Bildschirm müssen Sie ein *root*-Passwort für die Administration des Hypervisors vergeben:

Abb. 9: Setzen des root-Passworts für den Hypervisor

Geben Sie das *root*-Passwort zweimal ein und bestätigen Sie mit ENTER.

Nach einem weiteren Scan muss die endgültige Installation des Hypervisors nochmals bestätigt werden:

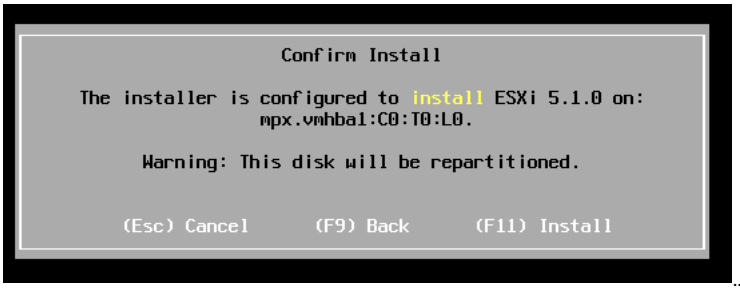

Abb. 10: Endgültige Bestätigung der Installation des Hypervisors

Bestätigen Sie die Installation mit F11. Daraufhin beginnt der eigentliche Installationsvorgang.

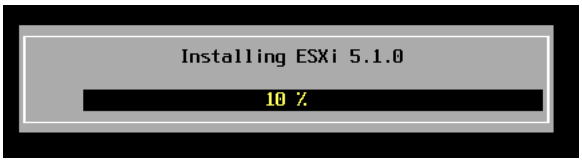

Abb. 11: Installationsvorgang des Hypervisors

Nach erfolgreichem Abschluss des Installationsvorgangs erscheint die folgende Meldung:

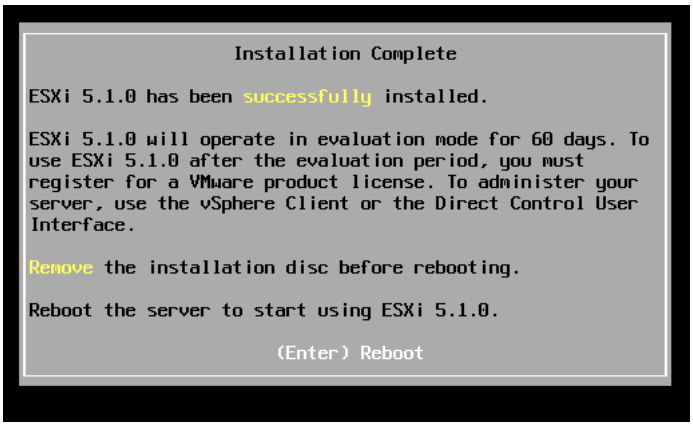

Abb. 12: Der Hypervisor wurde erfolgreich installiert

Bestätigen Sie den Neustart des Systems mit ENTER, das System führt einen Neustart aus:

Abb. 13: Neustart des Systems nach abgeschlossener Installation

Nach dem Neustart des Systems erscheint die Oberfläche des Hypervisors. Damit ist die Basisinstallation des Hypervisors abgeschlossen.

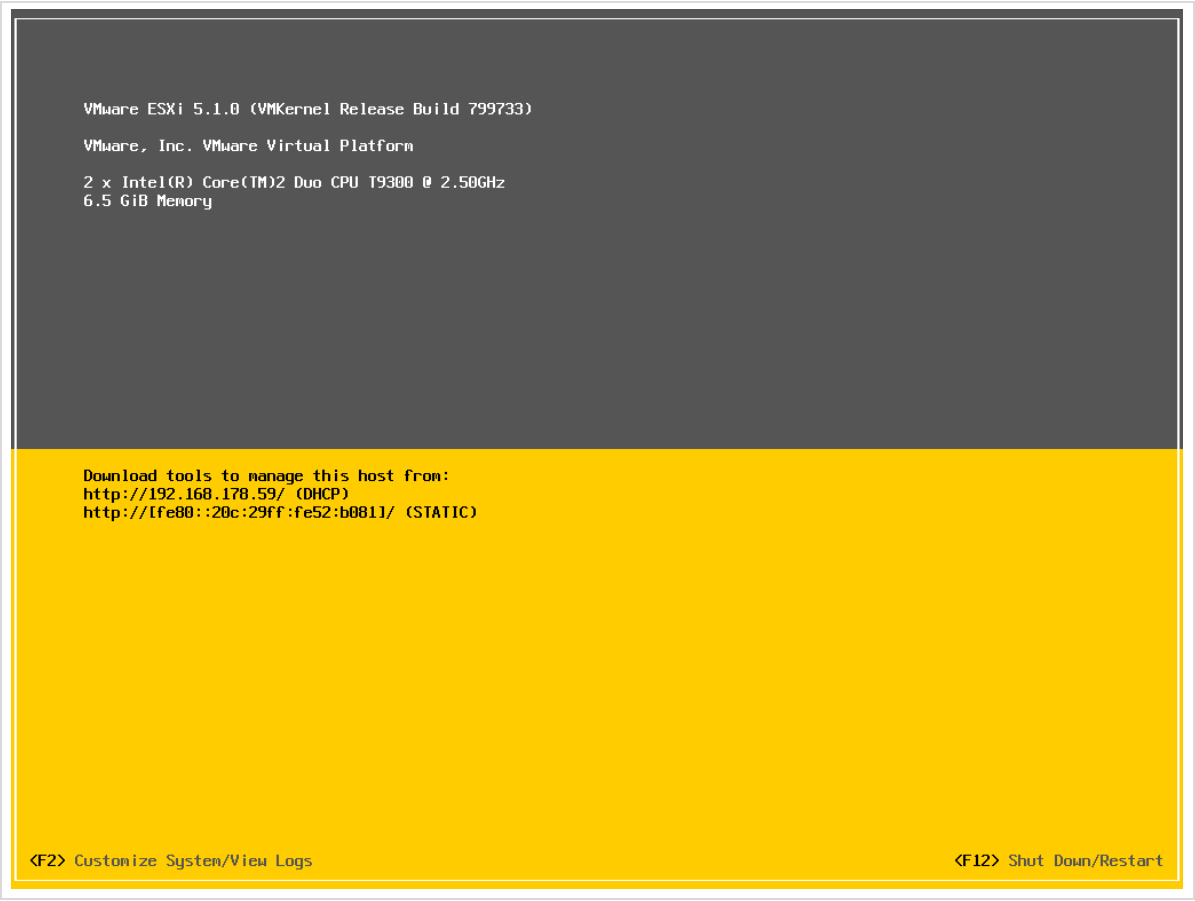

Abb. 14: Oberfläche des Hypervisors nach dem Neustart

2.4 Anschluss des Virtualisierungs-Hosts an die Netzwerkinfrastruktur der Schule

In der vorliegenden Anleitung wird von den folgenden Prämissen ausgegangen:

Netzbezeichnung	Verwendung
INTERNET	▪ Internetanschluss z.B. über einen DSL-Router wie zum Beispiel *Telekom Speedport*, *AVM FRITZ!Box,…* ▪ Außerdem Zugriff auf den Hypervisor per *vmware-Host-Client*
PAEDAGOGIK	▪ Netz mit strukturierter Verkabelung und evtl. WLAN für **schuleigene und von der *paedML Linux* verwaltete** Geräte
GAESTE	▪ „*Gäste-Netz*“ mit strukturierter Verkabelung und evtl. WLAN für **schulfremde bzw. nicht von der *paedML Linux* verwaltete** Geräte
MDM	▪ Optionales MDM-Netz für Geräte, die mit einem MDM verwaltet werden.
DMZ	▪ Optionales DMZ-Netz, das benötigt wird, wenn die Nextcloud zum Einsatz kommen soll.

Tabelle 2: Die Bezeichnungen der einzelnen Netze

Vor dem Durchführen der im nächsten Abschnitt beschriebenen Arbeiten empfehlen wir, vorerst nur eine der (mindestens) drei im Server vorhandenen Netzwerkkarten per Kabel anzuschließen. Dieses zuerst

eingesteckte Kabel sollte (eventuell über einen Switch) mit einer der LAN-Buchsen Ihres DSL-Routers verbunden sein.

Die schrittweise Vorgehensweise bezüglich der Verkabelung der beiden anderen im Server befindlichen Netzwerkkarten erleichtert die Zuordnung der Karten zu den im Verlauf der Installation noch einzurichtenden virtuellen Netzwerken.

2.5 Grundlegende Konfiguration Virtualisierungs-Host

Nach Abschluss der Basisinstallation und Neustart des Servers finden Sie sich auf der Startseite des Hypervisors wieder. Über die F2-Taste gelangen Sie – nach Eingabe von Benutzername (root) und zugehörigem Passwort – in das Konfigurationsmenü.

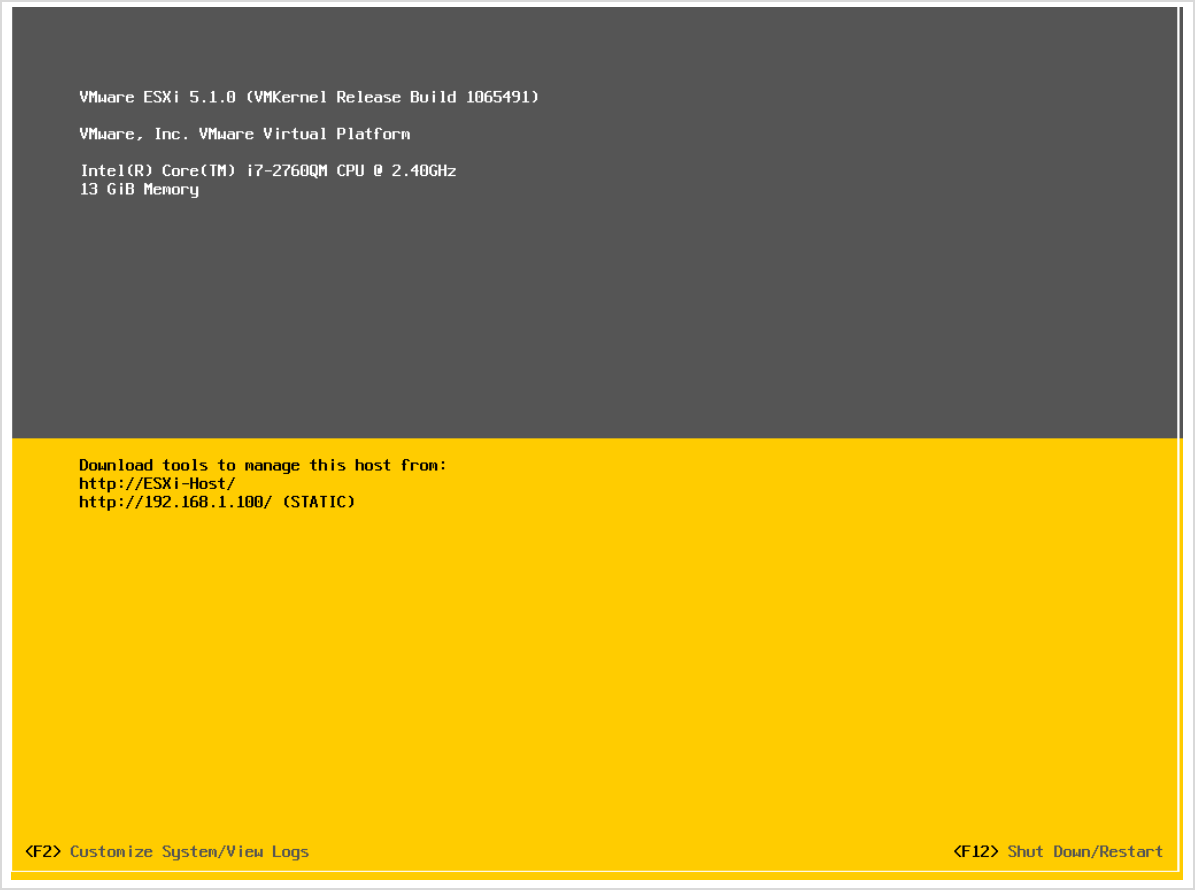

Abb. 15: Hypervisor nach Abschluss der Basisinstallation

Falls im Netz „*INTERNET*“ ein DHCP-Server vorhanden ist (z.B. auf einem DSL-Router), bekommt die externe Netzwerkkarte des Virtualisierungs-Hosts automatisch eine IP-Adresse zugewiesen. Aus Gründen der Wartbarkeit empfehlen wir jedoch, die IP-Adresse des ESXi-Servers statisch zu vergeben.

Im Folgenden wird ein Class C Netz verwendet. Der Router wird als Default-Gateway genutzt und läuft auf der IP-Adresse 192.168.1.1. Der ESXi-Server bekommt die Adresse 192.168.1.100 zugewiesen.

Im Folgenden wird der Virtualisierungs-Host so eingerichtet, dass der Hypervisor per *vmware-Host-Client*über eine statische IP-Adresse aus dem Netz „*INTERNET*“ erreichbar ist.

Das „Management Network“

In der VMware-Nomenklatur bezeichnet „*Management Network*" das Netzwerk, über das der Hypervisor mittels *vmware-Host-Client* zu Management-Zwecken erreichbar ist. Bei der Einrichtung der *paedML Linux* wird empfohlen das Management-Netz auf das Netzwerk „*INTERNET*" zu legen.

2.5.1 Verbinden der physischen NIC mit dem Netz „INTERNET"

Verbinden Sie zunächst nur diejenige Netzwerkkarte (NIC) des Virtualisierungs-Hosts, die für das Netz „*INTERNET*" vorgesehen ist. Verbinden Sie die Netzwerkkarte per LAN-Kabel mit dem entsprechenden Switch oder direkt mit der LAN-seitigen Buchse des DSL-Routers.

Durch Drücken der F2-Taste und anschließender root-Authentifizierung gelangen Sie in das Menü, in dem Sie die Netzwerkkonfiguration des Virtualisierungs-Hosts anpassen können.

Navigieren Sie per Pfeiltaste auf die Option „*Configure Management Network*" und bestätigen Sie mit Enter.

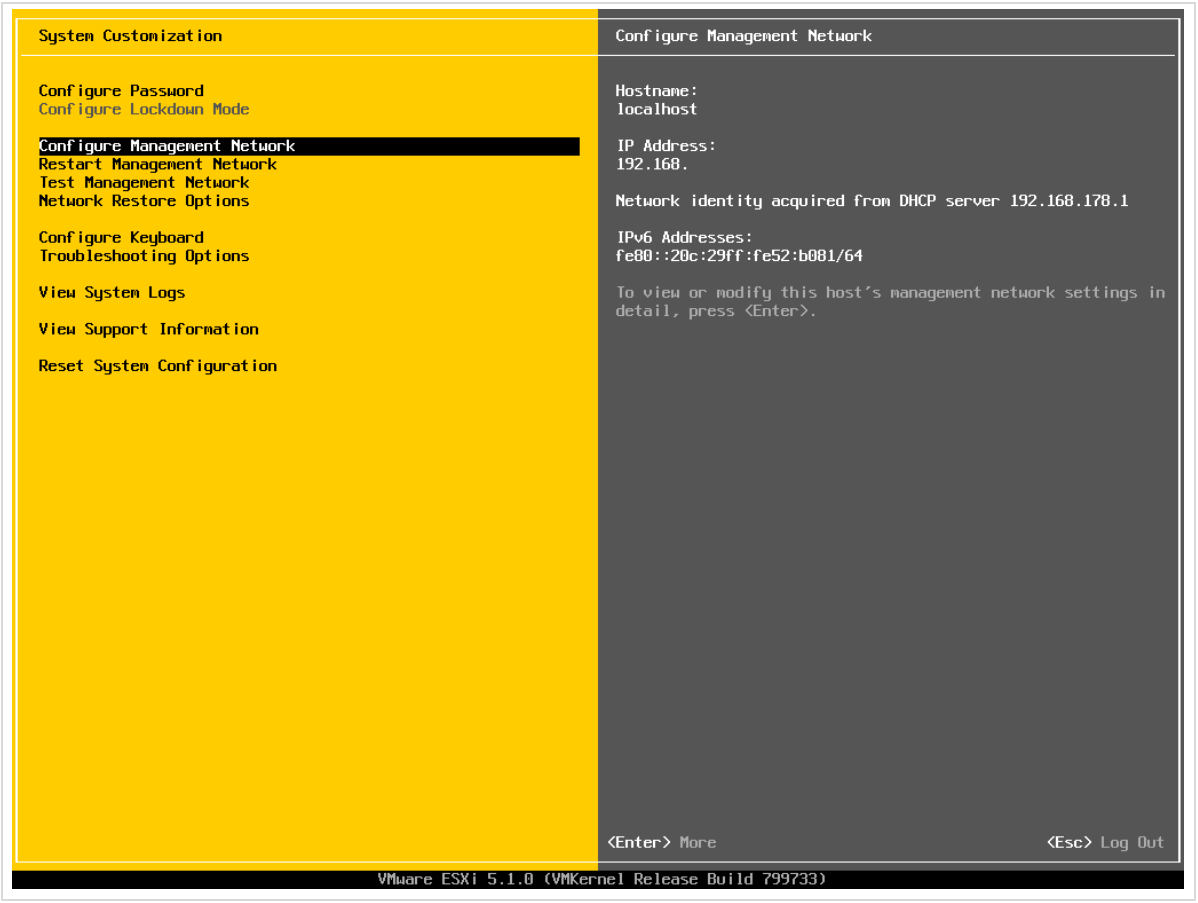

Abb. 16: Hauptmenü zur Konfiguration des Hypervisors

2.5.2 Auswahl der Netzwerkkarte für das „Management Network"

Wählen Sie im nächsten Menü per Pfeiltasten die Option „*Network Adapters*" aus und bestätigen Sie mit Enter:

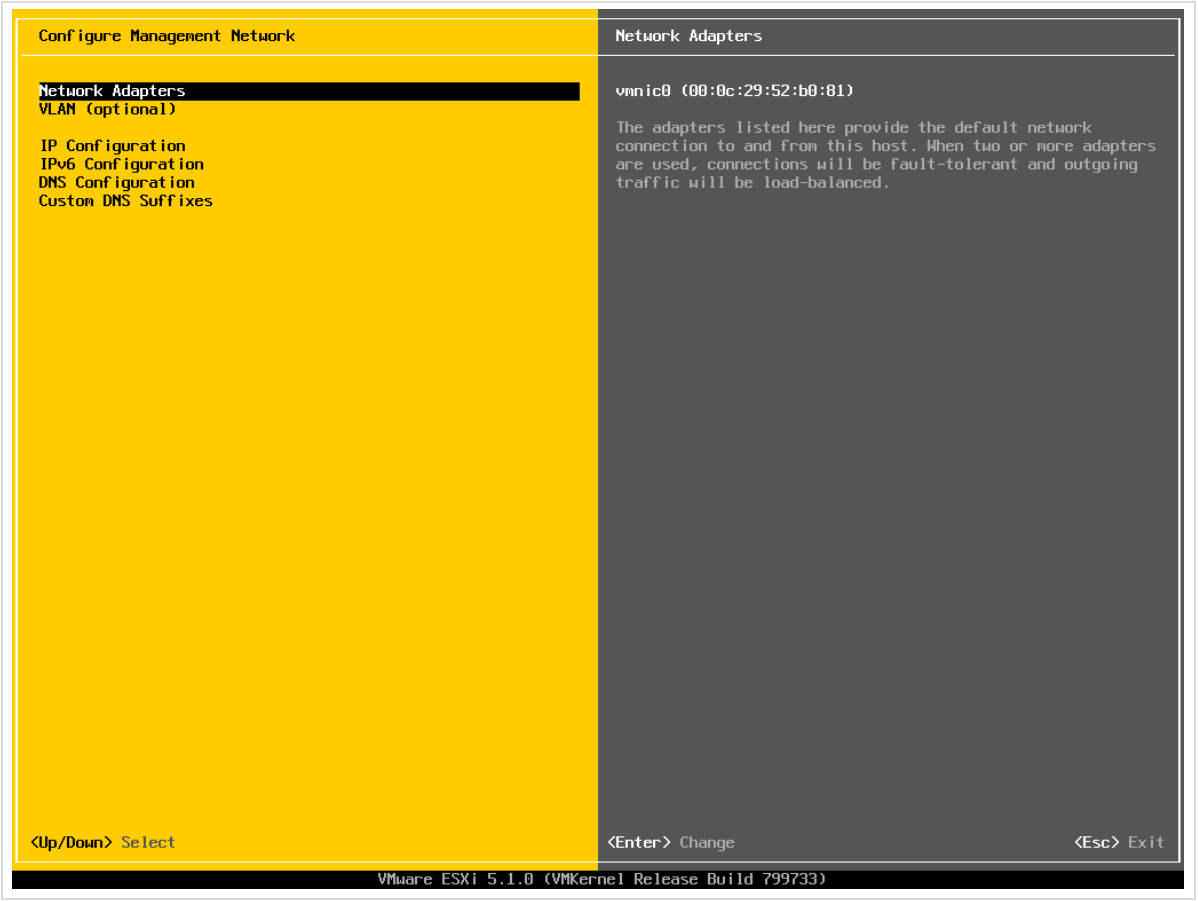

Abb. 17: Untermenü zur Konfiguration des „Management Networks“

Markieren Sie durch Drücken der Leertaste diejenige Netzwerkkarte, die den Status „*Connected*“ hat mit einem „*X*“. Entfernen Sie eventuell gesetzte Markierungen bei den anderen Netzwerkkarten. Bestätigen mit Enter.

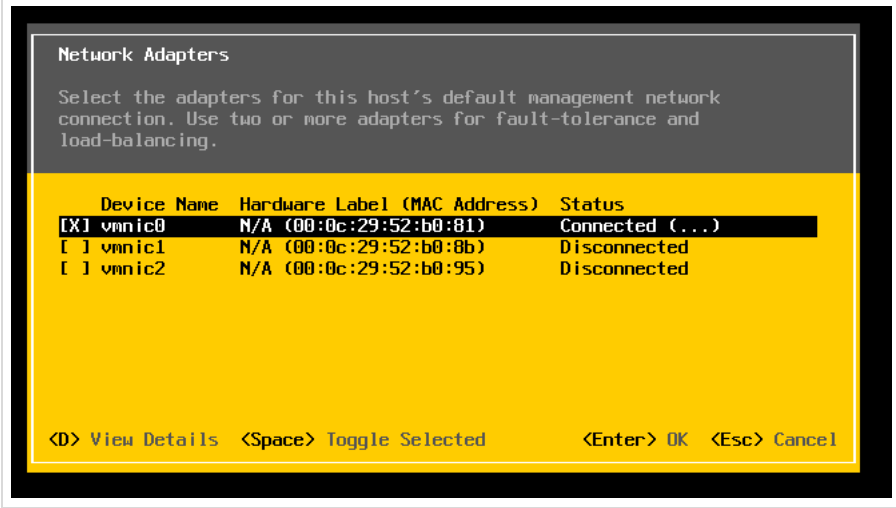

Abb. 18: Konfiguration der Netzwerkkarte für das „Management Network“

2.5.3 Setzen der IP-Adresse im „Management-Network“

Zurück im nachfolgenden Menü wählen Sie bitte per Pfeiltaste die Option „*IP Configuration*“ aus und bestätigen Sie dann die Auswahl mit Enter:

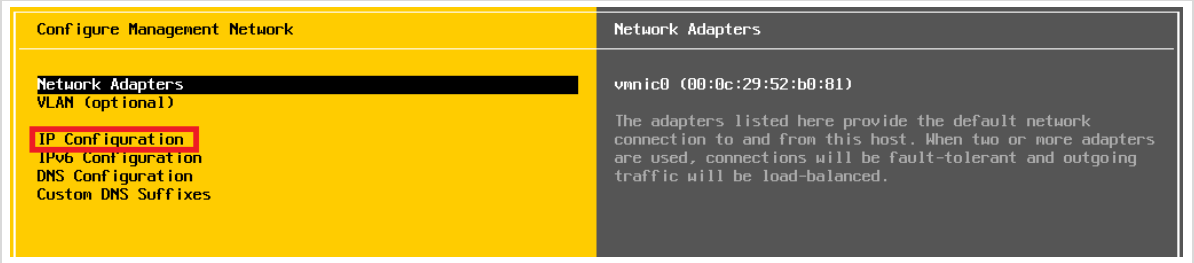

Abb. 19: Auswahl des Punkts „IP Configuration“

Wählen Sie die zweite Option („*Set static IP address…*“) aus. Vergeben Sie die statische IP (ggf. auf eigenen IP-Bereich anpassen!) und bestätigen Sie mit Enter.

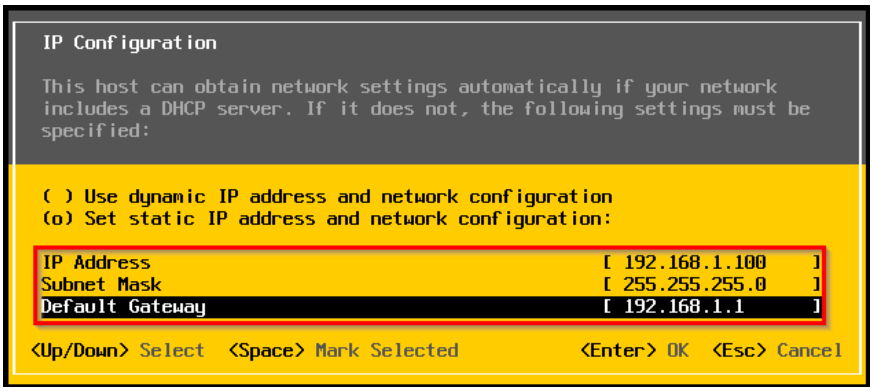

Abb. 20: Eintragen der statischen IP-Adresse

2.5.4 Deaktivieren von IPv6

Die Deaktivierung von IPv6 auf dem Hypervisor ist nicht zwingend erforderlich, wird jedoch empfohlen.

Wählen Sie im Konfigurationsmenü per Pfeiltaste die Option „*IPv6 Configuration*“ aus und bestätigen Sie dann die Auswahl mit Enter:

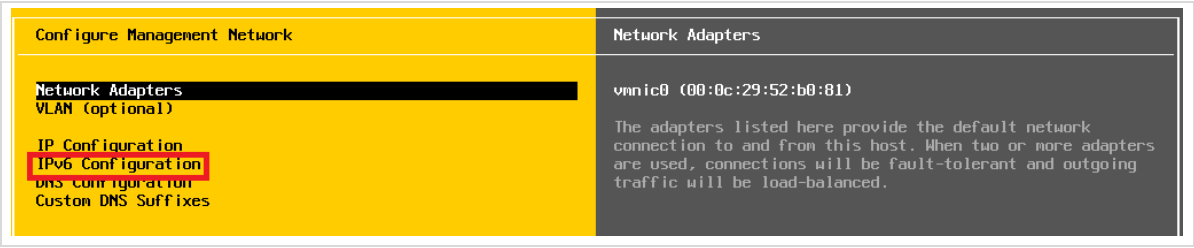

Abb. 21: Navigation zur Konfiguration von IPv6

Um IPv6 zu deaktivieren, muss das Kreuz bei „*Enable IPv6*“ entfernt werden. Bestätigen Sie dann die Auswahl mit Enter.

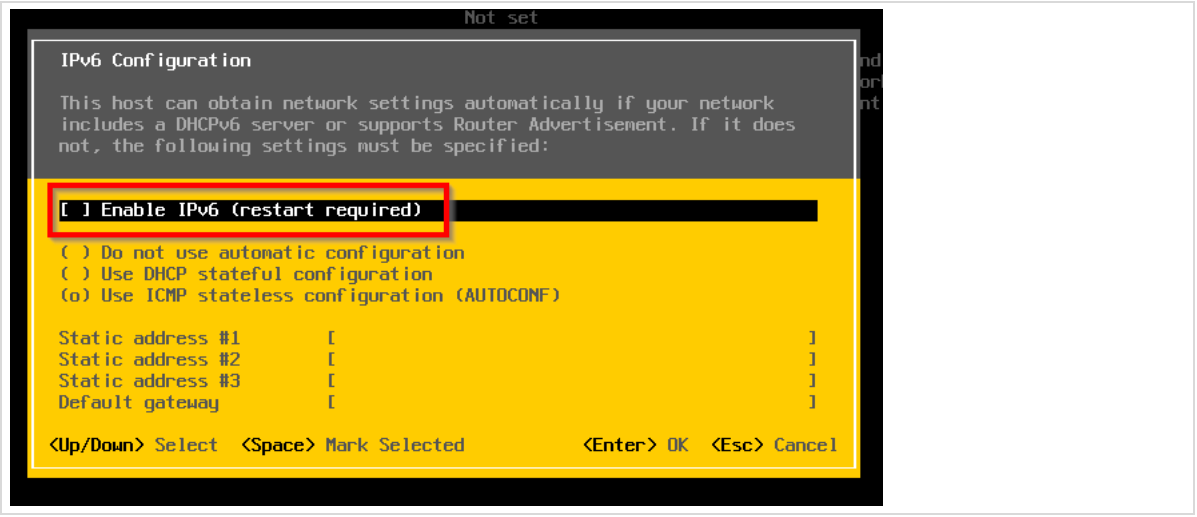

Abb. 22: Deaktivieren von IPv6: Kreuz entfernen

2.5.5 Konfigurieren von DNS und Hostname

Die Namensauflösung per DNS muss auf dem Virtualisierungs-Host unbedingt funktionieren, da davon weitere Dienste wie z.B. die Zeitsynchronisation aller virtuellen Maschinen abhängen!

Zurück im nachfolgend dargestellten Menü wählen Sie bitte per Pfeiltaste die Option „*DNS Configuration*“ aus. Bestätigen Sie die Auswahl mit Enter:

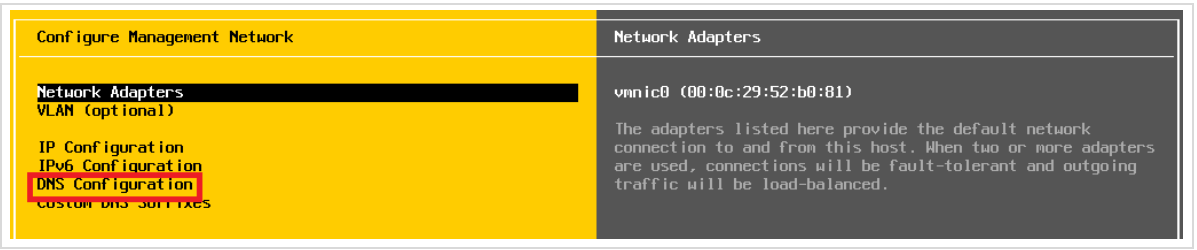

Abb. 23: Zur Konfiguration von DNS und Hostname

Wählen Sie die zweite Option („*Use the following DNS server addresses and hostname:*“) aus.

Tragen Sie zwei gültige DNS-Server ein. Die genauen Adressen hängen von der konkreten Netzkonfiguration in der Schule ab, denkbare DNS-Server sind:

- Die (interne) IP-Adresse ihres Internetzugangsrouters, falls auf diesem ein eigener DNS-Server läuft. Dies könnte z.B. *192.168.178.1* sein.
- Der DNS-Server, den Sie von ihrem Internetanbieter genannt bekommen. Im Falle eines BelWü-Zugangs ist dies dann z.B. *129.143.2.1* oder *129.143.2.4*.
- Einen öffentlich zugänglichen DNS-Server, z.B. die von Google betriebenen DNS-Server *8.8.8.8 und 8.8.4.4*.

Benennen Sie den Virtualisierungs-Host wie beispielhaft dargestellt. Bestätigen Sie mit Enter:

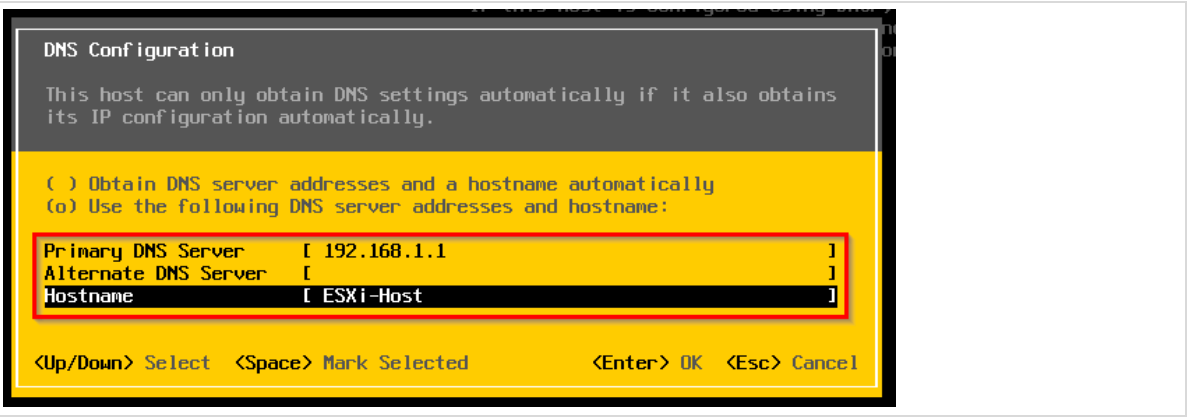

Abb. 24: Konfiguration von DNS und Hostname

2.5.6 Test der DNS-Namensauflösung

Melden Sie sich auf der Konsole des Virtualisierungs-Hosts (F2-Taste und anschließende Authentifizierung als Benutzer „*root*“) an und navigieren Sie mit den Pfeiltasten zum Punkt „*Test Management Network*“ und drücken Sie Enter.

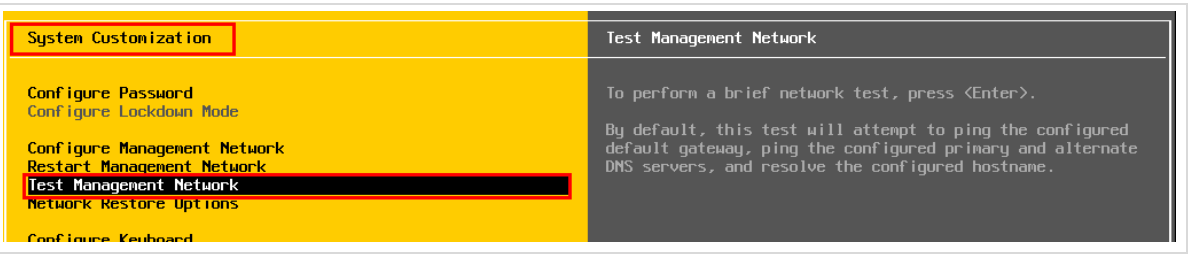

Abb. 25: Diagnosefunktionen des Hypervisors aufrufen

Mit der folgenden Maske können Sie IP-Adressen pingen und die DNS-Namensauflösung testen.

Tragen Sie einen externen Hostnamen in das letzte Feld ein (z.B. „www.heise.de“) und starten Sie den Test mit Klick auf Enter:

Eine erfolgreiche Namensauflösung wird mit „*OK*“ quittiert. Schlägt die Namensauflösung fehl (Meldung „*Failed*“), muss die Netzkonfiguration nochmals überprüft werden.

2.5.7 Test der Erreichbarkeit des Virtualisierungs-Hosts

Wenn die vorherigen Schritte korrekt ausgeführt worden sind, ist der Virtualisierungs-Host aus dem Netz „*INTERNET*“ zu erreichen.

- Schließen Sie für den Test den Management-PC an das Netz „*INTERNET*“ an.
- Vergeben Sie für diesen Rechner manuell eine IP-Adresse aus dem Netzbereich des Netzes „*INTERNET*“ (im obigen Beispiel z.B. *192.168.1.101*) und setzen Sie dessen Netzwerkmaske korrekt (im obigen Beispiel auf *255.255.255.0*).
- Öffnen Sie einen Browser auf dem Management-PC.
- Geben Sie in die Adresszeile des Browsers die IP-Adresse des Hypervisors ein (in unserem Beispiel https://192.168.1.100/ui). Je nach ESXi-Version kann die Adresse geringfügig abweichen.
- Klicken Sie danach auf „*ERWEITERT*“…

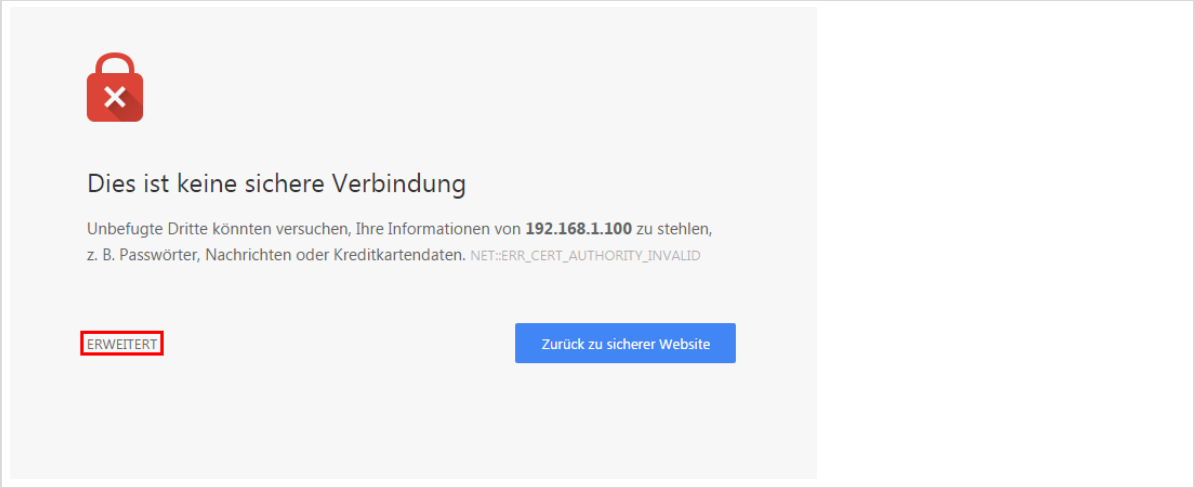

Abb. 26: Erweitert…

- …und bestätigen Sie die Weiterleitung zum *vSphere-Host-Client*:

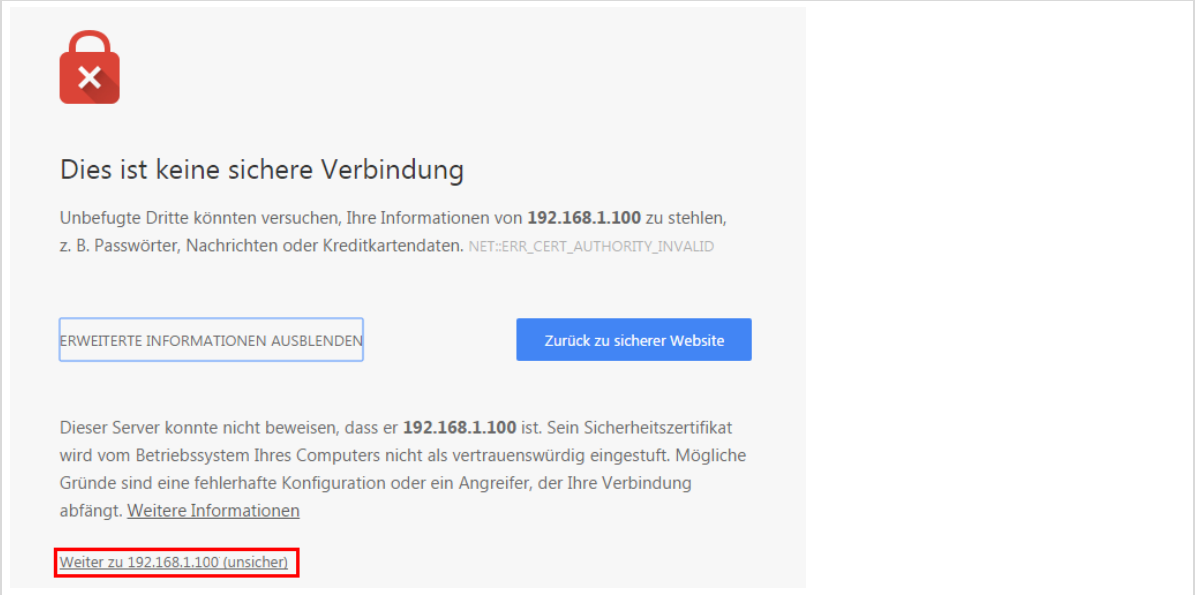

Abb. 27: Weiter zu… bestätigen

- Sie sollten nun dieses Bild sehen:

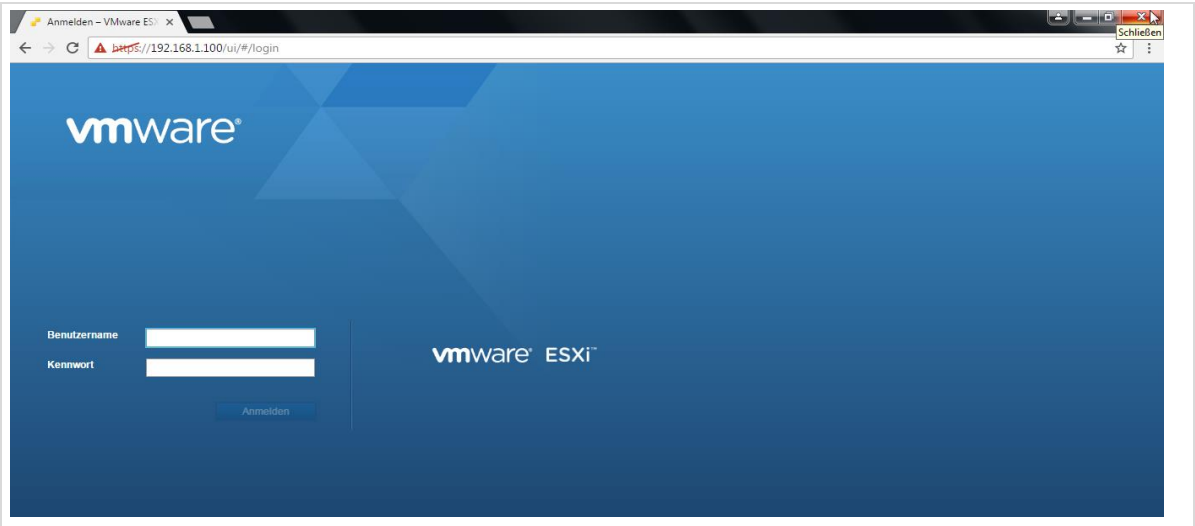

Abb. 28: Test des Zugriffs auf den Virtualisierungs-Host, IP-Adresse ist auf eigene Konfiguration anzupassen!

Wenn Sie diese Seite im Browser sehen, können Sie mit den nächsten Schritten fortfahren. Andernfalls muss die Netzwerkkonfiguration überprüft werden.

Beim ersten Login als *„root“* zeigt Ihnen der Server den Lizensierungsstatus *„60 Tage Testversion“* an, bestätigen Sie bitte durch Drücken auf *„OK“*: Damit ist der Zugriff vom *vmware-Host-Client* auf den Hypervisor eingerichtet.

2.5.8 Durchführen der Änderungen und Neustart des Virtualisierungs-Hosts

Verlassen Sie das Untermenü *„Configure Management Network“* durch Drücken von ESC. Im nachfolgenden Fenster werden Sie aufgefordert, die Änderungen am Virtualisierungs-Host zu bestätigen. Bestätigen Sie die Änderungen durch Drücken der Taste Y:

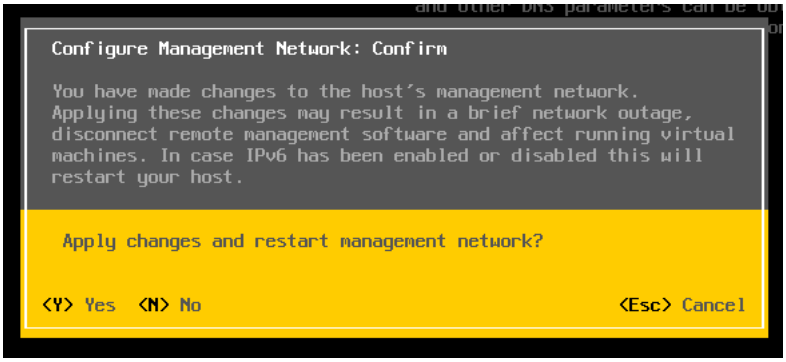

Abb. 29: Endgültige Bestätigung der Änderungen am „Management Network“

Im Anschluss wird ein Neustart des Virtualisierungs-Hosts durchgeführt:

Abb. 30: Neustart des Virtualisierungs-Hosts

Nach dem Neustart ist die Netzwerkkarte im Netz *„INTERNET“* für das Management des Virtualisierungs-Hosts eingerichtet. Auf der Startseite des Virtualisierungs-Hosts sollten die eben eingestellte IP-Adresse und der Hostname angezeigt werden:

Abb. 31: Startseite nach erfolgtem Reboot

2.6 Eingabe des Lizenzschlüssels

Als nächstes muss der Hypervisor lizenziert werden.

Klicken Sie im linken Menü auf *„Host“* (○) | *„Verwalten“* (○) und danach im rechten Fenster auf den Reiter „Lizenzierung“ (○). Klicken Sie dann auf *„Lizenz zuweisen“* (○).

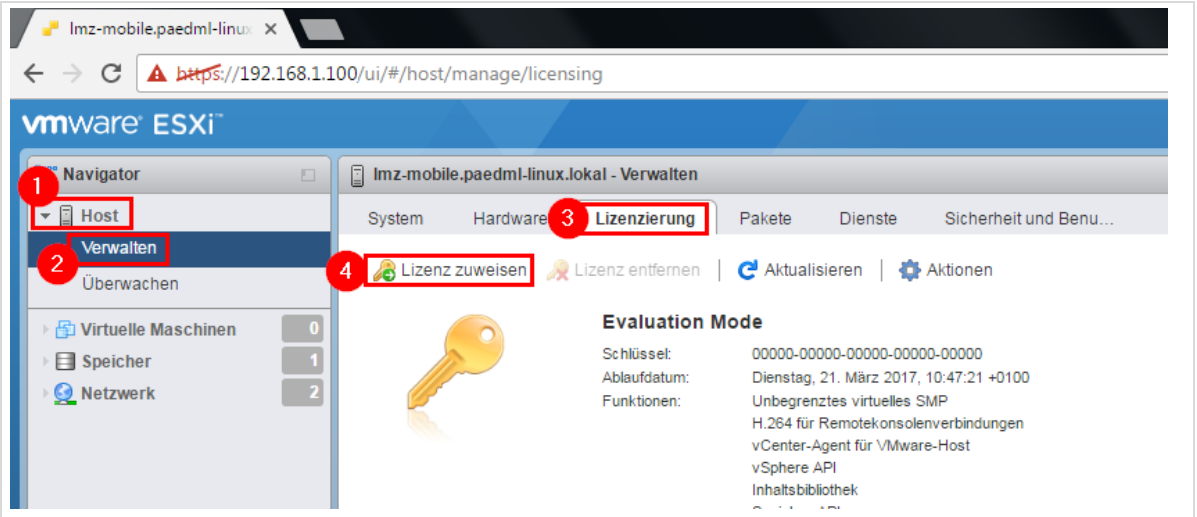

Abb. 32: Lizenz zuweisen

Geben Sie im darauffolgenden Fenster Ihren individuellen Lizenzschlüssel für den Hypervisor ein (○) und bestätigen Sie mit *„Lizenz zuweisen“* (○).

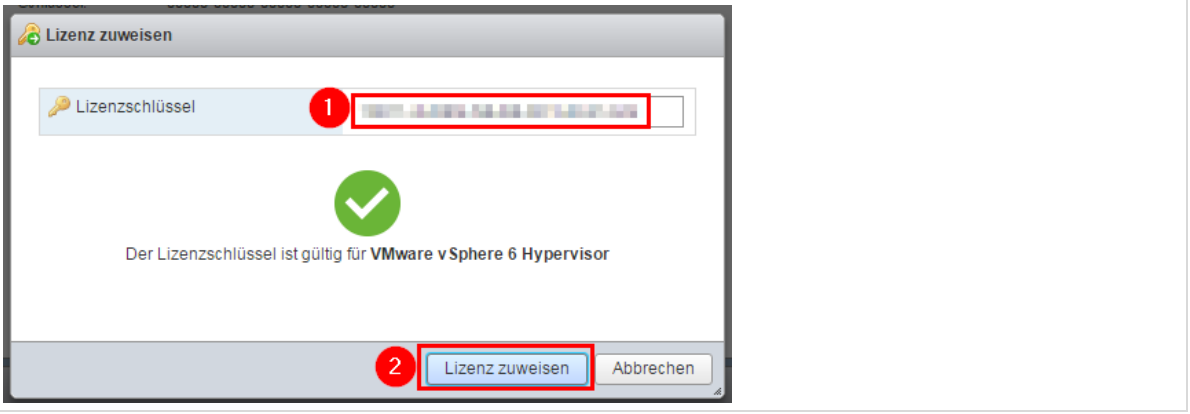

Abb. 33: Lizenzschlüssel eingeben

Der Lizensierungs-Status Ihres Virtualisierungs-Hosts sollte nun der folgenden Abbildung entsprechen. Eine erfolgreiche Eingabe des Lizenzschlüssels wird mit dem Eintrag *„Ablaufdatum: Nie“* im Informationstext des Reiters *„Lizenzierung“* angezeigt.

Abb. 34: Lizenzschlüssel wurde korrekt eingetragen

2.7 Zeitsynchronisation des Hypervisors

Im Folgenden wird der Hypervisor so eingerichtet, dass er die Uhrzeit stets mit Zeitservern im Internet per NTP („Network Time Protocol“) abgleicht. Dies ist notwendig, damit die virtuellen Maschinen ihrerseits die korrekte BIOS-Uhrzeit erhalten.

Die Zeitsynchronisation funktioniert nur, wenn das Management-Netz des Hypervisors Internetzugriff hat und die Namensauflösung funktioniert!

Klicken Sie im linken Menü auf *„Host“* (○) | *„Verwalten“* (○) und danach im rechten Fenster auf den Reiter *„System“* (○). Klicken Sie dann auf *„Uhrzeit und Datum“* (○) | *„Einstellungen bearbeiten“* (○).

