



linuxmuster.net

Release latest

linuxmuster.net

26.04.2024

1	Kennst Du linuxmuster.net noch nicht,	3
2	Hattest Du schon Kontakt mit einer Installation von	5
3	Installation from Scratch	7
4	Weitere Hilfe	9
4.1	Was ist linuxmuster.net?	9
4.2	Was ist neu in 7.2?	15
4.3	Installationablauf	17
4.4	Vorüberlegungen	17
4.5	Proxmox vorbereiten	22
4.6	Install-from-Scratch	61
4.7	Setup v7.2	113
4.8	Setup via Schulkonsole	116
4.9	Setup im Terminal	125
4.10	Benutzeraufnahme mit der Schulkonsole	136
4.11	Muster-Client aufsetzen	143
4.12	Upgrade v7.1 auf v7.2	238
4.13	Migration LINBO 2.4 zu 4.2	240
4.14	Migration auf linuxmuster 7.2	242
4.15	Migration eines bestehenden Linux-Clients	251
4.16	Clients in der linuxmuster.net	252
4.17	LINBO4 nutzen	254
4.18	Linux-Client - Anpassungen mit Postsync-Scripten	286
4.19	Leoclient 2 - Windows im Linuxclient	293
4.20	Ändern des eigenen Passwortes	318
4.21	Schülerverwaltung als Lehrer	321
4.22	Benutzer verwalten mit der Schulkonsole	327
4.23	Lehrer-Passwörter zurücksetzen	342
4.24	Festplattenplatz für Benutzer einschränken (Quota)	347
4.25	Vorbereitung am Schuljahresanfang	356
4.26	Schulkonsole des Lehrers	357
4.27	Prüfungsmodus	374
4.28	Zugriff auf WLAN, Internet und Drucker regeln	387
4.29	Anzeigen des eigenen Plattenplatzes	390
4.30	linuxmuster.net aktuell halten	392

4.31	Zugriffsrechte im Netzwerk	395
4.32	Anpassen der Festplattengröße	396
4.33	Netzwerkzugriff über Radius	412
4.34	Netzwerksegmentierung	418
4.35	Drucker einbinden	464
4.36	Schulkonsole des global-admin	479
4.37	Nutzung der Remote Server Administration Tools zum Anpassen der GPO	495
4.38	Softwareinstallation via GPO	498
4.39	OpenVPN konfigurieren	500
4.40	Installation eines Dockerhosts	516
4.41	Externe Authentifizierung - Moodle	521
4.42	Nextcloud für linuxmuster.net	525
4.43	Externe Authentifizierung - Aleksis	548
4.44	Unifi-WLAN-Lösung für linuxmuster.net	550
4.45	Mitarbeit linuxmuster.net	570
4.46	Active Directory-Domäne	581
4.47	LVM des Servers anpassen	589

Herzlich Willkommen zur Dokumentation von linuxmuster.net v7.2!

Diese beschreibt alle wichtigen Schritte ...

- ... von der Installation,
- ... der Einrichtung von Windows- und Linux-Rechnern als Clients,
- ... der Systemadministration,
- ... der Verwaltung von Nutzern,
- ... bis hin zu individuellen Anpassungen.

Wie es bei einem Projekt ist, dessen Entwicklungsgeschichte mittlerweile auf das Jahr 1999 zurückblickt, ist Dein Einstieg in die Beschreibung unseres Systems sicherlich unterschiedlich.

KAPITEL 1

Kennst Du linuxmuster.net noch nicht,

dann empfehlen wir Dir das Kapitel

Was ist linuxmuster.net?

Hattest Du schon Kontakt mit einer Installation von

linuxmuster.net Version 7?

Dann ist das Kapitel *Was ist neu in 7.2?* für Dich von Interesse.

Installation from Scratch

Diese Dokumentation führt Dich durch eine Installation von Grund auf. Dies bedeutet, dass zunächst die Vorbereitung der Virtualisierungslösungen - hier Proxmox - dokumentiert wird. Auf dem Virtualisierer sind sog. Virtuelle Maschinen (VM) anzulegen, um linuxmuster.net 7.2 installieren zu können. Hierzu gehört die spezifische Einrichtung des Netzwerks, des Speichers sowie die Vorbereitung der VM.

Neben dieser Dokumentation steht Dir unsere Community in unserem Hilfeforum und unser kostenfreier Telefon-Support helfend zur Seite.

Das Forum findest Du unter <https://ask.linuxmuster.net>.

Informationen zum Telefon-Support gibt es auf unser Projektseite <https://www.linuxmuster.net/de/support-de/>.

Hinweis: Suchst Du die Dokumentation zur Version linuxmuster.net 7.1 oder die Möglichkeit unsere Dokumentation herunterzuladen?

Dann schaue an das untere Ende der Menüleiste.

Nach einem Klick eröffnen sich Dir dort noch weitere Möglichkeiten:

4.1 Was ist linuxmuster.net?

Autor des Abschnitts: @cweikl, @MachtDochNix

linuxmuster.net ist eine Komplettlösung für den digital unterstützten Unterricht für Schüler:innen und Lehrer:innen einer zeitgemäßen Bildungseinrichtung.

Die langjährigen Erfahrungen aller Beteiligten aus der linuxmuster.net Gemeinde haben gezeigt, dass sich ein Firmennetzwerk fundamental von den Anforderungen an ein heutige Schulnetz unterscheiden.

Die Entwicklung von linuxmuster.net greift all diese Anforderungen auf und stellt eine modulare Lösung für ein Schulnetz zur Verfügung.

Diese kann von einer Ein-Server-Lösung bis hin zu einer Mehr-Server-Lösung mit Cloud-Anbindung und BYOD-Integration skaliert werden.

Die Anforderungen, die heute an ein Schulnetz gestellt werden, erklären wir im nachfolgenden Abschnitten detailliert. Im Anschluss zeigen wir auf, wie linuxmuster.net diese umsetzt.

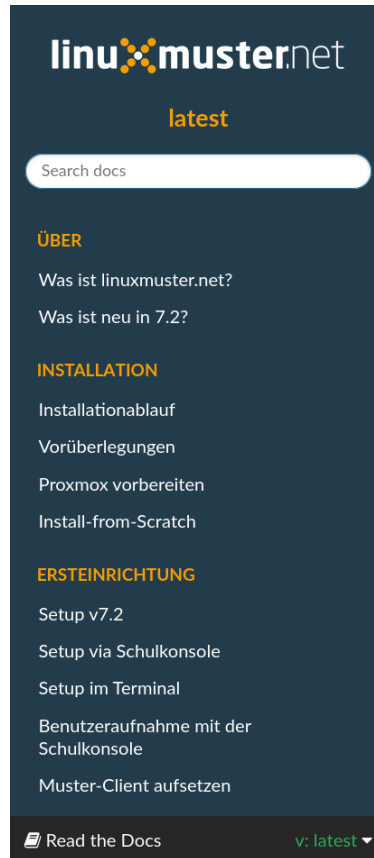


Abb. 1: Read the Docs Untermenü

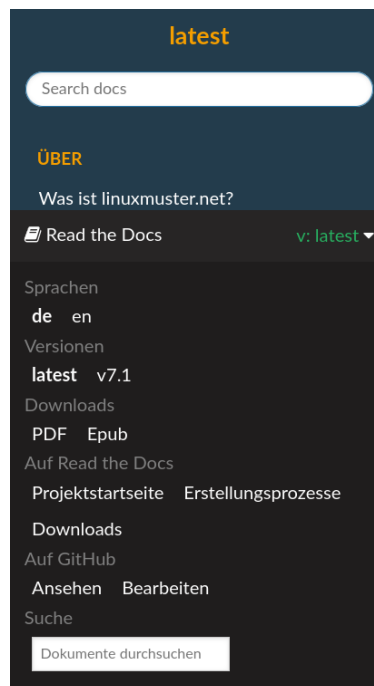


Abb. 2: Read the Docs geöffnetes Untermenü

4.1.1 Schulnetzwerk vs. „normales“ Netzwerk

Welche Unterschiede in der IT in einer Firma und einer Schule sind für uns relevant?

Im Prinzip gibt es vier große Merkmale, die auffallen:

1. Das Verhältnis der Anzahl von Usern zu den Arbeitsmitteln

Firma		Schule	
User	PC	User	PC
50	50	500	50

2. Die Zusammensetzung von Usern in Abteilungen

Firma		Schule	
User	Abteilung	User	Gruppe
A	Marketing	A	Klasse
			Kurs 1
			Kurs 2
B	Marketing	B	AG 1
			Klasse
			Kurs 3
			Kurs 2
			AG 1

3. Die Fluktuation im jährlichen Wechsel

Zum Schuljahreswechsel verlässt eine große Anzahl an Schüler:innen die Einrichtung und neue müssen in das System eingepflegt werden. Die Zusammensetzung der Klassen, Kurse und Arbeitsgruppen werden zu großen Teilen neu formiert.

Solch ein administrativen Aufwand ergibt sich in einer Firma selten.

4. Der Umgang mit den Arbeitsmitteln

Schüler:innen teilen sich ein und dasselbe Arbeitsmittel im schulischen Alltag. Dabei ist es für die nächste Unterrichtseinheit entscheidend, dass zum Start immer eine einheitliche Umgebung auf den Rechnern vorhanden ist. Die zeitliche Taktung zwischen den Wechseln kann sehr kurz sein.

Dies ist in einer Firma so nicht gegeben. Wenn ein User seinen Rechner verlässt, findet er ihn der Regel immer genauso wieder.

Aus diesen Gründen sprechen wir von einem

4.1.2 Schulnetz

Mit linuxmuster.net wird die schulische IT mit einer voll integrierten Open-Source-Lösung abgebildet. Dieses umfasst alle Bereiche, die in einer Bildungseinrichtung anzutreffen sind.

Unser Anspruch liegt dabei auf der Bereitstellung eines Systems, das folgende Punkte erfüllt:

- automatisierte Installation der Server-Komponenten
- durch einen freien Zugang zu einer umfänglichen Dokumentation eine möglichst einfache Installation
- einfache Integration in vorhandene Infrastruktur
- bestehend aus Server, Firewall und vorkonfigurierten Arbeitsstationen

- mehrstufige ausbau- und anpassbare Struktur mit heterogenen Clients und unterschiedlichsten Diensten bzw. Cloud-Lösungen
- ein frei zugängliches [Community-Wiki](#) mit einer Vielzahl an ergänzenden Anleitungen und Erweiterungen aus dem Umfeld der Unterstützer von linuxmuster.net

Schulnetz - Komplett - Anpassbar!

Ein Augenmerk liegt dabei auf der Unabhängigkeit von der eingesetzten Hard- und Software. Dieses wird unter anderem erkennbar an dem Umfang der unterstützten Betriebssysteme für die Arbeitsstationen.

Proprietäre Betriebssysteme, z. B. aus dem Hause Microsoft®, können aufgrund der Lizenzpolitik der Hersteller nicht von uns vorbereitet ausgeliefert werden. Diese lassen sich aber ebenso leicht in unsere Infrastruktur integrieren, wie solche, die als Open-Source erhältlich sind.

Auf der Basis von Linux stellen wir ein Open-Source-Betriebssystem zur Verfügung, das folgende Vorteile bietet:

- entwickelt von Praktikern für den täglichen Einsatz an Schulen
- mit hilfreichen Schulfunktionen für den Unterrichtseinsatz
- in einfacher Form anpass- und erweiterbar an die eigenen Bedürfnisse
- keine Lizenzkosten

Im Zusammenspiel der Clients mit dem Server und einer Firewall entsteht so die grundlegende professionelle Infrastruktur zur zentralen Administration der Schülergeräte und der Verwaltung des pädagogischen Schulnetzwerkes.

Dieses lässt sich aufgrund des modularen Aufbaus weiter an die darüber hinausgehenden Anforderungen, unter anderem einer schulweiten WLAN-Verfügbarkeit erweitern und anpassen.

Die Basis

Der linuxmuster.net-Server

Die Basisdienste des links abgebildeten Servers sind für die Funktion des ganzen Systems verantwortlich:

Benutzer- und Gruppenverwaltung

Die Benutzer- und Gruppenverwaltung orientiert sich an den Bedürfnissen, die der Schulbetrieb vorgibt.

- Schüler:innen bekommen mit der Einschulung ihren persönlichen Benutzer-Account.
- Dieser bleibt ihnen bis zum Ende ihrer Laufbahn an der Schule erhalten.
- Die Gruppenzugehörigkeit der einzelnen Schüler:innen werden in Klassen, Kursen und Projekten abgebildet.
- Zu Beginn eines Schuljahres können diese Daten und Abhängigkeiten aus der Schulverwaltung mittels Import der Daten eingespielt bzw. fortgeschrieben werden. Gleiches gilt selbstverständlich auch für Veränderungen während eines laufenden Schuljahres.
- Für Lehrer:innen gilt dies ebenso.

Unterrichtssteuerung

Vielfältige Möglichkeiten stehen den Lehrkräften zur Verfügung, um Einfluss auf die Rechner der zu Unterrichtenden zu nehmen.

- Internet - An/Aus
- Intranet - An/Aus
- Wi-Fi - An/Aus
- Drucker - An/Aus

Klassenarbeitsmodus

In Prüfungssituationen wie Abitur, Klassenarbeiten und andere Leistungsüberprüfungen kann die Lehrkraft mit einfachen Mitteln die Nutzung des Systems für die Prüfungsgruppe einschränken. Das Spektrum umfasst dabei alle Möglichkeiten der Unterrichtssteuerung ergänzt um die Sperrung des persönlichen Speicherbereichs.

Dateiverwaltung und -verteilung

Alle Nutzer besitzen einen persönlichen Bereich auf dem Netzwerkspeicher. Ebenso steht ein solcher den Gruppen für den Austausch ihrer gemeinschaftlichen Arbeit zur Verfügung.

Selbstheilende Arbeitsstationen durch LINBO 4.2

Das Konzept der Selbstheilenden Arbeitsstationen (SheilA) ermöglicht einheitliche, identische Schulungssysteme. Diese können bei jedem Start der Rechner in einen vorher definierten Zustand zurückgesetzt werden. Dieser Standard wird durch die letzte Veränderung oder Installation festgelegt, in dem ein Abbild des Betriebssystems auf dem Server gespeichert wird. Weitere Vorteile sind:

- verschiedene Betriebssysteme auf jedem Client möglich
- schnelle Erst- oder Neueinrichtung
- keine Einschränkung der Nutzer durch Benutzerrechte auf den Clients nötig
- einfache Wiederherstellung der Clients ist jedem Benutzer möglich
- einfache Softwareverteilung durch Installation auf einem Client - keine gesonderten Kenntnisse erforderlich, bei demjenigen, der die Software-Installation betreut.
- Möglichkeit der zeit- und/oder ferngesteuerten Aktualisierung der Clients.
- mit sogenannten Postsync-Scripten kann der Administrator für einzelne, raumweite oder für alle Geräte notwendige Konfigurationsänderungen beim Systemstart einpflegen.

Nähere Information sind im Kapitel „Clientverwaltung“ beschrieben.

Integration unterschiedlicher Geräte (BYOD)

Da sich alle Steuerungsfunktionen in unserer Lösung an den Benutzern orientieren, ist es unerheblich an welchem Gerät sie sich befinden. Das Gleiche gilt auch für mitgebrachte Geräte, mit denen sie sich mit dem Intranet via WLAN verbinden.

Firewall

OPNsense®: wird als Standard-Firewall ausgeliefert.

Durch die Integration der Firewall an AD DS (Active Directory Domain Services) des Servers (Samba4) werden sämtliche Benutzer-Zugriffe der Nutzer mittels Single-Sign-On auf das Internet geregelt.

Sämtliche verfügbaren Bausteine dieser Open-Source-Firewall stehen selbstverständlich zur Verfügung.

Für weitergehende Informationen siehe opnsense.org.

Bemerkung: Diese vorgestellten Bestandteile werden vom Verein **linuxmuster.net e. V.** entwickelt und unterstützt.

Diese Unterstützung wird durch das

Hilfe-Forum <https://www.linuxmuster.net/de/support-de/discourse-forum/>

und die

telefonische Hotline <https://www.linuxmuster.net/de/support-de/hotline/>

geleistet.

All diese Leistungen sind nicht von einer Mitgliedschaft im Verein abhängig.

Aufgrund der Vielzahl möglicher Einsatzszenarien umfasst der telefonische Support alle bereitgestellten Basis-Dienste, die in der Dokumentation beschrieben sind.

Das Support-Team berät aber gerne und zeigt alle Möglichkeiten und Alternativen auf.

Anpassbar

Alle bisher vorgestellten Basisdienste werden mithilfe des Setups konfiguriert, bleiben aber frei anpass- und erweiterbar. Es folgt eine einführende Beschreibung der letzten drei Bausteine, die linuxmuster.net zu der Komplettlösung machen.

Bemerkung: Die Unterstützung erfolgt für die nachfolgenden Bestandteile durch das

Hilfe-Forum <https://www.linuxmuster.net/de/support-de/discourse-forum/>

Die detaillierte Beschreibung ist nicht Gegenstand dieser Dokumentation, sondern wird durch die Community in deren Wiki festgehalten.

Community-Wiki: <https://wiki.linuxmuster.net/community/>

Alternative Firewall

Einsatzszenarien, die mit einer anderen Firewall als OPNsense® ausgestattet sein sollen, lassen sich mit linuxmuster.net ebenfalls umsetzen.

Wenn die eingesetzte (alternative) Firewall über die Möglichkeit einer Anbindung an den Samba4-Dienst des linuxmuster.net-Servers verfügt, kann diese alle aufgezeigten Vorteile nutzen.

Optionale Server

Für weitergehende Anpassungen besteht die Möglichkeit, optionale Server einzubinden.

In der Darstellung ist etwa ein Docker-Server als Erweiterung an die Bedürfnisse der Bildungseinrichtung eingebunden. Docker ist ein Open-Source-Projekt zur automatisierten Anwendungsverteilung durch Container, die alle benötigten Pakete mitbringen. So vereinfacht sich die Bereitstellung und Verteilung. Außerdem gewährleisten sie die Trennung und Verwaltung der auf dem Docker-Server genutzten Ressourcen.

Für weitergehende Informationen siehe die Docker-Homepage: <https://www.docker.com>

Extra

Ein Portfolio an unterschiedlichen externen Diensten lässt sich an die linuxmuster.net Lösung anbinden, sodass eine einheitliche Authentifizierung erfolgt.

Es können z.B. extern gehostete Server wie Nextcloud, Moodle oder Konferenzsysteme integriert werden.

Komplette Struktur als Inkscape SVG

4.2 Was ist neu in 7.2?

Autor des Abschnitts: Das Dokuteam

Linuxmuster.net 7.2 ist das Release-Update der linuxmuster.net v7.1. Es erfolgt eine Aktualisierung der bisher eingesetzten Ubuntu LTS Version auf die derzeit aktuellste Ubuntu Server LTS Version. Die Kernpakete der linuxmuster.net Lösung erhalten alle ein Update und stellen viele Verbesserungen und neue Features bereit.

4.2.1 Neue Funktionalitäten

Verbesserte Skalierbarkeit

- Mehrschulfähigkeit: Konsolidierung mehrerer Schulinstanzen auf einem Server möglich
- Gruppenorientierte Abbildung der Schule und flexible, regelbasierte Steuerung
- Moderne Bereitstellung zusätzlicher IT-Dienste der Schule innerhalb der Schullösung

Moderne Betriebssystembasis und Steuerung

- Aktuelle Betriebssysteme der Server (Ubuntu Server 22.04 LTS & OPNSense® 24.x) und der vorkonfigurierten, kostenlos bereitgestellten Linux-Arbeitsplätze
- Mit LINBO 4.2: Neues User-Interface für die Steuerung an den Clients, aktuellste Linux-Kernels für aktuelle Hardware, differentielle Images, ntfs3 Kernel-Treiber
- Webbasierte Steuerung der pädagogischen Funktionen mit einem **responsive design** (passt sich an alle Bildschirmgrößen und -auflösungen an).

- WebUI mit vielen administrativen Möglichkeiten, die zuvor nur an der Server-Konsole zu erreichen waren (Erstellen von Hardwareklassen, Erstellen von Client-Konfigurationen, Erstellen von differenziellen Images u.v.m.).

4.2.2 Technische Neuerungen

Vereinfachte Installation

- Standardmäßig bleibt linuxmuster.net eine Zwei-Serverlösung aus Firewall und Server. Optional können weitere Server / Docker-Instanzen angebunden werden.
- Die Installation erwartet eine vorkonfigurierte Virtualisierungslösung (Proxmox - andere sind ebenfalls möglich).

Bedienung und Administration

- Die WebUI als Verwaltungswerkzeug zur Administration und zur Steuerung von Unterricht weist viele zusätzliche Funktionen auf.
- Die vollständige Bedienbarkeit auf der Konsole bleibt erhalten.

Benutzerverwaltung

- Automatische Erkennung der Kodierung der Benutzerdaten, Sonderzeichen in Klarnamen
- Klassen- und Projektmanagement bleibt erhalten
- Zusätzliche sitzungsbasierende Berechtigungen für die Unterrichtsteuerung:
 - Gruppen können frei zusammengestellt werden
 - Benutzerbezogene statt rechnerbezogene Verwaltung

Netzwerkverwaltung

- Frei definierbare IP-Bereiche
- Standardmäßige Zugangskontrolle zum Internet über einen Proxyservice auf Single-Sign-On Basis - anstelle eines transparenten Proxy

Selbstheilende Arbeitsstationen

- LINBO ist weiterhin das zentrale Softwareverteilungssystem.
- Es erfolgt ein Major Release Update auf LINBO 4.2.
 - Umstellung der Images-Abbilder auf das qcow2 Format
 - Neues User-Interface für die Steuerung an den Clients
 - Differenzielle Images
 - Aktuelle Linux-Kernel ab 6.2.* und einem nativen NTFS-Kernel Treiber

4.3 Installationablauf

Autor des Abschnitts: @cweikl, @MachtDochNix

Um **linuxmuster.net latest** zu installieren musst Du folgende Schritte durchlaufen:

1. Planung der Infrastruktur (Server und Netzwerk)
2. ggf. Vorbereitung / Setup der Netzkomponenten
3. Einrichtung einer Basis für linuxmuster.net

Diese Dokumentation konzentriert sich auf die Umsetzung als Zwei-Server-Lösung auf einem Hypervisor (Proxmox). Andere Virtualisierungslösungen sind möglich, werden aber von linuxmuster.net nicht (mehr) offiziell unterstützt.

Falls Du einen anderen Hypervisor bevorzugst, kannst Du Dich dennoch an der Dokumentation orientieren und findest im linuxmuster.net Forum (<https://ask.linuxmuster.net>) und im Community-Wiki (<https://wiki.linuxmuster.net/community/>) Unterstützung.

4. Vorbereitung der benötigten Server

* Bei der aktuellen linuxmuster.net Version dient die LTS Version 22.04 als Basis.

5. Installation in die vorbereiteten VMs (virtuelle Maschinen)
6. Test der Netzwerkfunktionen
7. Ersteinrichtung (Setup) der Server
8. Anlegen der Benutzer und Gruppen
9. Einrichtung der Clients

Nachstehend kannst Du den Installationsablauf als Übersicht herunterladen:

Übersicht als PDF-Datei

Übersicht als Inkscape SVG-Datei

Zu tun: Grafik anpassen

4.4 Vorüberlegungen

Autor des Abschnitts: @cweikl, @Tobias

Linuxmuster.net wird als Zwei-Server-Lösung (Firewall und linuxmuster.net-Server) auf einem Hypervisor (Proxmox) betrieben.

Optional können weitere Server wie z. B. ein Docker-Host eingesetzt werden. Daneben gibt es mindestens eine Trennung in zwei logische Netzwerke, meist sind aber drei oder mehr davon gefordert (WLAN, DMZ, Lehrernetz).

Daraus leiten sich Voraussetzungen an Hardware, Netzwerkstrukturen und Software ab, die in diesem Kapitel benannt werden.

4.4.1 Hardware

OPNsense®

OPNsense® ist für x86-32 und x86-64 Bit Architekturen verfügbar und kann auf SD-Karte, SSDs oder HDDs installiert werden. Folgende Mindestanforderung muss erfüllt sein:

Prozessor	>= 1.5 GHz Multi-Core CPU (64 Bit)
RAM	>= 4 GiB
Installationsmethode	Video (VGA)
Festplatte	mind. 20 GByte, z.B. 120 GByte SSD
NIC	<ul style="list-style-type: none">• mind. 2 (intern + extern)• oder 3 (intern + extern + WLAN)

Achtung: Die Firewall erstellt viele Log-Einträge, so dass der Festplattenplatz und zudem auch der Arbeitsspeicher deutlich über der Mindestanforderung liegen sollten. Als Standard schreibt die OPNsense Einträge für einen 30 Tageszeitraum mit. Wir raten, den Zeitraum in den Einstellungen (System --> Einstellungen --> Protokollierung) individuell zu verkleinern und nur bei Bedarf und ausreichendem Plattenplatz zu erhöhen. Ein logrotate müsste bei Bedarf in der crontab angelegt werden.

Empfehlung: RAM -> 8GiB, HDD -> 50GiB

Weitere Hinweise zu möglichen Hardwareanforderungen bei unterschiedlichen Einsatzszenarien finden sich [hier](#).

Als Basis nutzt OPNsense® v24.1 das Betriebssystem FreeBSD v13.2. Hinweise zu den Anforderungen von FreeBSD bzw. zur Kompatibilität mit eingesetzten Hardware-Komponenten finden sich unter der [HCL - Hardware Compatibility List](#).

Server linuxmuster v7.2

Für linuxmuster.net v7.2 wird als Basis Ubuntu Server 22.04 LTS eingesetzt. Es wird empfohlen folgende Hardware-Mindestanforderungen zu erfüllen:

Prozessor	>= 2 GHz Multi-Core CPU (64 Bit)
RAM	>= 4 GByte
Festplatte System + Daten	<ul style="list-style-type: none">• mind. 25 GiB + 100 GiB• mind. 500 GiB für Daten und Backup• empfohlen >= 1 TiB

Festplattenspeicher

Der Festplattenplatz für den Server hängt stark von der Nutzerzahl und der intensiven Verwendung von LINBO-Abbildern ab. Ebenso muss für Backups weiterer Festplattenplatz z.B. auf einem NAS eingeplant werden.

Selbstverständlich können sowohl Daten als auch (bei Virtualisierung) die Server auf externem Speicher abgelegt werden (z. B. NFS-Speicher oder iSCSI-Speicher), um die Virtualisierungsumgebung ggf. bei Bedarf ausbauen zu können und auch ausfallsichere Szenarien leichter umsetzen zu können.

So *kann* bei minimaler Ausstattung einer mittleren Schule (ca. 500 Benutzer) ein kleiner Server oder ein gut ausgestatteter PC ausreichend sein, selbst wenn alle Server virtualisiert laufen.

Schule	Features	Festplatten		RAM	
		Standard	Empfohlen	Standard	Empfohlen
mittelgroß	minimal	~650 GByte	1500+ GByte	8 GByte	16+ GByte
groß	normal	~1000GB	2000GB+	10GB	16GB+

4.4.2 Netzwerkstruktur

In Abhängigkeit vom Einsatzszenario muss die Netzwerkstruktur der linuxmuster.net zu Beginn der Installation angepasst werden. Man sollte vor der Installation über den Umfang der eingesetzten Geräte Bescheid wissen. Dementsprechend den IP-Bereich nicht zu klein wählen, oder Subnetze einführen. Ebenso muss man den IP-Bereich auf die Umgebung (z.B. Verwaltungsnetz, extern vorgegebene Netze) abstimmen, damit keine Überschneidungen auftreten.

IP-Bereiche

Die linuxmuster.net-Lösung kann mit unterschiedlichen IP-Bereichen arbeiten. Standardmäßig wird das interne Netz aus dem privaten IPv4-Bereich 10.0.x.x mit der 16-Bit Netzmaske 255.255.0.0 (/16) eingerichtet.

Andere private Adressbereiche sind prinzipiell möglich, müssen aber händisch vorbereitet werden. *Netzbereich anpassen*

Standard IP-Adressen

Einige IP-Adressen sind für spezielle Server/Dienste vorgesehen:

Server	IP-Bereich 10.0.0.0/16
OPNsense®	10.0.0.254
Server	10.0.0.1
Admin-PC	10.0.0.10

Netz-Grundstruktur

Die Aufteilung der Netzbereiche mit linuxmuster.net sind in der Dokumentation mit Farben gekennzeichnet, um diese deutlich voneinander abzuheben:

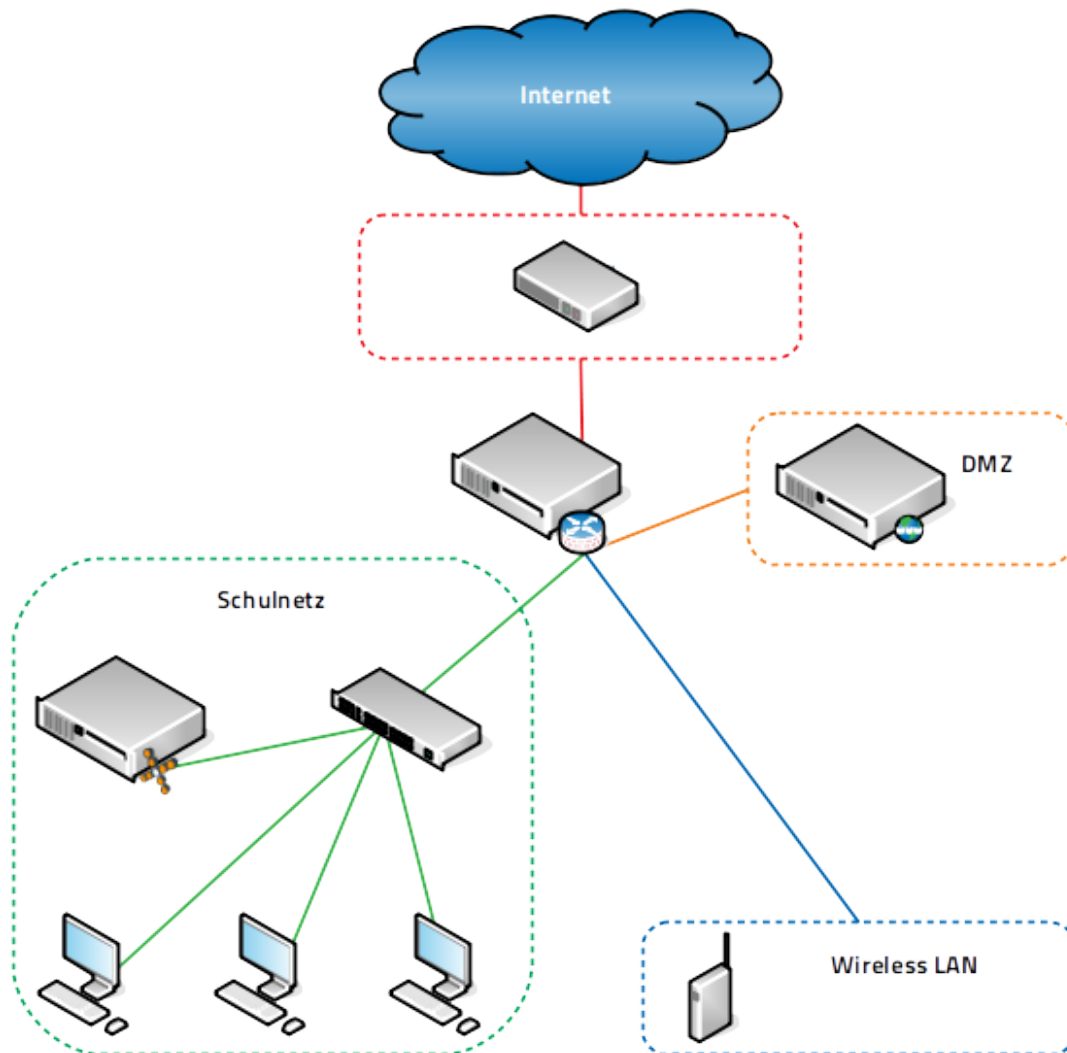


Abb. 3: Schematischer Aufbau eines Computernetzes mit linuxmuster.net.

- Das interne Netzwerk wird GRÜNES Netzwerk (GREEN) genannt.
- Das externe Netzwerk wird ROTES Netzwerk (RED) genannt, es ist über einen Router mit dem Internet verbunden.
- Optional kann z.B. für WLAN-Accesspoints ein weiteres Netzwerk aufgebaut werden (BLAU - BLUE), für welches andere Zugangsberechtigungen als im grünen Netzwerk gelten.

- Optional kann eine sog. demilitarisierte Zone (DMZ) als zusätzliches Netzwerk (ORANGE) aufgebaut werden, um z.B. extern zugängliche Web-Services bereitzustellen.

Daraus ergeben sich folgende Mindestvoraussetzungen für einen Virtualisierungshost:

- mindestens zwei Netzwerk-Interfaces (rotes und grünes Netz)
- bei WLAN-Nutzung eine zusätzliche Netzwerkkarte (blaues Netz)
- sollen Serverdienste im Internet von außen zugänglich sein, empfehlen wir diese in die DMZ auszulagern. Dafür wird eine weiteres Netzwerk-Interface benötigt (oranges Netz)

Durch die fortschreitende Digitalisierung in der Bildung ist der Auf- bzw. Ausbau einer funktionalen WLAN-Infrastruktur für jede Schule eine gute Entscheidung. Daraus ergibt sich aus unserer Sicht die Empfehlung zu mindestens drei Netzwerkkarten. Willst Du für alle möglichen Einsatzszenarien gut gerüstet sein, empfiehlt sich allerdings gleich den Virtualisierungshost mit vier und mehr Netzwerk-Interfaces auszulagern.

Das obige Prinzip ist bereits ein Beispiel für die Netzwerksegmentierung, die im nächsten Abschnitt näher erläutert wird.

Getrennte Netze und VLAN

Immer häufiger (z.B. durch Vorgaben vom Kultusministerium oder Lastverteilung) besteht Bedarf an einer weiteren Trennung des internen Netzes in mehrere logisch voneinander getrennte Netze. Neben den getrennten Netzen für WLAN oder eine demilitarisierte Zone (DMZ) wie oben abgebildet, erlaubt linuxmuster.net sehr flexibel eine beliebige Einteilung des Schulnetzes in Subnetze.

Wer vor der Entscheidung steht, Subnetze und/oder VLANs einzurichten, sollte zuvor das Kapitel *Netzsegmentierung mit linuxmuster.net* lesen.

4.4.3 Virtualisierung

Wenn man linuxmuster.net virtualisiert betreibt, gelten zu den obigen Voraussetzungen noch folgende Hinweise:

- Das Netzwerk wird virtualisiert. Dadurch werden virtuelle Switches („sog. bridges“) erstellt, denen die richtigen Schnittstellen zugeordnet werden müssen.

Wird kein Layer 3 - Switch eingesetzt, sollte der Virtualisierungshost (Hypervisor) wenigstens mit der obengenannten Anzahl von Netzwerkkarten ausgestattet sein.

Mit dem Einsatz eines Layer 3 - Switches wird die Konfiguration auf dem Hypervisor schnell komplex, die physikalische Verkabelung kann dadurch aber einfacher werden. So lassen sich auch neue Anforderungen durch zusätzliche VLANs realisieren.

- Der Speicherplatz wird virtualisiert. Darauf muss man bei der Verwendung externer (iSCSI/NFS) wie interner Speichersysteme (LVM) achten. Dies kann auch zur Vereinfachung eines Backupverfahrens beitragen. Es wird empfohlen sog. Shared Storage bei der Virtualisierung einzusetzen, um dadurch flexibler bei der Erweiterung zu sein (z.B. NAS-System mit iSCSI oder NFS-Anbindung).
- Da der VM-Host die einzelnen VMs kapselt, ist es aus Sicherheitsgründen empfehlenswert, diesen in ein eigenes Netzsegment zu bringen. Der VM-Host sollte nicht im internen Netz der VMs sein.

Hypervisoren

Die Voraussetzungen für einen virtualisierten Betrieb besteht natürlich darin, vorab den Hypervisor/den VM-Host installiert zu haben und Zugriff auf dessen Verwaltung zu haben.

Wo es uns möglich ist, haben wir eine Anleitung dazu geschrieben, um auf die Besonderheiten der Schulnetzumgebung an geeigneter Stelle hinzuweisen.

4.5 Proxmox vorbereiten

Autor des Abschnitts: @cweikl, @MachtDochNix

4.5.1 Hinweise

Für diese Anleitung haben wir uns entschieden, Proxmox als Virtualisierungslösung einzusetzen.

Proxmox ist eine Open Source-Virtualisierungsplattform. Diese kombiniert KVM- und Container-basierte Virtualisierung und verwaltet virtuelle Maschinen, Container, Storage, virtuelle Netzwerke und Hochverfügbarkeit-Cluster übersichtlich über ein web-basierte Managementkonsole.

Die zentrale Managementkonsole läuft direkt auf dem Server. Zudem kann die Virtualisierungsumgebung via SSH administriert werden.

Proxmox

Proxmox VE eignet sich für den virtuellen Betrieb von linuxmuster.net besonders, da dieser Hypervisor dem Open-Source-Konzept entspricht. Der Einsatz wird auf jeglicher Markenhardware unterstützt und es gibt zahlreiche professionelle 3rd-Party Software für Sicherungskopien und andere Features. „No-Name-Hardware“ kann hiermit ebenfalls meist verwendet werden.

Diese Anleitung beinhaltet Angaben zu den notwendigen Systemanforderungen und Festplattenkonfigurationen sowie der anschließenden Installation von Proxmox.

Systemvoraussetzungen

In der unten aufgeführten Tabelle findest Du die Systemvoraussetzungen zum Betrieb der virtuellen Maschinen. Die Systemanforderungen für die Installation von Proxmox selbst finden sich im Web unter <https://www.proxmox.com/de/proxmox-ve/systemanforderungen>.

Die Werte bilden die Mindestvoraussetzungen zur Planung. Für die Installation mit Proxmox und linuxmuster v7.2 wird als Standard der IP-Bereich 10.0.0.0/16 genutzt.

VM	IP	HDD	RAM
OPNsense®	10.0.0.254/16	10 GiB	4 GiB
Server	10.0.0.1/16	25 GiB u. 100 GiB	4 GiB
Proxmox-Host	10.0.0.10/16	500 GiB	4 GiB

Die Festplattengröße sowie der genutzte RAM der jeweiligen VMs kann ggf. vor deren Einrichtung einfach an die Bedürfnisse der Schule angepasst werden.

Bevor Du dieses Kapitel durcharbeitest, lese bitte zuerst die Abschnitte

- *Was ist linuxmuster.net?*
- *Was ist neu in 7.2?*
- *Installationablauf*
- *Vorüberlegungen*

Für den Betrieb des Hypervisor selbst (Proxmox VE) sollten ca. 2 bis 6 GB Arbeitsspeicher eingeplant werden. Um nach Anleitung installieren zu können, sollte der Server mit mindestens zwei Netzwerkkarten bestückt sein. Durch VLANs kann der Betrieb aber auch bereits mit nur einer NIC erfolgen - z. B. eine 10 Gbit-Karte an einem Core-VLAN-Switch (L3).

Der Proxmox-Host sollte gemäß o.g. Minimalanforderungen folgende Merkmale aufweisen:

- RAM gesamt: min. 16 GiB (besser: 32 GiB oder 64 GiB)
- Erste HDD: min. 100 GiB für Proxmox selbst
- Zweite HDD: für die VMs mit mind. 500 GB Kapazität (besser: 1 TiB oder 2 TiB)
- Zwei Netzwerkkarten
- Der Internetzugang des Proxmox-Hosts sollte zunächst gewährleistet sein, d. h. dieser wird z. B. an einen (DSL-)Router angeschlossen, der den Internetzugang sicherstellt. Sobald alles eingerichtet ist, bekommt der Proxmox-Host eine IP-Adresse im Schulnetz und die Firewall OPNsense® stellt den Internetzugang für alle VMs und den Proxmox-Host bereit.

Hinweis: Virtualisierungs-Hosts sollten grundsätzlich niemals im gleichen Netz wie andere Geräte sein, damit dieser nicht von diesen angegriffen werden kann. In dieser Dokumentation wird zur Vereinfachung der Fall dokumentiert, dass der Proxmox-Host zu Beginn im externen Netz mit Internet-Zugriff und nach Abschluss der Installation im internen Schulnetz mit Internet-Zugriff via OPNsense®-Firewall befindet.

4.5.2 Bereitstellen des Proxmox-Hosts

Hinweis: Der Proxmox-Host bildet das Grundgerüst für die Firewall *OPNsense®* und den Schulserver *server*. Die Virtualisierungsfunktionen der CPU sollten zuvor im BIOS aktiviert worden sein.

Die folgende Anleitung beschreibt die *einfachste* Implementierung ohne Dinge wie VLANs, Teaming oder RAID. Diese Themen werden in zusätzlichen Anleitungen betrachtet.

- *Anleitung Netzwerksegmentierung*

Die Download-Quellen für den Proxmox-Host selbst finden sich hier:

<https://www.proxmox.com/de/downloads/category/iso-images-pve/>

Dort findet sich das ISO-Image zur Installation von Proxmox.

Lade Dir dort das aktuellste Image herunter und erstelle Dir einen bootfähigen USB-Stick zur weiteren Installation.

Erstellen eines USB-Sticks zur Installation des Proxmox-Host

Nachdem Du die ISO-Datei für Proxmox heruntergeladen hast, wechselst Du in das Download-Verzeichnis. Danach ermittelst Du den korrekten Buchstaben für den USB-Stick unter Linux. Das X bei sdX ist durch den korrekten Buchstaben für den USB-Stick zu ersetzen (z.B. /dev/sda). Nachstehender Befehl als Benutzer *root* oder mit einem *sudo* vorangestellt einzugeben:

```
dd if=proxmox-ve_8.1-2.iso of=/dev/sdX bs=1M status=progress conv=fdatasync
```

Verkabelungshinweise

Es ist für linuxmuster.net ein internes Netz (grün) und ein externes Netz (rot) am Proxmox-Host zu unterscheiden. Sind zwei Netzwerkkarten im Proxmox-Host vorhanden, so ist die erste Netzwerkkarte (z. B. eth0, eno1 oder enp7s0), die zu Beginn eine IP aus dem bestehenden lokalen Netz (z. B. via DSL-Router) erhalten soll, mit dem Switch zu verbinden, der an den (DSL-)Router angeschlossen ist. Bei einem Home-DSL-Router ist der Switch i.d.R. Regel bereits eingebaut. DSL-Router mit Switch angeschlossen an die erste Netzwerkkarte stellen hier das rote / externe Netz dar. Der Admin-PC ist zu Beginn ebenfalls hier anzuschließen.

Die zweite Netzwerkkarte (z. B. eth1 oder enp7s1) ist dann an einen eigenen Switch anzuschließen, ebenso wie alle Clients, die im internen Netz (grün) eingesetzt werden.

Um zu Beginn den Proxmox-Host zu administrieren, ist ein Laptop/PC mit dem Switch zu verbinden, der an den lokalen (DSL-)Router angeschlossen ist (rotes Netz). Der Laptop/PC erhält ebenfalls eine IP aus dem lokalen (DSL-)Netz und kann sich dann auf die zu Beginn eingerichtete IP-Adresse des Proxmox-Host auf die grafische Verwaltungsoberfläche verbinden.

Abb. 4: Aufbau des Netzwerkes zur Proxmox Installation

Es werden zunächst alle Aktualisierungen durchgeführt und die benötigten ISO-Images auf den Proxmox-Host heruntergeladen. Erst danach wird die Konfiguration des Proxmox-Host so geändert, dass dieser nur noch im grünen Netz erreichbar ist.

4.5.3 Installieren von Proxmox

Basis-Installation

Vom USB-Stick booten, danach erscheint folgender Bildschirm:

Wähle **Install Proxmox VE (Graphical)** und starte die Installation mit **ENTER**.

Bestätige das **End-User-Agreement** mit **Enter**.

Wähle die gewünschte Festplatte auf dem Server zur Installation aus. Hast Du mehrere einzelne Festplatten im Server verbaut und kein RAID-Verbund definiert, so kannst Du hier mit der Schaltfläche *Optionen* weitere Einstellungen aufrufen. Hier kannst Du z. B. mehrere Festplatten angeben, die in einem sog. ZFS-Pool definiert werden sollen. Dies ist für das Erstellen von sog. Snapshots von Vorteil. Soll aber an dieser Stelle nicht vertieft werden. (siehe hierzu u. a.: <https://pve.proxmox.com/pve-docs/pve-admin-guide.html>)

Für unsere beispielhafte Installation wählen wir hier die kleinere der beiden angezeigten aus, also die SSD.

Gib bei **Location and Time Zone selection** als Land und Keyboard Layout **Germany** an. Wähle als Zeitzone **Europe/Berlin**.

Lege ein Kennwort für den Administrator des Proxmox-Host fest und gib eine E-Mail-Adresse an. Klicke auf **Weiter**.



Welcome to Proxmox Virtual Environment

```
Install Proxmox VE (Graphical)
Install Proxmox VE (Console)
Advanced Options
```

Abb. 5: Proxmox Boot Menue

Lege die IP-Adresse des Proxmox-Host fest. Solltest Du intern z. B. auf dem (DSL-)Router einen DHCP-Server laufen haben, dann erhältst Du hier bereits eine vorausgefüllte Konfigurationsseite. Passe diese Werte nun den gewünschten Werten an. Der Hostname des Proxmox-Host ist hier in gewünschter Form – hier *<hostname>* (z.B. *pve*).*linuxmuster.lan* – anzugeben.

Hinweis: Die IP muss zu diesem Zeitpunkt der Installation diejenige Adresse sein, die ebenfalls Zugriff auf das Internet hat. In einem lokalen Netz mit DSL-Router wäre dieses eine aus dem internen Netz, die der Router für die internen Clients verteilt - also z. B. 192.168.199.20/24. DNS- und Gateway-Adressen entsprechen der Router-IP.

Hier wurde die interne IP-Adresse *192.168.199.20/24* festgelegt.

Überprüfe auf der Übersichtsseite, dass alle Angaben korrekt sind und fahre anschließend fort.

Warte den Abschluss der Installation ab.

Nach erfolgreicher Installation lasse Proxmox über *Reboot* neu starten.

Proxmox Einrichtung

Nach dem Neustart von Proxmox kannst Du Dich über einen PC, der sich im selben Netz befindet, via Browser auf das grafische Webinterface zur Verwaltung des Proxmox-Hosts aufschalten. Hierzu gibst Du die URL <https://192.168.199.20:8006> ein. Du erhältst ein Warning, da ein mögliches Sicherheitsrisiko erkannt wurde. Dies ist auf das selbst ausgestellte SSL-Zertifikat des Proxmox-Host zurückzuführen.

Klicke auf **Erweitert** ..., es erscheint ein weiterer Hinweis auf das *self-signed certificate*. Dieses nimmst Du nun mit dem Button **Risiko akzeptieren und fortfahren** an.

Es erscheint die Anmeldemaske des Proxmox-Webinterface. Melde Dich als User *root* und dem vorher gesetzten Passwort an:

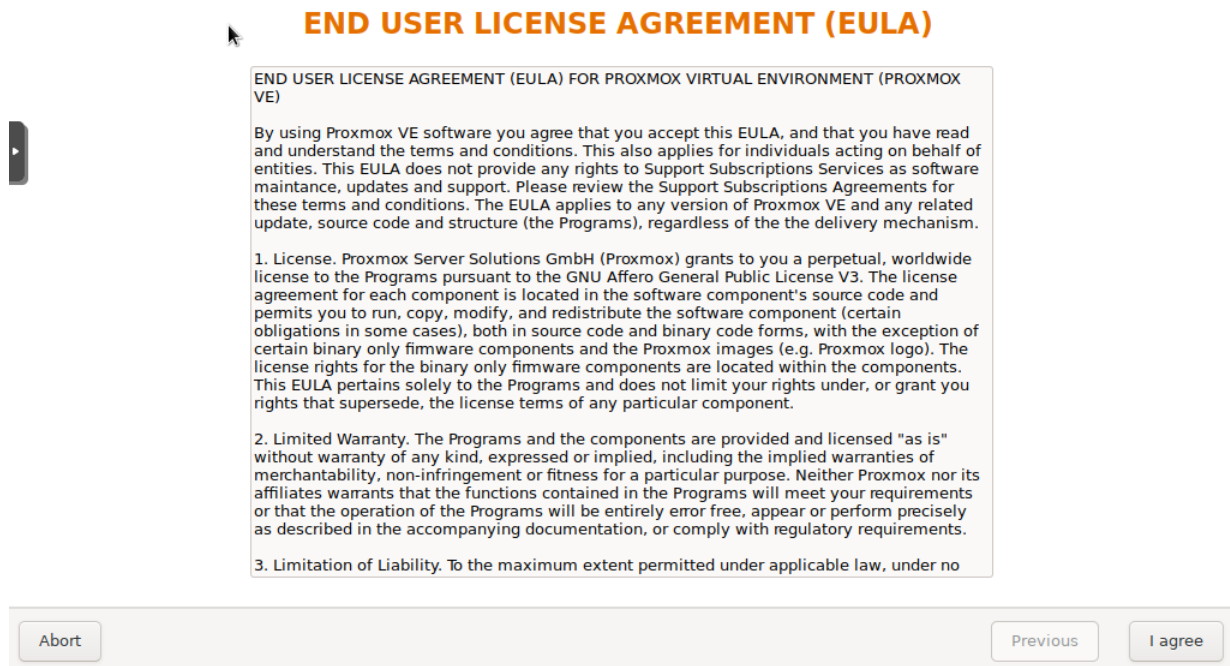


Abb. 6: Proxmox End-User-Agreement



Abb. 7: Proxmox Festplattenauswahl



Location and Time Zone selection

The Proxmox Installer automatically makes location based optimizations, like choosing the nearest mirror to download files. Also make sure to select the right time zone and keyboard layout.

Press the Next button to continue installation.

- **Country:** The selected country is used to choose nearby mirror servers. This will speedup downloads and make updates more reliable.
- **Time Zone:** Automatically adjust daylight saving time.
- **Keyboard Layout:** Choose your keyboard layout.

The screenshot shows the 'Location and Time Zone selection' screen of the Proxmox installer. It features three input fields: 'Country' with a text box containing 'Germany', 'Time zone' with a dropdown menu showing 'Europe/Berlin', and 'Keyboard Layout' with a dropdown menu showing 'German'. At the bottom of the screen, there are three buttons: 'Abort' on the left, 'Previous' in the center, and 'Next' on the right.

Abb. 8: Proxmox Zeitzone



Administration Password and E-Mail Address

Proxmox Virtual Environment is a full featured highly secure GNU/Linux system based on Debian.

Please provide the *root* password in this step.

- **Password:** Please use a strong password. It should have 8 or more characters. Also combine letters, numbers, and symbols.
- **E-Mail:** Enter a valid email address. Your Proxmox VE server will send important alert notifications to this email account (such as backup failures, high availability events, etc.).

Press the Next button to continue installation.

The image shows a configuration window from the Proxmox VE installer. It has a light gray background. At the top, there are three input fields. The first is labeled 'Password' and contains ten black dots. The second is labeled 'Confirm' and also contains ten black dots. The third is labeled 'E-Mail' and contains the text 'admin@linuxmuster.net'. Below these fields, there are three buttons: 'Abort' on the left, 'Previous' in the middle, and 'Next' on the right. The 'Next' button is highlighted with a blue border.

Abb. 9: Admin Password festlegen



Management Network Configuration

Please verify the displayed network configuration. You will need a valid network configuration to access the management interface after installation.

Afterwards press the Next button. You will be shown a list of the options that you chose during the previous steps.

- **IP address:** Set the IP address for your server.
- **Netmask:** Set the netmask of your network.
- **Gateway:** IP address of your gateway or firewall.
- **DNS Server:** IP address of your DNS server.

Management Interface:	ens18 - 32:12:2d:fb:71:c9 (virtio_net) ▼
Hostname (FQDN):	hv01.linuxmuster.lan
IP Address:	192.168.199.20
Netmask:	255.255.255.0
Gateway:	192.168.199.1
DNS Server:	192.168.199.1

Abort Previous Next

Abb. 10: Network Konfiguration



Summary

Please verify the displayed informations. Once you press the **Install** button, the installer will begin to partition your drive(s) and extract the required files.

Option	Value
Filesystem:	ext4
Disk(s):	/dev/sda
Country:	Germany
Timezone:	Europe/Berlin
Keymap:	de
E-Mail:	admin@linuxmuster.net
Management Interface:	ens18
Hostname:	hv01
IP:	192.168.199.20
Netmask:	255.255.255.0
Gateway:	192.168.199.1
DNS:	192.168.199.1

Abb. 11: Zusammenfassung der Installationsoptionen



Installation successful!

The Proxmox Virtual Environment is now installed and ready to use.

- **Next steps**

Reboot and point your web browser to the selected IP address on port 8006:

`https://192.168.199.20:8006`

Also visit www.proxmox.com for more information.

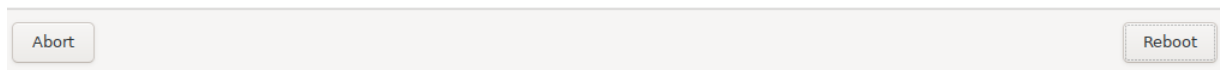


Abb. 12: Installation beendet

A login form titled 'Proxmox VE Login'. It has a light gray background. The form contains four input fields: 'User name:' with the value 'root', 'Password:' with masked characters, 'Realm:' with the value 'Linux PAM standard authentication', and 'Language:' with the value 'English'. Below these fields are two checkboxes: 'Save User name:' and a 'Login' button.

Abb. 13: Proxmox WebUI Login

Im Fenster *No valid subscription* wählst Du *OK* um das Fenster schließen:

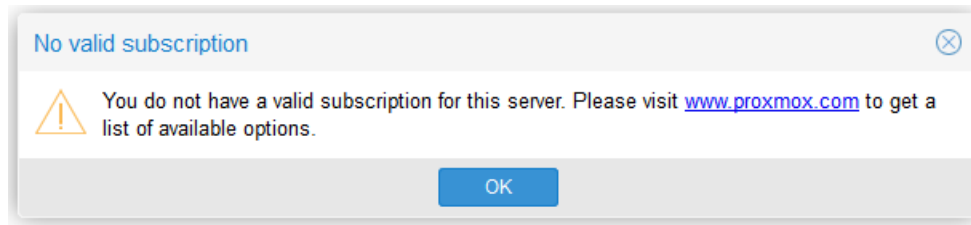


Abb. 14: Proxmox No valid subscription

Updates ermöglichen

Um Proxmox Updates installieren zu können, müssen in der Shell des Nodes <hostname> (z.B. pve) folgende Änderungen an den Repositorien vorgenommen werden. Dafür den Node im Datacenter auswählen und eine Shell öffnen.

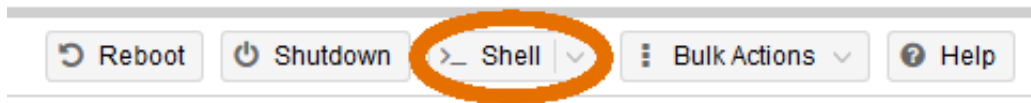


Abb. 15: Proxmox Shell

Kommentiere zuerst die Paketquellen für die Enterprise-Pakete aus, die nach der Erstinstallation automatisch eingerichtet wurden:

```
sed -i -e 's/^#/' /etc/apt/sources.list.d/pve-enterprise.list
sed -i -e 's/^#/' /etc/apt/sources.list.d/ceph.list
```

Füge dann für Proxmox VE eine neu Paketquelle für die No-Subscription-Pakete hinzu.

```
echo "deb http://download.proxmox.com/debian/pve bookworm pve-no-subscription" >> /etc/
apt/sources.list.d/pve-no-subscription.list
```

Aktualisiere danach die Paketquellen und die Pakete:

```
apt update
```

```
apt upgrade -y
```

Netzwerkbrücken einrichten

Für eine funktionierende Umgebung müssen zwei Netzwerkbrücken/Bridges (vSwitch) auf dem Hypervisor eingerichtet werden.

Eine für das interne Netz (green, 10.0.0.0/16) und eine für das externe Netz (red, externes Netz, Internetzugriff).

Nach der zuvor beschriebenen Erstinstallation von Proxmox wurde bislang **nur eine Bridge (vmbr0)** eingerichtet (rotes Netz). Diese ist mit der ersten Netzwerkschnittstelle (NIC) des Proxmox-Hosts verbunden. Das Ethernet-Kabel der 1. NIC ist mit dem (DSL)-Router verbunden. Verließ der vorherige Befehl zur Aktualisierung von Proxmox erfolgreich, so

weißt Du, dass diese Bridge bereits funktioniert und für die weitere Nutzung für das externe Netz (red) - vmbr0 genutzt werden kann.

Für die internen virtuellen Netze ist also eine **zweite Bridge** zu erstellen, die an die zweite Netzwerkkarte direkt gebunden wird. Dieser wird allerdings **keine** IP-Adresse zugeordnet.

Ausgangspunkt: <hostname> -> Network (in u.g. Bild: pve -> Network)

Die **bisherige** Netzwerkkonfiguration stellt sich wie folgt dar:

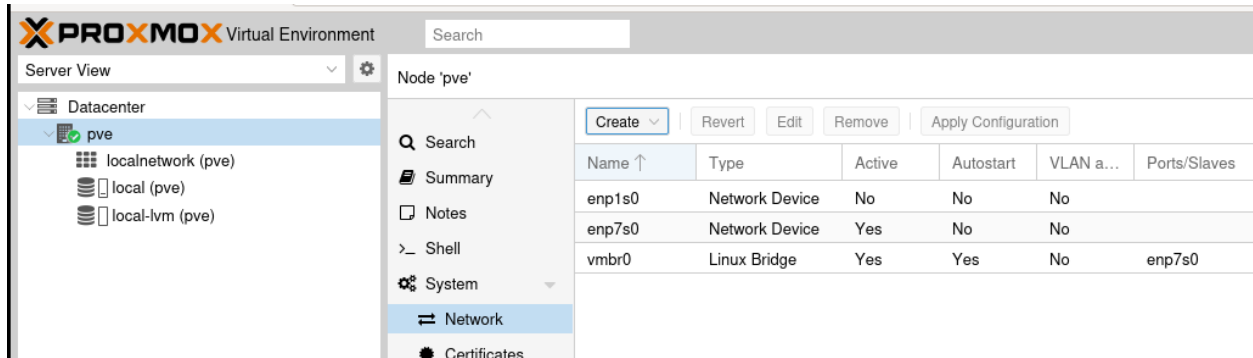


Abb. 16: Proxmox Network

Für die folgende Überprüfung öffnest Du nochmals die Konsole auf dem Hypervisor, falls sie nicht geöffnet sein sollte - wie zuvor beschrieben - und lässt Dir den Inhalt der Konfigurationsdatei anzeigen mittels:

```
cat /etc/network/interfaces
```

Dort befinden sich bisher folgende Eintragungen:

```
auto lo
iface lo inet loopback

# erste physikalische NIC
iface eno1 inet manual

# erste Netzwerkbrücke (bridge)
auto vmbr0
iface vmbr0 inet static
    address 192.168.199.20
    netmask 255.255.255.0
    gateway 192.168.199.1
    bridge_ports eno1
    bridge_stp off
    bridge_fd 0

# zweite physikalische NIC
iface eno2 inet manual
```

Hinweis: Die Bezeichnungen für die Netzwerkkarten eno1, eno2 können je nach eingesetztem System von der dargestellten Bezeichnung abweichen (z.B. enp1s0, enp7s0).

Für das weitere Vorgehen ist es hilfreich, die Funktion der Kommentierung der Netzwerkbrücken zu nutzen. Diese ist für die vmbr0 bisher noch nicht gesetzt.

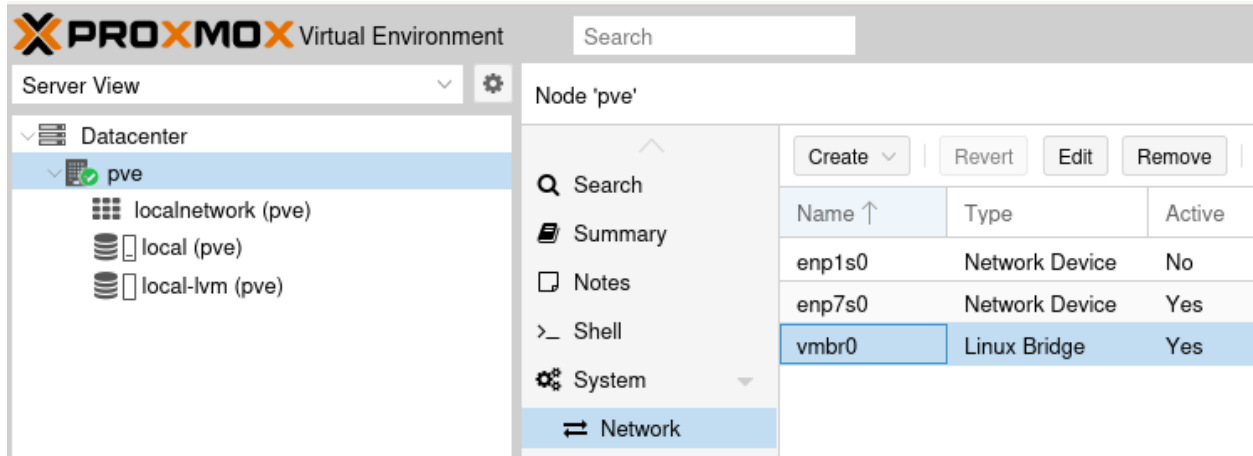


Abb. 17: Änderung der Bridge vmbr0

Markiere wie gezeigt **vmbr0** und betätige den **Edit**-Button, um das Konfigurationsfenster zu öffnen.

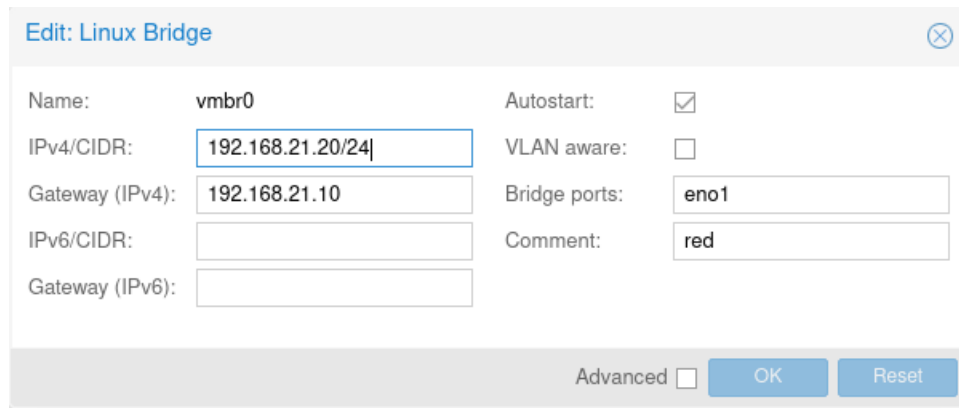


Abb. 18: Kommentar für vmbr0

Trage unter **Comment** einen Kommentar ein, der veranschaulicht, dass diese Brücke die Verbindung zum Internet stellt. Zum Beispiel wie hier gezeigt **red**.

Mit **OK** wird der Kommentar übernommen.

Nun erstellst Du die zweite Bridge **vmbr1**:

Dazu wähle das Menü **Datacenter** → **<hostname>** (z.B. **pve**) → **Network** → **Create** → **Linux Bridge**

Es öffnet sich ein neues Fenster. Dort sind folgende Einträge nötig:

Mit **Create** wird die Brücke erstellen.

Anschließend startest Du Proxmox über den Button **Reboot** oben rechts neu, um die neue Netzwerkkonfiguration zu laden. Node **<hostname>** (z.B. **pve**) muss dafür im Menü **Datacenter** links ausgewählt sein:

Die Netzwerkkonfiguration des Proxmox-Host kannst Du, nach dem Neustart mit `cat /etc/network/interfaces` wie oben gezeigt in der Konsole überprüfen.

Dort sollten sich nun nachstehende Eintragungen befinden. Bei der Bridge **vmbr0** muss die IP-Adresse derjenigen entsprechen, die bei der Installation eingetragen wurde.

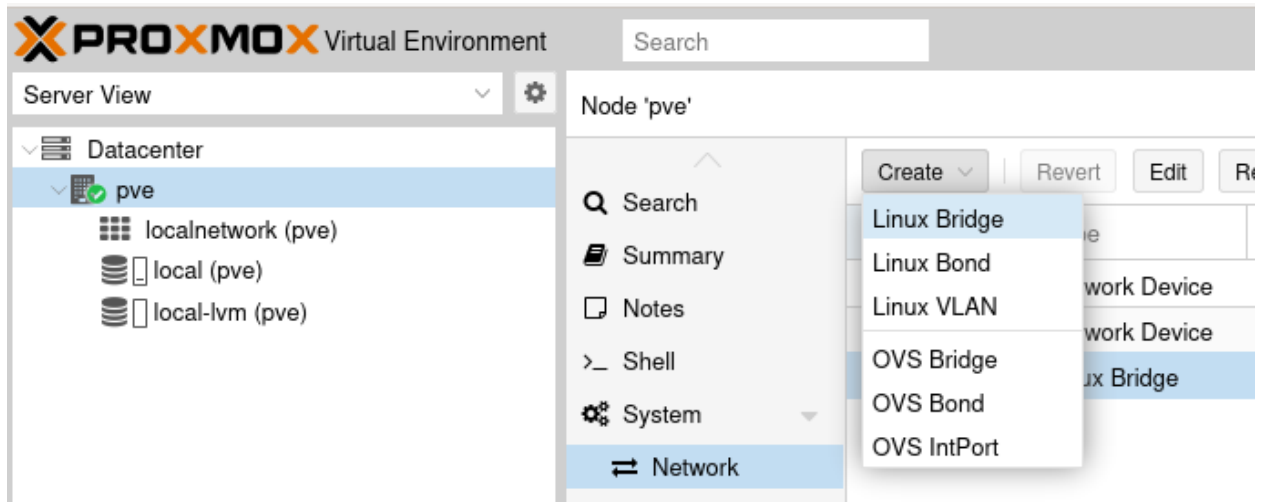


Abb. 19: Linux Bridge erstellen

Create: Linux Bridge

Name:	<input type="text" value="vmbr1"/>	Autostart:	<input checked="" type="checkbox"/>
IPv4/CIDR:	<input type="text"/>	VLAN aware:	<input type="checkbox"/>
Gateway (IPv4):	<input type="text"/>	Bridge ports:	<input type="text" value="eno2"/>
IPv6/CIDR:	<input type="text"/>	Comment:	<input type="text" value="green"/>
Gateway (IPv6):	<input type="text"/>		

☐ Advanced

Abb. 20: Linux Bridge erstellen

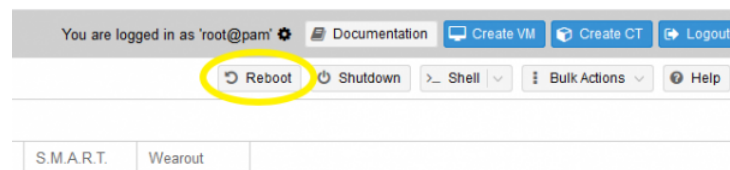


Abb. 21: Proxmox Neustart

```
auto lo
iface lo inet loopback

iface eno1 inet manual

iface eno2 inet manual

auto vmbr0
iface vmbr0 inet static
    address 192.168.199.20/24
    gateway 192.168.199.1
    bridge-ports eno1
    bridge-stp off
    bridge-fd 0
#red

auto vmbr1
iface vmbr1 inet manual
    bridge-ports eno2
    bridge-stp off
    bridge-fd 0
#green
```

Zur Veranschaulichung eine Grafik, die den Status der Konfiguration zeigt.

Abb. 22: Neue Netzwerkschnittstelle eno2 an vmbr1 erzeugt

Festplatten anpassen

In diesem Schritt wird die erste Festplatte angepasst und die zweite in Proxmox eingebunden, um diese als Storage für die virtuellen Maschinen zu nutzen.

Bemerkung: Gemäß der oben genannten Minimalanforderungen gehen wir davon aus, dass in deinem Proxmox-Host zwei Festplatten verbaut sind.

Solltest Du bei der Installation von Proxmox nur einen Speicher nutzen, kannst Du direkt weitergehen zu: [Vorbereiten des ISO-Speichers](#)

Abb. 23: Aufteilung der Festplatten nach der Proxmox Installation

local-lvm(<hostname> (z.B. pve))-Partition entfernen und Speicher freigeben

Während der Proxmox-Installation wurden die Storages `local` und `local-lvm` automatisch auf der ersten Festplatte erstellt. Da anfangs für die Linuxmuster-Maschinen eine zweite Festplatte als Storage eingerichtet wurde, wird `local-lvm` nicht benötigt. Deshalb wird nun `local-lvm` entfernt und `local` durch den freigewordenen Speicher vergrößert, sodass auf der ersten Festplatte der gesamte Speicher dem Hypervisor zur Verfügung steht.

1. auf <hostname> (z.B. pve) oben rechts Shell anklicken:

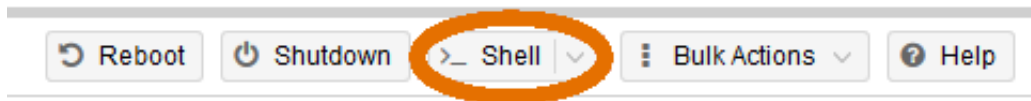


Abb. 24: Shell aufrufen

2. `lsblk` eingeben und mit der Enter-Taste bestätigen; folgende Ausgabe sollte erscheinen:

```
Linux hv01 5.4.44-2-pve #1 SMP PVE 5.4.44-2 (Wed, 01 Jul 2020 16:37:57 +0200) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@hv01:~# lsblk
NAME                                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda                                 8:16   0 111.8G  0 disk
├─sda1                             8:17   0 1007K  0 part
├─sda2                             8:18   0 512M   0 part /boot/efi
└─sda3                             8:19   0 111.3G  0 part
   ├pve-swap                       253:0    0   8G   0 lvm  [SWAP]
   ├pve-root                       253:1    0 27.8G  0 lvm  /
   ├pve-data_tmeta                 253:2    0   1G   0 lvm
   │ └pve-data                    253:4    0 59.7G  0 lvm
   └pve-data_tdata                 253:3    0 59.7G  0 lvm
     └pve-data                    253:4    0 59.7G  0 lvm
sdb                                 8:0    0 931.5G  0 disk
root@hv01:~#
```

Abb. 25: lsblk Befehl

Es ist zu sehen, dass die Festplatten `sda` (111.8G) und `sdb` (931.5G) vorhanden sind.

Die zweite Festplatte `sdb` ist eine HDD mit 1 TB Kapazität und soll für die VMs genutzt werden.

Die erste Festplatte ist eine SSD, auf der Proxmox selbst installiert wurde. Von dieser zweiten Platte startet dieses System automatisch Proxmox. Zudem befindet sich auf `sda3` ein sog. *LVM*. Bei der Erstinstallation wurde hier automatisch ein Bereich für die VMs eingerichtet. Dieser Bereich wird im Folgenden gelöscht und der frei werdende Platz auf `sda` wird vollständig dem Proxmox-Host zugeordnet.

Danach wird die Festplatte `sdb` als LVM für die VM eingerichtet.

3. Vorhandene `local-lvm` entfernen:

```
lvremove /dev/pve/data
```

```
root@hv01:~# lvremove /dev/pve/data
Do you really want to remove and DISCARD active logical volume pve/data? [y/n]: ☐
```

Abb. 26: lvmremove Frage

Bestätige die Nachfrage mit y

```
root@hv01:~# lvremove /dev/pve/data
Do you really want to remove and DISCARD active logical volume pve/data? [y/n]: y
Logical volume "data" successfully removed
root@hv01:~# ☐
```

Abb. 27: lvmremove Ausgabe

4. Speicherbereich von local erweitern:

```
lvresize -l +100%FREE /dev/pve/root
```

```
root@hv01:~# lvresize -l +100%FREE /dev/pve/root
Size of logical volume pve/root changed from 27.75 GiB (7104 extents) to <103.29 GiB
(26441 extents).
Logical volume pve/root successfully resized.
root@hv01:~# ☐
```

Abb. 28: lvresize

5. Filesystem anpassen:

```
resize2fs /dev/mapper/pve-root
```

6. Über lsblk sollte nun zu sehen sein, dass pve-data-Partitionen entfernt wurden:

Es ist zu erkennen, dass auf /dev/sda3 nur noch pve-swap und pve-root vorhanden sind.

7. Auf der Weboberfläche von Proxmox ist der local-lvm Eintrag noch über Datacenter → Storage local-lvm (<hostname> (z.B. pve)) mit dem Remove-Button grafisch zu entfernen:

Danach findest Du noch folgenden Speicher in der Weboberfläche:

In der schematischen Darstellung ergibt sich nun folgendes Bild:

Zweiten Datenträger als Speicher einbinden

Die SSD /dev/sda steht für den Proxmox-Host zur Verfügung.

Zweiten Datenträger vorbereiten

Die zweite Festplatte heißt sdb und ersetzt die pve-data-Partition, die im vorigen Schritt entfernt wurde. Um diese für Proxmox vorzubereiten, stellt man über Konsolenbefehle einige Konfigurationen ein. Falls die Shell noch nicht geöffnet ist, wie oben beschrieben, öffnen und folgende Befehle eingeben:

```

root@hv01:~# resize2fs /dev/mapper/pve-root
resize2fs 1.44.5 (15-Dec-2018)
Filesystem at /dev/mapper/pve-root is mounted on /; on-line resizing required
old_desc_blocks = 4, new_desc_blocks = 13
The filesystem on /dev/mapper/pve-root is now 27075584 (4k) blocks long.

root@hv01:~# █

```

Abb. 29: Konsolenausgabe

```

root@hv01:~# lsblk
NAME                MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
sda                  8:16   0 111.8G  0 disk
├─sda1                8:17   0  1007K  0 part
├─sda2                8:18   0   512M  0 part /boot/efi
└─sda3                8:19   0 111.3G  0 part
   ├─pve-swap          253:0    0    8G    0 lvm  [SWAP]
   └─pve-root          253:1    0 103.3G  0 lvm  /
sdb                  8:0    0 931.5G  0 disk
root@hv01:~# █

```

Abb. 30: lsblk Konsolenausgabe

The screenshot shows the Proxmox VE web interface. On the left, the 'Server View' sidebar shows the 'Datacenter' tree with 'hv01' selected, containing 'local (hv01)' and 'local-lvm (hv01)'. The main panel is titled 'Datacenter' and shows a table of storage configurations. The 'local-lvm' entry is selected and highlighted in blue.

ID ↑	Type	Content	Path/Target	Sh...	En...
local	Dir...	VZDump backup file, I...	/var/lib/vz	No	Yes
local-lvm	LV...	Disk image, Container		No	Yes

Abb. 31: Festplatten Default-Einstellungen

The screenshot shows the Proxmox VE web interface after the 'local-lvm' storage has been deleted. The 'Datacenter' sidebar still shows 'local (hv01)', but 'local-lvm (hv01)' is no longer present. The main panel shows only the 'local' storage entry in the table.

ID ↑	Type	Content	Path/Target	Sh...	En...
local	Dir...	VZDump backup file, I...	/var/lib/vz	No	Yes

Abb. 32: Zustand nach Löschung des local-lvm

Abb. 33: Aufteilung der Festplatten nach der Anpassung

Hinweis: Für folgende Schritte: Die Bezeichnungen `vg-xxx` & `lv-xxx` Namen solltest Du auf Deine Festplattengrößen entsprechend anpassen, die folgenden Grafiken dienen zur Orientierung: `vg-hdd-1000` eignet sich beispielsweise für ein Volume aus einer HDD mit 1 TiB Kapazität.

1. Datenträger vorher partitionieren, z. B. mit `fdisk /dev/sdb → g → n → w` (über `lsblk` den richtigen Datenträgernamen herausfinden; in diesem Fall `sdb`)

```
root@hv01:~# fdisk /dev/sdb

Welcome to fdisk (util-linux 2.33.1).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0xa613b408.

Command (m for help): g
Created a new GPT disklabel (GUID: 19024F29-2F14-004C-853A-E8C2DA023AE2).

Command (m for help): n
Partition number (1-128, default 1):
First sector (2048-1953525134, default 2048):
Last sector, +/-sectors or +/-size{K,M,G,T,P} (2048-1953525134, default 1953525134):

Created a new partition 1 of type 'Linux filesystem' and of size 931.5 GiB.

Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.

root@hv01:~#
```

Abb. 34: fdisk

2. Jetzt eine neue Partition auf der Festplatte anlegen - `pvccreate /dev/sd<xy>1`

Beispiel:

```
pvccreate /dev/sdb1
```

und anschließend mit `y` bestätigen:

```
root@hv01:~# pvccreate /dev/sda1
Physical volume "/dev/sda1" successfully created.
root@hv01:~#
```

Abb. 35: vgcreate

3. Nun wird eine virtuelle Gruppe auf der ersten Partition der zweiten Festplatte eingerichtet: `vgcreate vg-<disk>-<size> /dev/sd<xy>1`

Beispiel:

```
vgcreate vg-hdd-1000 /dev/sdb1
```

```
root@hv01:~# vgcreate vg-hdd-1000 /dev/sda1
Volume group "vg-hdd-1000" successfully created
root@hv01:~#
```

Abb. 36: vgcreate

4. mit `lvcreate -l 99%VG -n lv-<disk>-<size> vg-<disk>-<size>` nun das logical volume erstellen.
Hier ist die virtuelle Festplatte eine HDD mit 1 TiB Speicher, weshalb die Namen im Befehl so angepasst werden:

Beispiel:

```
lvcreate -l 99%VG -n lv-hdd-1000 vg-hdd-1000
```

```
root@hv01:~# lvcreate -l 99%VG -n lv-hdd-1000 vg-hdd-1000
Logical volume "lv-hdd-1000" created.
root@hv01:~#
```

Abb. 37: output lvcreate

5. `lvconvert --type thin-pool vg-<disk>-<size>/lv-<disk>-<size>` konvertiert den Speicherbereich der erstellten virtual group als „thin-pool“:

Beispiel:

```
lvconvert --type thin-pool vg-hdd-1000/lv-hdd-1000
```

```
root@hv01:~# lvconvert --type thin-pool vg-hdd-1000/lv-hdd-1000
Thin pool volume with chunk size 512.00 KiB can address at most 126.50 TiB of data.
WARNING: Pool zeroing and 512.00 KiB large chunk size slows down thin provisioning.
WARNING: Consider disabling zeroing (-Zn) or using smaller chunk size (<512.00 KiB).
WARNING: Converting vg-hdd-1000/lv-hdd-1000 to thin pool's data volume with metadata
wiping.
THIS WILL DESTROY CONTENT OF LOGICAL VOLUME (filesystem etc.)
Do you really want to convert vg-hdd-1000/lv-hdd-1000? [y/n]: y
Converted vg-hdd-1000/lv-hdd-1000 to thin pool.
root@hv01:~#
```

Abb. 38: lvconvert

Datenträger grafisch als Storage in Proxmox anbinden

1. Im Menü *Datacenter > Storage > Add* wählt man „LVM-Thin“ aus. Im ID-Feld wird der Name des virtuellen Datenträgers angegeben. In diesem Fall ist es eine HDD mit 1 TiB Speicherkapazität, weshalb die Bezeichnung `vd-hdd-1000` gewählt wird. Unter Volume Group die erstellte virtuelle Gruppe auswählen, welche hier `vg-hdd-1000` ist:
2. Nun sollte im linken Menü der zweite Storage zu sehen sein, auf welchem die Maschinen für Linuxmuster installiert werden können:

Hier noch der Vollständigkeitshalber die schematische Darstellung, wie sie sich jetzt zeigt:

Add: LVM-Thin

ID:vd-hdd-1000

Nodes:hv01

Volume group:vg-hdd-1000

Enable:☒

Thin Pool:lv-hdd-1000

Content:Disk image, Container

Help

Add

Abb. 39: LVM-Thin hinzugefügt

PROXMOX Virtual Environment

Search

Documentation

Create VM

Server View

Datacenter

hv01

- local (hv01)
- vd-hdd-1000 (hv01)

Search

Summary

Cluster

Ceph

Options

Storage

AddRemoveEdit

ID ↑	Type	Content	Path/Target
local	Dir...	VZDump backup file, I...	/var/lib/vz
vd-hdd-1000	LV...	Disk image, Container	

Abb. 40: Zweite HDD

Abb. 41: Aufteilung der Festplatten nach der Anpassung

4.5.4 Vorbereiten des ISO-Speichers

Um die v7.2 zu installieren, müssen zwei virtuelle Maschinen angelegt werden. OPNsense und Ubuntu Server LTS werden in diese VMs installiert. Dazu ist es erforderlich, dass Du die ISO-Images für OPNsense und Ubuntu Server LTS auf den Proxmox-Hypervisor in den Datenspeicher für ISO-Images lädst.

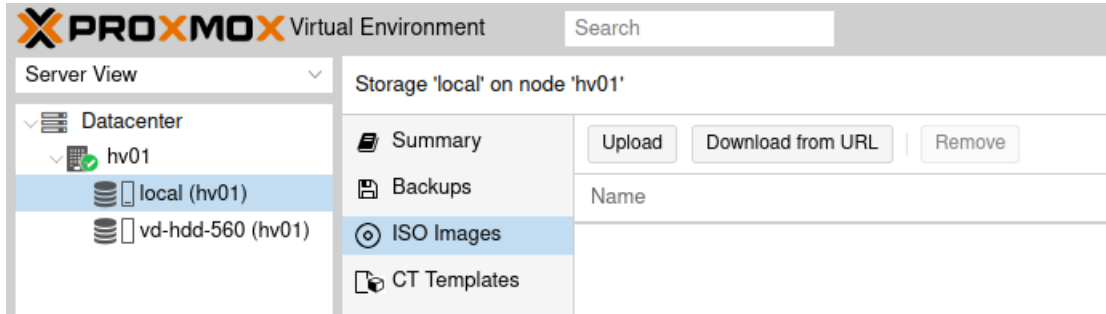


Abb. 42: ISO-Images

Gehe dazu auf Datacenter -> <proxmox-host> -> Datenspeicher (auf local oder zfsfile) -> ISO Images -> Download from URL

Ubuntu Server

Hinweis: Beachte für den Download des Ubuntu Servers, dass du immer die Version verwendest, die in den Systemvoraussetzungen genannt wurde. Gehe auf <https://releases.ubuntu.com/jammy/> und überprüfe die dort zum Herunterladen angebotene Version für 22.04.?-live-server-amd64 und deren Checksumme.

Zum jetzigen Zeitpunkt ist dies in der Angabe der URL berücksichtigt, muss also eventuell angepasst werden.

In dem nun geöffneten Fenster trägst Du die URL

`https://releases.ubuntu.com/jammy/ubuntu-22.04.3-live-server-amd64.iso`

ein (copy&paste). Anschließend betätigst Du dann den Button Query URL.

Abb. 43: Proxmox Download via URL

Wenn die Abfrage der URL positiv war, sollten sich die Felder ausgefüllt haben.

Zur Überprüfung der Integrität der Datei aktiviere `Verify certificates`, das sich unter den Advanced Optionen befindet.

Wähle wie dargestellt: SHA-256 und trage die Checksumme ein:

Hinweis: Sollte sich nach der Erstellung dieser Beschreibung eine Änderung der herunterzuladen Image-Datei ergeben haben, wirst du die Checksumme anpassen müssen.

```
a4acfda10b18da50e2ec50ccaf860d7f20b389df8765611142305c0e911d16fd
```

Das Herunterladen des ISOs beginnt mit Download.

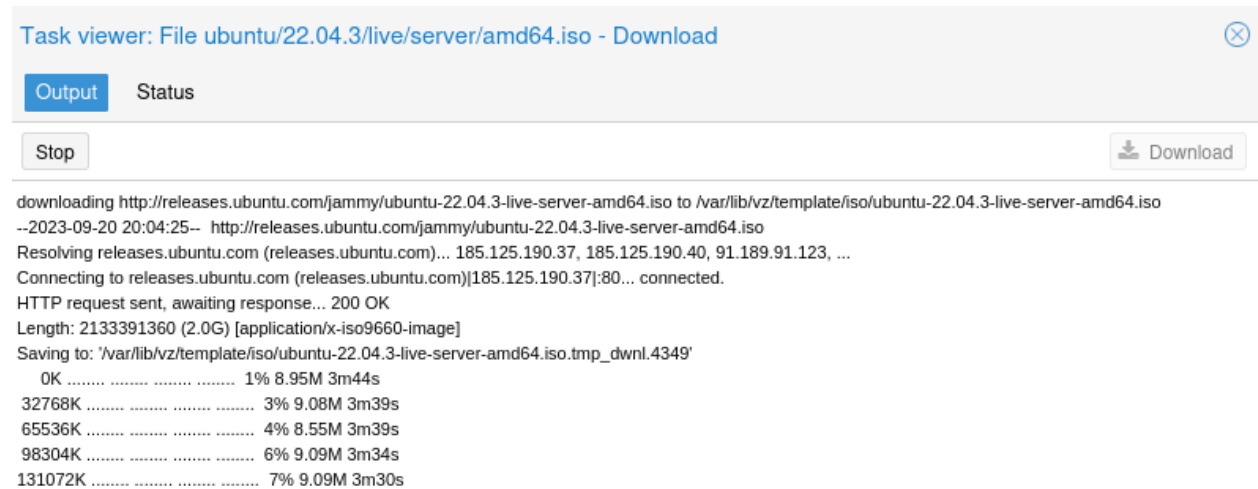


Abb. 44: Download Status

Zum Abschluss erfolgt die Überprüfung der Checksumme, die mit `OK, checksum verified` enden muss.

Nach dem Schließen des Fensters,

befindet sich das heruntergeladene Ubuntu-ISO nun in dem `ISO Images` und steht Dir für die weitere Verwendung zur Verfügung.

OPNsense

Die zuvor gezeigte Möglichkeit des einfachen Imports mit den Bordmitteln von Proxmox steht Dir für die OPNsense® leider nicht zur Verfügung, da nur der Download einer bz2-Datei möglich ist. Dir steht der Weg des Downloads auf einen lokalen PC, der Umwandlung des bz2-File in eine iso-Datei und dann der Upload über den Dir im Abschnitt Ubuntu aufgezeigten Ablauf frei. Dabei wählst Du dann nicht URL, sondern Upload.

Um Dir den Upload zu ersparen, beschreiben wir hier den Weg, um die benötigten Dateien direkt in Deine Proxmox-Maschine zu bringen:

Als Erstes startest Du die Konsole `xterm.js` wie dargestellt, falls sie nicht sowieso gestartet ist.

Mit ihr hast Du jetzt die Möglichkeit, mit Copy&Paste die folgenden bash-Zeilen direkt zu übernehmen.

Als Nächstes musst Du in das Verzeichnis wechseln, wo Proxmox die ISO-Dateien sucht. Dazu kopierst Du diese Zeile in das gezeigte Fenster.

Task viewer: File ubuntu/22.04.3/live/server/amd64.iso - Download

Output Status

Stop Download

```

1441792K ..... 70% 9.09M 1m49s
1474560K ..... 72% 8.57M 1m42s
1507328K ..... 73% 9.09M 96s
1540096K ..... 75% 9.07M 89s
1572864K ..... 77% 8.56M 83s
1605632K ..... 78% 9.09M 77s
1638400K ..... 80% 9.09M 70s
1671168K ..... 81% 8.54M 64s
1703936K ..... 83% 9.09M 58s
1736704K ..... 84% 9.09M 53s
1769472K ..... 86% 8.52M 47s
1802240K ..... 88% 9.09M 41s
1835008K ..... 89% 9.09M 35s
1867776K ..... 91% 8.55M 30s
1900544K ..... 92% 9.09M 24s
1933312K ..... 94% 8.09M 19s
1966080K ..... 95% 9.01M 14s
1998848K ..... 97% 9.09M 8s
2031616K ..... 99% 8.18M 3s
2064384K ..... 100% 9.09M=5m31s
2023-09-20 20:12:03 (6.14 MB/s) - '/var/lib/vz/template/iso/ubuntu-22.04.3-live-server-amd64.iso.tmp_dwnl.4645' saved [2133391360/2133391360]
calculating checksum...OK, checksum verified
download of 'http://releases.ubuntu.com/jammy/ubuntu-22.04.3-live-server-amd64.iso' to '/var/lib/vz/template/iso/ubuntu-22.04.3-live-server-amd64.iso' finished
TASK OK

```

Abb. 45: Prüfsummen bestätigt

PROXMOX Virtual Environment

Server View

Datacenter

- pve
 - localnetwork (pve)
 - local (pve)
 - local-lvm (pve)

Storage 'local' on node 'pve'

- Summary
- Backups
- ISO Images
- CT Templates
- Permissions

Upload Download from URL Remove

Name

ubuntu-22.04.3-live-server-amd64.iso

Abb. 46: ISO-Images

Abb. 47: Nach der Bereitstellung des Ubuntu Installationsmediums

Documentation Create VM Create

Reboot Shutdown

Shell

- noVNC
- SPICE
- xterm.js

Abb. 48: xterm shell öffnen

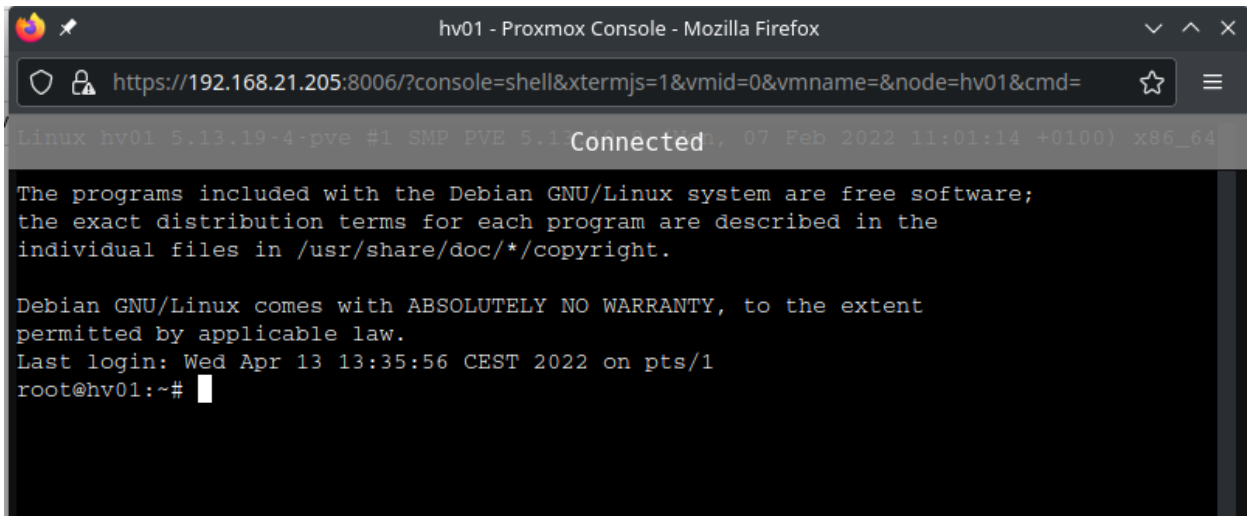


Abb. 49: xterm shell

```
cd /var/lib/vz/template/iso
```

Mit [Enter] wechselst Du dann in das Verzeichnis.

Dann musst Du die folgenden vier Dateien herunterladen:

Prüfsummendatei (<filename>.sha256)

```
wget https://mirror.informatik.hs-fulda.de/opnsense/releases/24.1/OPNsense-24.1-  
checksums-amd64.sha256
```

Signatur Datei (<filename>.sig)

```
wget https://mirror.informatik.hs-fulda.de/opnsense/releases/24.1/OPNsense-24.1-dvd-  
amd64.iso.sig
```

Der öffentliche Schlüssel von OPNsense® (<filename>.pub)

```
wget https://mirror.informatik.hs-fulda.de/opnsense/releases/24.1/OPNsense-24.1.pub
```

Die komprimierte ISO Datei (<filename>.iso.bz2)

```
wget https://mirror.informatik.hs-fulda.de/opnsense/releases/24.1/OPNsense-24.1-dvd-  
amd64.iso.bz2
```

Nun gilt es, die ISO-Datei auszupacken. Das machst Du mit folgendem Befehl:

```
bunzip2 OPNsense-24.1-dvd-amd64.iso.bz2
```

Das Entpacken kann einige Zeit in Anspruch nehmen. Anschließend sollte sich in dem Verzeichnis die OPNsense-ISO-Datei befinden.

Überprüfen der heruntergeladenen Dateien auf deren Integrität:

```
openssl base64 -d -in OPNsense-24.1-dvd-amd64.iso.sig -out /tmp/image.sig
```

```
openssl dgst -sha256 -verify OPNsense-24.1.pub -signature /tmp/image.sig OPNsense-24.1-
→dvd-amd64.iso.bz2
```

Der letzte Befehl sollte Dir ein Verified OK liefern.

Somit hast Du nun alle nötigen ISO-Dateien für die weitere Installation zusammen. Die daneben befindlichen anderen OPNsense-Datei kannst Du nun wieder löschen.

```
rm OPNsense*.sha256 OPNsense*.pub OPNsense*.sig
```

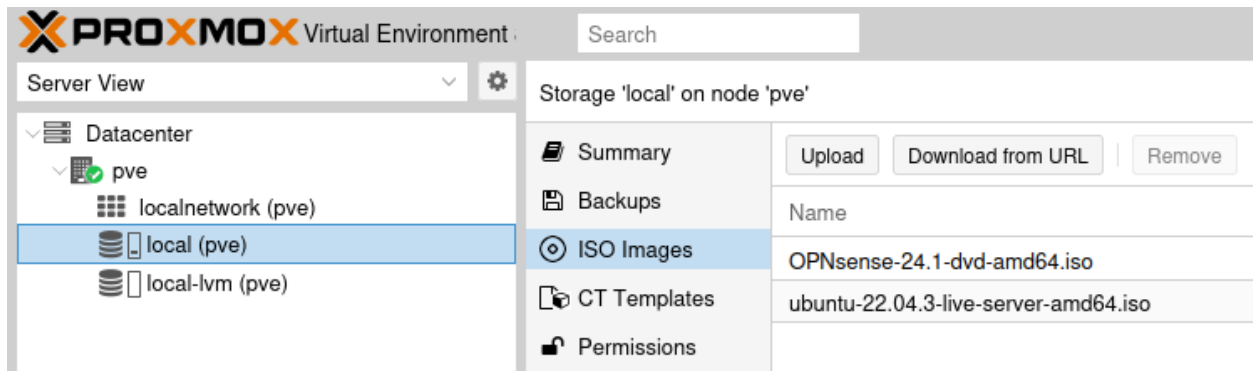


Abb. 50: ISO-Images

Es sind beide ISO Images auf den ISO-Speicher in Proxmox verfügbar, Du richtest nun die VMs ein.

Abb. 51: Nach der Bereitstellung des OPNsense Installationsmediums

4.5.5 Vorbereiten der virtuellen Maschinen

Anlegen der VM für OPNsense

Um für die OPNsense Firewall eine VM anzulegen, wählst Du in der Proxmox - Verwaltungsoberfläche den Button Create VM.



Abb. 52: VM anlegen

Es erscheint nun das Fenster zur Anlage der neuen VM. Trage hier einen Namen für die VM ein, anhand der Du Version und Funktion erkennst.

Klicke dann auf Next.

Wähle nun den ISO-Datenspeicher unter Storage aus. Das ist der Speicher, auf den Du vorher die ISO-Images abgelegt hast. Wähle dann das ISO image der OPNsense aus.

Klicke dann auf Next.

Belasse hier zunächst alle Voreinstellungen für Grafikkarte und Festplatten-Controller wie angezeigt.

Klicke dann auf Next.

Create: Virtual Machine

General OS System Disks CPU Memory Network Confirm

Node: pve Resource Pool:

VM ID: 100

Name: Imn-opnsense

Abb. 53: VM erstellen

Create: Virtual Machine

General OS System Disks CPU Memory Network Confirm

☒ Use CD/DVD disc image file (iso) Guest OS:

Storage: local Type: Linux

ISO image: OPNsense-24.1-dvd-amd64.iso Version: 6.x - 2.6 Kernel

☐ Use physical CD/DVD ☐ Do not use any disc image

Name	For...	Size
OPNsense-24.1-dvd-amd64.iso	iso	1.63 GB
ubuntu-22.04.3-live-server-amd64.iso	iso	2.13 GB

Abb. 54: VM ISO Image

Create: Virtual Machine

General OS System Disks CPU Memory Network Confirm

Graphic card: Default SCSI Controller: VirtIO SCSI single

Machine: Default (i440fx) Qemu Agent: ☐

Firmware

BIOS: Default (SeaBIOS) Add TPM: ☐

Abb. 55: VM OS

Wähle nun hier unter Storage den geeigneten Datenspeicher auf, um die Festplatte der VM dort abzulegen. In der Abb. wird der Datenspeicher Dataset verwendet. In dem Drop-down Menü siehst Du alle in Deinem System verfügbaren Datenspeicher.

Hinweis: Folgende Größenangaben beziehen sich, wie schon geschrieben, auf eine Testumgebung. Wie in der Dokumentation schon ausgeführt, solltest Du hier für den produktiven Einsatz - **mindestens 8 GiB RAM und 50 GiB für die Festplatte** wählen, um alle OPNsense® Standardfunktionen auszuführen.

Damit funktioniert jede Funktion, aber vielleicht nicht bei einer großen Anzahl von Benutzern oder hoher Last. Für andere Einsatzszenarien solltest Du Dich unbedingt mit den [Hardware-Anforderungen](#) gemäß der OPNsense®-Dokumentation auseinandersetzen.

The screenshot shows the 'Create: Virtual Machine' window with the 'Disks' tab selected. On the left, a list shows 'scsi0' with a red trash icon. The main area has two sub-tabs: 'Disk' (active) and 'Bandwidth'. Under 'Disk', the following settings are visible:

- Bus/Device: SCSI 0
- Cache: Default (No cache)
- SCSI Controller: VirtIO SCSI
- Discard: ☐
- Storage: Dataset
- Disk size (GiB): 10
- Format: Raw disk image (raw)

Abb. 56: VM Festplatte

Klicke dann auf Next.

Gib nun für die CPU Sockel und Kerne an.

The screenshot shows the 'Create: Virtual Machine' window with the 'CPU' tab selected. The settings are as follows:

- Sockets: 2
- Cores: 2
- Type: x86-64-v2-AES
- Total cores: 4

Abb. 57: VM CPU

Klicke dann auf Next.

Gib nun für die Firewall die gewünschte Größe des Arbeitsspeichers an.

Klicke dann auf Next.

Gib danach die Bridge `vmbri0` für die einzurichtende Netzwerkkarte an. Die zweite Netzwerkkarte fügst Du nach Anlage der VM hinzu. Dies muss noch vor der eigentlichen Installation erfolgen.

Klicke dann auf Next.

Zum Abschluss siehst Du nochmals alle Einstellungen für die VM. Überprüfe diese. Solltest Du Änderungen vornehmen wollen, kannst Du auf die entsprechende Reiterkarte klicken, Änderungen durchführen und wieder zur Reiterkarte **Confirm** wechseln.

Create: Virtual Machine

General

OS

System

Disks

CPU

Memory

Network

Confirm

Memory (MiB):

4096

Abb. 58: VM Arbeitsspeicher

Create: Virtual Machine

General

OS

System

Disks

CPU

Memory

Network

Confirm

☐ No network device

Bridge:

vmbr0

Model:

VirtIO (paravirtualized)

VLAN Tag:

no VLAN

MAC address:

auto

Firewall:

☒

Abb. 59: VM Netzwerkkarte

Create: Virtual Machine

General

OS

System

Disks

CPU

Memory

Network

Confirm

Key ↑	Value
cores	2
ide2	local:iso/OPNsense-24.1-dvd-amd64.iso,media=cdrom
memory	4096
name	lmn-opnsense
net0	virtio,bridge=vmbr0,firewall=1
nodename	lmn-proxmox-testserver
numa	0
ostype	l26
scsi0	Dataset:10
scsihw	virtio-scsi-pci
sockets	2
vmid	100

☐ Start after created

Advanced ☐

Back

Finish

Abb. 60: VM Erstellung bestätigen

Achte darauf, dass die Option `Start after created` unbedingt deaktiviert ist.

Klicke dann auf **Finish**.

Hinzufügen einer weiteren Netzwerkbrücke

Nachdem die VM angelegt wurde, wähle diese aus und klicke auf den Eintrag **Hardware**.

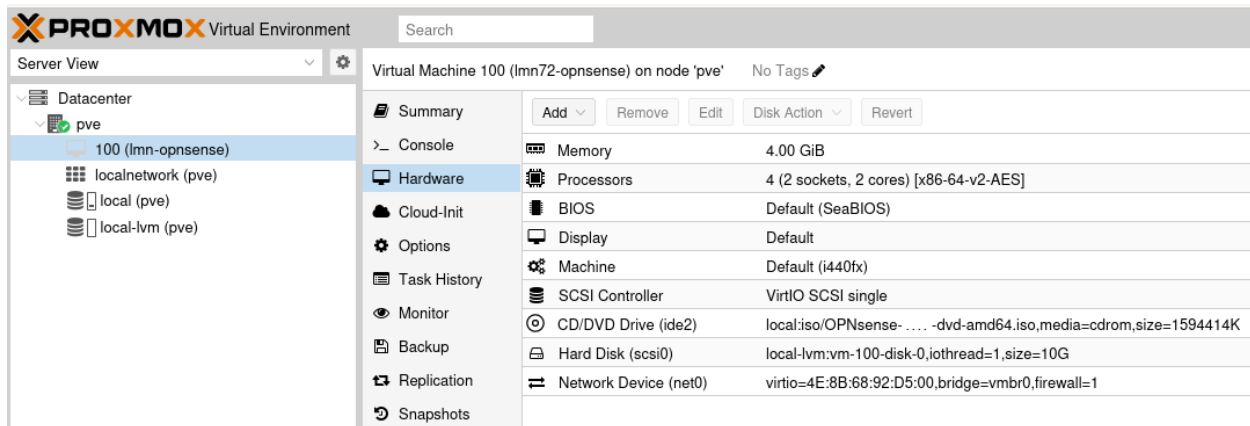


Abb. 61: VM Hardware

Füge nun die zweite Netzwerkkarte hinzu oder ggf. weitere NICs. Klicke hierzu oben auf die Reiterkarte **Add**. Es erscheint ein Drop-down Menü. Wähle hier den Eintrag **Network Device**.

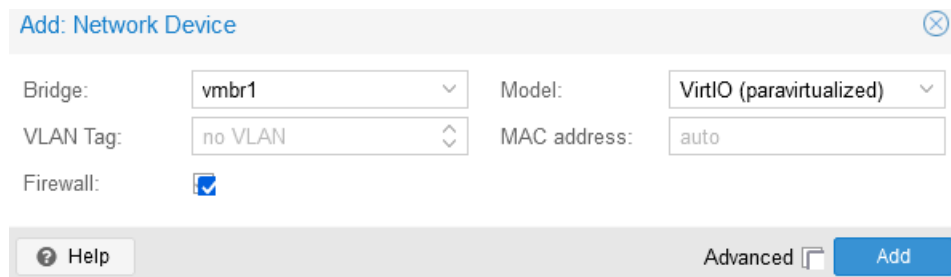


Abb. 62: VM zweite NIC anlegen

Wähle als Bridge die zweite zuvor eingerichtete Bridge – hier `vmbr1`.

Achte für die weitere Installation darauf, wie Du die Bridges zugeordnet hast:

1. `vmbr 0` - externes Netzwerk: red
2. `vmbr 1` - internes Netzwerk: green

Klicke auf **Add**.

Abb. 63: Stand nach der Erzeugung der Virtuellen Maschine OPNsense

Anlegen der VM für linuxmuster server

Um für den linuxmuster.net Server v7.2 die VM anzulegen, wählst Du erneut in der Proxmox - Verwaltungsoberfläche den Button Create VM.



Abb. 64: VM anlegen

Es erscheint nun das Fenster zur Anlage der neuen VM. Trage hier einen Namen für die VM ein, anhand der Du Version und Funktion erkennst.

Abb. 65: VM erstellen

Klicke dann auf Next.

Wähle nun den ISO-Datenspeicher unter Storage aus. Das ist der Speicher, auf den Du vorher die ISO-Images abgelegt hast. Wähle dann das ISO image des Ubuntu Server aus.

Name	For...	Size
OPNsense-23.7-dvd-amd64.iso	iso	1.63 GB
ubuntu-22.04.3-live-server-amd64.iso	iso	2.13 GB

Abb. 66: VM ISO Image

Klicke dann auf Next.

Belasse hier zunächst alle Voreinstellungen für Grafikkarte und Festplatten-Controller wie angezeigt.

Klicke dann auf Next.

The screenshot shows the 'Create: Virtual Machine' dialog box with the 'System' tab selected. The tabs are General, OS, System, Disks, CPU, Memory, Network, and Confirm. The 'System' tab contains the following settings:

- Graphic card: Default
- Machine: Default (i440fx)
- Firmware: BIOS
- BIOS: Default (SeaBIOS)
- SCSI Controller: VirtIO SCSI single
- Qemu Agent: ☐
- Add TPM: ☐

Abb. 67: VM OS

Wähle nun hier unter Storage den geeigneten Datenspeicher aus, um die Festplatte der VM dort abzulegen. In der Abb. wird der Datenspeicher Dataset verwendet. In dem Drop-down Menü siehst Du alle in Deinem System verfügbaren Datenspeicher.

The screenshot shows the 'Create: Virtual Machine' dialog box with the 'Disks' tab selected. The tabs are General, OS, System, Disks, CPU, Memory, Network, and Confirm. The 'Disks' tab contains the following settings for the 'scsi0' disk:

- Bus/Device: SCSI 0
- Cache: Default (No cache)
- SCSI Controller: VirtIO SCSI
- Discard: ☐
- Storage: Dataset
- Disk size (GiB): 25
- Format: Raw disk image (raw)

At the bottom left, there is an 'Add' button. At the bottom right, there are 'Back' and 'Next' buttons, and an 'Advanced' checkbox.

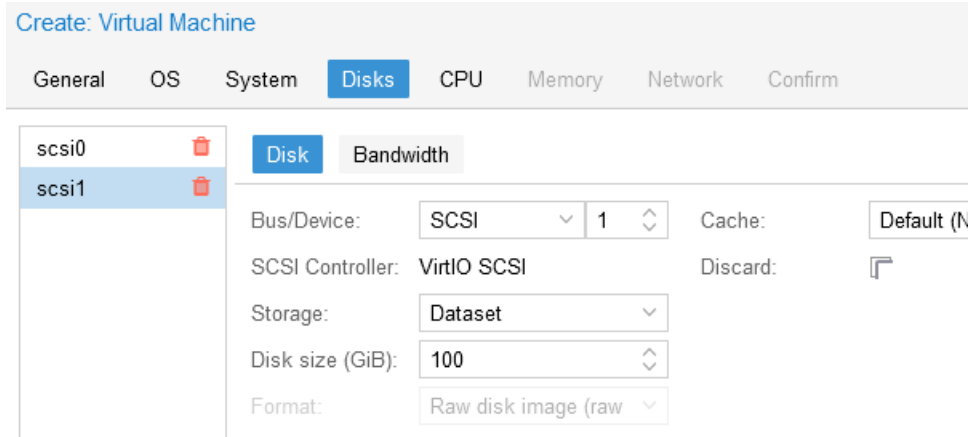
Abb. 68: VM Festplatten

Für die erste Festplatte wählst Du wie in obiger Abb. z. B. 25 GiB.

Füge dann mit dem Button unten links Add eine weitere Festplatte hinzu. Wähle hierbei wieder den geeigneten Datenspeicher aus und die Größe von z. B. 100 GiB, oder direkt für Deine Schule die gewünschte Größe z. B. 500 GiB aus.


Klicke dann auf Next.


Gib nun für die CPU Sockel und Kerne an.



Create: Virtual Machine

General OS System **Disks** CPU Memory Network Confirm

scsi0 

scsi1 

Disk Bandwidth

Bus/Device: SCSI 1 Cache: Default (N)

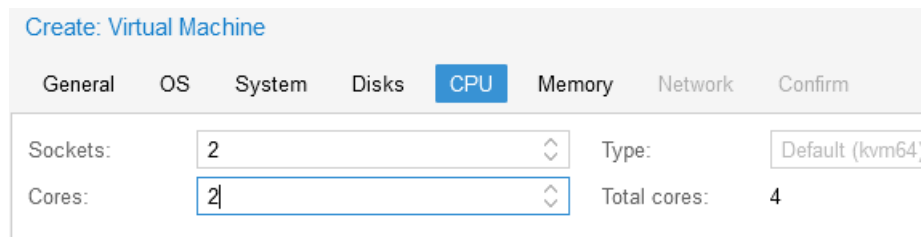
SCSI Controller: VirtIO SCSI Discard: ☐

Storage: Dataset

Disk size (GiB): 100

Format: Raw disk image (raw)

Abb. 69: Vm Festplatten



Create: Virtual Machine

General OS System Disks **CPU** Memory Network Confirm

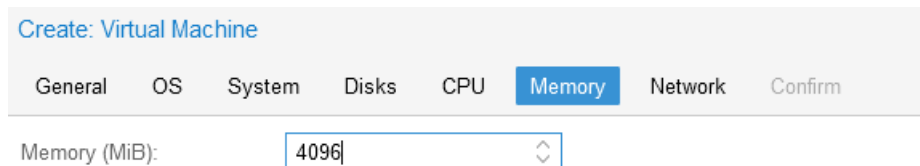
Sockets: 2 Type: Default (kvm64)

Cores: 2 Total cores: 4

Abb. 70: VM CPU

Klicke dann auf Next.

Gib nun für den Server die gewünschte Größe des Arbeitsspeichers an.



Create: Virtual Machine

General OS System Disks CPU **Memory** Network Confirm

Memory (MiB): 4096

Abb. 71: VM Arbeitsspeicher

Klicke dann auf Next.

Gib danach die Bridge `vmb1` für die einzurichtende Netzwerkkarte an. Dies muss die Bridge für das interne Netz (green) sein.

Klicke dann auf Next.

Zum Abschluss siehst Du nochmals alle getroffenen Einstellungen. Überprüfe diese. Solltest Du Änderungen vornehmen wollen, kannst Du auf die entsprechende Reiterkarte klicken, Änderungen durchführen und wieder zur Reiterkarte **Confirm** wechseln.

Achte darauf, dass die Option `Start after created` unbedingt deaktiviert ist.

Klicke dann auf Finish.

Nachdem die VM angelegt wurde, siehst Du diese links im Verzeichnisbaum Deines Proxmox-Host, in dem alle VMs dargestellt werden.

Create: Virtual Machine

General OS System Disks CPU Memory **Network** Confirm

☐ No network device

Bridge: Model:

VLAN Tag: MAC address:

Firewall: ☒

Abb. 72: VM Netzwerkkarte

Create: Virtual Machine

General OS System Disks CPU Memory Network **Confirm**

Key ↑	Value
cores	2
ide2	local:iso/ubuntu- -live-server-amd64.iso.media=cdrom
memory	4096
name	lmn-server
net0	virtio,bridge=vmbr0,firewall=1
nodename	lmn-proxmox-testserver
numa	0
ostype	l26
scsi0	Dataset:25
scsi1	Dataset:100
scsihw	virtio-scsi-pci
sockets	2
vmid	101

☐ Start after created

Advanced ☐ **Back** **Finish**

Abb. 73: VM erstellen

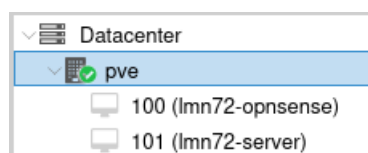


Abb. 74: VMs

Welches sich auch in der schematischen Übersicht zeigt:

Abb. 75: Stand nach der Erzeugung der Virtuellen Maschine Ubuntu

Abschließende Konfiguration der virtuellen Maschinen

Die nächsten beiden Einstellungen musst Du sowohl für die **Firewall als auch für den Server** vornehmen. Wir beschreiben es hier jetzt exemplarisch für die Firewall.

Boot-Optionen

Um bei der from Scratch Installation von CD zu starten, wählst Du die jeweilige VM (z.B. 100 (lmn7-opnsense) aus, klickst auf **Options** und klickst oben auf den Menüeintrag **Edit**.

<div><div>Summary</div><div>> Console</div><div>Hardware</div><div>Cloud-Init</div><div>Options</div><div>Task History</div><div>Monitor</div><div>Backup</div><div>Replication</div><div>Snapshots</div><div>Firewall</div><div>Permissions</div></div>	<div><div>Edit</div><div>Revert</div></div> <table><tr><td>Name</td><td>lmn71-opnsense</td></tr><tr><td>Start at boot</td><td>No</td></tr><tr><td>Start/Shutdown order</td><td>order=any</td></tr><tr><td>OS Type</td><td>Linux 5.x - 2.6 Kernel</td></tr><tr><td>Boot Order</td><td>scsi0, ide2, net0</td></tr><tr><td>Use tablet for pointer</td><td>Yes</td></tr><tr><td>Hotplug</td><td>Disk, Network, USB</td></tr><tr><td>ACPI support</td><td>Yes</td></tr><tr><td>KVM hardware virtualization</td><td>Yes</td></tr><tr><td>Freeze CPU at startup</td><td>No</td></tr><tr><td>Use local time for RTC</td><td>Default (Enabled for Windows)</td></tr><tr><td>RTC start date</td><td>now</td></tr><tr><td>SMBIOS settings (type1)</td><td>uuid=d73d9448-1f16-4174-a71a-0166043a1d46</td></tr><tr><td>QEMU Guest Agent</td><td>Default (Disabled)</td></tr><tr><td>Protection</td><td>No</td></tr><tr><td>Spice Enhancements</td><td>none</td></tr><tr><td>VM State storage</td><td>Automatic</td></tr></table>	Name	lmn71-opnsense	Start at boot	No	Start/Shutdown order	order=any	OS Type	Linux 5.x - 2.6 Kernel	Boot Order	scsi0, ide2, net0	Use tablet for pointer	Yes	Hotplug	Disk, Network, USB	ACPI support	Yes	KVM hardware virtualization	Yes	Freeze CPU at startup	No	Use local time for RTC	Default (Enabled for Windows)	RTC start date	now	SMBIOS settings (type1)	uuid=d73d9448-1f16-4174-a71a-0166043a1d46	QEMU Guest Agent	Default (Disabled)	Protection	No	Spice Enhancements	none	VM State storage	Automatic
Name	lmn71-opnsense																																		
Start at boot	No																																		
Start/Shutdown order	order=any																																		
OS Type	Linux 5.x - 2.6 Kernel																																		
Boot Order	scsi0, ide2, net0																																		
Use tablet for pointer	Yes																																		
Hotplug	Disk, Network, USB																																		
ACPI support	Yes																																		
KVM hardware virtualization	Yes																																		
Freeze CPU at startup	No																																		
Use local time for RTC	Default (Enabled for Windows)																																		
RTC start date	now																																		
SMBIOS settings (type1)	uuid=d73d9448-1f16-4174-a71a-0166043a1d46																																		
QEMU Guest Agent	Default (Disabled)																																		
Protection	No																																		
Spice Enhancements	none																																		
VM State storage	Automatic																																		

Abb. 76: Bootreihenfolge festlegen

Markiere mit der Maus den Eintrag ide2 (CD) und ziehe diesen an Position 1.