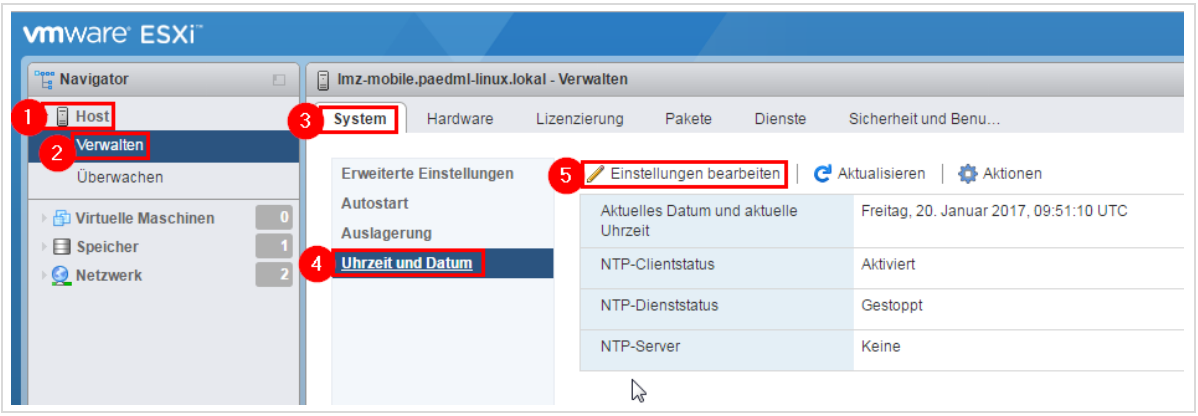

Abb. 35: Ändern der Uhrzeitkonfiguration

Aktivieren Sie den NTP-Client (○), setzen Sie bei „Startrichtlinie für NTP-Dienst“ den Wert *„Mit dem Host starten und beenden“* (○) und nehmen Sie unter NTP-Server folgende Eintragungen durch Kommas getrennt vor (○):

```
0.de.pool.ntp.org, 1.de.pool.ntp.org, 2.de.pool.ntp.org, 3.de.pool.ntp.org
```

Bestätigen Sie mit *„Speichern“* (○).

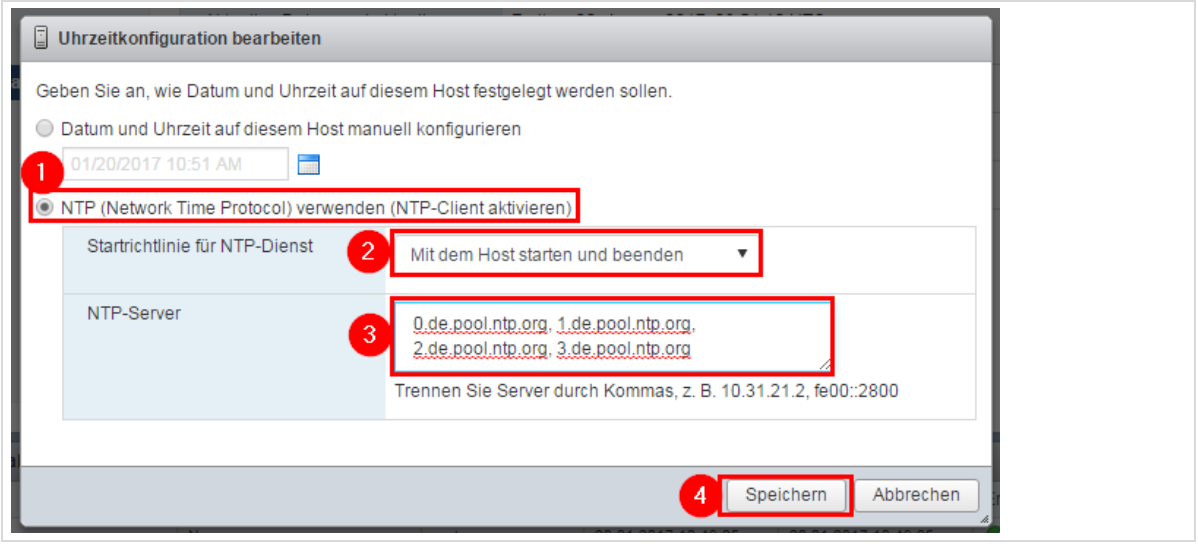

Abb. 36: NTP Client aktivieren, NTP-Server eintragen

Im vmware-Host-Clientsollten Sie nun die folgende Situation vorfinden:

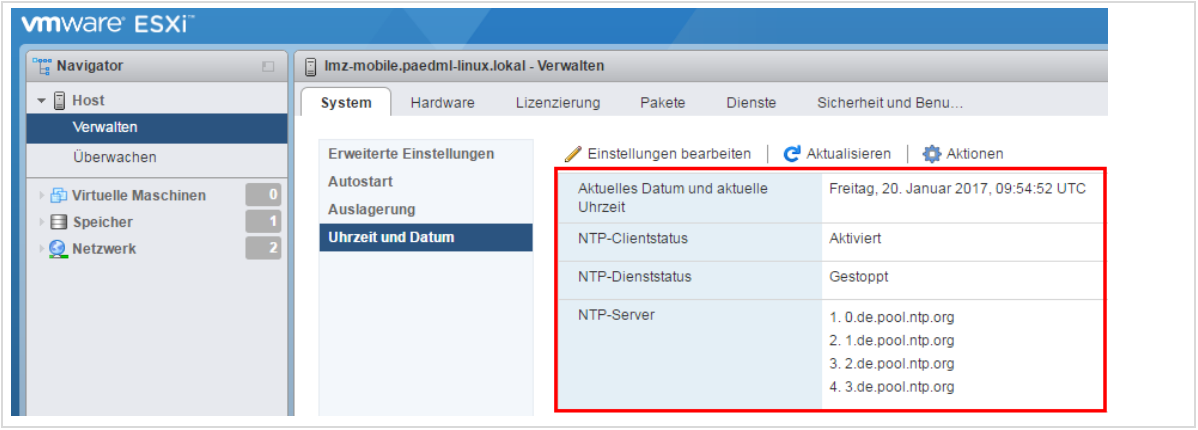

Abb. 37: Der NTP-Client ist erfolgreich eingerichtet

3 Konfiguration der virtuellen Netzwerke

3.1 Definition virtuelles Netzwerk „INTERNET“

Öffnen Sie den *vmware-Host-Client* über die IP-Adresse des ESXi-Hosts in einem Browser. Klicken Sie im linken Menü auf *„Netzwerk“* (○) | *„VM Network“* (○) und danach im rechten Fenster auf den Eintrag *„Aktionen“* (○). Klicken Sie dann auf *„Entfernen“* (○).

Bitte entfernen Sie auf keinen Fall das „Management Netzwerk“!

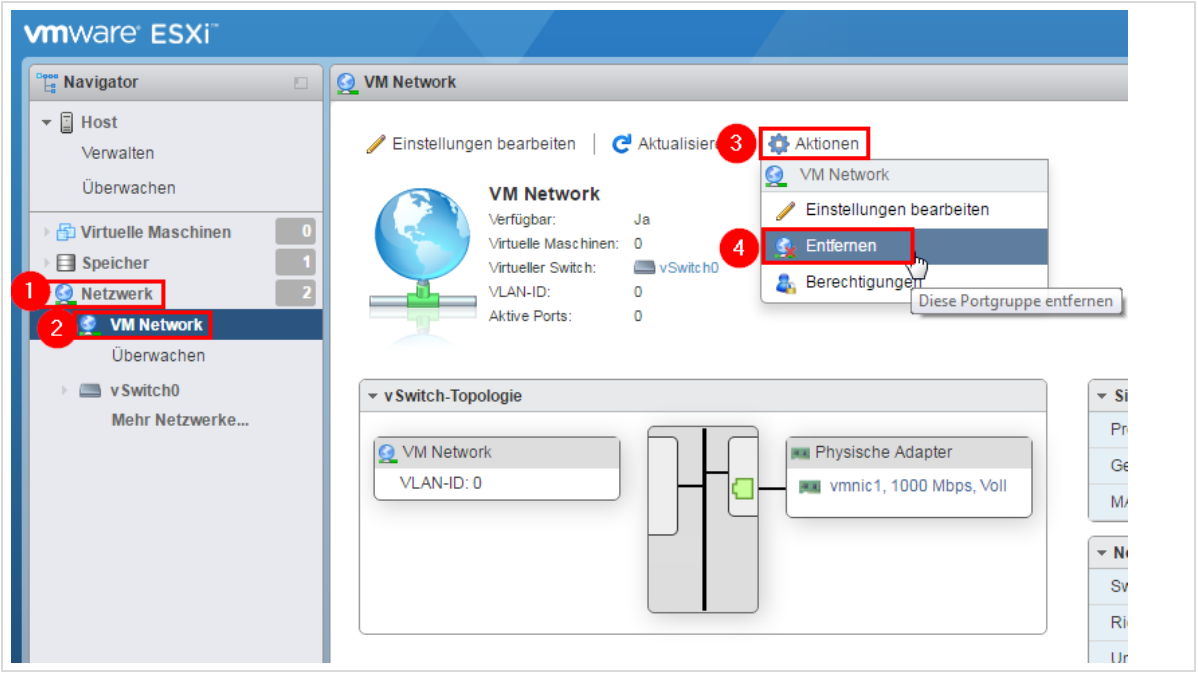

Abb. 38: VM Network entfernen

Bestätigen Sie im folgenden Fenster das Entfernen der Portgruppe *„VM Network“*.

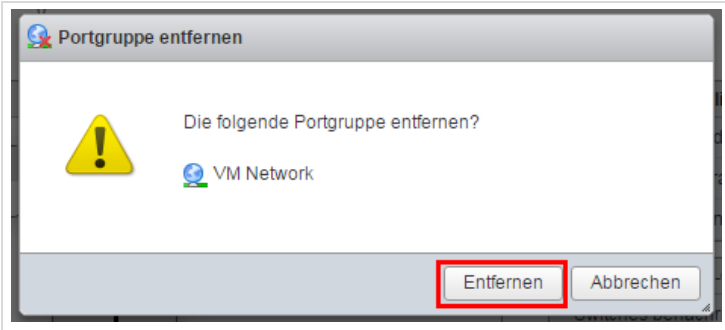

Abb. 39: Bestätigen: Entfernen der Portgruppe

Nun wird das virtuelle Netzwerk „INTERNET“ hinzugefügt. Klicken Sie dazu im linken Menü auf *„Netzwerk“* (○) und danach im rechten Fenster auf den Eintrag *„Portgruppe hinzufügen“* (○). Geben Sie im sich öffnenden Fenster als Name *„INTERNET“* (○) ein und bestätigen Sie mit *„Hinzufügen“* (○).

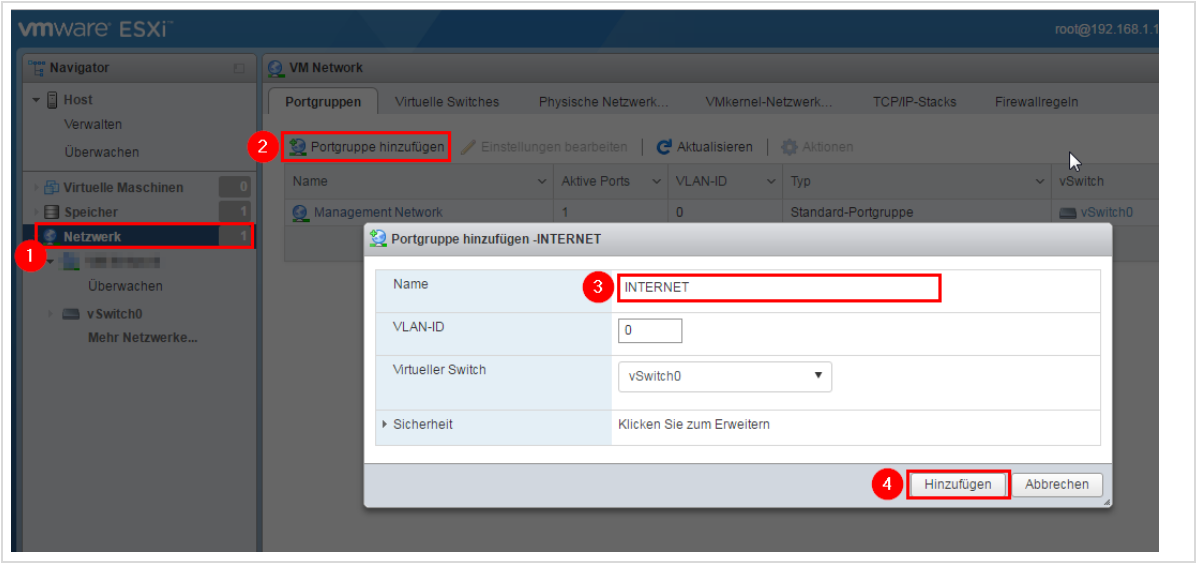

Abb. 40: Portgruppe „INTERNET“ hinzufügen

3.2 Definition virtuelles Netzwerk „PAEDAGOGIK“

Zunächst muss ein virtueller Switch namens „PAEDAGOGIK“ hinzugefügt werden. Klicken Sie dazu im linken Menü auf *„Netzwerk“* (○) und danach im rechten Fenster auf den Reiter *„Virtuelle Switche“* (○). Klicken Sie dann auf *„Virtuellen Standard-Switch hinzufügen“* (○).

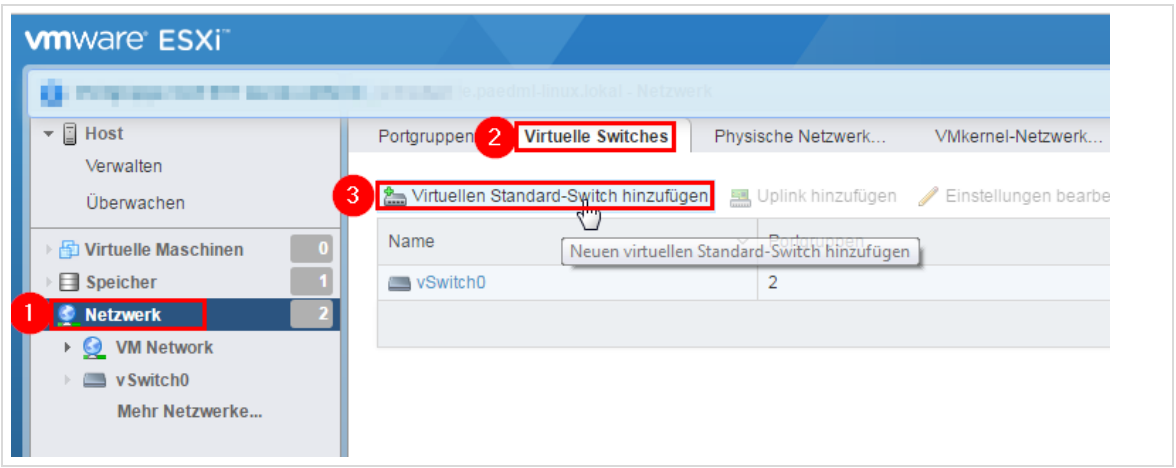

Abb. 41: Virtuellen Switch hinzufügen

Im folgenden Fenster geben Sie als vSwitch-Name *„PAEDAGOGIK“* (○) ein, wählen bei Uplink 1 *„vmnic1“* aus (○) und bestätigen Sie mit *„Hinzufügen“* (○).

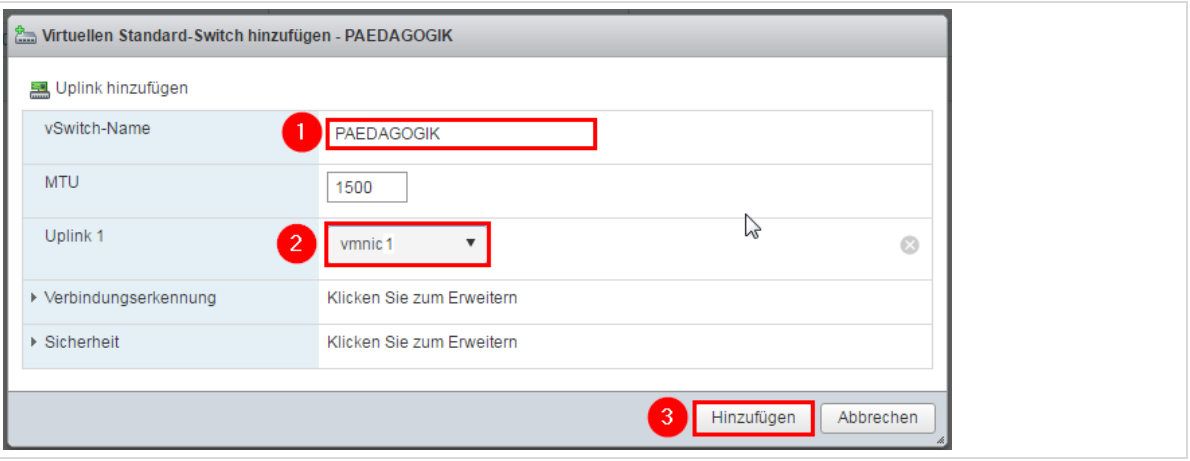

Abb. 42: Virtuellen Switch „PAEDAGOGIK“ hinzufügen

Klicken Sie nun im linken Menü auf *„Netzwerk“* (○) und danach im rechten Fenster auf den Eintrag *„Portgruppe hinzufügen“* (○). Geben Sie im sich öffnenden Fenster als Name *„PAEDAGOGIK“* (○) ein, wählen den virtuellen Switch „PAEDAGOGIK“ aus (○) und bestätigen Sie mit *„Hinzufügen“* (○).

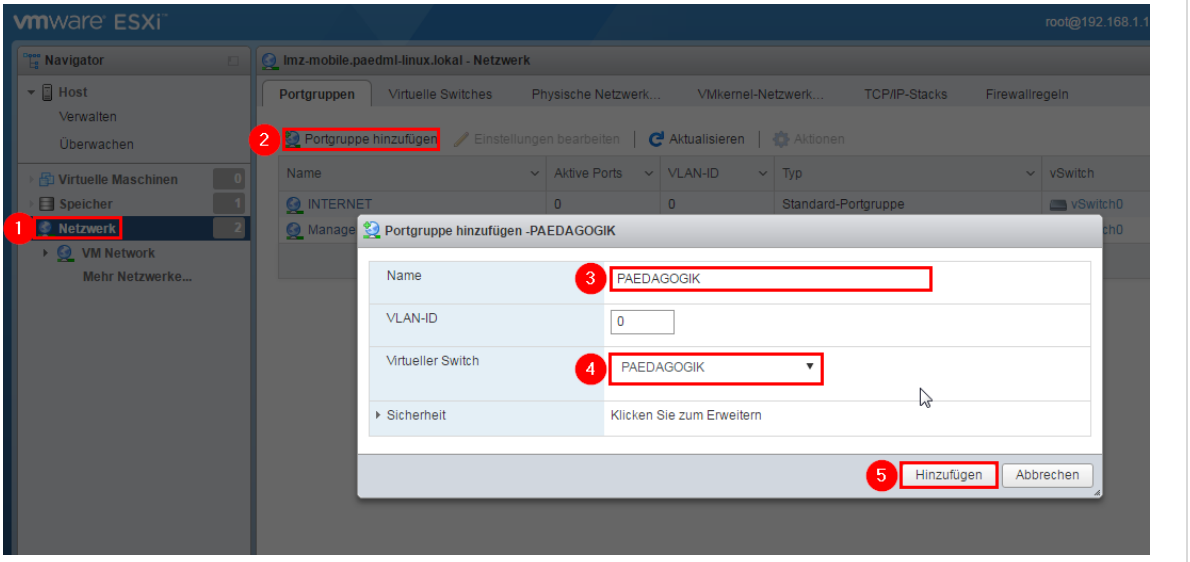

Abb. 43: Portgruppe „PAEDAGOGIK“ hinzufügen

3.3 Definition virtuelles Netzwerk „GAESTE“

Zunächst muss ein virtueller Switch namens *„GAESTE“* hinzugefügt werden. Klicken Sie dazu im linken Menü auf *„Netzwerk“* (○) und danach im rechten Fenster auf den Reiter *„Virtuelle Switche“* (○). Klicken Sie dann auf *„Virtuellen Standard-Switch hinzufügen“* (○).

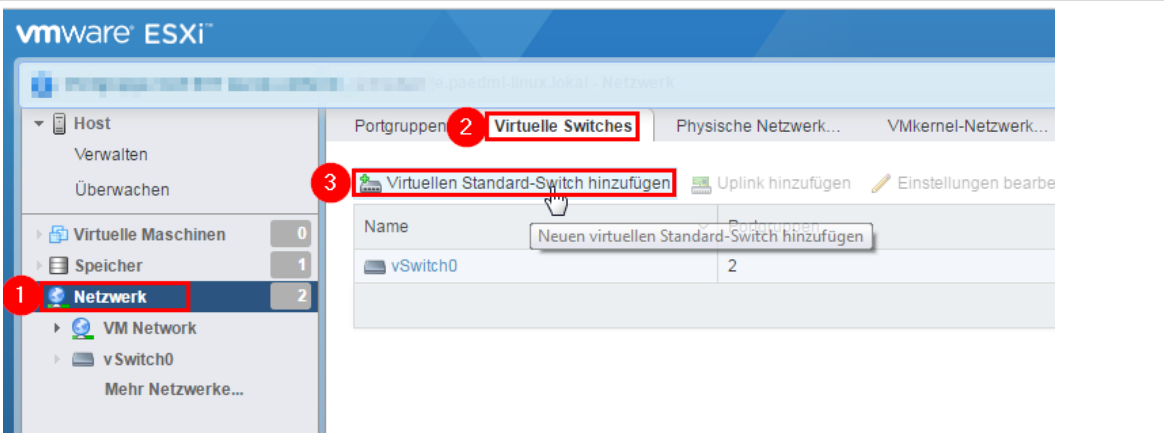

Abb. 44: Virtuellen Switch hinzufügen

Im folgenden Fenster geben Sie als vSwitch-Name *„GAESTE“* (○) ein, wählen bei Uplink 1 *„vmnic2“* aus (○) und bestätigen Sie mit *„Hinzufügen“* (○).

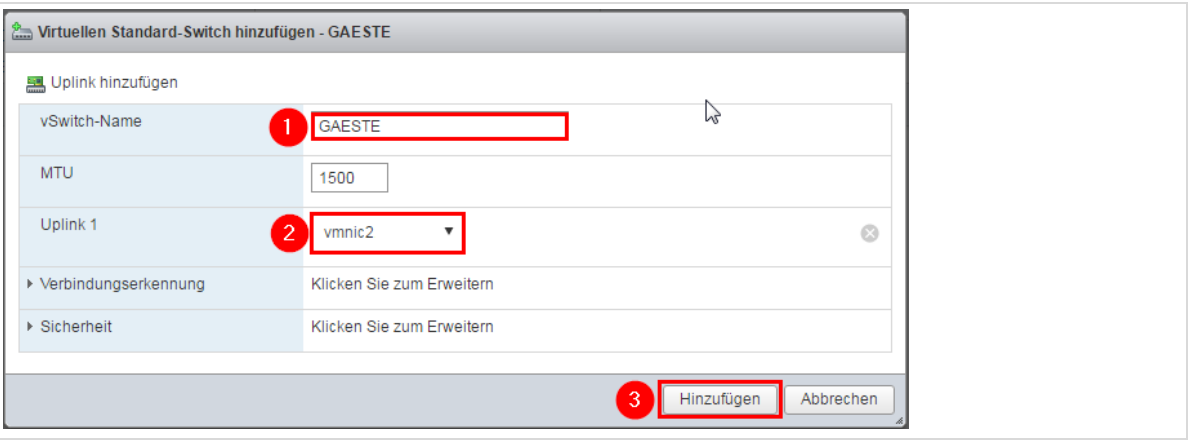

Abb. 45: Virtuellen Switch „GAESTE“ hinzufügen

Klicken Sie nun im linken Menü auf *„Netzwerk“* (○) und danach im rechten Fenster auf den Eintrag *„Portgruppe hinzufügen“* (○). Geben Sie im sich öffnenden Fenster als Name *„GAESTE“* (○) ein, wählen den virtuellen Switch *„GAESTE“* aus (○) und bestätigen Sie mit *„Hinzufügen“* (○).

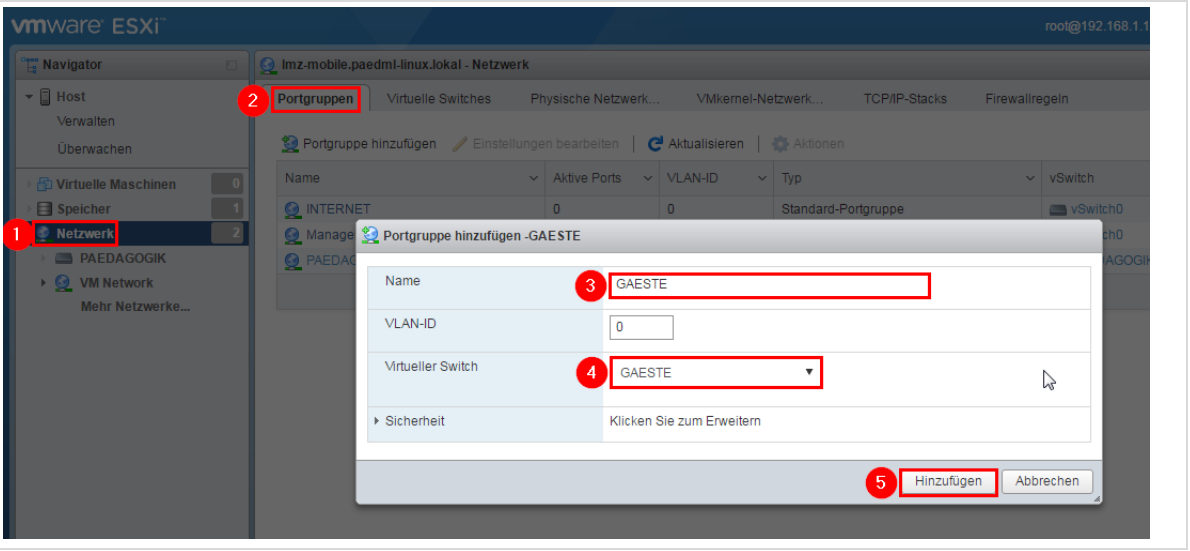

Abb. 46: Portgruppe „GAESTE“ hinzufügen

3.4 Überprüfen der virtuellen Netze

Sie sollten auf dem Virtualisierungs-Host nun die nachstehend abgebildeten virtuellen Netzwerke „*INTERNET*“, „*PAEDAGOGIK*“ und „*GAESTE*“ vorfinden.

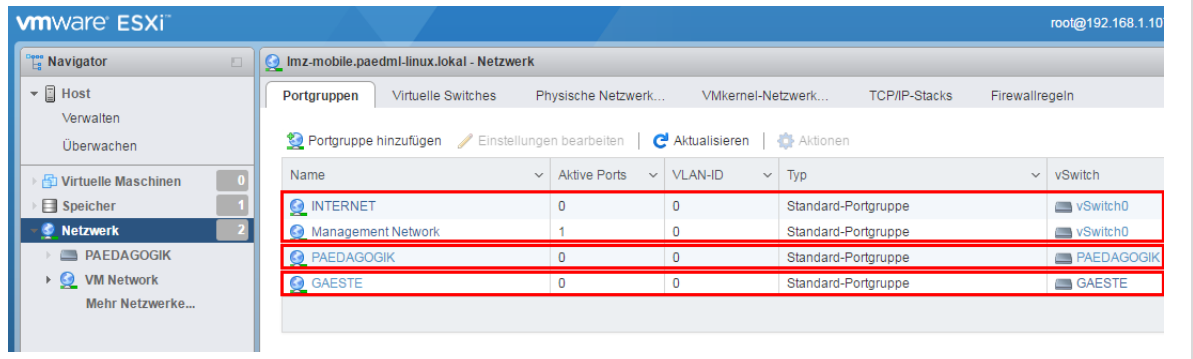

Abb. 47: Übersicht der auf dem Virtualisierungs-Host eingerichteten Netze

virtuelles Netz	Bedeutung	Physischer Adapter
„INTERNET“	Verbindung der Firewall zum Internet-Router (DSL, BelWü etc.), Zugriff auf Hypervisor („Management Network“)	vmnic0
„PAEDAGOGIK“	Verbindung zum pädagogischen Netz	vmnic1
„GAESTE“	Verbindung zum Netz für Gäste-Rechner	vmnic2

Tabelle 3: Zuordnung der virtuellen Netze zu physischen Adaptern

3.5 Definition optionales virtuelles Netz „DMZ“ (für Nextcloud)

Zunächst wird ein weiterer ***virtueller Switch*** (vSwitch) erstellt. Navigieren Sie dazu im Bereich Navigator zu Netzwerk.

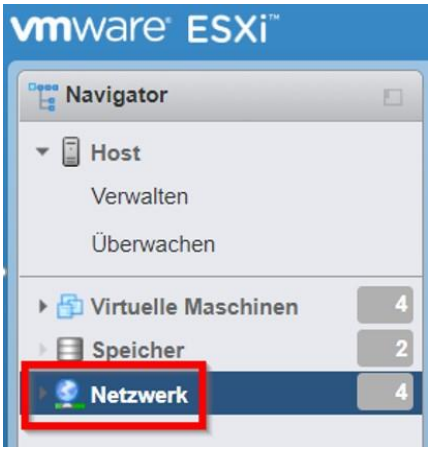

Abb. 48: Öffnen der Netzwerk-Einstellungen

Wechseln Sie in den Reiter ***Virtuelle Switches*** und fügen Sie einen neuen virtuellen Switch hinzu.

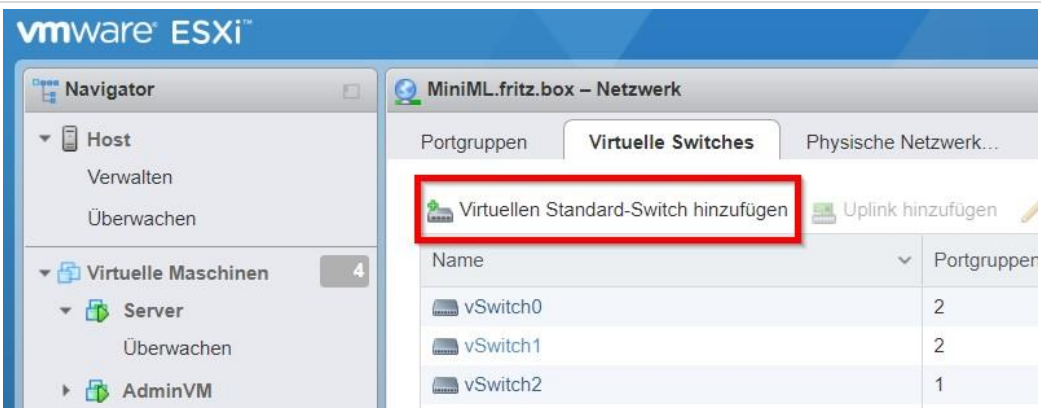

Abb. 49: vSwitch hinzufügen

Im folgenden Dialog sollte der Switch logisch benannt werden, geben Sie bei vSwitch-Name ***„vSwitch3“*** (❶) ***ein***. Durch ***„Hinzufügen“*** wird die Einstellung gespeichert (❷).

Abb. 50: Benennung des vSwitch

Jetzt wird ein weiteres Netz ***„DMZ“*** eingerichtet. In diesem befindet sich später die neue virtuelle Maschine (VM) ***Nextcloud.*** Navigieren Sie dazu zum Reiter ***Netzwerk*** (❶) und fügen Sie eine neue Portgruppe hinzu (❷).

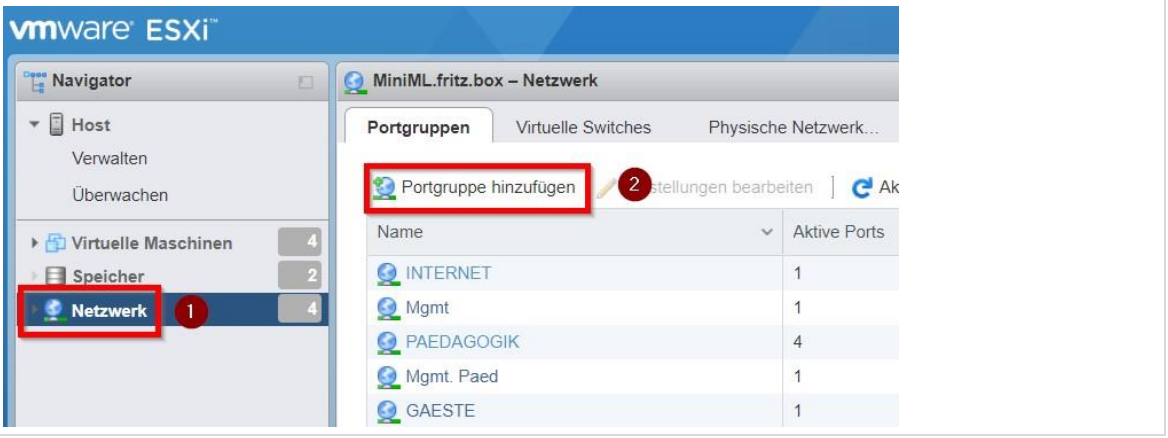

Abb. 51: Portgruppe hinzufügen 1

Bennen Sie die Portgruppe als ***„DMZ“*** (❶) und ordnen Sie den neu angelegten virtuellen Switch zu (❷).

Durch ***„Hinzufügen“*** (❸) wird die neue Portgruppe angelegt.

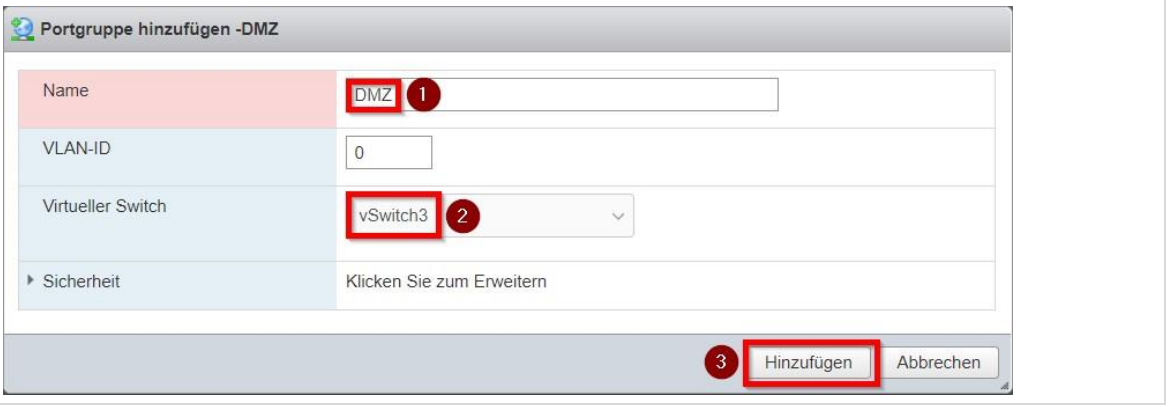

Abb. 52: Portgruppe hinzufügen 2

Damit ist das neue Netzsegment ***DMZ*** erstellt und einem Virtuellen Switch zugewiesen.

3.6 Definition optionales virtuelles Netz „MDM“

Melden Sie sich an Ihrem ESXi-Host mit dem Benutzer *root* an.

Fahren Sie die virtuellen Maschinen W10AdminVM; opsi-Server, Server und Firewall in dieser Reihenfolge herunter.

Klicken Sie auf den Reiter *Netzwerk* und wechseln Sie in den Reiter *Virtuelle Switches*. Klicken Sie auf *Virtuellen Standard-Switch hinzufügen*.

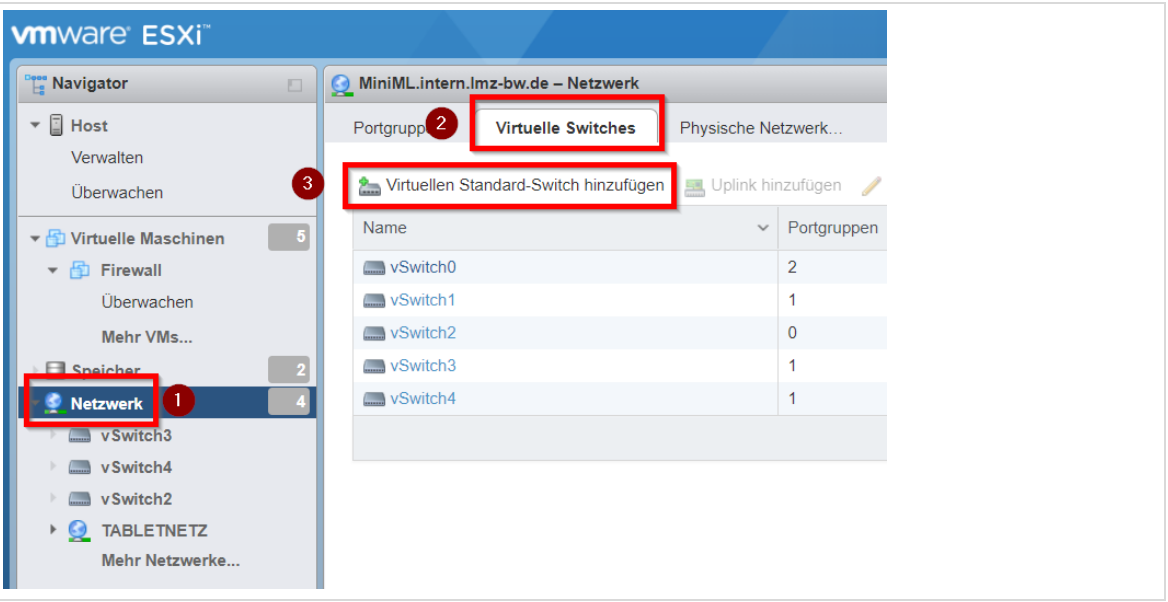

Abb. 53: Virtuellen Switch hinzufügen

Vergeben Sie einen Namen für den neuen virtuellen Switch, ordnen Sie einen freien physischen Adapter zu und klicken Sie auf *Hinzufügen*.

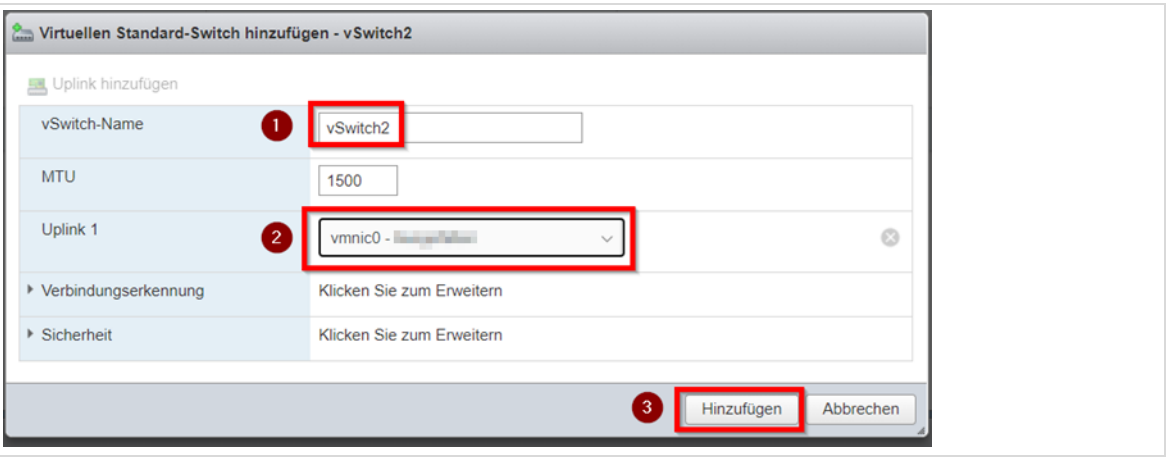

Abb. 54: Neuer Virtueller Switch

Der neu angelegte virtuelle Switch erscheint nun in der Übersicht.

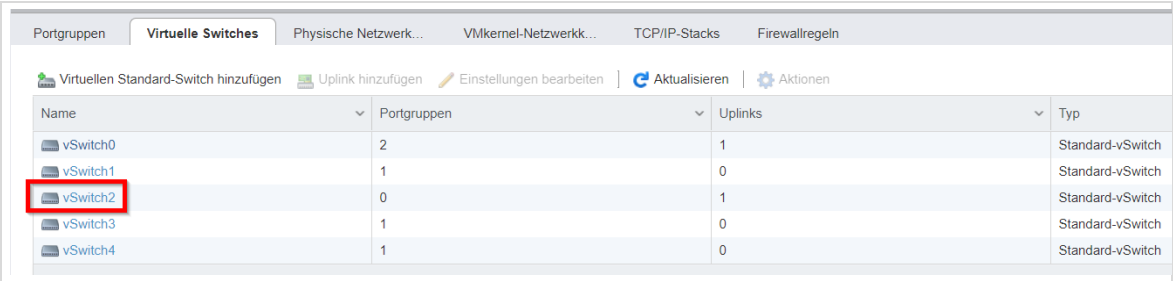

Abb. 55: Neuer virtueller Switch erfolgreich hinzugefügt

Wechseln Sie in den Reiter *Portgruppen* und gehen Sie dort auf *Portgruppe hinzufügen*.

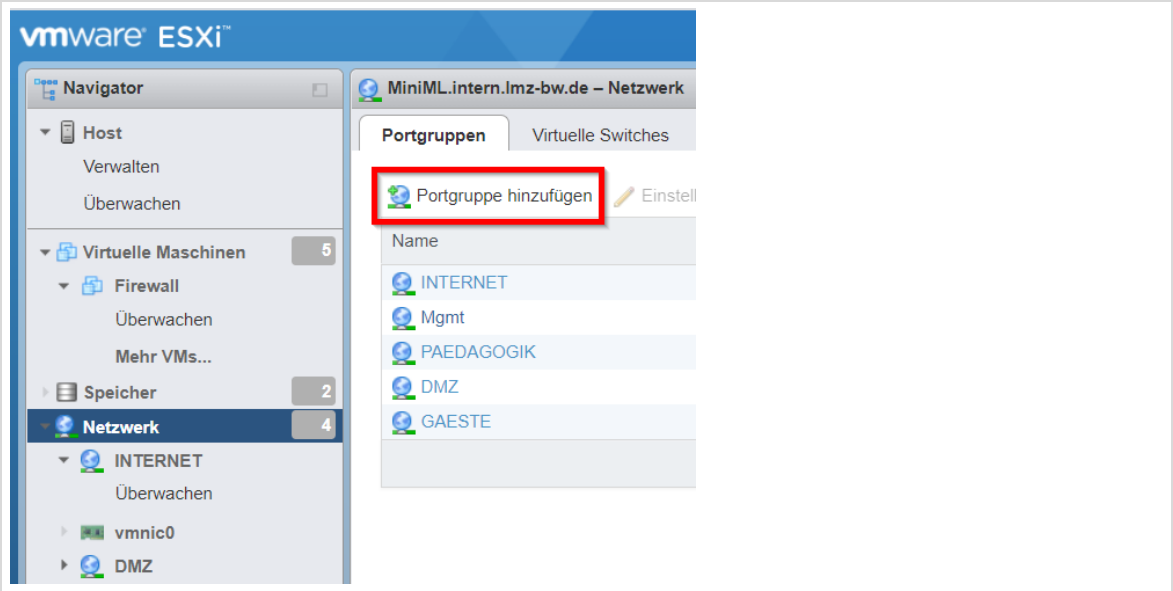

Abb. 56: Portgruppe hinzufügen

Vergeben Sie den Namen *MDM* und ordnen Sie den zuvor neu erstellten virtuellen Switch zu. Klicken Sie dann auf *Hinzufügen*.

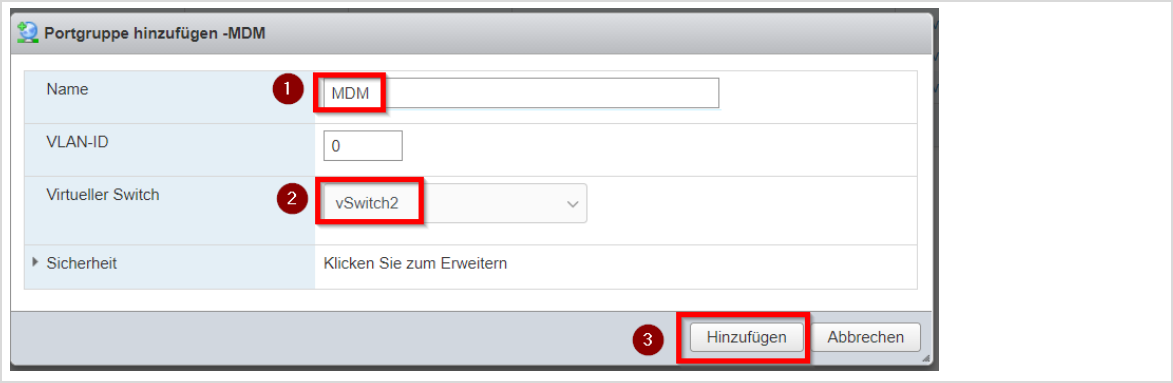

Abb. Portgruppe konfigurieren

Die neue Portgruppe erscheint in der Übersicht.

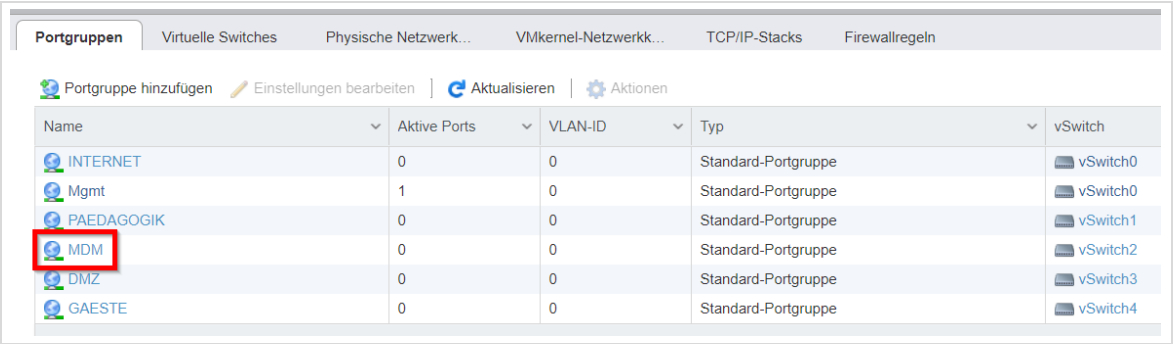

Abb. 57: Portgruppe Übersicht.

4 Import der virtuellen Maschinen

Im Verlauf des Imports kann bezüglich des Festplattenplatzes zwischen „Thin-Provisioning“ und „Thick-Provisioning“ gewählt werden.

„Thick-Provisioning“ stellt der VM den gesamten Festplattenplatz sofort zur Verfügung, dies ist zwar nicht plattenplatzsparend Sie werden dadurch aber keine Probleme wegen plötzlich voller Server-Festplatten haben, daher ist dies für eine Standardinstallation die bessere Wahl.

Wenn Sie mit mehreren Instanzen oder Testumgebungen arbeiten möchten, empfehlen wir Ihnen eine „Thin-Provisioned“ Festplatte. Die virtuellen Maschinen brauchen dann nur so viel Festplattenplatz auf dem Server, wie notwendig und sind dadurch in der Regel kleiner. Sobald die VM jedoch mehr Platz einfordert, muss der benötigte Festplattenplatz aber frei sein. Wäre dies nicht der Fall kann es zu Abstürzen oder Performance-Einbrüchen kommen.

4.1 Import der VM „Firewall“

Öffnen Sie den *vmware-Host-Client* über die IP-Adresse des ESXi-Hosts in einem Browser. Klicken Sie dann im linken Menü des *vmware-Host-Client* auf *„Virtuelle Maschinen“* (○) und danach im rechten Fenster auf den Eintrag *„VM erstellen/registrieren“* (○).

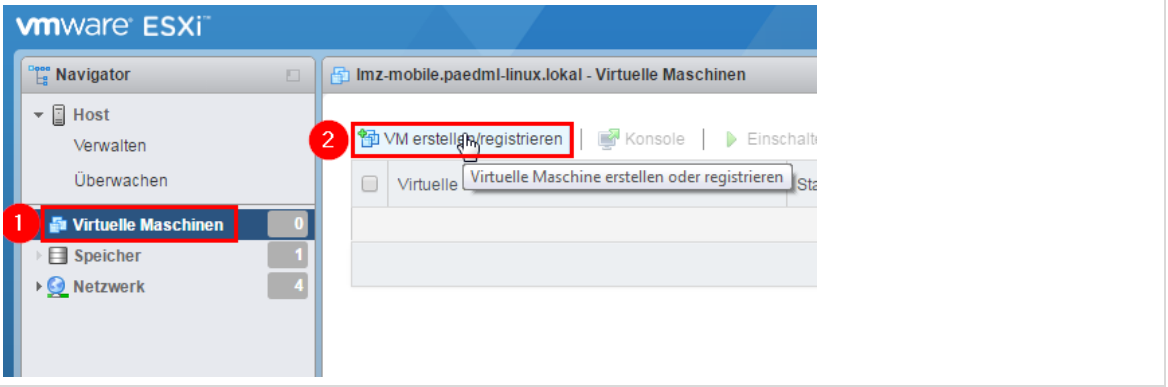

Abb. 58: Virtuelle Maschine erstellen

Wählen Sie im folgenden Fenster *„Eine virtuelle Maschine aus einer OVF- oder OVA-Datei..“* aus (❶) und gehen Sie mit „Weiter“ zum nächsten Schritt (❷):

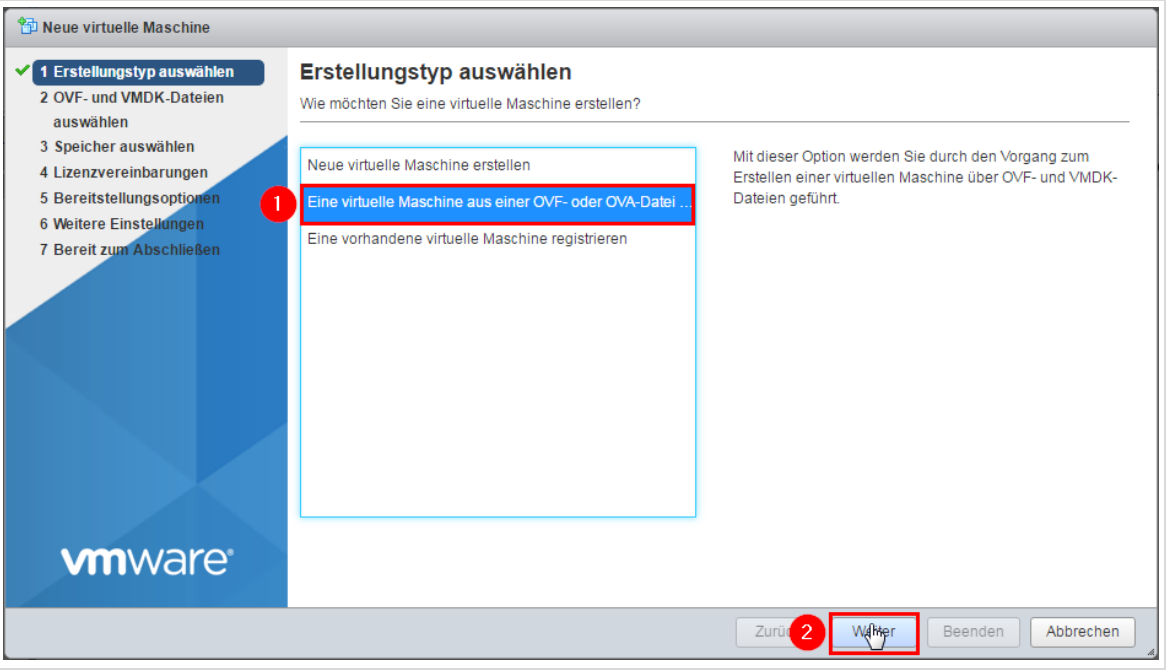

Abb. 59: Import eines OVA-Images

Geben Sie als Namen für die virtuelle Maschine „Firewall“ ein (❶) und klicken Sie in den Bereich darunter (❷), um die später zu importierenden Dateien auszuwählen. Sie können hier auch mit *„Ziehen und Ablegen“ („Drag and Drop“)* arbeiten.

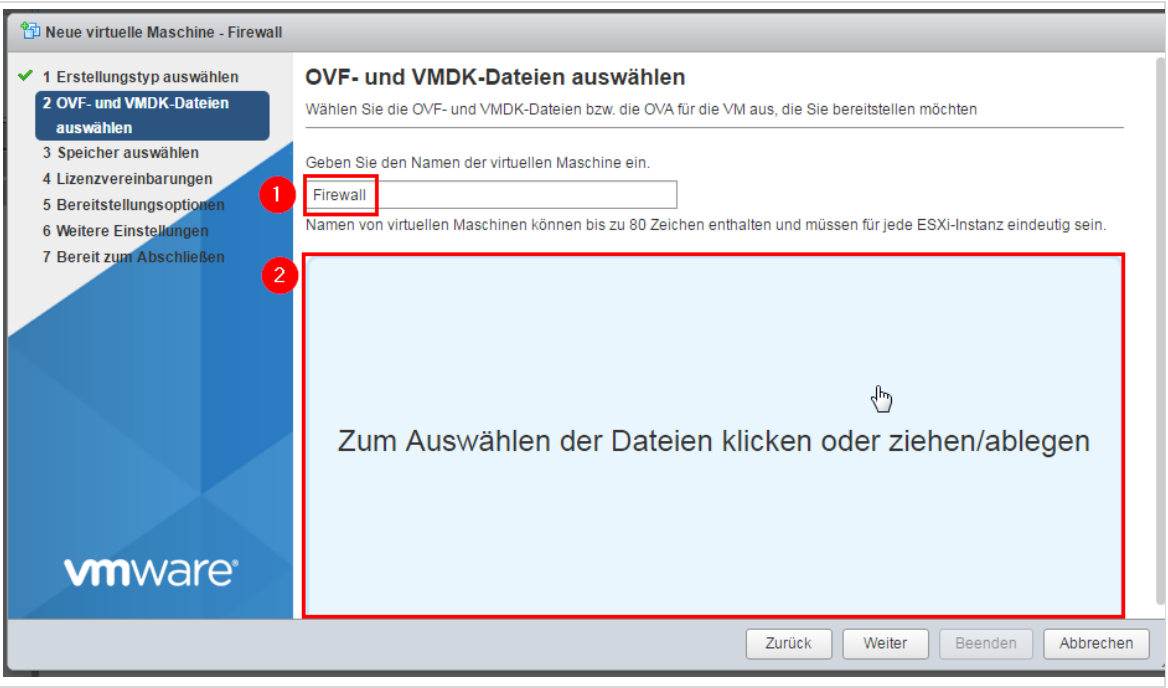

Abb. 60: OVA-Datei für die VM „Firewall“ auswählen

Wählen Sie das OVA-Image der Firewall aus (❶) und klicken Sie auf „*Öffnen*“ (❷):

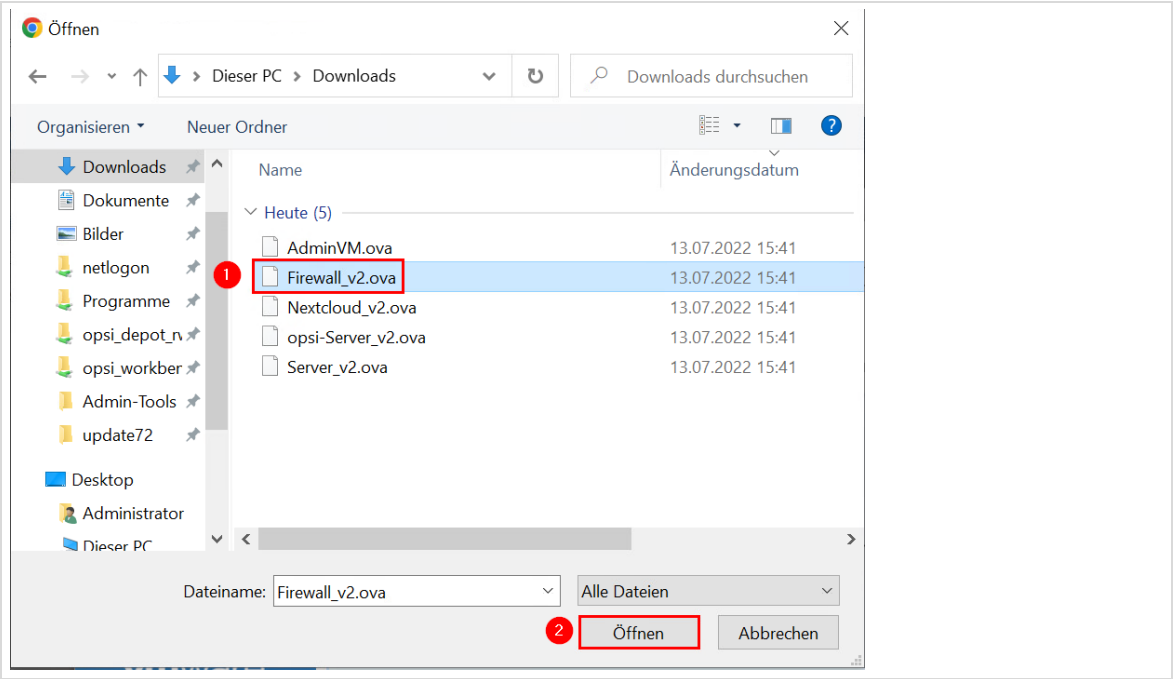

Abb. 61: Auswahl der OVA-Datei

Überprüfen Sie nochmals alle Angaben und klicken Sie auf „*Weiter*“:

Abb. 62: Alle Angaben sind korrekt.

Im nächsten Dialog müssen Sie denjenigen Datastore auswählen, auf dem die virtuelle Maschine gespeichert werden soll (❶). Bestätigen Sie anschließend mit „*Weiter*“ (❷).

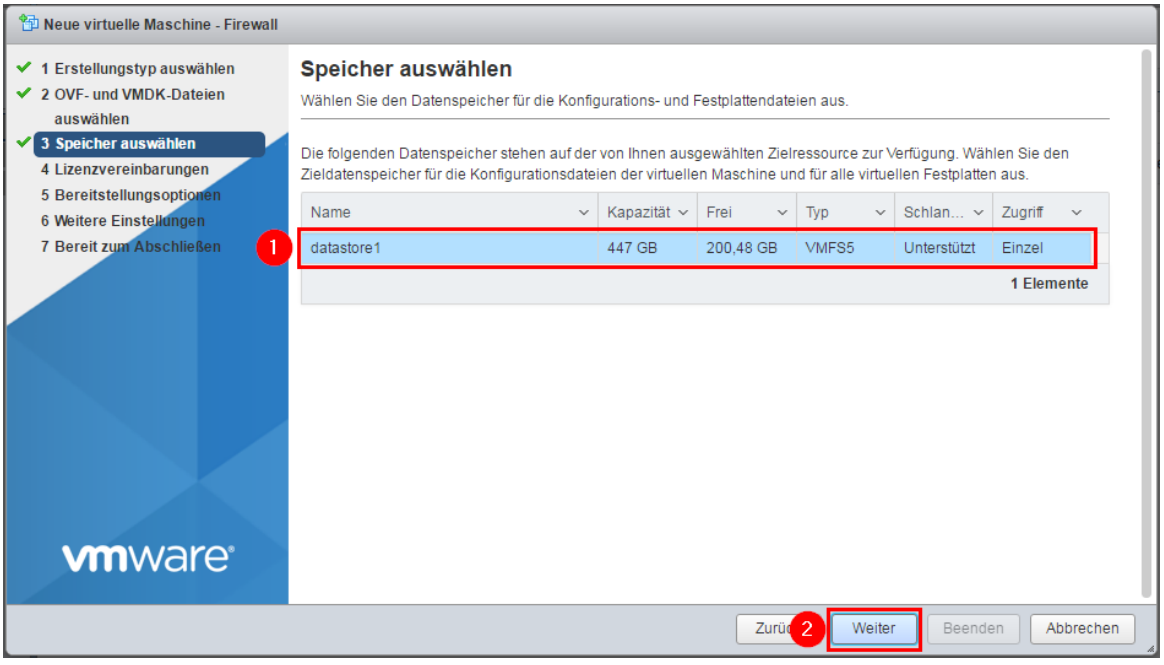

Abb. 63: Auswahl des Datastores

Im nachfolgenden Dialog werden das Festplattenformat und die Netzwerkzuordnungen der virtuellen Maschine festgelegt. Ordnen Sie die Netzwerke wie in der Abbildung (❶) zu, wählen Sie die Option „*Thick*“ aus (❷) und bestätigen Sie mit „*Weiter*“ (❸):

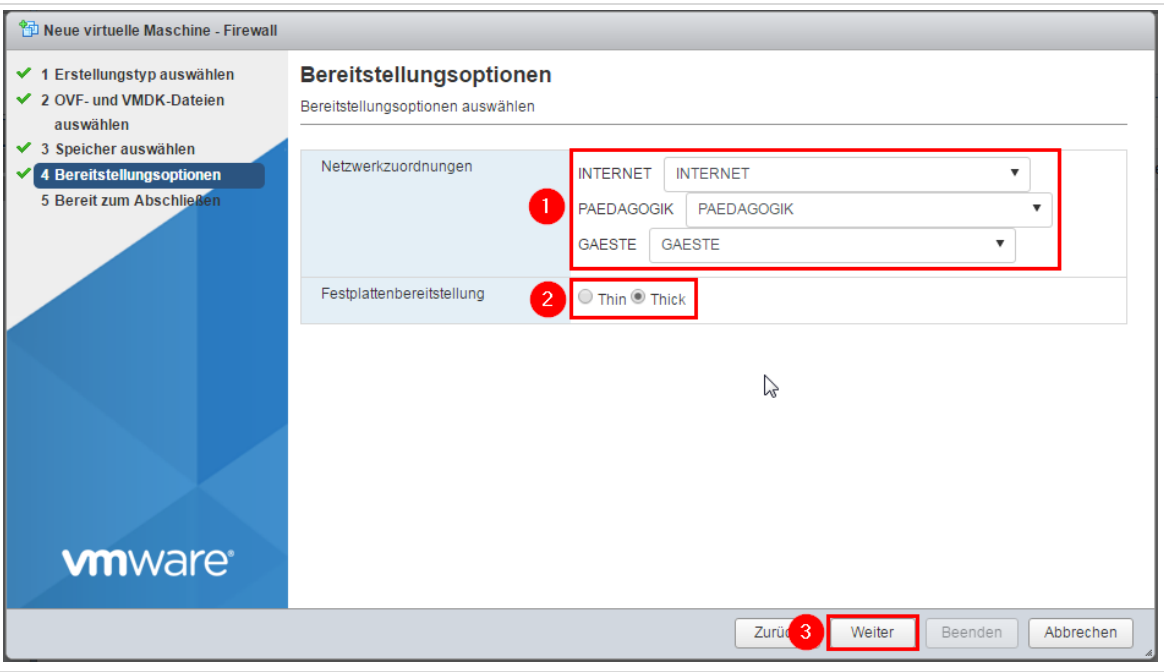

Abb. 64: Netzwerkzuordnungen und Auswahl des Festplattenformats „Thick“

Nachfolgend werden nochmals alle Einstellungen angezeigt. Kontrollieren Sie diese Einstellungen und bestätigen Sie den Dialog mit „*Beenden*“.

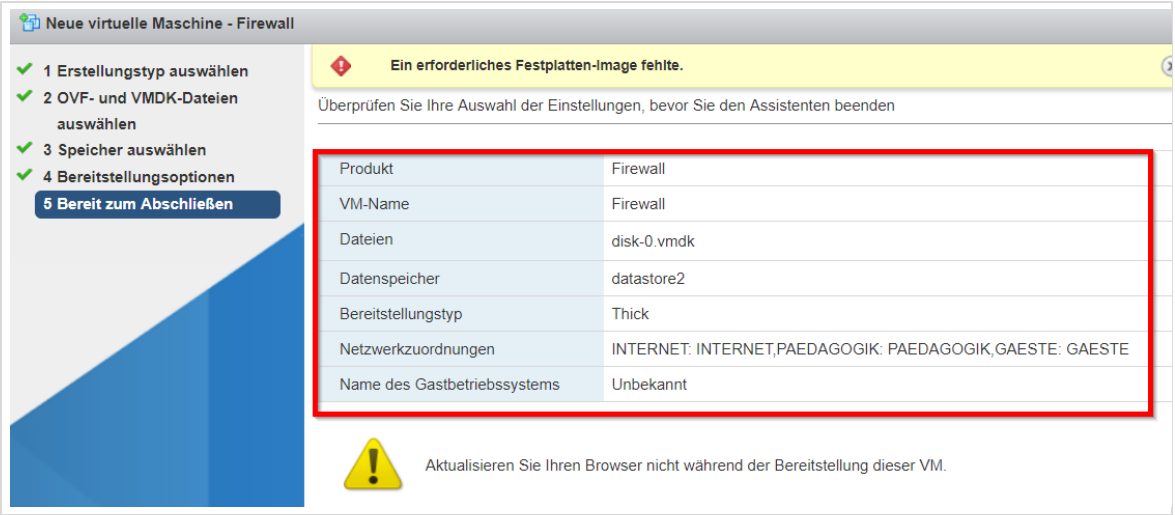

Abb. 65: Letzte Kontrolle der Einstellungen vor dem tatsächlichen Importvorgang

Nun beginnt der eigentliche Import der VM, dies kann je nach Systemleistung und Imagegröße einige Zeit in Anspruch nehmen.

4.2 Import der VM „Server“

Öffnen Sie den *vmware-Host-Client* über die IP-Adresse des ESXi-Hosts in einem Browser. Klicken Sie dann im linken Menü des *vmware-Host-Client* auf *„Virtuelle Maschinen“* (❶) und danach im rechten Fenster auf den Eintrag *„VM erstellen/registrieren“* (❷).

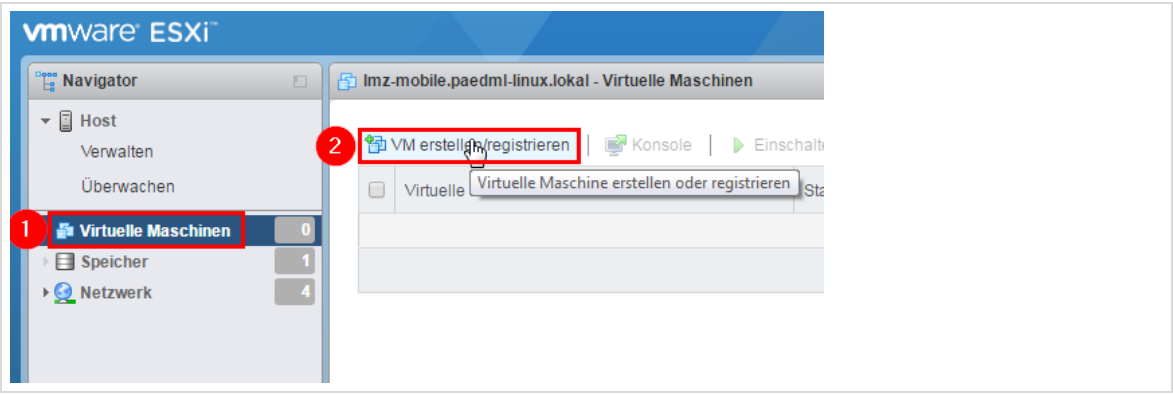

Abb. 66: Virtuelle Maschine erstellen

Wählen Sie im folgenden Fenster *„Eine virtuelle Maschine aus einer OVF- oder OVA-Datei..“* aus (❶) und gehen Sie mit *„Weiter“* zum nächsten Schritt (❷):

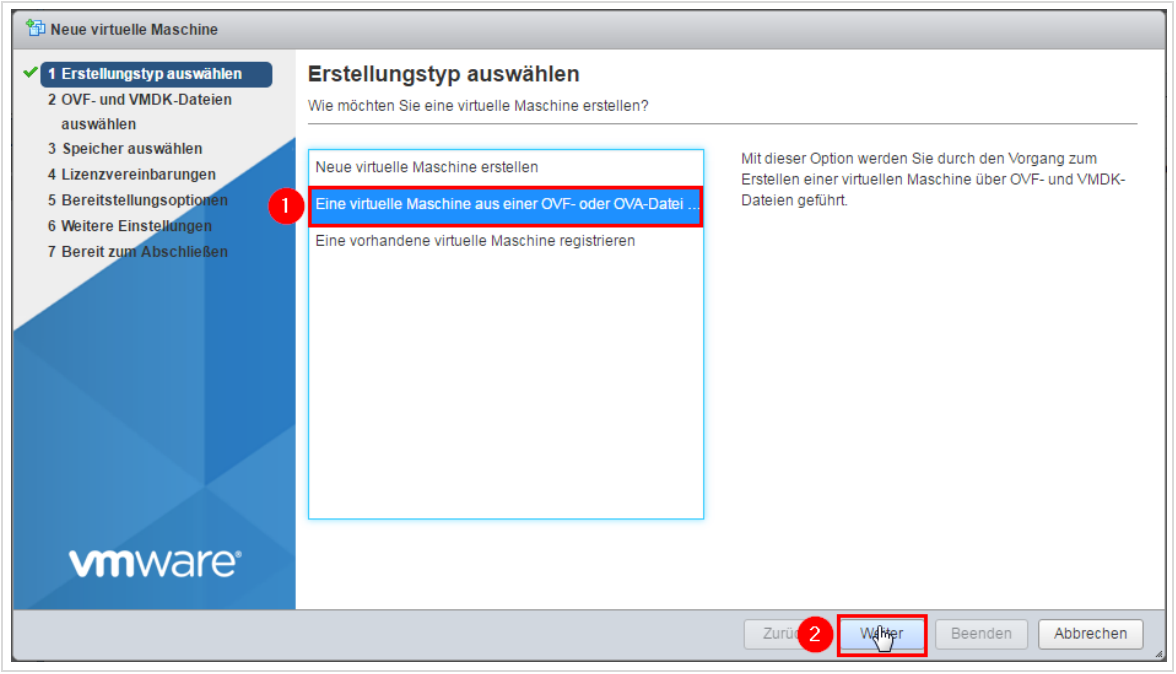

Abb. 67: Import eines OVA-Images

Geben Sie als Namen für die virtuelle Maschine *„Server“* ein (❶) und klicken Sie in den Bereich darunter (❷), um die später zu importierenden Dateien auszuwählen. Sie können hier auch mit *„Ziehen und Ablegen“ („Drag and Drop“)* arbeiten.

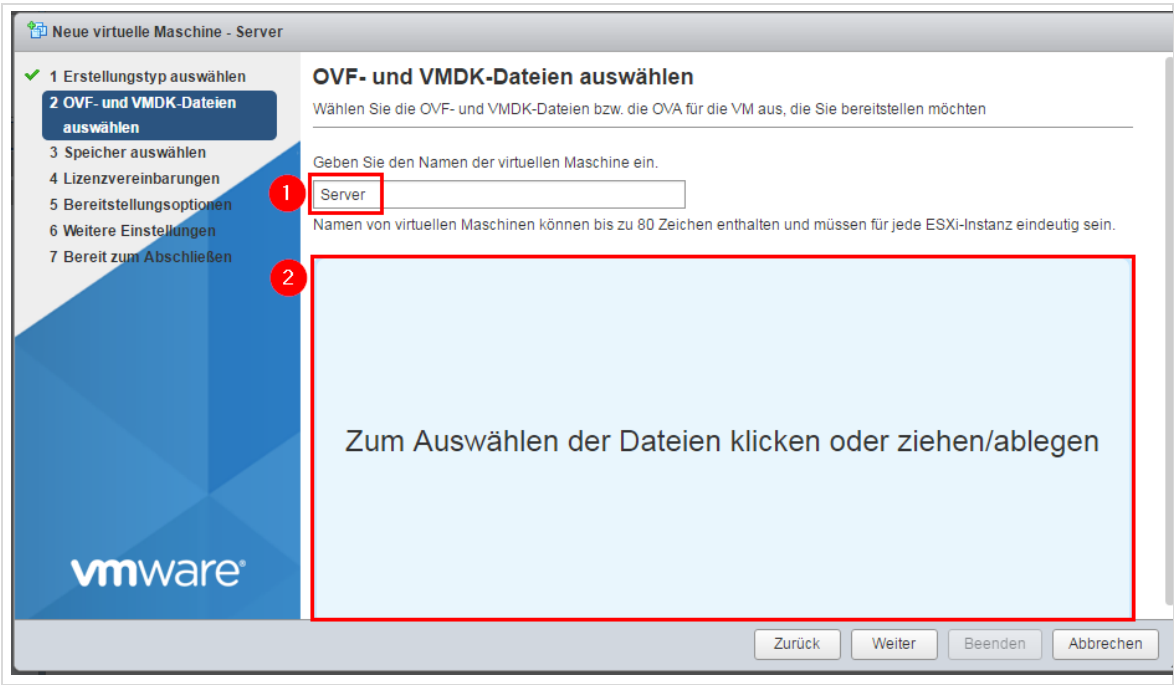

Abb. 68: OVA-Datei für die VM „Server“ auswählen

Wählen Sie das OVA-Image des Servers aus (❶) und klicken Sie auf *„Öffnen“* (❷):

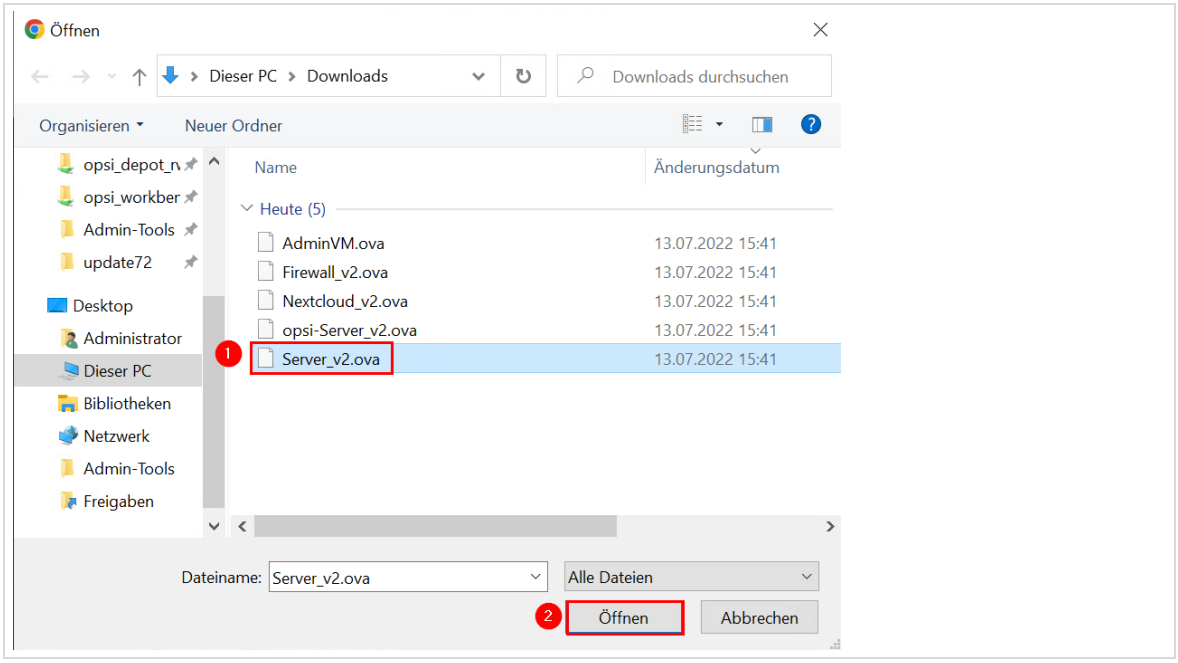

Abb. 69: Auswahl der OVA-Datei

Überprüfen Sie nochmals alle Angaben und klicken Sie auf „*Weiter*“:

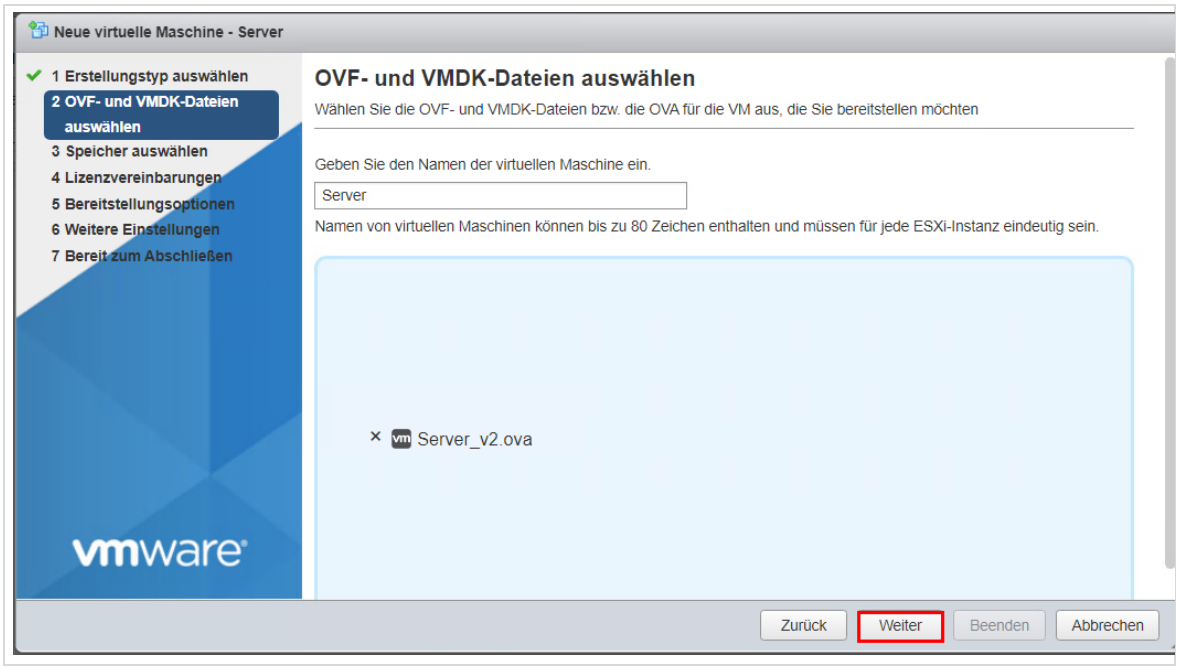

Abb. 70: Alle Angaben sind korrekt.

Im nächsten Dialog müssen Sie denjenigen Datastore auswählen, auf dem die virtuelle Maschine gespeichert werden soll (❶). Bestätigen Sie anschließend mit „*Weiter*“ (❷).

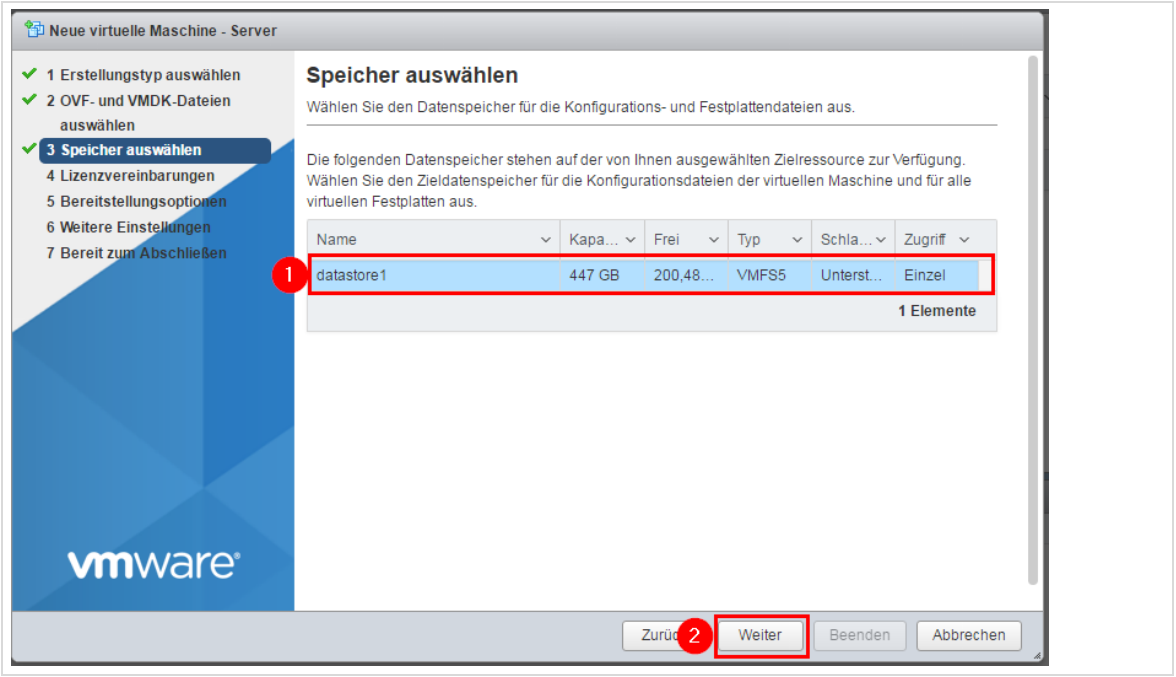

Abb. 71: Auswahl des Datastores

Im nachfolgenden Dialog werden das Festplattenformat und die Netzwerkzuordnungen der virtuellen Maschine festgelegt. Ordnen Sie die Netzwerke wie in der Abbildung (❶) zu, wählen Sie die Option „*Thick*“ aus (❷) und bestätigen Sie mit „*Weiter*“ (❸):

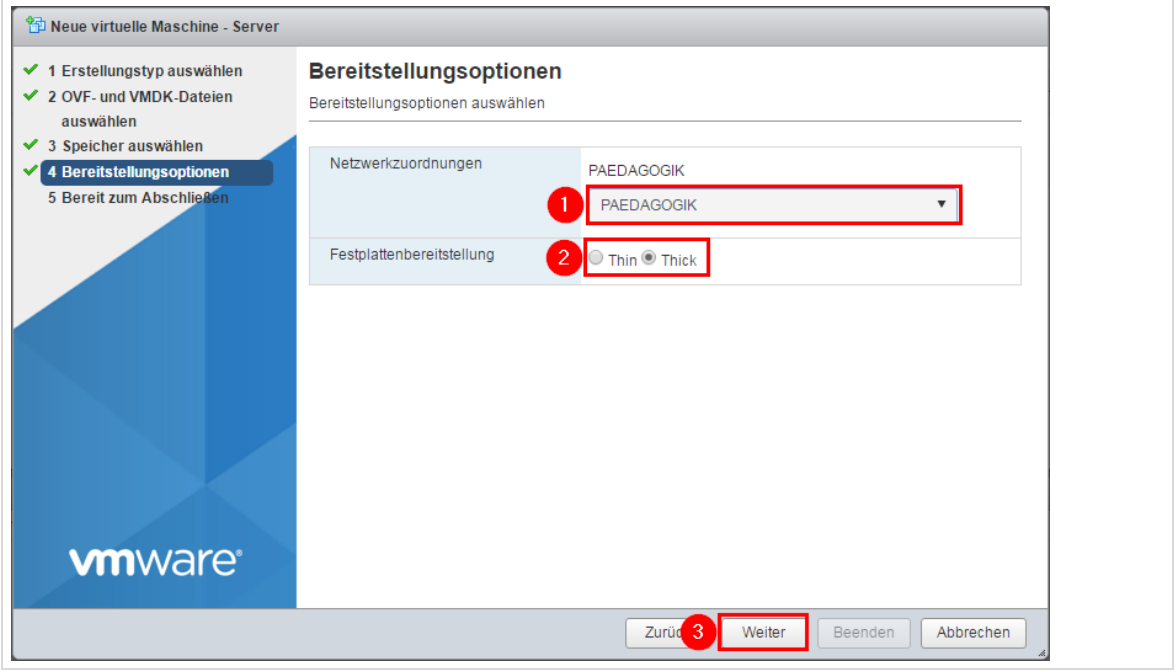

Abb. 72: Netzwerkzuordnungen und Auswahl des Festplattenformats „Thick“

Nachfolgend werden nochmals alle Einstellungen angezeigt. Kontrollieren Sie diese Einstellungen und bestätigen Sie den Dialog mit „*Beenden*“.

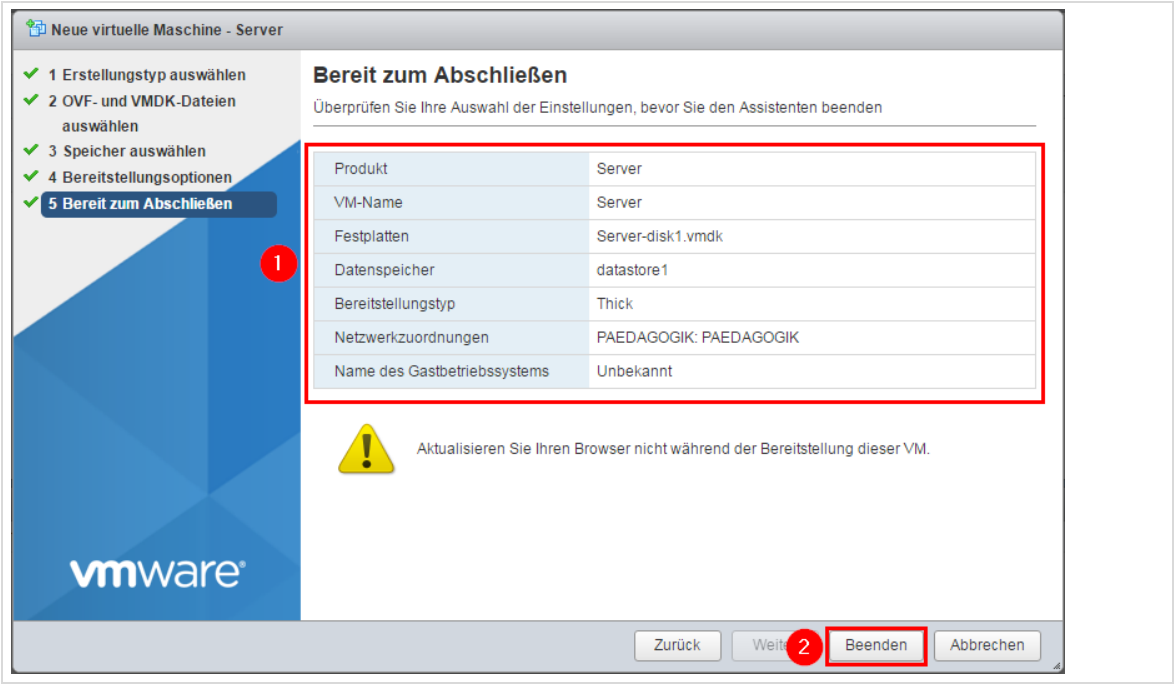

Abb. 73: Letzte Kontrolle der Einstellungen vor dem tatsächlichen Importvorgang

Nun beginnt der eigentliche Import der VM, dies kann je nach Systemleistung und Imagegröße einige Zeit in Anspruch nehmen.

4.3 Import der VM „opsi-Server“

Öffnen Sie den *vmware-Host-Client* über die IP-Adresse des ESXi-Hosts in einem Browser. Klicken Sie dann im linken Menü des *vmware-Host-Client* auf *„Virtuelle Maschinen“* (○) und danach im rechten Fenster auf den Eintrag *„VM erstellen/registrieren“* (○).

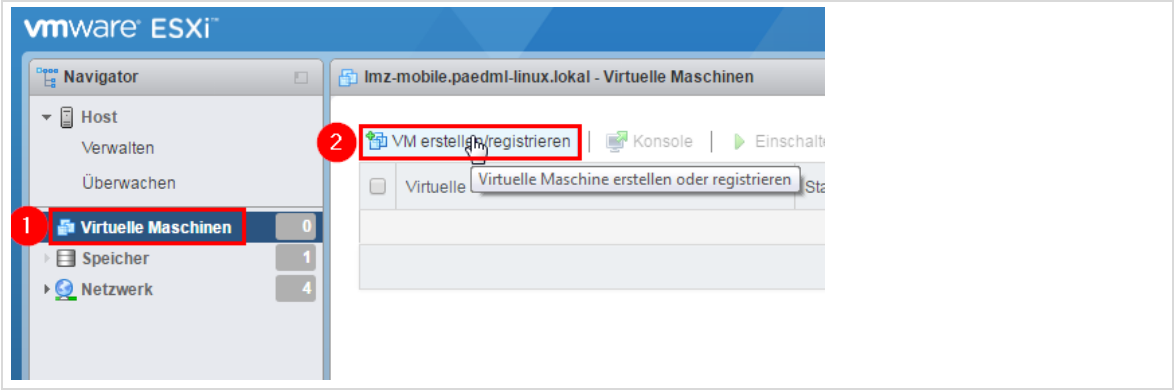

Abb. 74: Virtuelle Maschine erstellen

Wählen Sie im folgenden Fenster *„Eine virtuelle Maschine aus einer OVF- oder OVA-Datei..“* aus (❶) und gehen Sie mit *„Weiter“* zum nächsten Schritt (❷):

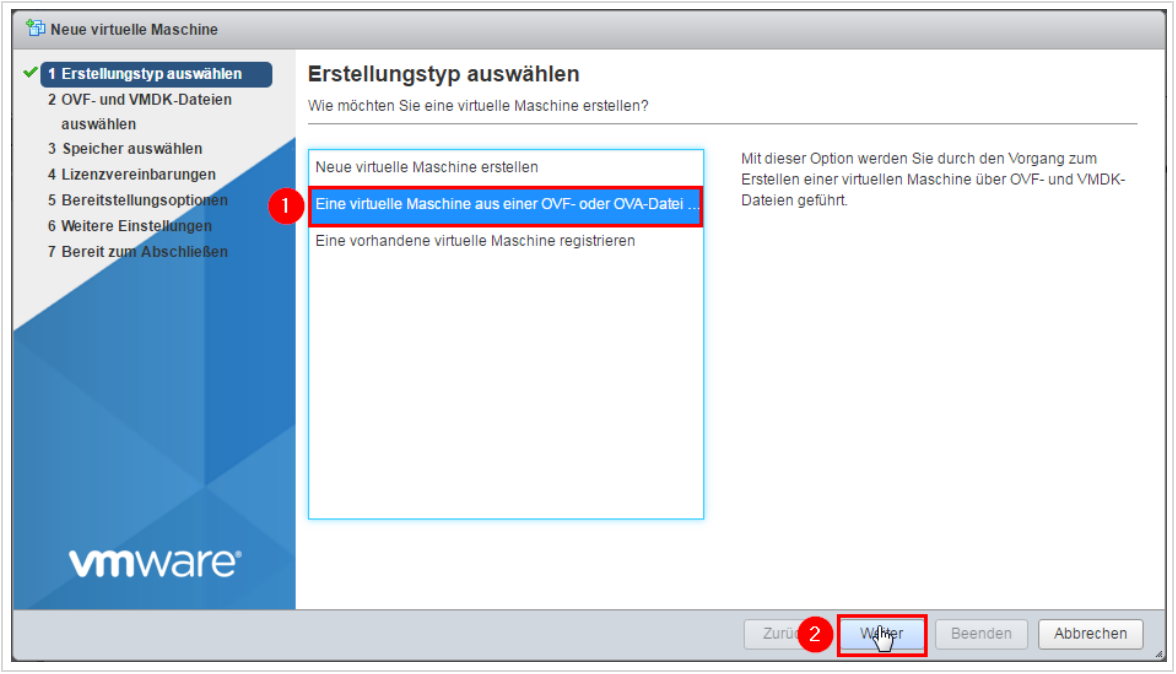

Abb. 75: Import eines OVA-Images

Geben Sie als Namen für die virtuelle Maschine *„OPSI-Server“* ein (❶) und klicken Sie in den Bereich darunter (❷), um die später zu importierenden Dateien auszuwählen. Sie können hier auch mit *„Ziehen und Ablegen“ („Drag and Drop“)* arbeiten.

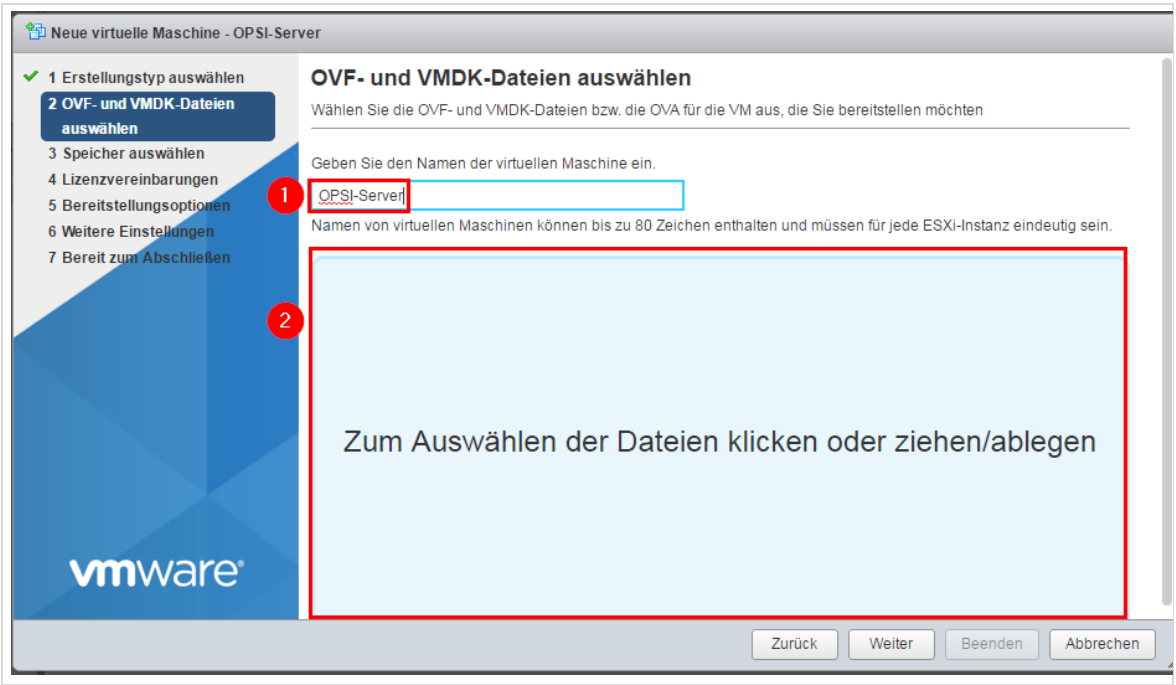

Abb. 76: OVA-Datei für die VM „OPSI-Server“ auswählen

Wählen Sie das OVA-Image des OPSI-Servers (❶) und klicken Sie auf „*Öffnen*“ (❷):

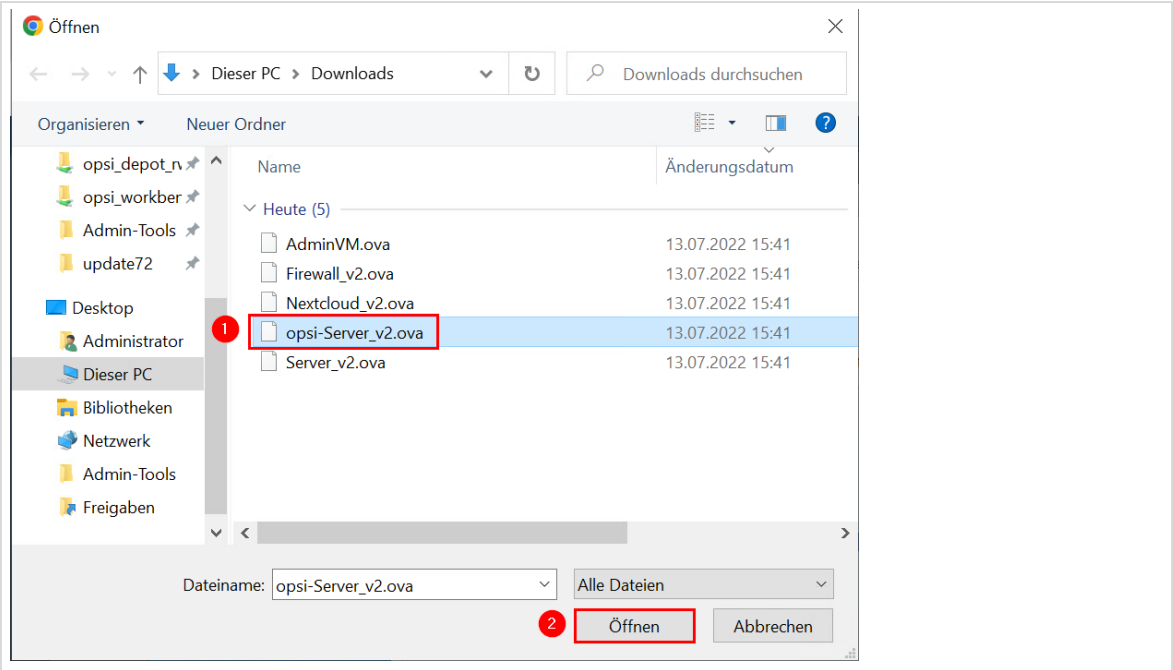

Abb. 77: Auswahl der OVA-Datei

Überprüfen Sie nochmals alle Angaben und klicken Sie auf „*Weiter*“:

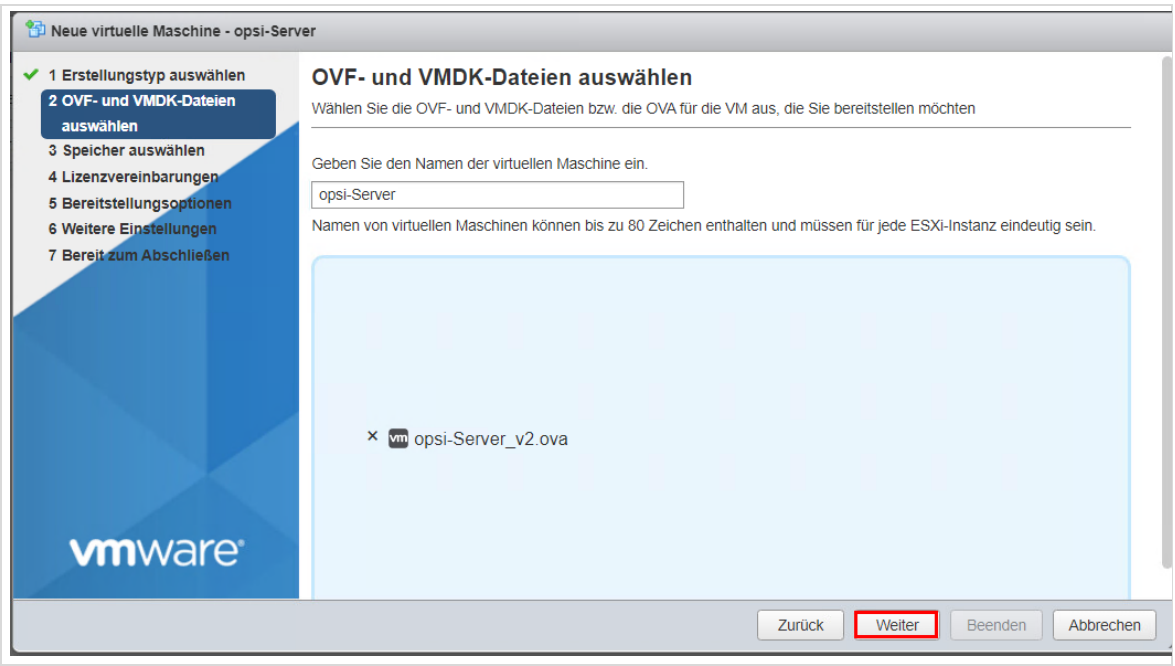

Abb. 78: Alle Angaben sind korrekt.

Im nächsten Dialog müssen Sie denjenigen Datastore auswählen, auf dem die virtuelle Maschine gespeichert werden soll (❶). Bestätigen Sie anschließend mit „*Weiter*“ (❷).