Vorher:

Nachher:

Edit: Boot Order ⓧ

#	Enabled	Device	Description
≡ 1	<input checked="" type="checkbox"/>	scsi0	vg-hdd-500:vm-100-disk-0,size=10G
≡ 2	<input checked="" type="checkbox"/>	ide2	local:iso/OPNsense- -OpenSSL-dvd-amd64.iso,me...
≡ 3	<input checked="" type="checkbox"/>	net0	virtio=16:5B:BA:30:41:C6,bridge=vibr0,firewall=1
≡ 4	<input type="checkbox"/>	net1	virtio=72:BD:56:E8:1D:04,bridge=vibr1,firewall=1

Drag and drop to reorder

ⓘ Help OK Reset

Abb. 77: vorher

Edit: Boot Order ⓧ

#	Enabled	Device	Description
≡ 1	<input checked="" type="checkbox"/>	ide2	local:iso/OPNsense- -OpenSSL-dvd-amd64.iso,me...
≡ 2	<input checked="" type="checkbox"/>	scsi0	vg-hdd-500:vm-100-disk-0,size=10G
≡ 3	<input checked="" type="checkbox"/>	net0	virtio=16:5B:BA:30:41:C6,bridge=vibr0,firewall=1
≡ 4	<input type="checkbox"/>	net1	virtio=72:BD:56:E8:1D:04,bridge=vibr1,firewall=1

Drag and drop to reorder

ⓘ Help OK Reset

Abb. 78: nachher

Hinzufügen einer seriellen Schnittstelle

Damit Dir *copy-and-paste* in der Oberfläche von Proxmox bei der Auswahl unter `>_ Console` zur Verfügung steht, musst Du die Nutzung von *xterm.js* ermöglichen. Als vorbereitende Maßnahme musst Du eine serielle Schnittstelle für die jeweilige VM aktivieren.

Wähle zuerst die gewünschte VM aus (z.B. *100 (lmn-opnsense)*), wähle danach den Eintrag *Hardware* für die VM aus und klicke dann oben rechts auf das Icon `>_ Console`.

Nachstehende Abb. zeigt den Zustand vor der Aktivierung.

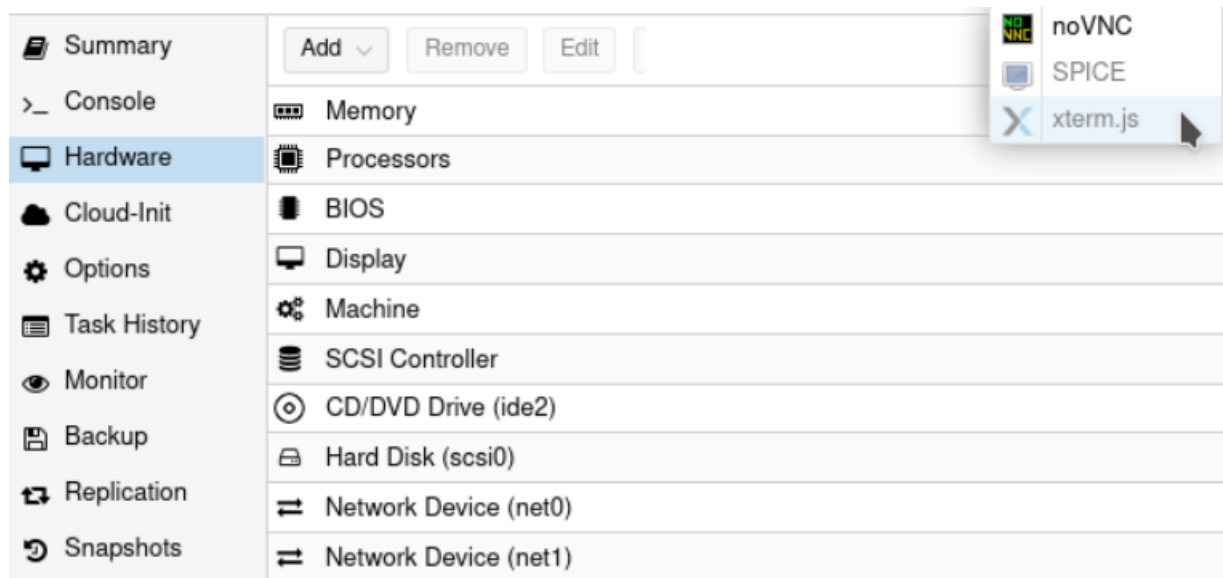


Abb. 79: Zustand vor der Aktivierung

Wähle die gewünschte VM *lmn-opnsense* aus, klicke dann `→ Add → Hardware → Serial Port`.

Lege einen Seriellen Port mit der Bezeichnung `0` an. Klicke danach auf `Add`.

Danach siehst Du den seriellen Port in der Hardware-Übersicht der VM. Klickst Du oben rechts auf `>_ Console`. Der der gezeigte Menüpunkt *xterm.js* sollte nun nicht mehr ausgegraut sein.

Kontrolliere nochmals alle Einstellungen der neu angelegten VM.

Die beiden letzten Einstellungen musst Du **nochmals für den linuxmuster.net Server (2. VM)** einrichten.

Hinweis: Für die weitere Nutzung von *xterm.js* ist allerdings noch eine Anpassung bei der laufenden OPNsense® bzw. dem Server nötig. Die nimmst Du zu einem geeigneten späteren Zeitpunkt vor, bis dahin musst Du noch die Konsole *noVNC* nutzen.

Die virtuellen Maschinen sind jetzt für die weitere Installation vorbereitet. Du kannst gemäß der Anleitung: *Erster Start der Firewall* mit der Installation fortfahren.

Hinweis: Jetzt wäre auch ein guter Zeitpunkt für ein Snapshoting und/oder dem Klonen der bisher erstellten VMs.

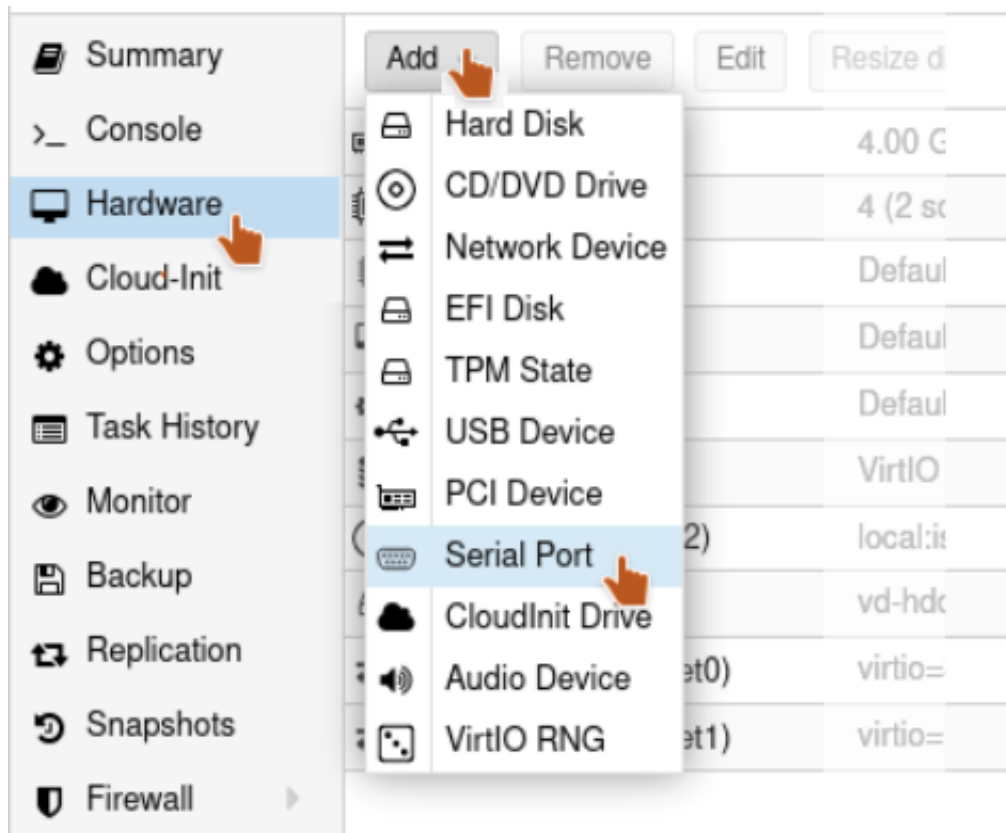


Abb. 80: Serial Port hinzufügen

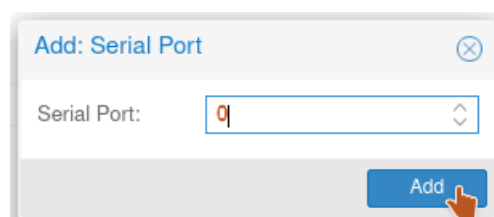


Abb. 81: Serielle Schnittstelle 0 hinzufügen

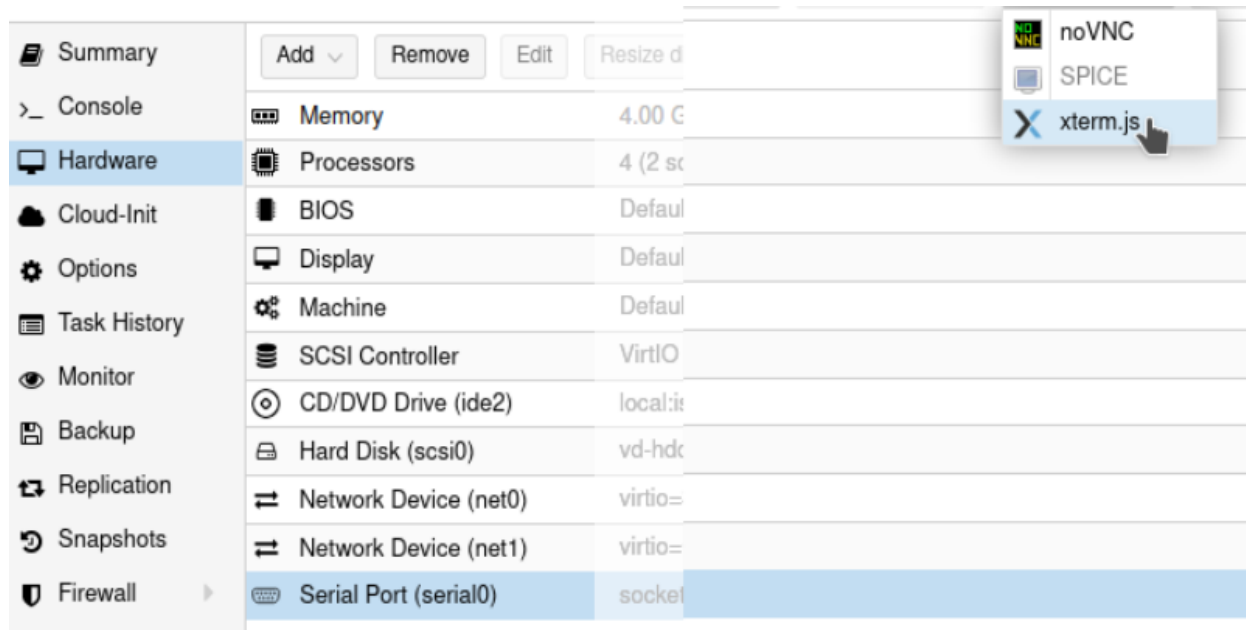


Abb. 82: Zustand nach der Aktivierung

4.6 Install-from-Scratch

Autor des Abschnitts: @cweikl @MachtDochNiX

In diesem Dokument findest Du eine „Schritt-für-Schritt“ Anleitung zur Installation der linuxmuster.net Musterlösung von Grund auf (install-from-scratch).

Lies zuerst die Abschnitte *Was ist neu in 7.2?* und *Vorüberlegungen*, bevor Du dieses Kapitel durcharbeitest.

Nach der Installation gemäß dieser Anleitung erhältst Du eine einsatzbereite Umgebung bestehend aus

- einer Firewall (OPNsense® für linuxmuster.net),
- und einem Server (linuxmuster.net).

Im Laufe der Installation benötigst Du einen Admin-PC. Das kann ein einfacher Laptop mit einem beliebigen Betriebssystem sein.

Vorgehensweise

- Zunächst installierst Du die Firewall OPNsense®.
- Danach installierst Du den Ubuntu-Server.
- Schließlich richtest Du linuxmuster.net ein.

4.6.1 Anlegen und Installieren der Firewall

Autor des Abschnitts: @cweigl @MachtDochNiX, @rettich,

Installation der OPNsense®

Bemerkung: Bist Du zuvor der Anleitung *Proxmox vorbereiten* gefolgt, dann kannst Du fortfahren mit: *Erster Start der Firewall*

Abb. 83: Stand nach der vorhergehenden Beschreibung

Falls Du Dich für eine andere Installationsart entschieden hast, musst Du den dargestellten Aufbau herstellen.

Lade Dir die ISO-Datei der OPNsense® von der Seite <https://opnsense.org/download/> herunter.

Hinweis: Die zuletzt freigegeben OPNsense Version für das Setup von linuxmuster.net v7.2 ist die Version 24.1 [Stand: Februar 24].

wget <https://mirror.informatik.hs-fulda.de/opnsense/releases/24.1/OPNsense-24.1-dvd-amd64.iso.bz2>

Nutze als Architektur amd64 und als image type dvd und einen Mirror, der in Deiner Nähe ist. Du erhältst dann ein mit bz2 komprimiertes ISO-Image. Entpacke die heruntergeladene Datei. Siehe hierzu auch *Proxmox vorbereiten* - dort Kapitel *Vorbereiten des ISO-Speichers* -> *OPNsense* |reg|.

Unter Linux ist folgender Befehl anzugeben:

```
bunzip2 OPNsense-24.1-dvd-amd64.iso.bz2
```

In der Virtualisierungsumgebung lädst Du die ISO-Datei auf den ISO-Speicher.

Hinweis: Willst Du in einer VM installieren, so musst Du für die neue VM folgende Mindesteinstellungen für die Hardware angeben:

- template - other install media, installation from ISO library,
 - Boot-Mode - UEFI (Achtung: xcp-ng: Boot/MBR),
 - 1 vCPU
 - 2 GiB RAM
 - storage 10 GiB
 - 2 NIC mit Zuordnung zu vSwitch red, green.
-

Für den produktiven Betrieb müssen diese Hardware-Einstellungen **deutlich** angehoben werden (z.B.: 4 vCPU, 8 GiB RAM, 50 GiB SSD, 3 NIC).

Erster Start der Firewall

Starte dann OPNsense® auf dem Rechner oder in der neu angelegten VM von Deinem Installationsmedium. Je nach Virtualisierungsumgebung hast Du ggf. die ISO-Datei bereits auf dem ISO-Datenspeicher des Hypervisors abgelegt. Boote dann die VM via ISO-Datei.

Achtung: Solltest Du unserer Anleitung gefolgt sein und PROXMOX nutzen, dann muss Du für die Installation die Konsole noVNC nutzen.

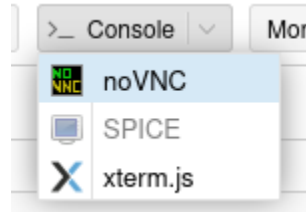


Abb. 84: Starte die OPNsense-VM

Am Ende des Boot-Vorgangs der OPNsense® gelangst Du zu folgendem Bildschirm:

```

LAN (vtnet0)    -> v4: 192.168.1.1/24
WAN (vtnet1)   -> v4/DHCP4: 192.168.1.203/24

HTTPS: SHA256 48 40 E7 1B 1C A2 BC BC 91 BF CE DD B4 53 7A 25
              4E 31 2E 55 01 1F 18 12 AE 93 FC DE 5B 8B 4F E6
SSH:   SHA256 4wFxR33ypzmBqRTW4LThUIKLo6lWvsSCJ1TFeYnApNA (ECDSA)
SSH:   SHA256 DsQRq575nD9BUMroCtPWm19HZfDqng4YzxQ8//sUUpI (ED25519)
SSH:   SHA256 Y4FgYk5kHQZzf/jF6HKec+OurOUNPdPi5BtSUlU3wmo (RSA)

Welcome! OPNsense is running in live mode from install media. Please
login as 'root' to continue in live mode, or as 'installer' to start the
installation. Use the default or previously-imported root password for
both accounts. Remote login via SSH is also enabled.

FreeBSD/amd64 (OPNsense.localdomain) (ttyv0)
login: 
```

Abb. 85: Bildschirm nach dem ersten Boot-Vorgang

Melde Dich als Benutzer `installer` mit dem Passwort `opnsense` an. Du gelangst direkt zum Installer und kannst das Layout der Tastatur festlegen.

Standardmäßig ist ein amerikanisches Tastaturlayout voreingestellt. Gehe mit den Pfeiltasten auf den Eintrag () German (no accent keys). Wählen diesen mit `<Select>` aus.

Teste danach das Tastaturlayout:

Bei der deutschen Tastatur werden ggf. die Umlaute im Test noch nicht korrekt wiedergegeben.

Wähle die eingestellte deutsche Tastatur aus:

Wähle `<Select>`.

Installiere nun OPNsense® via `Install (UFS)`.

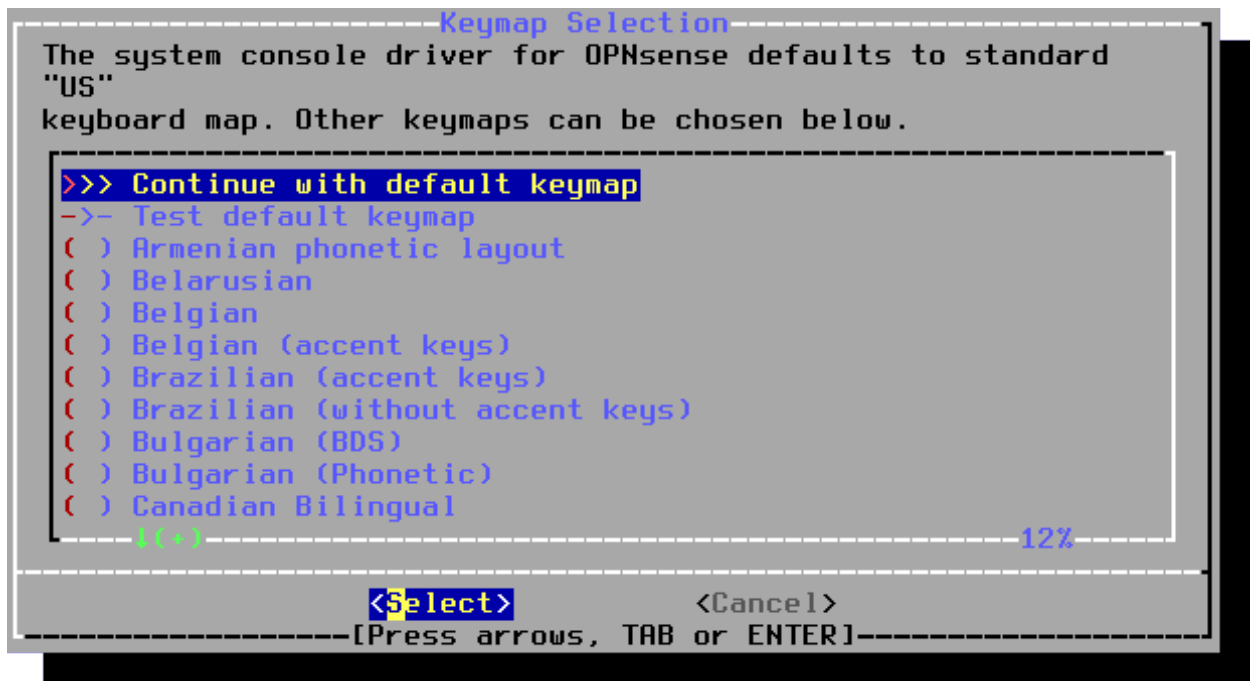


Abb. 86: INStaller: Tastaturlayout festlegen

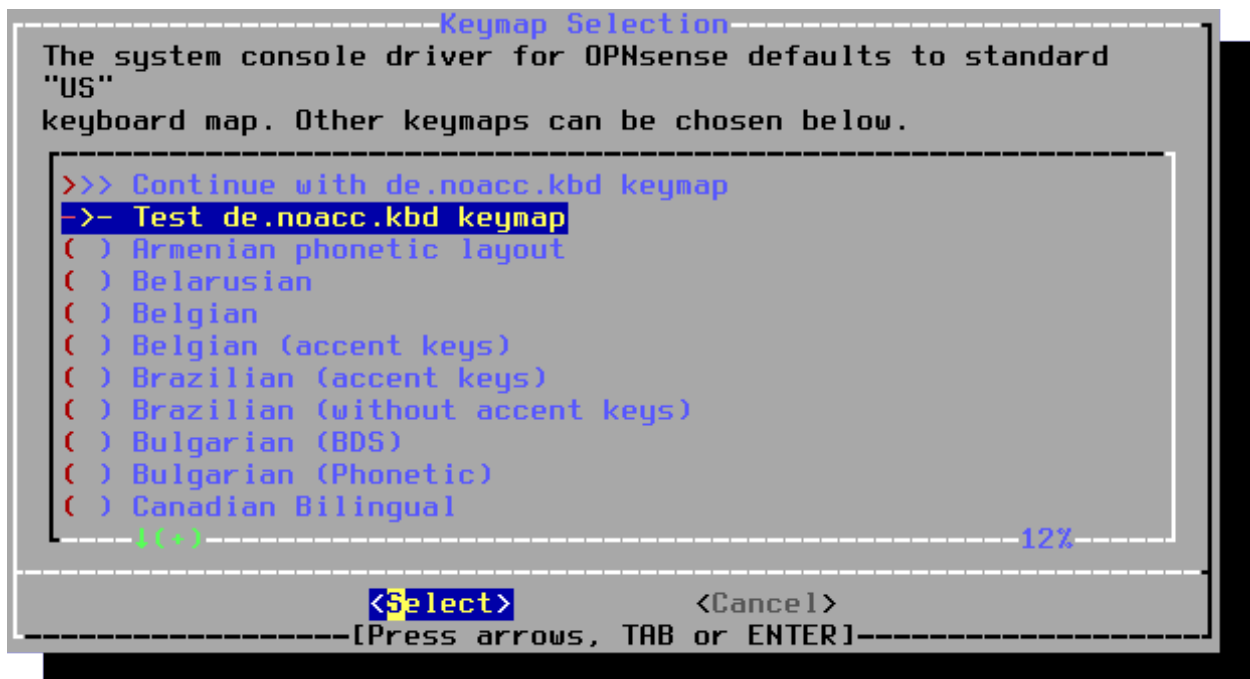


Abb. 87: Teste das Tastaturlayout

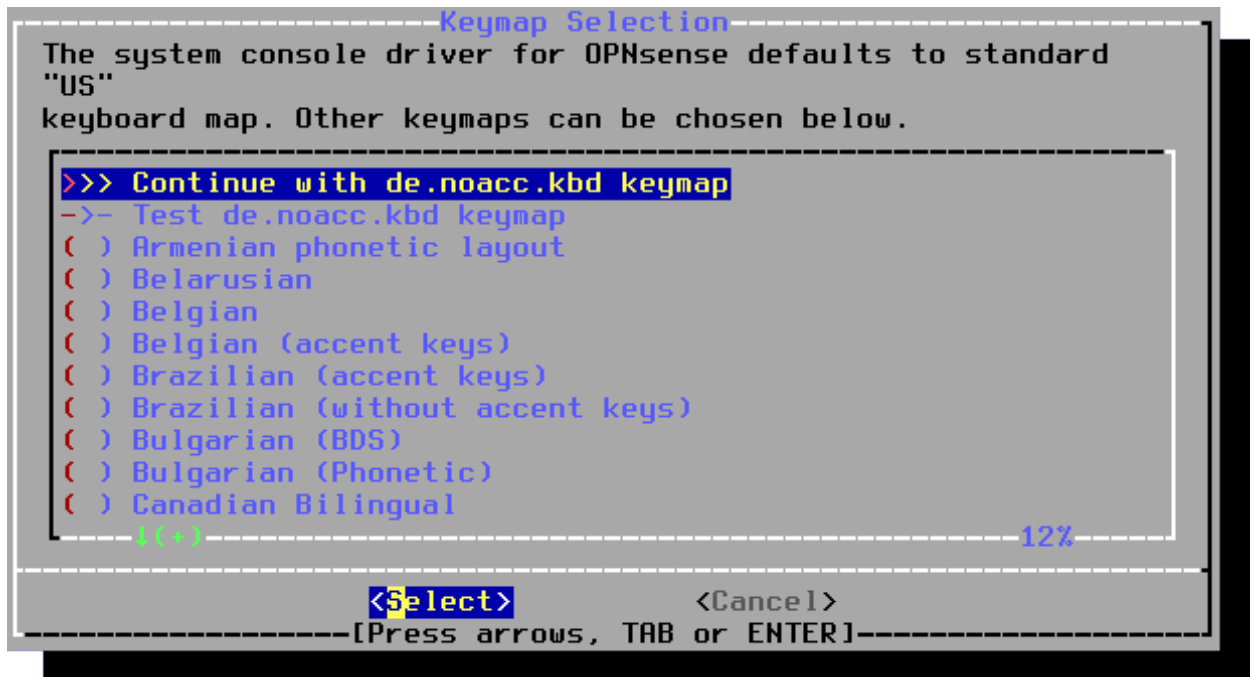


Abb. 88: Bestätige der Stataturlayout

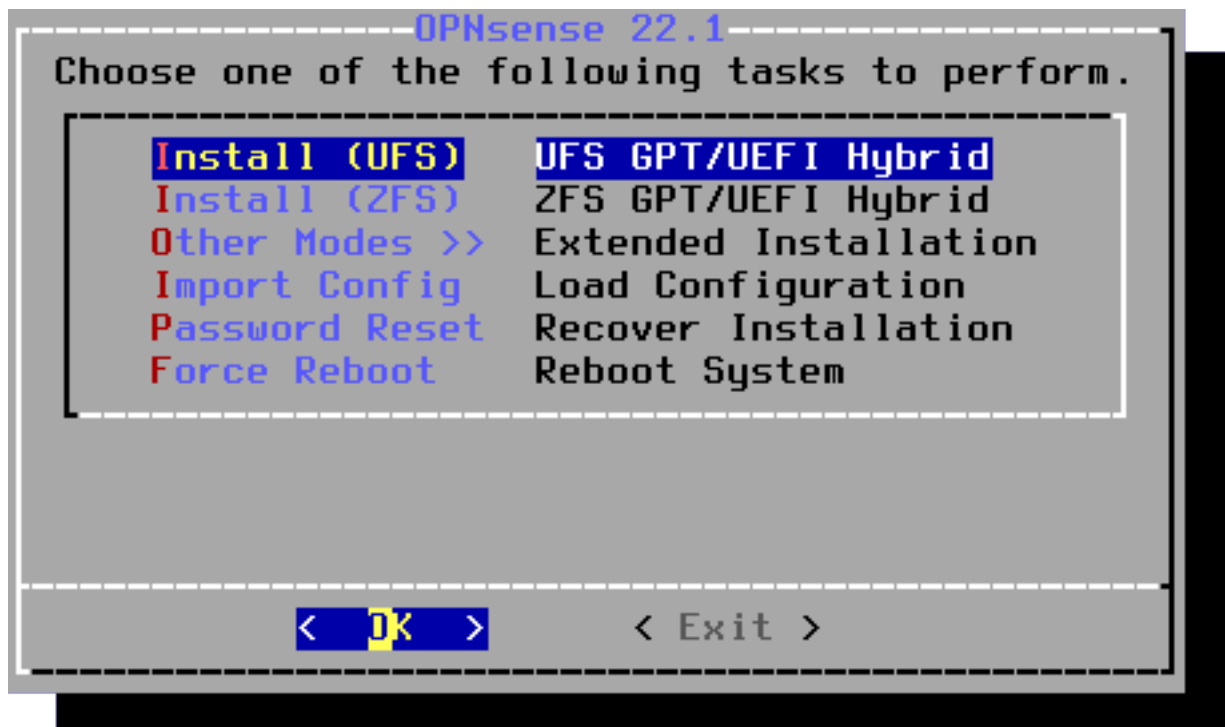


Abb. 89: Install (UFS)

Bestätige die Festplatte und wähle Install (UFS) UFS GPT/UEFI Hybrid.

Jetzt wird OPNsense® auf der Festplatte installiert. Zuvor musst Du diese noch auswählen.



Abb. 90: da0 QEMU HARDDISK

Mit OK übernimmst Du Deine Auswahl.

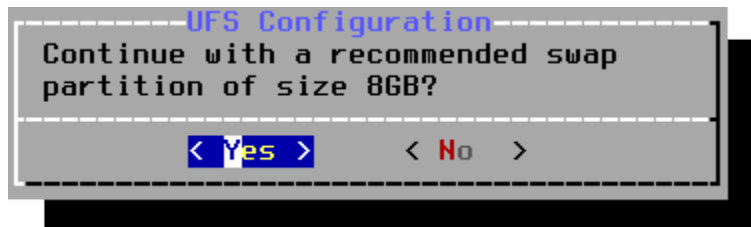


Abb. 91: SWAP Partition wählen

Sollte Dir dieses Fenster angezeigt werden, dann akzeptiere die Frage nach der empfohlenen Auslagerungsdatei.

Danach erfolgt die Rückfrage, ob die Festplatte wirklich überschrieben werden soll.

Bestätige diesen Vorgang, um die Installation zu starten.

Warte jetzt, bis die Installation abgeschlossen ist.

Zum Abschluss der Konfiguration musst Du das Kennwort für den Benutzer root neu setzen.

Achtung: An dieser Stelle muss als root-Passwort **Muster!** eingegeben werden, da später der lmn-Server beim Einrichten der Firewall davon ausgeht, dass das root-Passwort **Muster!** ist! Sollte dieses anders lauten, wird die komplette weitere Installation scheitern!

Gib das neue Passwort (**Muster!**) für root ein.

Gib dieses Kennwort erneut ein.

Setze es mit OK

Wähle danach die Option `Exit and reboot` aus.

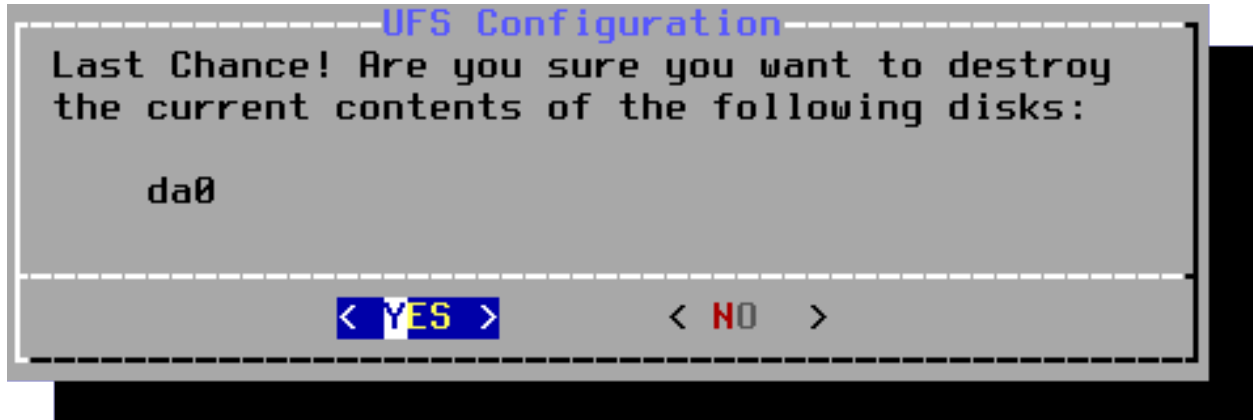


Abb. 92: Bestätige die Installation auf da0

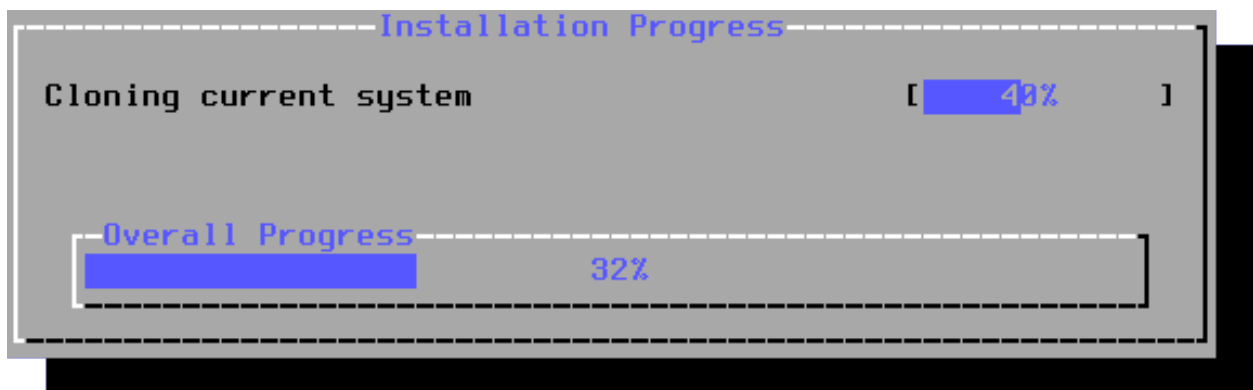


Abb. 93: Installationsfortschritt

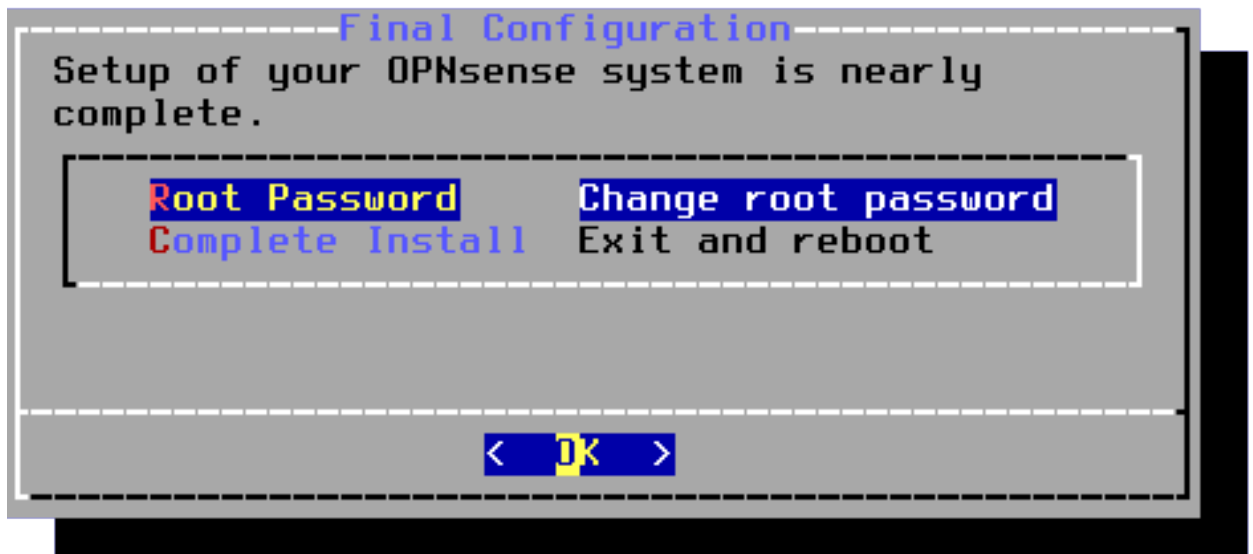


Abb. 94: Eingabe des Root Kennwortes



Abb. 95: Eingabe des neuen Root Kennwortes



Abb. 96: Bestätigung des neuen Root Kennwortes

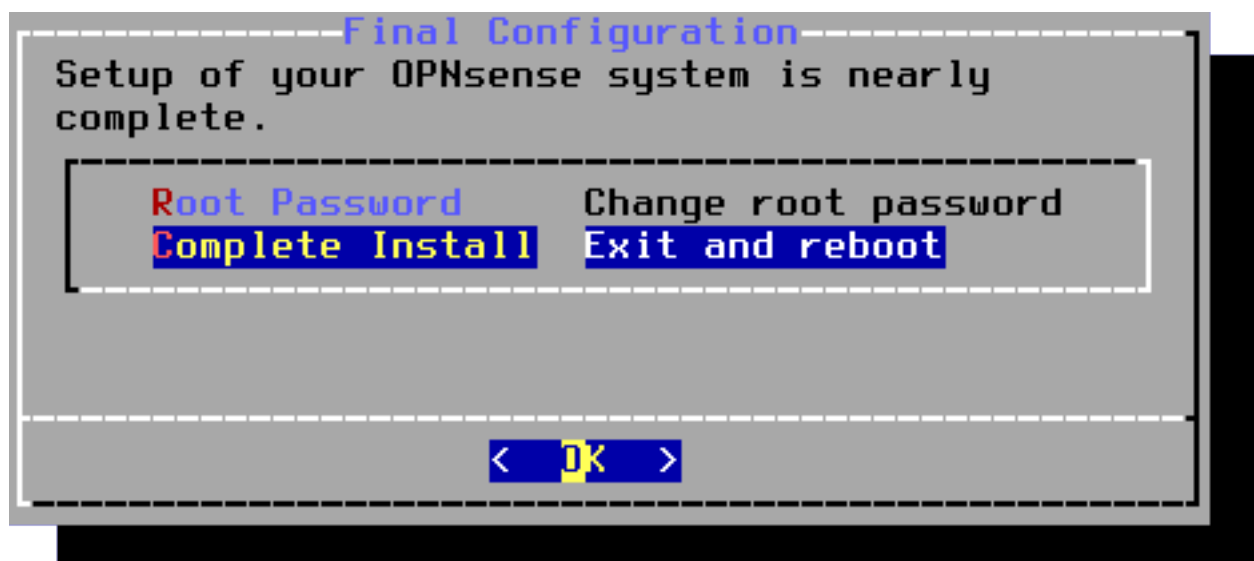


Abb. 97: Schließe die Installation ab

Hinweis: Solltest Du nicht zum Entfernen, das Installationsmedium aufgefordert werden, fahre Deine neue Firewall herunter (schalte sie aus).

Ändere die Boot-Reihenfolge zurück (Start via Festplatte).

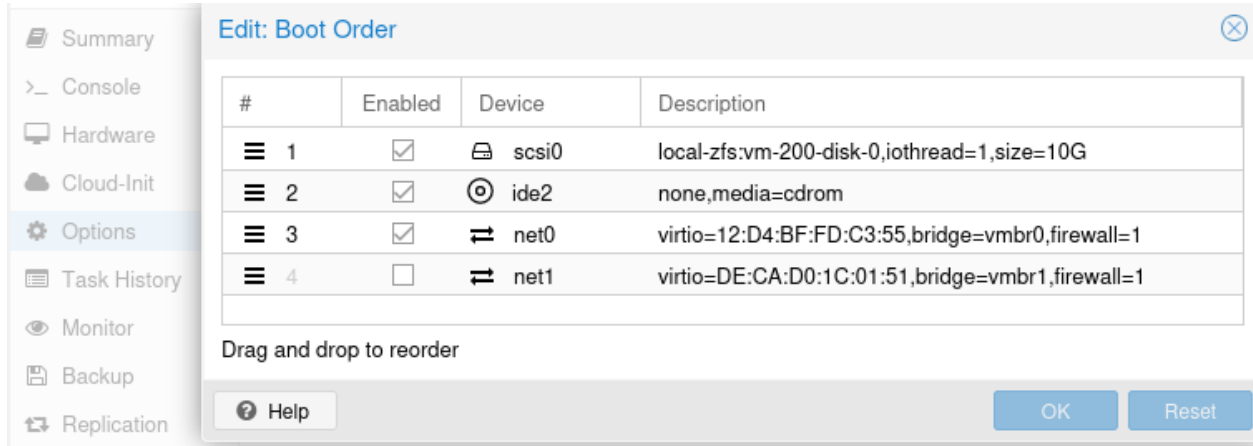


Abb. 98: Ändere die Boot-Reihenfolge
Werfe die ISO-Datei aus dem CD-Laufwerk aus.

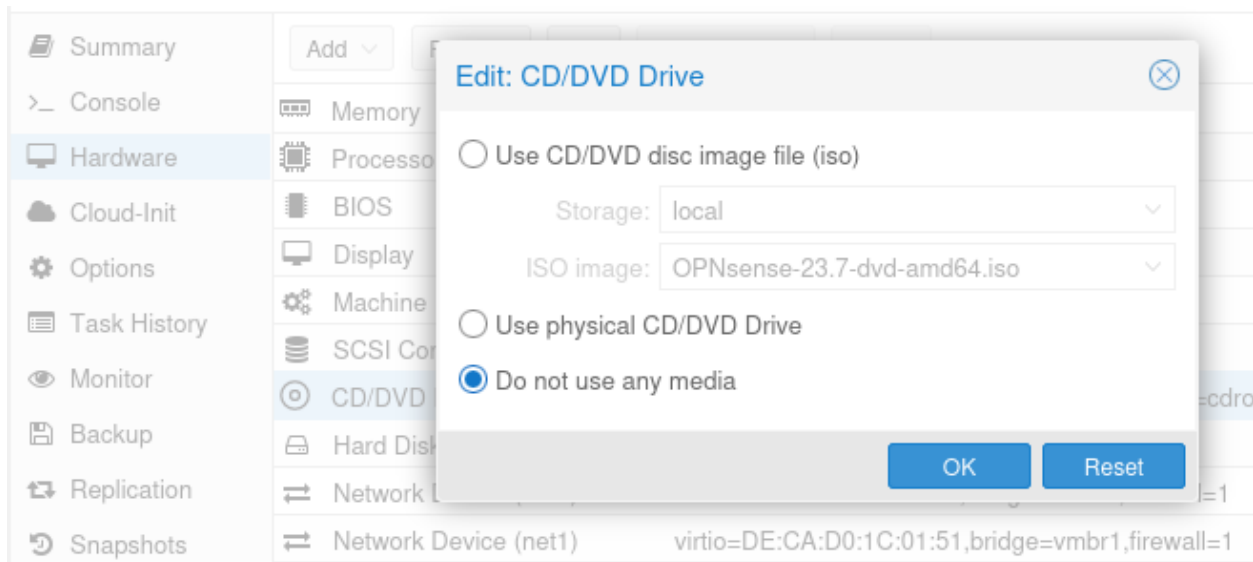


Abb. 99: Werfe die ISO-Datei aus dem Laufwerk aus.
Starte die VM neu, nachdem Du das Installationsmedium ausgeworfen hast und fahre mit der Installation fort.

Der Boot-Vorgang kann dann eine Weile dauern. Vor allem, wenn der Router kein DHCP anbieten sollte.

Wenn alles geklappt hat, ist Folgendes zu sehen:

Hinweis: Die dargestellten IPs und Netze können bei Deiner OPNsense® andere sein.

```

LAN (vtnet0)    -> v4: 192.168.1.1/24
WAN (vtnet1)    -> v4/DHCP4: 192.168.1.203/24

HTTPS: SHA256 48 40 E7 1B 1C A2 BC BC 91 BF CE DD B4 53 7A 25
              4E 31 2E 55 01 1F 18 12 AE 93 FC DE 5B 8B 4F E6

FreeBSD/amd64 (OPNsense.localdomain) (ttyv0)
login: █

```

Abb. 100: Login nach erfolgter Installation und Reboot

Basis-Konfiguration der OPNsense®

Melde Dich als root mit dem Passwort Muster! an der OPNsense® an.

Tastaturbelegung prüfen

```

0) Logout                      7) Ping host
1) Assign interfaces           8) Shell
2) Set interface IP address    9) pfTop
3) Reset the root password     10) Firewall log
4) Reset to factory defaults   11) Reload all services
5) Power off system            12) Update from console
6) Reboot system               13) Restore a backup

Enter an option: 8

```

Abb. 101: Tastaturbelegung überprüfen

Zuerst überprüfe, ob die Tastaturbelegung richtig ist. Dazu wähle den Punkt 8) Shell aus. Auf der Konsole kannst Du dann die Umlaute und Sonderzeichen der deutschen Tastaturbelegung testen. Sollte sie korrekt sein, verlässt Du mit exit die Konsole und bist wieder im Auswahl-Bildschirm.

Fahre mit *Überprüfung der Zuordnung der Netzwerkkarten* fort, ansonsten ...

Hinweis: Solltest Du feststellen, dass nach dem Neustart in der Konsole der OPNsense® die Tastaturbelegung immer noch falsch ist, stelle diese dauerhaft wie nachstehend beschrieben um:

```

cd /usr/share/syscons/keymaps    # Für den Buchstaben "z" musst Du die Taste "y" drücken.
↪;-)

ls german.iso.kbd                # listet das deutsche Tastaturlayout auf, sofern
↪vorhanden

kbdcontrol -l german.iso.kbd     # (-l = Language; "-" zu finden unter "?" ;-) stelle
↪temporär auf das neue Layout um
                                # - teste, ob es dem gewünschten Layout entspricht

echo "keymap='de'">>/etc/rc.conf # die Wahl des Tastaturlayouts dauerhaft hinzufügen

```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
cat /etc/rc.conf          # kontrolliere, ob der Eintrag vorhanden ist
exit                      # Konsole verlassen
```

Überprüfung der Zuordnung der Netzwerkkarten

```
LAN (vtnet0)    -> v4: 192.168.1.1/24
WAN (vtnet1)    -> v4/DHCP4: 192.168.1.203/24

HTTPS: SHA256 48 40 E7 1B 1C A2 BC BC 91 BF CE DD B4 53 7A 25
              4E 31 2E 55 01 1F 18 12 AE 93 FC DE 5B 8B 4F E6

FreeBSD/amd64 (OPNsense.localdomain) (ttyv0)
login: █
```

Abb. 102: Zuordnung der NICs prüfen

Die erste Netzwerkkarte (LAN) ist derzeit als LAN mit dem pädagogischen Netz verbunden. Die Netzwerkkarte `vtnet0` ist nach der bisherigen Installation allerdings mit dem roten Netz verbunden. Zudem vergibt die Installationsroutine der OPNsense® immer die IP 192.168.1.1/24 der LAN-Schnittstelle. Dies ist jetzt noch zu ändern.

Die zweite Netzwerkkarte (WAN) ist derzeit mit `vtnet1` verbunden. Dies müssen wir noch ändern.

Anpassung der Zuordnung der Netzwerkkarten

Rufe dazu den Menüeintrag 1) Assign interfaces auf. Die Nachfragen bezüglich LAGGs und VLANs verneinst du.

```
Enter an option: 1

Do you want to configure LAGGs now? [y/N]: N
Do you want to configure VLANs now? [y/N]: N
```

Abb. 103: Keine LAGGs und VLANs

Dann sind die MAC-Adressen der virtuellen Maschine, hier `vtnet0` und `vtnet1`

und denen der Netzwerkbrücken `vmbr0` und `vmbr1` zu überprüfen (Proxmox-Host → VM → Hardware → Network Device (net.)):

Unter Proxmox-Host → Network kannst Du Dir jetzt mittels des Kommentarfeldes wieder die Zuordnung der Bridges ins Gedächtnis rufen.

Bridge des Virtualisierers			<->	Virtuelle Maschine		
Kommentar	Brücke	MAC		MAC	Interfaces	Typ
red	vmbr0	0E:76:8B:51:85:15	<->	0e:76:8b:51:85:15	vtnet0	WAN
green	vmbr1	DA:97:1B:E1:35:9C	<->	da:97:1b:e1:35:9c	vtnet1	LAN

```
Valid interfaces are:

vtnet0      0e:76:8b:51:85:15 VirtIO Networking Adapter
vtnet1      da:97:1b:e1:35:9c VirtIO Networking Adapter

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: █
```

Abb. 104: Gültige NICs

Summary	Add ▾	Remove	Edit	Resize disk	Move disk	Revert
> Console	Memory	4.00 GiB				
Hardware	Processors	4 (2 sockets, 2 cores)				
Cloud-Init	BIOS	Default (SeaBIOS)				
Options	Display	Default				
Task History	Machine	Default (i440fx)				
Monitor	SCSI Controller	VirtIO SCSI				
Backup	CD/DVD Drive (ide2)	local:iso/OPNsense-22.1.2-OpenSSL-dvd-amd64.iso				
Replication	Hard Disk (scsi0)	vd-hdd-560:vm-1000-disk-0,size=10G				
Snapshots	Network Device (net0)	virtio=0E:76:8B:51:85:15,bridge=vbr0,firewall=1				
	Network Device (net1)	virtio=DA:97:1B:E1:35:9C,bridge=vbr1,firewall=1				

Abb. 105: Proxmox NICs der VM

Aus diesem Wissen und dem Vergleich erkennst Du ...

```
Enter the WAN interface name or 'a' for auto-detection: vtnet0
```

Abb. 106: WAN-Verbindung an vtnet0

..., dass das WAN dem Interface vtnet0 zuzuordnen ist.

```
Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): vtnet1
```

Abb. 107: LAN-Verbindung an vtnet1

..., dass das LAN zum Interface vtnet1 zuzuordnen ist.

```
Enter the Optional interface 1 name or 'a' for auto-detection
(or nothing if finished):
```

Hast Du kein weiteres Interface, dann gebe Enter ein.

Diese Zuordnung ist nun richtig, also weiter mit y ...

..., welches dann die Konfiguration startet. Nach Abschluss kommst Du wieder zum Konsolen-Menü.

Die Zuordnung des WAN-Interfaces ist hier zu erkennen und nun so wie beabsichtigt. Das erkennst Du daran, dass dessen IP-Adresse dem Adress-Pool des Routers entnommen ist (, sofern der DSL-Router via DHCP eine Adresse verteilt).

Hinweis: Starte die OPNsense® neu, nachdem Du die Netzwerkkarten neu zugeordnet hast.

WAN Zugang testen

Hast Du die OPNsense® neu gestartet und auf der WAN-Schnittstelle eine IP-Adresse erhalten, führe zwei erste Tests durch. Wähle 8) Shell auf der Kommandozeile und gib dort folgende Befehle ein:

Hinweis: Sollte einer der Tests scheitern, dann verlasse die Konsole mittels `exit` und nutze den Auswahlpunkt 11) `reload all Services`.

```
ping -c 3 8.8.8.8
```

Die Ausgabe sollte wie folgt aussehen:

```
ping -c 3 linuxmuster.net
```

Gib in der Konsole `exit` ein, um wieder zum Dashboard zurückzukommen.

Hinweis: Sollte einer der Test auch nach 11) `Reload all services` nicht erfolgreich verlaufen, dann stimmt etwas mit der Netzwerkkartenzuordnung nicht. Überprüfe Deine vorherige Netzwerk-Konfiguration auf Fehler.

```
The interfaces will be assigned as follows:
```

```
WAN -> vtnet0
```

```
LAN -> vtnet1
```

```
Do you want to proceed? [y/N]: y
```

Abb. 108: Netzwerkkarten zuordnen

```
Writing configuration...done.
Configuring loopback interface...done.
Creating wireless clone interfaces...done.
Configuring LAN interface...done.
Configuring WAN interface...done.
Creating IPsec VTI instances...done.
Setting up routes...done.
Configuring firewall.....done.
Starting DHCPv4 service...done.
Starting DHCPv6 service...done.
Starting router advertisement service...done.

```

Abb. 109: Konfiguration gestartet

```
LAN (vtnet1) -> v4: 192.168.1.1/24
WAN (vtnet0) -> v4/DHCP4: 192.168.21.212/24

HTTPS: SHA256 6A 73 35 96 E0 A3 D6 BE 2D B0 AC A9 F5 00 1D 09
            1D E2 46 A1 EC 7A 33 8F 8D F3 01 32 52 01 3A 53

0) Logout                                7) Ping host
1) Assign interfaces                     8) Shell
2) Set interface IP address              9) pfTop
3) Reset the root password               10) Firewall log
4) Reset to factory defaults             11) Reload all services
5) Power off system                      12) Update from console
6) Reboot system                         13) Restore a backup

Enter an option: 
```

Abb. 110: Prüfe die Zuordnung der Netzwerkkarten

```
root@OPNsense:~ # ping -c 3 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=118 time=22.587 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=22.334 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=20.747 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 20.747/21.889/22.587/0.814 ms
root@OPNsense:~ #
```

Abb. 111: Ping Test IP

```
root@OPNsense:~ # ping -c 3 linuxmuster.net
PING linuxmuster.net (95.217.39.157): 56 data bytes
64 bytes from 95.217.39.157: icmp_seq=0 ttl=54 time=44.433 ms
64 bytes from 95.217.39.157: icmp_seq=1 ttl=54 time=44.093 ms
64 bytes from 95.217.39.157: icmp_seq=2 ttl=54 time=44.091 ms

--- linuxmuster.net ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 44.091/44.206/44.433/0.161 ms
root@OPNsense:~ # █
```

Abb. 112: Ping Test URL

```
LAN (vtnet1)    -> v4: 192.168.1.1/24
WAN (vtnet0)   -> v4/DHCP4: 192.168.21.212/24

HTTPS: SHA256 6A 73 35 96 E0 A3 D6 BE 2D B0 AC A9 F5 00 1D 09
              1D E2 46 A1 EC 7A 33 8F 8D F3 01 32 52 01 3A 53

0) Logout                      7) Ping host
1) Assign interfaces           8) Shell
2) Set interface IP address    9) pfTop
3) Reset the root password     10) Firewall log
4) Reset to factory defaults   11) Reload all services
5) Power off system            12) Update from console
6) Reboot system               13) Restore a backup

Enter an option: █
```

Abb. 113: Konsolen Dashboard

IP-Adressen zuweisen

Solltest Du in Deiner Netzwerkkonfiguration von unserem Muster abweichen, musst Du bei nachfolgenden Schritten anstelle der dargestellten IPs Deine hierfür festgelegten IPs eintragen.

```

0) Logout
1) Assign interfaces
2) Set interface IP address
3) Reset the root password
4) Reset to factory defaults
5) Power off system
6) Reboot system
7) Ping host
8) Shell
9) pfTop
10) Firewall log
11) Reload all services
12) Update from console
13) Restore a backup

Enter an option: 2

```

Abb. 114: Setze die Interface IPs

Wähle in der Konsole der OPNsense® den Eintrag 2) Set interface IP address aus.

```

Available interfaces:

1 - LAN (vtnet1 - static, track6)
2 - WAN (vtnet0 - dhcp, dhcp6)

Enter the number of the interface to configure: 1

```

Abb. 115: LAN auswählen

Wähle 1 - LAN (...) für die nächsten Schritte.

```

Configure IPv4 address LAN interface via DHCP? [y/N] N

```

Abb. 116: IP nicht via DHCP zuweisen lassen

Bestätige die Nachfrage mit N und ENTER. (Alternativ wäre auch nur ENTER möglich, da der großgeschriebene Buchstabe in der Auswahlmöglichkeit darauf hinweist, was die Standard-Einstellung ist.)

Gib die IPv4 Adresse 10.0.0.254 ein, unter der die OPNsense® im lokalen Netz zu erreichen sein wird.

Gib die Netzmaske in CIDR-Notation an. Dies bedeutet, dass Du für unseren Fall die Zahl der Bits angibst, die in der Subnetzmaske gesetzt werden. Dies ist die Zahl 16 und führt zu der Subnetzmaske (255.255.0.0 - dezimal).

Da keine Eingabe eines Upstream-Gateways nötig ist, einfach ENTER eingeben.

Achtung: Gib ein n ein.

Gib ein N ein.

Da keine IPv6-Adresse benötigt wird: ENTER

Diese und die nächsten drei Fragen ebenfalls jeweils N und ENTER bzw. nur ENTER beantworten.

Nach der letzten Eingabe startet die Übernahme in das System.

```
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.0.0.254
```

Abb. 117: IP eintragen

```
Subnet masks are entered as bit counts (like CIDR notation).
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 16
```

```
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```

Abb. 118: Bestätige mit ENTER

```
Configure IPv6 address LAN interface via WAN tracking? [Y/n] n
```

Abb. 119: Überspringe IPv6 via WAN tracking

```
Configure IPv6 address LAN interface via DHCP6? [y/N] N
```

Abb. 120: Kein IPv6 via DHCP

```
Enter the new LAN IPv6 address. Press <ENTER> for none:
>
```

Abb. 121: Keine manuelle festgelegte IPv6-Adresse

```
Do you want to enable the DHCP server on LAN? [y/N] N
```

Abb. 122: Kein DHCP-Server für das LAN aktivieren

```
Do you want to change the web GUI protocol from HTTPS to HTTP? [y/N] N
```

Abb. 123: Keine Änderung des HTTPS-Protokolls

```
Do you want to generate a new self-signed web GUI certificate? [y/N] N
```

Abb. 124: Kein neues Zertifikat erstellen

```
Restore web GUI access defaults? [y/N] N
```

Abb. 125: GUI-Einstellungen nicht zurücksetzen

```
Writing configuration...done.  
Generating /etc/hosts...done.  
Generating /etc/resolv.conf...done.  
Configuring LAN interface...done.  
Setting up routes...done.  
Starting Unbound DNS...done.  
Setting up gateway monitors...done.  
Configuring firewall.....done.  
Starting PFLOG...█
```

Abb. 126: Wende Konfigurationsschritte an

Nach erfolgreicher Übernahme erhältst Du den Hinweis, dass Du Dich mit der LAN IP auf die GUI der OPNsense® aufschalten könntest.

```
You can now access the web GUI by opening  
the following URL in your web browser:  
  
https://10.0.0.254
```

Abb. 127: GUI IP

Bevor Du das aber machst, erfolgt ein letzter Test, und zwar mit der Aktualisierung der OPNsense®.

Aktualisierung der OPNsense®

Aktualisiere die OPNsense® in der Konsole, indem Du den Punkt 12) `Update from console` aufrufst und die Rückfrage mit `y` bestätigst.

Hinweis: Sollte hierbei keine Verbindung zu den externen Update-Servern möglich sein, dann stimmt etwas mit der Netzwerkkartenzuordnung nicht.

Als Erstes probiere es mit dem Neustart aller Netzwerk-Dienste. Dazu wählst Du den Punkt 11) `Reload all services`. Danach wiederholst Du das Upgrade nochmals mit dem Punkt 12) `Update from console`.

Sollte die Aktualisierung immer noch nicht erfolgreich durchgeführt werden, dann überprüfe Deine vorherige Netzwerk-Konfiguration auf Fehler.

Sollte sich eine Eingabe-Aufforderung wie hier dargestellt vorher öffnen, muss du zum Fortführen des Updates ein `q` eingeben. Um dir alle Mitteilungen anzusehen, verwende die Auf- bzw. Ab-Tasten.

Das Update ist erfolgreich durchgeführt, wenn du wieder zu dieser Ansicht gelangst.