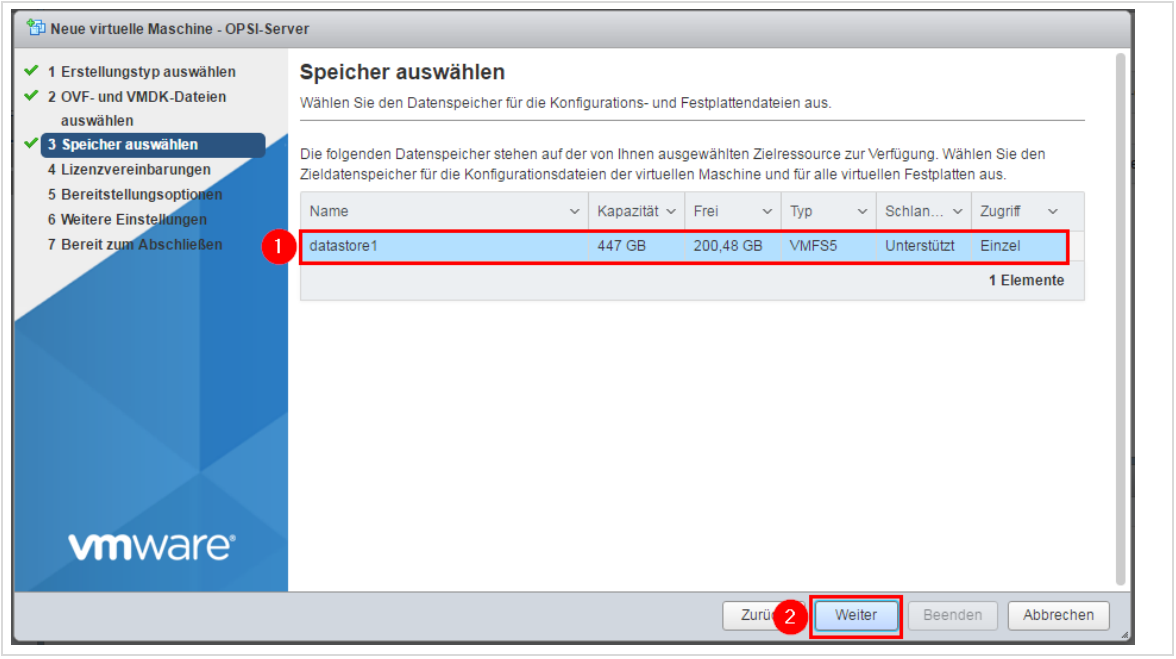

Abb. 79: Auswahl des Datastores

Im nachfolgenden Dialog werden das Festplattenformat und die Netzwerkzuordnungen der virtuellen Maschine festgelegt. Ordnen Sie die Netzwerke wie in der Abbildung (❶) zu, wählen Sie die Option „*Thick*“ aus (❷) und bestätigen Sie mit „*Weiter*“ (❸):

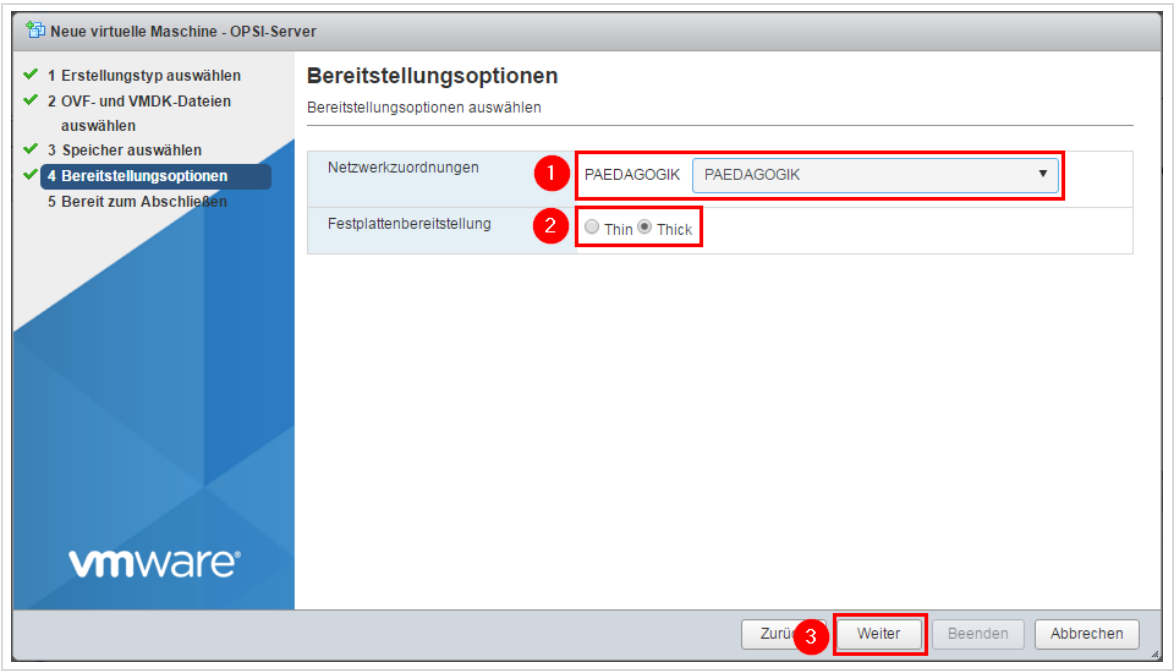

Abb. 80: Netzwerkzuordnungen und Auswahl des Festplattenformats „Thick“

Nachfolgend werden nochmals alle Einstellungen angezeigt. Kontrollieren Sie diese Einstellungen und bestätigen Sie den Dialog mit „*Beenden*“.

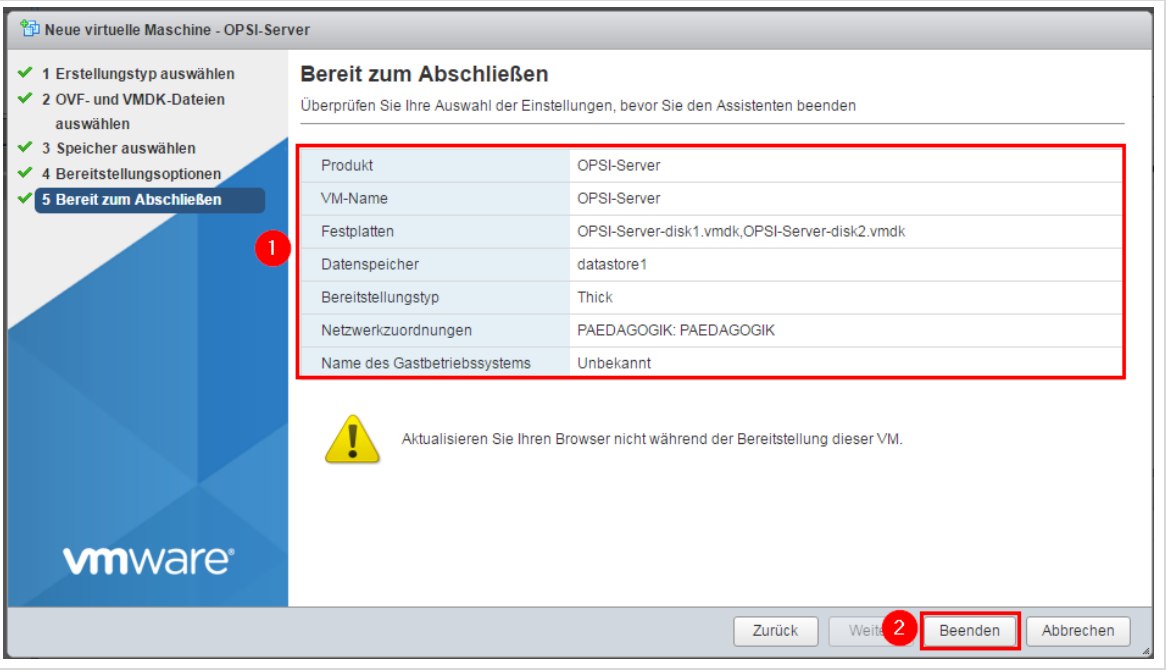

Abb. 81: Letzte Kontrolle der Einstellungen vor dem tatsächlichen Importvorgang

Nun beginnt der eigentliche Import der VM, dies kann je nach Systemleistung und Imagegröße einige Zeit in Anspruch nehmen.

4.4 Import der VM „W10AdminVM“

Hinweis: Das mit der AdminVM mitgelieferte Windows-Betriebssystem muss nach dem Import lizenziert werden.

Öffnen Sie den vmware-Host-Client über die IP-Adresse des ESXi-Hosts in einem Browser. Klicken Sie dann im linken Menü des vmware-Host-Client auf „Virtuelle Maschinen“ (1) und danach im rechten Fenster auf den Eintrag „VM erstellen/registrieren“ (2).

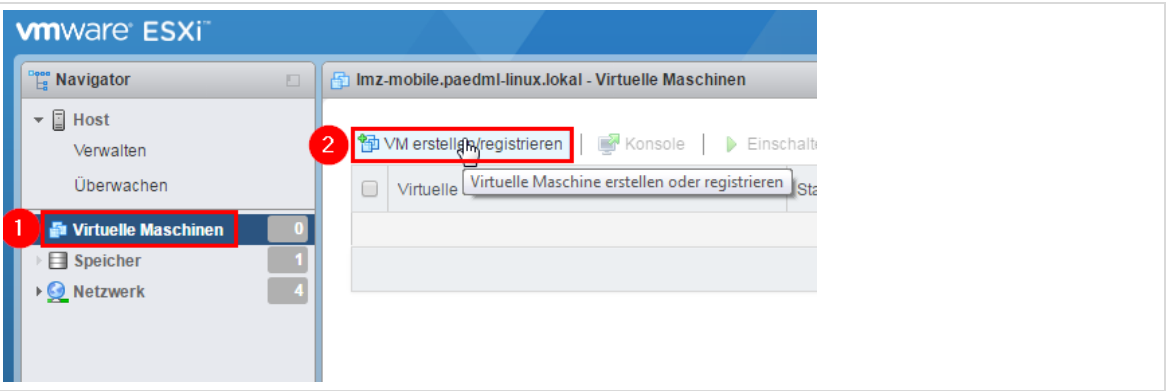

Abb. 82: Virtuelle Maschine erstellen

Wählen Sie im folgenden Fenster „Eine virtuelle Maschine aus einer OVF- oder OVA-Datei..“ aus (❶) und gehen Sie mit „Weiter“ zum nächsten Schritt (❷):

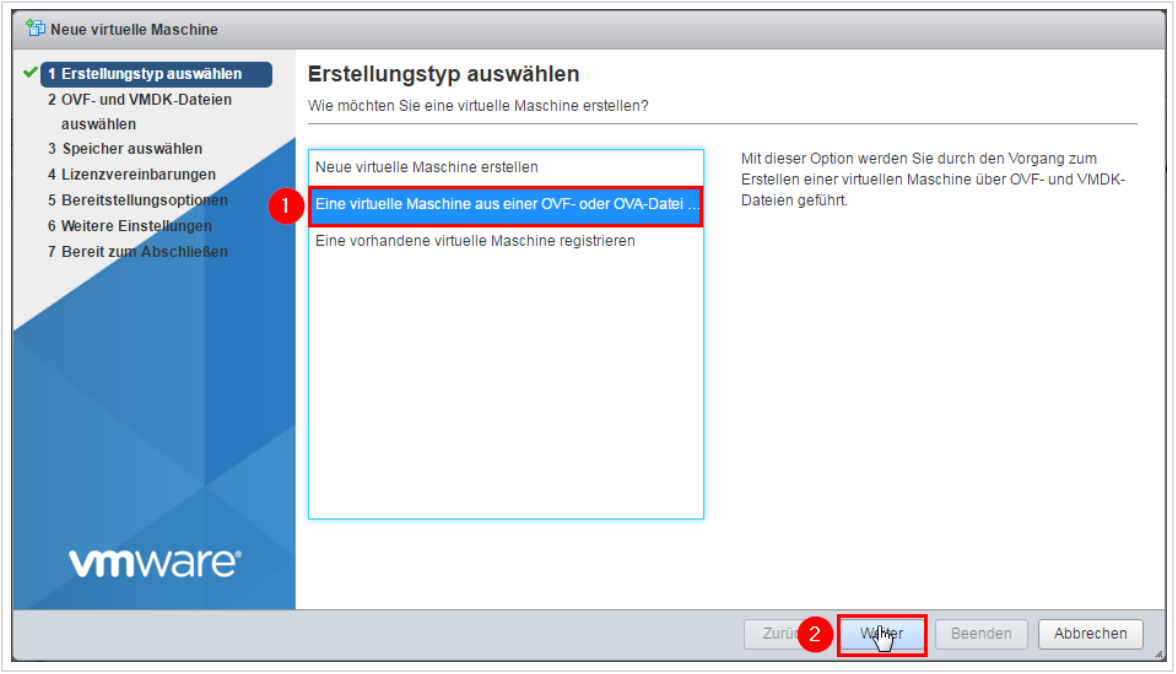

Abb. 83: Import eines OVA-Images

Geben Sie als Namen für die virtuelle Maschine „AdminVM“ ein (❶) und klicken Sie in den Bereich darunter (❷), um die später zu importierenden Dateien auszuwählen. Sie können hier auch mit „Ziehen und Ablegen“ („Drag and Drop“) arbeiten.

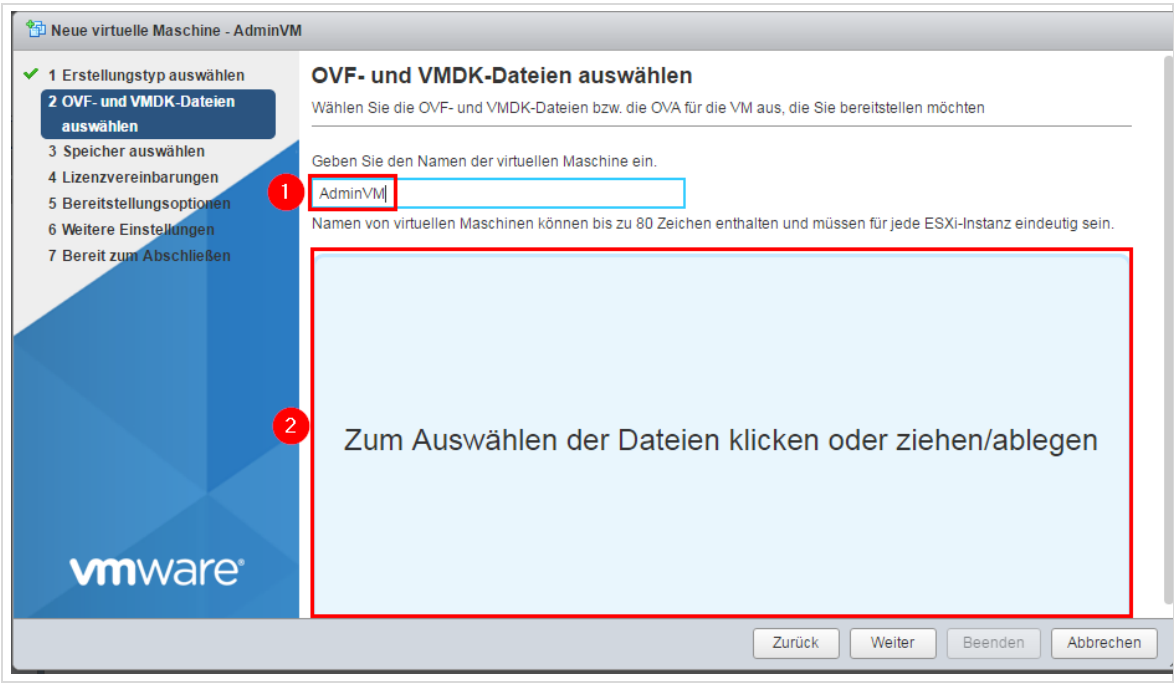

Abb. 84: OVA-Datei für die VM „Firewall“ auswählen

Wählen Sie die OVA-Datei der AdminVM auf dem paedML Linux-Datenträger aus (❶) und klicken Sie auf „Öffnen“ (❷):

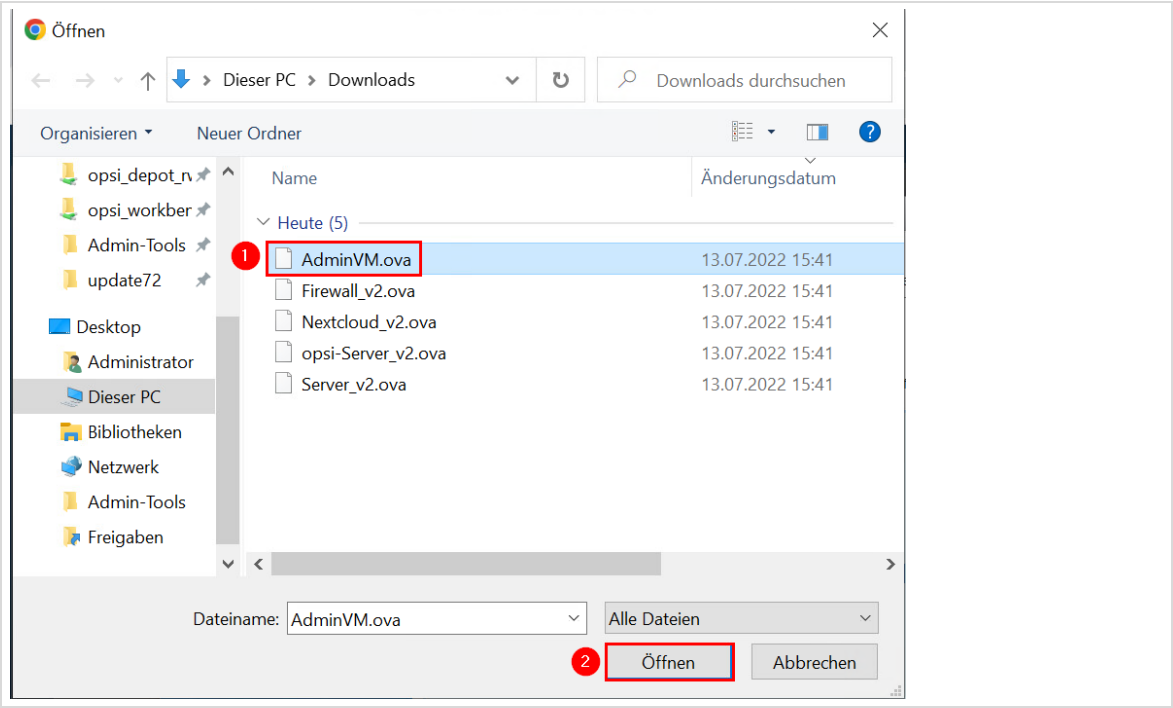

Abb. 85: Auswahl der OVA-Datei

Überprüfen Sie nochmals alle Angaben und klicken Sie auf „Weiter“:

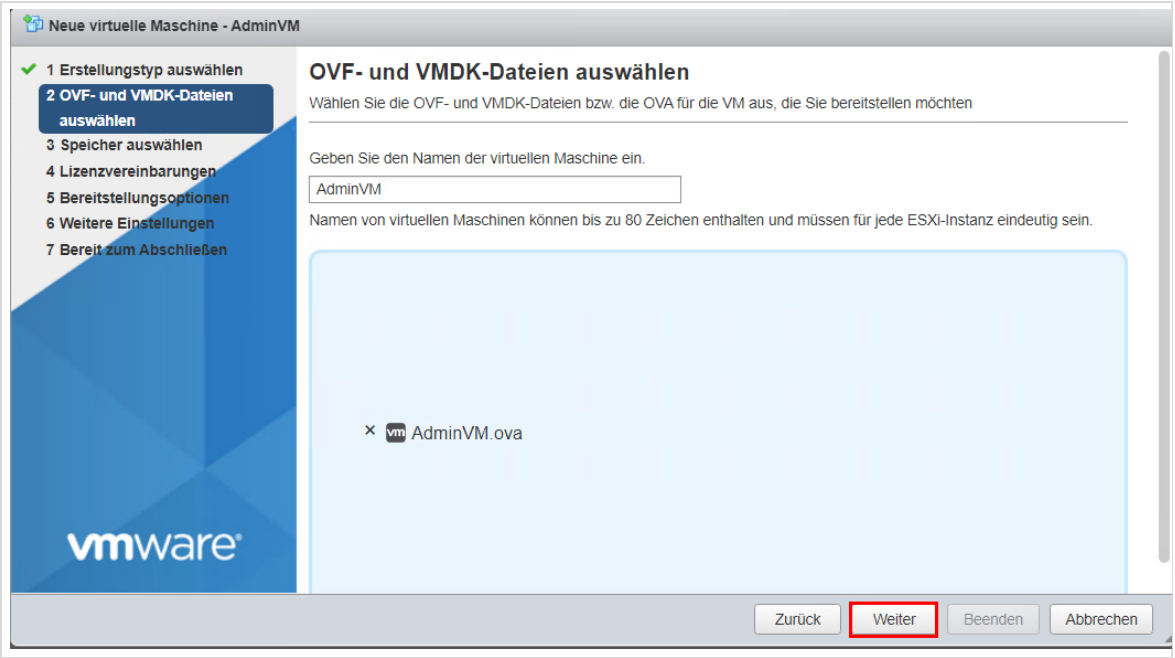

Abb. 86: Alle Angaben sind korrekt.

Im nächsten Dialog müssen Sie denjenigen Datastore auswählen, auf dem die virtuelle Maschine gespeichert werden soll (❶). Bestätigen Sie anschließend mit „Weiter“ (❷).

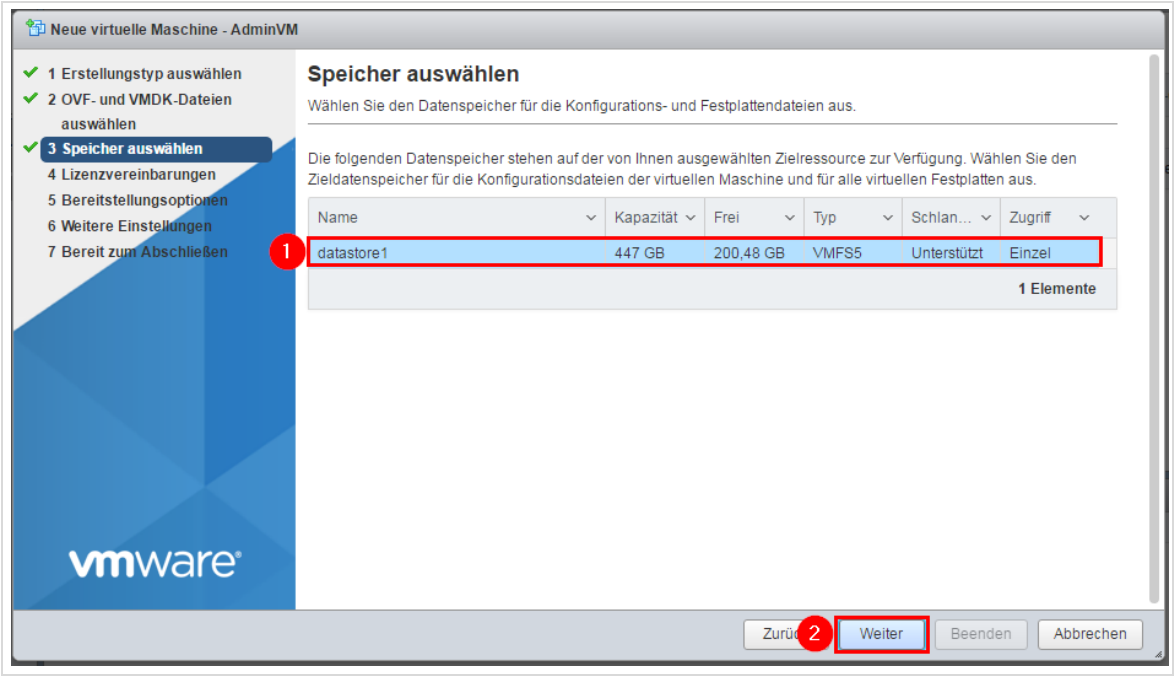

Abb. 87: Auswahl des Datastores

Im nachfolgenden Dialog werden das Festplattenformat und die Netzwerkzuordnungen der virtuellen Maschine festgelegt. Ordnen Sie die Netzwerke wie in der Abbildung (❶) zu, wählen Sie die Option „Thick“ aus (❷) und bestätigen Sie mit „Weiter“ (❸):

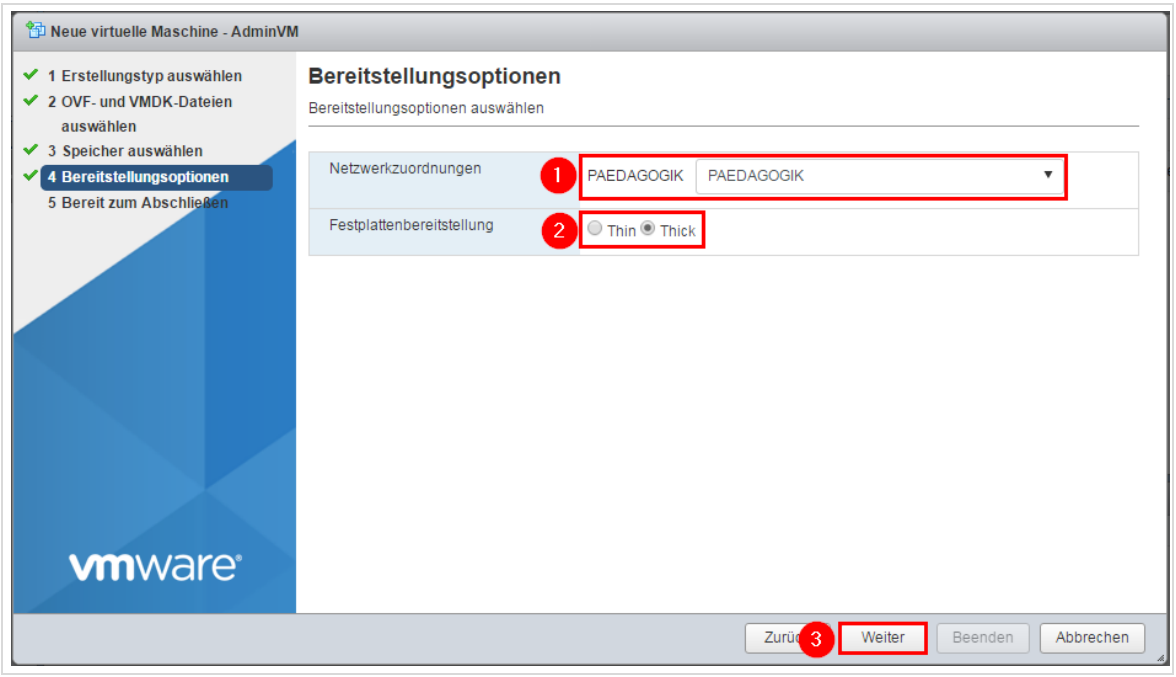

Abb. 88: Netzwerkzuordnungen und Auswahl des Festplattenformats „Thick“

Nachfolgend werden nochmals alle Einstellungen angezeigt. Kontrollieren Sie diese Einstellungen (❶) und bestätigen Sie den Dialog mit „Beenden“ (❷):

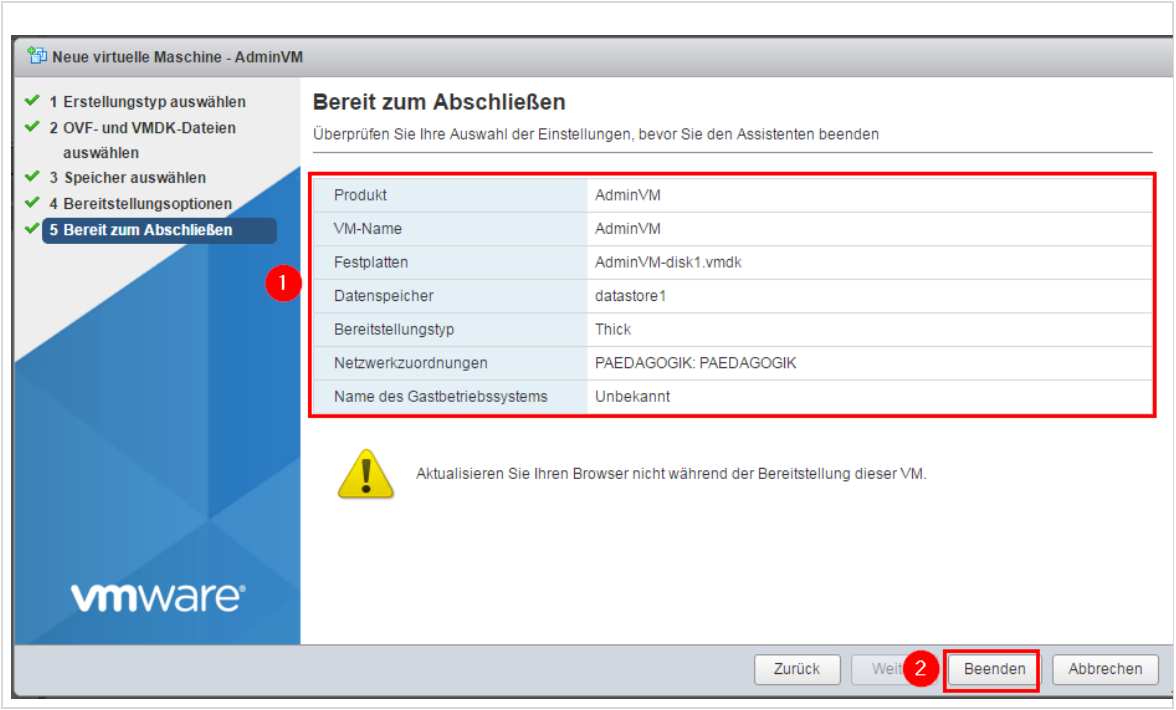

Abb. 89: Letzte Kontrolle der Einstellungen vor dem tatsächlichen Importvorgang

Nun beginnt der eigentliche Import der VM, dies kann je nach Systemleistung und Imagegröße einige Zeit in Anspruch nehmen.

4.5 Überprüfen des Imports

Sind alle virtuellen Maschinen erfolgreich importiert, so sollten Sie am Ende im *vmware-Host-Client* folgendes Bild vorfinden:

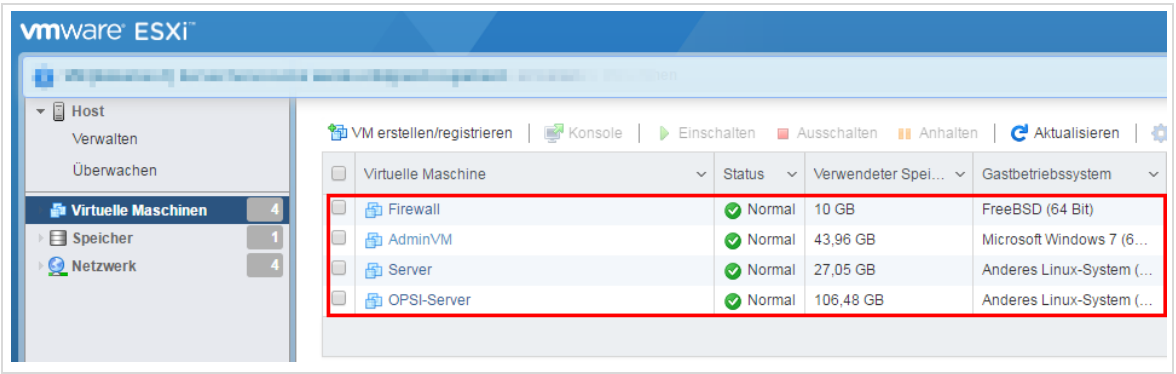

Abb. 90: Alle virtuellen Maschinen wurden erfolgreich importiert.

Überprüfen Sie den erfolgreichen Import der einzelnen virtuellen Maschinen, indem Sie diese per Mausklick im *vmware-Host-Client* anwählen.

4.6 Import der optionalen VM „Nextcloud“

Gehen Sie im linken Menü des ESXi-Host auf Virtuelle Maschinen (❶) und danach im rechten Fenster auf den Eintrag VM erstellen/registrieren (❷).

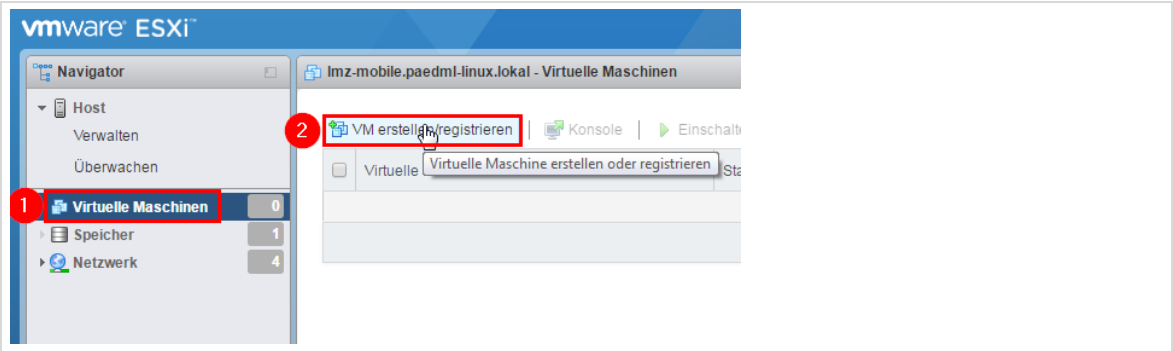

Abb. 91: Virtuelle Maschine erstellen

Wählen Sie im folgenden Fenster Eine virtuelle Maschine aus einer OVF- oder OVA-Datei… aus (❶) und gehen Sie mit Weiter zum nächsten Schritt (❷).

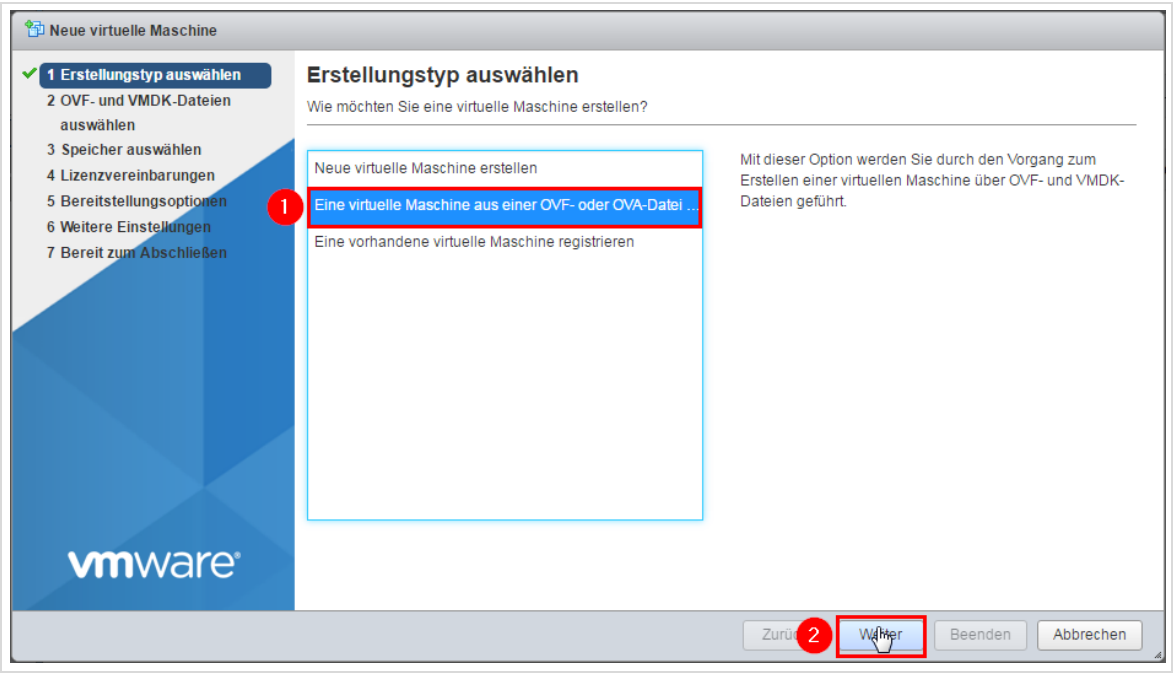

Abb. 92: Import eines OVA-Images

Geben Sie als Namen für die virtuelle Maschine *Nextcloud* ein und klicken Sie in den Bereich darunter, um die später zu importierenden Dateien auszuwählen.

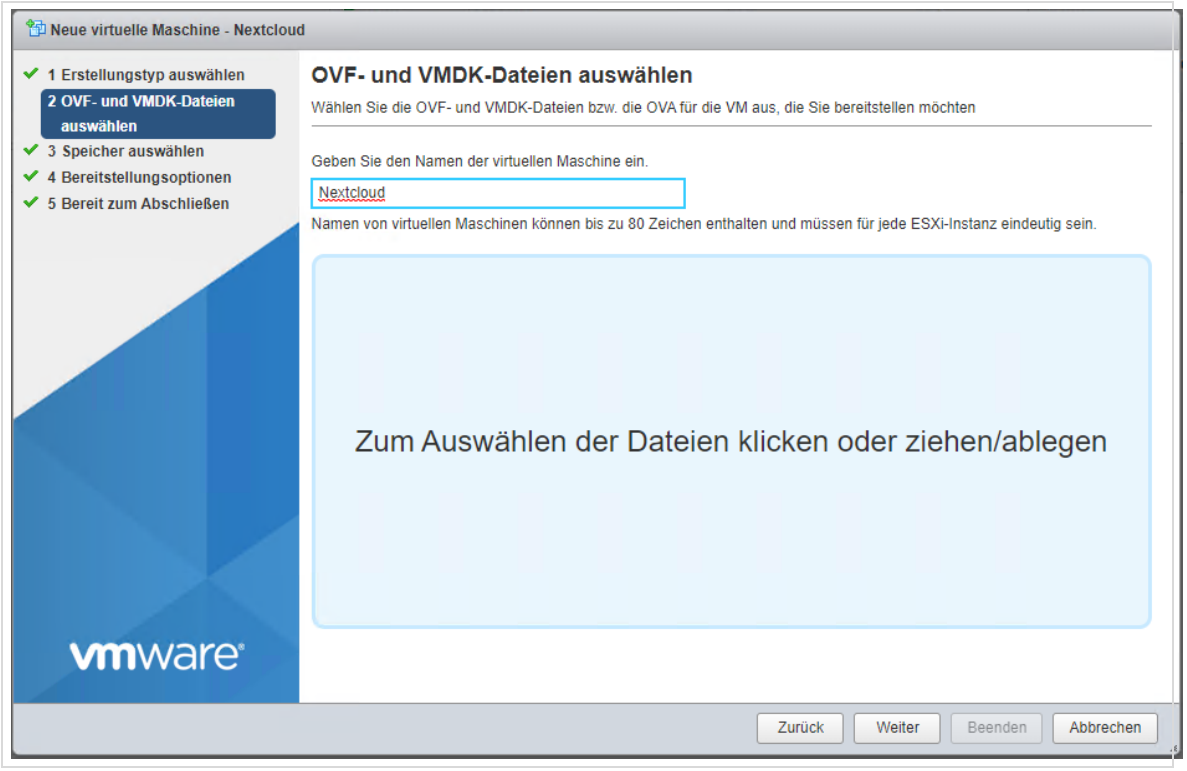

Abb. 93: OVA-Datei für die VM „Nextcloud“ auswählen

Wählen Sie die OVA-Datei der *Nextcloud* aus und klicken Sie auf *Öffnen*:

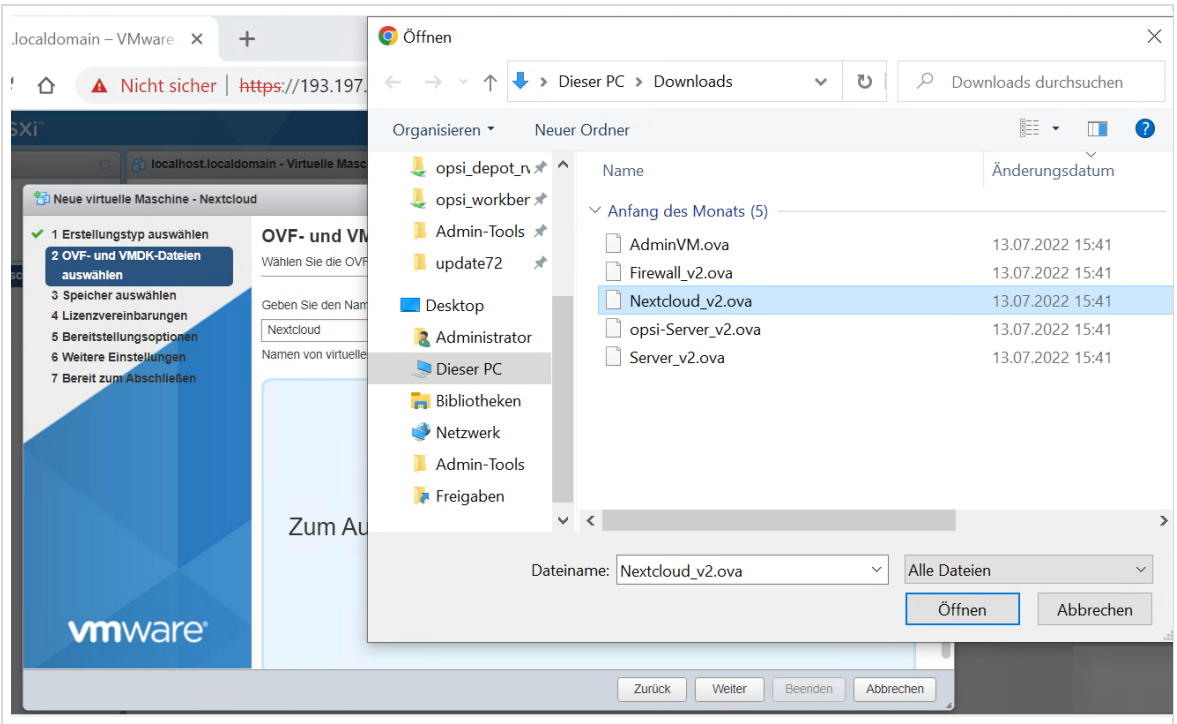

Abb. 94: Auswahl der OVA-Datei

Überprüfen Sie nochmals alle Angaben und klicken Sie auf *Weiter*:

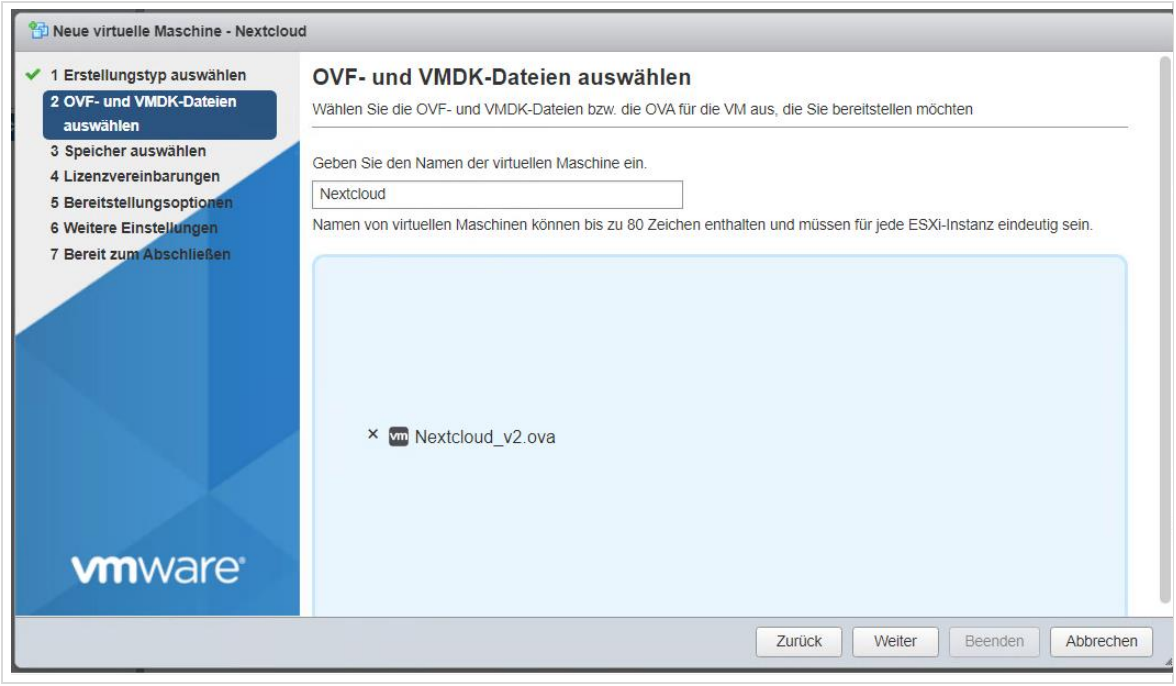

Abb. 95: Alle Angaben sind korrekt.

Im nächsten Dialog müssen Sie denjenigen Datastore auswählen, auf dem die virtuelle Maschine gespeichert werden soll. Bestätigen Sie anschließend mit *Weiter*.

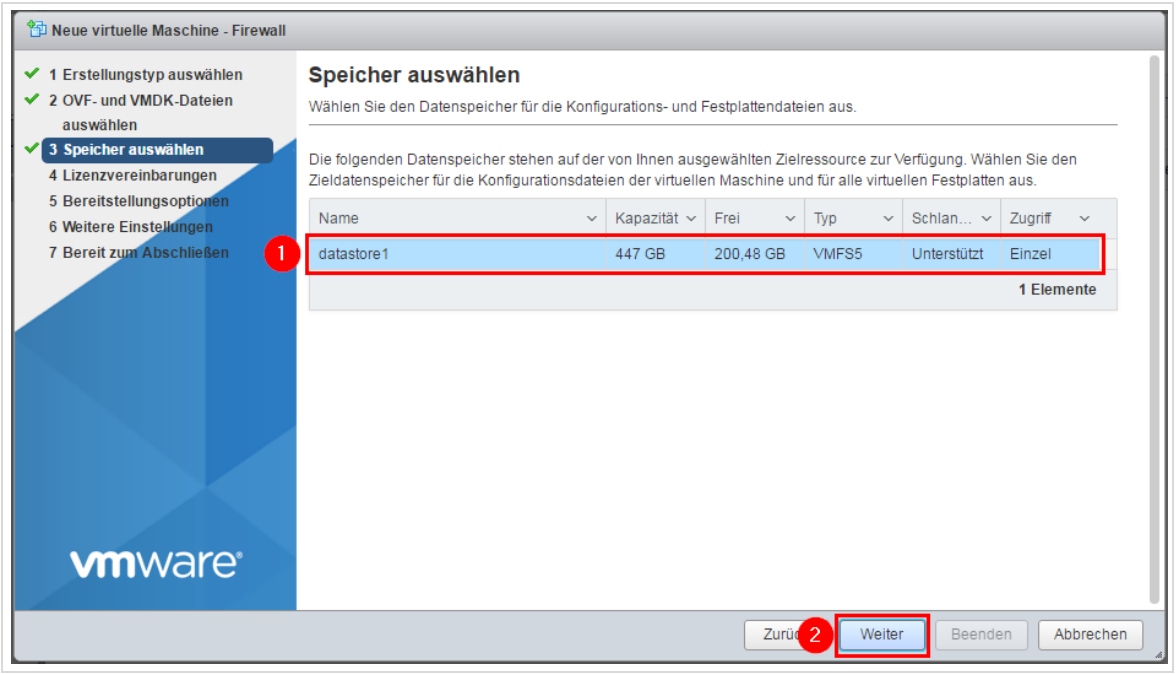

Abb. 96: Auswahl des Datastores

Im nachfolgenden Dialog werden das Festplattenformat und die Netzwerkzuordnungen der virtuellen Maschine festgelegt. Ordnen Sie die Netzwerke wie in der Abbildung zu, wählen Sie die Option *Thick* und *Automatisch einschalten* aus. Bestätigen Sie mit *Weiter*.

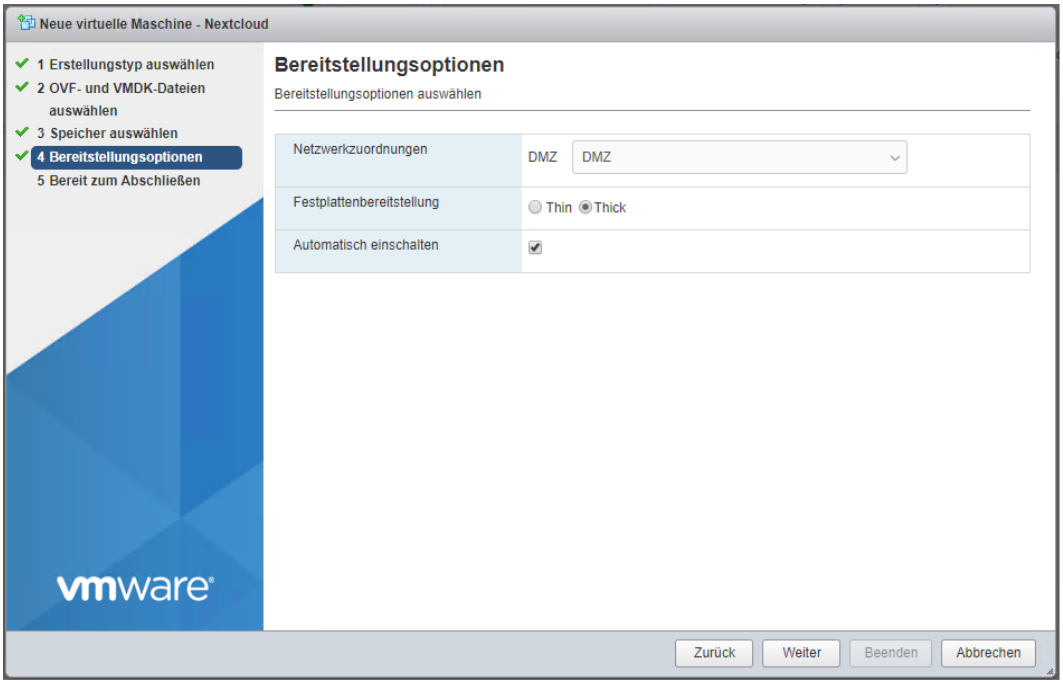

Abb. 97: Netzwerkzuordnungen und Auswahl des Festplattenformats „Thick“

Nachfolgend werden nochmals alle Einstellungen angezeigt. Kontrollieren Sie diese Einstellungen und bestätigen Sie den Dialog mit *Beenden*:

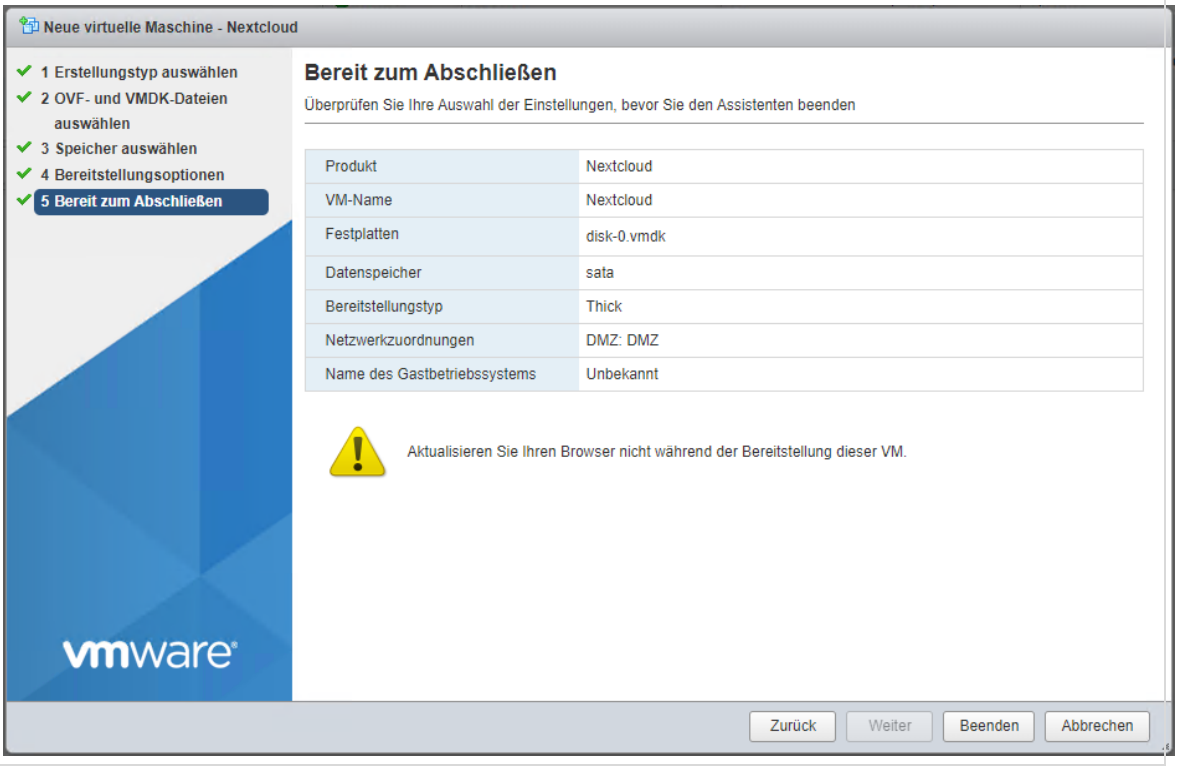

Abb. 98: Letzte Kontrolle der Einstellungen vor dem tatsächlichen Importvorgang

Nun beginnt der eigentliche Import der VM, dies kann je nach Systemleistung und Imagegröße einige Zeit in Anspruch nehmen.