Klappt das Update, starte die OPNsense® neu.

```

Hello world,

It is time to move back to Suricata version 7 after identifying the relevant
default option changes in order to keep IPS/Netmap happy when running it.
Kea also received a number of tweaks and updates as well as our VPN service
integrations.

Last but not least this includes FreeBSD 13.2-p10 and the recent DNS denial
of service attack mitigation.

Here are the full patch notes:

o system: accept colon character in log queries
o system: add issuer and logo to OTP link
o system: fix gateway migration issue causing individual items to be skipped
o reporting: update traffic graph colors to be contrast and consistent (contribu
ted by brotherla)
o interfaces: fix strpos() deprecation null haystack
o interfaces: add missing ACL entries for ARP/NDP tables
o interfaces: fix VXLAN validation
o firewall: change default traffic normalization behavior and choose "in" as sta
ndard direction for manual rules
o firewall: make select width more consistent on alias diagnostics table selecti
on
:

```

Abb. 128: OPNsense: Hello World - New Features

```

*** OPNsense.localdomain: OPNsense 24.1.2_1 ***

LAN (vtnet1)    -> v4: 10.0.0.254/16
WAN (vtnet0)    -> v4/DHCP4: 192.168.178.229/24

HTTPS: SHA256 8B F2 57 18 11 5E 06 6F 06 ED 5E 86 0E EC F3 87
              D8 A6 CB 42 F1 99 1E 7E 8F 5E D2 06 98 9D 3B 53

FreeBSD/amd64 (OPNsense.localdomain) (ttyv0)
login:

```

Abb. 129: NIC Zuordnung nach Neustart

Konfiguration der OPNsense®

Für die nachfolgende Konfiguration der OPNsense® brauchst Du einen Rechner mit Webbrowser im LAN-Bereich der OPNsense®. Das kann ein Laptop mit einem beliebigen Betriebssystem sein. Wichtig ist nur, dass er mit internen Switch im grünen Netzwerk verbunden ist, das mit dem LAN-Adapter der OPNsense® verbunden ist und sich im gleichen Netzwerk wie die OPNsense® befindet. In unserer Beschreibung gehen wir davon aus, dass der Laptop/PC manuell die IP-Adresse 10.0.0.10 mit der Subnetmask 255.255.0.0 (16 Bit) erhält.

Nachdem der Browser gestartet ist, gibst Du folgende URL für den Zugriff auf die GUI der OPNsense® ein:

`https://10.0.0.254`

Du erhältst zunächst eine Zertifikatswarnung, da OPNsense® ja ganz frisch installiert ist und ein selbst erstelltes Zertifikat nutzt.

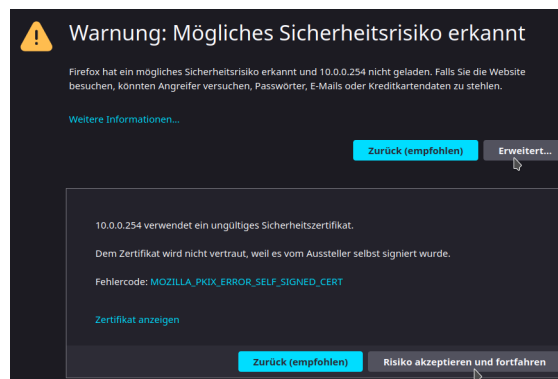


Abb. 130: Zertifikatswarnung

Klicke auf **Erweitert** und anschließend **Risiko akzeptieren und fortfahren**. Dies bringt Dich auf die Login-Seite.

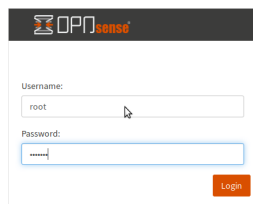


Abb. 131: GUI Login

Melde Dich mit **root** und dem Passwort **Muster!** an. Beim ersten Start erhältst folgende Information:

Gefolgt von folgender Aufforderung:

Starte den **General Setup Wizard** mit dem **Next**- Button. Dieser Wizard führt Dich durch die Konfiguration. Einige Dinge wurden zuvor bereits korrekt für die Basis-Konfiguration eingerichtet.

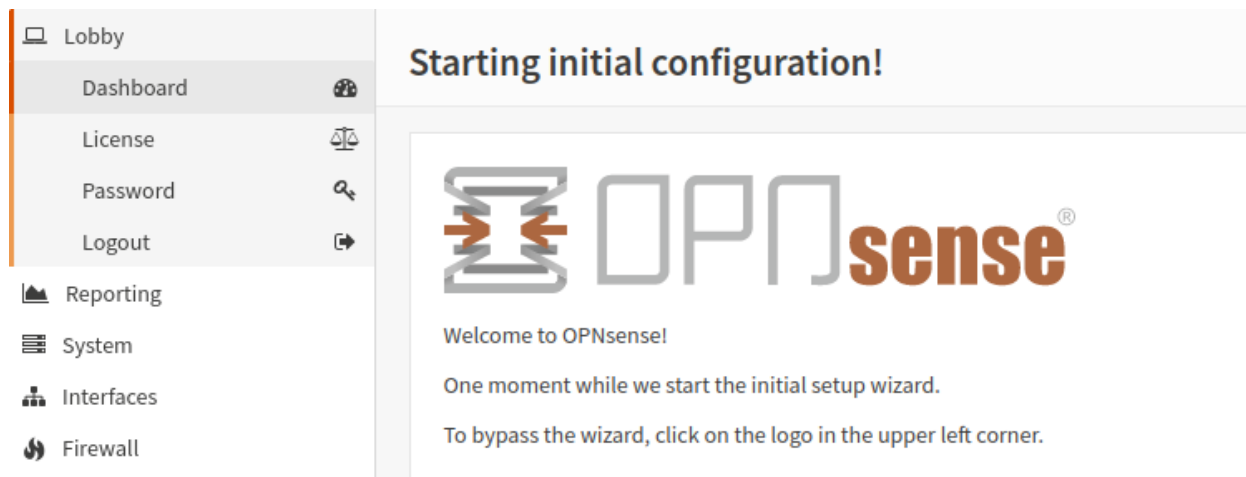


Abb. 132: GUI Erstkonfiguration nach erfolgter Anmeldung

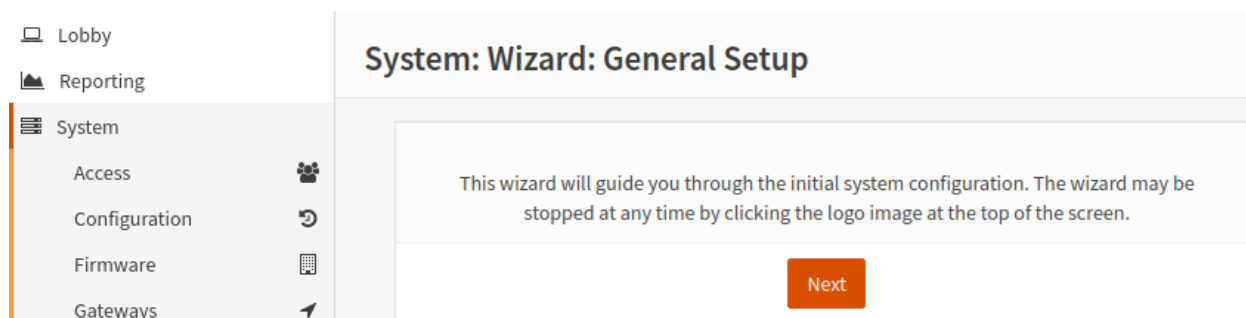


Abb. 133: Setup Wizard

System: Assistent: Allgemeine Information

Achtung: Die Länge des ersten Teils der Domäne darf maximal 15 Zeichen betragen. Die Domain „muster-gymnasium.de“ überschreitet diese Grenze um ein Zeichen, da „muster-gymnasium“ 16 Zeichen lang ist.

Eine gute Wahl ist beispielsweise `linuxmuster.lan`. Beim späteren Setup von linuxmuster.net wird diese ggf. für alle Server-Dienste angepasst.

Abb. 134: Setup: Allgemeine Angaben

Gib als Primary DNS, die neue IP des Upstream Gateway der externen WAN-Schnittstelle an und deaktiviere die Checkbox **Override DNS**.

Weiter geht es mit **Next**

System: Assistent: Zeitserverinformation

Abb. 135: Angabe des Zeitservers

Die Angaben zum Time Server belässt Du wie angegeben. Den Eintrag für die Zeitzone änderst Du auf **Europ/Berlin** wie in nachstehender Abbildung.

Abb. 136: Zeitzone einstellen

Die Angaben übernimmst Du mit **Next**.

System: Assistent: Konfiguriere WAN-Schnittstelle

Danach kommst Du zu den Einstellungen für die WAN-Schnittstelle. Nutzt Du hier DHCP z.B. eines vorgelagerten DSL-Routers, so gibst Du hier DHCP an, ansonsten ändere diese bitte auf **Static**.

The screenshot shows the 'WAN-Konfiguration' window. At the top, 'IPv4 Konfigurationstyp:' is set to 'Static'. Below this is the 'Allgemeine Konfiguration' section with fields for 'MAC-Adresse:', 'MTU:', and 'MSS:'. The 'MTU' field has a tooltip explaining its use for different connection types. The 'MSS' field has a tooltip explaining its use for TCP connections. Below this is the 'Statische IP-Konfiguration' section with fields for 'IP-Adresse:' (set to 192.168.10.5), a dropdown for the subnet mask (set to 24), and 'Upstream Gateway:' (set to 192.168.10.254).

Abb. 137: WAN NIC

Falls Deine Firewall eine statische IP-Adresse hat, die nicht über DHCP erteilt wird, trägst Du sie hier ein.

The screenshot shows a checkbox labeled 'Private RFC1918-Netzwerke blockieren:'. The checkbox is currently unchecked. Below the checkbox is a tooltip explaining that when checked, it blocks data traffic from IP addresses used in private networks (10/8, 172.16/12, 192.168/16) and Carrier Grade NAT addresses (127/8) and Carrier Grade NAT addresses (100.64/10). The tooltip also states that this option should only be used for WAN interfaces that use the public IP space.

Abb. 138: LAN private IP - Angabe RFC1918

Falls Dein Router eine private IP hat, musst Du den Haken bei **Private RFC1918-Netzwerke blockieren** entfernen. Diesen Eintrag findest Du ganz unten auf der Seite, nachdem Du mit der Laufleiste rechts nach ganz unten gegangen bist.

Mit **Weiter** übernimmst Du die von Dir vorgenommenen Einstellungen.

System: Assistent: Konfiguriere LAN-Schnittstelle

The screenshot shows the 'LAN-Konfiguration' window. It has two main fields: 'LAN-IP-Adresse:' (set to 10.0.0.254) and 'Subnetzmaske:' (set to 16). Below the IP address field is a tooltip that says '(leer lassen für keinen)'. At the bottom right is a red button labeled 'Weiter'.

Abb. 139: LAN Schnittstelle

Die IP-Adresse und die Subnetzmaske des Schulnetzes sollten hier eingetragen sein. Sollte dies nicht der Fall sein, ändere dies nun.

System: Assistent: Setze Root-Passwort

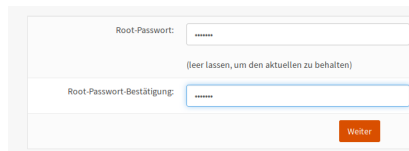


Abb. 140: Root Kennwort setzen

Hinweis: An dieser Stelle muss als root-Passwort **Muster!** eingegeben werden, da später der lmn-Server beim Einrichten der Firewall davon ausgeht, dass das root-Passwort **Muster!** ist!

System: Assistent: Konfiguration neu laden

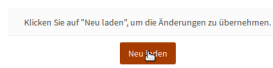


Abb. 141: System-Konfiguration neu laden

Nachdem Du die Einstellungen übernommen hast, können sich auch die Einstellungen des LAN-Netzwerks geändert haben. Dann wirst Du nicht - wie im nächsten Bild zu sehen - über die erfolgreiche Konfiguration informiert.

Initiale Konfiguration abgeschlossen!



Gratulation! OPNsense ist nun konfiguriert.

Bitte denken Sie darüber nach, an das Projekt zu spenden um uns dabei zu helfen, die Kosten zu decken. Besuchen Sie [unsere Webseite](#), um zu spenden oder verfügbare OPNsense-Unterstützungsdienste zu kaufen.

Klicken Sie um [zum Dashboard](#) zu gelangen. Or click to [check for updates](#).

Abb. 142: Erstkonfiguration erfolgreich

Sollte dies bei Dir der Fall sein, musst Du Deinem Admin PC die passende IP-Adresse 10.0.0.10/16, DNS: 10.0.0.254 und das Gateway 10.0.0.254 manuell geben. (hier exemplarisch für unseren Standard-LAN-Bereich)

Gehe dann mit einem Webbrowser auf <https://10.0.0.254>.

Hinweis: Falls Du Dich für das Netz der linuxmuster.net v6.2 entschieden hast, solltest Du die IP-Adresse 10.16.0.10/12, DNS: 10.16.1.254 und das Gateway 10.16.1.254 verwenden.

Du solltest dann auch mit einem Webbrowser auf <https://10.16.1.254> gehen.

Du erhältst eventuell wieder eine Zertifikatswarnung. Akzeptiere diese und fahre fort.

Melde Dich wieder mit root und dem Passwort Muster! an.

DHCP abschalten

Jetzt musst Du den DHCP-Service der Firewall abschalten. Der wird ja später vom Server übernommen.

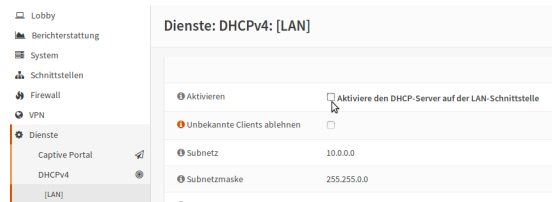


Abb. 143: DHCP deaktivieren

Gehe auf Dienste -> DHCPv4 -> [LAN] und lösche den Haken bei Aktivieren, wenn gesetzt. Speichern lässt Dich Deine Einstellungen unten auf der Seite.

Zusätzliche Netzwerkkarte hinzufügen (Optional)

Die linuxmuster.net v7 läuft bereits mit zwei Netzwerkkarten. Möchtest Du allerdings ein WLAN oder in einer DMZ einen Webserver betreiben, brauchst Du noch weitere Netzwerkkarten.

Wie das geht, siehst Du im Folgenden:

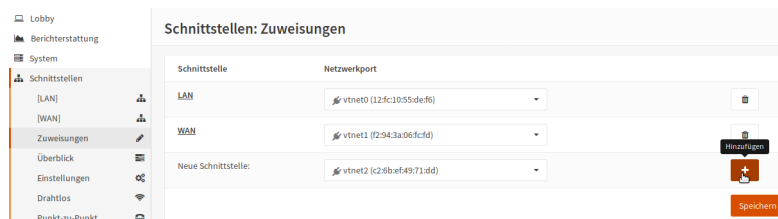


Abb. 144: Schnittstelle hinzufügen

Bei Schnittstellen -> Zuweisungen drückst Du +, um die dritte Schnittstelle Deinem System hinzuzufügen. Diese dritte Schnittstelle ist dann als OPT1 im System bekannt. OPT1 muss nur noch aktiviert und es muss ihr noch eine IP-Adresse zugewiesen werden.

Unter Schnittstellen -> [OPT1] kannst Du diese Einstellungen vornehmen. Der Screenshot zeigt ein Beispiel. Für weitere Netzwerkkarten verfährt Du entsprechend. OPT1 wird dann hochgezählt zu OPT2 etc.

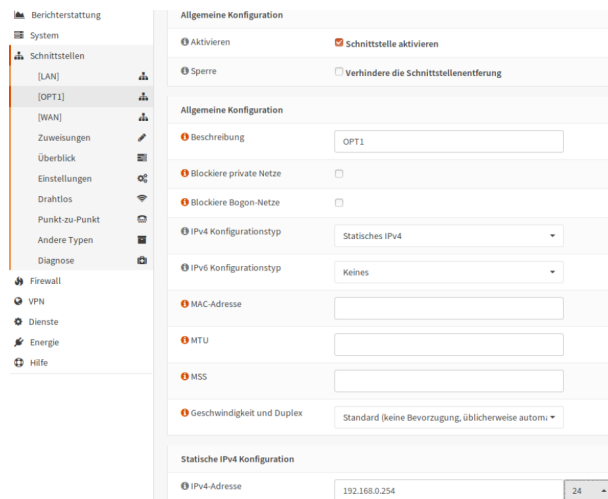


Abb. 145: Neue Schnittstelle konfigurieren

ssh erlauben

Achtung: Damit der Server für das weitere Setup Zugriff auf die OPNsense® hat, musst Du den ssh-Zugriff erlauben. Gehe dafür auf System -> Einstellungen -> Verwaltung.

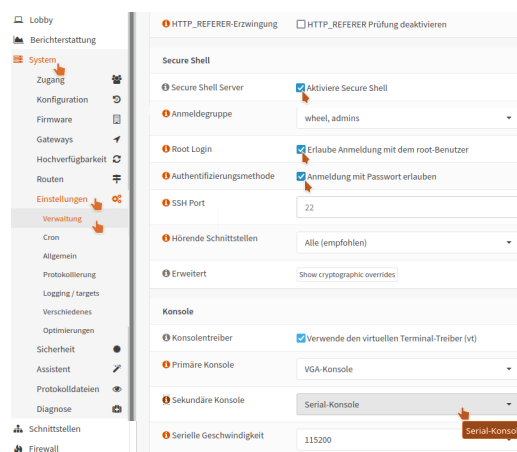


Abb. 146: SSH aktivieren

Setze jeweils den Haken bei Aktiviere Secure Shell, Erlaube Anmeldung mit dem root-Benutzer und Anmeldung mit Passwort erlauben.

Bei dem Punkt Sekundäre Konsole wähle die Serial-Konsole aus. Mit dieser Auswahl wird die *xterm.js-Konsole* nutzbar. (Zur Erinnerung: *Anlegen der VM für linuxmuster server*)

Diese Einstellungen wieder Speichern.

Update der OPNsense®

Aktualisiere nun die OPNsense®, indem Du unter

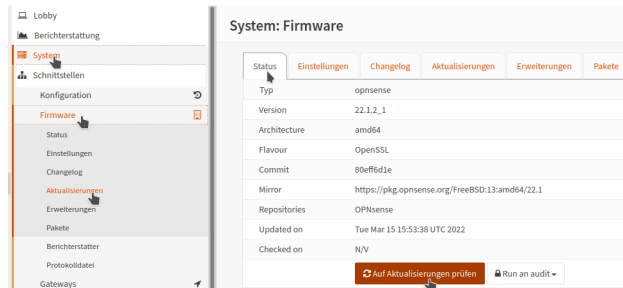


Abb. 147: Aktualisiere die Firmware

System -> Firmware --> Aktualisierungen ---> Status ----> Auf Aktualisierungen prüfen klickst.
Wenn keine Aktualisierungen verfügbar sind, erhältst Du folgende Meldung ...

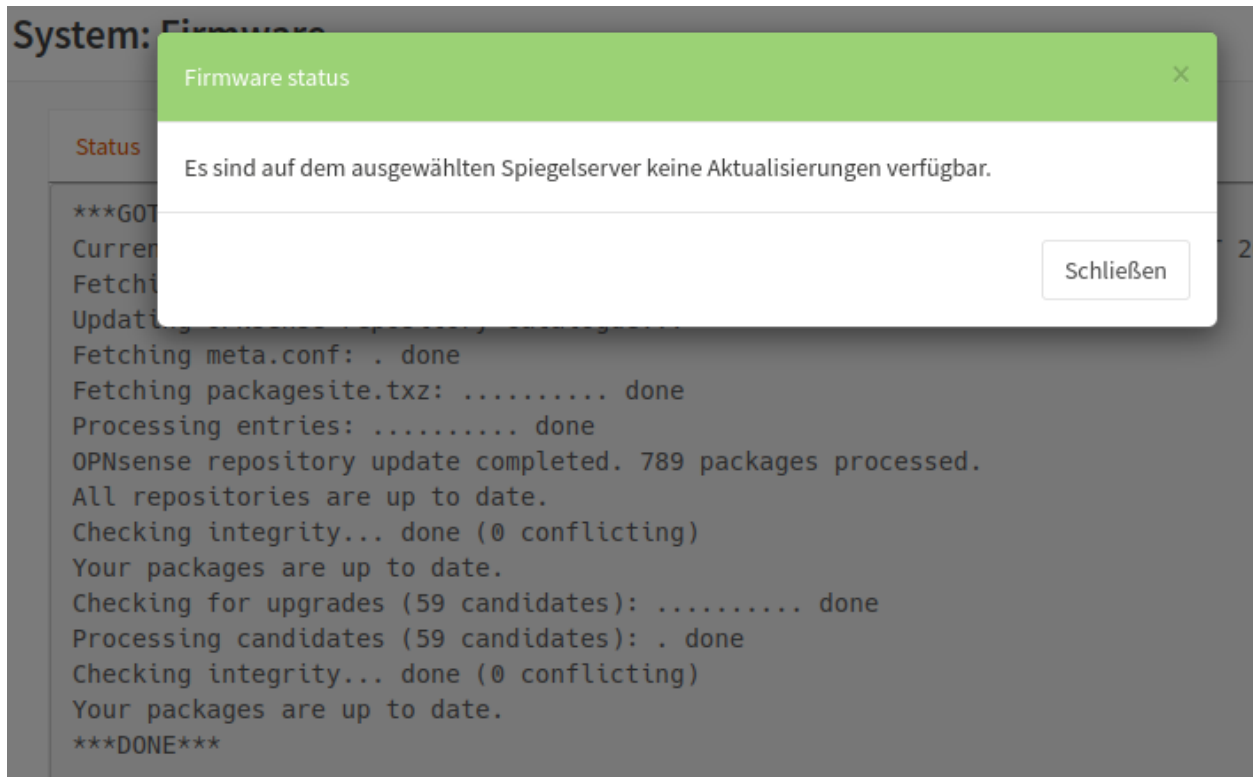


Abb. 148: Keine Aktualisierungen verfügbar

... und kannst zum abschließenden Schritt [Logout](#) gehen.

Sollten Dir - wie in nachstehender Abbildung - unter dem Reiter Aktualisierungen zu aktualisierende Pakete angezeigt werden ...

... dann klicke in o.g. Fenster Jetzt aktualisieren.

Hinweis: Falls Du nicht ins Internet kommst, kann es an der Gateway-Einstellung liegen. Gehe auf System ->

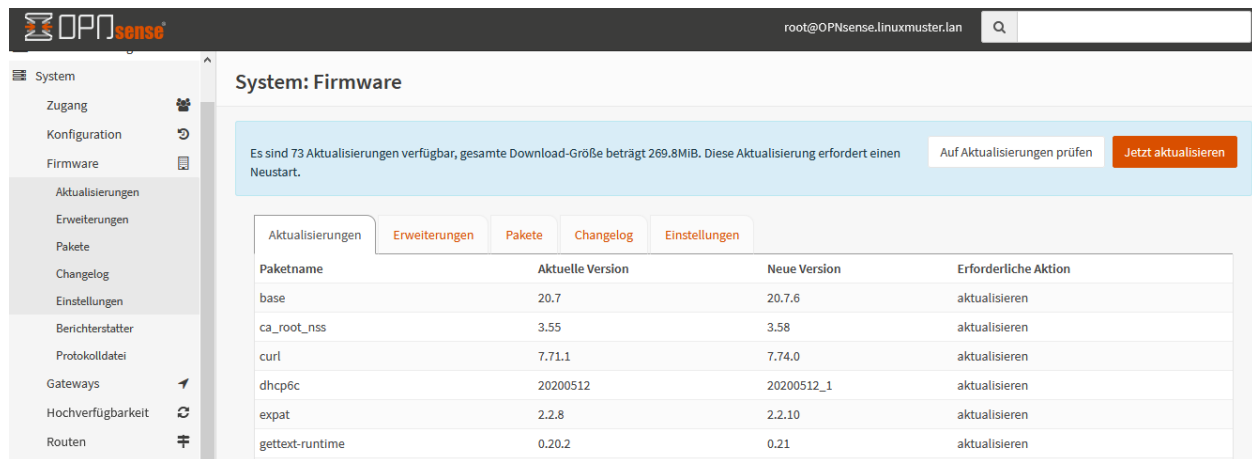


Abb. 149: Aktualisierungen verfügbar

Gateways → Einzeln und editiere Dein Gateway (WANGW).

Setze einen Haken bei **Deaktiviere Gatewayüberwachung**, speichere die Einstellung und übernimm die Änderung. Jetzt ist Dein Gateway online und Du kommst ins Internet. Erstaunlicherweise kannst Du die Gatewayüberwachung wieder aktivieren, ohne dass das Gateway offline geht.

Je nach gefundenen Aktualisierungen, kann ein Neustart erforderlich sein. Dies wird vor dem Update abgefragt und ist zu bestätigen.

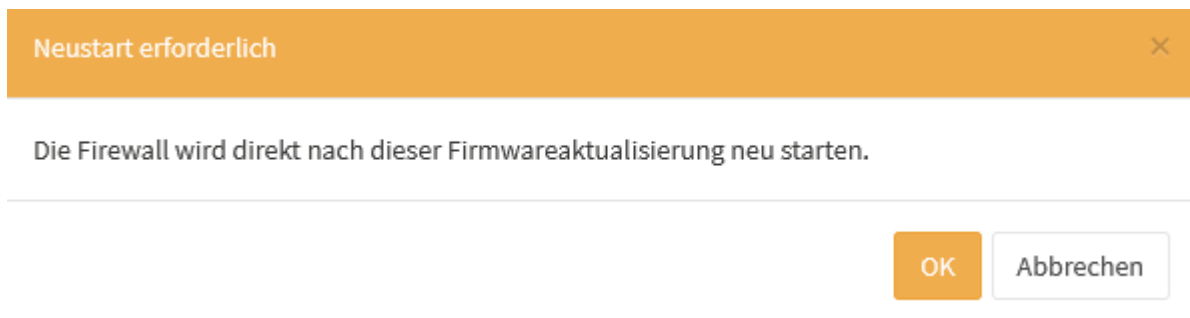


Abb. 150: Reboot bestätigen

Danach werden die Aktualisierungen heruntergeladen und angewendet.

Zum Abschluss erfolgt der Neustart automatisch.

Nach dem Neustart ist die OPNsense® soweit vorbereitet.

System: Firmware

Aktualisiere, bitte warten...

Aktualisierungen

Erweiterungen

Pakete

Changelog

Einstellungen

```
Number of packages to be upgraded: 62
Number of packages to be reinstalled: 2

The process will require 6 MiB more space.
70 MiB to be downloaded.
[1/71] Fetching unbound-1.13.0.txz: ..... done
[2/71] Fetching suricata-5.0.5.txz: ..... done
[3/71] Fetching sudo-1.9.4_1.txz: ..... done
[4/71] Fetching strongswan-5.9.1.txz: ..... done
[5/71] Fetching squid-4.13.txz: ..... done
[6/71] Fetching sqlite3-3.34.0,1.txz: ..... done
[7/71] Fetching rrdtool-1.7.2_4.txz: ..... done
[8/71] Fetching radvd-2.18_2.txz: ..... done
[9/71] Fetching python37-3.7.9_1.txz: ..... done
[10/71] Fetching py37-urllib3-1.25.11,1.txz: ..... done
[11/71] Fetching py37-sqlite3-3.7.9_7.txz: .... done
[12/71] Fetching py37-six-1.15.0.txz: ... done
```

Abb. 151: Aktualisierungen anwenden

Ihr Gerät startet neu

Die Aktualisierung wurde abgeschlossen und ihr Gerät startet nun neu, bitte warten... ⚙

Abb. 152: Automatischer Neustart

Logout

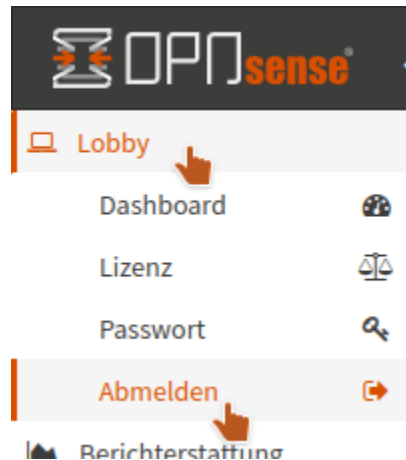


Abb. 153: Logout

Hinweis: Für Anwender einer Virtualisierungslösung empfehlen wir an dieser Stelle einen Snapshot zu erstellen!

4.6.2 Anlegen und Installieren des Servers

Autor des Abschnitts: @cweikl @MachtDochNiX

Bemerkung: Bist Du zuvor der Anleitung „Proxmox vorbereiten“ gefolgt, dann kannst Du fortfahren mit *Erster Start des Servers vom Installationsmedium*.

Hinweis: Willst Du in einer VM installieren, so must Du für die neue VM folgende Mindesteinstellungen angeben:

- Installation von Local/ISO,
- Gast OS: Linux, 6.X - 2.6 Kernel
- BIOS: Boot / MBR / SeaBIOS,
- 2 vCPU,
- 3 GiB RAM,
- storage -> hdd1: 25 GiB -> hdd2: 100 GiB,
- 1 NIC mit Zuordnung zu vSwitch green.

Achte darauf, dass vor dem Start der VM beide Festplatten der VM zugewiesen wurden.

Bei der Einrichtung des Servers musst Du nur einen Server mit 2 HDDs haben und Ubuntu auf der ersten HDD installieren. Die zweite HDD bleibt frei. Auf dieser 2. HDD richtest Du - wie nachstehend beschrieben - ein LVM ein.

Erster Start des Servers vom Installationsmedium

Sprachauswahl

Starte den Server Ubuntu 22.04 LTS Server ISO-Image. Es erscheint das erste Installationsfenster mit der Abfrage zur gewünschten Sprache.

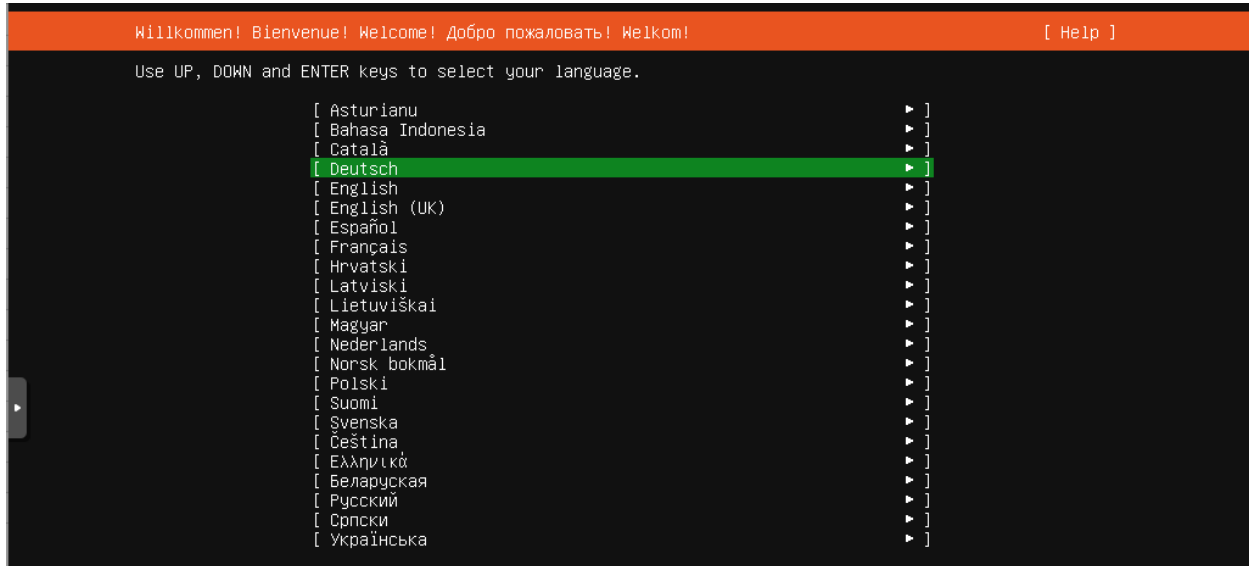


Abb. 154: Wähle Deine bevorzugte Sprache

Wähle Deine bevorzugte Sprache.

Tastaturlayout

Danach wähle Dein Tastaturlayout.

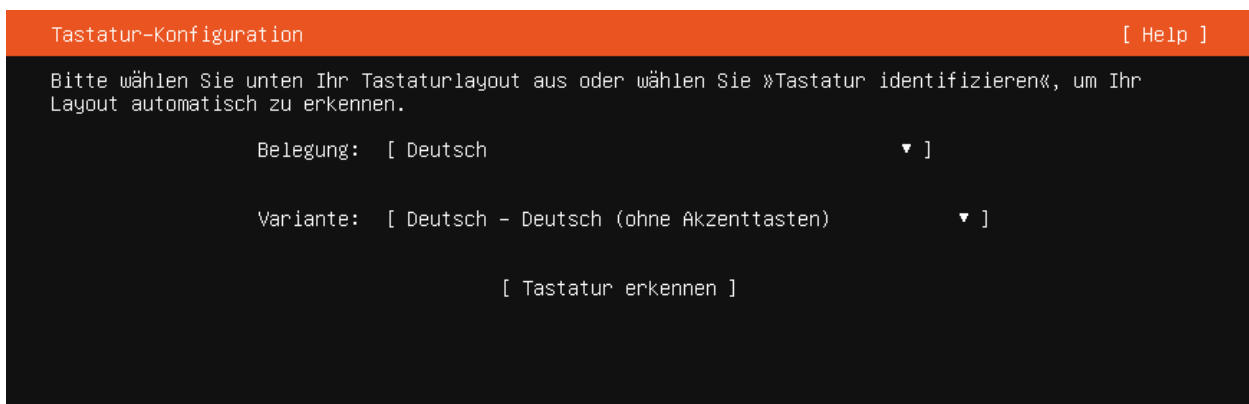


Abb. 155: Wähle Dein Tastaturlayout

Wähle das Tastaturlayout Deutsch und bestätige dies mit **Erledigt**.

Tipp: Wenn Du Dir nicht sicher bist, vor welcher Tastatur Du gerade sitzt:

Wähle nacheinander

Tastatur erkennen → OK → y → Ja → Shift + * → q → z → OK

Da sollte zumindest für eine deutsche Tastatur das richtige Layout finden. Für andere einfach den Abfragen folgen

Installationsart wählen

Wähle die Art der Installation für den Ubuntu Server aus. Es reicht die minimale Installation.

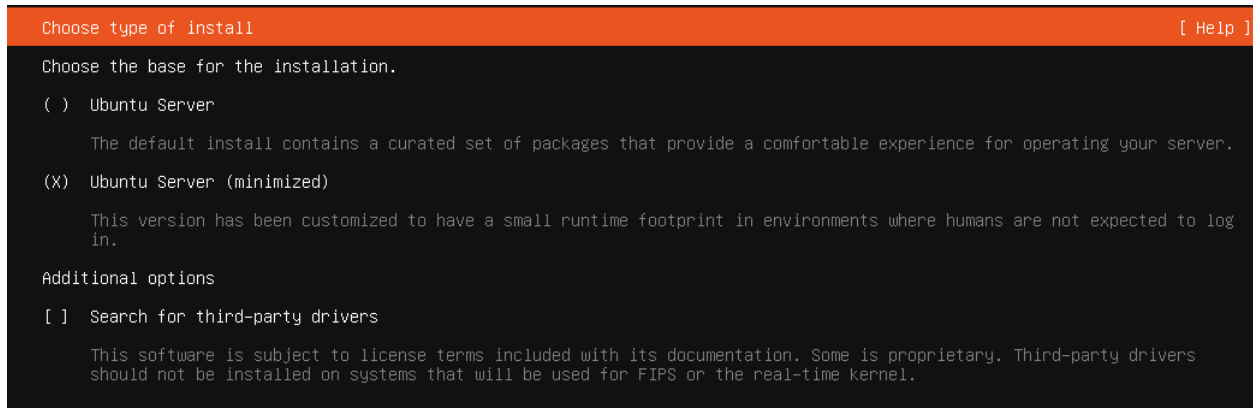


Abb. 156: Installationsart wählen

Netzwerk

Konfiguriere danach Deine Netzwerkkarte.

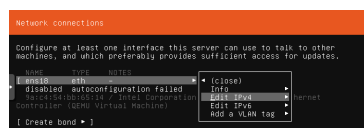


Abb. 157: Konfiguriere Deine Netzwerkkarte

In der Voreinstellung ist die Netzwerkkarte auf DHCP eingestellt. Das klappt natürlich nicht, da der DHCP-Service der Firewall deaktiviert wurde. Du musst also die Konfiguration manuell vornehmen.

Gehe dazu auf die Netzwerkkarte und wähle **Edit IPv4**.

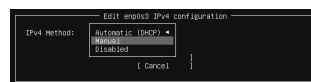


Abb. 158: Ändere die IPv4 Konfiguration

Wähle **Manual** aus.

Gib die Netzwerkkonfiguration, wie im oberen Bild ein beziehungsweise ...

Hinweis: ... passe sie Deinen Bedürfnissen an und übernehme diese mit **Speichern**.

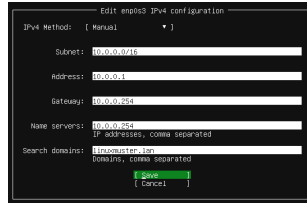


Abb. 159: Trage die IPv4 Einstellungen ein

Achtung: Die Länge des ersten Teils der Domäne darf maximal 15 Zeichen betragen. Die Domäne „muster-gymnasium.de“ überschreitet diese Grenze um ein Zeichen, da „muster-gymnasium“ 16 Zeichen lang ist.

Eine gute Wahl ist beispielsweise `linuxmuster.lan`. Beim späteren Setup von `linuxmuster.net` wird diese ggf. für alle Server-Dienste angepasst.

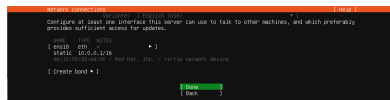


Abb. 160: Bestätige Deine Einstellungen

Mit **Erledigt** geht es weiter.



Abb. 161: Bestätige die Proxy-Einstellungen

Lass die Proxy-Adresszeile leer. Auch diese Anfrage verlässt Du mit **Erledigt**.

Die Mirror-Adresse übernimmst Du ebenfalls mit **Erledigt**.

Aktualisierung des Installers

Bei der angebotene Aktualisierung wählst Du **Aktualisieren auf neuen Installer**.

Speichermedien

Für die weitere Installation benötigst Du zwei unterschiedliche Speichermedien in Deinem Server.

Dabei ist es egal ob es sich dabei um ...

- ... eine reale Festplatte mit zwei Partionen.
- ... zwei reale Festplatten.
- ... zwei virtuelle Festplatten handelt.

In dieser Anleitung beschreiben wir zunächst die Installation auf Basis unserer Mindestanforderungen, also ...

- ... 25G Speichermedium für das System und
- ... 100G Speichermedium für Daten

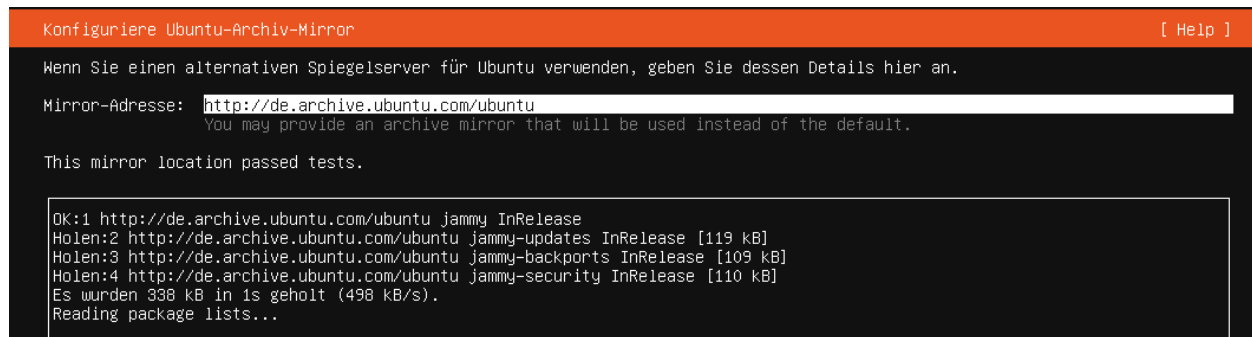


Abb. 162: Bestätige den Ubuntu Mirror Server

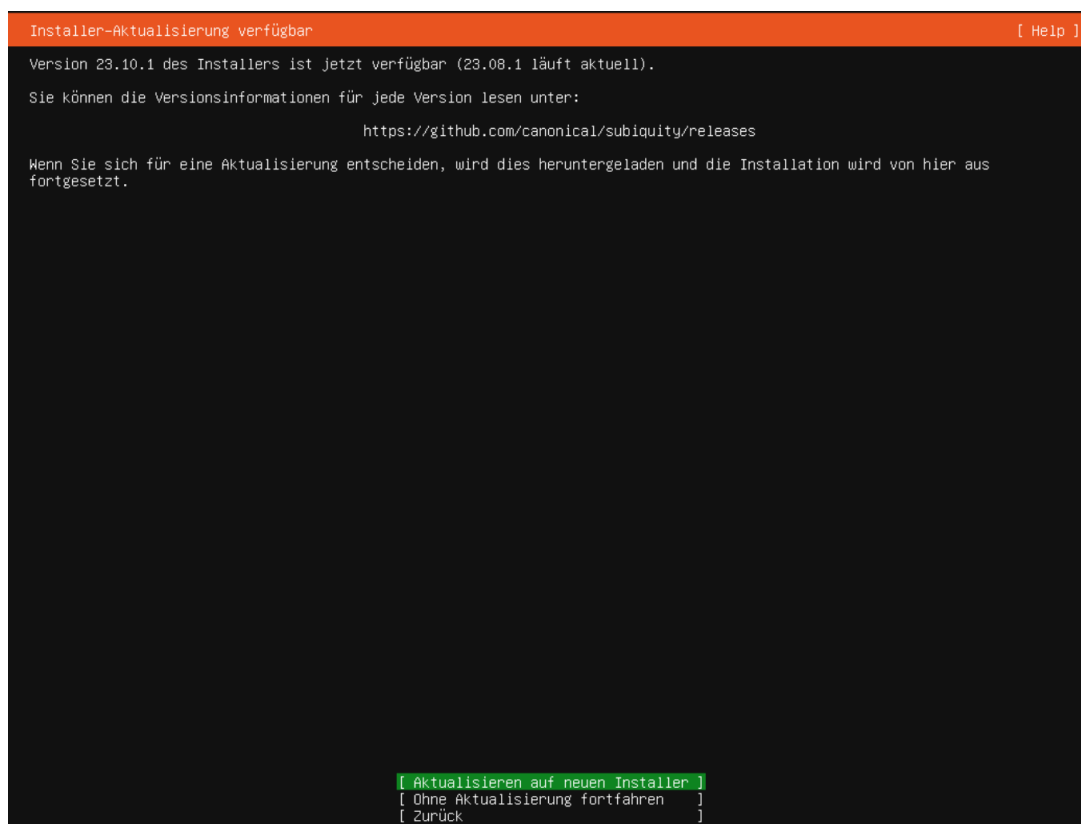


Abb. 163: Installer aktualisieren

Wobei anzumerken ist, dass die Installation des Speicherplatzes für das System / für alle Varianten identisch ist.

Speicher des Systems

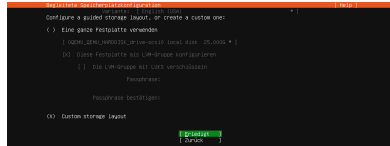


Abb. 164: Eigenes Festplattenlayout wählen

Wähle nun zur Einrichtung der Festplatten Custom Storage Layout aus, wie in obigen Bild dargestellt.

Es werden Dir dann die verfügbaren Geräte angezeigt.

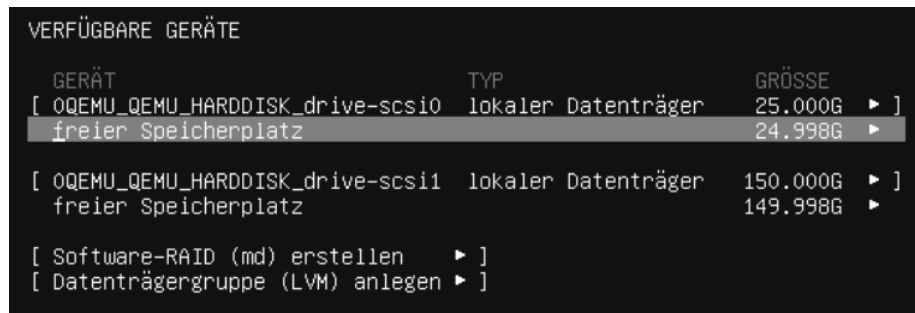


Abb. 165: Anzeige der verfügbaren Geräte - andere HDD-Größen als zuvor genannt

Wähle die erste Festplatte bzw. die erste Partition aus, auf der Du das System des Servers unterbringen möchtest. Es wird ein Kontextmenü angezeigt, bei dem Du mit Add GPT Partition diese erstellen musst.

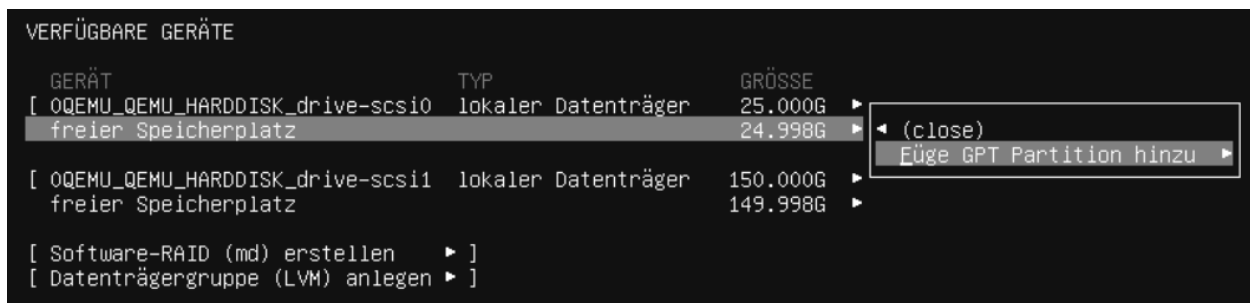


Abb. 166: Füge eine GPT Partition hinzu

Wähle den gesamten Festplattenplatz (einfach das Eingabefeld leer lassen) und formatiere diesen mit dem ext4-Dateiformat und weise diese dem Mount Point / zu.

Gehe auf Erstellen.

Danach gelangst Du zu nachstehendem Bildschirm.

Lasse das zweite Speichermedium unkonfiguriert.

Für das Setup werden noch weitere Partitionen benötigt, die so ohne weitere Angabe von dem später beschriebenen Skript lmn-prepare genutzt werden.

— Füge GPT Partition zum OQEMU_QEMU_HARDDISK_drive-scsi0 hinzu —

Größe (max. 24.998G):

Format: [ext4 ▼]

Mount: [/ ▼]

[Erstellen]

[Abbrechen]

Abb. 167: Lege die Partitionsgröße fest

Speicherplatzkonfiguration

ZUSAMMENFASSUNG DES DATEISYSTEMS

EINHÄNGEPUNKT	GRÖSSE	TYP	GERÄTETYP
[/	24.997G	neues ext4	neu Partition von lokaler Datenträger ▶]

VERFÜGBARE GERÄTE

GERÄT	TYP	GRÖSSE
[OQEMU_QEMU_HARDDISK_drive-scsi1	lokaler Datenträger	150.000G ▶]
freier Speicherplatz		149.998G ▶]

[Software-RAID (md) erstellen ▶]

[Datenträgergruppe (LVM) anlegen ▶]

GENUTZTE GERÄTE

GERÄT	TYP	GRÖSSE
[OQEMU_QEMU_HARDDISK_drive-scsi0	lokaler Datenträger	25.000G ▶]
Partition 1	neu, BIOS grub spacer	1.000M ▶]
Partition 2	neu, formatiert werden als ext4, Nach / eingebunden	24.997G ▶]

[Erledigt]

[Zurücksetzen]

[Zurück]

Abb. 168: Speicherplatzkonfiguration

Hinweis: Für kleine Schulen oder eine Test-Installation sollten diese Vorgaben passen.

LV Name	LV Pfad	Mountpoint	Größe
var	/dev/sg_srv/var	/var	10G
linbo	/dev/sg_srv/linbo	/srv/linbo	40G
global	/dev/sg_srv/global	/srv/samba/global	10G
default-school	/dev/sg_srv/default-school	/srv/samba/schools/default-school	40G ¹

Achtung: Unser lmn-prepare nimmt Dir die nötigen vorbereitenden Aktionen ab. Du läßt also das *zweite Speichermedium unkonfiguriert*.

Speicherplatzkonfiguration übernehmen

Übernehme die Speicherplatzkonfiguration und wähle **Erledigt** aus.

Danach erhältst Du die Rückfrage, ob die Installation fortgesetzt werden soll und die Daten auf der Festplatte hierbei gelöscht werden.

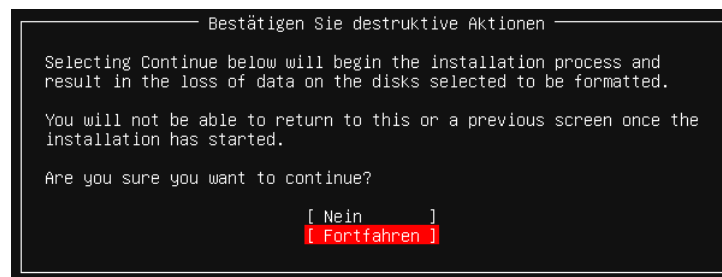


Abb. 169: Bestätige die Partitionseinstellungen

Bestätige dies mit **Fortfahren**.

Benutzerprofil anlegen

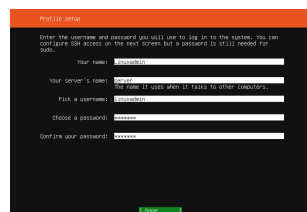


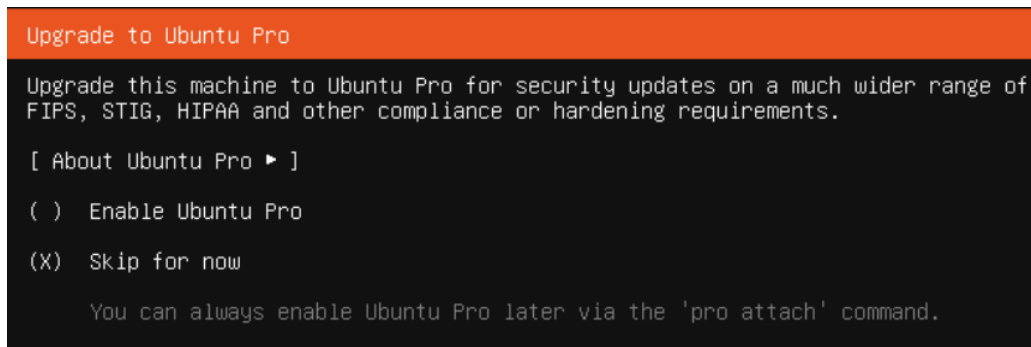
Abb. 170: Lege ein Benutzerprofil an

Nenne den Server **server**. Der Benutzername (linuxadmin) und das Passwort (Muster!) sind frei wählbar - wie in der Abb. dargestellt.

¹ Sollte Deine Festplatte größer sein als die vorgeschlagene Mindestgröße, so wird für diese Partition der maximal übrige freie Platz verwendet. Du kannst zudem eigene Größenangaben vornehmen, sofern Deine Voraussetzungen abweichen.

Abfrage Ubuntu Pro

Danach wirst Du gefragt, ob Die Ubuntu Pro aktiviert werden soll. Überspringe dies.



```
Upgrade to Ubuntu Pro

Upgrade this machine to Ubuntu Pro for security updates on a much wider range of
FIPS, STIG, HIPAA and other compliance or hardening requirements.

[ About Ubuntu Pro ► ]

( ) Enable Ubuntu Pro
(X) Skip for now

You can always enable Ubuntu Pro later via the 'pro attach' command.
```

Abb. 171: Überspringe die Aktivierung von Ubuntu Pro

Abfrage OpenSSH-Zugang

Solltest Du eine Möglichkeit für einen Fernzugang zu dem Server wünschen, aktiviere OpenSSH-Server installieren.

Achtung: Wenn Du dies machst, mache Dir auch Gedanken wie Du diesen Zugang absichern kannst.

Wir empfehlen das PublicKey-Verfahren. <https://wiki.ubuntuusers.de/SSH/#PublicKey-Authentifizierung> (externer Link)

Optionale Server-Pakete

Installiere keine weiteren optionalen Pakete.

Bestätige den Start des Installationsvorganges mit **Erledigt**.

Zum Abschluß der Installation wird automatisch versucht, Updates zu installieren ...

... und danach gilt es den Server neu zu starten.

Hinweis: Bei einer VM achte vor dem Neustart darauf, dass Du die ISO-Datei / DVD ausgeworfen hast und die Boot-Reihenfolge so umgestellt hast, dass die VM direkt von HDD bootet.

Wann die Installation abgeschlossen ist, erkennst Du daran, dass die Anzeige am unteren Bildschirmrand von auf gewechselt ist.

Den Neustart veranlasst Du mit **Jetzt neustarten**, wenn es Dir angeboten wird.

Tipp: Folgendes Vorgehen bietet sich an, wenn der Server virtualisiert betrieben wird und der Hypervisor so schnell den Neustart einleitet, dass Du keine Chance hast, das Installationsmedium zu entfernen.