Nach abgeschlossenem Import sind die Arbeiten auf dem ESXi beendet.

5 Basiskonfiguration der virtuellen Maschinen

Es erfolgt die Basiskonfiguration der drei importierten Maschinen „*Firewall*“, „*Server*“ und „*opsi-Server*“, die Maschine „*AdminVM*“ erfordert ein gesondertes Vorgehen, dies wird in Kapitel 0 ab Seite 81 beschrieben.

Schalten Sie die virtuellen Maschinen immer in der angegebenen Reihenfolge ein!

Warten Sie dabei stets mit dem Start der nächsten Maschine, bis die vorherige vollständig hochgefahren ist!

Die virtuellen Server „*Firewall*“, „*Server*“ und „*opsi-Server*“ müssen nun in der folgenden Reihenfolge eingeschaltet werden.

1. *Firewall*
2. *Server*
3. *opsi-Server*

Markieren Sie dazu im *vmware-Host-Client* jeweils die entsprechende Maschine mit der Maus und klicken Sie auf den Button „*Einschalten*“.

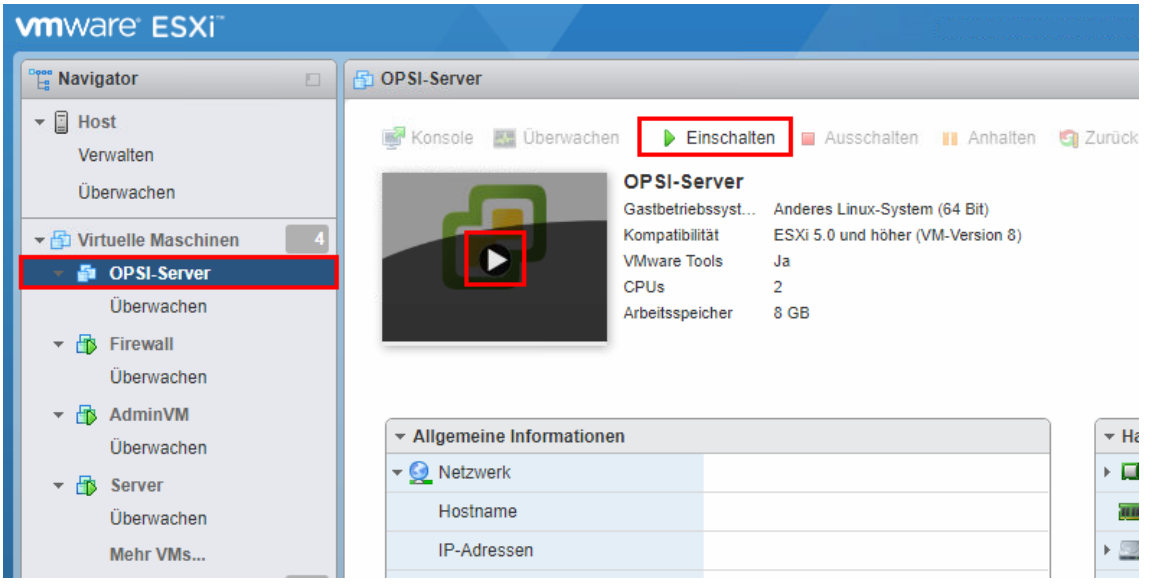

Abb. 99: Einschalten einer virtuellen Maschine über den vmware-Host-Client

Die **Passwörter** für alle zentralen Benutzerkonten wie *root* oder *Administrator* (Domänen-Administrator) sind initial auf den Wert „*paedmllinux*“ gesetzt.

5.1 Basiskonfiguration der VM „Firewall“

Die externe Netzwerkkarte der Firewall (Netz „*INTERNET*“) ist im Auslieferungszustand auf den Bezug von dynamischen IP-Adressen konfiguriert. Falls die Firewall über das externe Interface keine IP-Adresse

per DHCP, zugewiesen bekommt (z.B. bei einem DSL-Router), muss das externe Netzwerkinterface zwingend auf eine statische IP-Adresse umgestellt werden.

Veränderungen an den Einstellungen der Firewall dürfen nur per Browser über die Web-Schnittstelle („*WebGUI*“) vorgenommen werden.

Die über die Textkonsole angebotenen Funktionen zur Netzkonfiguration dürfen nicht genutzt werden!

5.1.1 Optional: Hinzufügen des Netzwerkadapters MDM zur VM Firewall

Bei Verwendung des MDM-Netzes klicken Sie im ESXi-Host auf *Virtuelle Maschinen* und auf *Firewall*. *Bearbeiten* Sie die virtuelle Maschine *Firewall*.

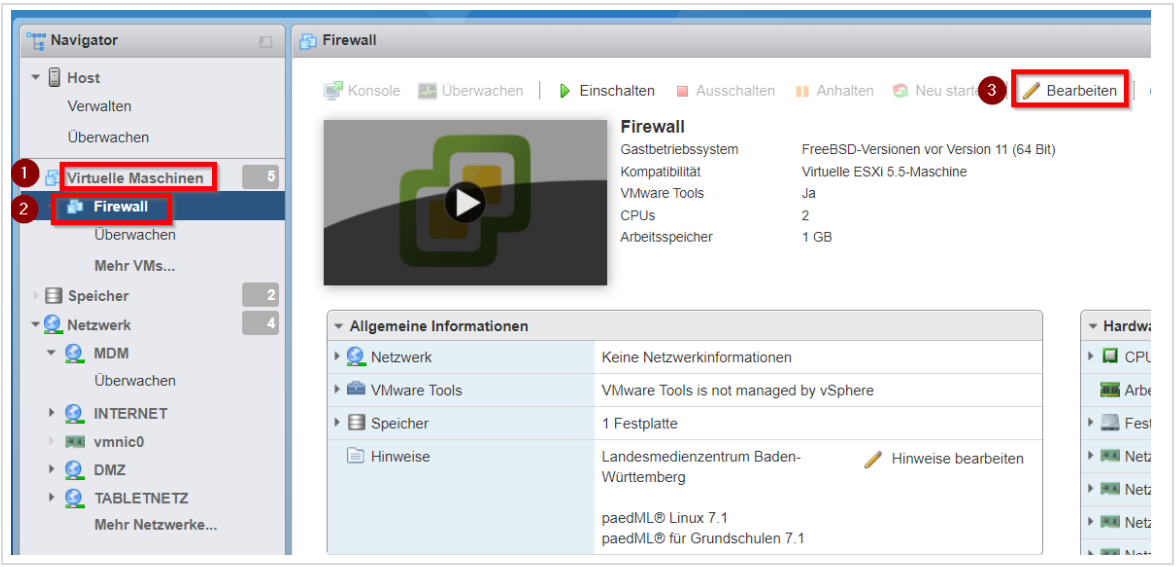

Abb. 100: Firewall bearbeiten.

Klicken Sie im nächsten Dialog auf *Netzwerkadapter hinzufügen*.

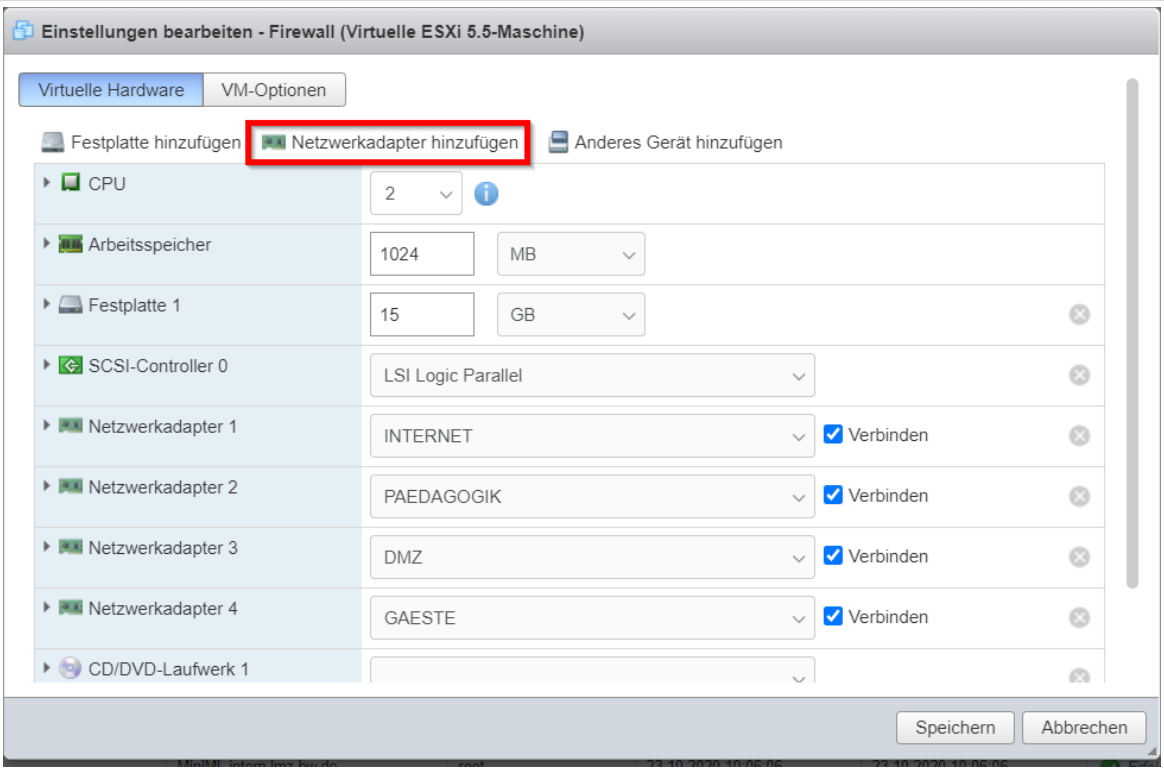

Abb. 101: Netzwerkadapter hinzufügen.

Ordnen Sie dem Netzwerkadapter die Portgruppe *MDM* zu und klicken Sie auf *Speichern*.

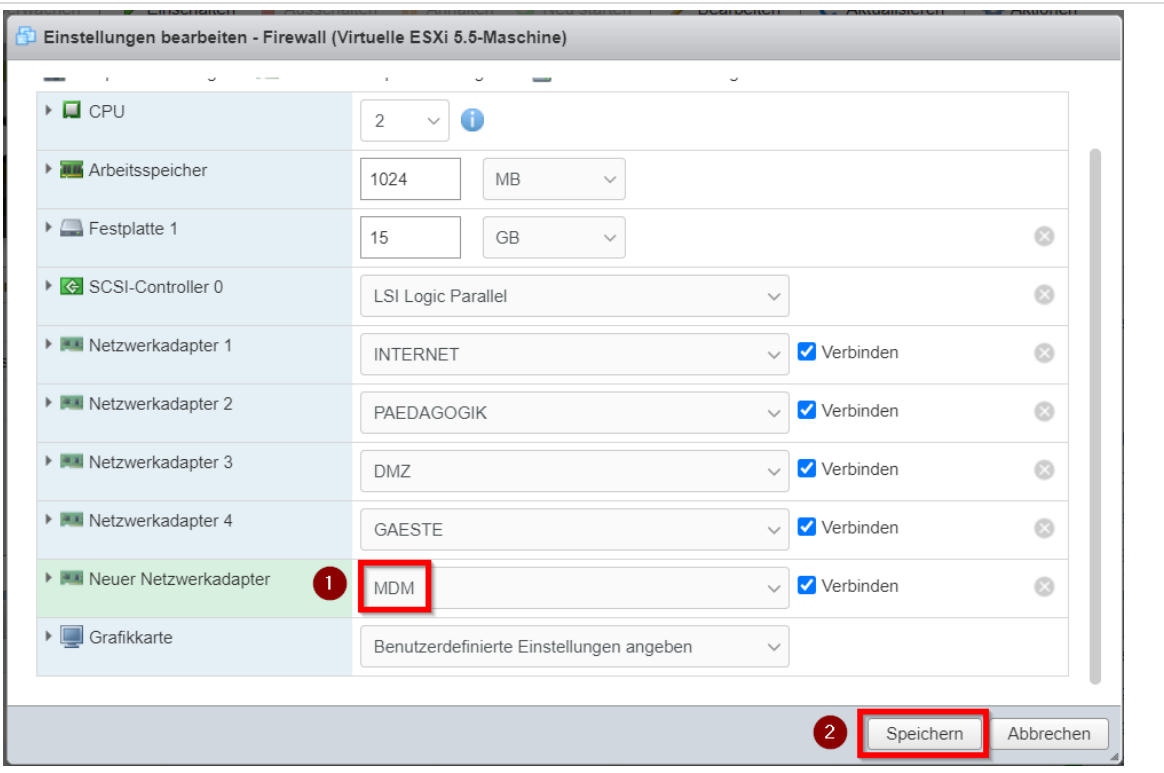

Abb. 102: Netzwerkadapter konfigurieren.

Sollten Sie einzelne Netze nicht einsetzen, können Sie die Haken bei Verbinden herausnehmen.

5.1.2 Optional: Hinzufügen des Netzwerkadapters DMZ zur VM Firewall

Beachten Sie dieses Kapitel bitte nur, wenn Sie die VM Nextcloud verwenden.

Fahren Sie die VM ***Firewall*** herunter. Markieren Sie dazu die VM und klicken Sie auf ***Herunterfahren***.

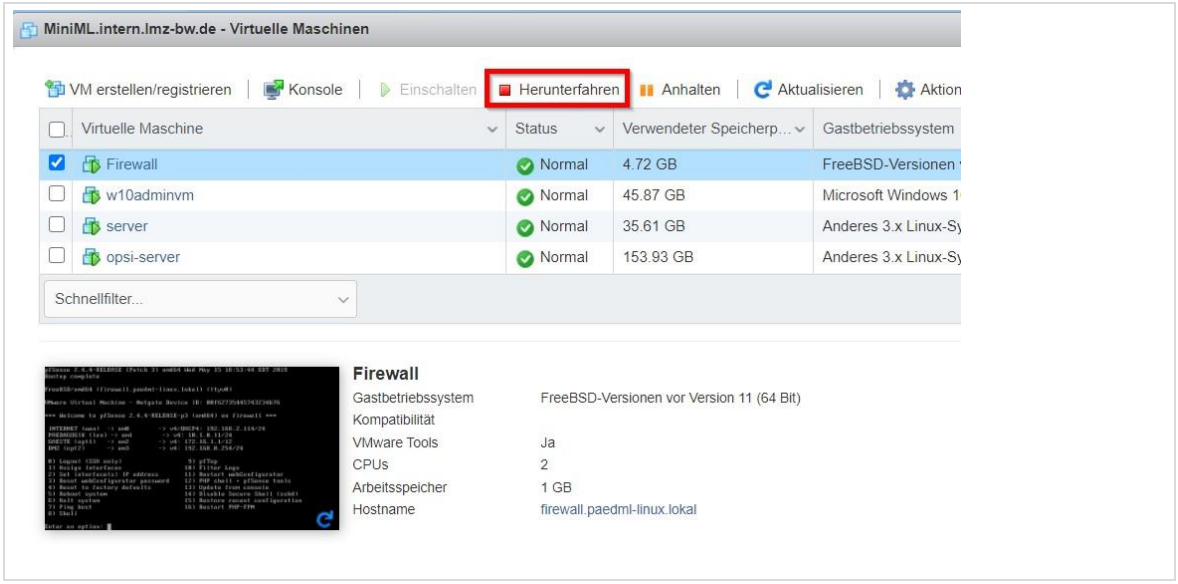

Abb. 103: Firewall herunterfahren

Gehen Sie mit Rechtsklick auf die VM ***Firewall*** und klicken Sie auf ***Einstellungen bearbeiten***.

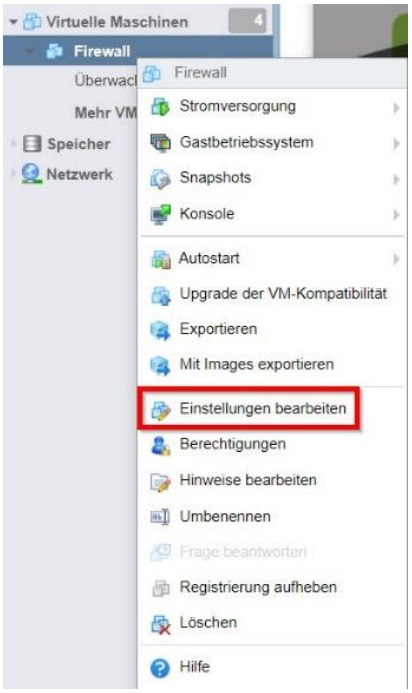

Abb. 104: Einstellungen bearbeiten

Wählen Sie Netzwerkadapter hinzufügen.

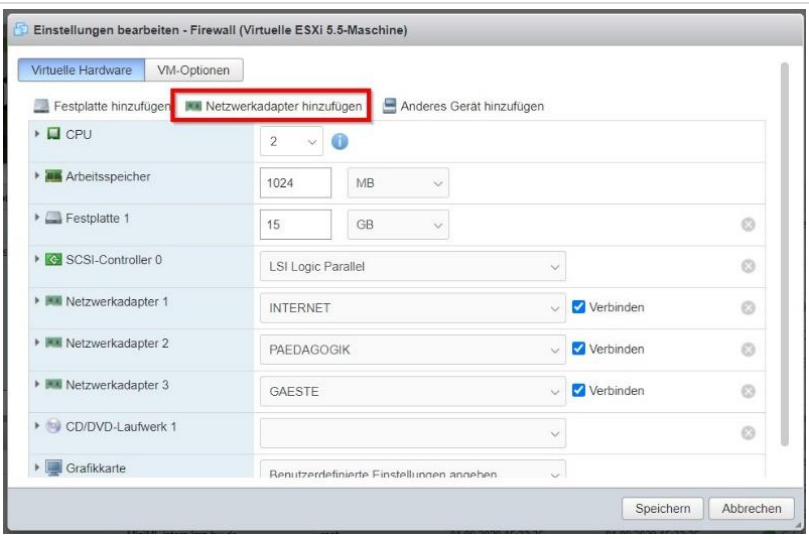

Abb. 105: Netzwerkadapter hinzufügen

DMZ erscheint als neuer Netzwerkadapter. Bestätigen Sie mit ***speichern*** und starten Sie anschließend die VM ***Firewall***.

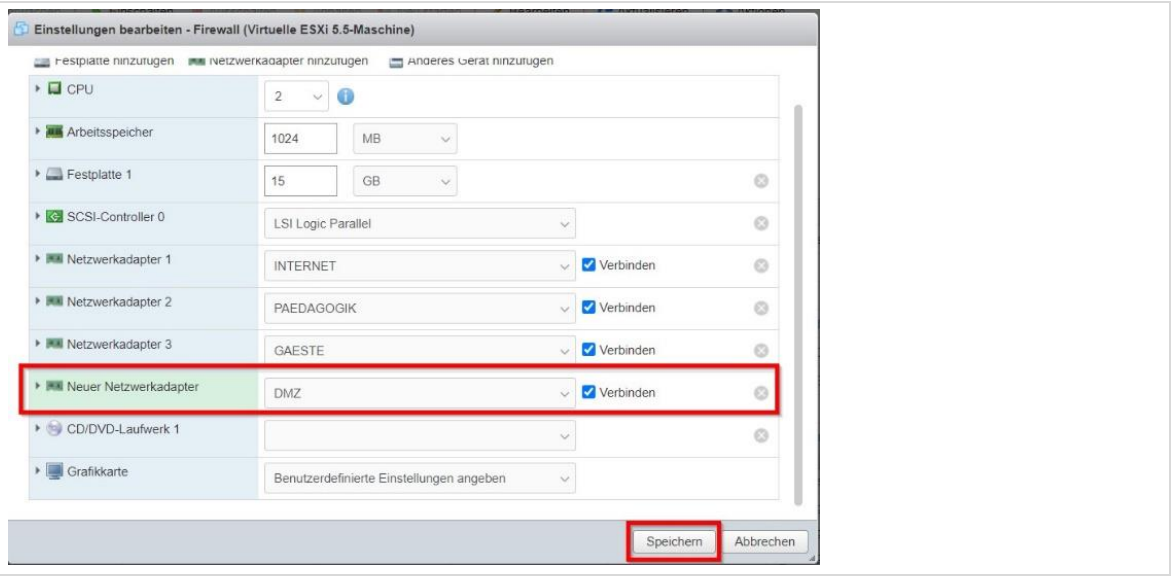

Abb. 106: Neuer Netzwerkadapter DMZ

Die Firewall muss nun wieder eingeschaltet werden.

5.1.3 IP-Konfiguration der externen Netzwerkkarte (statische IP-Adresse)

Login auf der WebGUI der Firewall

Öffnen Sie im Browser die WebGUI der Firewall unter http://firewall.paedml-linux.lokal oder http://10.1.0.11 und melden Sie sich als Benutzer „*Administrator*“ an (auch möglich mit „*admin*“ und initialem Passwort „*paedmllinux*“). Um die WebGUI der Firewall aufrufen zu können, ist das Booten eines Clients im pädagogischen Netz mit einer Live-Linux Distribution[3] (mithilfe einer Live-CD oder eines Live-USB-Sticks) oder eines anderen Betriebssystems denkbar.

[3] z.B. „Xubuntu“ https://xubuntu.org/ oder „Knoppix“ http://www.knopper.net/knoppix/, abgerufen am 25.07.2022

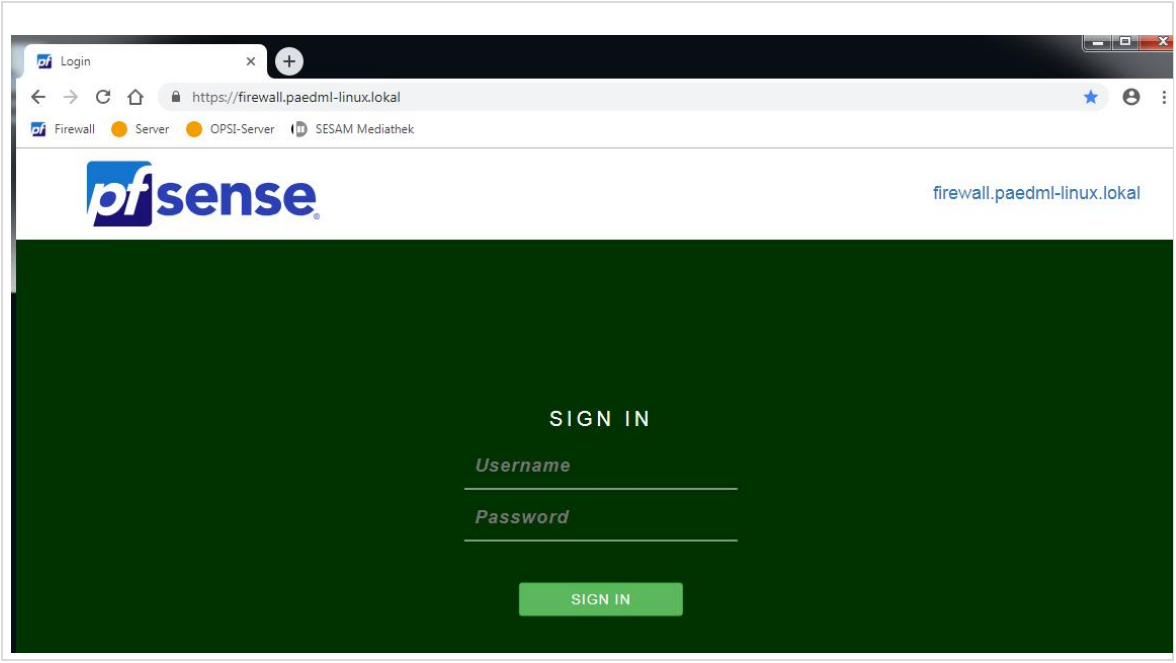

Abb. 107: Login-Maske der Firewall

Umstellen der externen Netzwerkkarte auf statische IP-Adresse

Navigieren Sie zum Punkt *„Schnittstellen | INTERNET“* um die Einstellungen der externen Netzwerkkarte zu ändern.

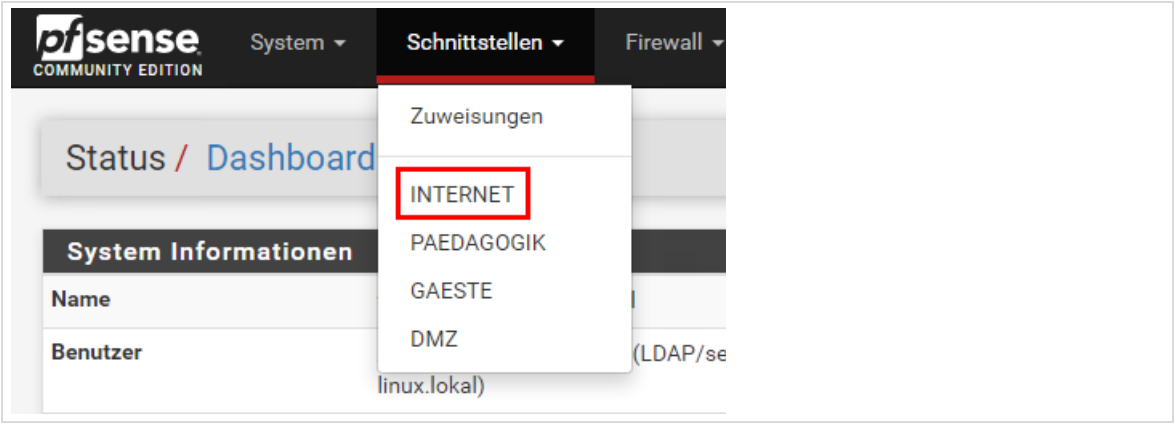

Abb. 108: Navigation zu den Einstellungen der externen Netzwerkkarte

Führen Sie im folgenden Fenster folgende Änderungen durch:

- Ändern Sie die Einstellung *„IPv4 Konfigurationstyp“* auf *„Statische IPv4“*.
- Tragen Sie im Feld *„IPv4 Adresse“* die statische IP-Adresse des externen Interfaces sowie den Netzbereich ein. **Die Adresse und die Subnetzmaske sind abhängig von der lokal gegebenen Netzwerkkonfiguration und muss an diese angepasst werden!**
- Wählen Sie im Feld „IPv4 Upstream Gateway“ die IP-Adresse des Gateways für den Internetzugang (z.B. die interne IP-Adresse ihres DSL-Routers) aus, falls das Gateway der Firewall schon bekannt ist. Im Regelfall ist dieses Gateway der Firewall aber noch nicht bekannt und muss zunächst durch Klick auf *„Ein neues Gateway hinzufügen“* angelegt werden.

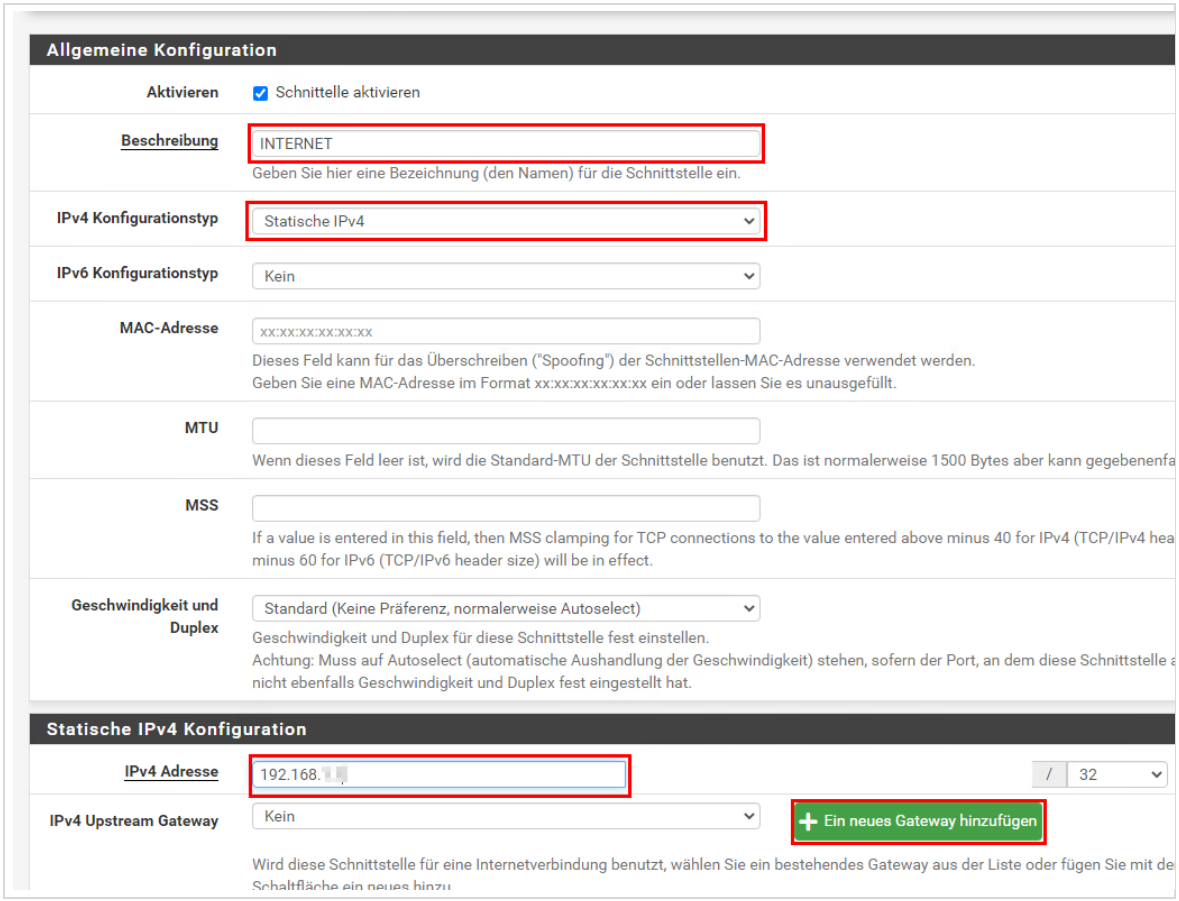

Abb. 109: Einstellen der externen IP-Adresse

Nach Klick auf „*Ein neues Gateway hinzufügen*“ kann das Gateway in der Firewall angelegt werden:

- Setzen Sie den Haken bei „*Standardgateway*
- Vergeben Sie unter „*Gateway Name*“ einen Namen für das Gateway oder übernehmen Sie die Voreinstellung „*INTERNETGW*“
- Tragen Sie unter „*Gateway IPv4*“ die LAN-seitige IP-Adresse des Gateways ein.
- Vergeben Sie unter „*Beschreibung*“ eine Beschreibung für das Gateway (Freitextfeld).
- Speichern Sie die Änderungen durch Klick auf „*Hinzufügen*“.

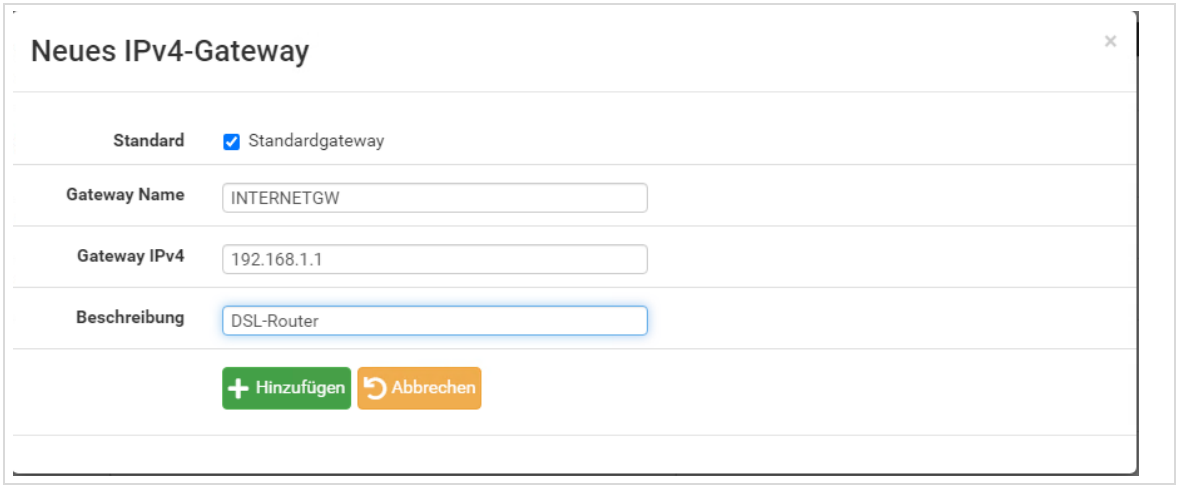

Abb. 110: Anlegen eines neuen Gateways

Nun kann das eben angelegte Gateway ausgewählt werden. Speichern Sie mit Klick auf „*Save*“.

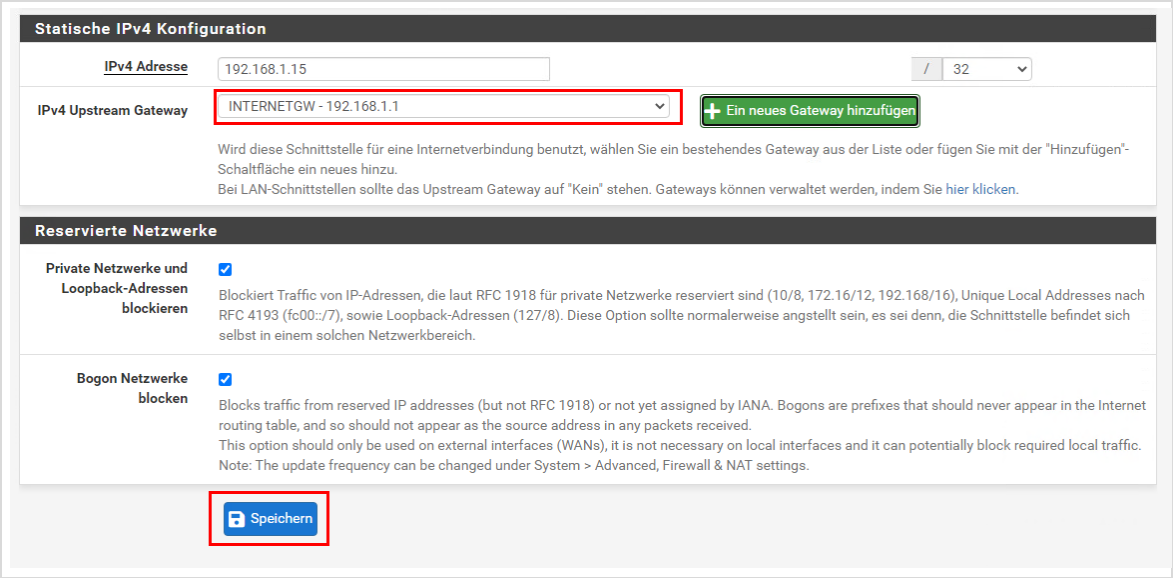

Abb. 111: Eintragen des Gateways

Die neue Konfiguration muss anschließend übernommen werden. Dies geschieht über einen Klick auf „*Änderungen übernehmen*“.

Einstellen der DNS-Server

Wird die IP-Adresse der externen Netzwerkkarte manuell eingetragen, dann müssen die zu verwendenden DNS-Server ebenfalls manuell eingestellt werden. Navigieren Sie dazu auf „*System | Allgemeine Einstellungen*“.

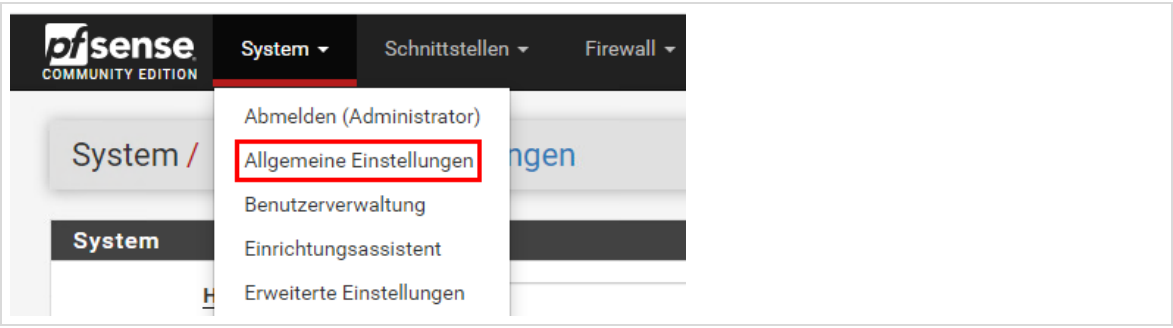

Abb. 112: Navigation zu den Grundeinstellungen der Firewall

Tragen Sie nun die IP-Adressen der DNS-Server in die entsprechenden Felder ein. Wir empfehlen dringend hier einen DNS-basierten Jugendschutzfilter einzutragen, z.B. JusProgDNS oder einen anderen Jugendschutzfilter Ihrer Wahl. Ein HowTo zur Verwendung des JusProgDNS-Jugendschutzfilters kann unter https://www.lmz-bw.de/netzwerkloesung/produkte-paedml/paedml-linux/downloads/#howtos abgerufen werden.

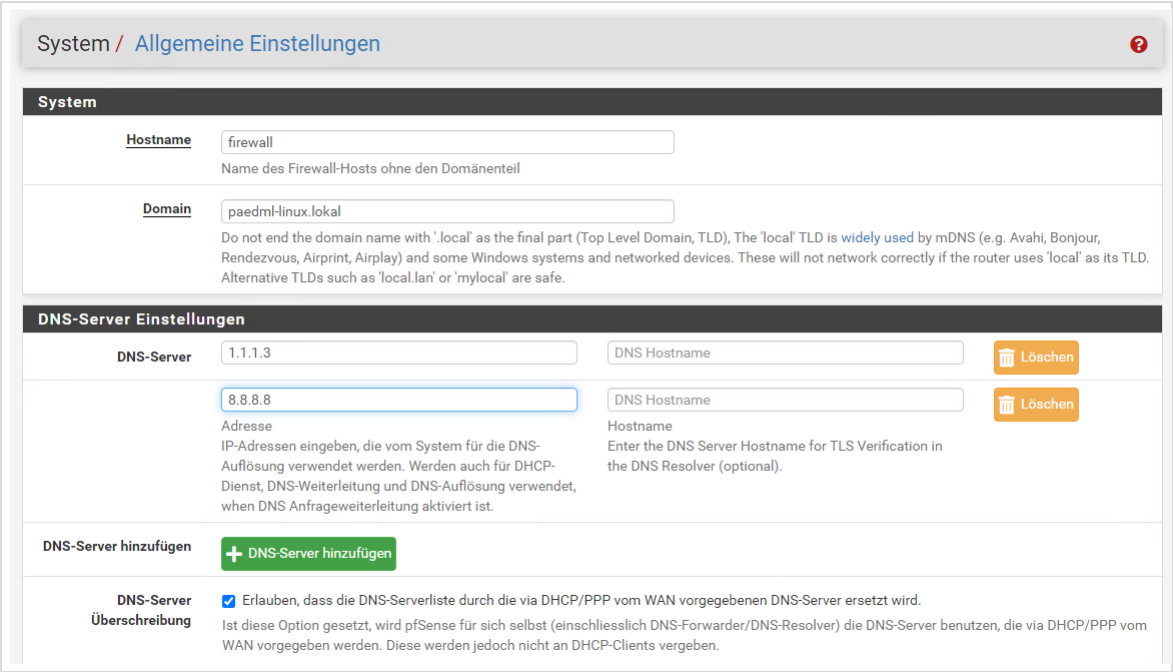

Abb. 113: Eintragen der DNS-Server

Speichern Sie die Einstellungen mit einem Klick auf „Speichern“ ganz unten auf der Seite.

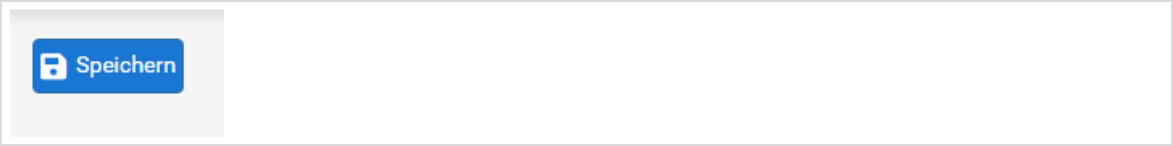

Abb. 114: Speichern

Die Einrichtung der Firewall ist hiermit abgeschlossen. Sie können die Internetverbindung testen, in dem Sie über das *pfSense*-Menü „*Diagnostics | Ping*“ eine Internetseite pingen.

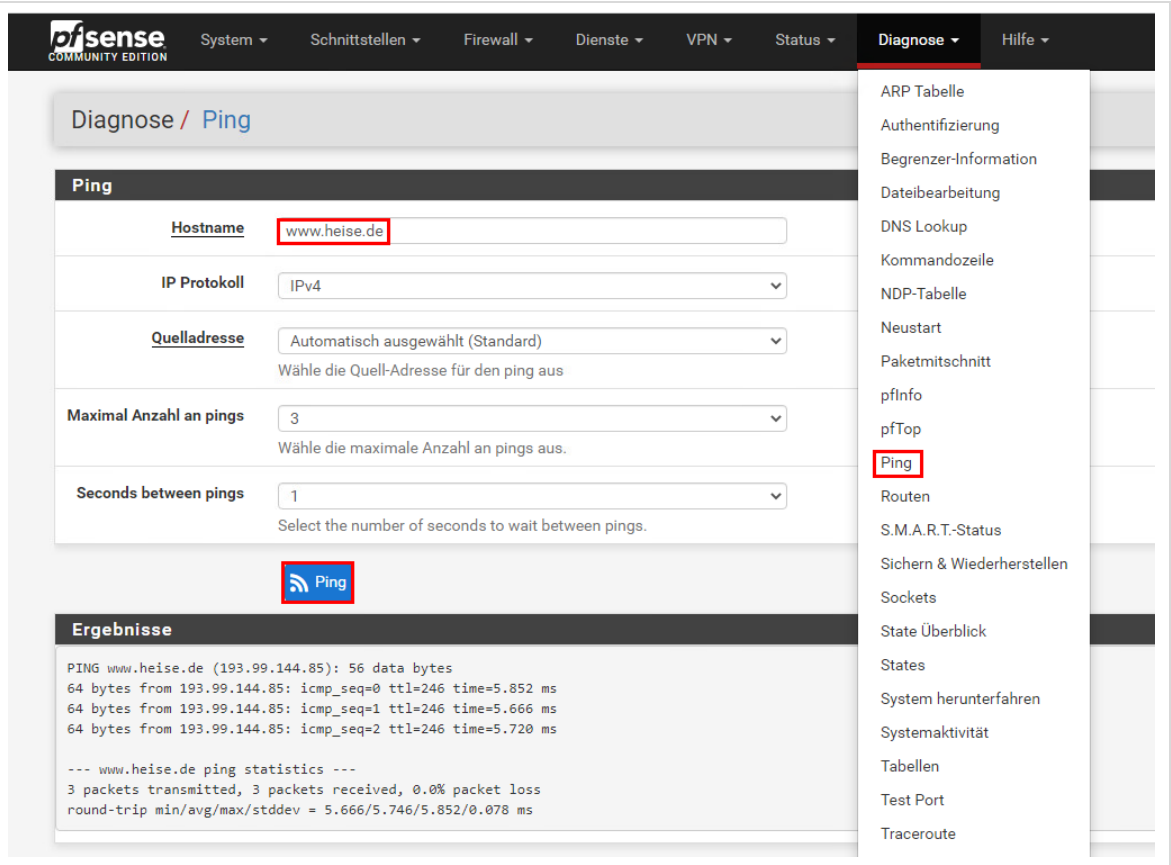

Abb. 115: Erfolgreicher Ping-Versuch auf www.heise.de

5.1.4 Updaten der Firewall

Die in der *paedML Linux* verwendete Firewall-Lösung „*pfSense*“ besitzt einen einfachen Updatemechanismus, mit dem die Software der Firewall (in *pfSense*-Nomenklatur „Firmware“) stets aktuell gehalten werden kann.

Zu Beginn der *paedML Linux*-Installation sollte die Firmware der *pfSense* manuell auf den aktuellen Stand gebracht werden.

Das System ist so konfiguriert, dass es automatisch prüft, ob Aktualisierungen verfügbar sind.

Überprüfen Sie bitte regelmäßig, ob es Aktualisierungen der *pfSense* gibt und installieren Sie diese gegebenenfalls.

5.1.4.1 Updatevariante 1: Web-Oberfläche

Öffnen Sie für das Update der Firewall die Startseite über ein Browserfenster. Sie erreichen die Seite über die URL https://firewall.paedml-linux.lokal.

Melden Sie sich als Benutzer Administrator mit dem zugehörigen Kennwort an.

Auf der Startseite wird angezeigt, wenn Aktualisierungen verfügbar sind („Version * ist verfügbar“). Unter dem „Downloadsymbol“ versteckt sich der Link, der angeklickt werden muss, um das Update anzustoßen.

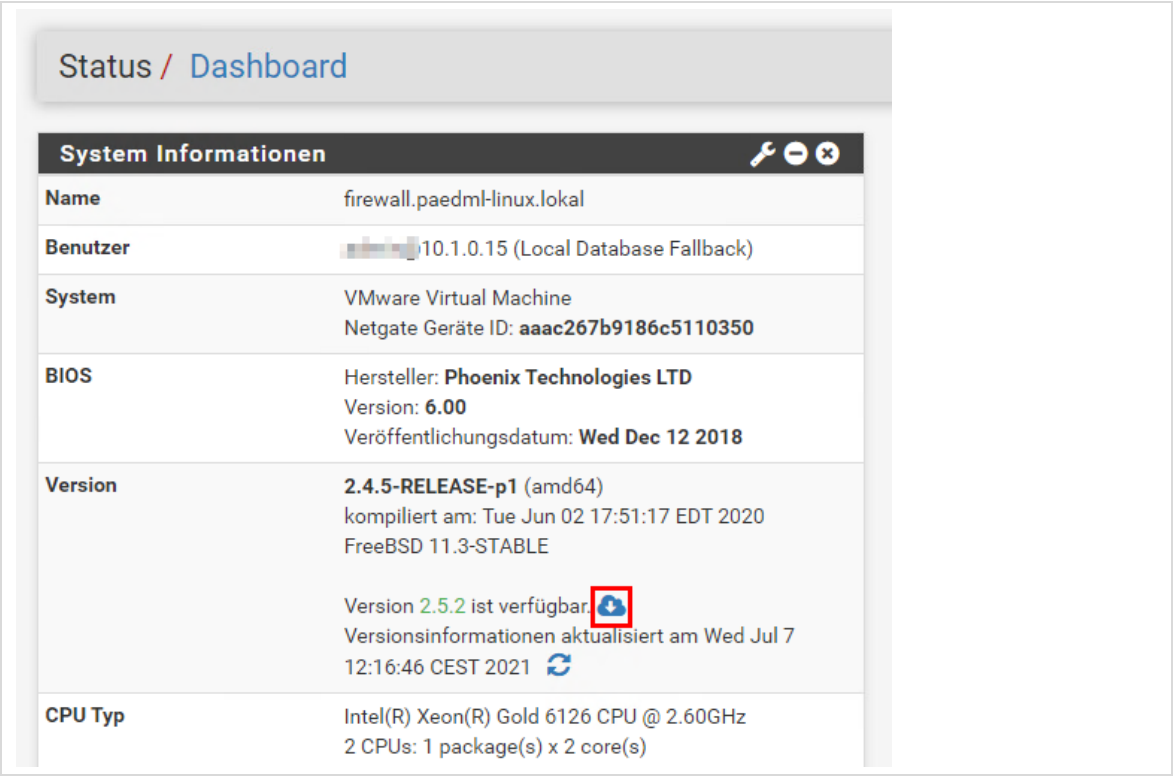

Abb. 116: Aufruf der pfSense-Startseite mit verfügbarem Update

Sollte auf der Startseite der Firewall die Meldung *„Unable to check for updates“* erscheinen, aktualisieren Sie die Firewall über die Konsole. Dies ist im nachfolgenden Kapitel 5.1.4.2 auf Seite 74 beschrieben.

Auf den nächsten Seiten werden Informationen zu dem verfügbaren Update angezeigt. Über den Knopf „*Bestätigen*“ können Sie die Systemaktualisierung starten.

Im Anschluss wird das Update heruntergeladen und installiert. Nach der Installation wird die Firewall neu gestartet.

Schalten Sie die Firewall während des Updatevorgangs auf keinen Fall aus!

5.1.4.2 Updatevariante 2: Konsole

1. Öffnen Sie die Konsole der Firewall im vmware-Host-Client mit einem Rechtsklick auf die Firewall | Konsole | Remotekonsole starten (Um die Remotekonsole nutzen zu können muss die VMRC installiert sein.)

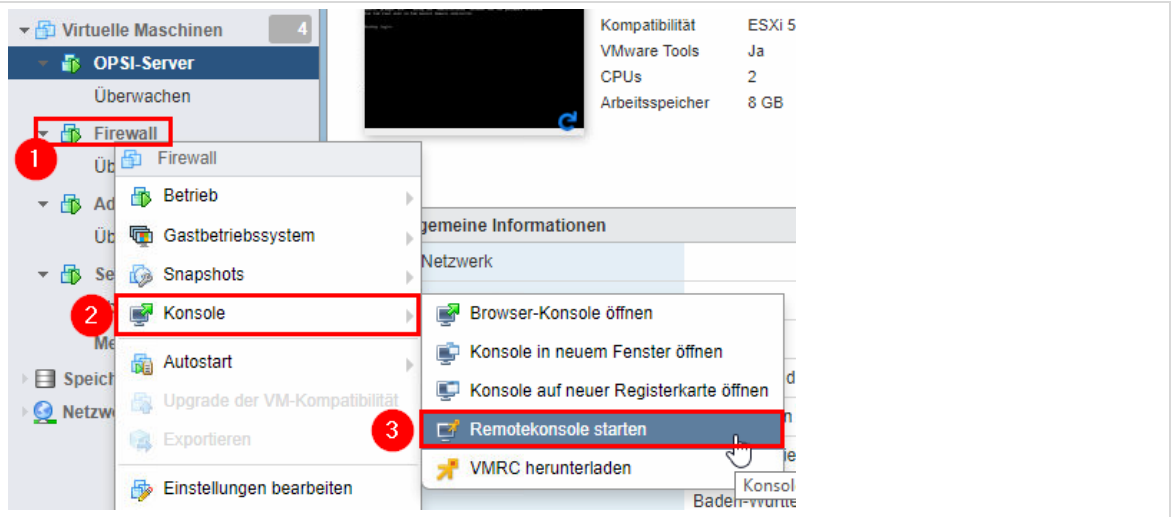

Abb. 117: Die Konsole der Firewall öffnen

2. Tippen Sie danach `13` (Update from console) ein und bestätigen Sie mit der Enter-Taste. Die Firewall wird daraufhin aktualisiert:

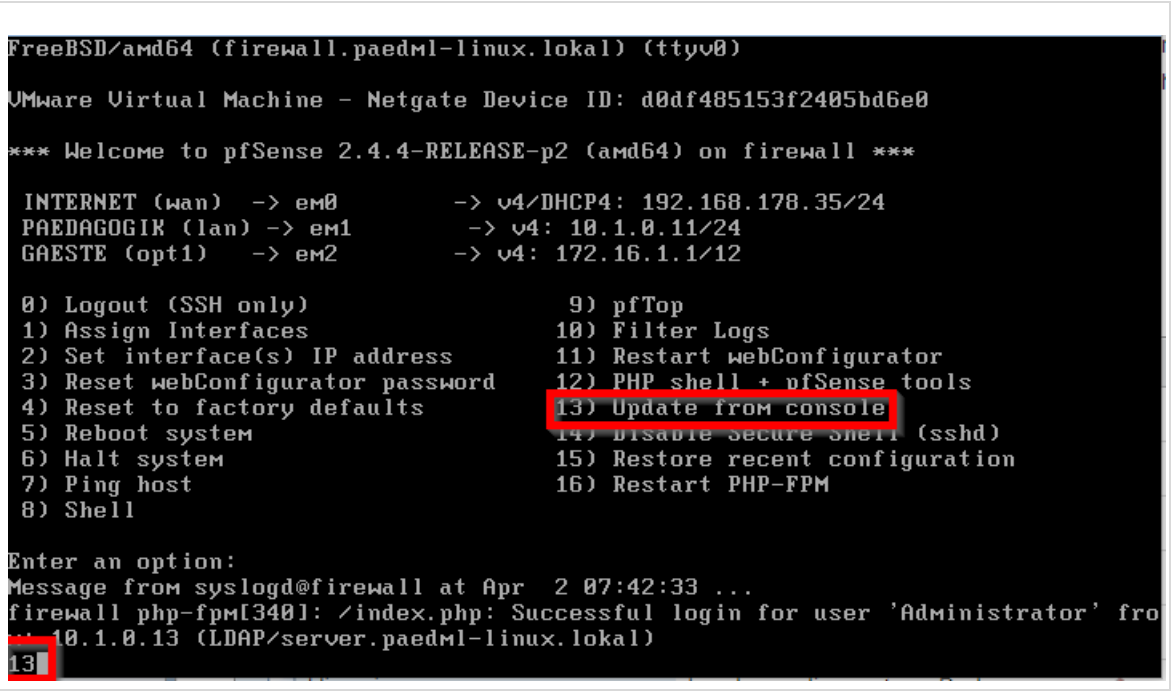

Abb. 118: Die Firewall über die Konsole aktualisieren

5.2 Basiskonfiguration der VM „Server“

Auf der VM „*Server*“ muss nach dem Import die **Systemindividualisierung** durchgeführt werden.

Im Auslieferungszustand sind alle *paedML Linux*-Installationen zunächst vollständig identisch, so sind alle Passwörter auf „*paedmllinux*“ gesetzt.

Für einen sicheren Betrieb muss die *paedML Linux*-Installation individualisiert werden, hierbei werden unter anderem alle Passwörter geändert, die SSH-Schlüssel und SSL-Zertifikate neu generiert sowie weitere sicherheitsrelevante Konfigurationen ausgetauscht.

Bei der Individualisierung werden außerdem Lizenzinformationen, die für den Betrieb der *paedML Linux* notwendig sind, in das System übernommen.

5.2.1 Durchführen der Systemindividualisierung

Die Systemindividualisierung kann nur bei bestehender Internetverbindung durchgeführt werden!

Um Ihren Server einzurichten, benötigen Sie Zugangsdaten, die Sie nach der Bestellung erhalten.

Führen Sie die im Folgenden beschriebenen Arbeitsschritte ausschließlich direkt an der Serverkonsole und NICHT per ssh aus!

1. Melden Sie sich an der Server-Konsole als Benutzer *root* an.
2. Vergewissern Sie sich, dass die virtuellen Maschinen „*opsi-Server*“ und „*Firewall*“ ebenfalls eingeschaltet und per Netzwerk vom Server aus erreichbar sind:
   2.1. Pingen der VM „*opsi-Server*“: `#ping backup.paedml-linux.lokal`
   2.2. Pingen der VM „*Firewall*“: `#ping firewall.paedml-linux.lokal`
3. Vergewissern Sie sich, dass der Server eine Verbindung zum Internet hat: `#ping www.heise.de`
4. Rufen Sie das Skript für den Individualisierungs-Prozess mit dem Befehl `#lmz-initial-setup` auf:

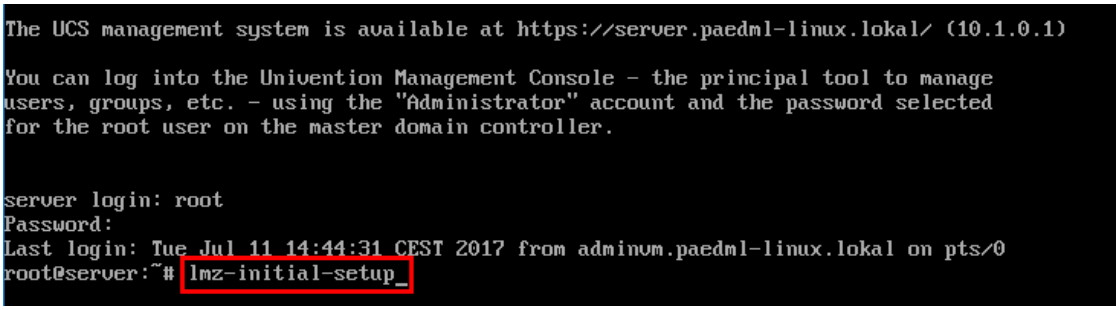

Abb. 119: Start der Systemindividualisierung auf der Konsole des Servers

Das System fragt Sie zunächst nach Ihrer *paedML Linux*-Installationsnummer, die Sie vom LMZ erhalten, und dem dazugehörigen Passwort. Geben Sie diese beiden Werte ein:

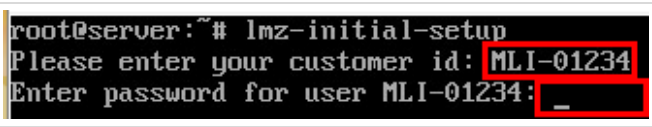

Abb. 120: Abfrage der Installationsnummer

Anschließend werden Sie nach den gewünschten neuen Passwörtern für zentrale Benutzerkonten gefragt. Tragen Sie dort ein **selbst gewähltes Passwort** ein. Dieses Passwort wird für die folgenden Benutzer gesetzt:

- *root* (Server, opsi-Server)
- *Administrator* (Domänen-Administrator, *pfSense*-Administrator, opsi-Administrator)
- *domadmin* (Konto für die Clientaufnahme)

- *netzwerkberater* (administratives Benutzerkonto mit eingeschränkten Rechten)

Abb. 121: Vergabe eines neuen Passwortes für zentrale Benutzerkonten

Nun beginnt der Individualisierungsprozess. Dieser kann einige Minuten dauern, die Ausgabe kann auf der Konsole beobachtet werden:

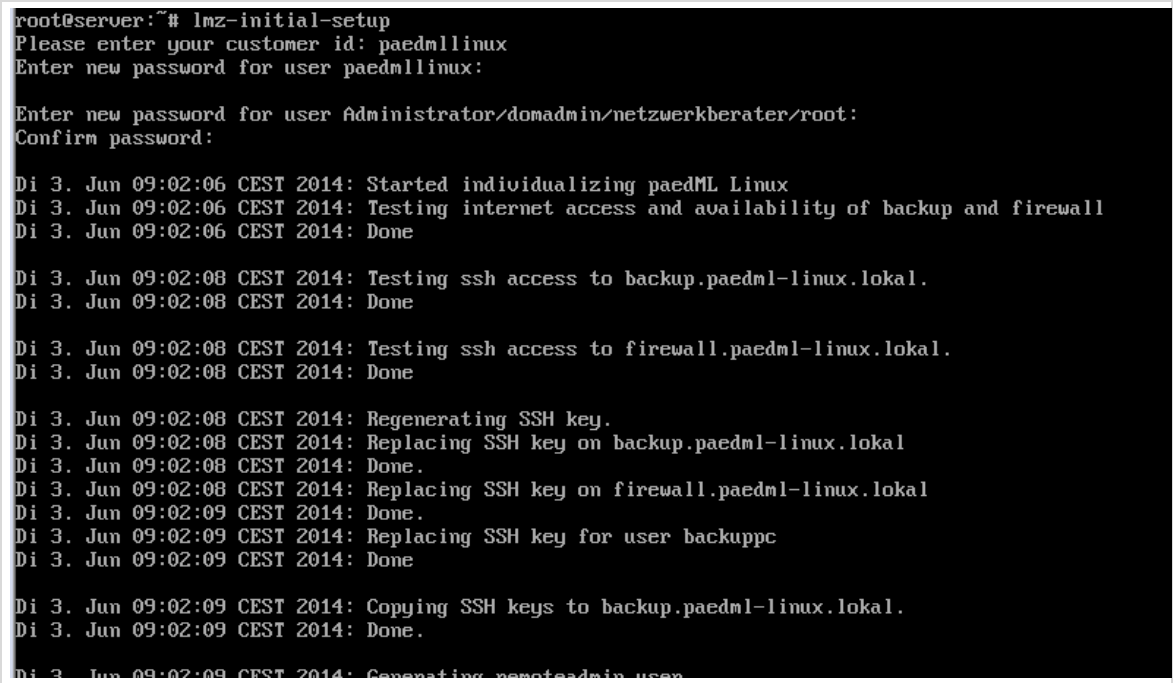

Abb. 122: Die Systemindividualisierung wird durchgeführt

Erfolgreicher Durchlauf

Läuft das Skript erfolgreich durch, so sollten Sie die Meldung „*Finished individualizing paedML*“ sehen.

Wenn diese Meldung nicht erscheint, war die Systemindividualisierung nicht erfolgreich!

Drücken Sie Enter, daraufhin werden alle *paedML Linux* Server neu gestartet.

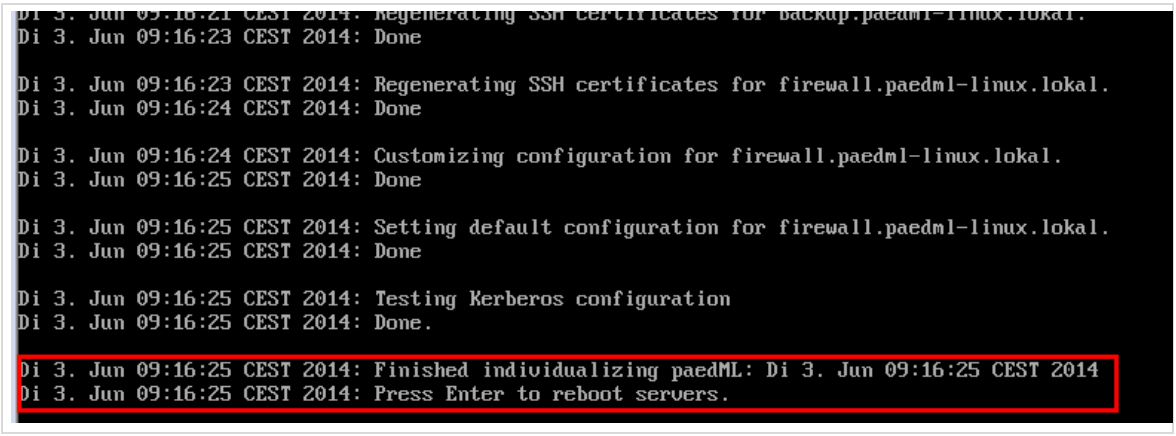

Abb. 123: Erfolgreicher Abschluss des Individualisierungsprozesses mli-04198

Mögliche Fehlerquellen

Falls keine Internetverbindung besteht oder die anderen Maschinen per Netzwerk nicht erreichbar sind, so bricht das Skript mit einer der folgenden Meldungen ab:

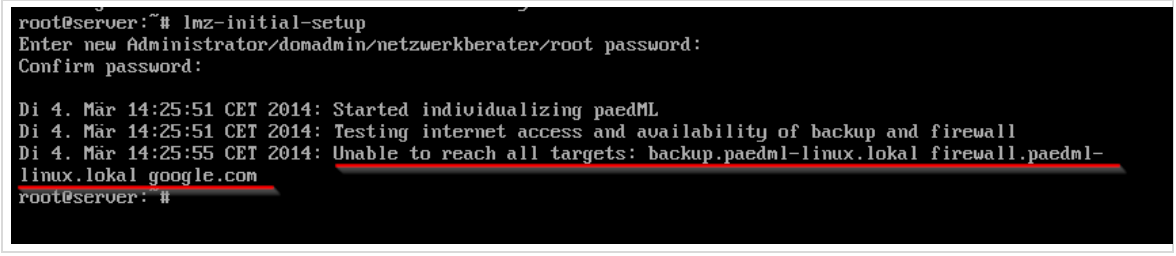

Abb. 124: Abbruch des Individualisierungsprozesses bei fehlender Internetverbindung

Abb. 125: Abbruch des Individualisierungsprozesses

Brechen Sie das ggf. noch laufende Skript mit Strg+C ab. Stellen Sie daraufhin sicher, dass

- alle virtuellen Maschinen eingeschaltet sind,
- die Konfiguration der virtuellen Netzwerke korrekt durchgeführt wurde,
- alle Maschinen sich untereinander mit dem DNS-Namen pingen können,
- vom Server aus eine Internetverbindung besteht.

Starten Sie den Individualisierungsvorgang nach der Behebung möglicher Fehler erneut.

5.2.2 Optional: Ändern des Passwortes von „domadmin“

Dieser Schritt ist notwendig, wenn Sie die Domänenaufnahme von Geräten durch Personen, die nicht Dienstleister oder Netzwerkberater sind, durchführen lassen.

Das Kennwort des Accounts *domadmin* sollte in diesem Fall von den Kennwörtern der Benutzer *root, Administrator* und *netzwerkberater* abweichen!

Da bei der Systemindividualisierung mit `#lmz-initial-setup` alle Kennwörter auf den gleichen Wert gesetzt werden, ist es gegebenenfalls notwendig, das Kennwort des Benutzers *domadmin* zu ändern.

Hier wird nur die Passwortänderung für den Benutzer *domadmin* erklärt.

Im Administratorhandbuch ist die Änderung der Kennwörter administrativer Benutzer beschrieben.

Zum Ändern des domadmin-Passworts gehen Sie wie folgt vor:

1. Melden Sie sich als Benutzer *root* auf der Konsole des Servers an.
2. Rufen Sie das Kommando `#lmz-initial-setup --domadmin` auf.
3. Geben Sie auf Nachfrage das neue Passwort für den Benutzer *domadmin* ein.
4. Geben Sie auf Nachfrage das neue Passwort ein zweites Mal ein.
5. Daraufhin wird das Passwort für den Benutzer *domadmin* geändert. Nach Ablauf des Skripts drücken Sie auf ENTER.
6. In der Regel ist danach – im Gegensatz zur vollständigen Systemindividualisierung – kein Neustart der Server mehr nötig.
7. Melden Sie sich von der Konsole mit dem Befehl `#exit` ab.

5.2.3 Aktualisieren des Basissystems der VM „Server“

Zu Beginn müssen Sie das Basissystem einmalig manuell auf den aktuellen Softwarestand bringen. Spätere Updates werden dann automatisch ausgeführt.

Loggen Sie sich als Benutzer „*root*“ auf der Konsole der VM „*Server*“ ein. Starten Sie den Vorgang mit dem Befehl

```
#univention-upgrade --updateto=4.4-99
```

Es wird eine Liste von aktualisierbaren Paketen angezeigt. Es folgt nochmals eine Abfrage:
„Do you want to continue [Y|n]?“

Bestätigen Sie diese Abfrage durch Eingabe von y und Enter. Darauf werden die aktuellen Updates eingespielt, Dieser Vorgang kann – je nach Größe der Updates und Geschwindigkeit der Internetverbindung – einige Zeit in Anspruch nehmen. Am Ende des Updatevorgangs erscheint wieder der Cursor.

Starten Sie nach dem Update den Server neu, damit alle geänderten Systemdienste neu gestartet werden können.

5.3 Basiskonfiguration der VM „opsi-Server“

Bitte beachten Sie, dass die opsi-Lizenzdatei jährlich erneuert werden muss, da sonst opsi nicht mehr verwendet werden kann. Dies ist im Administratorhandbuch in Kapitel 6.2.1 „Erneuerung des opsi-Lizenzschlüssels“ beschrieben.

Hinweis: Die VM „*opsi-Server*“ wird auf der Konsole unter dem Namen als „*backup*“ angezeigt.

5.3.1 opsi-Lizenzierung

opsi-Lizenzierung im Rahmen der paedML gültig ab 01.08.2022

Seit Sommer 2022 ist neben den opsi-Erweiterungen UEFI, Secureboot, Local Image/WinVHD und Directory Connector auch das mySQL-Backend für paedML Schulen lizenziert.

Jede paedML-Schule erhält vom Landesmedienzentrum Baden-Württemberg jährlich eine Freischaltung bis 500 Clients für Ihren opsi-Server.

Verwaltet eine Schule mehr als 500 Clients mit opsi, so sind für die zusätzlichen Clients opsi-Subscriptionskosten ab dem 501 Client in Höhe von 2 € pro Client / pro Jahr fällig, ab dem 1001 Client 1,5 € pro Client / pro Jahr.

Die Mengen sind in 50er Schritten erweiterbar.

Zusätzliche opsi-Erweiterungen, die nicht in der paedML enthalten sind, können als Subscription ab dem 1. Client zum Subscriptionspreis von 1,5 € pro Client / pro Jahr und ab dem 1001 Client 1 € pro Client / pro Jahr lizenziert werden. Mindestmenge sind hier 500 Clients.

Für ein konkretes Angebot wenden Sie sich bitte an paedml@uib.de.

Voraussetzung ist die Version UCS 4.4-9 errata1233 oder höher.

5.3.2 Aktualisieren des Basissystems der VM „opsi-Server“

Zu Beginn müssen Sie das Basissystem einmalig manuell auf den aktuellen Softwarestand bringen. Spätere Updates werden dann automatisch ausgeführt.

Loggen Sie sich als Benutzer „*root*“ auf der Konsole der VM „opsi-*Server*“ ein. Starten Sie den Vorgang mit dem Befehl

```
#univention-upgrade --updateto=4.4-99
```

Es wird eine Liste von aktualisierbaren Paketen angezeigt. Es folgt nochmals eine Abfrage:
„Do you want to continue [Y|n]?“

Bestätigen Sie diese Abfrage durch Eingabe von y und Enter. Darauf werden die aktuellen Updates eingespielt, Dieser Vorgang kann – je nach Größe der Updates und Geschwindigkeit der Internetverbindung – einige Zeit in Anspruch nehmen. Am Ende des Updatevorgangs erscheint wieder der Cursor.

Starten Sie nach dem Update den opsi-Server neu, damit alle geänderten Systemdienste neu gestartet werden können.

5.4 Basiskonfiguration der optionalen VM „Nextcloud“

5.4.1 Einstellungen der VM Nextcloud bearbeiten

Um die Einstellungen der Maschine anzuzeigen, klicken Sie auf Virtuelle Maschinen, wählen die Nextcloud und klicken auf Aktionen und wählen Einstellungen bearbeiten. Dort können Sie (wenn die Nextcloud VM heruntergefahren ist) die Anzahl der zugewiesenen CPU-Kerne und den Hauptspeicher verändern.

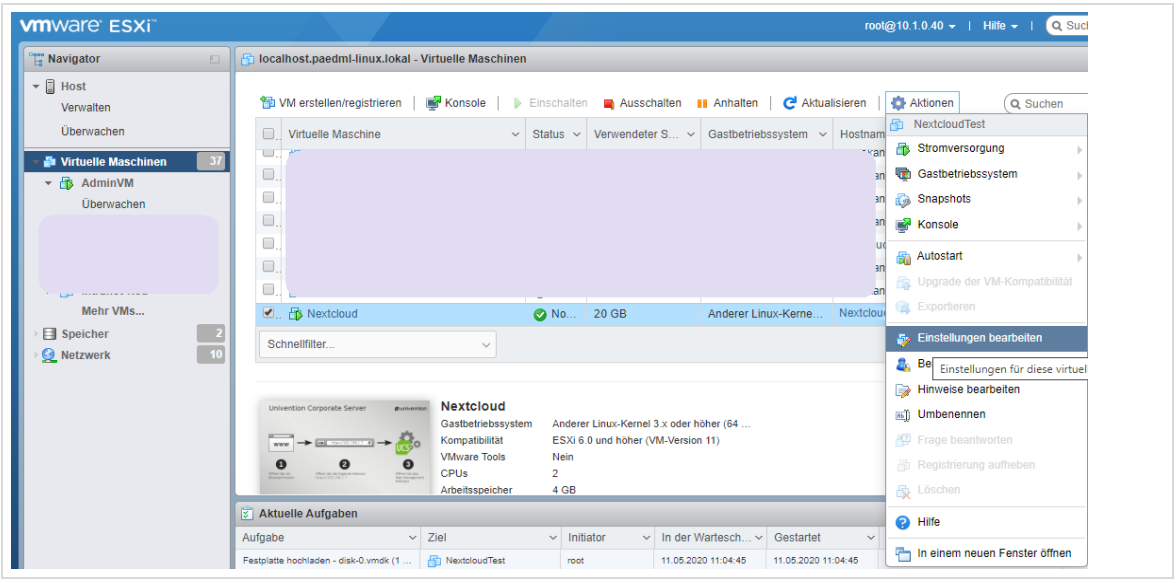

Abb. 126: VM-Einstellungen der Nextcloud anzeigen/bearbeiten

5.4.2 Weitere Konfiguration von Nextcloud

Weitere Informationen zur Konfiguration der VM Nextcloud entnehmen Sie bitte der Nextcloud-Installationsanleitung, die unter https://www.lmz-bw.de/netzwerkloesung/produkte-paedml/paedml-linux/downloads/#manuals für die Version 7.2 zu finden ist.

6 Anpassen der VM „W10AdminVM“

Rolle und Funktion der VM „AdminVM“

Es gibt einige Services für den Betrieb der paedML Linux (z.B. die Windows-Aktivierung, Gruppenrichtlinien), die auf einem Windows-Rechner laufen müssen. Dafür ist die virtuelle Maschine „AdminVM“ vorgesehen. Die AdminVM ist bereits mit Windows 10 Professional 64-Bit installiert und den notwendigen Werkzeugen, wie z.B. VAMT oder RSAT. Einige wenige Anpassungen müssen jedoch noch vorgenommen werden.

6.1 Import der VM aus OVA-Vorlage

Der Import der OVA-Vorlage sollte bereits erfolgt sein, damit steht auf dem Virtualisierungs-Host schon eine virtuelle Maschine bereit.

Falls der Import der OVA-Vorlage noch nicht erfolgt ist, führen Sie die Kapitel 4.4 (Seite 54) beschriebenen Schritte aus.

6.2 Anpassen der MAC-Adresse der Netzwerkkarte

Nach dem Import der *AdminVM* muss noch die MAC-Adresse der Netzwerkkarte auf 00:50:56:00:00:01 geändert werden. Die *AdminVM* muss zunächst ausgeschaltet sein. Klicken Sie dann im vmware-Host-Client mit der rechten Maustaste auf die *AdminVM* und danach auf *„Einstellungen bearbeiten…“*.

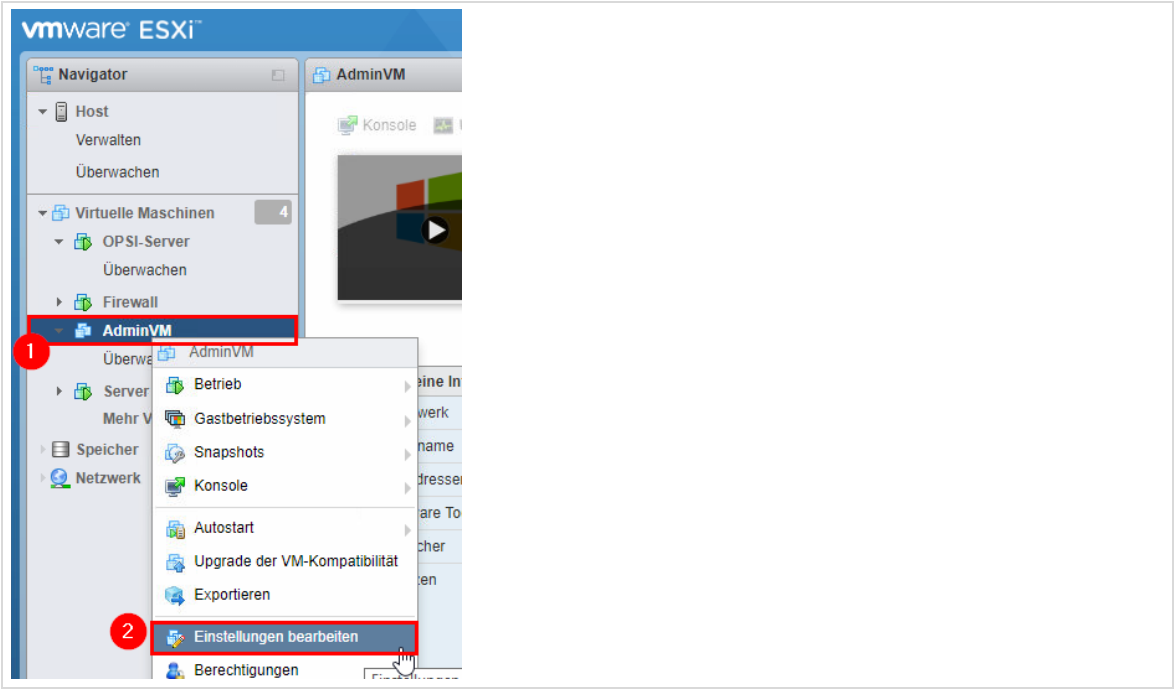

Abb. 127: Einstellungen der AdminVM bearbeiten

Wählen Sie dann den Netzwerkadapter, stellen die MAC-Adresse auf „Manuell“ um (1) und tippen Sie die MAC-Adresse 00:50:56:00:00:01 ein (2). Bestätigen Sie die Einstellungen mit „Speichern“.

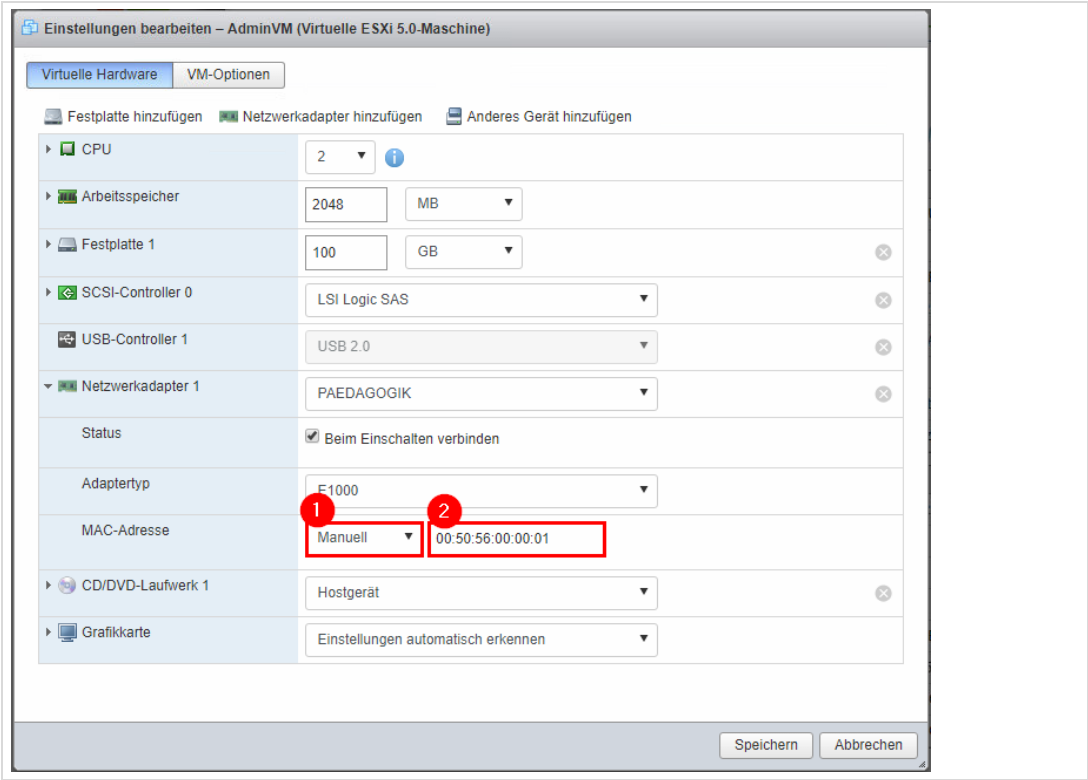

Abb. 128: Ändern der MAC-Adresse

6.3 Integration der AdminVM in die Domäne

Vor dem ersten Hochfahren muss die *AdminVM* in die Domäne *paedml-linux.lokal* aufgenommen werden. Dazu melden Sie sich an der opsi-Server-Konsole als *root* an.

Führen Sie den Befehl *opsi-admin -d method setProductActionRequest windomain adminvm.paedml-linux.lokal setup* aus.

Abb. 129: Der Befehl opsi-admin -d method setProductActionRequest windomain adminvm.paedml-linux.lokal setup

6.4 SSL-Zertifikat installieren

Starten Sie nun die *AdminVM* und melden Sie sich als *Administrator* der Domäne *paedml-linux-lokal* an. Auf der *AdminVM* starten Sie den *opsi config editor*.

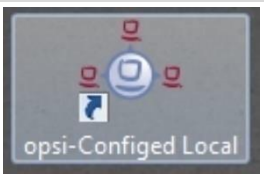

Abb. 130: Symbol des opsi config editor

Klicken Sie auf die AdminVM in der Clientliste (1). Wählen Sie im Reiter „Produktkonfiguration“ das Produkt „zertifikat“ (2) aus und setzen es in der Spalte „Angefordert“ auf „setup“ (3).

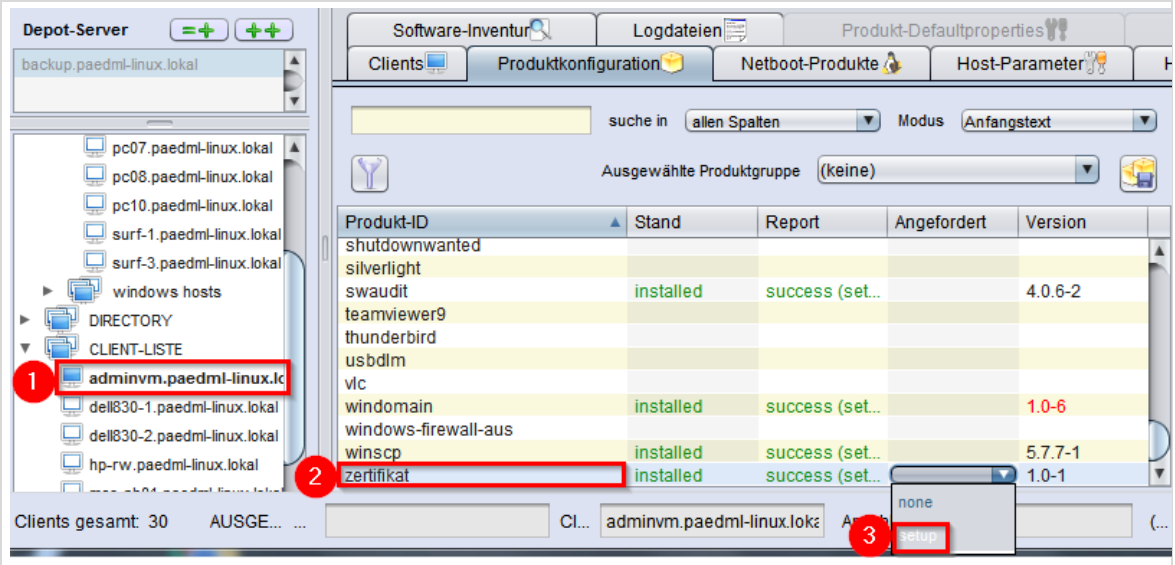

Abb. 131: SSl-Zertifikat auf der AdminVM installieren

Speichern Sie die Konfiguration mit einem Klick auf den roten Haken und starten Sie die *AdminVM* neu.

6.5 RDP-Zugriff auf die W10AdminVM

Es gibt mehrere technische Möglichkeiten, um auf die W10*AdminVM* zuzugreifen

- per vmware-Host-Client
- per Remote Desktop Protocol (RDP)
- per Software von Drittanbietern (z.B. TeamViewer, VNC etc.)

Da RDP standardmäßig auf jedem Windows-Rechner installiert ist, empfehlen wir diesen Weg.

6.5.1 Test des Zugriffs per RDP auf die W10AdminVM

Dieser Schritt ist nicht Teil der Installation. Er kann auch zu einem späteren Zeitpunkt von jedem *Windows*-Rechner im Schul-Netz ausgeführt werden.

Öffnen Sie von demjenigen Rechner, von dem Sie auf die W10*AdminVM* zugreifen wollen, die Remotedesktopverbindung die Suchfunktion von Windows 10.

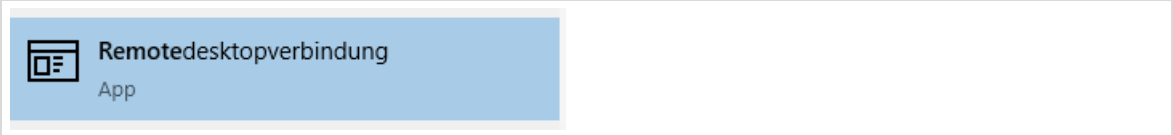

Abb. 132: Remotedesktopverbindung

Tragen Sie im Feld „*Computer*“ den Wert *w10adminvm.paedml-linux.lokal* ein. Sollte dies aufgrund der DNS-Konfiguration fehlschlagen, können Sie alternativ die IP-Adresse *10.1.0.15* eintragen.

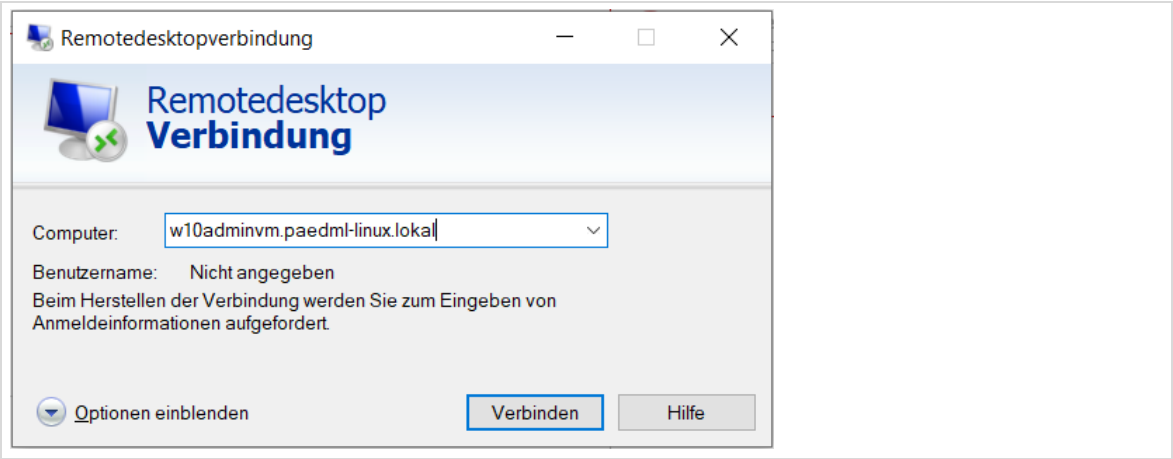

Abb. 133: Aufbau einer Remotedesktopverbindung zur AdminVM

Nun müssen Sie sich an der *AdminVM* authentifizieren. Geben Sie dazu den Benutzernamen *Administrator* (=Domänenadministrator) und das zugehörige Kennwort ein:

Wir empfehlen ausdrücklich, die **Anmeldedaten nicht zu speichern** (Haken nicht setzen!).

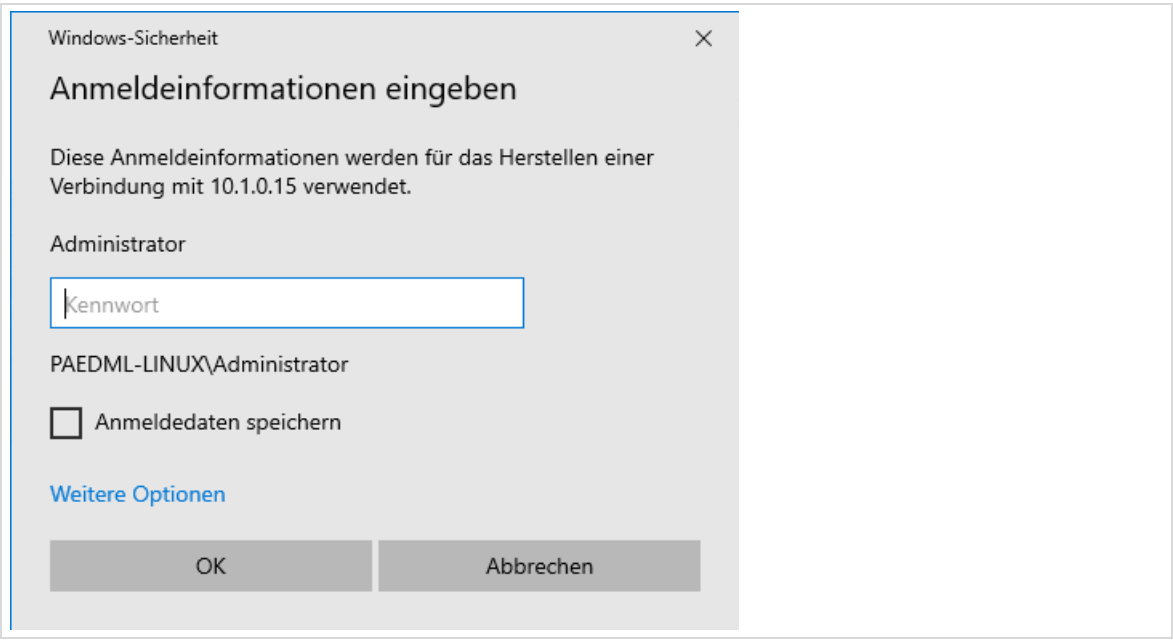

Abb. 134: Anmeldung an der W10AdminVM

Daraufhin sollte der Desktop der *W10AdminVM* in einem Fenster angezeigt werden und Sie können an diesem Rechner arbeiten. Sie beenden die RDP-Sitzung einfach, indem Sie das Fenster schließen.

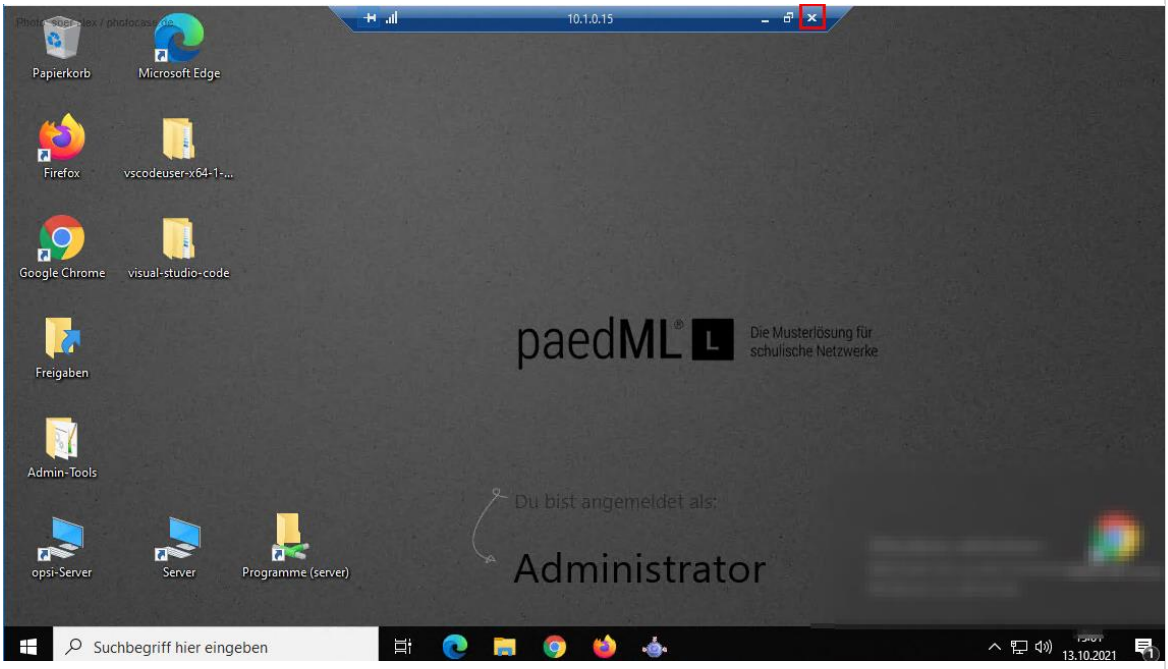

Abb. 135: Zugriff per RDP auf die W10AdminVM

7 Aktualisierung der OPSI-Produkte

7.1 Lizenzierung von OPSI

Melden Sie sich an der AdminVM als *Administrator* der Domäne *paedml-linux.lokal* an.

Die Lizenzierung von OPSI erfolgt mit Hilfe der Datei *opsi-initial-setup.exe*. Diese finden Sie unter auf dem opsi-Server unter \\backup\opsi_depot_rw\update72\Skripte

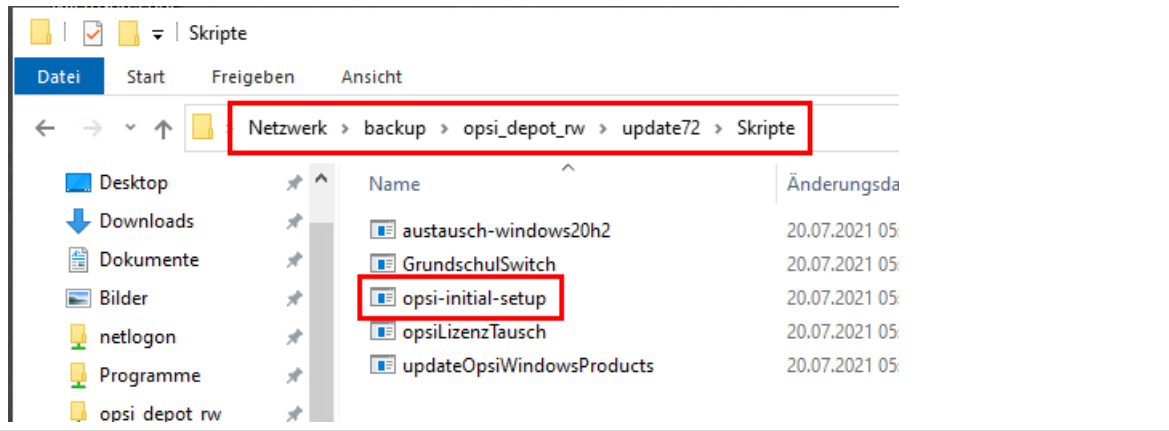

Abb. 136: Aufruf von opsi-initial-setup.ps1

Mit einem Doppelklick auf die Datei starten Sie das Skript. Sie werden durch die einzelnen Schritte geführt.

7.2 Aktualisierung der OPSI-Produkte

Auf der VM „*opsi-Server*" müssen im nächsten Schritt alle *opsi*-Produkte auf den neusten Stand gebracht werden

Melden Sie am opsi-configed als Administrator an. Sie lösen den Updatevorgang mit dem folgenden Befehl aus:

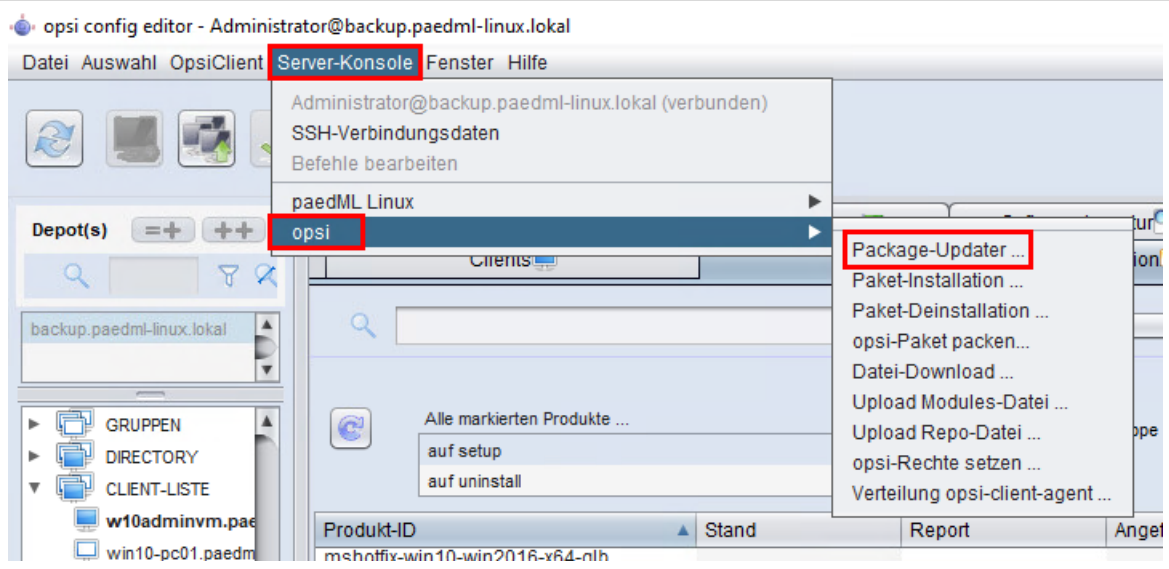

Abb. 137: opsi-Pakete aktualisieren

Durch Eingabe dieses Befehls werden die *opsi* -Produkte auf den neusten Stand gebracht. Dieser Vorgang kann – abhängig von Menge und Größe der Updates und der Internetbandbreite – einige Zeit (auch mehrere Stunden) in Anspruch nehmen.

8 Automatischer Start der virtuellen Maschinen

Die *hier* beschriebenen Schritte für den automatischen Start virtueller Maschinen sollten **UNBEDINGT** ausgeführt werden.

Nur so kann der Server zum Beispiel im Falle eines Stromausfalles ohne Eingriff von außen wieder gestartet werden.

VMware bietet die Möglichkeit, dass virtuelle Maschinen beim Start des Hypervisors automatisch gestartet werden. Dies kann und sollte für den Fall, dass der Server ausgeschaltet wird, eingerichtet werden.

Beispiel-Szenario:

Ein Bagger hat bei Bauarbeiten ein Stromkabel beschädigt, über das die Schule mit Strom versorgt wird. Der Schaden wurde repariert und das Schulnetz soll wieder in Betrieb genommen werden. Der Schulserver (Hypervisor) wird wieder angeschaltet und (im Idealfall) ca. eine Viertelstunde später kann der IT-Betrieb der Schule wieder aufgenommen werden, da die virtuellen Maschinen beim Start des Servers gestartet werden.

Sofern der Autostart nicht konfiguriert wurde, müssen die virtuellen Maschinen von Hand gestartet werden. Dies kann über den *Management-PC* geschehen. Im „schlimmsten Fall“ muss der Dienstleister vor Ort kommen und diese Aufgaben durchführen.