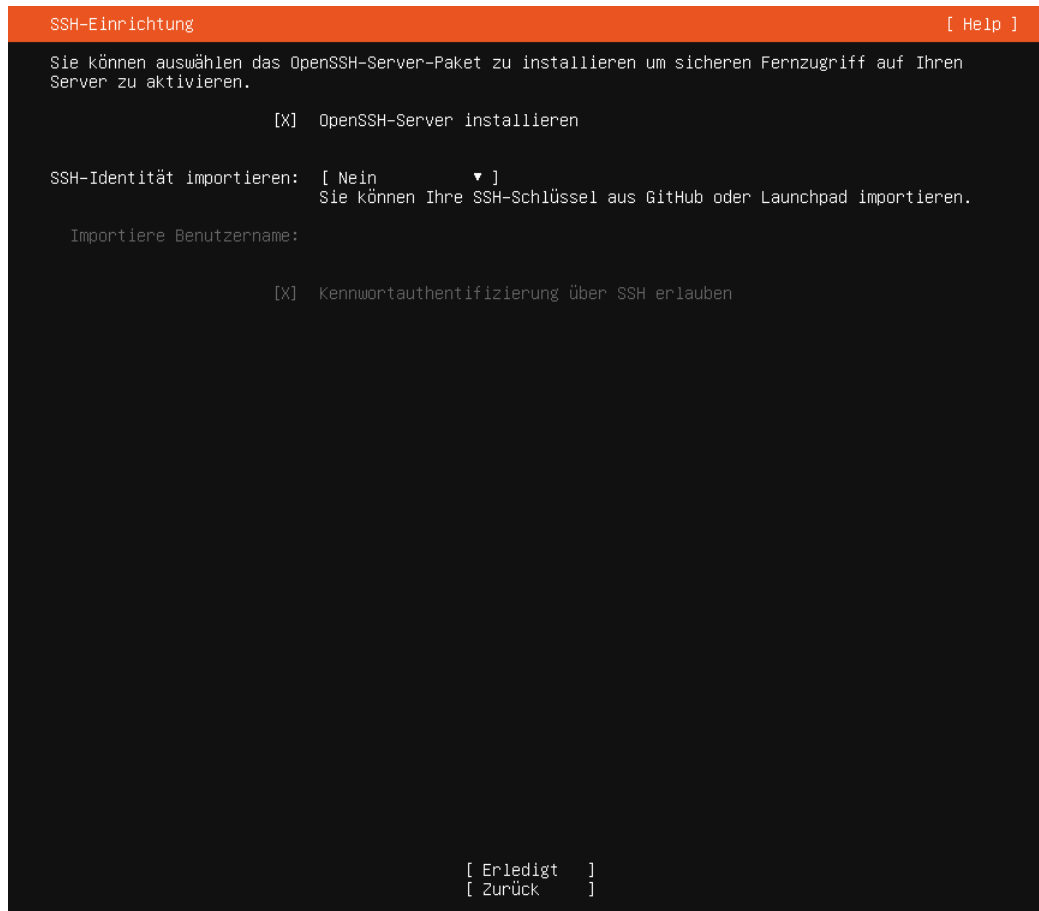


Abb. 172: Aktiviere den SSH-Server

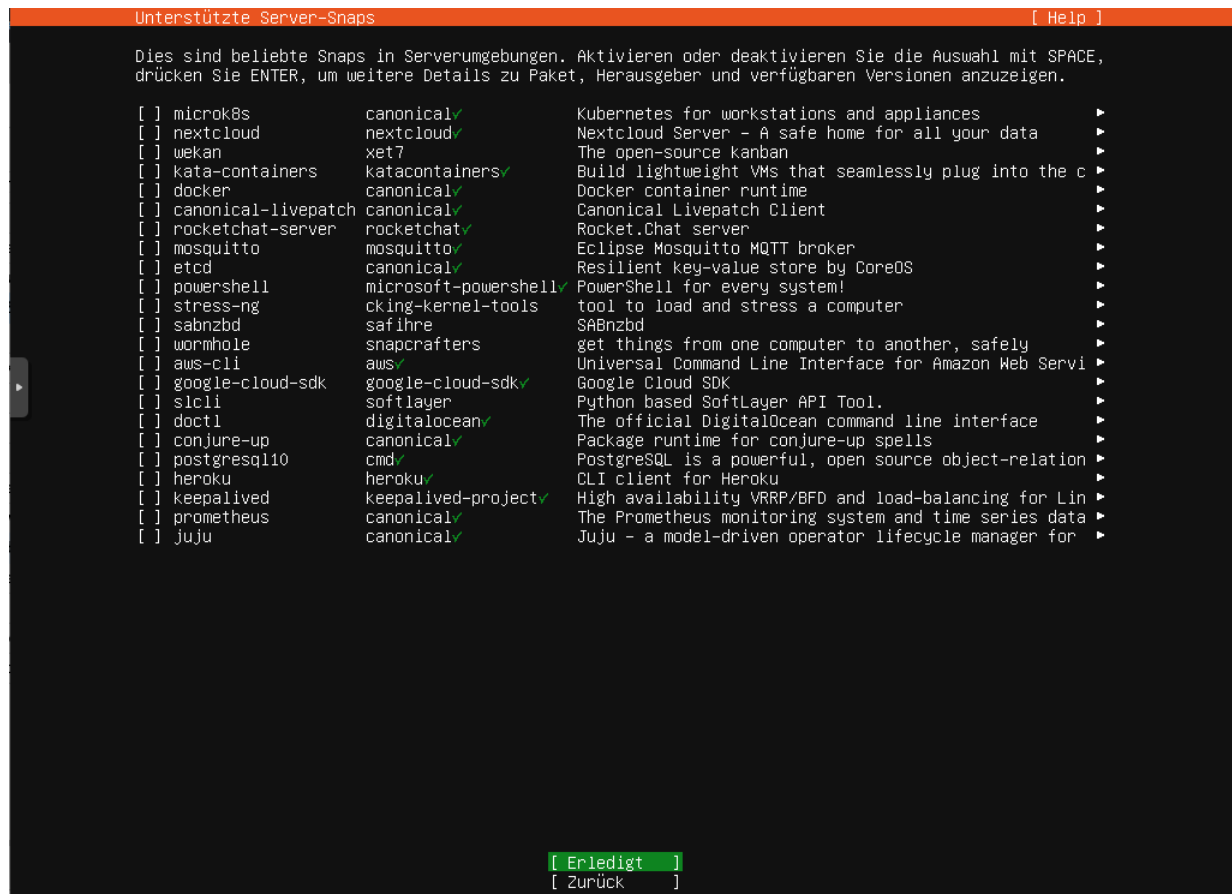


Abb. 173: Deaktiviere alle Server Snaps

```

Installation komplett! [ Help ]

    configuring disk: disk-sdb
    configuring lvm_volgroup: lvm_volgroup-0
    configuring disk: disk-sda
    configuring partition: partition-sda1
    configuring partition: partition-sda2
    configuring format: format-0
    configuring mount: mount-0
    writing install sources to disk
    running 'curtin extract'
    curtin command extract
    acquiring and extracting image from cp:///media/filesystem
    configuring installed system
    running '/snap/subiquity/2651/bin/subiquity-configure-apt
/snap/subiquity/2651/usr/bin/python3 true'
    curtin command apt-config
    curtin command in-target
    running 'curtin curthooks'
    curtin command curthooks
    configuring apt configuring apt
    installing missing packages
    configuring iscsi service
    configuring raid (mdadm) service
    installing kernel
    setting up swap
    apply networking config
    writing etc/fstab
    configuring multipath
    updating packages on target system
    configuring pollinate user-agent on target
    updating initramfs configuration
    configuring target system bootloader
    installing grub to target devices
    finalizing installation
    running 'curtin hook'
    curtin command hook
    executing late commands
    final system configuration
    configuring cloud-init
    downloading and installing security updates -

[ View full log ]
[ Aktualisierung abbrechen und neustarten ]

```

Abb. 174: SchlieÙe die Installation ab

```

[ View full log ]
[ Aktualisierung abbrechen und neustarten ]

```

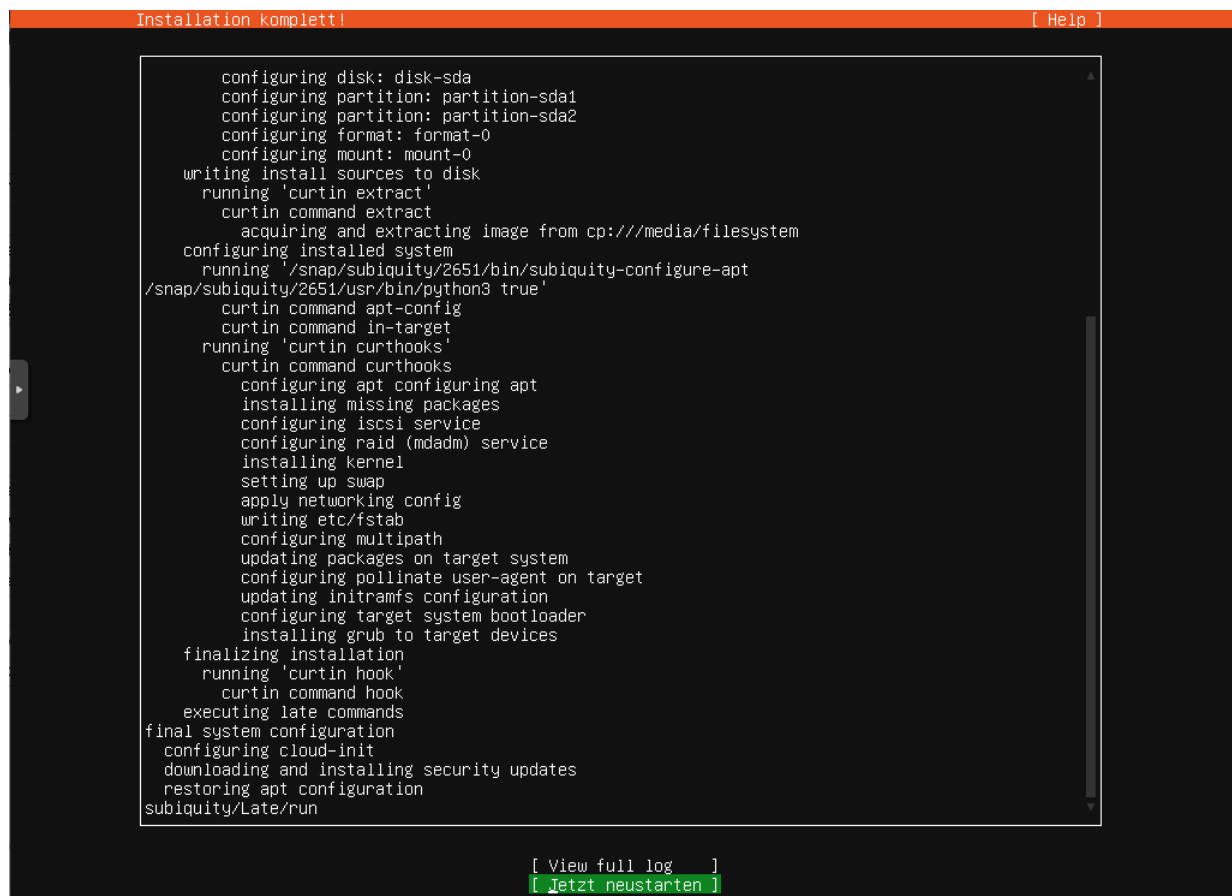
Abb. 175: Server-Aktualisierungen

```

[ View full log ]
[ Jetzt neustarten ]

```

Abb. 176: ... abgeschlosse



```
Installation komplett! [ Help ]

configuring disk: disk-sda
configuring partition: partition-sda1
configuring partition: partition-sda2
configuring format: format-0
configuring mount: mount-0
writing install sources to disk
  running 'curtin extract'
    curtin command extract
      acquiring and extracting image from cp:///media/filesystem
configuring installed system
  running '/snap/subiquity/2651/bin/subiquity-configure-apt
/snap/subiquity/2651/usr/bin/python3 true'
    curtin command apt-config
    curtin command in-target
  running 'curtin curthooks'
    curtin command curthooks
      configuring apt configuring apt
      installing missing packages
      configuring iscsi service
      configuring raid (mdadm) service
      installing kernel
      setting up swap
      apply networking config
      writing etc/fstab
      configuring multipath
      updating packages on target system
      configuring pollinate user-agent on target
      updating initramfs configuration
      configuring target system bootloader
      installing grub to target devices
finalizing installation
  running 'curtin hook'
    curtin command hook
  executing late commands
final system configuration
  configuring cloud-init
  downloading and installing security updates
  restoring apt configuration
subiquity/Late/run

[ View full log ]
[ Jetzt neustarten ]
```

Abb. 177: Starte den Server neu

Alternative zum Jetzt Neustarten gehe zum Punkt Hilfe oben rechts. Dort wählst Du den Menüpunkt Enter Shell aus, wo Du dann den Server gezielt mit `init 0` herunterfährst. Es folgt noch ein Hinweis, dass Du die Entfernung des Installationsmediums mit Enter bestätigen sollst. Im Anschluss daran fährt der Server herunter und Du kannst ihn von neuem starten.

Bei laufender und wie zuvor beschriebener Einrichtung der OPNsense® sollte dies erfolgreich verlaufen.

Basis-Konfiguration des Servers

term.js für die Konsolen-Nutzung in Proxmox aktivieren

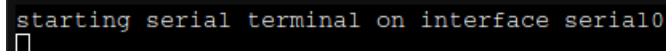
Nachdem Du Dich erneut als `linuxadmin` beziehungsweise mit dem von Dir angelegten Nutzer an der noVNC Konsole angemeldet hast, gib diese zwei Zeilen Code nacheinander ein:

```
sudo systemctl enable serial-getty@ttyS0.service
```

```
sudo systemctl start serial-getty@ttyS0.service
```

Fahre nun die virtuelle Maschine (VM) herunter und starte sie erneut.

Wähle jedoch oben rechts `>_ Console -> xterm.js`. Es öffnet sich das Terminal-Fenster der VM und es erscheint folgender Hinweis:



```
starting serial terminal on interface serial0
█
```

Abb. 178: Starte die serielle Schnittstelle

Nach einem Enter wirst Du zur Eingabe Deines Passwortes aufgefordert.

Nach erfolgter Anmeldung mit Deinem Account kannst Du die ab jetzt folgenden Codezeilen einfach zwischen der Anleitung und dem Server mittels Copy-and-paste übertragen. Abhängig von dem Betriebssystem Deines Administration-PCs klappt vielleicht auch Drag-and-drop. Einfach mal testen.

```
stty cols 120 rows 60
```

Bemerkung: Der Befehl sorgt dafür, dass die Zeilenumbrüche hoffentlich zu Deiner Konsolen-Anzeige passen. Ansonsten musst Du die Angaben für die Zeichen (cols) und Zeilen (rows) anpassen.

Proxmox Guest-Agent installieren

Um mit Proxmox die Server VM herunterfahren zu können, oder für den Snapshot diese vorher korrekt „einzufrieren“, ist die Installation eines Gast-Agenten unter Ubuntu Server 22.04 erforderlich. Zudem musst Du noch dem Agenten unter Proxmox aktivieren.

Gehe dabei wie folgt vor:

1. Installiere auf der Server-Konsole die benötigten Pakete für den QEMU-Gast-Agenten:

```
sudo apt update
sudo apt install qemu-guest-agent
```

2. Aktiviere auf Ubuntu Server den QEMU-Gast-Agenten als Daemon via Konsole:

```
sudo systemctl enable qemu-guest-agent
```

3. Fahre die virtuelle Maschine herunter: `sudo shutdown -h now`
 4. Wähle in der Proxmox WebUI die virtuelle Maschine für den Ubuntu Server aus. Gehe dort zu **Options**

QEMU Guest Agent

Default (Disabled)

Abb. 179: Proxmox QEMU Guest Agent aufrufen

5. Wähle den QEMU Guest Agent aus und klicke dann oben auf **Edit**.
 6. Aktiviere den QEMU Guest Agent, indem Du den Haken setzt und dies mit **OK** bestätigst.

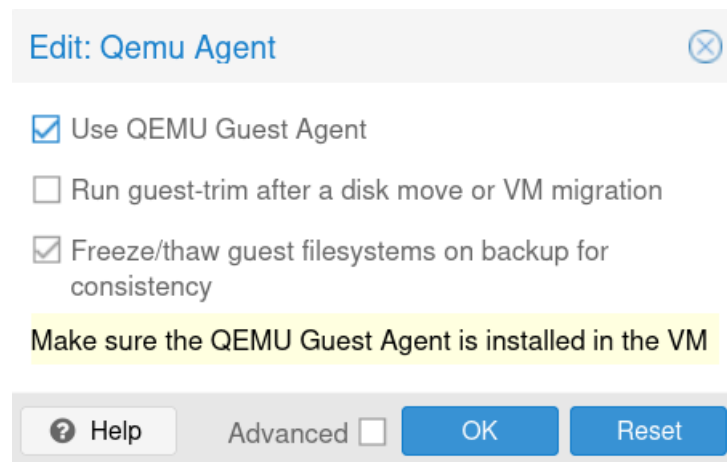


Abb. 180: Aktiviere den QEMU Guest Agent

7. Starte danach die VM neu.

Automatische Updates abschalten

Der frisch installierte Ubuntu-Server hat automatische Updates aktiviert. Das solltest Du abschalten, denn nur so kannst Du sicher sein, dass Updates nicht während der Unterrichtszeit in Deiner Einrichtung durchgeführt werden und zu eventuellen Problemen im Schulalltag führen.

Werde mit ...

```
sudo -i
```

... zum Nutzer `root` und editiere, beispielsweise mit `nano`, die Datei ...

```
apt install nano
nano /etc/apt/apt.conf.d/20auto-upgrades
```

Ersetze bei `APT::Periodic::Unattended-Upgrade` die `"1"` durch `"0"`; Mit `<Strg>+o` und anschließend `Enter` speicherst Du die Änderung ab. Und mit `<Strg>+x` verlässt Du `nano` wieder.

Jetzt kannst Du den Server updaten, mit ...


```
apt update && apt dist-upgrade
```

Nachdem Dir neue Pakete zur Anzeige gebracht wurden, startest Du den Upgrade-Prozess mit `j`. Du erhältst die Rückfrage, welche Dienste, die noch mit alten Bibliotheken arbeiten, neu gestartet werden sollen.

Hier spielt es keine Rolle, welche Dienste Du angibst, denn zum Abschluss startest Du den Server einmal neu mit dem Befehl `reboot`. Danach sind alle Dienste mit den jeweils neu installierten Bibliotheken neu gestartet.

Achtung: Durch das Deaktivieren der automatischen Updates liegt jetzt natürlich die Verantwortung des zeitnahen Einspielen von Updates bei Dir bzw. der Person, die für die Administration verantwortlich zeichnet!

Test der Verbindung zur Firewall

Es folgt ein letzter Test, um sicherzustellen, dass die SSH-Verbindung zwischen dem Server und der Firewall funktioniert. Diese ist für das weitere Vorgehen entscheidend.

Nach dem erneuten Einloggen ruft Du folgende Zeile an der Konsole des Servers auf:

```
ssh root@10.0.0.254
```

Da es die erste Kontaktaufnahme zwischen dem Server und der Firewall ist,

```
linuxadmin@server:~$ ssh root@10.0.0.254
The authenticity of host '10.0.0.254 (10.0.0.254)' can't be established.
ECDSA key fingerprint is SHA256:WS8ycmtRQGABoFoguzx0MlvaeygMf1AxikPTVyFKSOg.
Are you sure you want to continue connecting (yes/no)? yes
```

Abb. 181: Akzeptiere den ECDSA Schlüssel der OPNsense

ist es notwendig, dass Du den Key akzeptierst.

Anschließend sollte der Log-in nach der Eingabe des Passwortes `Muster!` erfolgreich sein.

Mit `0`) Logout beendest Du die Verbindung.

Hinweis: Für Anwender einer Virtualisierungslösung empfehlen wir an dieser Stelle einen Snapshot zu erstellen!

Weiter geht es jetzt mit *Server auf lmn7.2 vorbereiten*

4.6.3 Server auf lmn7.2 vorbereiten

Autor des Abschnitts: @cweikl @MachtDochNiX

Nachdem Du die Firewall und den Server wie beschrieben installiert hast, müssen beide Maschinen fertig konfiguriert werden.

Passe zuerst die Zeitzone an und deinstalliere `cloud-init`.

```

*** OPNsense.linuxmuster.lan: OPNsense 23.7.5 ***

LAN (vtnet1)    -> v4: 10.0.0.254/16
WAN (vtnet0)    -> v4/DHCP4: 192.168.122.250/24

HTTPS: SHA256 72 35 19 78 64 6E 13 6C 23 DA 24 62 FB 96 9A 30
          44 F2 17 40 54 29 B6 4C C4 0F F2 AA FC 1F 14 26
SSH:   SHA256 y1lv1d7XvCaxcv5m7/GosT3PhoJfYLjyh7tK4By9qmM (ECDSA)
SSH:   SHA256 b3nm3jvxrQn1IBcouqQbpNen+5z8Tmwj9htiSyASoDI (ED25519)
SSH:   SHA256 bpAxd0claSi4Vb95RodMSVC+WhY/WuFFJiHwCa6NEw0 (RSA)

0) Logout                                7) Ping host
1) Assign interfaces                     8) Shell
2) Set interface IP address              9) pfTop
3) Reset the root password               10) Firewall log
4) Reset to factory defaults             11) Reload all services
5) Power off system                      12) Update from console
6) Reboot system                         13) Restore a backup

Enter an option: 0

FreeBSD/amd64 (OPNsense.linuxmuster.lan) (ttyv0)

login: █

```

Abb. 182: OPNsense Login Bildschirm

Vorbereitungen

Zeitservereinstellungen überprüfen

Nachdem Du nun den Server vorbereitet hast, überprüfe die Zeiteinstellungen auf dem Server. Dazu gibst Du in der Konsole folgenden Befehl an:

```
timedatectl
```

Es wird hier noch die UTC-Zeit angegeben. Wie für die OPNsense muss nun die Zeitzone angepasst werden. Die erfolgt mit folgendem Befehl:

```
sudo timedatectl set-timezone Europe/Berlin
# erneute Ausgabe der Zeiteinstellungen mit
timedatectl
```

Du solltest nun als Zeitzone Europe/Berlin und die korrekte Lokalzeit sowie die korrekte UTC - Zeit angezeigt bekommen.

Cloud-init deinstallieren

Cloud-init kannst Du unter Ubuntu mit folgenden Schritten löschen:

```
# Disable start
sudo touch /etc/cloud/cloud-init.disabled
# Uninstall
sudo apt-get purge cloud-init
sudo rm -rf /etc/cloud/ && sudo rm -rf /var/lib/cloud/
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
# Reboot
sudo reboot
```

Führe aber zuvor nachstehende Schritte aus.

Default-Locale setzen

Erzeuge zuerst die Locales mit:

```
sudo localectl status
System Locale: LANG=C.UTF-8
    VC Keymap: n/a
    X11 Layout: de
    X11 Model: pc105
```

Prüfe, welche Locales installiert sind:

```
locale -a
C
C.utf8
POSIX
```

Sollte das Paket Locales nicht installiert sein, führe folgenden Befehl aus:

```
sudo apt install apt-utils locales
```

Erzeuge nun die Locales neu:

```
sudo dpkg-reconfigure locales
```

Configuring locales

Locales are a framework to switch between multiple languages **and** allow users to use their language, country, characters, collation order, etc.

Please choose which locales to generate. UTF-8 locales should be chosen by default, particularly **for** new installations. Other character sets may be useful **for** backwards compatibility **with** older systems **and** software.

- | | |
|----------------------|-----------------------------|
| 1. All locales | 252. gl_ES ISO-8859-1 |
| 2. C.UTF-8 UTF-8 | 253. gl_ES.UTF-8 UTF-8 |
| 3. aa_DJ ISO-8859-1 | 254. gl_ES@euro ISO-8859-15 |
| 4. aa_DJ.UTF-8 UTF-8 | 255. gu_IN UTF-8 |
| 5. aa_ER UTF-8 | 256. gv_GB ISO-8859-1 |
| 6. aa_ER@saaho UTF-8 | 257. gv_GB.UTF-8 UTF-8 |
| 7. aa_ET UTF-8 | 258. ha_NG UTF-8 |
| 8. af_ZA ISO-8859-1 | 259. hak_TW UTF-8 |
| 9. af_ZA.UTF-8 UTF-8 | 260. he_IL ISO-8859-8 |
| 10. agr_PE UTF-8 | 261. he_IL.UTF-8 UTF-8 |
| 11. ak_GH UTF-8 | 262. hi_IN UTF-8 |
| 12. am_ET UTF-8 | 263. hif_FJ UTF-8 |

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
Locales to be generated: de_DE.UTF-8

1. None 2. C.UTF-8 3. de_DE.UTF-8
Default locale for the system environment: 3

Generating locales (this might take a while)...
de_DE.UTF-8... done
Generation complete.
```

Du kannst die Default-Locale ggf. auch mit folgenden Befehl neu setzen:

```
$sudo localectl set-locale LANG=de_DE.UTF-8
```

Achtung: Wichtiger Hinweis, schon jetzt!

Solltest Du mit Deiner Konfiguration von unseren Standard-Vorgaben bei dem zuletzt genannten Punkt abweichen, musst Du Deine Einstellungen unbedingt bei Aufruf des Skriptes `lmn-prepare` anpassen!

Hinweis: Erstelle jetzt einen Snapshot Deiner Server-VM.

Letzter Test vor Anwendung des Skriptes `lmn-appliance`

Als letzte Überprüfung, bevor Du das Skript einsetzt, verbinde Dich vom Server aus mit der Firewall via ssh.

```
ssh root@10.0.0.254
```

Du solltest Dich nach der Eingabe des Passwortes `Muster!` auf der Konsole der OPNsense® wiederfinden. Eventuell musst Du auch vorher deren Key akzeptieren. Mit `0` solltest Du Dich wieder ausloggen und zurück auf der Server-Konsole sein.

Sollte dieser Test erfolgreich sein, steht der abschließenden Vorbereitung nichts mehr im Wege:

Das Skript `lmn-appliance`

Das Skript `lmn-appliance` bereitet den Server / die Appliance vor:

- Es bringt das Betriebssystem auf den aktuellen Stand,
- richtet das linuxmuster.net-Paket-Repo ein,
- installiert das Paket `linuxmuster-prepare` und
- startet dann das Vorbereitungsskript `lmn-prepare`, - das die für das jeweilige Appliance-Profil benötigten Pakete installiert, - das Netzwerk konfiguriert, - das root-Passwort auf `Muster!` setzt und - im Falle des Serverprofils optional LVM einrichtet.

Wenn Du nicht mehr an Deinem Server eingeloggt bist, melde Dich erneut an.

Überprüfe Deine Festplatten und Partitionen mit

```
lsblk
```

NAME	MAJ:MIN	RM	SIZE	RO	TYPE	MOUNTPOINTS
sda	8:0	0	50G	0	disk	
└─sda1	8:1	0	1M	0	part	
└─sda2	8:2	0	50G	0	part	/
sdb	8:16	0	200G	0	disk	
sr0	11:0	1	1024M	0	rom	

In o.g. Beispiel wurde Ubuntu Server auf der 1. Festplatte (sda) installiert. Die zweite Festplatte (sdb) kennt noch keine Partitionen.

Skript herunterladen

Führe danach folgende Befehle in der Eingabekonsole aus:

Wechsele Deinen Log-in und werde zu root, falls du es nicht mehr sein solltest:

```
sudo -i
```

Lade das lmn-appliance Skript herunter und setze die Ausführungsberechtigung:

```
wget https://raw.githubusercontent.com/linuxmuster/linuxmuster-prepare/master/lmn-
↪appliance
chmod +x lmn-appliance
```

Aufruf lmn-appliance

Das Skript ist generell wie folgt zu starten:

```
./lmn-appliance <Optionen>
```

Die möglichen Optionen findest Du hier dokumentiert: <https://github.com/linuxmuster/linuxmuster-prepare>

Für unsere Beispielkonfiguration rufe nun das Skript lmn-appliance so auf, dass Dein Server vorbereitet wird. Das LVM wird dann auf der zweiten Festplatte eingerichtet wird.

```
./lmn-appliance -p server -u -l /dev/sdb
```

Mit dem Parametern -u (unattended) und -l wird dann ein LVM - hier auf der 2. Festplatte (sdb) - mit folgenden Werten eingerichtet:

- var: 10 GiB
- linbo: 40 GiB
- global: 10GiB
- default-school: restlicher Plattenplatz

Installation mit Deinen Vorgaben

Nachstehendes Beispiel geht davon aus, dass Du eine zweite HDD mit einer Größe von 1TiB hast.

```
./lmn-appliance -p server -l /dev/sdb -v var:50,linbo:500,global:50,default-school:100
↪%FREE
```

Es wird hier also mit dem Profil server auf der zweiten Festplatte (/dev/sdb) ein LVM eingerichtet. Auf der zweiten Platte werden vier Volumes mit den Größen

- var: 50GiB
- linbo: 500GiB
- global: 50GiB
- default-school: verbleibender Rest der zweiten Festplatte - hier 400 GiB -

eingerichtet.

Achtung: Passe die Größenangaben auf Deine Situation an.

Ablauf

Es wird zuerst das LVM auf der zweiten Platte eingerichtet, danach werden alle erforderliche Pakete geladen und installiert. Dies kann etwas dauern. Nach Abschluss des Installations- und Vorbereitungsarbeiten wirst Du aufgefordert, den Server neu zu starten.

```
## Passwords
# root ... OK!
# linuxadmin ... OK!
## Writing configuration

## The system has been prepared with the following values:
# Profile    : server
# Hostname   : server
# Domain     : linuxmuster.lan
# IP         : 10.0.0.1
# Netmask    : 255.255.0.0
# Firewall   : 10.0.0.254
# Gateway    : 10.0.0.254
# Interface  : ens18
# Swapsize   : 2G
# LVM device: /dev/sdb
# LVM vlms   : var:10,linbo:40,global:10,default-school:100%FREE

### Finished - a reboot is necessary!
```

Ist lmn-appliance ohne Fehler durchgelaufen, starte danach den Server neu mit dem Befehl:

```
reboot
```

Danach steht dem Setup v7.2 nichts mehr im Wege.

Paketquellen eintragen

Hinweis: Dies muss nur ausgeführt werden, sofern Du den Server bzw. die VM nicht mit dem Skript `lmn-appliance` vorbereitet haben solltest.

Es müssen für linuxmuster.net v7.2 sowohl die Paketquellen für die v7.1 als auch die Paketquellen für die v7.2 eingetragen werden.

Zur Eintragung der Paketquellen führe folgende Befehle in der Eingabekonsole aus:

```
sudo sh -c 'wget -qO- "https://deb.linuxmuster.net/pub.gpg" | gpg --dearmor -o /usr/
↳share/keyrings/linuxmuster.net.gpg'
```

Hinweis: -O -> [-][Großbuchstabe O]

Damit installierst Du den Key für das Repository von linuxmuster.net und aktivierst ihn.

Danach fügst Du zuerst das Linuxmuster 7.1 Repository hinzu.

```
sudo sh -c 'echo "deb [arch=amd64 signed-by=/usr/share/keyrings/linuxmuster.net.gpg]
↳https://deb.linuxmuster.net/ lmn71 main" > /etc/apt/sources.list.d/lmn71.list'
```

Zuletzt fügst Du das Linuxmuster 7.2 Repository hinzu.

```
sudo sh -c 'echo "deb [arch=amd64 signed-by=/usr/share/keyrings/linuxmuster.net.gpg]
↳https://deb.linuxmuster.net/ lmn72 main" > /etc/apt/sources.list.d/lmn72.list'
```

Aktualisiere die Softwareliste des Servers:

```
sudo apt update
```

4.6.4 Proxmox in das interne Netz bringen

Autor des Abschnitts: @cweikl @MachtDochNiX

Du hast bis hiering bereits folgende Schritte absolviert:

- Du hast die Firewall installiert,
- eine Erstkonfiguration der Firewall erstellt,
- Du hast einen Snapshot der Firewall-VM erstellt,
- Du hast die Server-VM erstellt
- Du hast Ubuntu-Server installiert und vorkonfiguriert
- Du hast den Server mit `lmn-prepare` für das spätere linuxmuster-setup vorbereitet,
- Du hast von der Server-VM einen Snapshot erstellt.

Hast Du diese Schritte erfolgreich durchlaufen, gilt es jetzt, die Netzwerk-Konfiguration des Proxmox-Host umzukonfigurieren.

Ziel ist es, dass der Proxmox-Host nunmehr **nur noch im internen Netzwerk (green)** erreichbar ist. Der Host wird dann durch die OPNsense - Firewall geschützt. Die OPNsense ist zugleich das neue Gateway für den Proxmox-Host, um Zugriffe in das externe Netz zu ermöglichen.

Um dies umzusetzen, sind die Bridges umzukonfigurieren.

1. vmbr0 - red - externes Netzwerk (IP im Beispiel 192.168.0.20/24 bzw. IP via DHCP)
2. vmbr1 - green - internes Netzwerk (IP im LAN: 10.0.0.20/16)

Rufe auf dem Proxmox-Host eine Eingabekonzole auf und ändere die Datei `/etc/network/interfaces` wie folgt:

```
auto lo
iface lo inet loopback

iface eno1 inet manual

iface eno2 inet manual

auto vmbr0
iface vmbr0 inet dhcp          #holt dynamisch eine IP-Adresse
    bridge-ports eno1
    bridge-stp off
    bridge-fd 0
#red

auto vmbr1
iface vmbr1 inet manual
    address 10.0.0.20/16
    gateway 10.0.0.254
    bridge-ports eno2
    bridge-stp off
    bridge-fd 0
#green
```

Danach must Du noch die Datei `/etc/hosts` anpassen:

```
127.0.0.1 localhost.localdomain localhost
10.0.0.20 proxmox.mydomain.local proxmox

# The following lines are desirable for IPv6 capable hosts

::1      ip6-localhost ip6-loopback
fe00::0  ip6-localnet
ff00::0  ip6-mcastprefix
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
ff02::3  ip6-allhosts
```

Diese Einstellungen werden mit dem nächsten Start des Proxmox-Hosts aktiv.

Daher gilt es sicherszustellen das die OPNSense® automatisch startet. Dafür bei (Proxmox-Host → VM → Options → Start on boot) die Aktivierung setzen.

Hast Du dies erfolgreich umgesetzt, dann starte den Proxmox-Host neu.

Du musst den Admin-PC an den internen Switch des grünen Netzes nach dem Neustart des Proxmox-Host, wie dargestellt, anschließen. Der Admin-PC benötigt nun eine manuell vergebene IP:

- IP Address: 10.0.0.10/16
- Subnetzmaske: 255.255.0.0

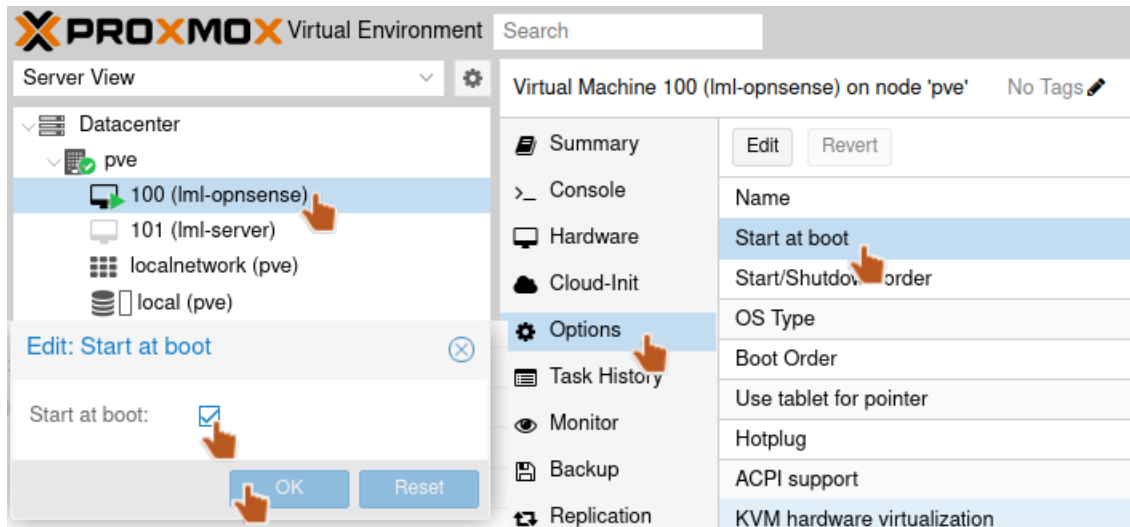


Abb. 183: Autostart der OPNSense®

Abb. 184: Proxmox Netzwerk

- Gateway: 10.0.0.254
- DNS: 10.0.0.254, 8.8.8.8

Danach solltest Du vom Admin-PC aus folgende Hosts erreichen können:

1. 10.0.0.20 - Proxmox-Host
2. 10.0.0.254 - OPNSense
3. 8.8.8.8 - externer DNS-Server
4. linuxmuster.net - externe URL

Der Proxmox-Host ist nun „hinter“ der OPNSense® und kann über diese auf das Internet zugreifen. Dafür muss die virtuelle Maschine der OPNSense® aktiv sein, was Du mit dem vorherigen Schritt sichergestellt hast.

4.7 Setup v7.2

Autor des Abschnitts: @cweikl, @MachtDochNix

Achtung: Alle linuxmuster 6.x Systeme können statt einer Neuinstallation über eine [Migration auf linuxmuster 7.2](#) umgezogen werden, dennoch ist die Erstkonfiguration hier eine notwendige Voraussetzung.

Alle linuxmuster 7.1 Systeme werden lediglich über ein [Upgrade v7.1 auf v7.2](#) auf linuxmuster v7.2 aktualisiert. Ein erneutes Setup ist dann nicht mehr erforderlich.

Es gibt 2 Möglichkeiten, die Erstkonfiguration durchzuführen:

1. Setup mit der Schulkonsole
2. Setup im Terminal

Lies zunächst alle wichtigen Hinweise des Setup Kapitels und mache dann entweder auf der Schulkonsole (grafisch / GUI) oder im Terminal weiter.

4.7.1 Wichtige Hinweise

- Nach Abschluss dieses Setups sind die (AD-)Domäne und andere Details des Netzwerks permanent festgelegt und nur durch eine erneute Neuinstallation änderbar.

Es ist daher wichtig, zu diesem Zeitpunkt ein **Snapshot/Backup von Server und Firewall** anzufertigen.

Sollte es beim Setup Fehler geben, oder Einstellungen nochmals geändert werden müssen, sind die virtuellen Maschinen auf den Stand des Snapshots zurückzusetzen und das Setup muss erneut aufgerufen werden.

- Beim Domänennamen ist zu beachten:
 - nutze immer eine echte externe Domain, die auf Deine Organisation registriert ist -> z.B. `meineschule.de`
 - für das Setup von linuxmuster benötigst Du nun eine Subdomain, die vom AD DNS-Server autoritativ intern aufgelöst wird, aber niemals von extern.
 - der AD DNS-Server arbeitet immer nur für diese eine Subdomain und die darunter liegenden Namensräume autoritativ.
 - alle internen Clients müssen den AD DNS-Server als DNS-Server nutzen.
 - diese Subdomain darf nicht länger als 15 Zeichen sein (NetBIOS-Name) und keine Satzzeichen enthalten.
 - der Fully Qualified Domain Name (FQDN) darf nicht länger als 64 Byte sein.
 - nutze niemals nicht registrierte Domains wie z.B. `.local` -> `meineschule.local`
- Beim Setup von linuxmuster gibst Du also einen Domänennamen nach folgendem Schema an:

hostname.subdomain=NetBIOS-Name.domain.tld ein funktionierendes Beispiel wäre: server01ad.linuxmuster.meineschule.de

- server01ad -> hostname
 - linuxmuster -> subdomain
 - domain -> meineschule
 - de -> tld
- Es wird also eine extern auflösbare, registrierte Domain genutzt und bei der Einrichtung des Servers wird eine eigene interne Subdomain als AD-Domäne angegeben.

Zum Beispiel `linuxmuster.meineschule.de` -> linuxmuster als Subdomain zur Domain `meineschule.de`.
Der erste Part `linuxmuster` wird in diesem Beispiel dann als SAMBA-Domäne verwendet.
Der volle Name(FQDN) des Servers ist dann `server.linuxmuster.meineschule.de`.

Hinweis: Daraus folgt wie in einem reinen MS-Netzwerk, dass der linuxmuster.net-Server immer den Service DNS für die Vertrauensstellung liefern muss, denn er übernimmt die Rolle des Domänencontrollers für die Active Domäne. In unserer Beschreibung als SAMBA-Domäne bezeichnet.

- Alle Hosts, die im Setup konfiguriert werden, müssen bereits laufen (OPNsense und Server) und sie müssen sich im internen LAN gegenseitig erreichen.
- v6.x Systeme, die mithilfe der Migration auf linuxmuster.net 7.2 migriert werden, können dabei für eine neue (oder die alte) Domäne konfiguriert werden.

4.7.2 Anpassung des Netzbereichs

Die Standardkonfiguration sieht vor, dass Geräte im Netzbereich 10.0.0.0/16 sind.

v6.x Systeme, die mithilfe der Migration auf linuxmuster.net 7.2 migriert werden, sollten den bisher verwendeten Netzbereich beibehalten.

Hinweis: Die erforderlichen Anpassungen der Netzkonfiguration - sofern diese von dem Standard abweichen sollen - sind vor der Ausführung der Erstkonfiguration durchzuführen. Zur Durchführung der Anpassungen folge bitte dem Kapitel *Netzbereich anpassen*.

4.7.3 Auswahl der Setup-Variante

Server-Konsole

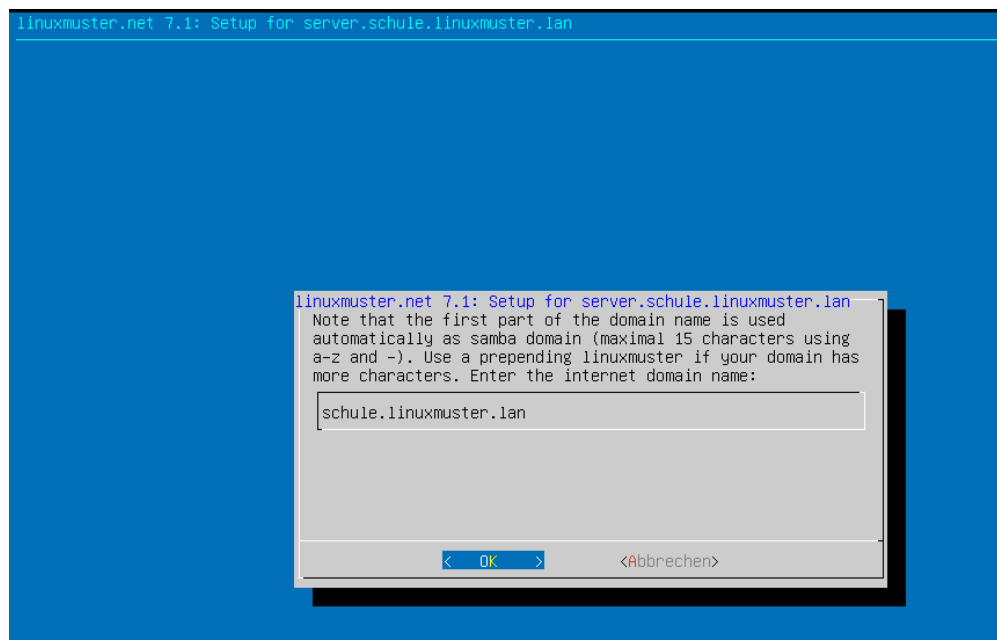


Abb. 185: Hier geht es zum *Setup im Terminal*

WEB UI

(formerly known as Schulkonsole)

Welcome to linuxmuster.net V7



Please follow the next few steps to quickly configure your system

System language

de

GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <<https://fsf.org/>>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

THE GNU OPERATING SYSTEM IS A FREE SOFTWARE, FREELY AVAILABLE TO EVERYONE.

☒ I accept the license terms

NEXT

Abb. 186: Hier geht es zum *Setup via Schulkonsole*

4.8 Setup via Schulkonsole

Autor des Abschnitts: @cweikl, @MachtDochNix

4.8.1 Setup über die Schulkonsole

Die Weboberfläche (WebUI/Schulkonsole) erreicht man über einen Browser eines Gerätes (im folgenden Admin-PC genannt) im Servernetzwerk. Dafür konfiguriert man den Admin-PC mit der festen IP-Adresse `10.0.0.10` (entsprechend `x.x.x.10` in jeder anderen Netzwerkkonfiguration) der Netzwerkmaske `255.255.0.0`, dem Gateway `10.0.0.254` und dem DNS-Eintrag `10.0.0.1`.

Öffne auf dem Admin-PC mit einem Webbrowser die URL `http://10.0.0.1`. Melde Dich hier einmalig mit dem Benutzer `root` und dem Passwort `Muster!` an.

Hinweis: Achte darauf, dass vor dem Setup die Verbindung zur Schulkonsole via URL noch unverschlüsselt mit HTTP erfolgt.

Es erscheint der Hinweis, dass Du das Webinterface nicht als Benutzer `root` benutzen sollst, es sei denn, Du verwendest dieses das erste Mal.

Bei einem unkonfiguriertem System wird direkt das Setup aufgerufen.

Es erscheint der Einrichtungsassistent. Hier musst Du zunächst die gewünschte Sprache auswählen. Zudem musst Du die GNU Lizenzbedingungen akzeptieren, indem Du bei `I accept the licence terms` einen Haken setzt.

Danach klickst Du auf `Weiter`.

Im nächsten Dialog musst Du den Schulnamen, die Stadt, das Bundesland und das Landeskürzel eintragen bzw. auswählen. Zudem trägst Du einen Hostnamen für den Server ein. Der Domainname spielt eine besondere Rolle, insbesondere,




root

.....

Log in

Abb. 187: Anmeldung als Benutzer root

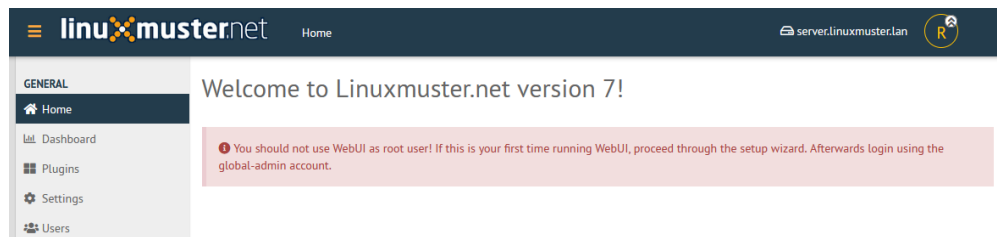


Abb. 188: Willkommen bei linuxmuster.net

Welcome to linuxmuster.net V7



Please follow the next few steps to quickly configure your system

System language

de

GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <<https://fsf.org/>>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software distribution in the form of executable code.

☒ I accept the license terms

NEXT

Abb. 189: Akzeptiere die Lizenzvereinbarung

wenn eine Adresse verwendet werden soll, die intern und extern identisch sein soll, so dass mit dem FQDN intern und extern gearbeitet wird.

Hinweis:

schule.de oder linuxmuster.lan stellen den Domainnamen mit der sog. Top Level Domain (TLD) dar. Die TLD lan wird nicht extern verwendet, sondern ist nur für den internen Gebrauch sinnvoll. Die TLD de wird extern genutzt. Hat Deine Schule die De-Domain meineschule.de registriert, dann musst Du hier eine Subdomain angeben, die zugleich die sog. Samba-Domain darstellt. Für den Namen dieser Sub-/Samba-Domain gibt es Einschränkungen, die unbedingt beachtet werden müssen: Es werden nur englische Kleinbuchstaben a bis z akzeptiert. Sonst keinerlei Zeichen. Es dürfen zudem maximal 15 Zeichen verwendet werden.

Richtig: gshoenningen (12 Zeichen, keine Umlaute und Satzzeichen etc.), **Falsch:** GSO-Heinrich-Böll-Hönningen (26 Zeichen, Großbuchstaben, Umlaute, Bindestriche)

School Information

School name

Berthold-Brecht-Gesamtschule

Location

Bad Hönningen

State

Rheinland-Pfalz

Language

de

Server & Domain Information

Server name

server

Domain name

gshoenningen.gs-hoenningen.de

Note: The first part (up to the first dot) of the domain name will be used as the SAMBA domain and has a maximal length of 15 characters. We suggest to use "linuxmuster" or "lmn" and prepend it to your domain.
Valid characters are: a-z

Server FQDN

server.gshoenningen.gs-hoenningen.de

BACK

NEXT

Abb. 190: Setup: Schulinformationen

Danach klickst Du auf Weiter/Next.

Der nächste Dialog legt das Passwort des globalen Administrators global-admin und das von root fest. Die Einschränkungen zur Passwortsicherheit sind dem Hilfetext zu entnehmen.

Wichtig: Nach dem erfolgreichen Abschluss der Erstkonfiguration gilt für root das neu gesetzte Passwort.

Hinweis:

- Das beim Setup eingegebene Adminpasswort wird für folgende administrativen User gesetzt:

Account Information

Global-Admin and root password

.....

.....

Note: Minimal length is 7 characters. Use upper, lower and special characters or numbers. (e.g. mUster!)

Valid characters are: a-z A-Z 0-9 !\$+-@#%&*()[]{}

BACK

NEXT

Abb. 191: Kennwort für die Benutzer global-admin und root festlegen

- root auf dem Server
 - root auf der Firewall
 - global-admin (AD)
 - pgmadmin (AD)
 - linbo (/etc/rsyncd.secrets)
- Es sollten die Passwörter der o.g. User nach dem Setup geändert werden, so dass jeder User ein eigenes Password hat.
 - Achte darauf, dass Dein Passwort den Komplexitätsanforderungen entspricht, die mit samba4 aktiviert sind: Mind. 7 Zeichen, Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen. Zulässige Sonderzeichen sind: a-z A-Z 0-9 ?!\$+-@#%&*()[]{}
 - In der Datei /etc/linuxmuster/sophomorix/default/school/school.conf sind die Kennwortlängen für Schüler (Standard: 10 Zeichen) und Lehrer (12 Zeichen) angegeben.
 - Die Grundeinstellungen für Kennwörter in samba4 kannst Du Dir auf dem Server in der Konsole mit `samba-tool domain passwordsettings show` anzeigen lassen.

Danach klickst Du auf Weiter/Next.

Du erhältst die Rückfrage, ob die Firewall ggf. nicht konfiguriert werden soll. Sofern Du das System zusammen mit der OPNsense als Firewall **neu einrichtest**, setzt Du **keinen** Haken und klickst Du auf Weiter/Next.

External Services

Skip Firewall Configuration ☐

BACK

NEXT

Abb. 192: Überspringe die Firewall Konfiguration

Es wird danach die Zusammenfassung der vorgenommenen Einstellungen in der Übersicht dargestellt. Du kannst die getroffenen Einstellungen auch noch prüfen lassen. Danach wird Dir wie in der Abb. die geprüfte Zusammenfassung angezeigt

Summary

Almost done...

We got all information needed for the provisioning process.
Before proceeding please check your data **carefully!**

School Information

School Name: **Berthold-Brecht-Gesamtschule**
Location **Bad Hönningen**
State **Rheinland-Pfalz**
Country **de**

Server & Domain Information

Server name **server**
Domain name **gshoenningen.gs-hoenningen.de**
Server FQDN **server.gshoenningen.gs-hoenningen.de**

External Services

Firewall Firewall will be **configured!**

BACK

START PROVISIONING

Abb. 193: Zusammenfassung der Setup-Einstellungen

Hinweis: Sollte die Installation anhalten oder fehlschlagen, sollte man alle Appliances auf den Zustand vor dem Setup zurücksetzen.

Starte nun die Installation, in dem Du auf **Start Provisioning** klickst.

Es erscheint ein Installationsfenster, in dem die verschiedenen Installationsschritte angezeigt werden. Dieser Vorgang dauert eine ganze Weile. Ist die Installation abgeschlossen, gelangst Du zu folgendem Fenster:

Setup

```

Create WebUI Upload Folder
* WebUI Setup Success!

##### final #####
##### Disabling service iscsid ..... Success! #####
##### Disabling service dropbear ..... Success! #####
##### Disabling service lxcfs ..... Success! #####
##### Restarting apparmor service ..... Success! #####
##### Writing school name to school.conf ..... Success! #####
##### Starting device import ..... Success! #####
##### Starting subnets import ..... Success! #####
##### Creating web proxy sso keytab ..... Success! #####
##### Removing admin password from setup.ini ..... Success! #####

##### linuxmuster-setup finished at 2023-12-21 12:15:59 #####

```

Options
☒ Autoscroll

FINISH

Abb. 194: Setup-Fenster

Zum Abschluss siehst Du den Eintrag

```
### linuxmuster-setup finished at ... ###
```

Schliesse das Setup nun mit **Finish** ab. Es erscheint eine Statusmeldung, dass das Setup abgeschlossen ist und Du Dich danach mit dem Benutzer **global-admin** anmelden sollst.

Bestätige dies mit **Close**.

Rufe auf dem Server das Terminal auf und starte den Server neu:

```
sudo reboot
```

Setup complete

Information

The setup was completed.

If you hit the close button you will be forwarded to a ssl encrypted version of LinuxMuster Webui. Unless you install a trusted certificate you will be asked to confirm the untrusted, just created, certificate. Confirm this certificate to proceed

Keep in mind **not** to login as root user. Login using the **global-admin** credentials you specified during the setup.

CLOSE

Abb. 195: Abschluss des Setups

4.8.2 Anmeldung an der Schulkonsole

Es wurde beim Setup ein self-signed certificate erstellt, so dass Du dieses beim erstmaligen Aufruf mit dem Browser akzeptieren musst.

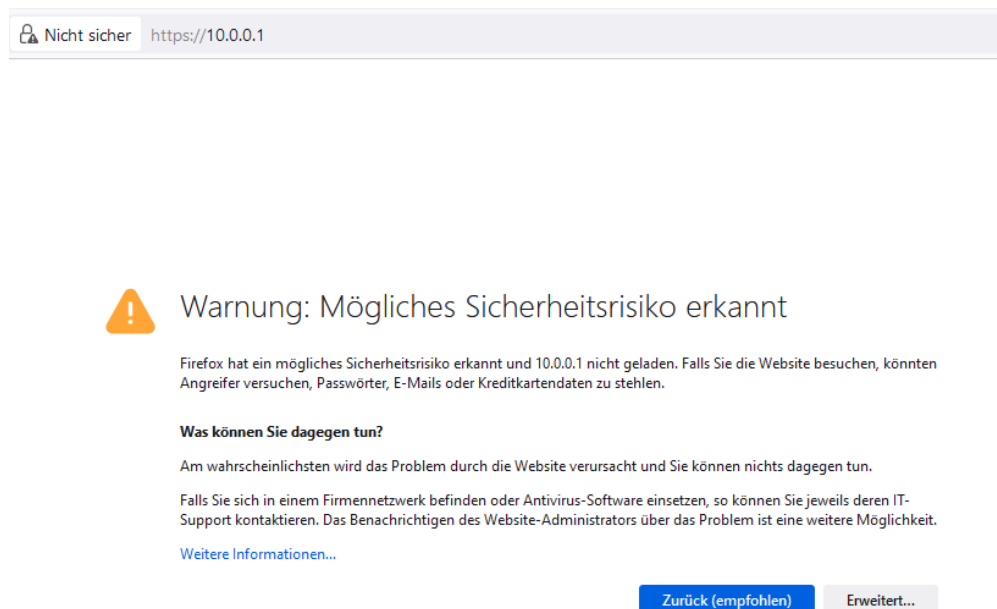


Abb. 196: SSL: Mögliches Sicherheitsrisiko - Erweitert

Der Browser zeigt Dir den Warnhinweis an. Klicke auf **Erweitert...**

Es erscheint auf der gleichen Seite unten ein weiterer Eintrag. Bestätige diesen, indem Du den Button **Risiko akzeptieren und fortfahren** auswählst.

Danach kommst Du zur Anmeldeseite der WebUI/Schulkonsole. Melde Dich nun als Benutzer **global-admin** an und nutze das während des Setups festgelegte Kennwort.

Nach erfolgreicher Anmeldung gelangst Du zur Hauptseite der Schulkonsole.

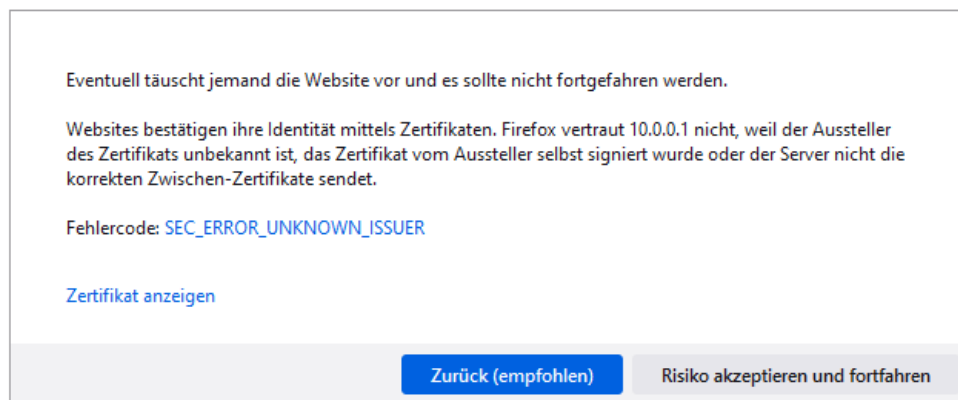


Abb. 197: SSL: Risiko akzeptieren und fortfahren



Abb. 198: Login als Benutzer global-admin

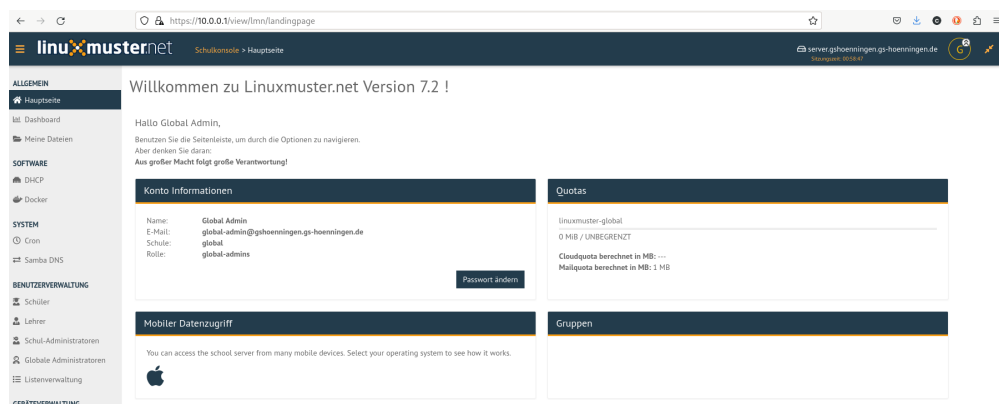


Abb. 199: Hauptseite der Schulkonsole

4.8.3 Berechtigungen der Log-Dateien anpassen

Nach dem erfolgreichen Setup verbindest Du Dich via ssh auf den Server.

Zum Abschluss sind noch die Dateiberechtigungen für die linuxmuster Log-Dateien anzupassen.

Setze die Berechtigungen nun mit folgendem Befehl als Benutzer root:

```
chmod 600 /var/log/linuxmuster/setup.*.log
```

Lasse Dir den Inhalt des Verzeichnisses danach ausgeben und kontrollieren, ob Besitzer und Gruppe root sind und der Benutzer root lesen und schreiben darf.

```
ls -alh /var/log/linuxmuster/
```

Der Inhalt des Verzeichnisses sollte sich wie folgt darstellen:

```
root@server:~# ls -alh /var/log/linuxmuster/
total 308K
drwxr-xr-x  3 root  root  4,0K Dez 28 12:12 .
drwxrwxr-x 14 root  syslog 4,0K Dez 23 19:02 ..
drwxr-xr-x  2 nobody root  4,0K Dez 28 17:38 linbo
-rw-----  1 root  root   632 Dez 28 12:12 setup.add-server.log
-rw-----  1 root  root   49K Dez 28 12:14 setup.final.log
-rw-----  1 root  root  1,1K Dez 28 12:12 setup.firewall.log
-rw-----  1 root  root   316 Dez 28 12:10 setup.fstab.log
-rw-----  1 root  root  1,3K Dez 28 12:10 setup.ini.log
-rw-----  1 root  root  3,1K Dez 28 12:11 setup.linbo.log
-rw-----  1 root  root   11K Dez 28 12:14 setup.log
-rw-----  1 root  root   14K Dez 28 12:10 setup.samba-provisioning.log
-rw-----  1 root  root 165K Dez 28 12:12 setup.samba-users.log
-rw-----  1 root  root  7,5K Dez 28 12:10 setup.ssh.log
-rw-----  1 root  root   10K Dez 28 12:10 setup.ssl.log
-rw-----  1 root  root  6,9K Dez 28 12:10 setup.templates.log
root@server:~#
```

Abb. 200: Liste den Inhalt des Verzeichnisses auf

4.8.4 OPNsense® Unbound DNS anpassen

Das linuxmuster-setup richtet in der OPNsense® als voreingestellte DNS-Server diejenigen des DNS0.EU - Projekts ein. Dies sind europäische öffentliche DNS-Server, die darauf zielen, bösartige Domains zu blocken, Ende-zu-Ende Verschlüsselung zu gewährleisten und gefährdende Inhalte zu filtern (<https://www.dns0.eu/de>).

Nach der Installation muss im Unbound DNS-Resolver der OPNsense diese Voreinstellung noch aktiviert werden. Die DNS-Einstellungen der OPNsense kannst Du unter **System -> Einstellungen -> Allgemein** kontrollieren.

Zur Aktivierung gehe auf **Dienste -> Unbound DNS -> Query Forwarding**.

Setze den Haken für **Use System Nameservers**, dort siehst Du dann die in obiger Abb. dargestellten DNS-Einträge. Klicke zur Aktivierung auf **Anwenden**.

Mit sog. Overrides können im Unbound DNS genutzt werden, um die DNS-Ergebnisse in gewünschter Form anzupassen oder aber spezielle DNS Einträge bereitzustellen. Weitergehende Informationen findest Du hier: <https://docs.opnsense.org/manual/unbound.html>

Setze die Ersteinrichtung fort, indem Du

Benutzeraufnahme mit der Schulkonsole und *Rechneraufnahme* aufrufst.

Alternativ: Wenn Du eine Migration durchführen willst, geht es weiter mit

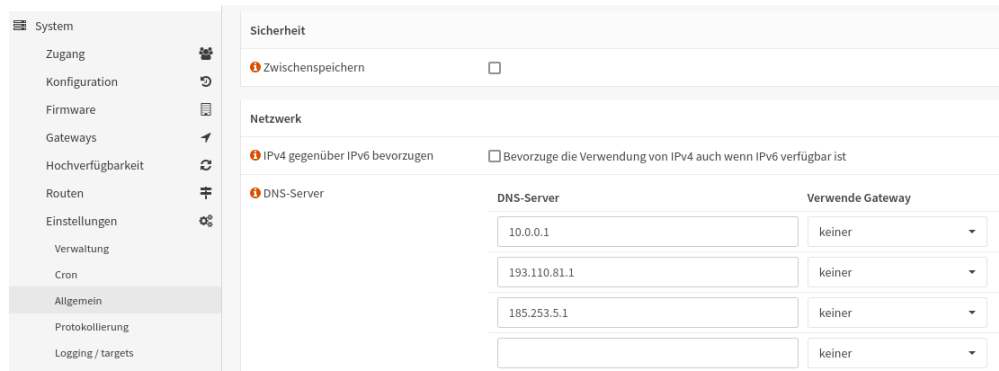


Abb. 201: DNS-Einträge

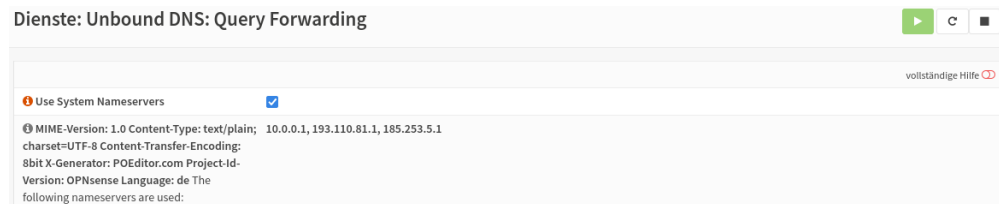


Abb. 202: Unbound-DNS: Query Forwarding

Migration auf linuxmuster 7.2

4.9 Setup im Terminal

Autor des Abschnitts: @cweikl, @MachtDochNix

Melde Dich als Benutzer **root** mit dem Passwort **Muster!** auf dem Server an.

Für diese Anmeldung kannst Du die xterm.js Konsole von Proxmox verwenden, wenn Du unserer Anleitung gefolgt bist. Alternativ kannst Du Dich via ssh von einem anderen Rechner mit dem Server verbinden, wenn er sich im gleichen Netzwerksegment befindet.

Im Terminal wirst Du mit dem Erstbildschirm von linuxmuster.net v7.2 begrüßt.

Das Setup wird über den Befehl **linuxmuster-setup** gestartet.

Erfolgt der Aufruf direkt mittels **linuxmuster-setup** müssen mindestens folgende Setup-Parameter als Kommandozeilenparameter übergeben werden (in einer Zeile) - die angegebene Werte nach dem Gleichheitszeichen sind selbstverständlich nur Beispielwerte:

```
linuxmuster-setup --location="Bad Tuxhausen" --schoolname="Linus-Benedict-Gesamtschule" -
↪ --country=de --state=SH
```

Weitere Parameter können auf der Kommandozeile angegeben werden. Werden aber auch in einem Dialogsystem abgefragt. Um alle Parameter zu sehen, verwende ...