Einrichtung des automatischen Starts

1. Öffnen Sie den *vmware-Host-Client* und melden Sie sich mit Ihren Zugangsdaten an.
2. Wählen Sie im „*Verwalten*“ aus (1).
3. Wählen Sie den Reiter „*System*“ (2).
4. Im Abschnitt „*Autostart*“ (3) wählen Sie den Punkt „*Einstellungen bearbeiten*" (4) aus.
5. Es öffnet sich ein neues Fenster.

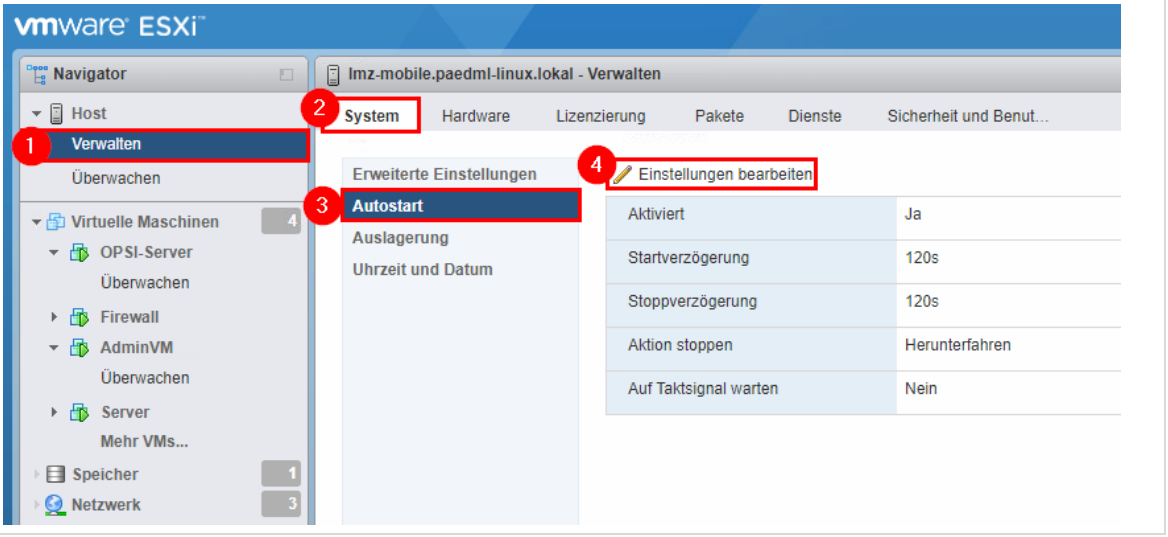

Abb. 138: Konfiguration von automatischem Start der virtuellen Maschinen

6. Hier aktivieren Sie die Option „Ja“ bei „Aktiviert“ und klicken auf „Speichern“.
   Das automatische Starten und Herunterfahren setzt voraus, dass auf den virtuellen Maschinen *„VMware-Tools“* installiert sind.

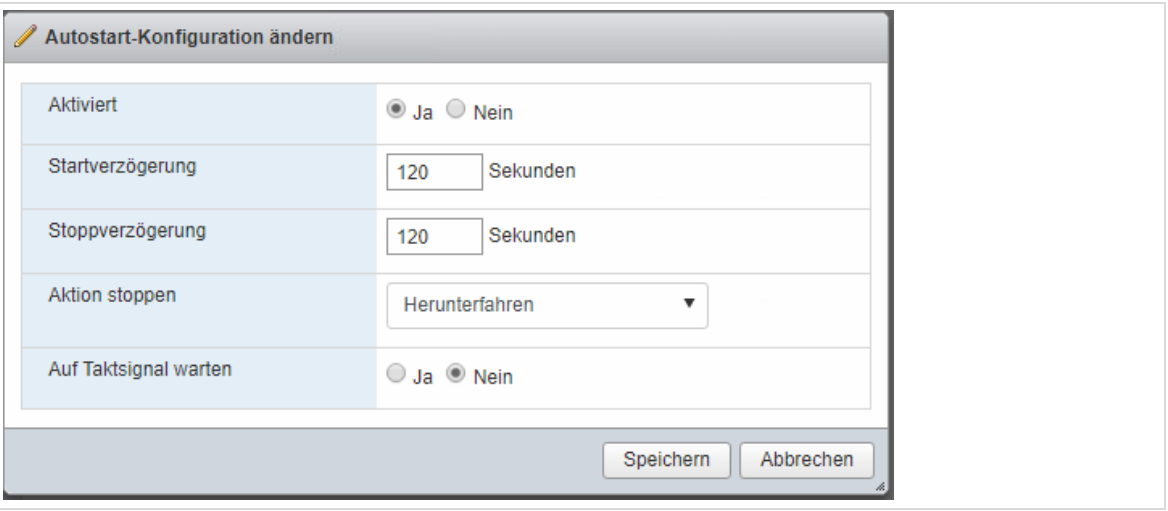

Abb. 139: Konfiguration von automatischem Start der virtuellen Maschinen

7. Aktivieren Sie den Autostart aller virtuellen Maschinen, indem Sie einen Rechtsklick auf die jeweilige Maschine ausführen (1), „Autostart“ auswählen (2) und „Aktivieren“ anklicken (3).

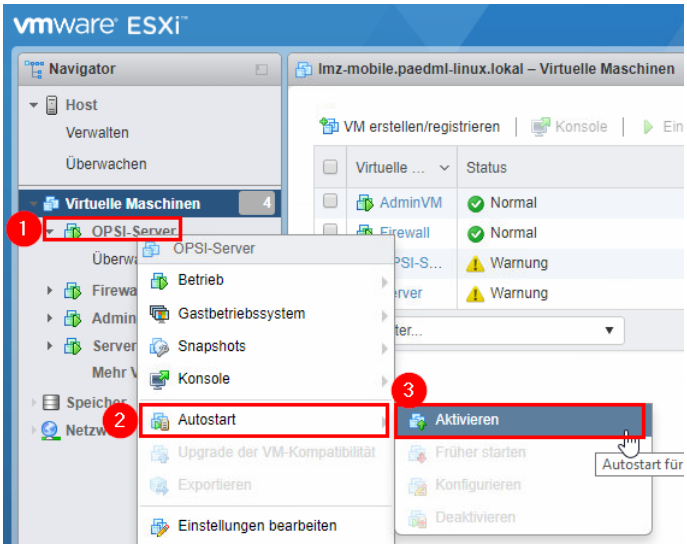

Abb. 140: Konfiguration von automatischem Start der virtuellen Maschinen

8. Abschließend muss die Startreihenfolge der virtuellen Maschinen festgelegt werden. Wechseln Sie hierfür in die Übersicht *„Virtuelle Maschinen“* (1) und wählen Sie die automatisch zu startende virtuelle Maschine aus. In der Spalte „Autostart-Reihenfolge“ wird die Reihenfolge angezeigt, nach der die virtuellen Maschinen gestartet werden (2). Die Reihenfolge kann verändert werden, indem Sie mit der rechten Maustaste auf die virtuelle Maschine klicken und *„Autostart“* auswählen“ (3). Mit *„Später starten“* und *„Früher starten“* können Sie die Position der virtuellen Maschinen in der Liste ändern. Wiederholen Sie den Vorgang für alle automatisch zu startenden Rechner. Die folgende Startreihenfolge muss eingestellt werden:
   - Firewall
   - Server
   - opsi-Server
   - AdminVM
   - (optional:) weitere Server, sofern eingerichtet.

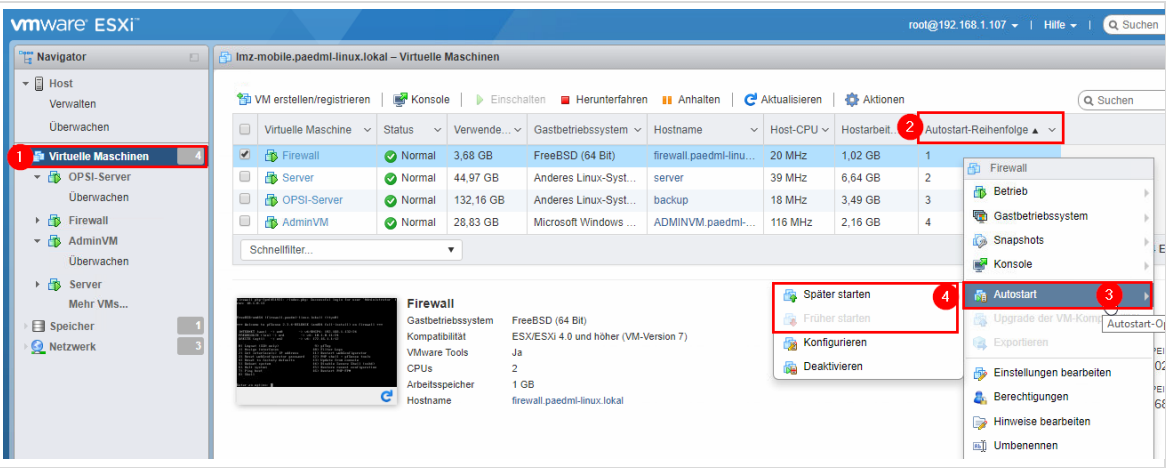

Abb. 141: Konfiguration von automatischem Start der virtuellen Maschinen

9 Starten und Stoppen von virtuellen Maschinen

Zum Starten und Stoppen der virtuellen Maschinen gibt es mehrere Möglichkeiten, die im Folgenden beschrieben werden.

9.1 Starten von virtuellen Maschinen

Der *vmware-Host-Client* bietet eine Vielzahl an Möglichkeiten, eine VM einzuschalten, drei Möglichkeiten sind im Folgenden dargestellt:

- Klick auf „Virtuelle Maschinen“ (1) | virtuelle Maschine auswählen (2) | „Einschalten“ (3)
- Rechtsklick auf die virtuelle Maschine (4) | „Betrieb“ (5) | „Einschalten“ (6)

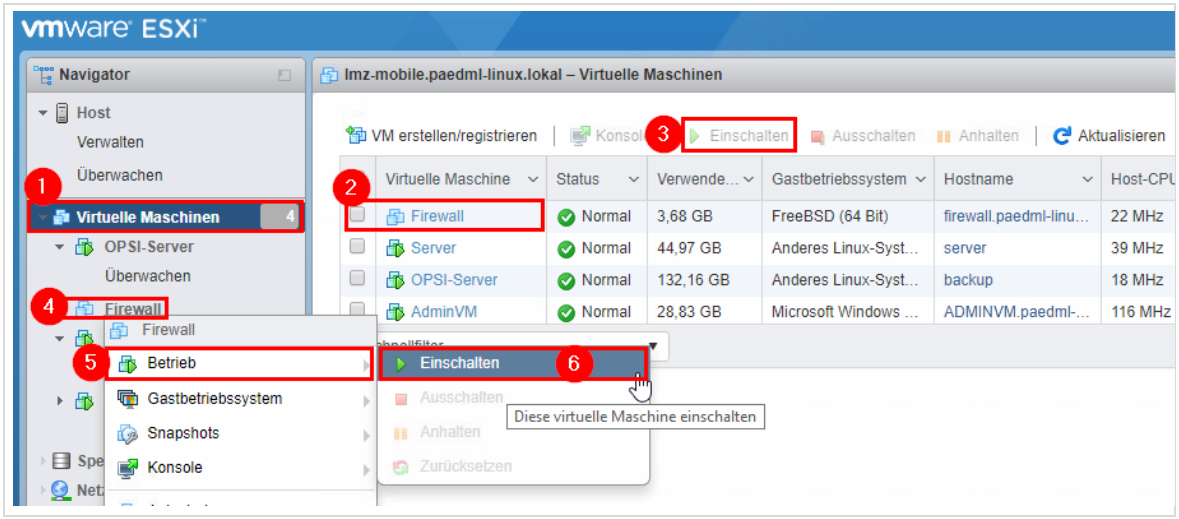

Abb. 142: Möglichkeiten zum Starten einer virtuellen Maschine

- Klick auf die virtuelle Maschine (1) | „Einschalten“ über (2) oder (3).

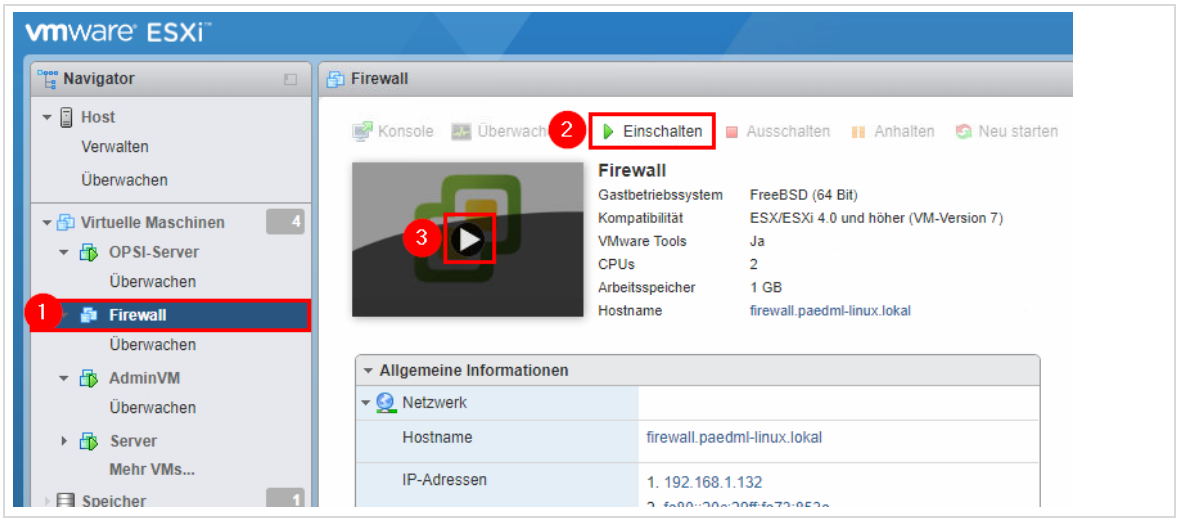

Abb. 143: Möglichkeiten zum Starten einer virtuellen Maschine

9.2 Startreihenfolge

Starten Sie virtuelle Maschinen immer in der folgenden Reihenfolge. Beobachten Sie den Startvorgang und schalten Sie die nächste VM erst dann ein, wenn die vorherige vollständig hochgefahren ist.

- *Firewall*
- *Server*
- *opsi-Server*
- *AdminVM*

9.3 Herunterfahren und Neustart virtueller Maschinen

Für das sichere Herunterfahren der virtuellen Maschinen gibt es - je nach Betriebssystem- verschiedene Methoden. Welche Methode Sie wählen, hängt vom konkreten Einsatzfall ab. Fahren Sie die Maschinen in umgekehrter Startreihenfolge zurück, d.h.

- *AdminVM*
- *opsi-Server*
- *Server*
- *Firewall*

9.3.1 Herunterfahren über die Konsole des Betriebssystems

Falls sie gerade auf der auszuschaltenden VM arbeiten, (Textkonsole bei Server, *ospi*--Server und Firewall, Grafische Konsole bei *AdminVM*) können Sie die VM direkt von der Konsole aus herunterfahren bzw. neu starten. Die Vorgehensweisen sind dabei unterschiedlich:

9.3.1.1 AdminVM (Windows)

Fahren Sie das virtuelle System über die gewohnte *Windows*-Abmeldung herunter.

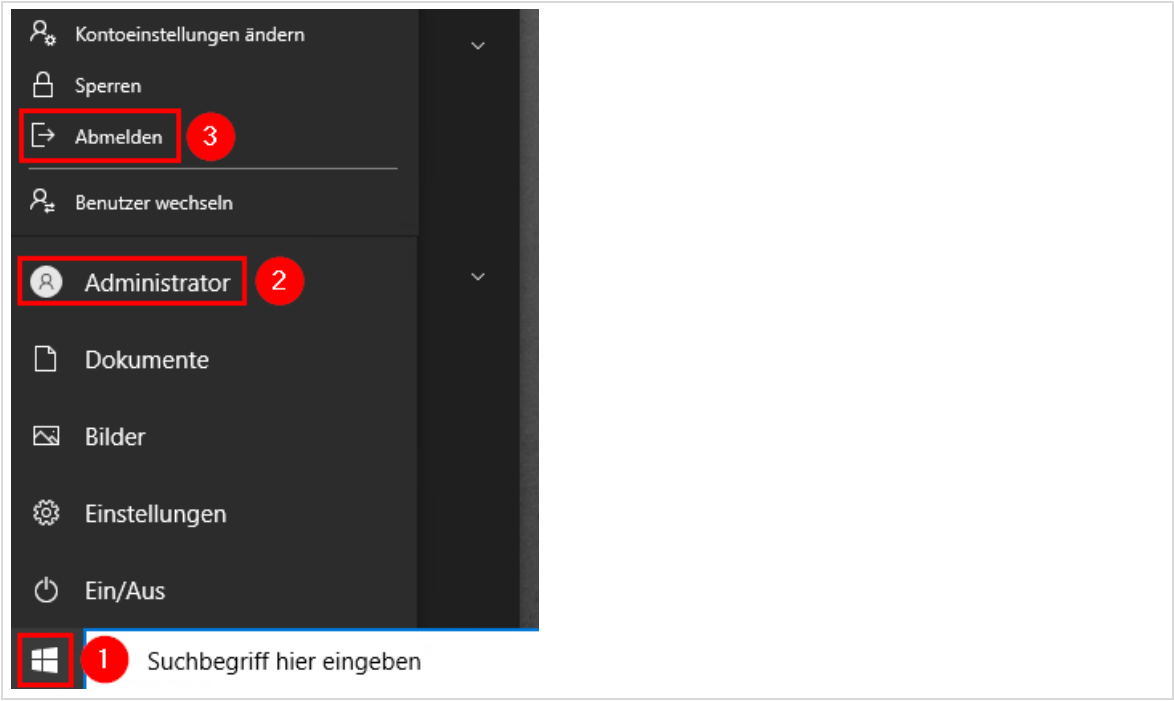

Abb. 144: Normaler Windows Shutdown

9.3.1.2 Server / opsi-Server

Melden Sie sich als root an der Textkonsole an und führen Sie einen der folgenden Befehle aus:

`# poweroff` (Maschine herunterfahren)

`# reboot` (Maschine neu starten)

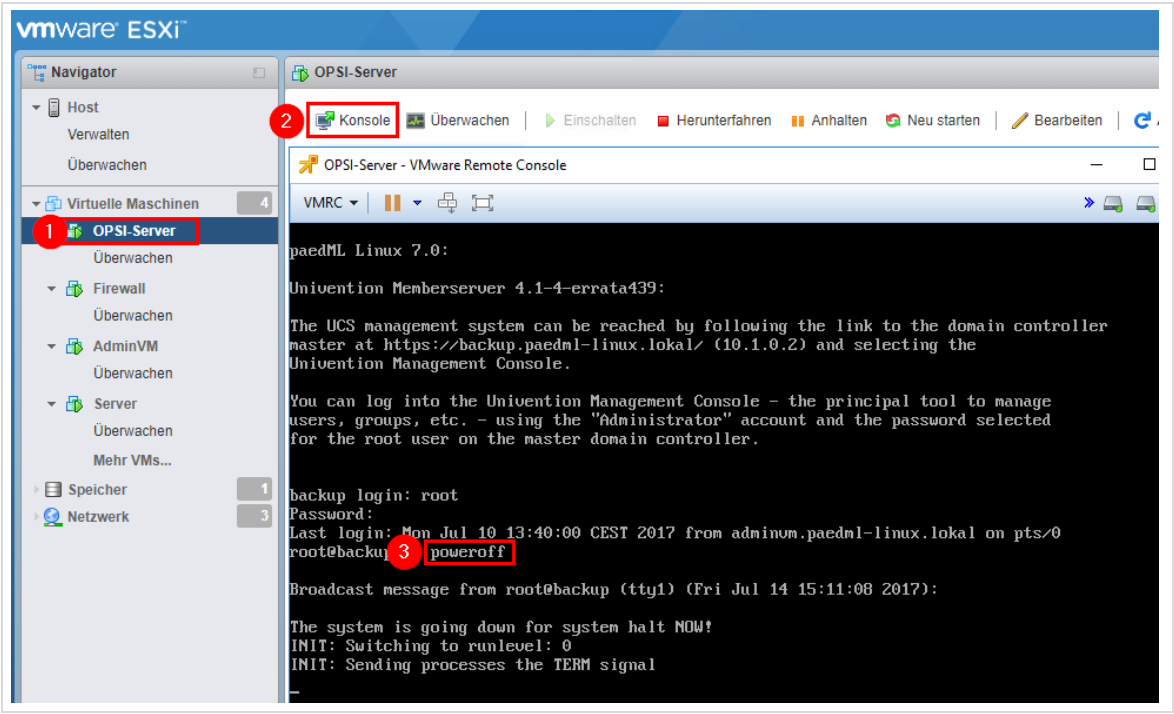

Abb. 145: Herunterfahren der VM Server bzw. OPSI-Server von der Textkonsole aus]

9.3.1.3 Firewall

Wählen Sie auf der Textkonsole der Firewall die Option "*5) Reboot system*" bzw. "*6) Halt system*" und bestätigen Sie die Auswahl mit „*y*“.

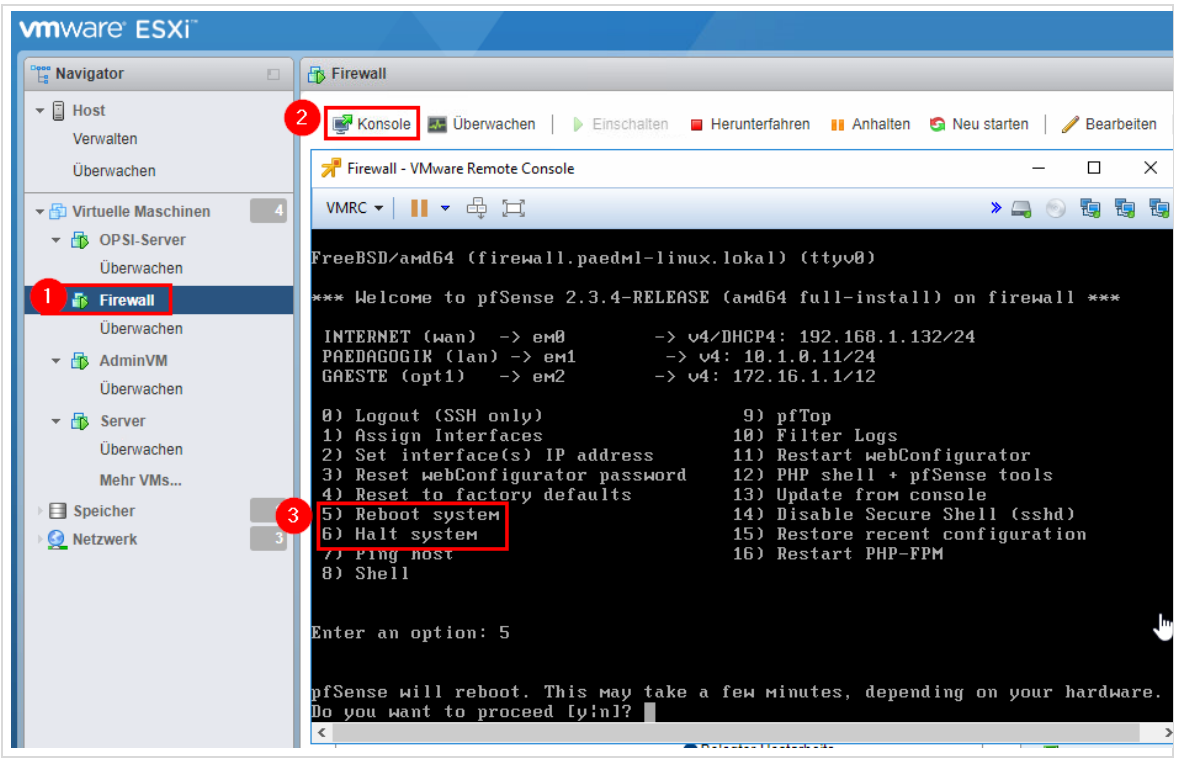

Abb. 146: Herunterfahren der Firewall von der Textkonsole aus

9.3.2 Herunterfahren / Neustart durch vmware-Host-Client

Ein Herunterfahren bzw. ein Neustart kann auch über den *vmware-Host-Client* ausgelöst werden. Die *VMware-Tools* auf der VM sorgen für das Auslösen eines sicheren Shutdowns. Auf den VM „*Server*“, „*opsi-Server*“ und „*Firewall*“ sind die *VMware-Tools* im Auslieferungszustand bereits installiert, auf der VM „*AdminVM*“ müssen die *VMware-Tools* nachträglich installiert werden.

Markieren Sie die VM, klicken Sie auf das „*Stop-Symbol*“ in der oberen Menüleiste. Alternative: Rechtsklick auf die VM, dann *"Betrieb | Gast herunterfahren*".

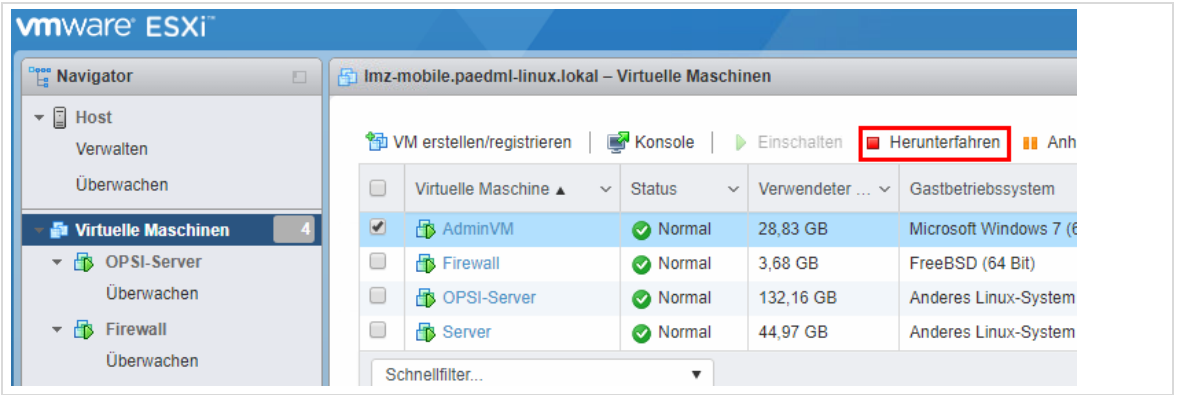

Abb. 147: Gastsystem über Stop-Symbol herunterfahren

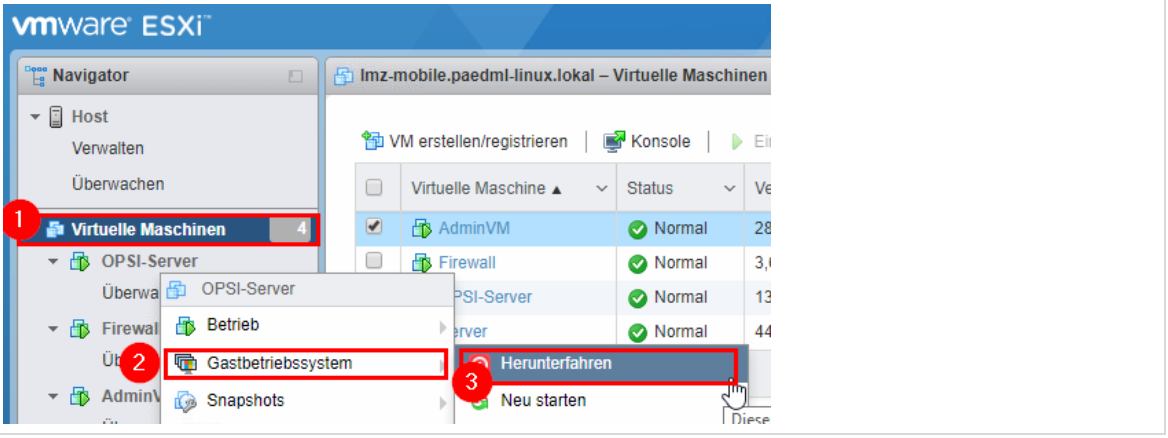

Abb. 148: Gastsystem über Kontextmenü herunterfahren

Für einen Neustart klicken Sie auf das Neustart-Symbol. Alternative: Rechtsklick auf die VM, dann "*Gastbetriebssystem | Neu starten*"

Abb. 149: Gastsystem über Reboot-Symbol neu starten

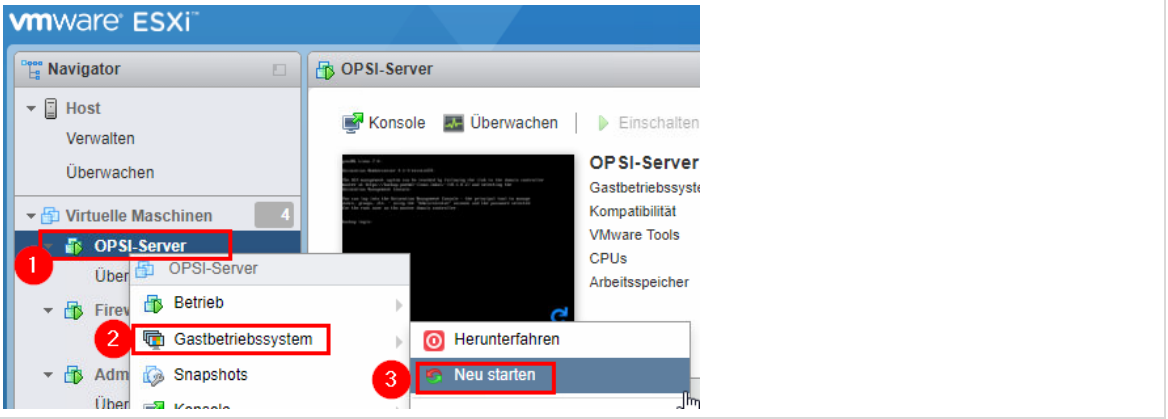

Abb. 150: Gastsystem über Kontextmenü neu starten

9.4 Hartes Ausschalten/ Harter Neustart

ACHTUNG!

Das *„harte Ausschalten“* entspricht der Betätigung eines Ein-Ausschalters bzw. das Ziehen des Netzsteckers und sollte – wenn irgendwie möglich – vermieden werden! Der einzige Grund, eine VM hart

auszuschalten liegt vor, wenn ein sicheres Herunterfahren – z.B. aufgrund eines Systemabsturzes – nicht möglich sein sollte.

Um eine VM hart auszuschalten, klicken Sie mit der rechten Maustaste auf die VM und wählen Sie den Menüpunkt "*Betrieb | Ausschalten*" bzw. "*Betrieb | Zurücksetzen*"

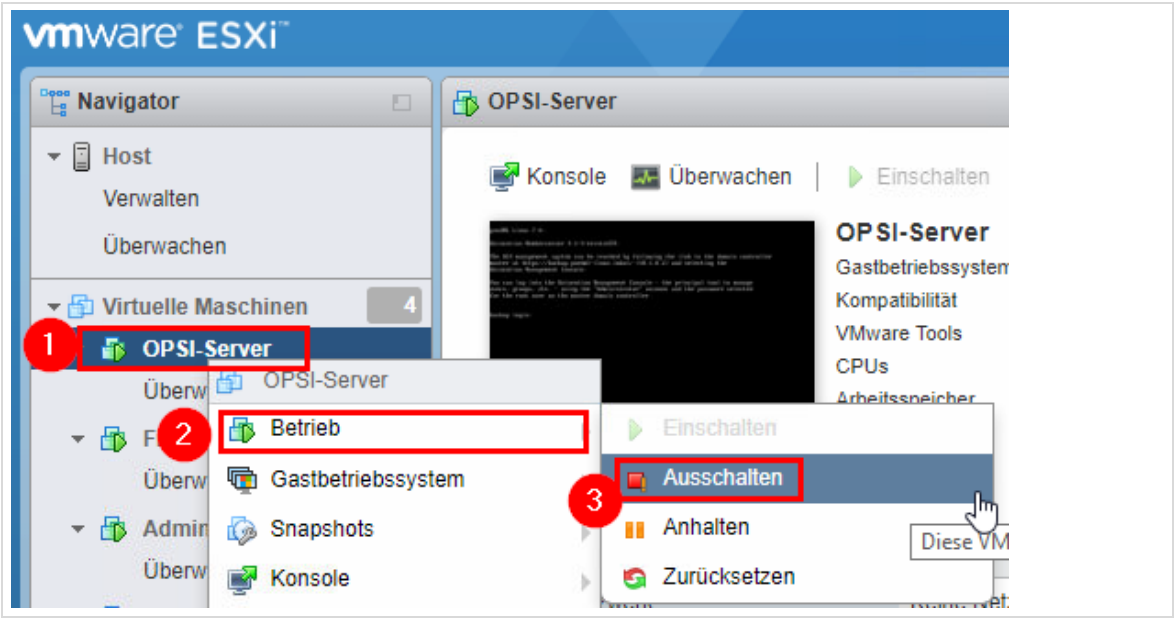

Abb. 151: Harter Shutdown

Abb. 152: Zurücksetzen einer VM

10 Rahmenbedingungen für die Backuplösung

Im Dokument *„Installation und Nutzung von Veeam Backup & Replication“* wird die Vollsicherung des Systems mit *„Veeam Backup & Replication“* beschrieben, sodass im *„Worst Case“* das gesamte System wiederhergestellt werden kann, ohne eine Neuinstallation durchführen zu müssen:

https://www.lmz-bw.de/nc/netzwerkloesung/produkte-paedml/paedml-linux/#howtos

Soll eine Vollsicherung des Systems implementiert werden, sind dort u.a. auch Voraussetzungen beschrieben, die bei der Neuinstallation der *paedML Linux* beachtet werden sollten. Die Integration des Backups kann natürlich auch zu einem späteren Zeitpunkt erfolgen.

Die Sicherung des Systems ist dringend empfohlen!

11 Snapshots der virtuellen Maschinen erstellen

11.1 Grundsätzliche Informationen zu Snapshots

An dieser Stelle kann die Thematik von Snapshots nicht umfassend behandelt werden, für ein tieferes Verständnis verweisen wir auf die Dokumentation des Hypervisors unter https://www.vmware.com/support/pubs/

Ein Snapshot ist das temporäre Abbild einer virtuellen Maschine. Da die virtuellen Maschinen der *paedML Linux* jedoch eine Einheit bilden, sollten Sie unbedingt beim Erstellen von Snapshots der *paedML Linux* Maschinen folgende Hinweise beachten:

- Die virtuellen Maschinen „Server“ und „opsi-Server“ müssen immer gemeinsam gesichert und wiederhergestellt werden. Das Sichern oder auch Wiederherstellen nur einer einzelnen virtuellen Maschine kann zu Dateninkonsistenzen und im schlimmsten Fall zu einem nicht mehr lauffähigen paedML Linux System führen.
- Snapshots dürfen nur angelegt werden, wenn die virtuellen Maschinen ausgeschaltet sind.
- Das Vorhalten vieler Snapshots kann sich eventuell negativ auf die Performance der virtuellen Maschinen auswirken und belegt zusätzlichen Plattenplatz.
- Ein Snapshot ist KEIN ERSATZ FÜR EINE DATENSICHERUNG.

11.2 Erstellen von Snapshots von „Server“ und „opsi-Server“

Herunterfahren der virtuellen Maschinen

Fahren Sie zunächst alle Clients im Netzwerk und die *AdminVM* herunter. Danach fahren Sie die virtuellen Maschinen „*Server*“ und „*opsi-Server*“ kontrolliert herunter, hierzu gibt es drei Möglichkeiten.

1. Über **vSphere-Client:** Rechtsklick im vSphere-Client auf die entsprechende VM, danach Klick auf „*Betrieb | Gast herunterfahren*“.
2. **Über Schulkonsole:** Melden Sie aus einem Browser im Netz „*PAEDAGOGIK*“ (z.B. aus der „*AdminVM*“ als „*Administrator*“ auf der Schulkonsole des Servers („*server.paedml-linux.lokal*“) oder auf der Schulkonsole des *opsi*-Servers („*backup.paedml-linux.lokal*“) an. Wählen Sie im Menü „*System*“ den Untermenüpunkt „*Neustarten*“ aus und im nächsten Fenster die Aktion „*Herunterfahren*“.
3. **Über Textkonsole:** Anmelden als Benutzer „*root*“ auf der Konsole der VM „*Server*“ bzw. „*opsi-Server*“, dann „`poweroff`“ ausführen.

Vom „harten Ausschalten“ aus dem *vSphere-Client* heraus über „*Betrieb | Ausschalten*“ sollte unbedingt abgesehen werden, da Datenverlust möglich ist!

Erstellen des Snapshots der VM „Server“

Rechtsklick auf die virtuelle Maschine „*Server*“, Auswahl von „*Snapshot* | *Snapshot erstellen…*“

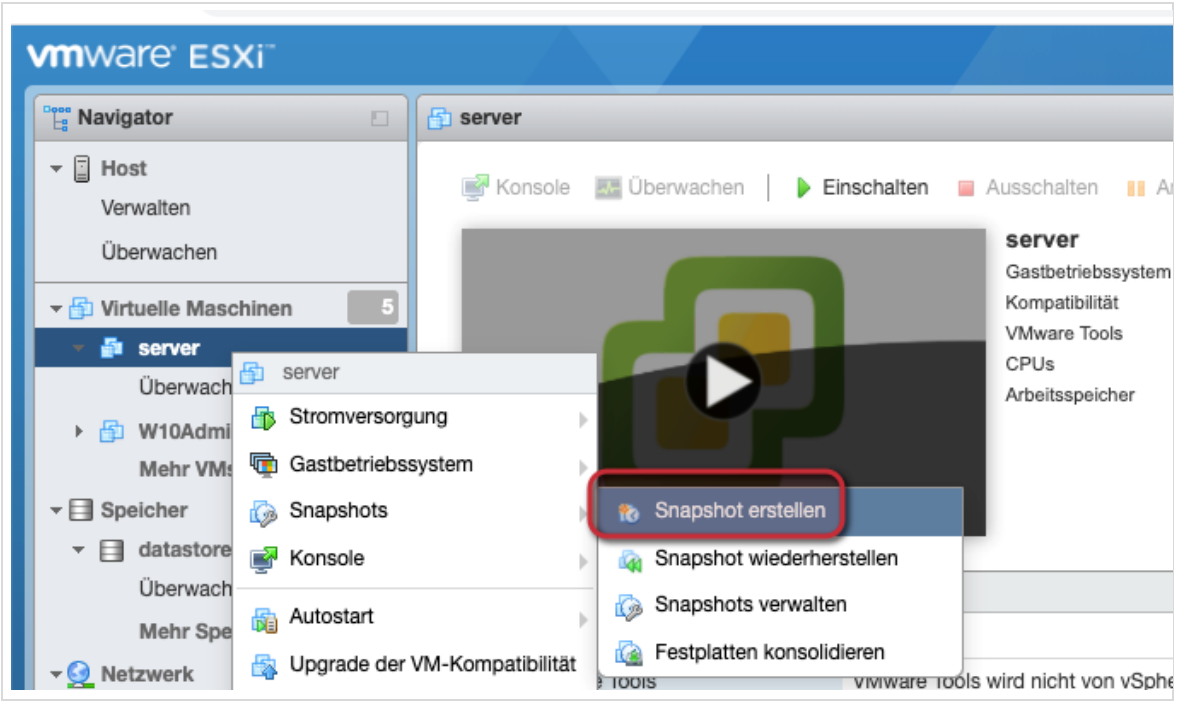

Abb. 153: Erstellen eines Snapshots der VM „Server“

Vergeben Sie einen aussagekräftigen Namen für den Snapshot sowie eine ausführliche Beschreibung und starten Sie den Vorgang mit „*OK*“. Der Snapshot wird anschließend erstellt.

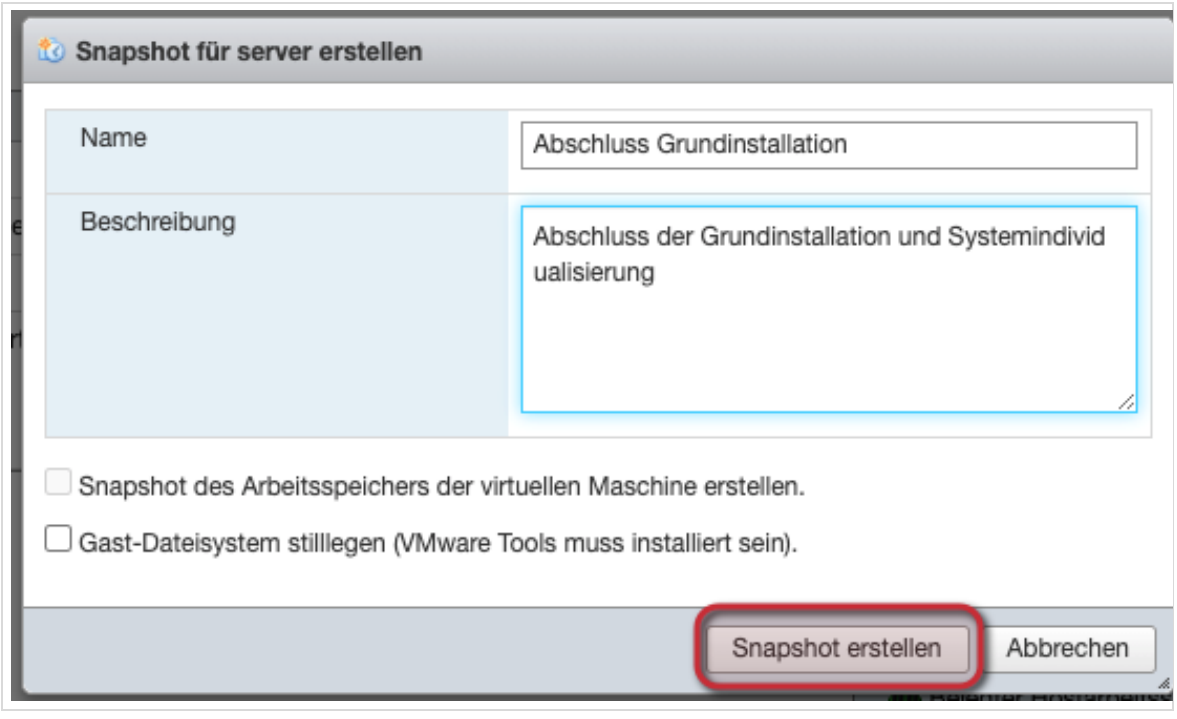

Abb. 154: Name und Beschreibung des Snapshots angeben.

Erstellen des Snapshots der VM „opsi-Server“

Erstellen Sie auf gleiche Art und Weise einen Snapshot der VM „*opsi-Server*“. Vergeben Sie dabei ebenfalls einen aussagekräftigen Namen und eine ausführliche Beschreibung. Empfohlen wird

außerdem, die Namen der Snapshots anzupassen, um später den gleichen Versionsstand der zusammengehörenden Snapshots wiederherzustellen. Dies kann beispielsweise über einen Zeitstempel im Namen des Snapshots geschehen.

Beispiele für Namen von Snapshots:

- Server-2021-07-09-UCS43
- Opsi-Server-2021-07-09-UCS43

Der Fortschritt der Snapshots kann im unteren Bereich des *vSphere-Clients* beobachtet werden.

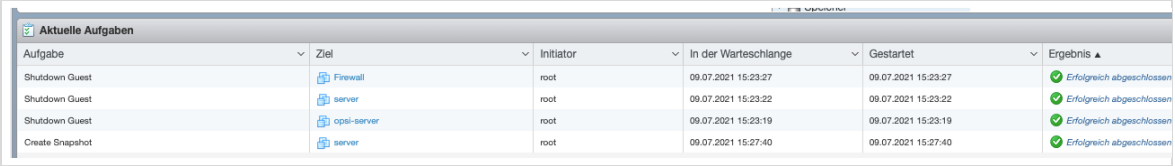

Abb. 155: Snapshot einer virtuellen Maschine wird erstellt.

Wenn beide Snapshots angelegt sind, wird dies wie folgt im *vSphere-Client* angezeigt:

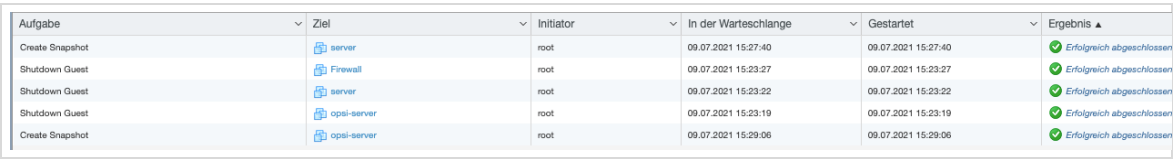

Abb. 156: Anlegen der Snapshots ist abgeschlossen

Hochfahren der virtuellen Maschinen

Fahren Sie abschließend zuerst die VM Server und danach die VM opsi-Server wieder hoch.

11.3 Snapshots der Firewall

Erstellen Sie einen Snapshot der VM Firewall wie oben beschrieben. Eine zeitlich gemeinsame Sicherung bzw. Wiederherstellung mit den Maschinen „Server“ bzw. „opsi-Server“ kann erfolgen, ist jedoch nicht notwendig.

11.4 Snapshots weiterer virtueller Maschinen (z.B. AdminVM)

Für eventuell weitere im System befindliche Maschinen (z.B. „*AdminVM*“) können natürlich ebenfalls Snapshots angelegt werden. Dies ist optional, aber empfohlen. Snapshots der *AdminVM* können auch zeitlich unabhängig von den Maschinen „*Server*“ und „*opsi-Server*“ angelegt und wiederhergestellt werden.

11.5 Wiederherstellen eines Snapshots

Beim Wiederherstellen eines Snapshots werden die virtuellen Maschinen „*Server*“, „*opsi-Server*“ und „*Firewall*“ vollständig auf den Stand des Erstellungszeitpunkts des Snapshots zurückgesetzt. Die beiden Maschinen „*Server*“ und „*opsi-Server*“ können nur zusammen wiederhergestellt werden. Dies setzt voraus, dass von beiden Maschinen Snapshots zum gleichen Zeitpunkt angefertigt wurden.

Achtung, potenzieller Datenverlust!

Beim Wiederherstellen eines Snapshots werden sämtliche System-Einstellungen und Benutzerdaten auf den Stand des Snapshots zurückgesetzt.

Nach Erstellung des Snapshots geänderte Daten (neu angelegte/geänderte Dateien von Benutzern, geänderte Benutzerkonten, Konfigurationsänderungen am System, Änderungen von Benutzerpasswörtern,…) gehen verloren.

Herunterfahren der beiden virtuellen Maschinen

Fahren Sie die beiden virtuellen Maschinen „*Server*“ und „*opsi-Server*“ herunter.

Optional: Anlegen eines Snapshots

Da der aktuelle Zustand der virtuellen Maschinen beim Wiederherstellen eines anderen Snapshots unwiederbringlich verloren geht, sollte an dieser Stelle überlegt werden, ob das Anlegen eines neuen Snapshots vor der Wiederherstellung eines alten Snapshots sinnvoll ist.

Wiederherstellen eines Snapshots der VM „Server“

Klicken Sie im vSphere-Client mit Rechts auf die VM „Server“ und wählen Sie „Snapshots | Snapshot verwalten:

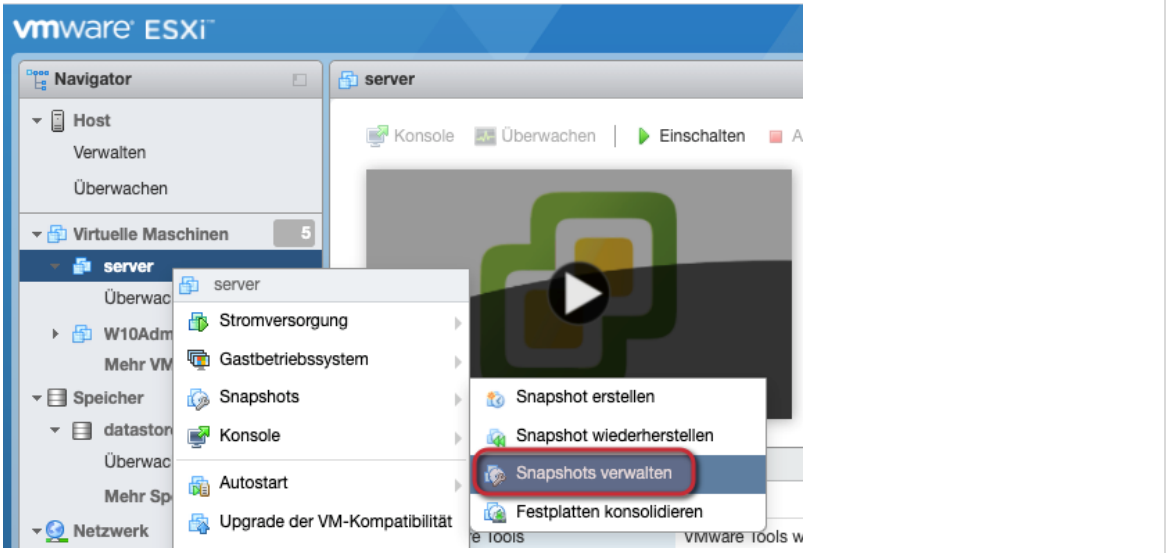

Abb. 157: Öffnen des Snapshot-Managers

Wählen Sie nun denjenigen Snapshot aus, auf den Sie zurückwechseln möchten und klicken Sie auf *„Snapshot wiederherstellen“:*

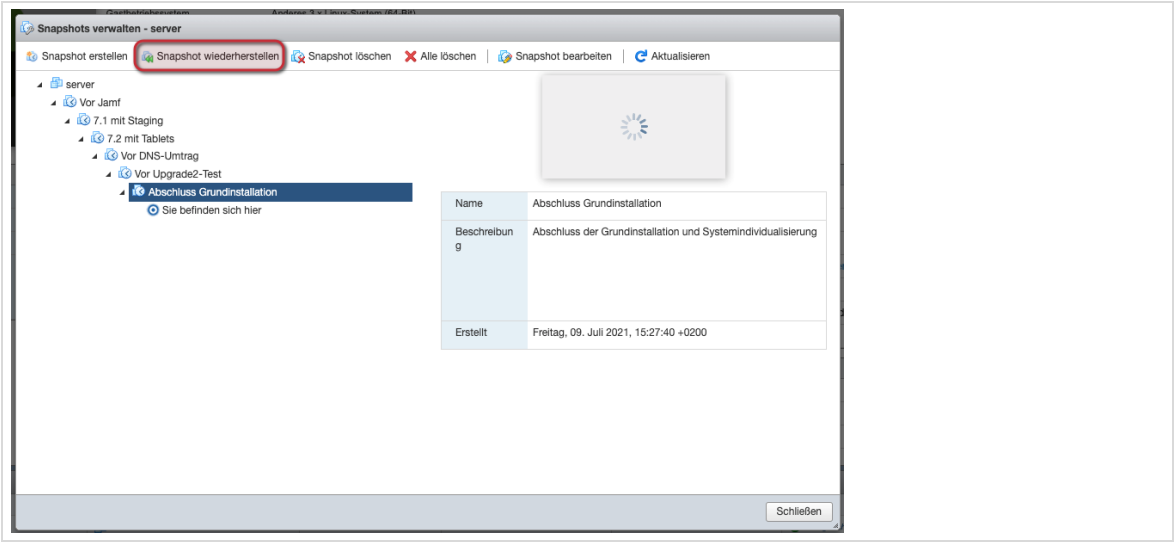

Abb. 158: Auswahl eines angelegten Snapshots

Bestätigen Sie die Sicherheitsabfrage, um die Wiederherstellung des Snapshots anzustoßen.

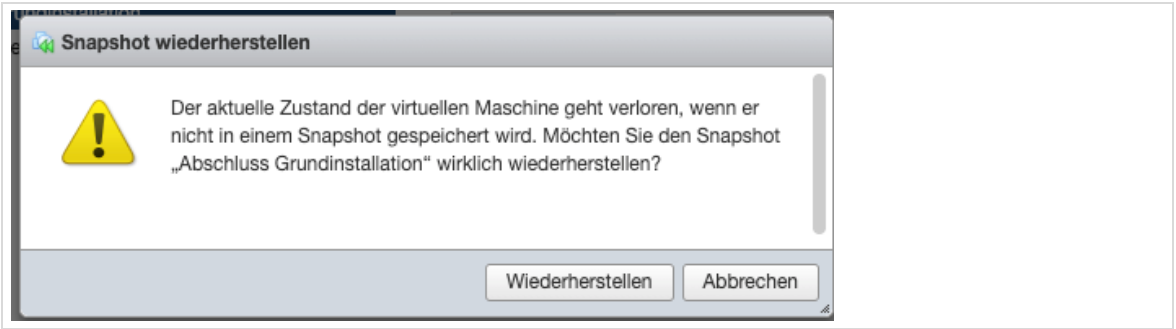

Abb. 159: Sicherheitsabfrage vor dem endgültigen Wechsel zu einem früheren Snapshot

Schließen Sie das Fenster des Snapshot-Managers über den Knopf „*Schließen*“

Stellen Sie anschließend den Snapshot der VM „*opsi-Server*“ wieder her. Achten Sie darauf, dass sie den zur VM „*Server*“ passenden Snapshot auswählen.

Hochfahren der virtuellen Maschinen

Fahren Sie anschließend beide Maschinen wieder hoch.

Optional: Domänenmitgliedschaft der Clients wiederherstellen

Beim Wiederherstellen der virtuellen Maschinen kann es vorkommen, dass Clients ihre Domänenzugehörigkeit verlieren, da die *Windows*-Clients in regelmäßigen Abständen die Kennwörter ihrer Domänenkonten ändern.

Ein Snapshot, der die letzte Kennwortänderung der *Windows*-Clients nicht enthält, führt dazu, dass sich Benutzer, bzw. Rechner nicht mehr an der Domäne anmelden können. Dies gilt auch für die W10AdminVM.

Falls ein erneuter Domänenbeitritt der Clients notwendig sein sollte, kann dieser über das *opsi*-Produkt *windomain* angestoßen werden. Um den Rechner wieder in die Domäne aufzunehmen, muss das Paket *windomain* erneut auf dem Rechner installiert werden. Genauere Informationen zu *opsi* finden Sie im Administrationshandbuch.

11.6 Verwalten von Snapshots

Snapshots stellen vor allem bei Konfigurationsänderungen am *paedML Linux* System, eine bequeme Art dar, jederzeit wieder auf einen funktionierenden Zustand zurückwechseln zu können. Hierüber können gefahrlos Konfigurationsänderungen getestet werden. Es sollten jedoch nicht bedenkenlos zu viele Snapshots angelegt werden, denn

- das Bevorraten mehrerer Snapshots kann unter Umständen massiv Festplattenplatz belegen, da im Snapshot alle Benutzerdaten gespeichert sind.
- bei Snapshots werden – vereinfacht dargestellt – nur die Unterschiede zu Vorgänger-Snapshots gespeichert. Beim Betrieb mit mehreren Snapshots besteht der aktuelle „Zustand“ aus einem Grundzustand und mehreren Änderungen. Der häufige Gebrauch von Snapshots kann sich negativ auf die Performance des Systems auswirken.

Löschen von Snapshots

Um Speicherplatz zu sparen, können „alte“, nicht mehr benötigte Snapshots gelöscht werden. Das Löschen von „alten“ Snapshots ist jedoch eine sehr aufwändige Operation, da die Daten des gelöschten Snapshots unter Umständen in einen darauf basierenden späteren Snapshot integriert werden müssen.

Löschen Sie Snapshots einer virtuellen Maschine nur dann, wenn diese ausgeschaltet ist!

12 Umstellung auf die paedML für Grundschulen

Ab Version 7.1 der paedML Linux erhalten paedML für Grundschulen Kunden denselben Satz virtueller Maschinen wie paedML Linux Kunden. Die Installation einer paedML für Grundschulen erfolgt gemäß Kapitel 1 bis 11 dieses Handbuchs. Im Anschluss muss das Skript *Grundschul-Switch* ausgeführt werden. Dieses aktiviert die Gruppenrichtlinie *paedMLL_GS*, installiert die opsi-Pakete „*Grundschul-Software*“ und „*Schulkonsole-Grundschule*“ auf dem opsi-Server, setzt das *paedml-login-opsi-Paket* auf *Grundschule* und ermöglicht Schüler-Passwörter mit einer Länge von vier Zeichen zu setzen.

Führen Sie die Datei „GrundschulSwitch.exe“ im Ordner *backup**opsi_depot_rw**update72**Skripte* aus und folgen Sie den Anweisungen.

13 Erweiterungsmöglichkeiten der *paedML Linux*

Die *paedML Linux* bietet Erweiterungsmöglichkeiten, die im Folgenden beschrieben werden.

13.1 Integration weiterer Server

Die *paedML Linux* kann durch den Betrieb weiterer Server auf individuelle Bedürfnisse angepasst bzw. erweitert werden. Für den Betrieb dieser Server ist ein spezieller IP-Bereich vorgesehen, um (zukünftige) Konflikte mit dem *paedM Linux* System zu vermieden.

Auf den bestehenden Servern dürfen keine weiteren Services (z.B. Webserver, Datenbankserver) installiert werden.

Sollen innerhalb des Schulnetzes weitere Services (z.B. Webserver, Datenbankserver für Unterrichtszwecke) betrieben werden, so darf dies nicht auf den virtuellen *paedML* Servern geschehen[4]. Für diese Zwecke müssen eine oder mehrere weitere virtuelle Maschinen auf dem Virtualisierungs-Host angelegt werden und ins Netz „*PAEDAGOGIK*“ eingebunden werden.

Für die Installation eines eigenen virtuellen Servers gibt es mehrere Möglichkeiten:

- Virtualisierung einer bereits bestehenden physikalischen Maschine.
- Neuinstallation von CD bzw. ISO-Datei.
- Verwenden von vorkonfigurierten VMware-Images (als ..zip-Archiv oder OVF-Vorlage), die direkt auf den Hypervisor importiert werden können. Dazu gibt es im Internet ein reichhaltiges Angebot für die unterschiedlichsten Einsatzwecke, zum Beispiel unter
  - Turnkey Linux (http://www.turnkeylinux.org)
  - Bitnami (http://www.bitnami.com)

Netzanbindung

Im Netz „*PAEDAGOGIK*“ ist der IP-Adressbereich *10.1.0.1 – 10.1.0.31* reserviert, Adressen oberhalb von *10.1.0.31* werden vom DHCP-Server für die Client-Rechner vergeben.

Der Bereich *10.1.0.1 – 10.1.0.20* ist für *paedML Linux*-eigene Maschinen reserviert (z.B. Server, Firewall oder Router zur Anbindung weiterer Netze). Diese IP-Adressen dürfen nicht für eigene Server verwendet werden!

Der Bereich *10.1.0.21 – 10.1.0.31* kann für zusätzliche Server genutzt werden. Wählen Sie eine IP aus diesem Bereich aus.

IP-Bereich	Verwendung
10.1.0.1 – 10.1.0.20	reservierte IP-Adressen für *paedML Linux* VMs
10.1.0.21 – 10.1.0.31	IPs-Adressen für weitere Server

Tabelle 4: Aufteilung des unteren IP-Bereichs

Auch wenn zum jetzigen Zeitpunkt nicht alle IP-Adressen aus dem Bereich *10.1.0.1* bis *10.1.0.20* in Verwendung sind, kann dies in späteren *paedML Linux*-Versionen durchaus der Fall sein. Verwenden Sie keine IP-Adressen aus diesem Bereich für eigene Maschinen!

[4] Leider zeigt die Erfahrung, dass Modifikationen an Systemdiensten häufig zu Fehlern im Betrieb der *paedML* führen. Um dies zu vermeiden, sollten eigenständige Anpassungen an den *paedML* Maschinen weitestgehend vermieden werden.

Abhängig vom Einsatzzweck der zusätzlichen Server müssen eventuell noch weitere Konfigurationen durchgeführt werden.

13.2 Vergrößern der Festplatten der VM „Server“

Falls die im Auslieferungszustand definierten Festplattengrößen der virtuellen Server nicht ausreichen, können diese vergrößert werden.

Wenn die Rede von „Festplatten“ ist, muss zwischen den folgenden Begriffen unterschieden werden.

- **Physische Festplatten des Virtualisierungs-Hosts**: Reale Festplatten, die entweder intern (SCSI, SATA) im Virtualisierungs-Host eingebaut oder z.B. per SAN mit dem Hypervisor verbunden sind.
- **Datastores**: Im Hypervisor eingerichtete Partitionen auf den physikalischen Festplatten, auf denen virtuelle Maschinen einschließlich ihrer virtuellen Festplattenabbilder gespeichert werden.
- **virtuelles Festplattenabbild**: Eine oder mehrere zusammengehörige Dateien (z.B. „*my-vm-disk001.vmdk*“), innerhalb eines Datastores des Hypervisors, innerhalb der die Daten für eine Festplatte einer virtuellen Maschine gespeichert werden. **Festplatte einer virtuellen Maschine**: Jede VM benötigt in der Regel mindestens eine Festplatte. Diese wird beim Anlegen (oder beim Import) der VM erstellt und besitzt eine festgelegte Größe (z.B. 60 GB).

Soll die Festplatte einer virtuellen Maschine vergrößert werden, wird grundsätzlich empfohlen, eine weitere Festplatte hinzuzufügen: Es wird eine weitere Festplatte in die virtuelle Maschine „eingebaut“.

13.2.1 Hinzufügen einer Festplatte zu einer virtuellen Maschine

Das Verändern der Festplattenkonfiguration stellt einen massiven Eingriff in die Konfiguration des gesamten paedML-Systems dar. Im Fehlerfall kann ein vollständiger Datenverlust eintreten.

Sichern Sie vor der Anpassung der Festplattenkonfiguration alle virtuellen Festplattenabbilder auf einem externen Speichermedium.

Überprüfen Sie vorher die VM-Kompatibilität. Die virtuellen Maschinen sollten mit der ESXi-Version 5.5 kompatibel sein.

Stellen Sie zunächst sicher, dass auf dem Datastore des Virtualisierungs-Hosts genügend Speicherplatz für die neue Festplatte vorhanden ist.

Loggen Sie sich im *vmware-Host-Client* ein und wählen Sie die VM aus, zu der Sie eine weitere Festplatte hinzufügen möchten (1). Klicken Sie auf „*Aktionen*“ (2) und auf „*Einstellungen bearbeiten*“ (3).

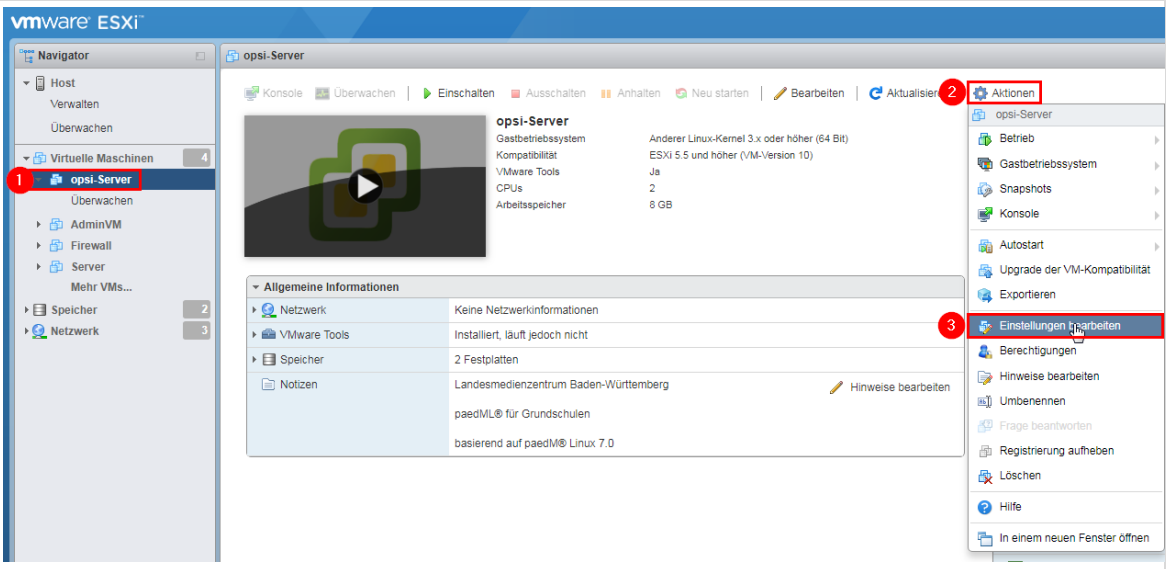

Abb. 160: Bearbeiten der Einstellungen der VM

Klicken Sie im nächsten Fenster auf „*Festplatte hinzufügen*“ | „*Neue Festplatte*“.

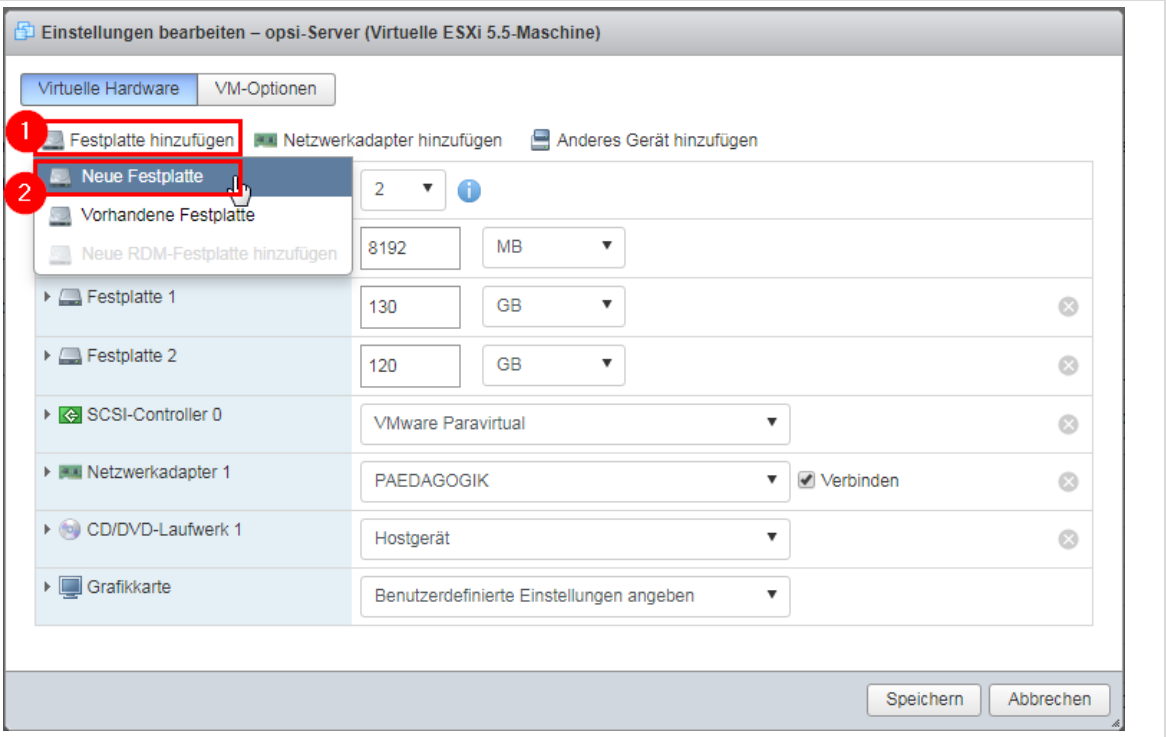

Abb. 161: Hinzufügen eines neuen Geräts zu einer virtuellen Maschine

Geben Sie die gewünschte Größe der neuen Festplatte an (1) und klicken Sie auf „Speichern“ (2).

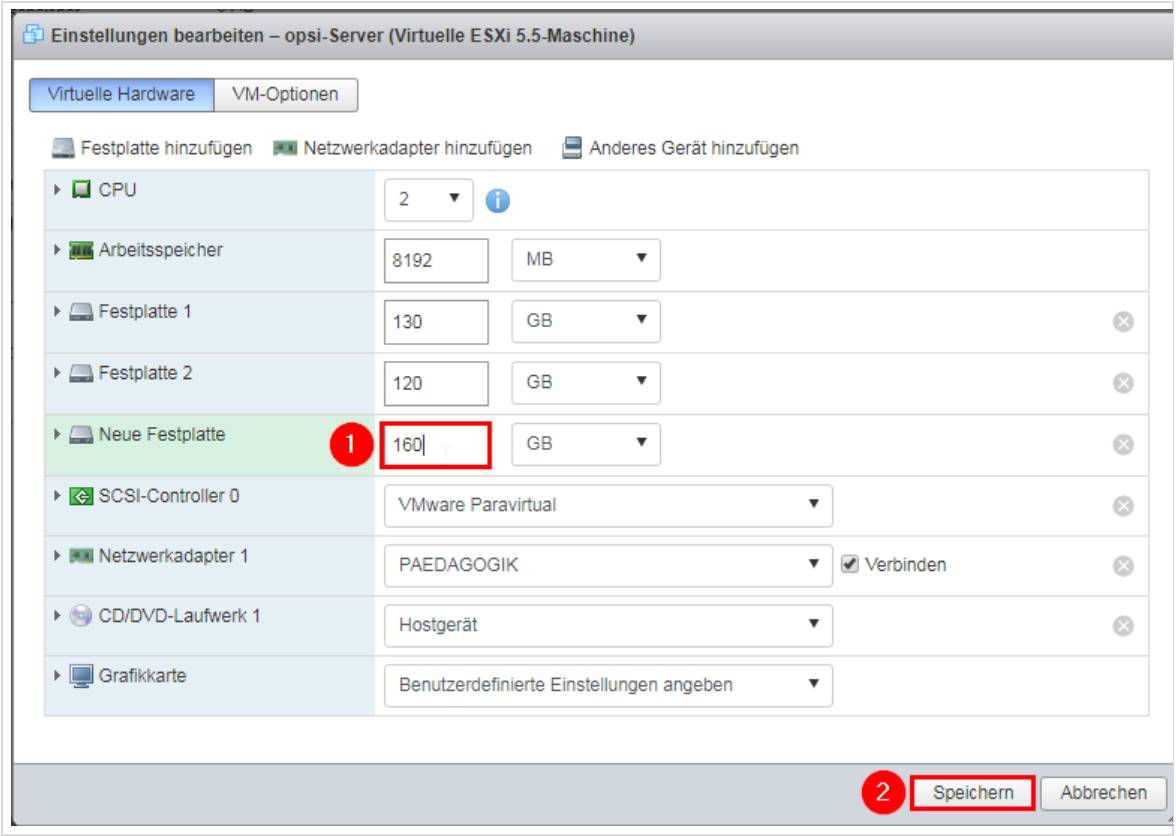

Abb. 162: Festplattengröße angeben und speichern

Nachdem die neue Festplatte angelegt wurde, sollte diese in den Einstellungen der virtuellen Maschine wie folgt erscheinen:

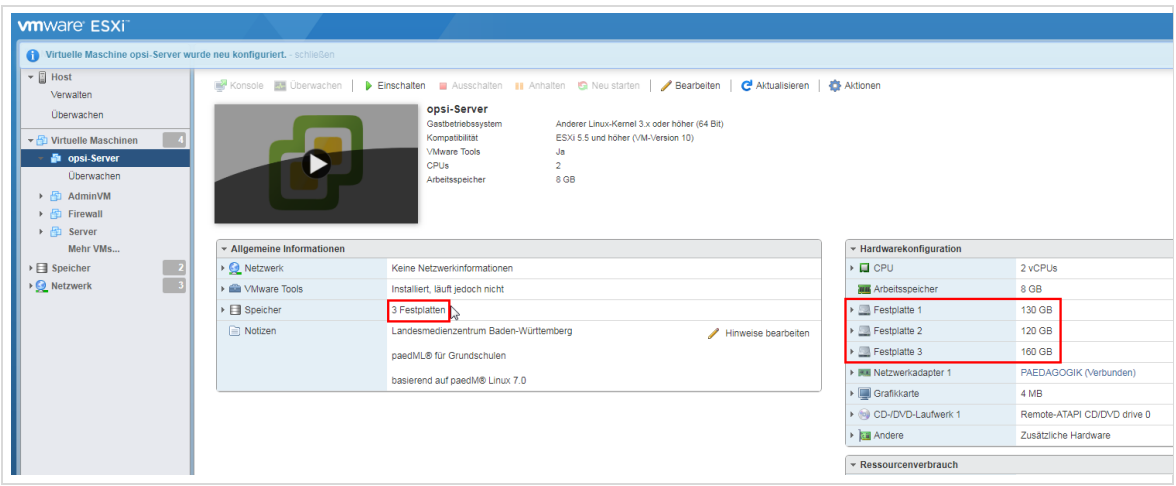

Abb. 163: Die neue Festplatte wurde erfolgreich angelegt.

13.2.2 Vorbereiten der neuen Festplatte

Achten Sie im Folgenden darauf, was Sie eintippen. Ein falsches Zeichen kann die gesamte *paedML Linux*-Installation unbrauchbar machen! Im Folgenden wird die Änderung der Datenträger mit dem Linux-Werkzeug *fdisk* beschrieben. Bei Änderungen gehen alle auf der Festplatte vorhandenen Daten verloren. Erstellen Sie bei Bedarf vorher eine Datensicherung.

Loggen Sie sich als nächstes auf der Konsole der virtuellen Maschine als *root* ein.

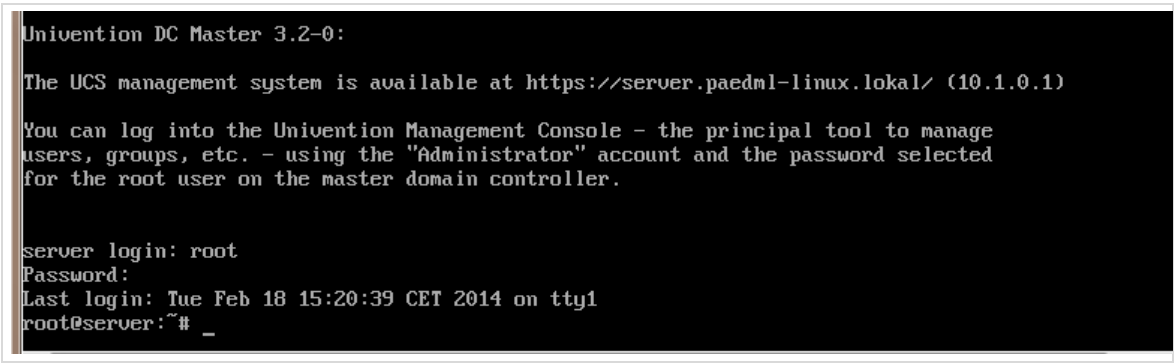

Abb. 164: Login auf der Konsole des Servers

13.2.2.1 Anlegen einer neuen Partitionstabelle

Mit dem Befehl `#fdisk -l` können sich eine Liste der am System angeschlossenen Geräte ausgeben lassen.

Die Ausgabe „GPT PMBR size mismatch (277xxx != 314xxx) will be corrected by w(rite).“ ist kein Fehler im Dateisystem oder des Volumes, sondern nur ein Hinweis (*fdisk* kann die GPT-Tabelle nicht richtig lesen).

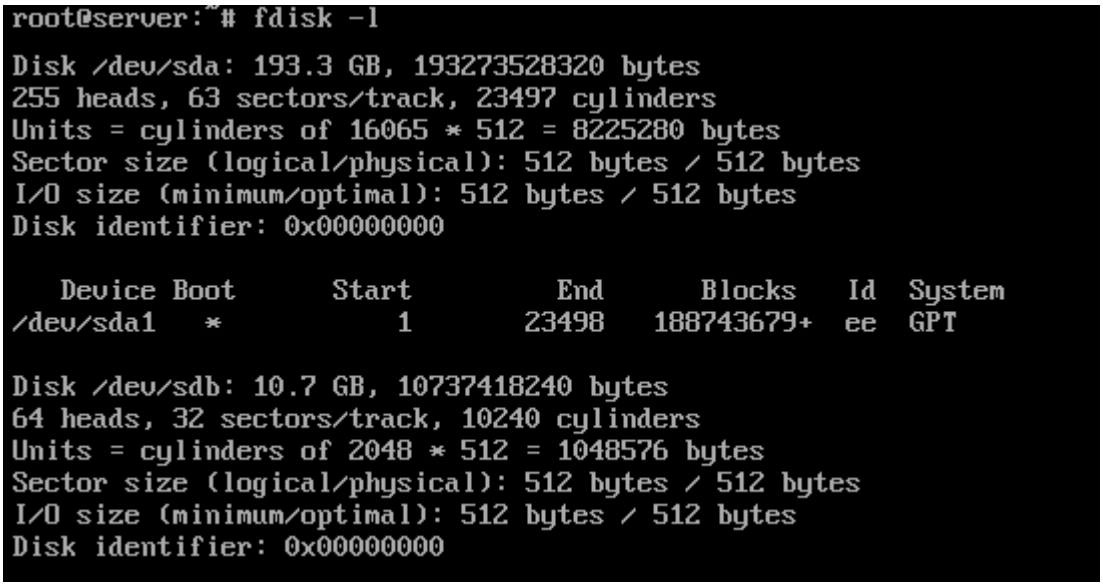

Abb. 165: Ausgabe der am System angeschlossenen Festplatten via fdisk

Zunächst muss auf der neu angelegten Festplatte eine Partitionstabelle angelegt werden, starten Sie dazu das Partitionierungstool *fdisk* unter Angabe der Gerätedatei der neu angelegten Platte. Normalerweise wird dies */dev/sdb* sein.

Beispiel:

```
#fdisk /dev/sdb
```

Eine Liste aller in *fdisk* verfügbaren Befehle erhalten Sie durch Drücken der Tasten h oder m.

- Drücken Sie die Taste o, um eine neue, leere Partitionstabelle anzulegen.
- Drücken Sie danach die Taste w, um die Änderungen tatsächlich durchzuführen.
- Drücken Sie q, falls Sie fdisk verlassen wollen ohne Änderungen zu speichern.

13.2.2.2 Anlegen einer Partition

Starten Sie das Tool *fdisk* erneut unter Angabe der Gerätedatei der neuen Festplatte:

Beispiel:

```
#fdisk /dev/sdb
```

- Drücken Sie die Taste n, um eine neue Partition anzulegen
- Drücken Sie p für „primäre Partition“.
- Drücken Sie 1, um die Nummer der anzulegenden Partition anzugeben.
- Übernehmen Sie die Voreinstellung für „*first cylinder*“ durch Drücken von Enter
- Übernehmen Sie die Voreinstellung für „*last cylinder*“ durch Drücken von Enter.
- Drücken Sie w um die Änderungen tatsächlich durchzuführen.

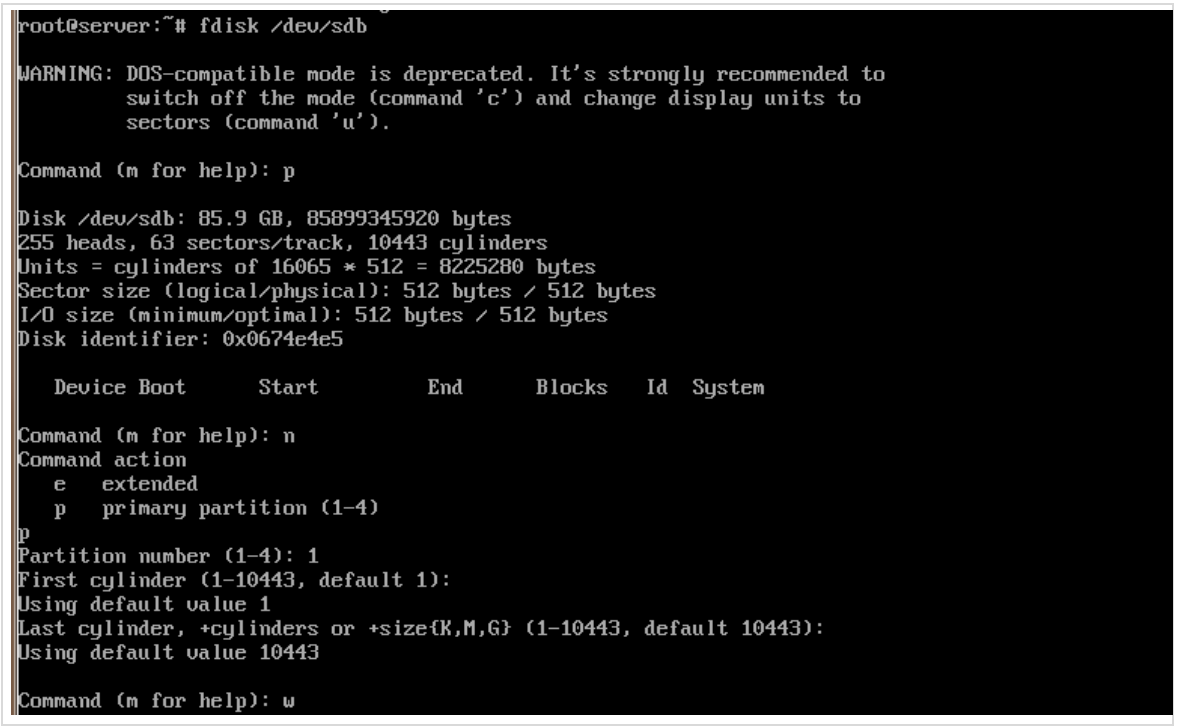

Abb. 166: Anlegen einer neuen Partition

Überprüfen Sie anschließend die Partitionierung durch Eingabe von `fdisk -l <Gerätedatei>`

Beispiel:

```
#fdisk -l /dev/sdb
```

In der Ausgabe sollte die neue Partitionstabelle mit einer einzigen Partition erscheinen:

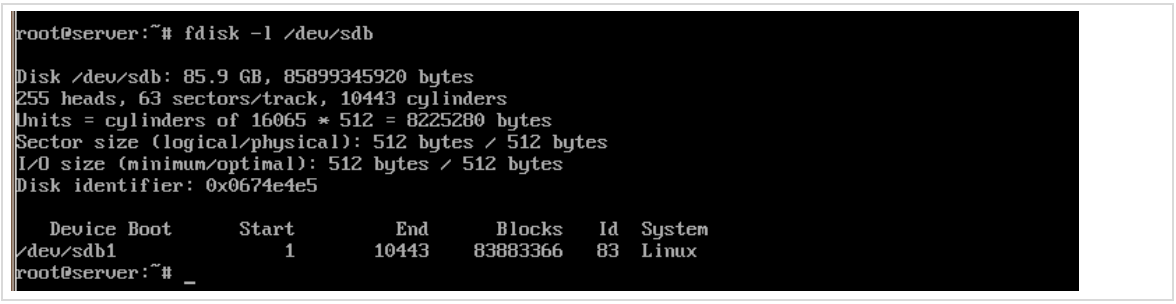

Abb. 167: Überprüfen der neu angelegten Partition

13.2.2.3 Formatieren der Partition als „Physical Volume“

Im nächsten Schritt muss die Partition mit dem Tool „*pvcreate*“ als sogenannte „*Physical Partition*“ formatiert werden, um vom *Logical Volume Manager* (*LVM*) genutzt werden zu können.

Beispiel:

```
# pvcreate /dev/sdb1
```

13.2.2.4 Erweitern der Volume Group „vg_ucs“

Die neue Partition muss nun in die Volume Group „*vg_ucs*“ des LVM aufgenommen werden, damit der Speicherplatz genutzt werden kann:

Beispiel:

```
# vgextend vg_ucs /dev/sdb1
```

Überprüfen Sie, ob die Partition korrekt in die volume group „*vg_ucs*“ aufgenommen wurde mit

```
# lvm pvscan
```

In der Ausgabe sollte die neu hinzugefügte Platte als Bestandteil des Volume Group „*vg_ucs*“ angezeigt werden:

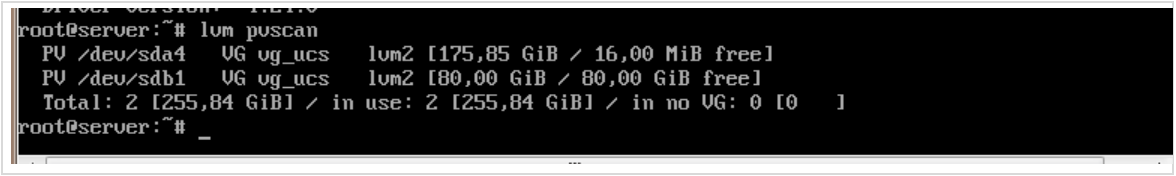

Abb. 168: Die neue Partition wurde in die Volume Group „vg_ucs“ aufgenommen.

Damit steht der Speicherplatz der neuen Festplatte dem LVM zur Verfügung.

13.2.2.5 Vergrößern des Logical Volumens

Der zusätzliche Speicherplatz kann nun durch LVM-Befehle an die *Logical Volumens* vergeben werden. Im folgenden Beispiel vergeben wir den kompletten neuen (freien) Speicherplatz an das *Logical Volume „/hohe“*.

```
Beispiel:# lvresize --extents +100%FREE vg_ucs/homefs
```

Abb. 169: Ausgabe des Kommandos lvresize

Nachdem das Volume vergrößert wurde, muss noch das Dateisystem ebenfalls angepasst werden:

Beispiel:

```
# resize2fs /dev/vg_ucs/homefs
```

Abb. 170: Ausgabe des Kommandos resize2fs

Dieser Vorgang kann einige Zeit in Anspruch nehmen. Damit ist die Vergrößerung abgeschlossen.

Alternativ könne auch nur ein Teil des neuen Speicherplatzes (z.B. nur 20GB) an das *Logical Volume* vergeben werden, der Befehl dazu würde dann lauten

Beispiel:

```
# lvresize --size +20G vg_ucs/homefs
```

13.2.2.6 Übersicht über die Logical Volumes

Die LVM-Konfiguration im Auslieferungszustand:

virtuelle Maschine	Volume Group	Logical Volume und Größe	Einhängepunkt und Verwendung
Server	„vg_ucs“	homefs (180 GB)	/home : Benutzerdaten
		rootfs (20 GB)	/Root-Verzeichnis
		varfs (55 GB)	/var
opsi-Server	vg_ucs	rootfs (20 GB)	/home
		varfs (100 GB)	/var

Tabelle 5: LVM-Konfiguration der paedML Linux

14 Einrichtung des Fernzugriffs für die Hotline

Der Fernzugriff durch die Mitarbeiter der Linux-Hotline erfolgt über das Programm Teamviewer. Durch Teamviewer kann – ohne Einrichtung von Firewallregeln – direkt aus dem Internet auf einen Rechner zugegriffen und eine Fernwartung durchgeführt werden.

Das Programm liegt als opsi-Paket vor und kann über opsi installiert werden oder Sie können es unter www.teamviewer.com herunterladen und auf den fern zu steuernden Rechner einspielen.

Die Software *Teamviewer* ist NUR für den privaten Gebrauch kostenlos. Für die kommerzielle Nutzung – und hierzu zählt auch der Einsatz in der Schule – muss eine Lizenzgebühr an den Hersteller abgeführt werden.

14.1 Zugriff auf Teamviewer

Nachdem *Teamviewer* installiert wurde, können Sie das Programm auf dem fernzusteuernden Rechner ausführen, z.B. auf der W10AdminVM.

Das Hauptfenster des Programmes zeigt eine ID und ein zugehöriges Kennwort. Mit diesen Daten kann eine Remote-Verbindung zu dem Rechner aufgebaut werden. Das Kennwort ändert sich, sobald das Programm neu gestartet wird.

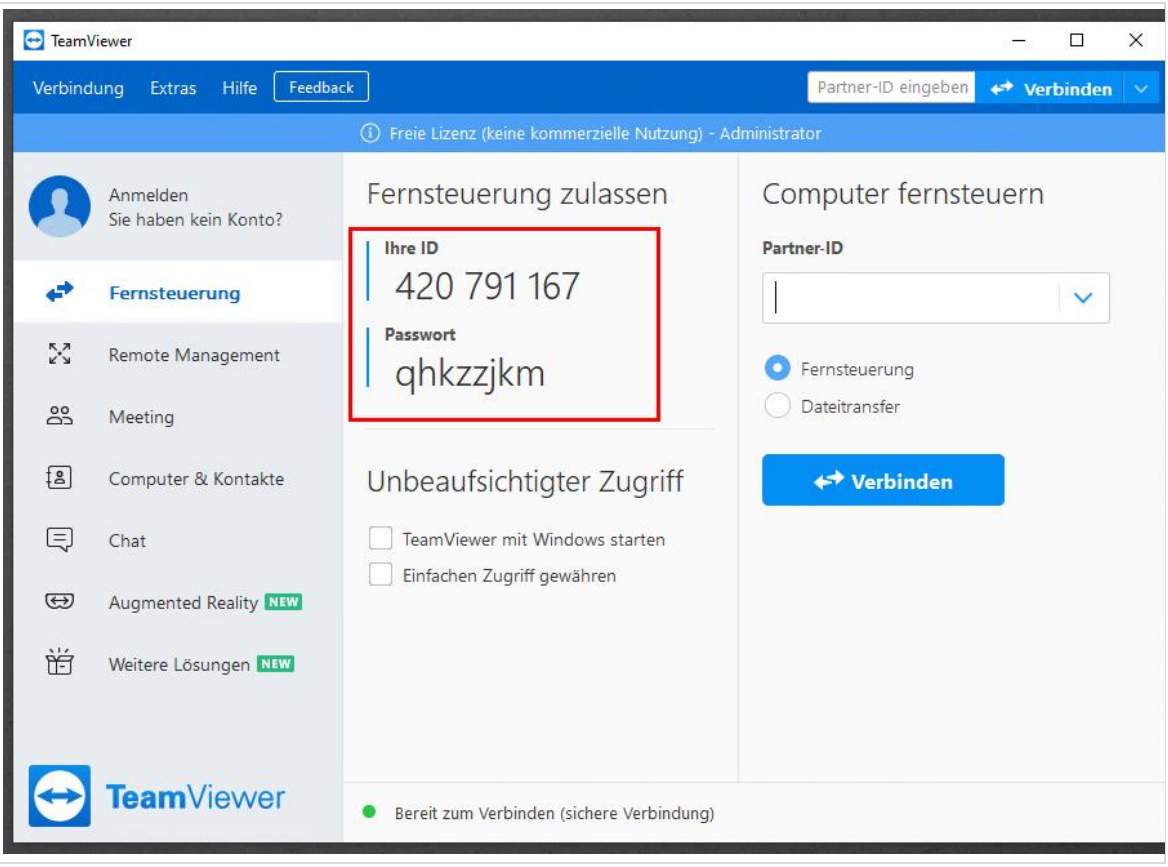

Abb. 171: Teamviewer

Es gibt zwei Optionen, wie die Hotline auf Ihren Rechner zugreift:

1. Sie richten Teamviewer als Systemdienst ein, der automatisch beim Systemstart des Rechners gestartet wird (empfohlen).
2. Sie müssen der Hotline jedes Mal den Zugriff gewähren, in dem Sie die ID und das tagesaktuelle Kennwort an den Hotline-Mitarbeiter übermitteln.

Wir empfehlen Ihnen ausdrücklich *Teamviewer* als Systemdienst zu installieren.

Dies hat den entscheidenden Vorteil, dass die Hotline jederzeit auf das System zugreifen kann, selbst wenn Sie nicht vor Ort sind. Somit kann eine Fehleranalyse durch die Hotline auch in Ihrer unterrichtsfreien Zeit erfolgen.

14.2 Einrichtung von Teamviewer als Systemdienst

Damit die Hotline-Mitarbeiter jederzeit auf Ihr System zugreifen können, müssen Sie *Teamviewer* als Systemdienst mit *Windows* starten. Öffnen Sie hierfür das Menü „Extras | Optionen“

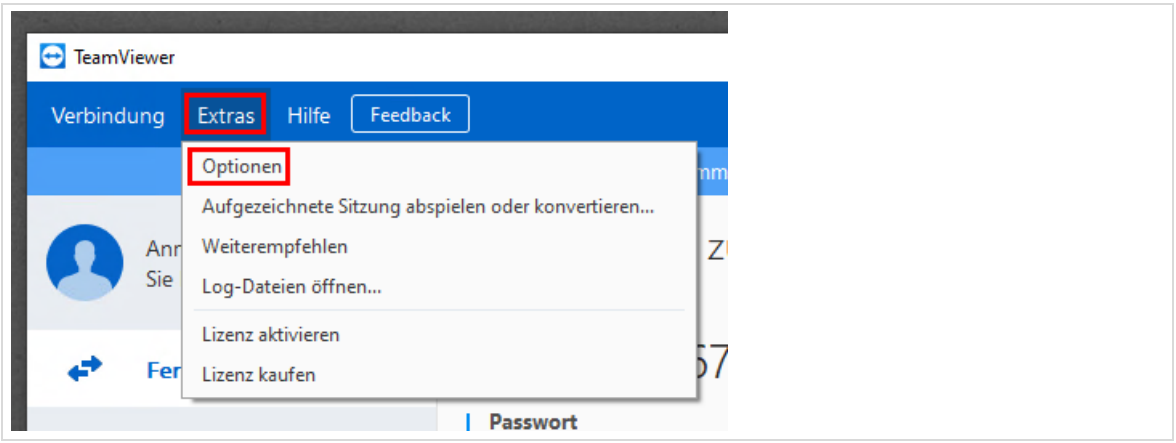

Abb. 172: Einrichtung Teamviewer als Systemdienst

Klicken Sie dann auf „Erweitert“ → „Erweiterte Einstellungen anzeigen“.

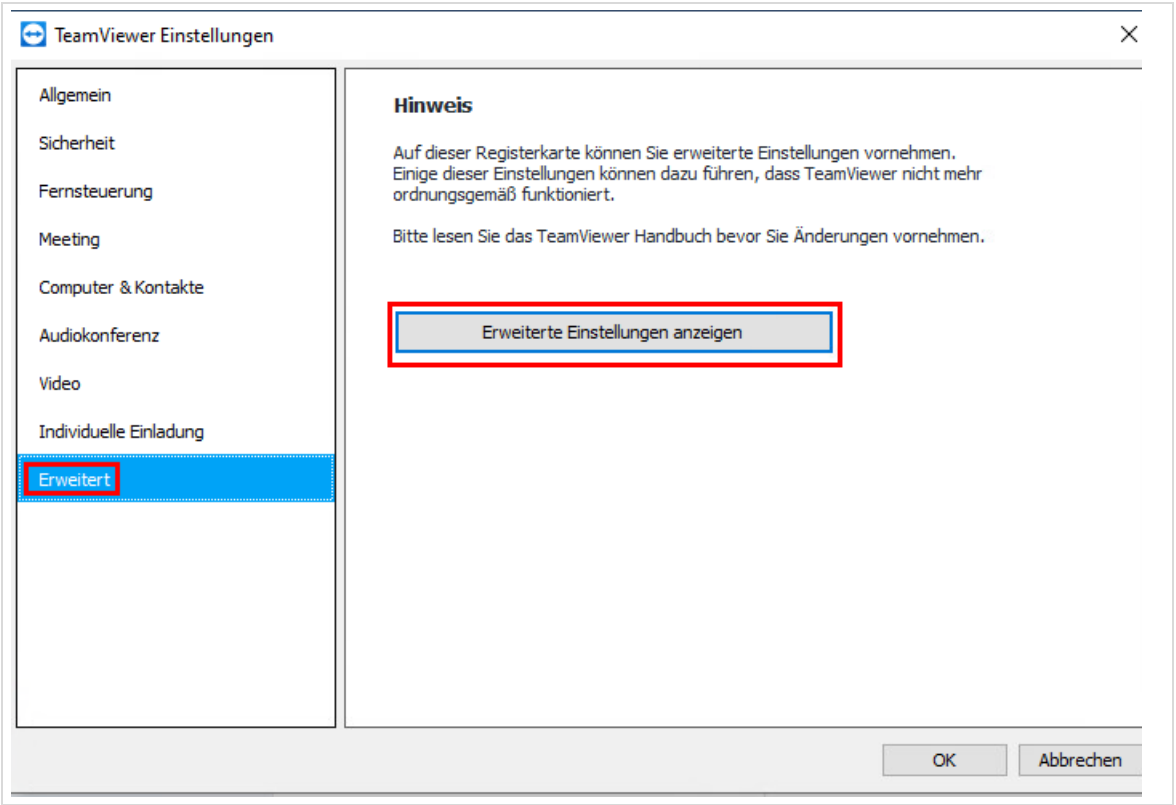

Abb. 173: Einrichtung Teamviewer als Systemdienst 1

Scrollen Sie dann bis zum Abschnitt „Persönliches Kennwort“. Geben Sie hier ein Kennwort ein, bestätigen Sie mit „OK“ und teilen Sie das Kennwort der Hotline mit.

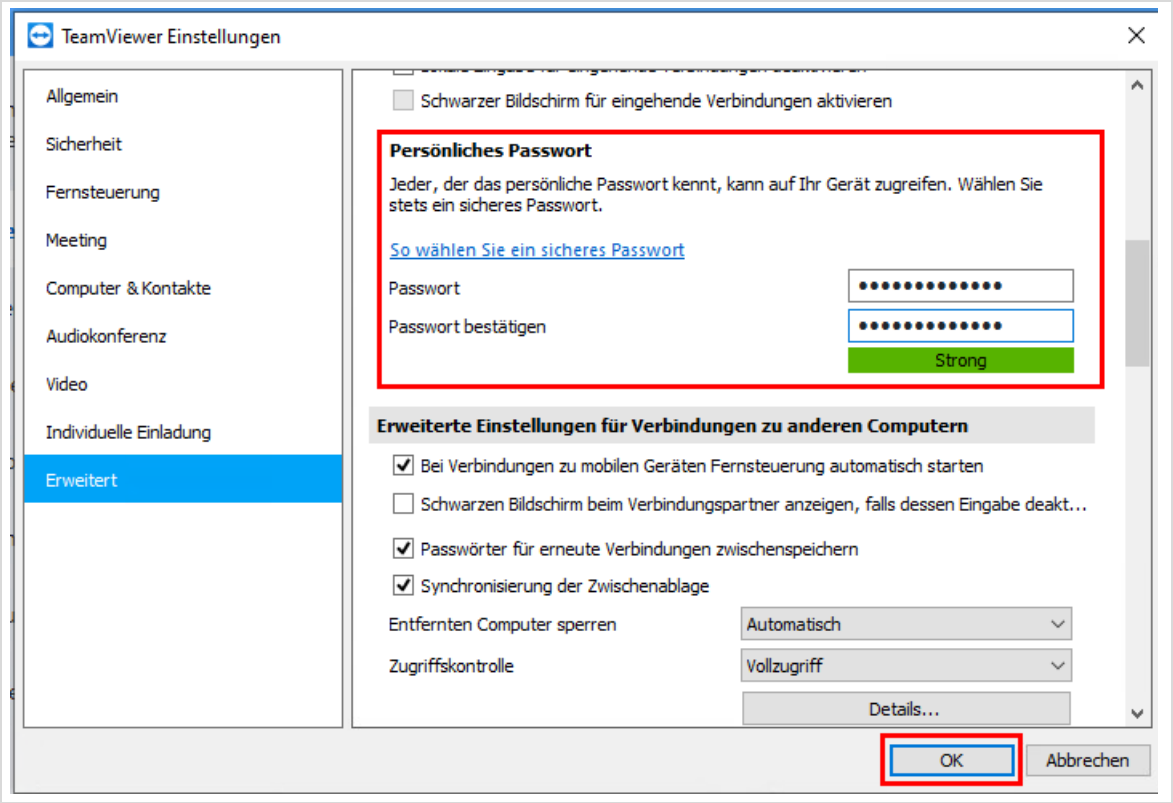

Abb. 174: Einrichtung Teamviewer als Systemdienst 2

Im Anhang dieser Anleitung finden Sie eine Übersicht, auf der die Informationen für den Fernzugriff dokumentiert werden sollten. Übermitteln Sie bitte das für den permanenten Zugriff gesetzte Kennwort und die Teamviewer-ID der Hotline und testen Sie den Zugriff!

Anhang A Dokumentation der Zugangsdaten

Bitte lassen Sie die folgende Seite von Ihrem Dienstleister ausfüllen und übermitteln Sie die Daten an die Hotline.

Schuldaten
Name der Schule:
Adresse:

Teamviewer
Teamviewer-ID:
Passwort:

vmware
IP-Adresse / DynDns:
Passwort:

Server
Administrator-Passwort:
Netzwerkberater-Passwort:

Landesmedienzentrum Baden-Württemberg (LMZ)
Support Netz
Rotenbergstraße 111

70190 Stuttgart