```
linuxmuster-setup --help
```

Die dazugehörige Ausgabe:

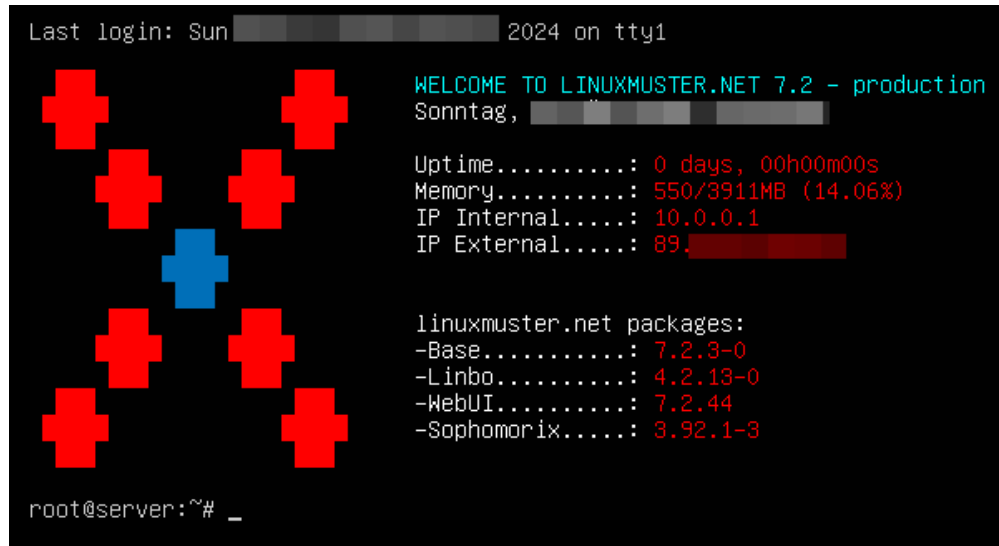


Abb. 203: Welcome to lmn.net

```
Usage: linuxmuster-setup [options]
[options] may be:
-n <hostname>,    --servername=<hostname>    : Set server hostname.
-d <domainname>,  --domainname=<domainname>    : Set domainname.
-r <dhcprange>,   --dhcprange=<dhcprange>    : Set dhcp range.
-a <adminpw>,     --adminpw=<adminpw>         : Set admin password.
-e <schoolname>,  --schoolname=<schoolname>       : Set school name.
-l <location>,    --location=<location>       : Set school location.
-z <country>,     --country=<country>        : Set school country.
-v <state>,       --state=<state>            : Set school state.
-c <file>,        --config=<file>            : path to ini file with setup values
-u,              --unattended               : unattended mode, do not ask questions
-s,              --skip-fw                  : skip firewall setup per ssh
-h,              --help                     : print this help
```

Alternativ kannst Du eine Konfigurationsdatei mit dem Parameter `--config` übergeben.

Willst Du diese Möglichkeit nutzen, lege eine `config.txt` mittels des nächsten Befehls an:

```
echo -e "[setup] \nservername = \ndomainname = \ndhcprrange = \nschoolname = \nlocation = \n\ncountry = \nstate = \nskipfw = False" > ~/config.txt
```

Diese Datei musst Du noch mit Deinen Angaben füllen. Hier beispielhaft mit dem Editor nano gezeigt

```
nano ~/config.txt
```

Hast Du diese Textdatei mit deinen Einträgen gespeichert [Strg]+[X] -> [Y] -> [Enter], kannst Du das Setup mit folgendem Befehl aufrufen:

```
linuxmuster-setup --config /root/config.txt
```

Nach dessen Aufruf, erscheinen in der Konsole nach und nach nochmals relevante Parameter. Hattest Du diese bereits festgelegt, so siehst Du Deine Werte. Bei nicht festgelegten, siehst Du die standardmäßig vorbelegten Werte. Prüfe alle Parameter und passe deren Werte gegebenenfalls an.

```

GNU nano 2.9.3 /root/config.txt Modified

[setup]
servername = server
domainname = lbgs.linuxmuster.lan
dhcprange = 10.0.0.100 10.0.0.200
schoolname = Linux-Benedict-Gesamtschule
location = Bad Tuxhausen
country = de
state = Schleswig-Holstein
skipfw = False

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line

```

Abb. 204: Editor Nano: config.txt

Klicke jeweils auf < OK >, um zum nächsten Schritt zu gelangen.

Danach gelangst Du zur Angabe der sogenannten Domain. Beachte bei dessen Festlegung u.g. Hinweise zum FQDN.

Hinweis: Der Domain name spielt eine besondere Rolle für das Setup.

Besonders, wenn eine Adresse verwendet werden soll, die intern und extern identisch sein soll, sodass mit dem FQDN intern und extern gearbeitet wird. Um Dir das zu verdeutlichen, zeigen wir das an zwei Beispielen:

- **meineschule.de**
- **linuxmuster.lan**

Die einzelnen Teile des Domainnamens werden durch einen einzelnen Punkt getrennt.

Die beiden rechten Teile **de** beziehungsweise **lan** stellen die sogenannte Top-Level-Domain (TLD) dar.

Die TLD **lan** wird nicht extern verwendet, sondern ist nur für den internen Gebrauch sinnvoll.

Die TLD **de** wird extern genutzt.

Hat Deine Schule die de-Domain **meineschule.de** registriert, dann musst Du hier eine Subdomain angeben, da **meineschule** zugleich die sogenannten Samba-Domain darstellt.

Wie aufgezeigt wird aus dem ganz linken Teil die Samba-Domain gebildet. Für diese gibt es definativ einige Einschränkungen:

- Es dürfen maximal 15 Zeichen verwendet werden.
- Es werden nur englische Kleinbuchstaben a bis z akzeptiert.

Richtig: gshoenningen (12 Zeichen, keine Umlaute und Satzzeichen etc.)

Falsch: GSO-Heinrich-Böll-Hönningen (26 Zeichen, Großbuchstaben, Umlaute, Bindestriche)

Weitergehende Informationen findest du hier: https://wiki.samba.org/index.php/Active_Directory_Naming_FAQ

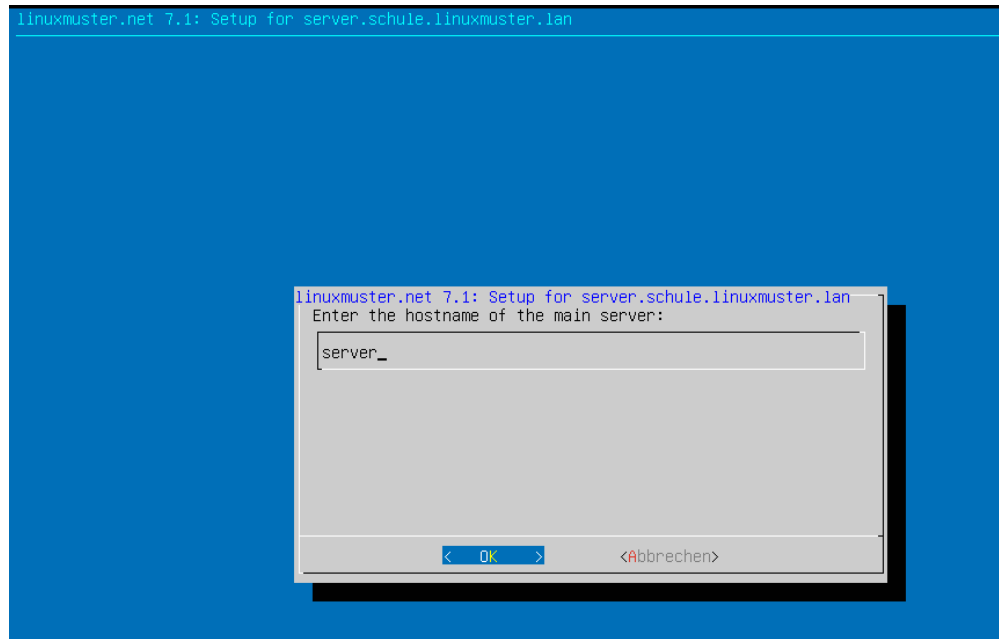


Abb. 205: Terminal Setup Hostname

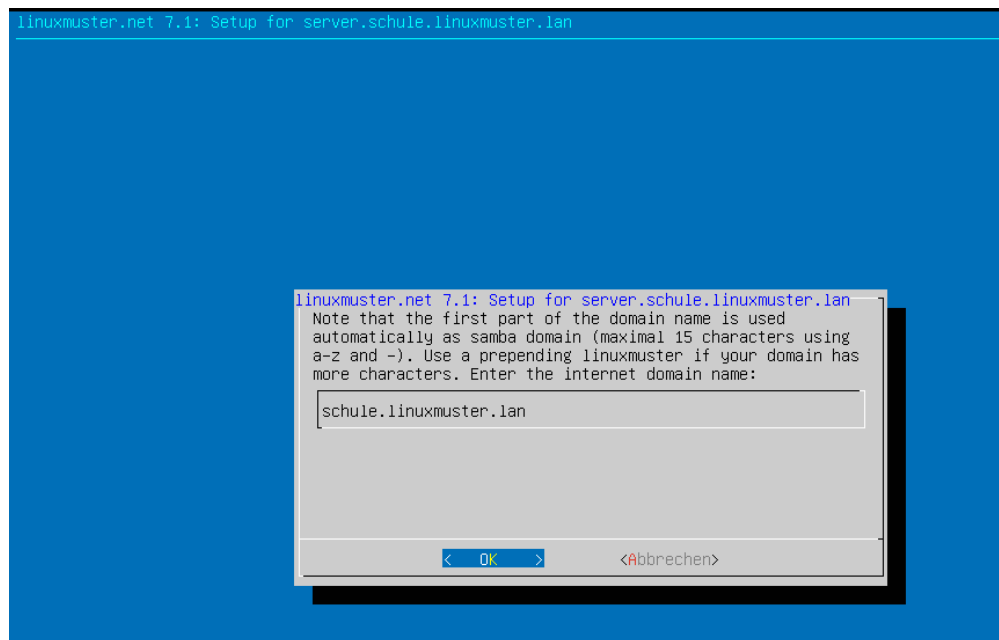


Abb. 206: Terminal Setup FQDN

Bestätige Deine Eingabe mit < OK >.

Es erscheint der IP-Adressbereich, der für die Rechneraufnahme mit Linbo reserviert wird. In der Abb. ist dies der Bereich 10.0.0.100 bis 10.0.0.200.

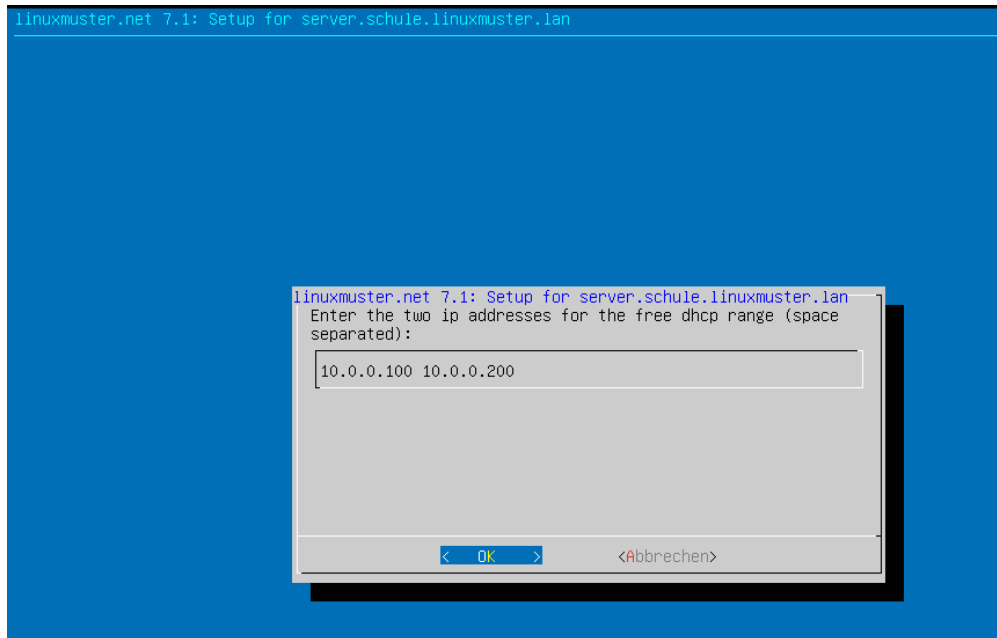


Abb. 207: Terminal Setup: DHCP Bereich festlegen

Wechsele mit < OK > zur nächsten Eingabemaske.

Hier setzt Du ein neues Administrations-Kennwort. Dieses wird zugleich das neue Kennwort aller administrativen Benutzer, so auch vom global-admin in der Schulkonsole.

Hinweis: Passwortbeschränkungen: Valid characters are: a-z A-Z 0-9 ?!\$+-@#%&*()[]{} }

Hinweis:

- **Das beim Setup eingegebene Admin-Passwort wird für folgende administrativen User gesetzt:**
 - root auf dem Server
 - root auf der Firewall
 - global-admin (AD)
 - pgmadmin (AD)
 - linbo (/etc/rsyncd.secrets)
- Es sollten die Passwörter der o.g. User nach dem Setup geändert werden, sodass jeder User ein eigenes Passwort hat.
- Achte darauf, dass Dein Passwort den Komplexitätsanforderungen entspricht, die mit samba4 aktiviert sind: Mind. 7 Zeichen, Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen (zulässige Sonderzeichen wie oben genannt)

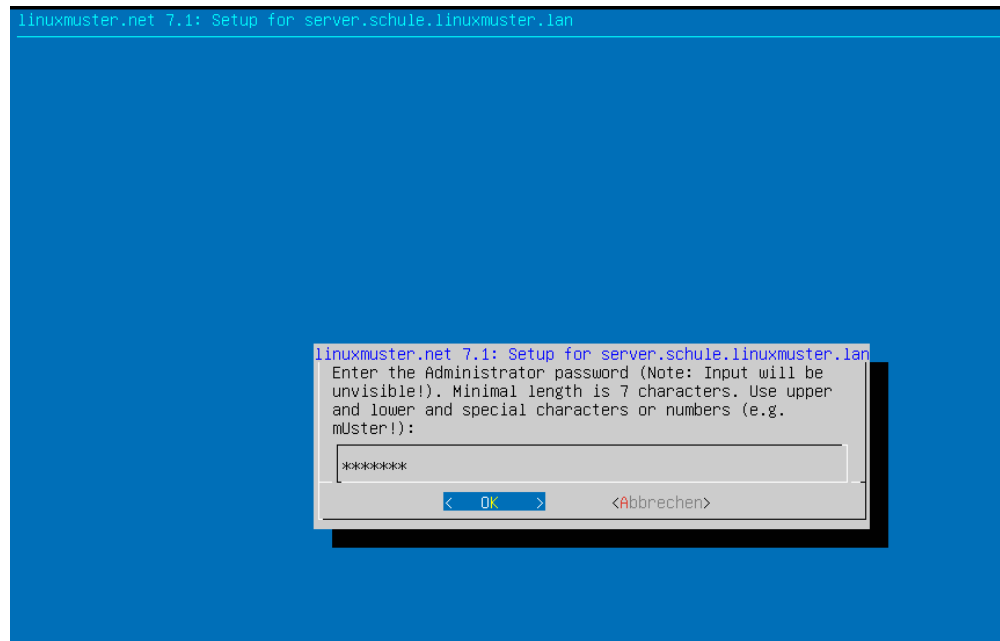


Abb. 208: Terminal Setup: Global-admin und root Kennwort festlegen

- In der Datei `/etc/linuxmuster/sophomorix/default/school/school.conf` sind die Kennwortlängen für Schüler (Standard: 10 Zeichen) und Lehrer (12 Zeichen) angegeben.
- Die Grundeinstellungen für Kennwörter in samba4 kannst Du Dir auf dem Server in der Konsole mit `samba-tool domain passwordsettings show` anzeigen lassen.

Gebe das Kennwort ein und klicke auf `< OK >`.

Bestätige dieses Kennwort und klicke auf `< OK >`.

Danach wird das Setup gestartet. Es dauert einige Zeit, bis alle erforderlichen Dienste und die OPNsense eingerichtet wurden.

Nach Abschluss des Setups siehst Du im Terminal, dass das Setup beendet wurde.

Danach muss noch der Dienst für die WebUI/Schulkonsole oder der Server neu gestartet werden.

```
# systemctl restart linuxmuster-webui.service
```

alternativ

```
# reboot
```

Das erste Verfahren hat den Vorteil, dass Du nicht die Zeit des Neustarts abwarten, Dich erneut verbinden und anmelden musst.

Hinweis: Starte nach dem erfolgreichen Setup ebenfalls die OPNsense | reg | neu.

Nach abgeschlossenem Setup und dem Neustart des Dienstes `linuxmuster-webui` bzw. eventuellen Neustart des Servers, kannst Du Dich mit einem PC via Browser an der Schulkonsole von `linuxmuster.net v7.2` anmelden.

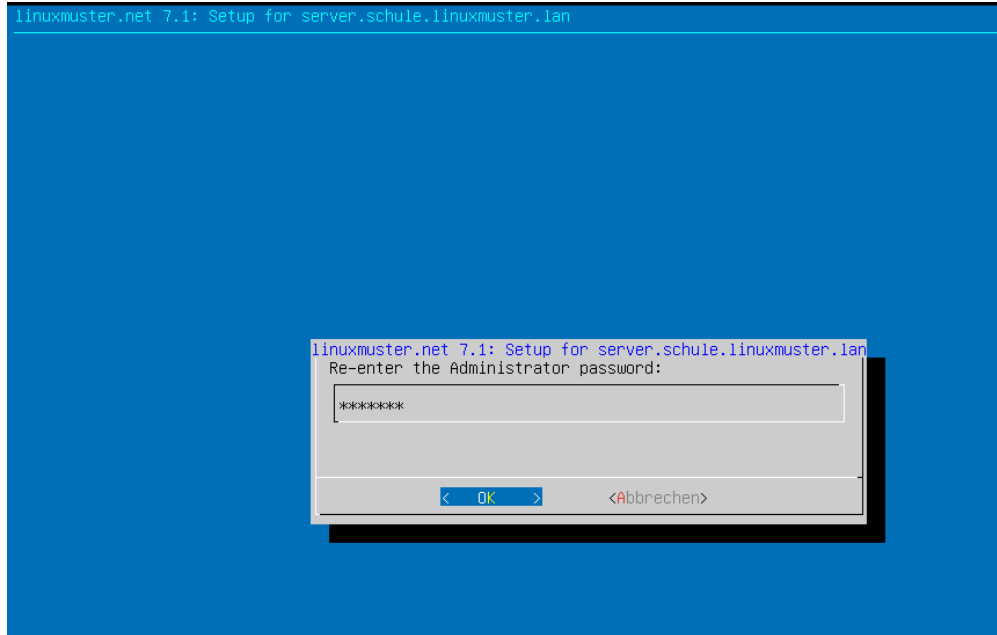


Abb. 209: Terminal Setup: Kennwort bestätigen

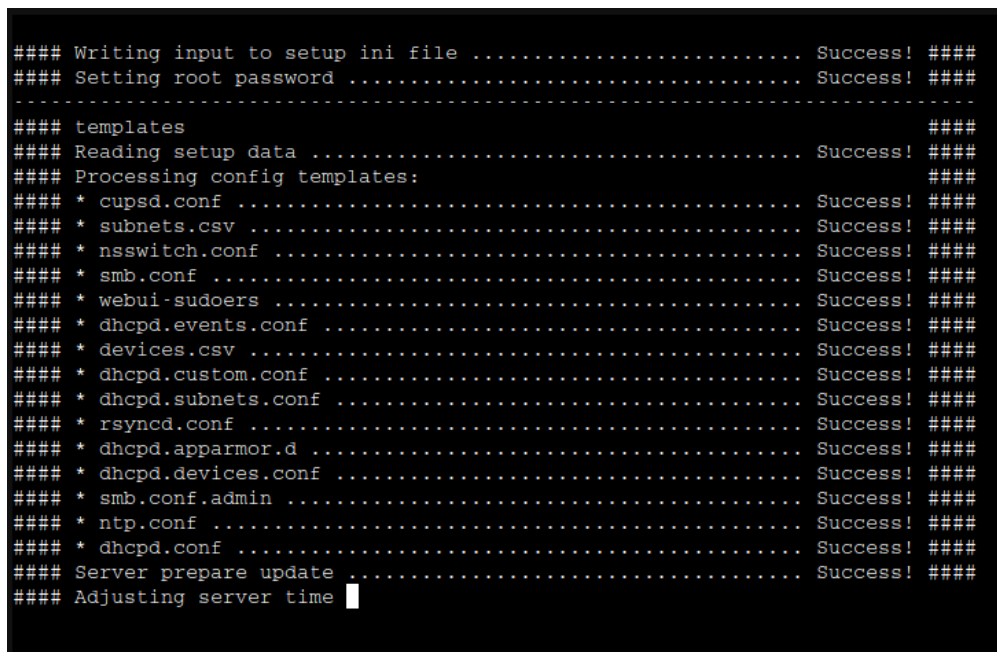


Abb. 210: Terminal Setup: Fortschritt des Setups

```

#### * Saving api credentials ..... Success! ####
#### Uploading firewall configuration: ####
#### put 10.0.0.254 /var/cache/linuxmuster/opnsense.xml /tmp/opnsense.xml ####
#### * Upload finished successfully. ####
#### Creating web proxy sso auth config file ####
#### put 10.0.0.254 /tmp/pre-auth.conf /tmp/pre-auth.conf ####
#### Installing extensions and rebooting firewall ####
#### put 10.0.0.254 /usr/share/linuxmuster/firewall/opnsense/fwsetup.sh /tmp/fwsetup.sh ####
#### Executing ssh command on 10.0.0.254: ####
#### * -> "chmod +x /tmp/fwsetup.sh" ####
#### * SSH connection successfully established. ####
#### * SSH command execution finished successfully. ####
#### Executing ssh command on 10.0.0.254: ####
#### * -> "/tmp/fwsetup.sh" ####
#### * SSH connection successfully established. ####
#### * SSH command execution finished successfully. ####
-----
#### webui ####
* Create Webui Configuration
Bundle certificate for webui
Run Sophomorix-UI to add permissions
* Create Webui Upload Folder
ACL set on webuiUpload with WORKGROUP SCHULE
* WebUI Setup Success!
-----
#### final ####
#### Reading setup data ..... Success! ####
#### Restarting apparmor service ..... Success! ####
#### Writing school name to school.conf ..... Success! ####
#### Starting device import ..... Success! ####
#### Waiting for opnsense to come up ####
#### Executing ssh command on 10.0.0.254: ####
#### * -> "exit" ####
#### * SSH connection successfully established. ####
#### Starting subnets import ..... Success! ####
#### Creating web proxy sso keytab ..... Success! ####
#### Removing admin password from setup.ini ..... Success! ####
-----
#### linuxmuster-setup finished at 2024-02-20 18:22:38 ####
-----
root@server:~#

```

Abb. 211: Terminal Setup: Abschluss des Setups

Nachdem sich Dein Client eine IP-Adresse via DHCP aus dem Adressbereich für die Rechneraufnahme geholt hat, ist dieses aber nicht möglich. Dessen Adressen sind aus sicherheitstechnischen Erwägungen nur auf das allernötigste beschränkt.

Daher muss sich der Rechner in einem besonderen LAN-Bereich befinden, etwa mit der IPv4-Adresse 10.0.0.10/16. Diese IP-Adresse musst Du manuell in Deinem Admin-PC einrichten.

4.9.1 Anmeldung an der Schulkonsole als global-admin

Öffne die URL `https://10.0.0.1` mit dem Admin-PC. Es wurde beim Setup ein self-signed certificate erstellt, sodass Du dieses beim erstmaligen Aufruf mit dem Browser akzeptieren musst.



Abb. 212: SSL: Mögliches Sicherheitsrisiko - Erweitert

Der Browser zeigt Dir den Warnhinweis an. Klicke auf **Erweitert**

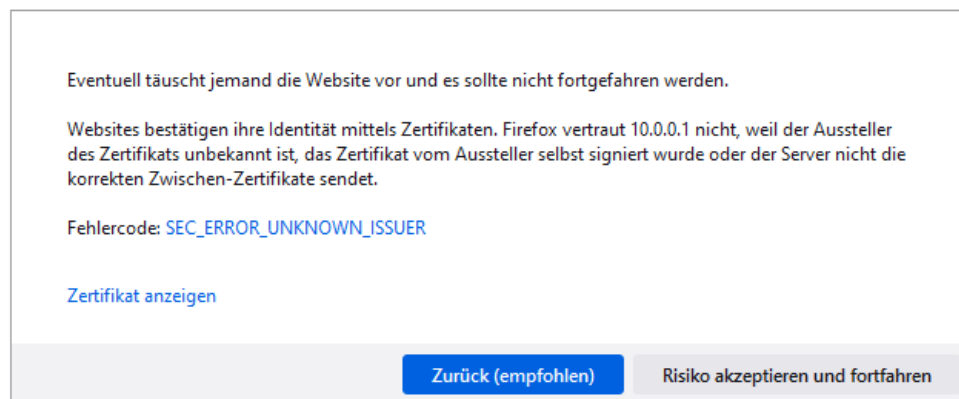


Abb. 213: SSL: Risiko akzeptieren und fortfahren

Es erscheint auf der gleichen Seite unten ein weiterer Eintrag. Bestätige diesen, indem Du den Button Risiko akzeptieren und fortfahren auswählst.

Danach kommst Du zur Anmeldeseite der WebUI/Schulkonsole. Melde Dich nun als Benutzer global-admin an und nutze das während des Setups festgelegte Kennwort.



Abb. 214: Login global-admin

Nach erfolgreicher Anmeldung gelangst Du zur Hauptseite der Schulkonsole.

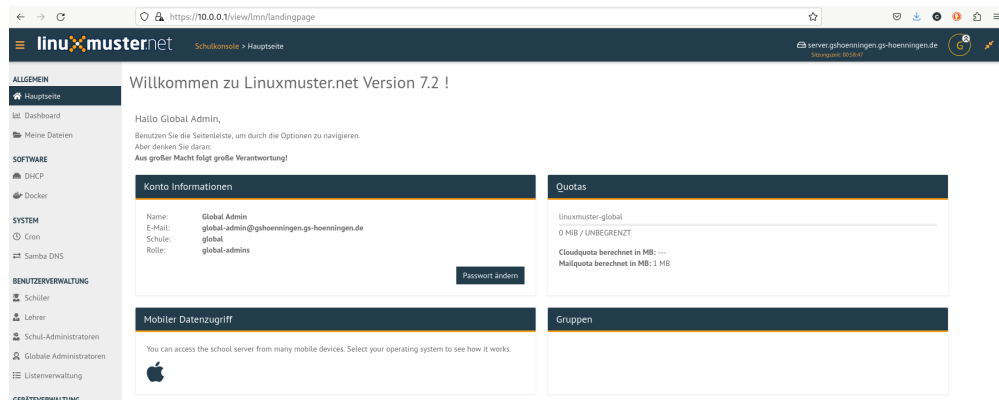


Abb. 215: Hauptseite der Schulkonsole

4.9.2 Berechtigungen der Log-Dateien anpassen

Nach dem erfolgreichen Setup verbindest Du Dich via ssh auf den Server.

Zum Abschluss sind noch die Dateiberechtigung für die linuxmuster Log-Dateien anzupassen.

Setze die Berechtigungen nun mit folgendem Befehl als Benutzer root:

```
chmod 600 /var/log/linuxmuster/setup.*.log
```

Lasse Dir den Inhalt des Verzeichnisses danach ausgeben und kontrollieren, ob Besitzer und Gruppe root sind und diese lesen und schreiben dürfen.

```
ls -alh /var/log/linuxmuster/
```

Der Inhalt des Verzeichnisses sollte sich wie folgt darstellen:

```
root@server:~# ls -alh /var/log/linuxmuster/
total 308K
drwxr-xr-x  3 root  root  4,0K Dez 28 12:12 .
drwxrwxr-x 14 root  syslog 4,0K Dez 23 19:02 ..
drwxr-xr-x  2 nobody root  4,0K Dez 28 17:38 linbo
-rw-----  1 root  root   632 Dez 28 12:12 setup.add-server.log
-rw-----  1 root  root   49K Dez 28 12:14 setup.final.log
-rw-----  1 root  root   1,1K Dez 28 12:12 setup.firewall.log
-rw-----  1 root  root    316 Dez 28 12:10 setup.fstab.log
-rw-----  1 root  root   1,3K Dez 28 12:10 setup.ini.log
-rw-----  1 root  root   3,1K Dez 28 12:11 setup.linbo.log
-rw-----  1 root  root    11K Dez 28 12:14 setup.log
-rw-----  1 root  root   14K Dez 28 12:10 setup.samba-provisioning.log
-rw-----  1 root  root  165K Dez 28 12:12 setup.samba-users.log
-rw-----  1 root  root   7,5K Dez 28 12:10 setup.ssh.log
-rw-----  1 root  root   10K Dez 28 12:10 setup.ssl.log
-rw-----  1 root  root   6,9K Dez 28 12:10 setup.templates.log
root@server:~#
```

Abb. 216: Liste die Berechtigungen der Dateien auf

4.9.3 OPNsense® Unbound DNS anpassen

Das linuxmuster-setup richtet in der OPNsense® als voreingestellte DNS-Server diejenigen des DNS0.EU - Projekts ein. Dies sind europäische öffentliche DNS-Server, die darauf zielen, bösartige Domains zu blocken, Ende-zu-Ende Verschlüsselung zu gewährleisten und gefährdende Inhalte zu filtern (<https://www.dns0.eu/de>).

Nach der Installation muss im Unbound DNS-Resolver der OPNsense diese Voreinstellung ggf. noch aktiviert werden. Die DNS-Einstellungen der OPNsense kannst Du unter System -> Einstellungen -> Allgemein kontrollieren.

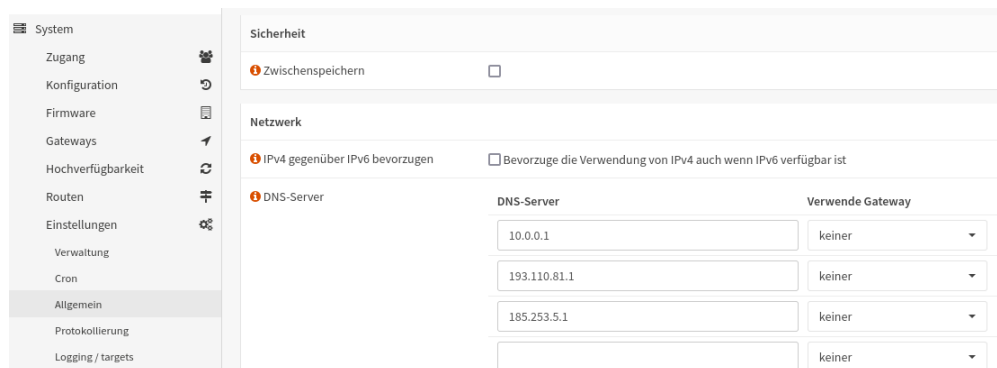


Abb. 217: DNS-Einträge

Zur Aktivierung gehe auf Dienste -> Unbound DNS -> Query Forwarding.

Setze den Haken für Use System Nameservers, dort siehst Du dann die in obiger Abb. dargestellten DNS-Einträge. Klicke zur Aktivierung auf Anwenden.

Mit sog. Overrides können im Unbound DNS genutzt werden, um die DNS-Ergebnisse in gewünschter Form anzupassen oder aber spezielle DNS Einträge bereitzustellen. Weitergehende Informationen findest Du hier: <https://docs.opnsense.org/manual/unbound.html>

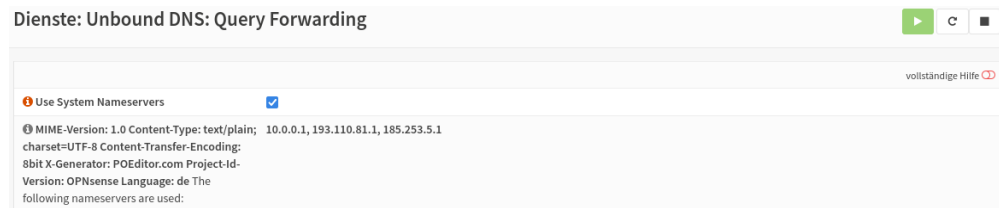


Abb. 218: Unbound-DNS: Query Forwarding

Setze die Ersteinrichtung fort, indem Du *Benutzeraufnahme mit der Schulkonsole* und *Rechneraufnahme* aufrufst.

Alternativ: Willst Du eine Migration durchführen, geht es weiter mit: *Migration auf linuxmuster 7.2*

4.10 Benutzeraufnahme mit der Schulkonsole

Autor des Abschnitts: @Tobias, @cweikl

In einer Schule müssen meist mehrere hundert bis einige tausend Schüler als Benutzer angelegt werden. Die Schulkonsole (WebUI) erlaubt das Einlesen aller Schülerdaten aus einer Text-Datei, die z.B. aus dem Schulverwaltungsprogramm der Schule bezogen wurde. Anschließend werden

- Konten aller Schüler dieser Liste, die im System noch nicht vorhanden sind, angelegt,
- solche mit einer neuen Klasse versetzt und
- Konten nicht mehr aufgeführter Schüler schrittweise aus dem System entfernt.

In diesen Abschnitten werden beispielhaft ein Lehrer händisch angelegt und per Datei-Import einige Schüler aufgenommen. Melde Dich dafür an der Schulkonsole als `global-admin` an.

4.10.1 Zeichenkodierung wählen

Die Zeichencodierung für die zu importierenden CSV-Benutzerdateien kann in der WebUI festgelegt werden. Der Standard ist eine Auto-Erkennung der Codierung festgelegt. Ist die Kodierung der Eingabedatei bekannt, so kann diese auch direkt vorgegeben werden.

Klicke dazu auf das Menü **Einstellungen** --> **Schuleinstellungen**.

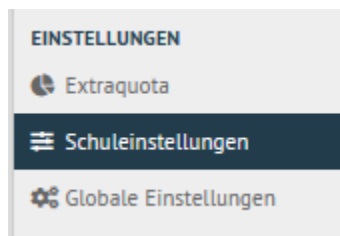


Abb. 219: Schuleinstellungen wählen

Klicke rechts auf die Reiterkarte **Listenimport**, unterhalb von **Zeichencodierung** ist im Beispiel UTF-8 erkannt worden.

Klicke auf das Drop-down Menü für die Listenkodierung und wähle die gewünschte Kodierung aus. Schließe die Eingabe mit „Speichern“ ab.

Für den Listenimport gibt es drei verschiedene CSV-Dateien:

[Allgemein](#)
[Listenimport](#)
[Kontingent](#)
[Druck-Daten](#)
[Benutzerdefinierte Felder](#)
[Subnetze](#)

Benutzername und Passwörter

	Schüler	Lehrer	Extrасhüler
Nachname und Vorname im Benutzernamen umkehren	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Nachname Zeichen	6	0	6
Vornamen Zeichen	2	0	2
Passwortlänge	10	12	10
Zufallspasswort	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Tage bis zum Deaktivieren nach Austreten	30	60	40
Tage bis zum endgültigen Löschen	60	90	80
Ersetze Schrägstrich(/) in Klassenname durch Bindestrich(-)	<input checked="" type="checkbox"/>		

Zeichenkodierung

	students.csv Kodierung	teachers.csv Kodierung	extrastudents.csv Kodierung
Listenkodierung	auto	auto	auto
Erkannter Zeichensatz	utf-8	utf-8	utf-8

Benutzerdefinierte Filter

[Speichern](#)
[↺](#)

Abb. 220: Listenimport und Zeichenkodierung

1. `students.csv`: Liste für den Schülerimport
2. `teachers.csv`: Liste für den Lehrerimport
3. `extrastudents.csv`: Liste für den Import von Benutzern für z.B. Fortbildungen, Kurse etc.

Diese CSV-Dateien folgen nachstehendem Aufbau:

```
Klasse;Nachname;Vornamen;Geburtsdatum;ID
```

Trennzeichen ist das Semikolon (;). Klasse ist nur für Schüler anzugeben. Die ID kann nachgestellt sein und stammt i.d.R. aus den Schulverwaltungsprogrammen. Auf diese Weise wird sichergestellt, dass für identische Benutzer immer nur ein Zugang angelegt wird.

4.10.2 Lehrer importieren

Wähle das Menü **Benutzerverwaltung** --> **Listenverwaltung**.

Wähle rechts oben die Reiterkarte **Lehrer**.

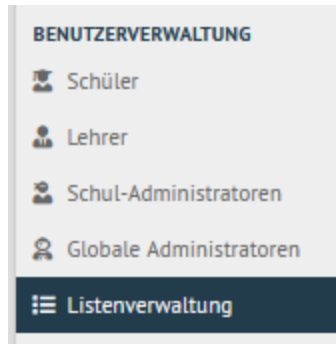


Abb. 221: Menüeintrag Listenverwaltung

Einzelnen Lehrer hinzufügen

Klicke auf den Button + Lehrer hinzufügen. Es wird eine leere Zeile hinzugefügt, die nun mit den angezeigten Daten zu füllen ist.

Nachname	Vorname	Geburtsdatum	Benutzername
Bo	Hans	01.01.1980	bo.hans

Abb. 222: Lehrer hinzufügen

Hinweis: Wie dargestellt führt der Benutzername bo.hans zu einem Importfehler! Im Benutzernamen darf kein Punkt enthalten sein. vornamenachname oder nur nachname wären hingegen zulässige Benutzernamen.

Achtung: Der angegebene Benutzername darf keine Leerzeichen, Punkte und Großbuchstaben enthalten. Anderfalls kommt es bei Speichern & Prüfen zu einer Fehlermeldung

Mit + Lehrer hinzufügen können auf diese Art und Weise weitere Lehrer einzeln aufgenommen werden. Klicke nach dem Eintragen aller der Daten unten auf den Button Speichern & Prüfen.

Es erscheint ein Fenster, in dem Du siehst, wie mit den angegebenen Benutzerdaten verfahren wird.

In o.g. Fenster ist zu sehen, dass ein neuer Lehrer hinzugefügt wird. Mit dem Button Übernehmen werden die dargestellten Aktionen ausgeführt (hinzufügen, aktualisieren, löschen).

Der Importdialog zeigt den Fortschritt an und meldet zurück, wenn die Aufnahme abgeschlossen wurde.

Bestätige dies mit dem Button Schliessen.

Die neue oder geänderten Benutzer findest Du nun im Menü Benutzerverwaltung --> Lehrer. Hier können deren Kontoinformationen abgerufen und z.B. Erstpasswörter (zurück-)gesetzt werden.

Prüfergebnis

Übersicht

Hinzuzufügen

i Benutzer werden hinzugefügt: 1

teachers

bo

Bo Hans

teacher

default-school

i Benutzer werden aktualisiert: 0**i** Benutzer werden gelöscht: 0☒ Neue Benutzer hinzufügen

ÜBERNEHMEN

ABBRECHEN

Abb. 223: Prüfergebnis für den Import der Nutzerdaten

Änderungen werden übernommen

```
2) Line 9: SMB::@@SCHOOL@@/@@TEACHERCLASS@@/@@USER@@/@@TRANSFER_DIR_HOME@@/:root::root::0755::teacher.transfer.ntacl::
OK (0): /usr/bin/smbclient -U administrator%***** //server/default-school -c 'mkdir "teachers/becker/transfer"'
OK (0): smbcacls-NTACL on //server/default-school teachers/becker/transfer
DONE with 2) Line 9: SMB::@@SCHOOL@@/@@TEACHERCLASS@@/@@USER@@/@@TRANSFER_DIR_HOME@@/:root::root::0755::teacher.transfer.ntacl:
#### Repairing from file: repdir.teacher_home (end) ####
#### Creating user 2: becker (end) ####

#### Running hook scripts ADD_HOOK_DIR: ####
#### Removing lock in /var/lib/sophomnix/lock/sophomnix.lock ####
#### /usr/sbin/sophomnix-add terminated regularly ####
Calling console printout
LOG : /usr/sbin/sophomnix-add terminated regularly
2 users added
```

Optionen

☒ Autoscroll

SCHLIESSEN

Abb. 224: Import fertiggestellt

Schüler **Lehrer** Extra-Schüler

Filter 🔍 ⌵ Felder ⌵ Zeilen ⌵

Nachname	Vorname	Geburtsdatum	Benutzername	
Bo	Hans	01.01.1980	bo	🗑
Becker	Miriam	01.01.1981	becker	🗑

+ Lehrer hinzufügen

Abb. 225: Benutzerverwaltung: Lehrer

4.10.3 Schüler importieren

Schüler können analog zu Lehrern einzeln hinzugefügt werden.

Alternativ können **alle** Schüler (alte wie neue) importiert werden. Wähle im Menü **Benutzerverwaltung** --> / **Listenverwaltung** --> **Schüler** (es erscheint automatisch die Schülerliste).

Mit der Schaltfläche unterhalb der dargestellten Schüler CSV kannst Du verschiedene Möglichkeiten ansteuern, eine CSV-Datei zu erstellen, diese zu bearbeiten oder eine neue bereitzustellen.

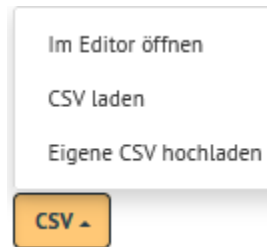


Abb. 226: Eigene CSV hochladen

Eine zu importierende Datei sollte folgende Daten aufweisen:

Klassenbezeichnung;Nachname;Vorname;Geburtsdatum;ID (optional aus einem
 ↳ Schulverwaltungsprogramm)

Nachstehende Daten könnten lokal erstellt, als CSV-Datei mit der UTF-8 Codierung abgespeichert und danach mit o.g. Option **Eigene CSV hochladen** importiert werden.

```
10A;Testuser;Heinz;1.1.2006;1234
13a;Musterfrau;Tanja;2.1.2003;1235
5b;Hausmann;Hans;3.1.2016;1236
```

Achtung: Die Datei muss alle alten und neuen Schüler enthalten, sonst werden alle fehlenden Schüler zur Entfernung (Versetzung aus der Schule) vorgemerkt. Siehe auch [Fehlerkorrektur](#) unten. Die Dateinamen sind ebenso eindeutig vorgegeben. Für Schüler ist die Datei students.csv zu nennen.

Mit der Option **Eigene CSV hochladen** kann eine so formatierte Datei nun hochgeladen werden. Die Schüler der zu importierenden Datei sind dann in der Listenverwaltung unter den Schülern zu sehen.

Schüler Lehrer Extra-Schüler				
Filter				<div> <div>🔍</div> <div>*** Felder</div> <div>≡ Zeilen</div> </div>
Class	Last Name	First Name	Birthday	
10A	Testuser	Heinz	1.1.2006	🗑
13a	Musterfrau	Tanja	2.1.2003	🗑
5b	Hausmann	Hans	3.1.2015	🗑
+ Schüler hinzufügen				

Abb. 227: Schüler hinzufügen

Mit Speichern werden eventuelle Konsistenzfehler überprüft. Die Schaltfläche **SPEICHERN & PRÜFEN** zeigt nun an, wieviele Schüler bei **ÜBERNEHMEN** ins System übernommen, versetzt (aktualisiert) oder gelöscht werden.

Prüfergebnis

Übersicht

Hinzuzufügen

1 Benutzer werden hinzugefügt: 3

10a	testushe	Testuser Heinz	student	default-school
5b	hausmaha	Hausmann Hans	student	default-school
13a	musterta	Musterfrau Tanja	student	default-school

1 Benutzer werden aktualisiert: 0**1 Benutzer werden gelöscht: 0**☒ Neue Benutzer hinzufügen**ÜBERNEHMEN****ABBRECHEN**

Abb. 228: Überprüfung der zu importierenden Benutzer

Mit Klick auf den Button **Übernehmen** werden die dargestellten Aktionen ausgeführt. Der abgeschlossene Import ist im Fenster zu sehen:

Ab der erfolgreichen Übernahme können die Schüler unter dem Menüpunkt **Benutzerverwaltung** --> Schüler gefunden und deren Konten bearbeitet werden.

Änderungen werden übernommen

```

2) Line 9: SMB::@SCHOOL@/$directory_students/@ADMINCLASS@/@USER@/@TRANSFER_DIR_HOME@/:root::root::0755::student.transfe
OK (0): /usr/bin/smbclient -U administrator%***** //server/default-school -c "mkdir "students/5b/hausmaha/transfer""
OK (0): smbcacls-NTACL on //server/default-school students/5b/hausmaha/transfer
DONE with 2) Line 9: SMB::@SCHOOL@/$directory_students/@ADMINCLASS@/@USER@/@TRANSFER_DIR_HOME@/:root::root::0755::stud
#### Repairing from file: repdir.student_home (end) ####
#### Creating user 3: hausmaha (end) ####

#### Running hook scripts ADD_HOOK_DIR: ####
#### Removing lock in /var/lib/sophomox/lock/sophomox.lock ####
#### /usr/sbin/sophomox-add terminated regularly ####
Calling console printout
LOG : /usr/sbin/sophomox-add terminated regularly
3 users added

```

Optionen
☒ Autoscroll

SCHLIESSEN

Abb. 229: Benutzer importiert

4.10.4 Fehlerkorrektur

Hat man fehlerhafte Daten in das System eingepflegt und hat sie noch nicht importiert, lassen sich Schüler und Lehrerlisten aus einer Sicherung zurückholen. Der Knopf für die Sicherung ist rechts unten in der Listenverwaltung.

Hast Du z.B. bei der zuvor importierten CSV-Datei die IDs vergessen, kannst Du diese in der CSV-Datei ergänzen, diese erneut importieren. Es werden Dir dann die Änderungen angezeigt. In diesem Fall wird die uid auf die neu eingetragenen ID geändert.

Unter Listenverwaltung hast Du bei den jeweiligen Benutzern (Schüler, Lehrer, Extraschüler) unten rechts das Dropdown-Menü für die CSV-Dateien.

Klickst Du auf CSV --> Im Editor öffnen wird die `students.csv` auf dem Server geöffnet und Du kannst Änderungen vornehmen.

Eine ausführlichere Dokumentation zur Benutzerverwaltung findet sich im entsprechenden Abschnitt dieser Dokumentation.

4.11 Muster-Client aufsetzen

Autor des Abschnitts: @cweikl, @MachtDochNix

linuxmuster.net ermöglicht es, Clients mithilfe von LINBO automatisiert zu verwalten. Auf den Clients kann ein Betriebssystem oder es können mehrere Multi-Boot Betriebssysteme auf dem Client installiert, aktualisiert, ausgerollt und zurückgesetzt werden. Mithilfe von LINBO erfolgt so ein automatisches Ausrollen der Clients im Netzwerk, das Verteilen zusätzlich zu installierender Software oder die Wiederherstellung eines funktionierenden Clients in den Ausgangszustand z.B. nach einer Laborübung, in der die Clients gezielt umkonfiguriert wurde.

Die Nutzung von LINBO erfordert die Einrichtung eines Muster-Clients. Dies erfordert nachstehende drei Installationsschritte:

Hardwareklasse erstellen

Mittels der Hardwareklasse teilst Du LINBO mit, welche Konfiguration für die Geräte anzuwenden ist. Dies umfasst:

- Name der Hardwareklasse

Prüfergebnis

Übersicht

Zu versetzen

i Benutzer werden hinzugefügt: 0**i** Benutzer werden aktualisiert: 3

musterta	• Unid : --- --> 234112
hausmaha	• Unid : --- --> 234113
testushe	• Unid : --- --> 234111

i Benutzer werden gelöscht: 0☒ Benutzer versetzen

ÜBERNEHMEN

ABBRECHEN

Abb. 230: Benutzer aktualisiert

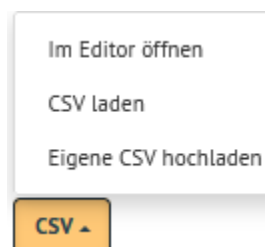


Abb. 231: Eigene CSV hochladen

/etc/linuxmuster/sophomorix/default-school/students.csv

Datei hier hin schieben um sie zu importieren

```
1 10A;Testuser;Heinz;1.1.2006;234111
2 13a;Musterfrau;Tanja;2.1.2003;234112
3 5b;Hausmann;Hans;3.1.2015;234113
4
```

SPEICHERN CSV HERUNTERLADEN ABBRECHEN

Abb. 232: CSV-Datei mit der WebUI im Browser editieren

- Allgemeine Informationen
 - IP des TFTP-Servers, der das Image vorhält.
 - Startoptionen des Clients
 - eventuell benötigte Kernel-Optionen für den Start-Vorgang
- Angaben zu der Partitionierung des Clients

Rechneraufnahme

Bei der Rechneraufnahme legst Du fest, welche Konfigurationen für jede einzelne Arbeitsstation gelten sollen. Das sind:

- Raum, in dem sich der Rechner befindet,
- Name des Rechners
- Name der Hardwareklasse, welcher der Rechner angehören soll,
- MAC-Adresse des Rechners
- IP-Adresse, die der Rechner erhalten soll,
- Art des Gerätes
- Aktivierung von LINBO

Wie Du aus den letzten beiden Punkten erkennen kannst, ist die Aktivierung von LINBO nicht für jedes Gerät zwingend notwendig. So benötigt z.B. ein Netzwerk-Drucker kein eigenes Image. Dieser benötigt nur eine IP und eine Raumzuordnung. Des Weiteren ist seine Aufnahme notwendig, damit er im Active Directory des Samba-Dienstes des linuxmuster.net Servers aufgenommen wird und somit dem System bekannt ist.

Es gibt drei Möglichkeiten die Rechneraufnahme durchzuführen. Diese findest Du im Kapitel *Rechneraufnahme* ausführlich beschrieben.

OS-Installation

Im letzten Schritt wird nun das eigentliche Betriebssystem auf dem Muster-Client erstellt, in die Domäne eingebunden und das endgültige Image auf den linuxmuster.net Server geschrieben. Da sich das Vorgehen je nach verwendetem System unterscheidet, gehen die Unterkapitel von *Betriebssysteme installieren* detailliert darauf ein.

4.11.1 Hardwareklasse (HWK) / Gruppe erstellen

Autor des Abschnitts: @cweikl, @MachtDochNix (pics)

Melde Dich als Benutzer `global-admin` an der Web-UI an.

Erstelle nun die Konfiguration für die neue Hardwareklasse. Klicke links im Menü auf den Eintrag *Geräteverwaltung* --> *Linbo4*.

Nun klickst Du unten links auf **+ERSTELLEN**.

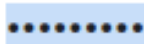
Es öffnet sich ein Kontextmenü. Du kannst entweder ein leere `start.conf` nutzen, oder ein bereits vordefiniertes Template für Dein gewünschtes Betriebssystem auswählen. Hierbei kannst Du Templates für ein oder mehrere Betriebssysteme mit oder ohne UEFI-BIOS auswählen und diese ggf. nach Deinen Vorstellungen anpassen.

Es öffnet sich ein Fenster, in dem Du die Namen der neuen Hardwareklasse angibst. Diesen wirst Du später benötigen, um Geräte dieser Hardwareklasse zuzuweisen.

Die Liste der angelegten Hardwareklassen kann dann - z.B. wie nachstehend dargestellt - aussehen (andere Namen für die HWK verwendet):



global-admin



Anmelden

Abb. 233: Anmeldung als Benutzer global-admin

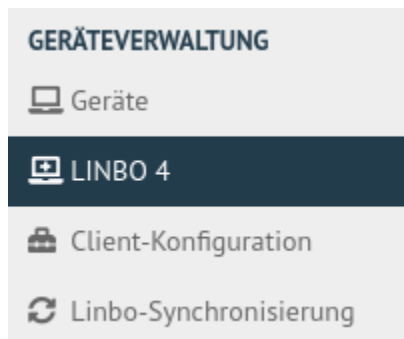


Abb. 234: Menü LINBO4



Abb. 235: Template für die start.conf auswählen

New name

my-ubuntu-22-04-lts-muster-client

OK

ABBRECHEN

Abb. 236: Namen für die neue Hardwareklasse festlegen







Gruppen		Abbilder
Gruppenname	Verwendete Images	Aktionen
win10efi	win10.qcow2	  
ubu20efi	ubuntu.qcow2	  

Abb. 237: Übersicht der Hardwareklassen / Gruppen

Du rufst nun die Einstellungen der zuvor angelegten Hardwareklasse auf, indem Du das Stift-Symbol rechts daneben aufrufst.

Es erscheint ein Fenster mit den Einstellungen der Hardwareklasse. Dort gibt es die Reiterkarten Allgemein und Partitionen.

Unter Allgemein legst Du die IP des Servers fest, gibst das Startverhalten und ggf. Kernel-Optionen (Linux) für den Boot bei besonderer Hardware an.

my-ubuntu-22-04-lts-muster-client

Allgemein Partitionen

TFTP Server 10.0.0.1 Administrator wegen Zeitlimit ausgeloggt 600

Systemtyp UEFI 64Bit Download Typ torrent

Startoptionen

- ☐ Beim Start partitionieren
- ☐ Beim Start formatieren
- ☐ Beim Start Cache aktualisieren
- ☐ Nur für diese Schule verfügbar (default-school)

Linbo GUI Anpassung

- ☐ Minimales Layout verwenden
- ☐ Clientdetails standardmäßig anzeigen

Sprache Hintergrundfarbe Die Farbe des Vordergrunds wird automatisch angepasst

Kernel-Optionen quiet splash Add

SPEICHERN ↻ SCHLIESSEN

Abb. 238: Allgemeine Einstellungen für die Hardwareklasse

Unter Partitionen legst Du fest, welche Partitionen auf der Festplatte vorgesehen werden sollen.

Löschst Du dort z.B. die Partitionen swap und data so sieht Deine Partitionierung wie folgt aus:

Um Einstellungen für das jeweilige Betriebssystem vorzunehmen, klickst Du auf das Stift-Icon neben dem angegebenen Betriebssystem. Es öffnet sich ein weiteres Fenster, um Einstellungen für das Betriebssystem vorzunehmen.

Unter der Reiterkarte OS legst Du für das Betriebssystem (OS) die gewünschten Icons, die Start-Optionen und u.a. auch den Namen für das Basisimage fest.

Um ein neues Image festzulegen, klickst Du auf das + - Zeichen und trägst einen neuen Namen für das Image ein. Achte darauf, dass die Dateiendung `.qcow2` lautet. Um nun das neue Image zu erstellen, startest Du den Client neu. Es wird das bestehende Image, das unter Basisimage angelegt bzw. ausgewählt wurde - hier das noch nicht existierende Image `pop_os_mim.qcow2` - überschrieben.

Auf dem linuxmuster.net Server werden die `start.conf`-Dateien im Verzeichnis `/srv/linbo` abgelegt. Jede Hardwareklasse hat eine eigene `start.conf`-Datei. Für die neu angelegte Hardwareklasse des Muster-Clients wurde dort nun eine Datei `start.conf.<name-der-hwk>` erstellt (z.B. `start.conf.ubu20efi`).

Diese Datei muss normalerweise nicht händisch editiert werden, da sich alle nötigen Einstellungen in der WebUI vornehmen lassen. Das folgende Beispiel dient nur dazu, zu zeigen, was „unter der Decke“ passiert.

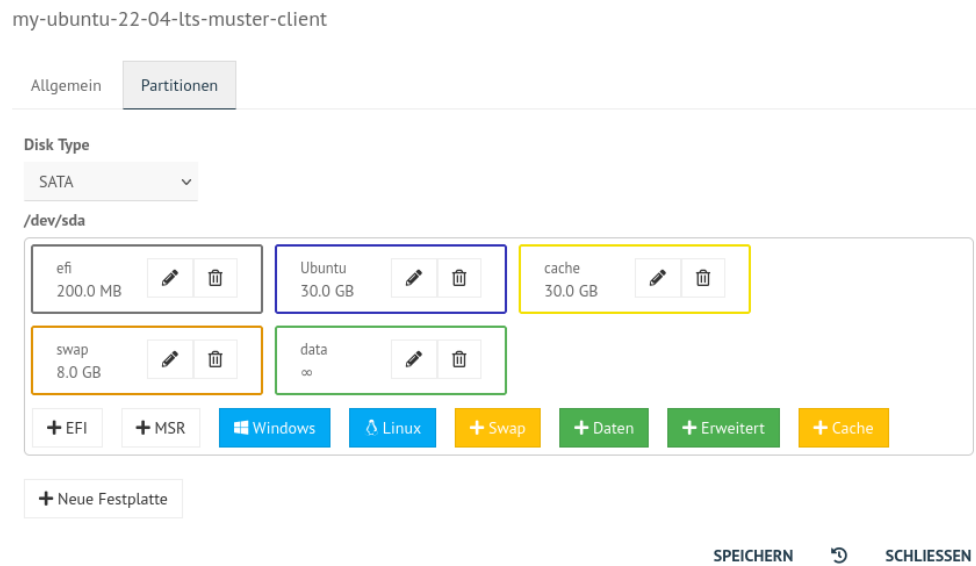


Abb. 239: Partitionen festlegen

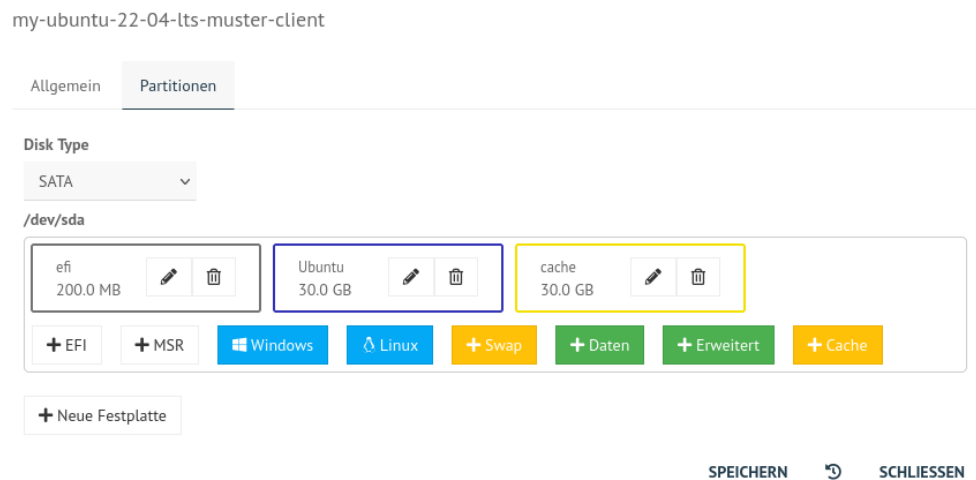



Abb. 240: Partitionen anpassen


Partition **OS**

Name	Version
Pop! OS	22.04 LTS

Standard Start	Symbol
Sync & start ▼	 ▼

Basisimage

pop_os_mlm.qcow2 ▼



Start Optionen

- ☒ Start
- ☒ Sync & start
- ☒ New start
- ☒ Autostart

Autostart-Timeout

5

Abb. 241: Einstellungen des Betriebssystems anpassen

Folgende Konfiguration zeigt ein mögliches Beispiel für die Hardwareklasse `ubu20efi` (hier als Linux-Client). Diese würde sich in der Datei `/srv/linbo/start.conf.ubu20efi` befinden. Hierbei wird von einem UEFI-BIOS und Linux als Betriebssystem ausgegangen:

```
[LINBO]
Server = 10.0.0.1
Group = ubu20efi           #Hardwareklasse
Cache = /dev/sda3
RootTimeout = 600
AutoPartition = no
AutoFormat = no
AutoInitCache = no
GuiDisabled = no           # disable gui <yes/no>
UseMinimalLayout = no     # gui layout style <yes/no>
Locale = de-DE            # gui locale <de-de/en-gb/fr-fr/es-es>
DownloadType = torrent
SystemType = efi64        # UEFI-BIOS
KernelOptions = quiet splash # hier muessen bei spezieller Hardware ggf. Kernel-
↪Parameter angegeben werden wie nomodeset

[Partition]
Dev = /dev/sda1
Label = efi
Size = 200M
Id = ef
FSType = vfat
Bootable = yes

[Partition]
Dev = /dev/sda2
Label = ubuntu
Size = 12G
Id = 83
FSType = ext4
Bootable = no

[Partition]
Dev = /dev/sda3
Label = cache
Size = 12G
Id = 83
FSType = ext4
Bootable = no

[Partition]
Dev = /dev/sda4
Label = swap
Size = 2G
Id = 82
FSType = swap
Bootable = no

[Partition]
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```

Dev = /dev/sda5
Label = data
Size =           # verbleibender Plattenplatz wird der Partition zugewiesen
Id = 83
FSType = ext4
Bootable = no

[OS]
Name = Ubuntu
Version = 20.04 LTS
Description = Ubuntu 20.04
IconName = ubuntu.svg
Image =
BaseImage = ubuntu.qcow2 # Name des neu angelegten Images in obiger Abb. ist dies: pop_
↪os_mlm.qcow2
Boot = /dev/sda2
Root = /dev/sda2
Kernel = /boot/vmlinuz
Initrd = /boot/initrd.img
Append = ro splash
StartEnabled = yes
SyncEnabled = yes
NewEnabled = yes
Autostart = no
AutostartTimeout = 5
DefaultAction = sync
RestoreOpsiState = no
ForceOpsiSetup =
Hidden = yes

```

Hinweis: Sollte der Client beim Boot-Vorgang Probleme haben (z.B. initializing hardware ...), dann müssen zur Behebung Kernel-Parameter für den Linux-Client in der Conf-Datei eingetragen werden. Dies kann insbesondere bei neueren Grafik- und Netzwerkkarten der Fall sein, so dass hier weitere Optionen anzugeben sind. Oftmals führt bereits folgende Zeile zum Erfolg:

```
KernelOptions = quiet splash nomodeset
```

Hilfreich können auch KernelOptions sein wie z.B.:

```
modprobe.blacklist=radeon oder i915.alpha_support=1
```

Wenn bei neueren Realtek-Netzwerkkarten mit r8169-Chip in linbo >=4.1.26 sehr niedrige Download-Raten auftreten, können die Kerneloptionen `pcie_aspm=off` und `loadmodules=r8168` Besserung bringen.

4.11.2 Rechneraufnahme

Autor des Abschnitts: @cweikl, @Alois, @Tobias, @michael_kohls

Der PC, der als Hardware zum Aufbau des Muster-Clients genutzt werden soll, ist via Kabel mit dem Netzwerk zu verbinden.

Alternativ kann für den Aufbau des Muster-Clients eine VM in der Virtualisierungsumgebung angelegt werden.

Nachstehende Angaben stellen ein Beispiel für die Rahmendaten einer solchen VM dar:

- 4 GiB vRAM
- mind. 1 vCPU mit 2 Kernen
- VGA mit 16 MiB Speicher
- 1x vNIC (ggf. im „richtigen“ VLAN)
- PXE-Boot einstellen (Bootreihenfolge: NIC first)
- Boot Firmware: BIOS oder UEFI (je nach später genutzten PCs) - Achtung: start.conf von linbo ggf. anpassen -> siehe Hinweise bei den Client-Systemen
- z.B. 50 GiB HDD (20 GiB OS + 20 GiB Cache + ggf. SWAP oder andere Partitionen)

Hinweis: Die Gerätenamen dürfen nur aus ASCII-Zeichen (nur Kleinbuchstaben), Ziffern von 0 bis 9 und dem Bindestrich bestehen. Ein Geräte-Name darf nicht mit einem Bindestrich beginnen oder enden.

Für den Gerätenamen dürfen maximal 15-Zeichen verwendet werden.

Beispiel: g001-r101-pc001

... mit der WebUI

Um einen Rechner mit der Schulkonsole aufzunehmen, meldest Du Dich zunächst an der Schulkonsole als `global-admin` an.

Wähle dann links im Menü Geräteverwaltung --> Geräte.



Abb. 242: Menü Geräte

Danach siehst Du rechts die Liste mit allen bereits in der Gerätedatei eingetragenen Geräten. Standardmäßig sind nach dem Setup die konfigurierten Server schon in der Liste mit der Rolle `Server` eingetragen.

Klicke unterhalb der Liste auf den Button `+ Gerät hinzufügen`, um ein neues Gerät einzutragen. Es wird eine neue, noch leere Zeile am Anfang der Geräteliste eingefügt.

In der neuen Zeile gibst Du nun folgendes an:

Raum	Rechnername	Gruppe	MAC	IP	Sophomorix-Rolle	PXE		
server	server	nopxe	0e:d9:57	10.0.0.	Domänencontr ▾	Kein PXE ▾		
server	firewall	nopxe	72:BD:5E	10.0.0.	Server ▾	Kein PXE ▾		
server	verw-pc	nopxe	EE:05:C3	10.0.0.	Lehrer-PC ▾	Kein PXE ▾		

[+ Gerät hinzufügen](#)

Abb. 243: Eingetragene Server

Raum	Rechnername	Gruppe	MAC	IP	Sophomorix-Rolle	PXE		
Room	Hostname	Group	MAC	IP	Schüler-PC im Klassenz ▾	Linbo-PXE ▾		
a001	a001-pc01	pop-os-22-04-lts	52:54:00:a1:c6:0	10.0.1.1	Schüler-PC im Klassenz ▾	Linbo-PXE ▾		

Abb. 244: Neues Gerät hinzufügen

1. Raum: Name des Raums (Achtung: keine Binde- und Unterstriche verwenden, keine Umlaute, max. 10 Zeichen)
2. Hostname: Name des Geräts (Erlaubte Zeichen a-z A-Z 0-9 -; Achtung: Keine Unterstriche verwenden; max. 15 Zeichen)
3. Gruppe: Bezeichnung der Linbo-Hardwareklasse. Gleiche Bezeichnungen für Raum und Gruppe sind unzulässig. Reservierte Wörter, wie „con“ und „man“, dürfen nicht verwendet werden.
4. MAC: Media Access Control - Hardware-Adresse des Netzwerkadapters. Trage 12 Hexadezimalzahlen mit einem Doppelpunkt als Trennzeichen nach zwei Ziffern ein.
5. IP: Gib eine IP-Adresse für das Gerät an, das diesem automatisch zugewiesen werden soll. Z.B. Raum 202 im Gebäude G erhält den Bereich 10.0.202.x/16 und PC01 erhält die IP 10.0.202.1
6. Sophomorix-Rolle: Hier gibst Du an, welche Art von Gerät Du einbindest. Für PCs im Fachraum gibst Du z.B. Schüler-PC im Klassenzimmer an.
7. PXE: Lege über das Drop-down Menü fest, ob der PC mit Linbo-PXE synchronisiert werden soll oder nicht.

Hinweis: Die Bedeutung der Sophomorix-Rolle wird auf [Github](#) beschrieben.

Die o.g. Zeile könnte ausgefüllt wie folgt aussehen:

G202	G202-pc01	ubu20	AA:BB:11	10.0.20	Schüler-PC im K ▾	Linbo-PXE ▾		
------	-----------	-------	----------	---------	-------------------	-------------	--	--

Abb. 245: Eintragungen für neuen Client

Die Schaltfläche **Speichern** überprüft die Eingabe, **Speichern & importieren** werden die neuen Geräte importiert. Mit dem Button **Im Editor öffnen** wird die Datei `/etc/linuxmuster/sophomorix/default-school/devices.csv` im Editor geöffnet und kann bearbeitet werden.

Im folgenden erscheinen einige Log-Meldungen und - wenn der Import erfolgreich war - „Import abgeschlossen“

Um weitere Geräte hinzuzufügen, wiederholst Du den beschriebenen Vorgang in der Schulkonsole entsprechend.

Hinweis: Sind nun die gewünschten Geräte aufgenommen, kannst Du mit ...

... der Erstellung eines Muster-Clients fortfahren, so dass alle PCs einer Linbo Hardwareklasse ein identisches Image erhalten. Gehe zu [Betriebssysteme installieren](#)

Speichern

Speichern & importieren

Im Editor öffnen

Abb. 246: Schaltflächen

Importiere Gerät

```

#### g202-pc01 | ubu20efi #####
#### g202-pc02 | ubu20efi #####
#### h201-pc01 | win10efi #####
-----
#### Working on linbo/grub configuration for groups: #####
#### | linbo start.conf | grub cfg #####
#### -----+-----+----- #####
#### ubu20efi | present | replaced #####
#### win10efi | present | created #####
-----
#### Restarting services: #####
#### * isc-dhcp-server ..... OK! #####
-----
#### linuxmuster-import-devices finished at 2022-02-22 17:49:58 #####
-----

```

Optionen

☒ Autoscroll

DETAILS AUSBLENDEN

SCHLIESSEN

Abb. 247: Import abgeschlossen

... dem Verteilen eines vorhandenen Images auf die aufgenommenen Geräte beginnen. Gehe zu [LINBO4 nutzen](#)

... mittels der Datei devices.csv

Wenn Du sehr viele Geräte hinzufügen möchtest, deren MAC-Adressen Du bereits kennst, dann ist die o.g. Option **Im Editor öffnen** eine Möglichkeit, die Datei devices.csv direkt zu editieren.

Auf dem Server kannst Du Dir in der Konsole mit

```
man devices.csv
```

die man pages anzeigen lassen. Hier kannst Du Dir alle Felder der CSV-Datei mit Erklärungen ausgeben lassen.

Weitere Hinweise zu den möglichen Rollen eines Gerätes in der devices.csv findest Du hier:

<https://github.com/linuxmuster/sophomorix4/wiki/objectClasses>

Die Datei kann hier auch zur lokalen Bearbeitung heruntergeladen und wieder hochgeladen werden.

Hinweis: Es sind nun die gewünschten Geräte aufgenommen und Du kannst mit ...

... der Erstellung eines Muster-Clients fortfahren, so dass alle PCs einer Linbo Hardwareklasse ein identisches Image erhalten. Gehe zu [Betriebssysteme installieren](#)

... dem Verteilen eines vorhandenen Images auf die aufgenommenen Geräte beginnen. Gehe zu [LINBO4 nutzen](#)

/etc/linuxmuster/sophomorix/default-school/devices.csv

Datei hier hin schieben um sie zu importieren

```

1 # modified by linuxmuster-setup at 20211228121015
2 # /etc/linuxmuster/sophomorix/default-school/devices.csv
3
4 # thomas@linuxmuster.net
5 # 20190323
6
7 # Example:
8 #r100
9
10 # For Details see devices.csv.5
11
12 server;server;nopxe;0e:d9:57:72:1a:20;10.0.0.1;;;addc;0;;;SETUP;
13 server;firewall;nopxe;72:80:56:E8:1D:04;10.0.0.254;;;server;0;;;SETUP;
14 server;verw-pc;nopxe;EE:05:C3:23:2F:E9;10.0.0.10;;;staffcomputer;0;;;
15 G202;G202-pc01;ubu20;AA:BB:11:22:22:AF;10.0.202.1;;;classroom-studentcomputer;1;;;
16

```

SPEICHERN CSV HERUNTERLADEN ABBRECHEN

Abb. 248: devices.csv im Editor anpassen

... mittles LINBO

Wurde z.B. ein neuer Schulungsraum mit 20 PCs ausgestattet, deren MAC-Adressen Du nicht kennst, dann bietet sich diese Möglichkeit an.

Dazu hat sich folgendes Vorgehen bewährt:

1. Der Clientrechner muss mit dem Schulnetzwerk verbunden sein und den Server erreichen können.
2. Um LINBO zu starten, den PC über das Netzwerk booten (PXE). Dazu entweder im BIOS-Setup in der Bootreihenfolge PXE-Boot als erstes Bootmedium einstellen oder über das Bootmenü PXE-Boot auswählen. Dies gelingt je nach Rechner meistens über die Tasten F2, F10 oder F12. Als virtueller Rechner auf einem Hypervisor unter VMxyz --> Options --> Bootorder ist hier die Netzwerkkarte als erstes Boot-Medium zu wählen.
3. Es sollte bei einem erfolgreichen Bootvorgang via PXE folgender Startbildschirm zu sehen sein:
4. Wähle in dem LINBO Startbildschirm nun rechts das Werkzeug-Symbol aus. Es erscheint die Kennwortabfrage. Gib das Kennwort des Linbo-Root-Benutzers an, wie es beim Setup erstellt wurde.

Achtung: Deine Eingabe ist nicht zu sehen, es werden auch keine Sternchen für die eingegebenen Ziffern dargestellt.

5. Es werden nun zwei weitere Menü-Symbole dargestellt:
6. Wähle den Eintrag **Register** aus.
7. Es öffnet sich ein Fenster, um den Client zu registrieren. Fülle alle Felder aus. Achte darauf, dass Du als Host group die zuvor neu angelegte einträgst.

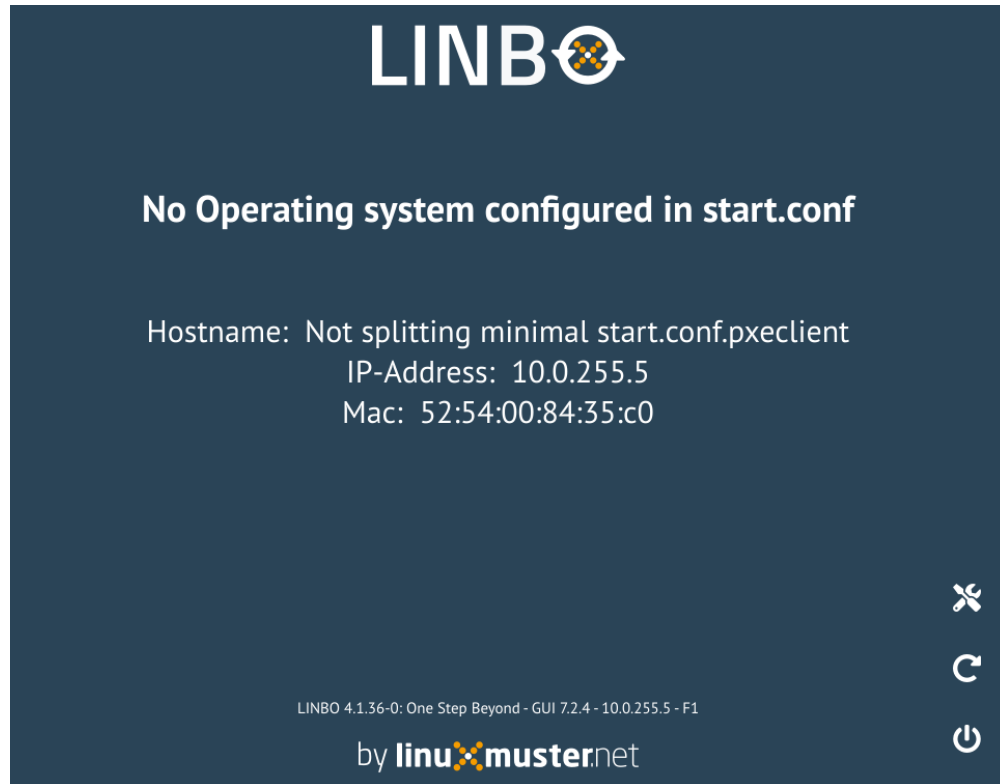


Abb. 249: PXE-Bootvorgang auf dem Client

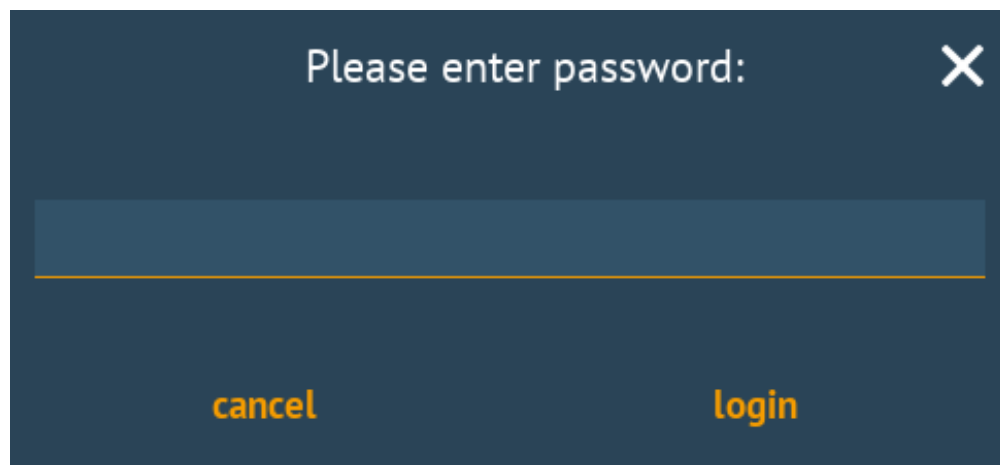


Abb. 250: Eingabe des LINBO Kennworts

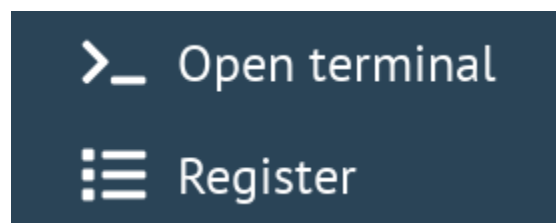
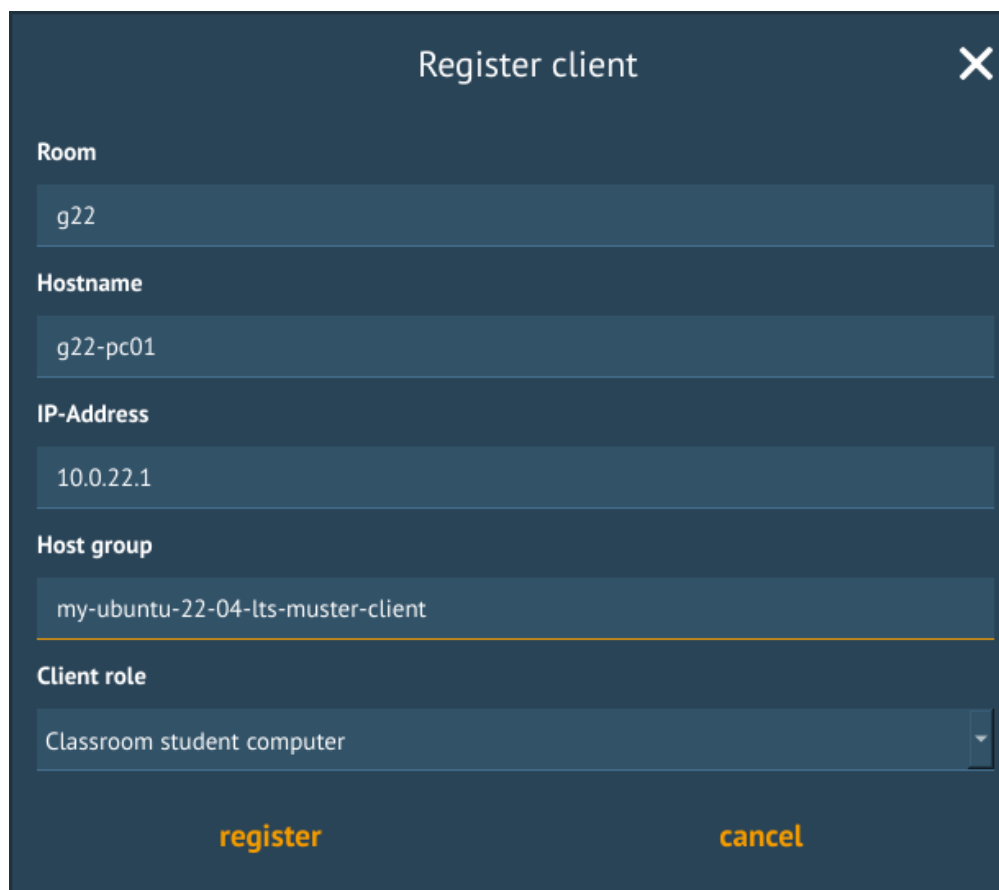


Abb. 251: Werkzeug-Symbol - Untermenü



A dark-themed dialog box titled "Register client" with a close button (X) in the top right corner. The dialog contains five input fields, each with a label above it: "Room" (value: g22), "Hostname" (value: g22-pc01), "IP-Address" (value: 10.0.22.1), "Host group" (value: my-ubuntu-22-04-lts-muster-client), and "Client role" (value: Classroom student computer, shown as a dropdown menu). At the bottom, there are two buttons: "register" in orange and "cancel" in white.

Register client

Room
g22

Hostname
g22-pc01

IP-Address
10.0.22.1

Host group
my-ubuntu-22-04-lts-muster-client

Client role
Classroom student computer

register cancel

Abb. 252: Register Client

8. Klicke dann auf den Eintrag `register`. Nach Abschluss der Neuaufnahme siehst Du nachstehende Meldung:

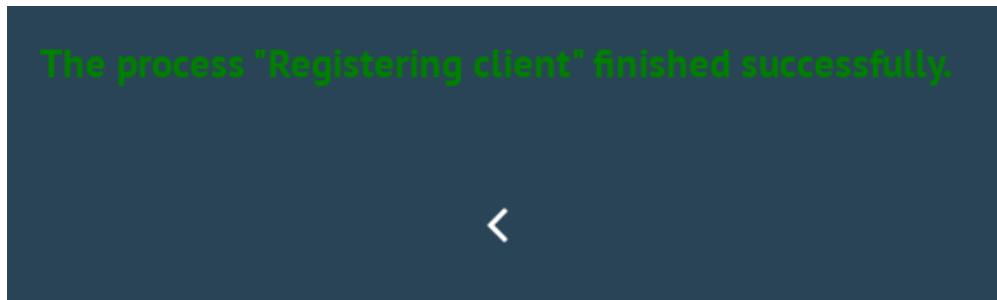












Abb. 253: Registrierung abgeschlossen

9. Führe o.g. Vorgang für alle neu aufzunehmenden Clients durch.
10. Wenn alle PCs so registriert wurden, öffne an Deinem Administrations-Rechner die Schulkonsole und melde Dich wieder als `global-admin` an. Wähle im Menü `Geräteverwaltung` --> `Geräte` aus. Du siehst nun neben den schon vorhandenen Geräten ebenfalls die neu aufgenommenen Geräte (in der Abb. sind dies die PCs für den Raum g202):

Raum	Rechnername	Gruppe	MAC	IP	Sophomorix-Rolle	PXE		
g202	g202-pc01	ubu20efi	F6:E8:80	10.0.2(Schüler-PC im ▾	Linbo-PXE ▾		
g202	g202-pc02	ubu20efi	16:07:27	10.0.2(Schüler-PC im ▾	Linbo-PXE ▾		
server	server	nopxe	0e:d9:57	10.0.0.	Domänencontr ▾	Kein PXE ▾		
server	firewall	nopxe	72:BD:5€	10.0.0.	Server ▾	Kein PXE ▾		
server	verw-pc	nopxe	EE:05:C3	10.0.0.	Lehrer-PC ▾	Kein PXE ▾		


 Gerät hinzufügen

Abb. 254: Neu aufgenommene Geräte

11. Klicke nun auf `Speichern & importieren`. Wurde der Vorgang abgeschlossen, siehst Du dies im Importfenster.

Hinweis: Es sind nun die gewünschten Geräte aufgenommen und Du kannst mit ...

... der Erstellung eines Muster-Clients fortfahren, so dass alle PCs einer Linbo Hardwareklasse ein identisches Image erhalten. Gehe zu [Betriebssysteme installieren](#)

... dem Verteilen eines vorhandenen Images auf die aufgenommenen Geräte beginnen. Gehe zu [LINBO4 nutzen](#)

Importiere Gerät

```

##### Working on linbo/grub configuration for devices: #####
##### g202-pc01      | ubu20efi      #####
##### g202-pc02      | ubu20efi      #####
##### Working on linbo/grub configuration for groups: #####
#####      | linbo start.conf | grub cfg      #####
##### -----+-----+----- #####
##### ubu20efi      | present      | created      #####
##### Restarting services: #####
##### * isc-dhcp-server ..... OK! #####
##### linuxmuster-import-devices finished at 2021-12-29 13:03:42 #####

```

Optionen
☒ Autoscroll

DETAILS AUSBLENDEN SCHLIESSEN

Abb. 255: Import abgeschlossen

4.11.3 Betriebssysteme installieren

Autor des Abschnitts: @cweikl, @MachtDochNix

Mit LINBO kannst Du mehrere Betriebssysteme auf einem Client verwalten und als Muster-Clients bereistellen und ausrollen. Du kannst so flexibel verschiedene Anforderungen in PC-Räumen (z.B. Linux mit Virtualisierungs-Partition ohne Synchronisation oder unterschiedliche Images in einem Raum für den Lehrer-PC und die PCs der Schülerinnen und Schüler) abbilden. linuxmuster.net ist darauf ausgelegt, als durchgängige Linux-Lösung genutzt zu werden. Hierzu wurden für den Linux-Client speziell angepasste Ubuntu - Pakete entwickelt, die eine Aufnahme in die Domäne, das Einbinden der Freigaben etc. übernehmen. Windows|ltrim| Betriebssysteme können ebenfalls als Clients vollständig genutzt werden.

Das Partitionierungsschema für die Clients einer Hardwareklasse hast Du mit den Schritten in [Hardwareklasse \(HWK\) / Gruppe erstellen](#) festgelegt und im darauf aufbauenden Kapitel [Rechneraufnahme](#) Deinem Client zugewiesen. Solltest Du das noch nicht gemacht haben, dann hole dies jetzt nach.

Achtung: Folgende Punkte sind sicherzustellen:

- Es darf keine Zeitdifferenz zwischen dem Client und dem linuxmuster.net-Server bestehen.
- Der Client muss via Kabel am Netzwerk angeschlossen sein.
- Die Botreihenfolge des Clients ist so eingestellt, dass dieser via Netzwerkkarte (PXE) zuerst bootet.
- Der Client erreicht den Server im gleichen Netzwerk und erhält so eine IP_Adresse.
- Die Hardwareklasse wurde angelegt und der PC wurde als Gerät in der Schulconsole oder der devices.csv aufgenommen und importiert.

Festplatte mit LINBO vorbereiten

Bevor Du mit der eigentlichen Installation des Client-Betriebssystems beginnen kannst, musst Du die Festplatte mittels LINBO vorbereiten. Dieses wird detailliert unter [Festplatte mit LINBO vorbereiten](#) beschrieben.

Betriebssysteme installieren

Danach kannst Du das gewünschte Betriebssystem auf dem Client installieren. Das Vorgehen hierzu wird ausführlich für

1. *Linux-Client*
2. *Windows 10 Clients*

beschrieben.

Muster-Client als NoProxy Gerät

Für den Zeitraum der Installation und Aktualisierung des Muster-Clients ist es wichtig, dass dieser Internet-Zugriff hat, um Aktualisierungen laden zu können. Dazu ist es erforderlich, dass nachdem der Client als Gerät importiert wurde, Du die IP-Adresse des Gerätes in der sog. NoProxy Gruppe in der Firewall der OPNsense aufnimmst.

Dazu meldet Du Dich an der OPNsense als Benutzer **root** an und wählst links im Menü unter **Firewall** -> **Aliase** aus.

Du siehst dann anstehende Firewall: Aliase.

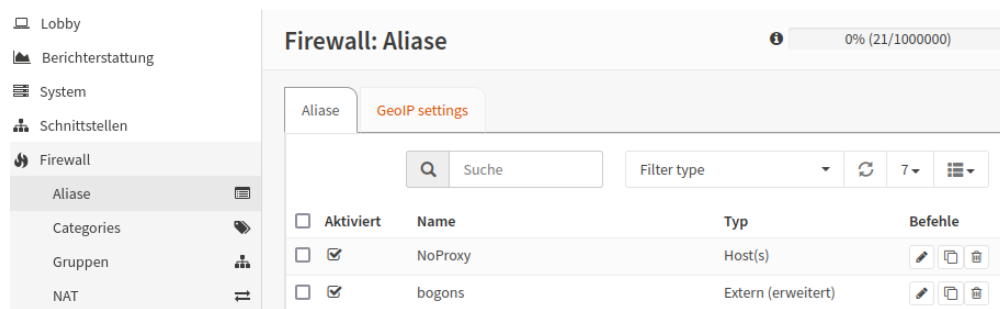


Abb. 256: NoProxy aufrufen

Klicke rechts neben dem Eintrag der Alias-Gruppe NoProxy das Stift-Symbol zum Editieren der Gruppe. Trage hier im Feld **Inhalt** nun die IP-Adresse des Muster-Clients ein.

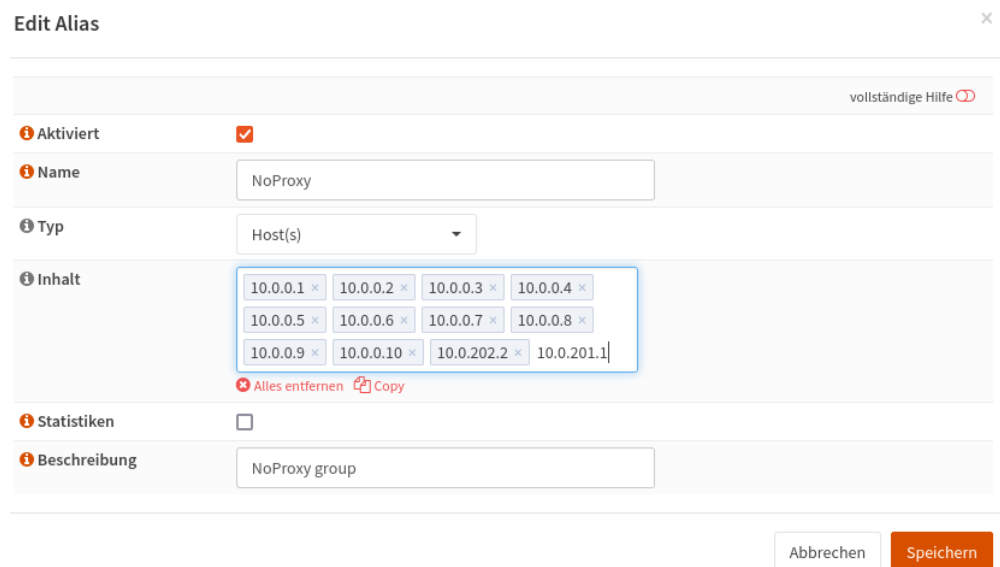


Abb. 257: IP des Clients in die NoProxy Gruppe eintragen

Bestätige die IP mit ENTER, so dass der Eintrag grau hinterlegt wird. Klicke zum Abschluss auf **Speichern** und anschließend auf **Anwenden**, um die Einstellungen zu speichern und zu übernehmen.

Nach Abschluss der Installation und Konfiguration des Muster-Clients kannst Du diesen wieder aus der NoProxy - Gruppe entfernen. Es sei denn, Du nutzt exklusiv immer den identischen Client zur Weiterentwicklung des Muster-Clients.

Festplatte mit LINBO vorbereiten

Autor des Abschnitts: @cweikl, @MachtDochNix (pics)

Du bootest nun den zuvor aufgenommen Client via PXE, so dass dieser vom Server eine IP-Adresse erhält und Du folgenden LINBO-Bildschirm siehst (hier als Beispiel für eine Hardwareklasse für Ubuntu):



Abb. 258: LNBO PXE Startbildschirm

Wähle nun das Werkzeug-Symbol rechts aus.



Abb. 259: Werkzeug-Symbol

Es erscheint die Aufforderung, dass Du das LINBO-Passwort eingeben musst. Dies entspricht nach der Installation i.d.R. dem des global-admin. Bei der Eingabe des Kennwortes werden Dir keine Zeichen angezeigt - auch keine Sternchen.

Es erscheint dann das LINBO-Tools Menü.

Wähle hier nun den Eintrag **Festplatte partitionieren** aus, damit die Festplatte Deines Clients wie zuvor in der Hardwareklasse angegeben, partitioniert und formatiert wird. Bevor der Vorgang angewendet wird, erhältst Du die



Abb. 260: Eingabe des LINBO Kennwortes



Abb. 261: LINBO Werkzeug-Menü

Rückfrage, ob damit wirklich alle Daten auf dem Laufwerk gelöscht werden sollen.

Bestätige dies mit Ja.

Während der Partitionierung und Formatierung der Festplatte des Clients siehst Du eine Status-Anzeige.

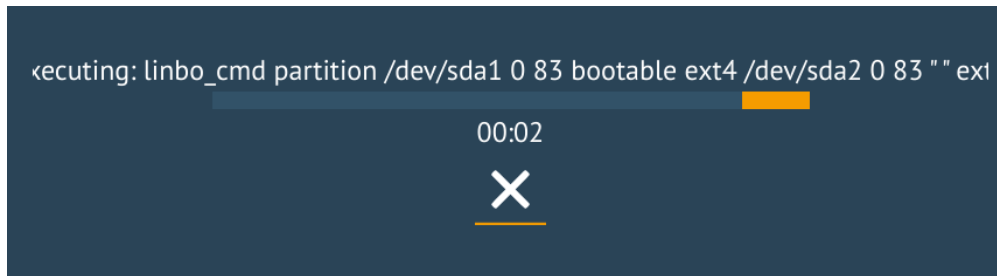


Abb. 262: Partitionierung der Client Festplatte

Wurde der Vorgang abgeschlossen, so findest Du nachstehende Status-Meldung:

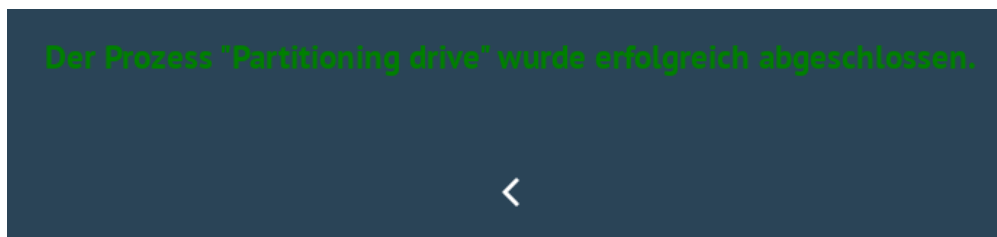


Abb. 263: Fertigstellung der Partitionierung

Klicke dann auf das Kleiner-Zeichen <.

Fahre nun den Client herunter, indem Du folgenden Button klickst:



Abb. 264: Client herunterfahren

Nachdem der Client heruntergefahren wurde, achte darauf, dass das Installationsmedium (z.B. USB-Stick mit ISO-Image oder DVD) für das gewünschte Betriebssystem eingelegt ist.

Starte dann den Client neu, drücke während des Boot-Vorgangs F2, F10, F12, usw., um in das BIOS Boot-Menü zu gelangen. Als virtueller Rechner auf einem Hypervisor wählst Du unter VMxyz Options Bootorder` das eingelegte Installationsmedium aus.

Setze nun die Installation fort ...

1. *Linux-Client*
2. *Windows 10 Clients*

Linux-Client

Autor des Abschnitts: @cweikl, @dorian

linuxmuster.net stellt für Ubuntu basierte Clients das Paket `linuxmuster-linuxclient7` bereit. Es führt automatisch den Domänenbeitritt aus und vereinheitlicht das Management von Linux- und Windows-Clients durch Auslesen der GPO-Konfigurationen im Active Directory.

Offiziell wird derzeit Ubuntu 22.04 und Pop!_OS 22.04 mit gdm3 und Gnome unterstützt. Andere Ubuntu basierte Distributionen mit gdm3 und Gnome könnten aber auch funktionieren.

Voraussetzung

Du hast bereits:

1. PC im Netz angeschlossen / VM angelegt und geeignete Netzwerkverbindung definiert
2. Eine Hardwareklasse für den PC / die VM konfiguriert
3. PC/VM als Rechner aufgenommen
4. PC/VM via PXE mit Linbo gestartet
5. Die Festplatte mit Linbo partitioniert und formatiert

Falls Du das noch nicht getan hast, starte zuerst mit den Schritten, die im Kapitel [Rechneraufnahme](#) beschrieben werden und mache erst danach hier weiter.

Einrichten eines Linux-Clients

Imagennamen eintragen (HWK)

Vor der Installation bzw. Imageerstellung musst Du eine Hardwareklasse (HWK) zuweisen, sofern nicht bereits bei der Rechneraufnahme erfolgt.


Gehe dazu in der WebUI auf **Geräteverwaltung** -> **Linbo 4** -> **Gruppen** -> **<hwk auswählen>**. Klicke für die gewünschte HWK das Stift-Symbol, um die Einstellungen anzupassen. Es öffnet sich das Fenster mit den Einstellungen für die HWK. Wähle hier unter **Partitionen** Dein Betriebssystem (Reiterkarte OS) aus und klicke das Stift-Icon. Klicke in dem sich öffnenden Fenster die Reiterkarte unter OS und klicke auf das + - Symbol, um einen neuen Eintrag für das **Basisimage** festzulegen. Alternativ kannst Du auch einen Namen aus der Drop-down Liste auswählen. Bei der Erstellung des Erstimages wird ein vorhandenes überschrieben. (vgl. hierzu auch das Vorgehen unter ref:[add-computer-label](#)).

Übernehme die Eintragungen jeweils mit **Speichern & Importieren**. Danach wird automatisch ein Import der Geräte ausgeführt, um diese Einstellungen für alle Geräte der HWK zu übernehmen.

Hinweis: Das neue Image befindet sich später auf dem Server unter `/srv/linbo/images/<os>/` - also für o.g. Abb. z.B. `/srv/linbo/images/ubuntu/pop_os_mlm.qcow2`


Partition **OS**

Name	Version
Pop! OS	22.04 LTS

Standard Start	Symbol
Sync & start ▼	 ▼

Basisimage

pop_os_mlm.qcow2 ▼



Start Optionen

- ☒ Start
- ☒ Sync & start
- ☒ New start
- ☒ Autostart

Autostart-Timeout

5

Abb. 265: Festelegen des Dateinamens für das Basisimage

Client OS installieren

Gib im PC / in der VM nun an, dass von dem gewünschten ISO-Image / der Installations-DVD gestartet werden soll. Hierbei musst Du darauf achten, die Boot-Reihenfolge so zu ändern, dass nicht mehr vom Netzwerk, sondern von der ISO-Datei / der Installations-DVD gebootet wird.

Starte nun den PC / die VM mit den neuen Einstellungen, sodass Ubuntu vom ISO-Image / von der Installations-DVD startet. Nachdem der Start ausgeführt wurde, wähle auf dem ersten Bildschirm aus, dass Du Ubuntu installieren möchtest.

Nachstehend findest Du die Beschreibung zur Installation von Ubuntu.

Möchtest Du pop!os installieren, so folge dieser Beschreibung [Linux-Client: pop!os](#)

Installation Ubuntu

Hinweis: Bei Ubuntu sollte man darauf achten, dass der Firefox nicht als Snap-Paket installiert wird, da damit SSO nicht funktioniert! Möglicherweise trifft das auch auf andere Distributionen zu!

Hast Du den PC / die VM von vom ISO-Image / der Installations-DVD gestartet, siehst Du zunächst folgenden Start-Bildschirm:



Abb. 266: Installationsart festlegen

Gib in den ersten Schritten der Installation die gewünschte Sprache und Tastaturbelegung an.

Lege danach die Installationsart sowie weitere Optionen fest. Falls Du hier Aktualisierungen herunterladen wählst, so muss für dieser Client in der OPNSense[reg] in der NoProxy Gruppe eingetragen sein.

Bei der Installationsart wählst Du Etwas Anderes aus.

Du hattest mit LINBO bereits die Festplatte partitioniert und formatiert.

Es werden Dir also die bereits vorhandenen Partitionen und Dateisysteme angezeigt. Je nach genutzter Virtualisierungsumgebung / Hardware können die Festplattenbezeichnungen hier auch als /dev/xvda und die Partionen als /dev/xvda1 etc. angezeigt werden.

Wähle, wie in der nachstehenden Abb. zu sehen, die Partition aus, auf der Ubuntu installiert werden soll.

Klicke nun auf Ändern und es erscheint das nächste Fenster:

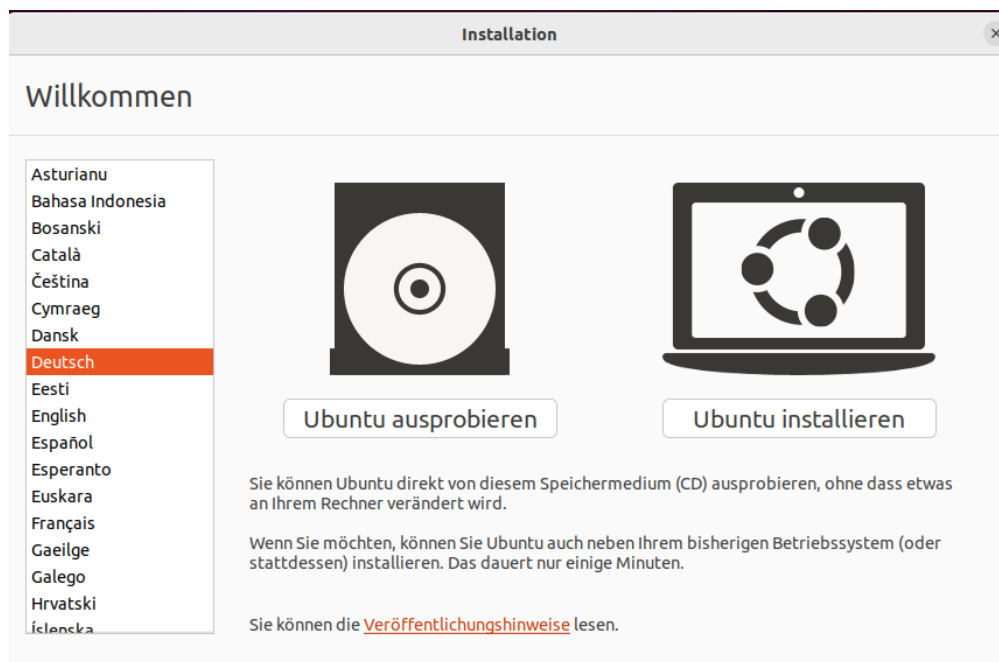


Abb. 267: Sprache auswählen

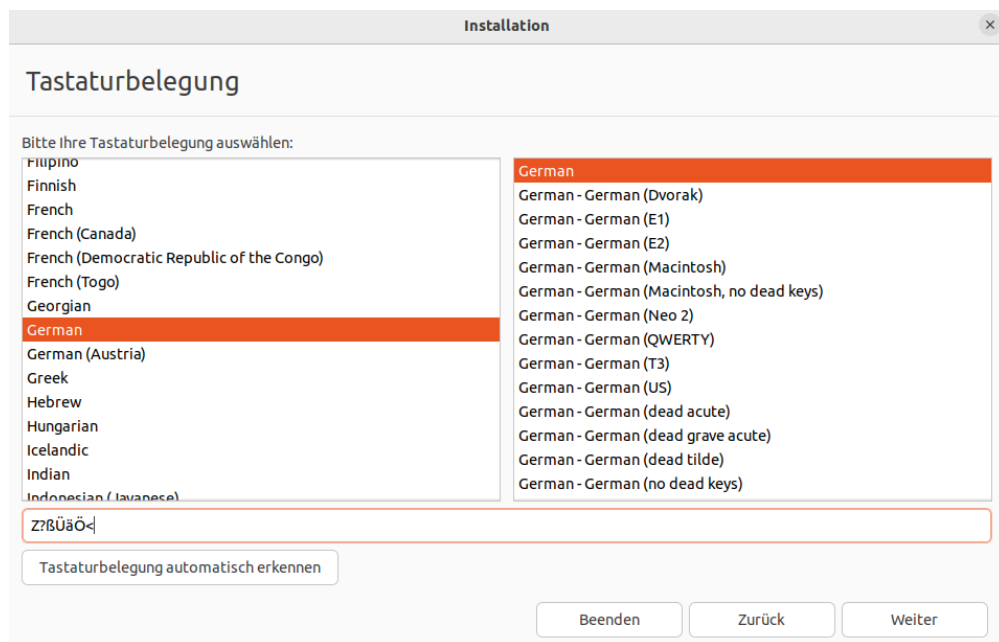


Abb. 268: Tastaturlayout auswählen

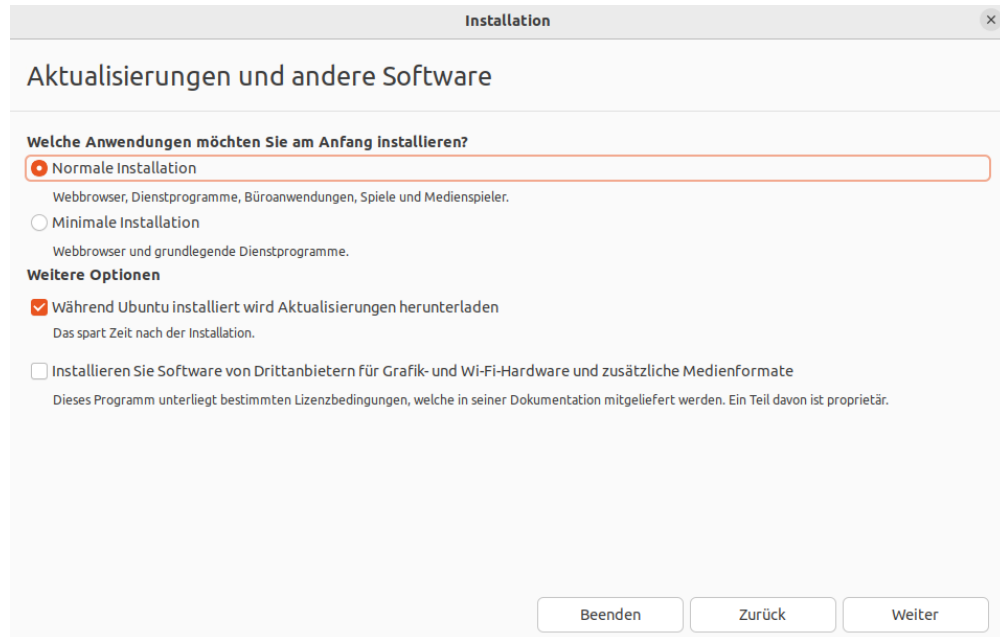


Abb. 269: Installationsart und -optionen festlegen

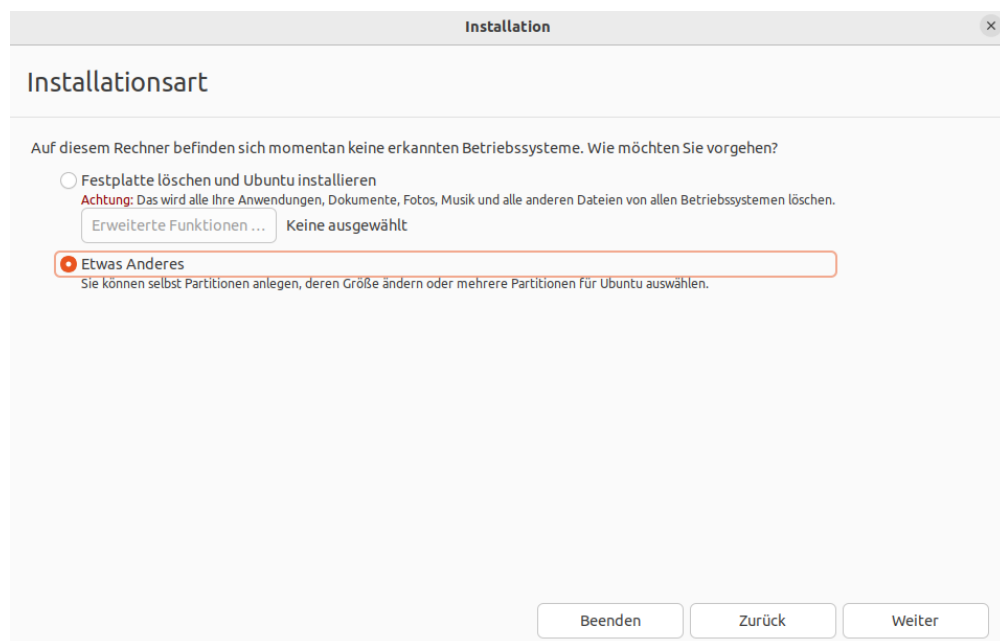


Abb. 270: Installationsart festlegen

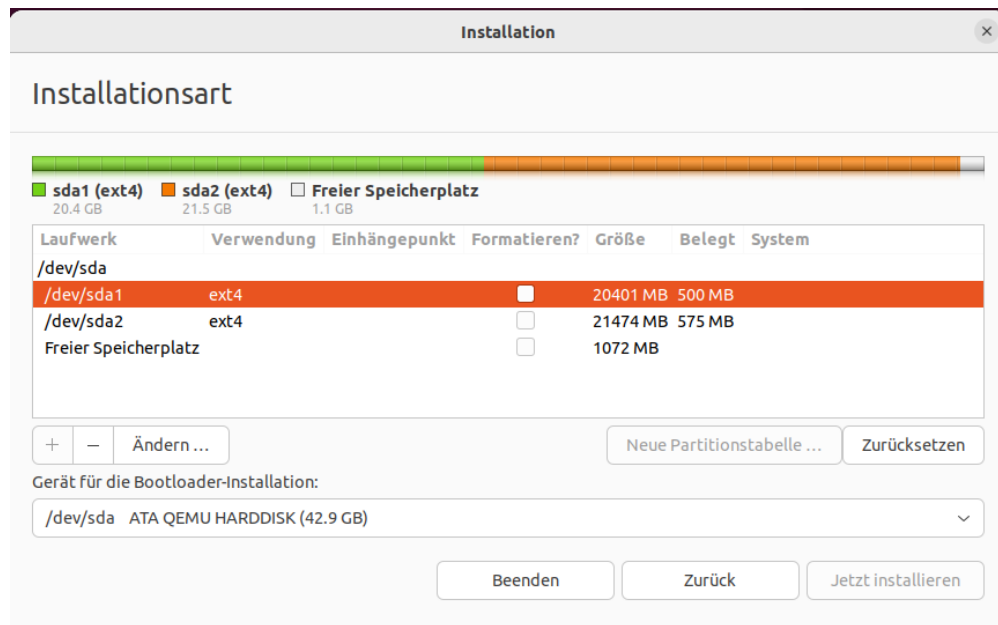


Abb. 271: Wähle die Ubuntu-Partition aus

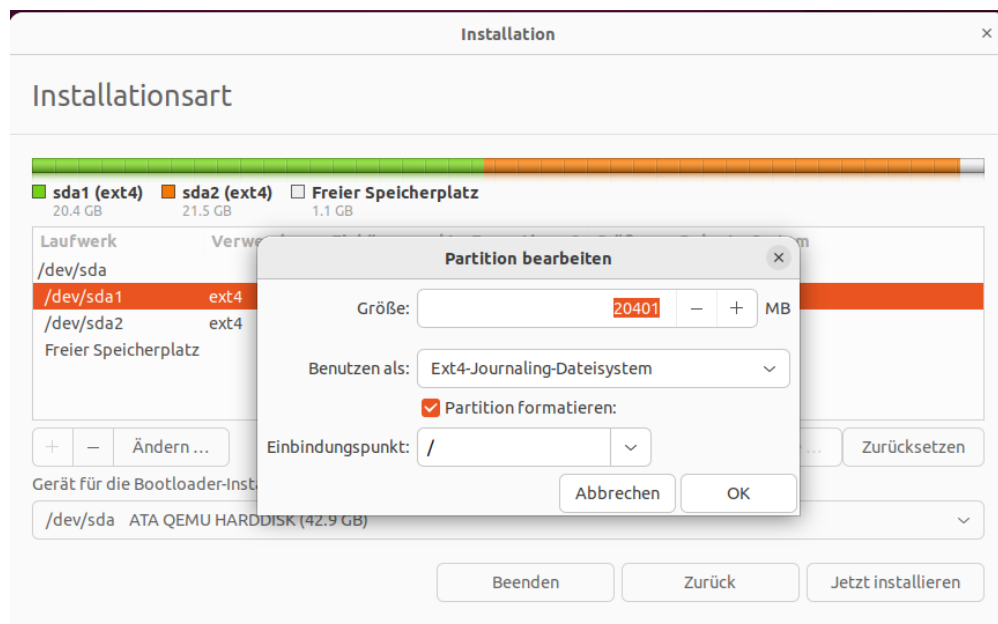


Abb. 272: Partition bearbeiten

Belasse die angezeigte Größe und das Dateisystem. Setze den Haken bei Partition formatieren und wähle als Einbindungspunkt das Root-Verzeichnis / aus.

Klicke auf ok und es werden nochmals alle Einstellungen angezeigt:

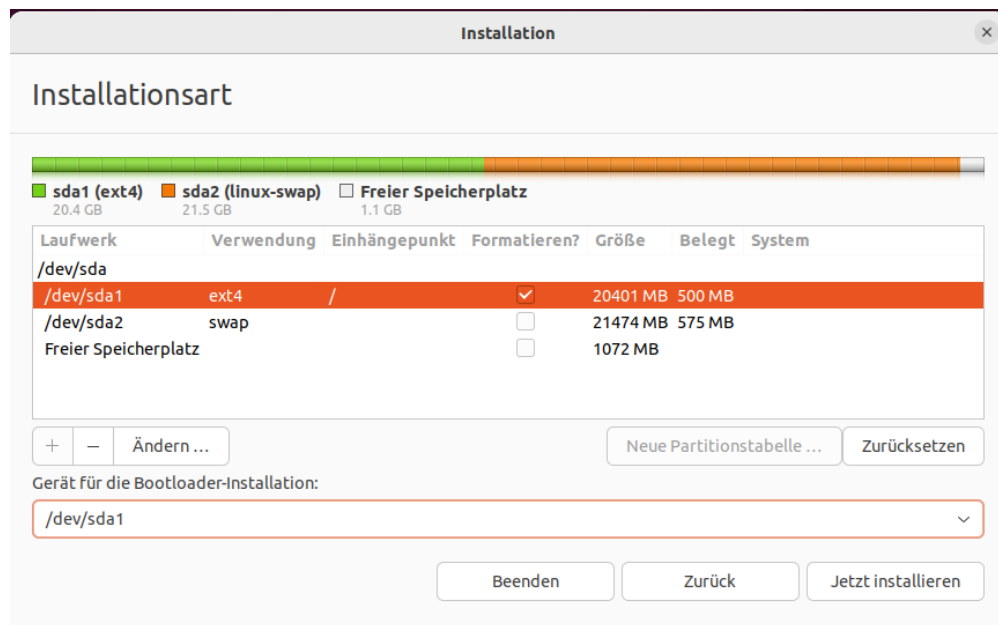


Abb. 273: Übersicht der Partitionen

Sind diese Einstellungen korrekt, prüfe noch, ob das Gerät für die Bootloader-Installation die Ubuntu-Partition ist (hier in der Abb. /dev/sda1). Falls nicht passe dies an. Der Bootloader sollte nicht auf den MBR der Festplatte installiert werden (hier also nicht auf /dev/sda).

Setze die Installation mit dem Button **Jetzt installieren** fort.

Im Verlauf der Installation wirst Du nach dem Namen für den Computer und dem Benutzernamen und Kennwort für den neuen Administrator gefragt. Gib hier als Benutzername **linuxadmin** ein. Beim Namen des Rechners musst Du den Namen des PCs / der VM angeben, wie Du ihn in der Gerätekonfiguration des festgelegt hast.

Am Ende der Installation wirst Du aufgefordert, den Rechner neu zu starten. Fahre die VM herunter und werfe das ISO-Image / die Installations-DVD aus.

Erstimage erstellen

Passe die Boot-Reihenfolge für den PC / die VM jetzt so an, dass diese wieder via PXE bootet. Du siehst dann die Startoptionen in Linbo für das installierte Ubuntu 22.04.

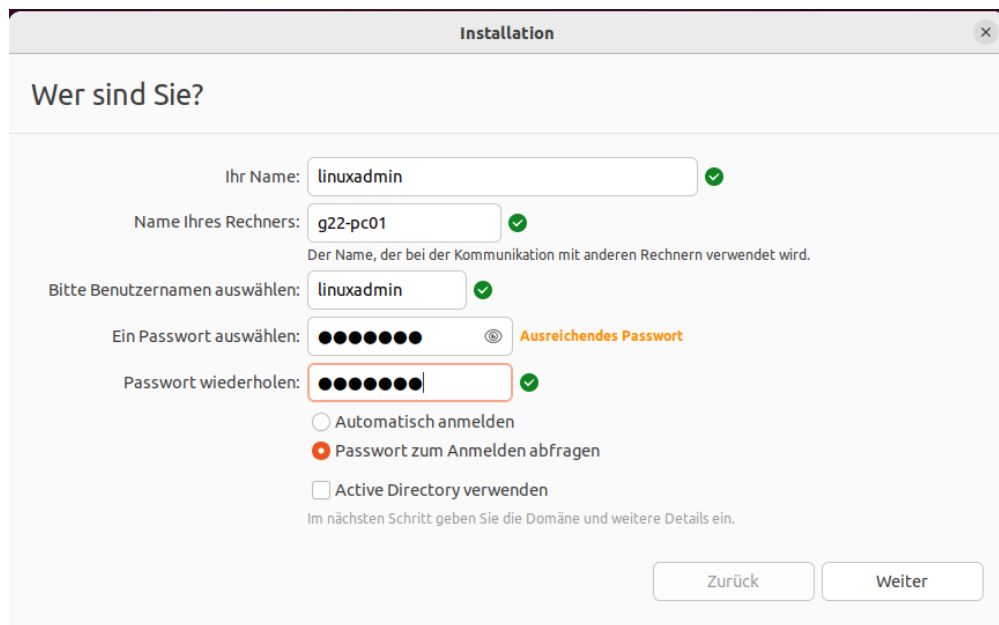
Klicke nun unten rechts auf das Werkzeug-Symbol, um zum Menü für die Imageerstellung zu gelangen.

Du wirst nach dem Linbo-Passwort gefragt. Gib dieses ein.

Achtung: Deine Eingabe wird hierbei nicht angezeigt.

Klicke dann auf **anmelden** und Du gelangst zu folgender Ansicht:

Klicke auf das große Festplatten-Symbol, das in der Ecke rechts unten farblich markiert ist, um nun ein Image zu erstellen.



Installation

Wer sind Sie?

Ihr Name: linuxadmin ✓

Name Ihres Rechners: g22-pc01 ✓
Der Name, der bei der Kommunikation mit anderen Rechnern verwendet wird.

Bitte Benutzernamen auswählen: linuxadmin ✓

Ein Passwort auswählen: ●●●●●● ● Ausreichendes Passwort

Passwort wiederholen: ●●●●●● | ✓

☐ Automatisch anmelden
☒ Passwort zum Anmelden abfragen
☐ Active Directory verwenden

Im nächsten Schritt geben Sie die Domäne und weitere Details ein.

Zurück Weiter

Abb. 274: Benutzer festlegen

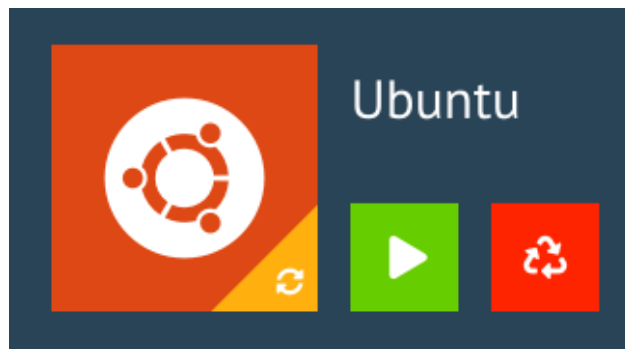


Abb. 275: LINBO Startoptionen



Abb. 276: Werkzeug-Symbol

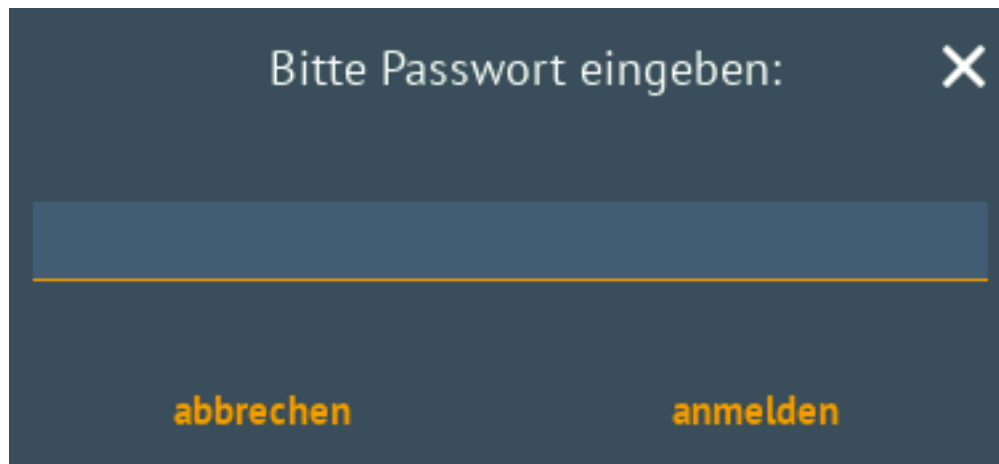


Abb. 277: LINBO Kennwort

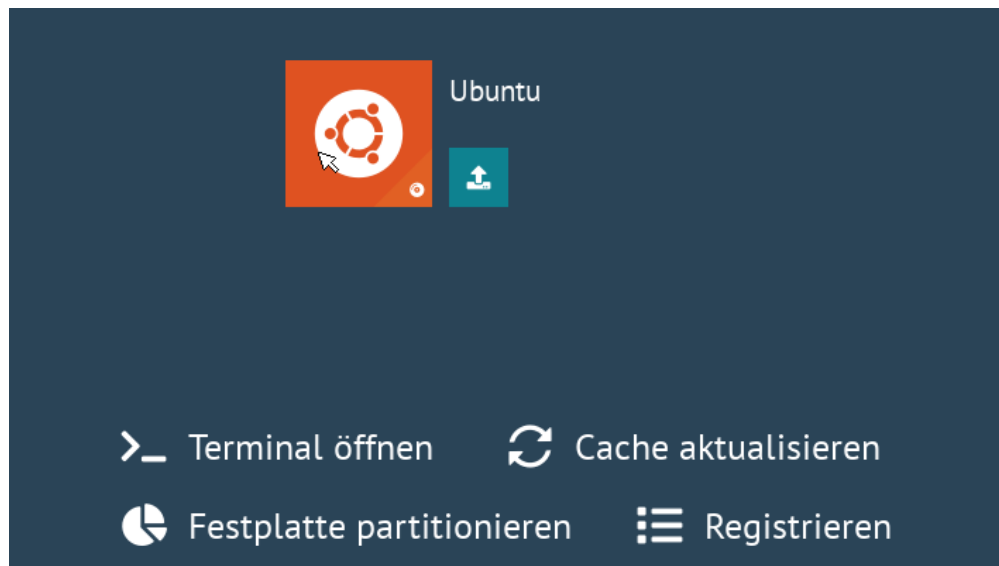


Abb. 278: Werkzeug-Menü



Abb. 279: Imaging-Symbol Ubuntu

Anstatt des Festplatten-Symbol wird bei Dir eventuell das Symbol des Betriebssystems angezeigt, dass Du in der WebUI festgelegt hast.

Es wird ein neues Fenster geöffnet:

Gibt es das Image noch nicht, so wird ein neues Image mit dem zuvor in der WebUI festgelegten Namen erstellt. Sollte ein Image bereits vorhanden sein, so wird dieses überschrieben. Soll ein neuer Dateiname für das neue Image festgelegt werden, so muss dies zuerst in der WebUI in der Hardwareklasse festgelegt und ein neuer Import ausgeführt werden.

Klicke nun **erstellen + hochladen**.

Während des Vorgangs siehst Du nachstehenden Bildschirm:

Zum Abschluss erscheint die Meldung, dass das Image erfolgreich hochgeladen wurde.

Gehe durch einen Klick auf das Zeichen < zurück und klicke im nächsten Bildschirm das obere Symbol auf der rechten Seite an, um Dich abzumelden.

Du siehst nun drei Start-Symbole. Der grosse Symbol started das Image synchronisiert, während das grüne Icon das lokale Image aus dem Cache ohne Synchronisation startet.

Starte nun Ubuntu synchronisiert.

Paket linuxmuster-linuxclient7 installieren

Melde Dich an dem gestarteten Ubuntu 22.04 als Benutzer `linuxadmin` an.

Installiere das Paket `linuxmuster-linuxclient7` wie folgt:

1. Importiere den GPG-Schlüssel des linuxmuster.net Respository.
2. Trage das linuxmuster.net Repository ein.
3. Installiere das Paket

Image erstellen

Auszuführende Aktion:

☒ Neues Basisimage erstellen

☐ Neues differentielles Image erstellen

Image Beschreibung:

Ubuntu 22.04 LTS Basisinstallation

Was soll nach dem Ende des Prozesses passieren?

☒ nichts

☐ herunterfahren

☐ neu starten

☐ abmelden

erstellen

erstellen + hochladen

abbrechen

Abb. 280: Image erstellen



Abb. 281: Imageerstellung

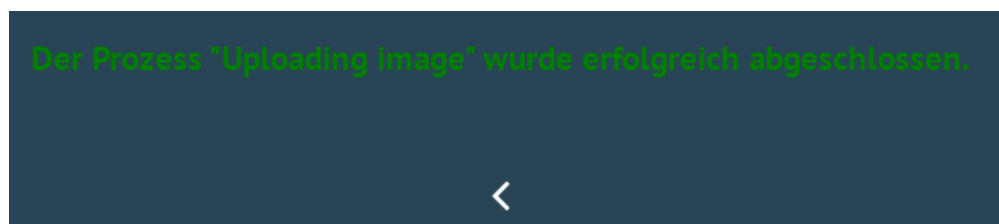


Abb. 282: Image wurde erfolgreich erstellt und auf den Server geladen

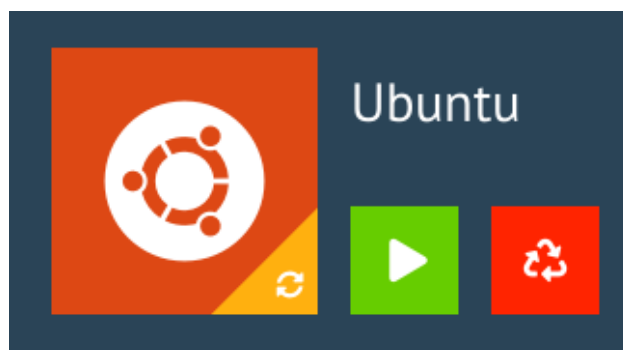


Abb. 283: LINBO Start-Symbole

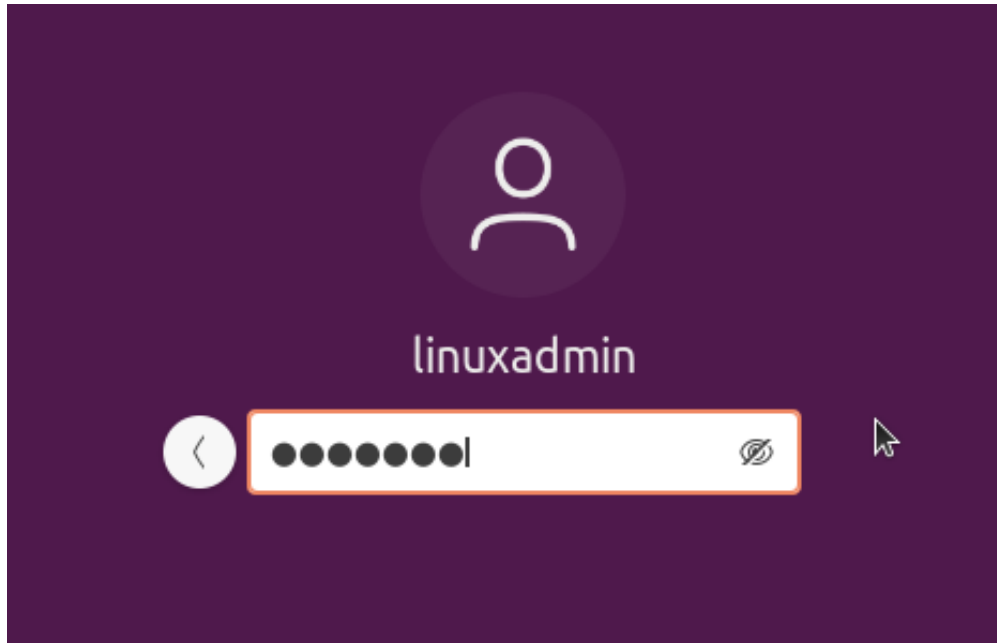


Abb. 284: Anmelden als Benutzer linuxadmin

1. Schritt

Öffne ein Terminal unter Ubuntu mit `strg + T` oder klicke unten links auf die Kacheln und gib in der Suchzeile als Anwendung `Terminal` ein.

Importiere nun den GPG-Schlüssel des linuxmuster.net Repository:

```
sudo sh -c 'wget -qO- "https://deb.linuxmuster.net/pub.gpg" | gpg --dearmor -o /usr/  
↪share/keyrings/linuxmuster.net.gpg'
```

2. Schritt

Trage das linuxmuster.net Repository in die Paketquellen des Clients ein:

```
sudo sh -c 'echo "deb [arch=amd64 signed-by=/usr/share/keyrings/linuxmuster.net.gpg]   
↪https://deb.linuxmuster.net/ lmn71 main" > /etc/apt/sources.list.d/lmn71.list'
```

Aktualisiere die Paketinformationen mit `sudo apt update`.

3. Schritt

Führe die Installation des Pakets mit `sudo apt install linuxmuster-linuxclient7 -y` durch.

Es kommt während der Paketinstallation die Nachfrage, welches voreingestellte Realm für Kerberos 5 zu verwenden. Dieser Eintrag bleibt leer.

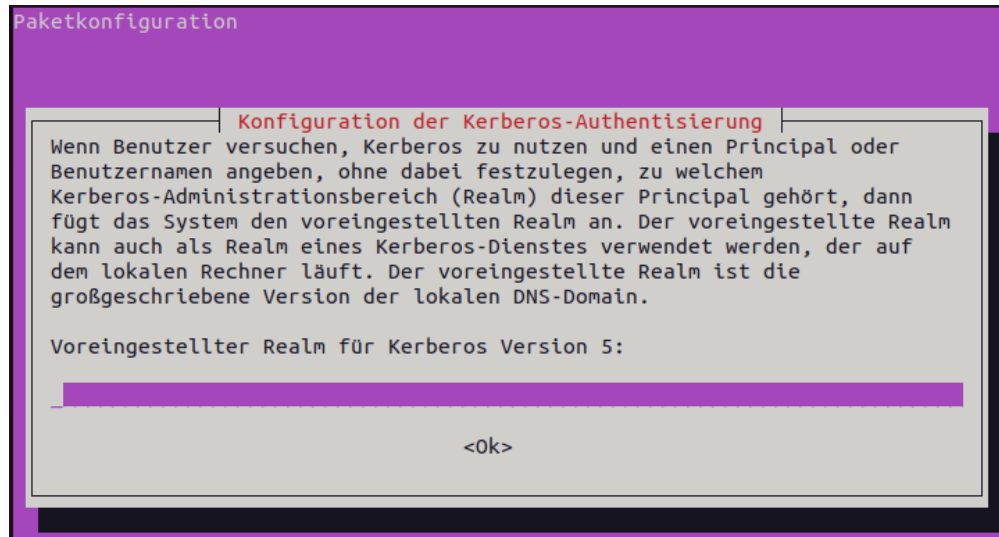


Abb. 285: Paketkonfiguration

Lasse das Feld leer und bestätige die Paketkonfiguration mit OK.

Setup

Um den Domänenbeitritt auszuführen, rufe das Setup des `linuxmuster-linuxclient7` auf:

```
sudo linuxmuster-linuxclient7 setup
```

Für den Domänenbeitritt wird das Kennwort des Domänen-Admins `global-admin` abgefragt.

Am Ende des Domänenbeitritts erfolgt eine Bestätigung, dass dieser erfolgreich durchgeführt wurde. Falls nicht, musst Du das Setup für den `linuxmuster-linuxclient7` erneut durchlaufen.

Image vorbereiten

Der Linux-Client muss nun für die Erstellung des Images vorbereitet werden. Rufe hierzu den Befehl auf:

```
sudo linuxmuster-linuxclient7 prepare-image -y
```

Der Client erhält dadurch Aktualisierungen und es werden einige Dateien (`journalctl` & `apt-caches`) aufgeräumt, um Speicherplatz im Image zu sparen.

Achtung: Danach unbedingt **S O F O R T** ein neues Image mit Linbo erstellen. Beim Neustart via PXE darf Ubuntu **N I C H T** gestartet werden.

Image erstellen

Führe einen Neustart des Linux-Client durch, sodass die VM via PXE in Linbo bootet.

Nun erstellst Du in Linbo - genauso wie zuvor unter **Erstimage erstellen** beschrieben - das Image des neuen Muster-Clients für Linux. Das bisherige Image wird dadurch ersetzt. Wähle **erstellen** + **hochladen**.

Wurde der Vorgang erfolgreich beendet, kannst Du Dich wieder abmelden und den vorbereiteten Linux-Client synchronisiert starten. Nun sollte die Anmeldung mit jedem in der Schulkonsole eingetragenen Benutzer funktionieren.

Eigene Anpassungen im Image

Um den Linux-Client als Mustervorlage zu aktualisieren und Anpassungen vorzunehmen, startest Du den Client synchronisiert und meldest Dich mit dem Benutzer **linuxadmin** an.

Danach installierst Du die benötigte Software und nimmst die gewünschten Einstellungen vor.

Beispielsweise installierst Du auf dem Linux-Client zuerst Libre-Office:

```
sudo apt update
sudo apt install libreoffice
```

Hast Du alle Anpassungen vorgenommen, musst Du den Linux-Client noch zur Erstellung des Images vorbereiten.

Das machst Du mit folgendem Befehl:

```
sudo linuxmuster-linuxclient7 prepare-image
```

Achtung: Falls Du die history Deines Terminals nutzt um Befehle wieder zu nutzen, dann achte darauf das Du den Parameter **-y** entfernst.

Sollte während des Updates oder der Image-Vorbereitung die Meldung erscheinen, dass lokale Änderungen der PAM-Konfiguration außer Kraft gesetzt werden sollen, wähle hier immer **Nein** (siehe Abb.), da sonst der konfigurierte Login nicht mehr funktioniert.

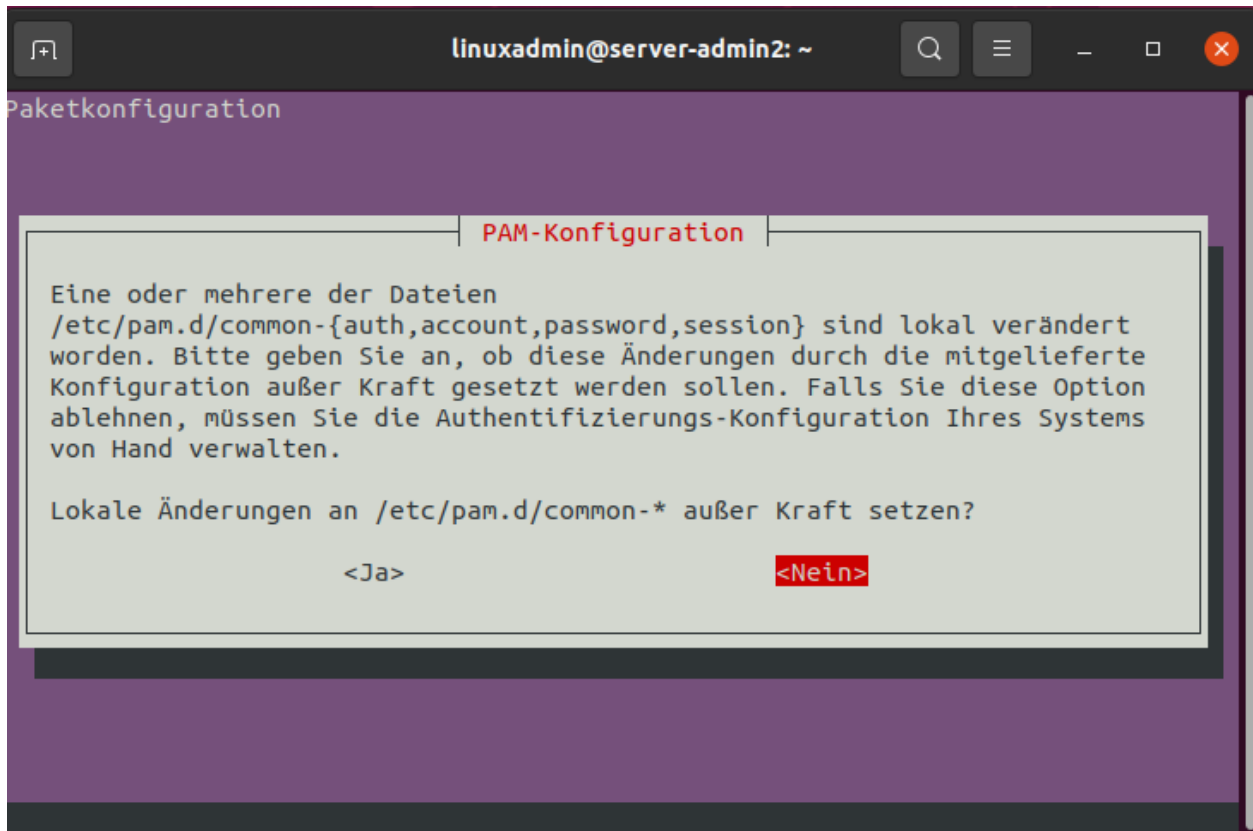
Solltest Du versehentlich **ja** ausgewählt haben, kannst Du die Anmeldung mit folgendem Befehl reparieren:

```
sudo linuxmuster-linuxclient7 upgrade
```

Im Anschluss startest Du Deinen Linux-Client neu und erstellst wiederum, wie zuvor beschrieben, ein neues Image.

Serverseitige Anpassungen

Damit der Linux-Client die Drucker automatisch ermittelt und der Proxy korrekt eingerichtet wird, ist es erforderlich, dass auf dem linuxmuster.net Server einige Anpassungen vorgenommen werden.



Proxy-Einstellungen

Bei der Anmeldung vom Linux-Client werden sog. Hook-Skripte ausgeführt.

Diese finden sich auf dem linuxmuster.net Server im Verzeichnis: `/var/lib/samba/sysvol/linuxmuster.lan/scripts/default-school/custom/linux/`.

Hinweis: Ersetze `linuxmuster.lan` durch den von Dir beim Setup festgelegten Domännennamen.

Hier findet sich das Logon-Skript (`logon.sh`). Es wird immer dann ausgeführt, wenn sich ein Benutzer am Linux-Client anmeldet.

In diesem Logon-Skript musst Du die Einstellungen für den zu verwenden Proxy-Server festlegen, sofern dieser von den Linux-Clients verwendet werden soll.

Editire die Datei `/var/lib/samba/sysvol/linuxmuster.lan/scripts/default-school/custom/linux/logon.sh` und füge folgende Zeilen hinzu. Passe die `PROXY_DOMAIN` für Dein Einsatzszenario an.

```
PROXY_DOMAIN=linuxmuster.lan #change it to your DOMAIN
PROXY_HOST=http://firewall.$PROXY_DOMAIN
PROXY_PORT=3128

# set proxy via env (for Firefox)
lmn-export no_proxy=127.0.0.0/8,10.0.0.0/8,192.168.0.0/16,172.16.0.0/12,localhost,.local,
↪.$PROXY_DOMAIN
lmn-export http_proxy=$PROXY_HOST:$PROXY_PORT
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
lmn-export ftp_proxy=$PROXY_HOST:$PROXY_PORT
lmn-export https_proxy=$PROXY_HOST:$PROXY_PORT

# set proxy gconf (for Chrome)
gsettings set org.gnome.system.proxy ignore-hosts "['127.0.0.0/8','10.0.0.0/8','192.168.
↪0.0/16','172.16.0.0/12','localhost','.local','.$PROXY_DOMAIN']"
gsettings set org.gnome.system.proxy mode "manual"
gsettings set org.gnome.system.proxy.http port "$PROXY_PORT"
gsettings set org.gnome.system.proxy.http host "$PROXY_HOST"
gsettings set org.gnome.system.proxy.https port "$PROXY_PORT"
gsettings set org.gnome.system.proxy.https host "$PROXY_HOST"
gsettings set org.gnome.system.proxy.ftp port "$PROXY_PORT"
gsettings set org.gnome.system.proxy.ftp host "$PROXY_HOST"
```

Drucker vorbereiten

Hinweis: Dies sind nur kurze allgemeine Hinweise. Im Kapitel *Drucker einbinden* findet sich eine ausführliche Anleitung.

Damit die Drucker richtig gefunden und via GPO administriert werden können, ist es erforderlich, dass jeder Drucker im CUPS-Server als Namen exakt seinen Hostnamen aus der Geräteverwaltung bekommt.

Die Zuordnung von Druckern zu Computern geschieht auf Basis von Gruppen im Active Directory. Im Kapitel *Drucker einbinden* gibt es weitere Informationen dazu.

Damit auf jedem Rechner nur die Drucker angezeigt werden, die ihm auch zugeordnet wurden, muss auf dem Server in der Datei `/etc/cups/cupsd.conf` der Eintrag `Browsing On` auf `Browsing Off` umgestellt werden. Ansonsten werden auf jedem Rechner ALLE Drucker angezeigt, nicht nur die ihm zugeteilt.

Weiterführende Dokumentation

- [Entwicklerdokumentation](#)
- *LINBO4 nutzen*

Linux-Client: pop!os

Autor des Abschnitts: @cweikl

Hast Du alle Vorarbeiten wie im Kapitel *Linux-Client* ausgeführt, startest Du nun den PC/die VM von CD/DVD/USB-Stick mit pop!os.

Hinweis: Die ISO-Datei zur Erstellung des Installationsmediums findest Du unter: <https://pop.system76.com>
z.B. https://iso.pop-os.org/22.04/amd64/intel/35/pop-os_22.04_amd64_intel_35.iso

Zur Erinnerung - folgende Vorarbeiten sollten bereits erledigt sein:

1. Lege in der WebUI unter LINBO4 eine neue Hardwareklasse (HWK) an.
2. Vergebe für die HWK einen eindeutigen Namen.

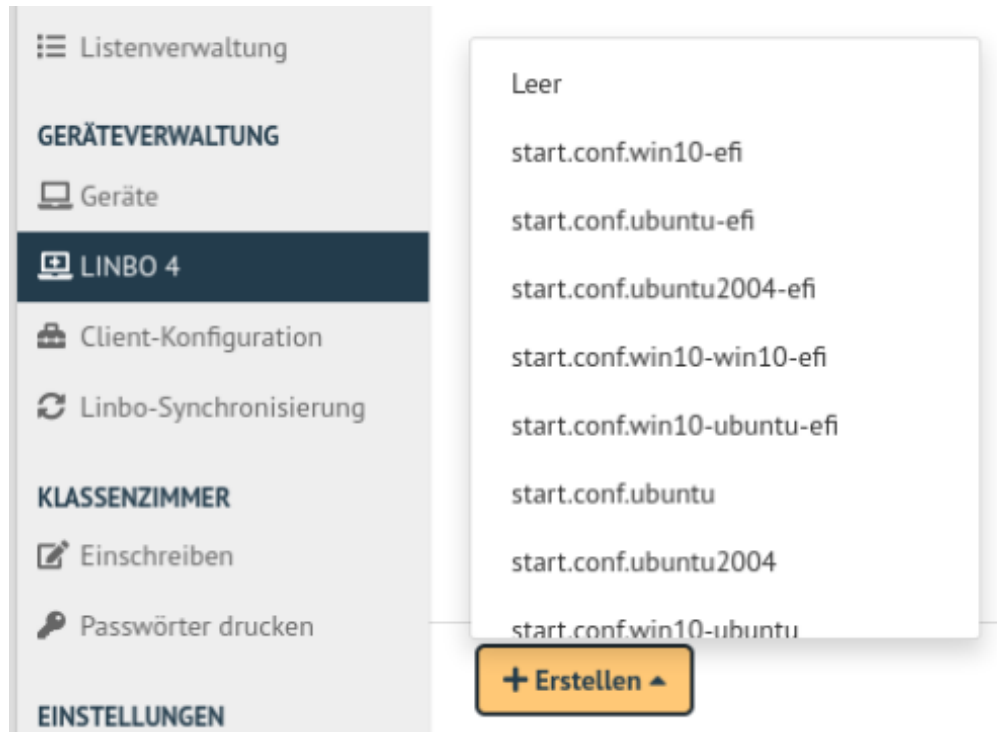


Abb. 286: Hardwareklasse hinzufügen



Abb. 287: Name der HWK festlegen

3. Editiere die Eintragungen für die HWK, in dem Du auf das Stift-Symbol klickst.
4. Trage unter der Reiterkarte Allgemein die Server IP sowie den Systemtyp ein.
5. Gebe auf der Reiterkarte Partitionen die erforderlichen Partitionen EFI (für UEFI-Systeme - mind 1 GiB), pop!os, cache und swap an. Die Größenangaben richten sich nach Deinen Anforderungen und sollten i.d.R. größer sein als auf der Abbildung.

Hinweis: Bei pop!os sollte darauf geachtet werden, dass bei UEFI-System die EFI-Partition eine Größe von mind. 1 GiB aufweist!

6. Bearbeite die Partition pop!os mit dem Stift und gebe auf der Reiterkarte OS einen eindeutigen Namen an. Lege den Namen für das Basisimage fest. Dies erreichst Du über das +-Symbol und der Angabe eines neuen Namens, der auf .qcow2 enden muss. Danach kannst Du diesen aus der Dropdown-Liste auswählen.

Nutzt Du ein UEFI-System, so musst Du für pop!os die Einträge für Kernel und initrd anpassen, die auf das Verzeichnis boot/ verweisen, das auf der EFI-Partition liegt.




Gruppen	Abbilder	
Gruppenname	Verwendete Images	Aktionen
pop-os-22-04-lts		  

Abb. 288: HWK editieren

pop-os-22-04-lts

Allgemein Partitionen

TFTP Server
10.0.0.1

Administrator wegen Zeitlimit ausgeloggt
600

Systemtyp
UEFI 64Bit

Download Typ
torrent

Startoptionen
☐ Beim Start partitionieren
☐ Beim Start formatieren
☐ Beim Start Cache aktualisieren

Linbo GUI Anpassung
☐ Minimales Layout verwenden
☒ Clientdetails standardmäßig anzeigen

Sprache
Deutsch

Hintergrundfarbe
Die Farbe des Vordergrunds wird automatisch angepasst

Kernel-Optionen
linux splash

Speichern

Schließen

pop-os-22-04-lts

Allgemein Partitionen

Disk Type

SATA

/dev/sda

efi 2.0 GB	pop/los 18.0 GB	cache 18.0 GB
swap 4.0 GB		
+ EFI	+ MSR	Windows Linux + Swap + Daten + Erweitert + Cache

+ Neue Festplatte

Speichern Schließen

Abb. 289: Allgemeine Einstellungen der HWK

/dev/sda2


Partition	OS
Name	Version
pop!os	22.04 LTS
Standard Start	Symbol
Sync & start	
Basisimage	
popos2202.qcow2	
+	

Abb. 290: Partitionen festlegen

7. Gebe in der WebUI für diesen PC als Gruppe die neu angelegte HWK - hier pop-os-22-04-lts - an und klicke auf **Speichern & importieren**.
8. Starte danach den Client via PXE und LINBO.
9. Klicke auf das Werkzeugsymbol, authentifiziere Dich mit dem Kennwort des LINBO-Admins (dieses siehst Du bei der Eingabe nicht - auch keine Sternchen).
10. In der sich öffnenden Anzeige klicke auf den Eintrag **Festplatte partitionieren**.
11. Gehe nach erfolgreicher Ausführung mit dem Pfeil-Symbol zurück und schalte danach den Client aus.
12. Stelle die Bootreihenfolge auf dem Client so um, dass dieser nun vom pop!os Installationsmedium startet.

Installation pop!os

Nach dem Start von dem Installationsmedium erhältst Du den Hinweis, dass pop!os gestartet wird. Es kann einige Zeit dauern, bis Du den grafischen Installations-Bildschirm siehst.

Wähle die gewünschte Sprache und bestätige dies mit **Select**.

Wähle die gewünschte Tastaturbelegung. Diese kannst Du im Eingabefeld testen. Bestätige Deine Wahl mit **Auswählen**.

Die Partitionen auf Deinem Muster-Client sind bereits mit LINBO angelegt worden, so dass Du hier die Option **Custom (Advanced)** auswählst und bestätigst.

Du gelangst zu nachstehendem Bildschirm, in dem Deine bisherigen Partitionen angezeigt werden.

Du hattest mit LINBO bereits die Festplatte partitioniert und formatiert.

Es werden Dir die bereits vorhandenen Partitionen und Dateisysteme angezeigt. Je nach genutzter Virtualisierungsumgebung / Hardware können die Festplattenbezeichnungen hier auch als `/dev/vda` und die Partitionen als `/dev/vda1`

/dev/sda2

Partition

OS

Name

pop!os

Version

22.04 LTS

Standard Start

Sync & start



Symbol



Basisimage

popos2202.qcow2



Start Optionen



Start



Sync & start



New start



Autostart

Kernel

boot/vmlinuz

Initrd

boot/initrd.img

Raum	Rechnername	Gruppe	MAC	IP	Sophomore-Rolle	PXE
a001	a00101	pop-os-22-04-ltd	52:54:00:a1:c6:c	10.0.1.1	Schüler-PC im Klassenzimmer	Linbo-PXE

Abb. 291: Gerät der HWK zuordnen und importieren

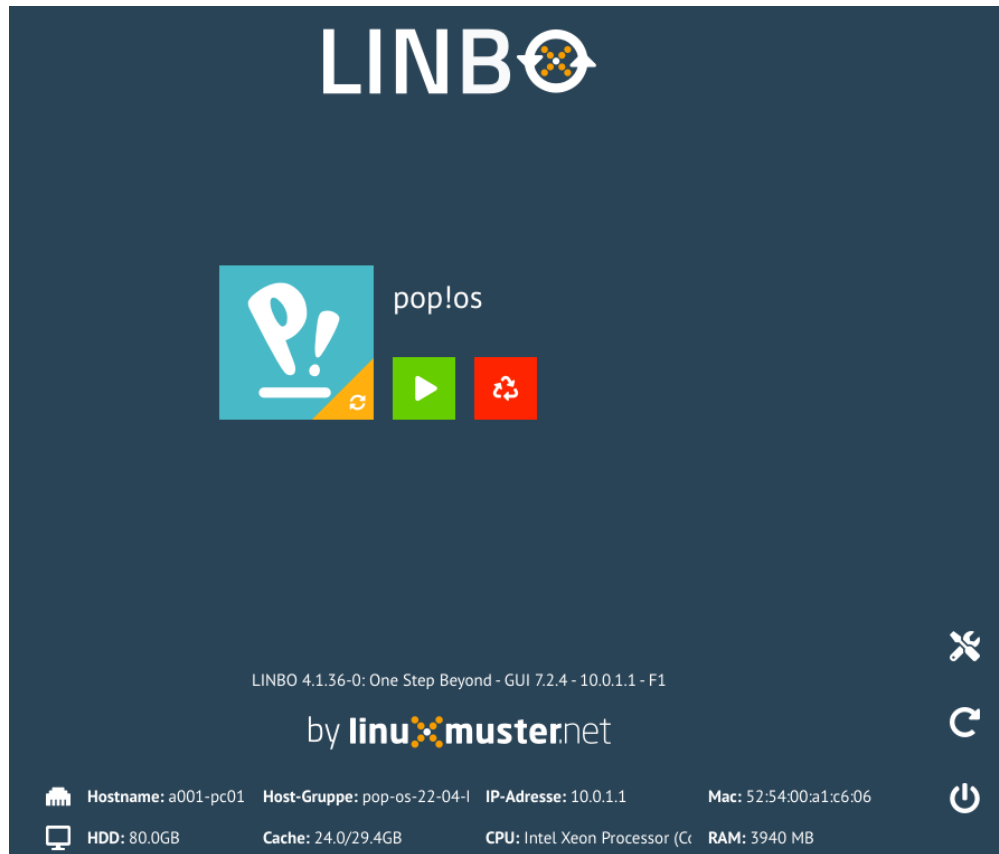


Abb. 292: LINBO Startbildschirm pop!os



Abb. 293: LINBO Werkzeugleiste - Menüeinträge für pop!os

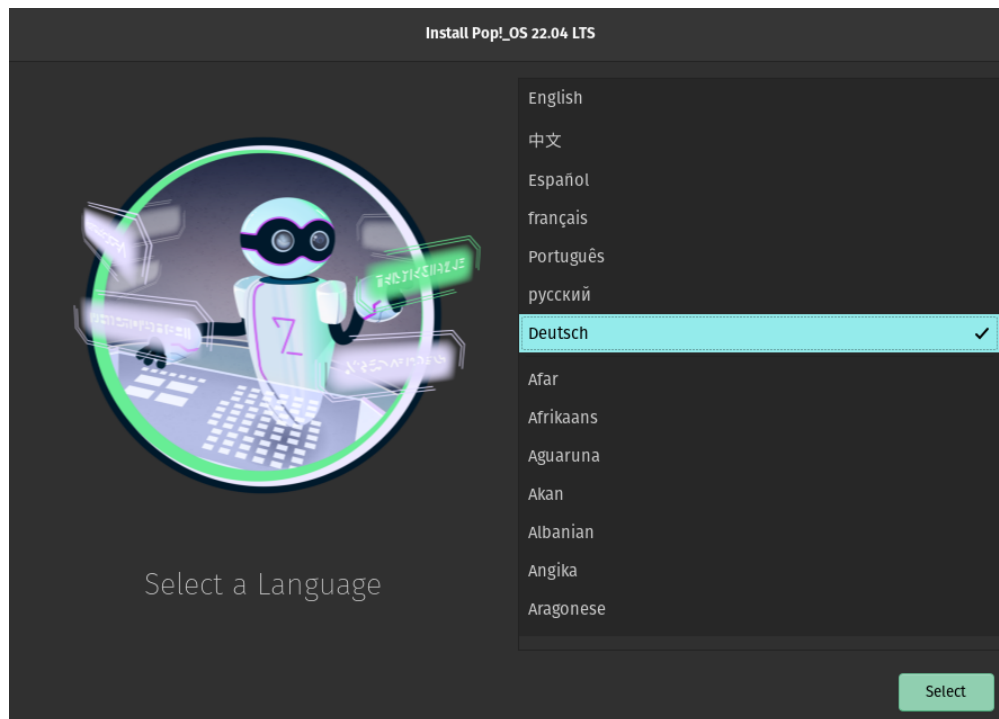


Abb. 294: Sprache auswählen



Abb. 295: Tastaturlayout festlegen

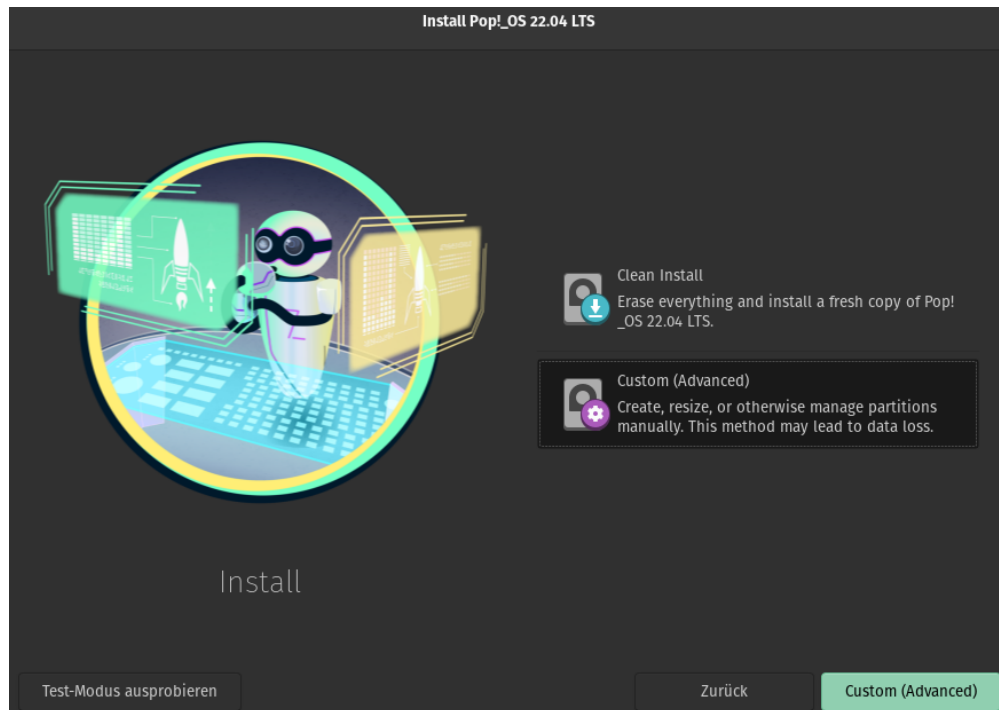


Abb. 296: Installationsart wählen



Abb. 297: Partitionsübersicht

etc. angezeigt werden.

Markiere zunächst Die EFI-Partition (gelb) und lege fest, dass diese Partition verwendet werden soll.

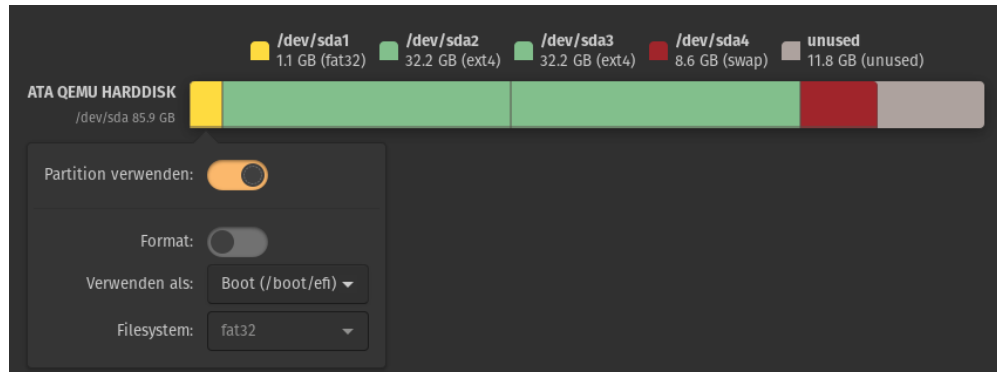


Abb. 298: EFI-Partition aktivieren

Diese soll unter pop!os als /boot/efi Boot-Partition eingehangen, aber **N I C H T** formatiert werden.

Klicke danach auf die pop!os-Partition und binde diese als Root-Partition (/) ein. Diese ist ebenfalls nicht zu formatieren.

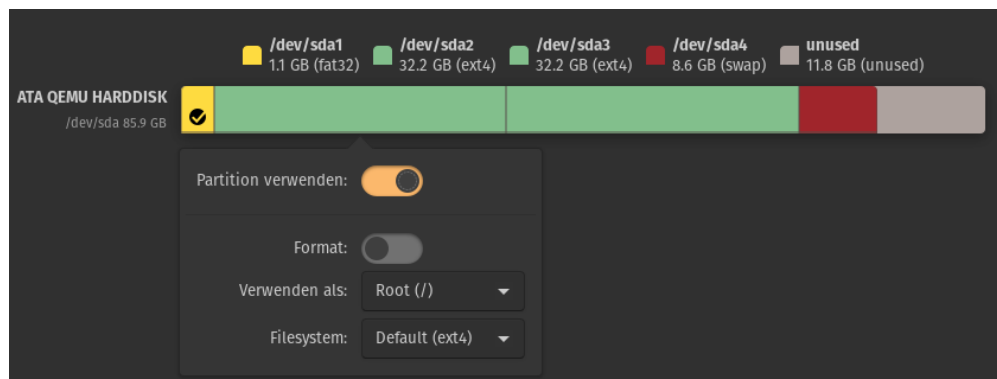


Abb. 299: Partition für pop!os einhängen

Klicke abschliessend auf die SWAP-Partition (rot) und binde diese als Swap ein.

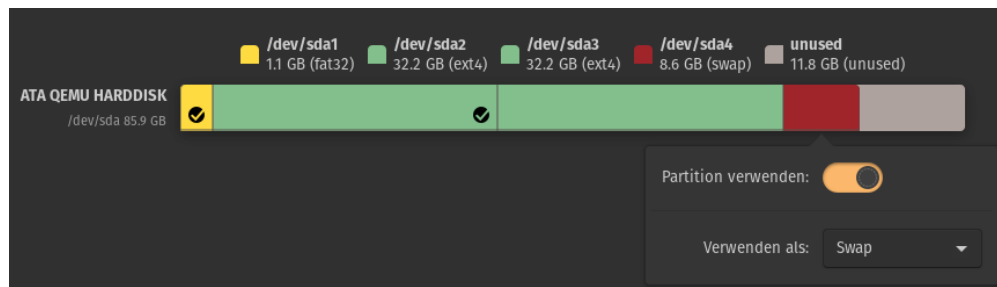


Abb. 300: SWAP-Partition einhängen

Danach siehst Du Deine eingebundenen Partitionen, die jeweils mit einem Häkchen gekennzeichnet sind.

Starte die Installation mit dem Button **Löschen** und **installieren**.

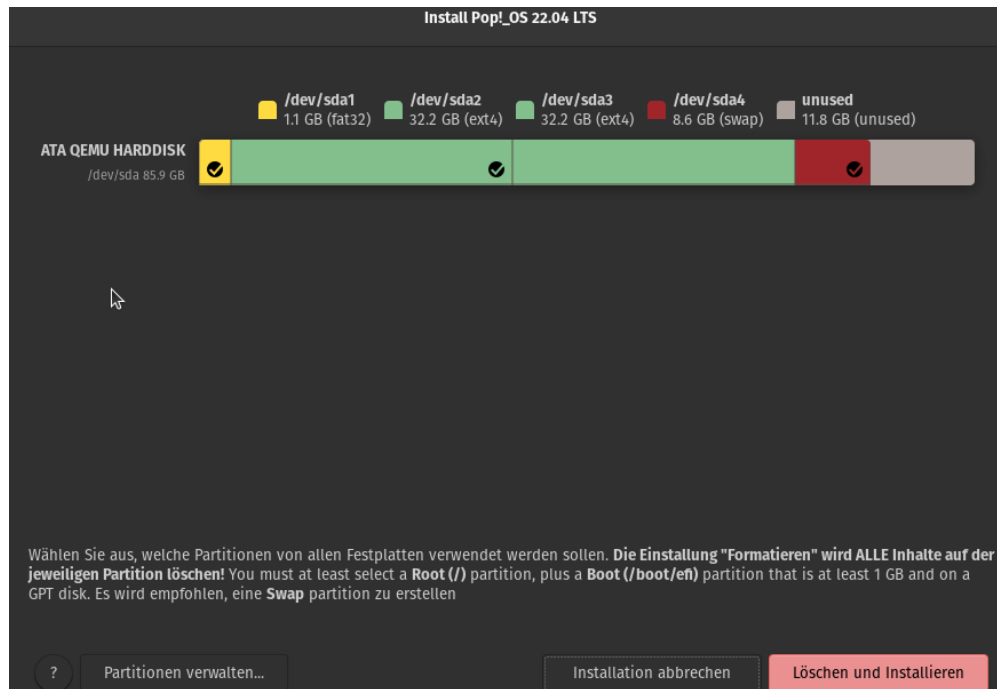


Abb. 301: Übersicht der Partitionen

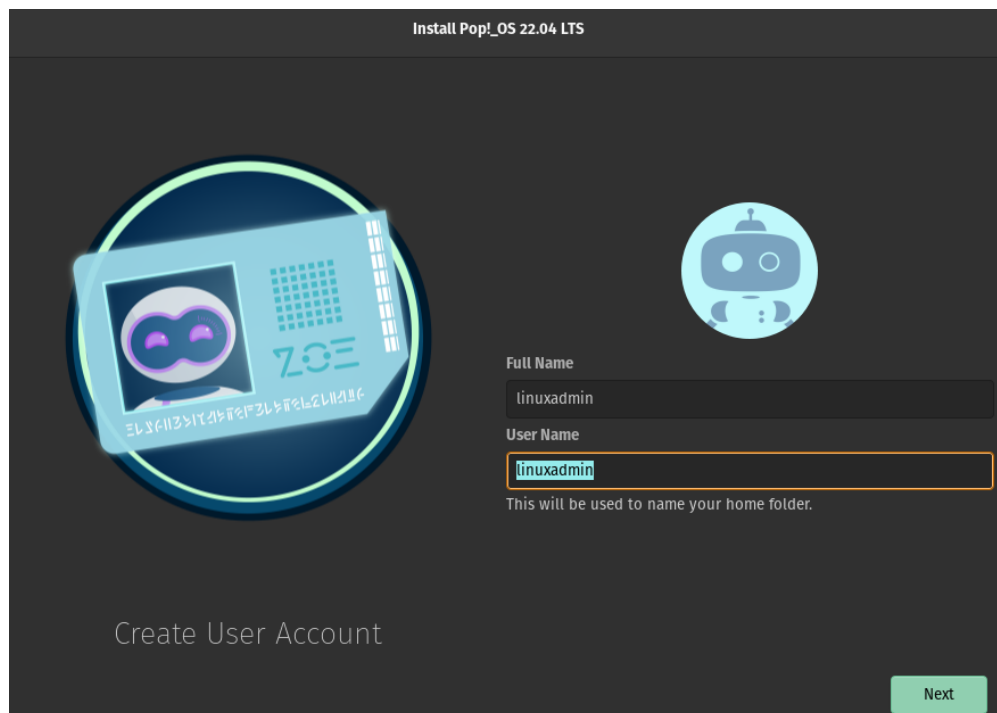


Abb. 302: Neuen Benutzer linuxadmin anlegen

Danach musst Du noch einen neuen Benutzer `linuxadmin` festlegen.

Lege für den neuen Benutzer ein Kennwort fest, das mind. 8 Zeichen aufweist.

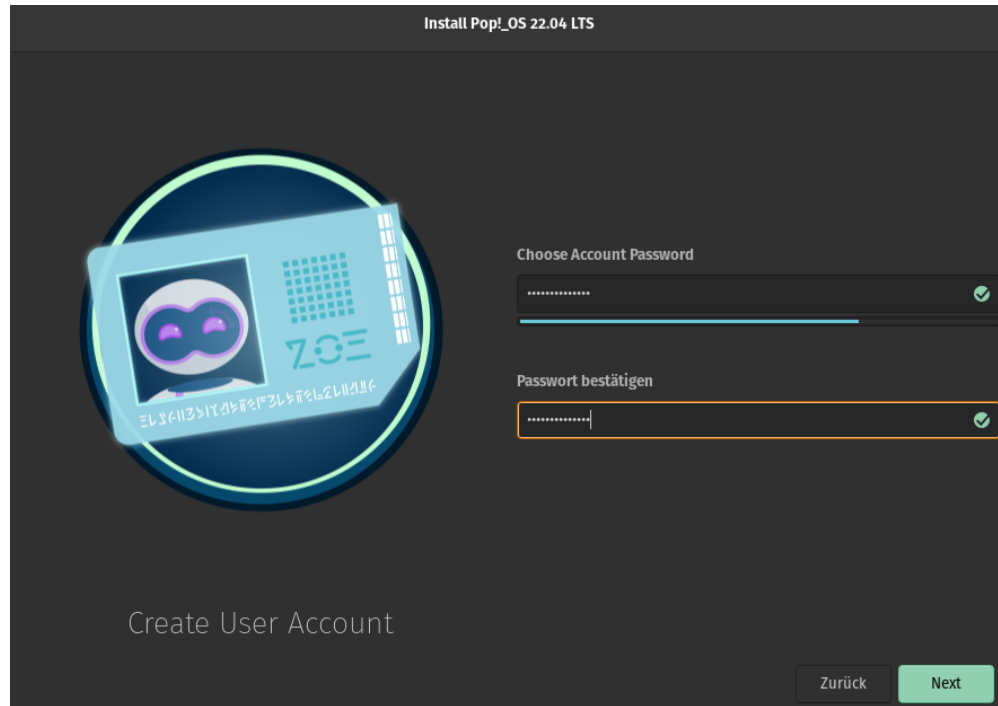


Abb. 303: Kennwort für `linuxadmin` festlegen

Bestätige dies mit **Next**. Danach startet die Installation.

Gelangst Du nach erfolgreicher Installation zum Abschluss-Bildschirm, so wähle hier **Herunterfahren** aus.

Werfe das Installationsmedium aus.

Erstimage erstellen

Passe die Boot-Reihenfolge für den PC / die VM jetzt so an, dass wieder via PXE/LINBO gebootet wird. Du siehst dann die Startoptionen in Linbo für das installierte pop!os.

Klicke nun unten rechts auf das Werkzeug-Icon, um zum Menü für die Imageerstellung zu gelangen.

Du wirst nach dem Linbo-Passwort gefragt. Gib dieses ein.

Achtung: Deine Eingabe wird hierbei nicht angezeigt.

Klicke dann auf **anmelden** und Du gelangst zu folgender Ansicht:

Klicke auf das große Festplatten-Symbol, das in der Ecke rechts unten farblich markiert ist, um nun ein Image zu erstellen. Anstatt des Festplatten-Symbols wird bei Dir eventuell das Symbol des Betriebssystems angezeigt, dass Du in der WebUI festgelegt hast.

Es wird ein neues Fenster geöffnet:

Starte den Vorgang mit **erstellen & hochladen**.

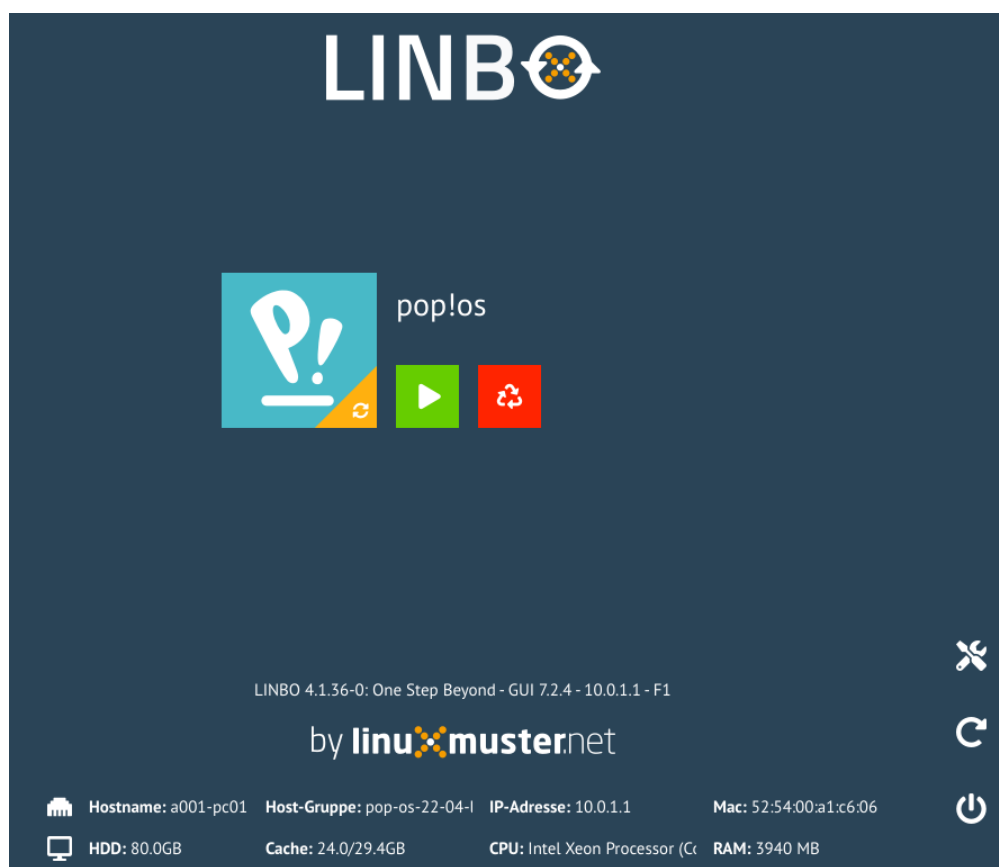


Abb. 304: LINBO Startbildschirm für pop!os

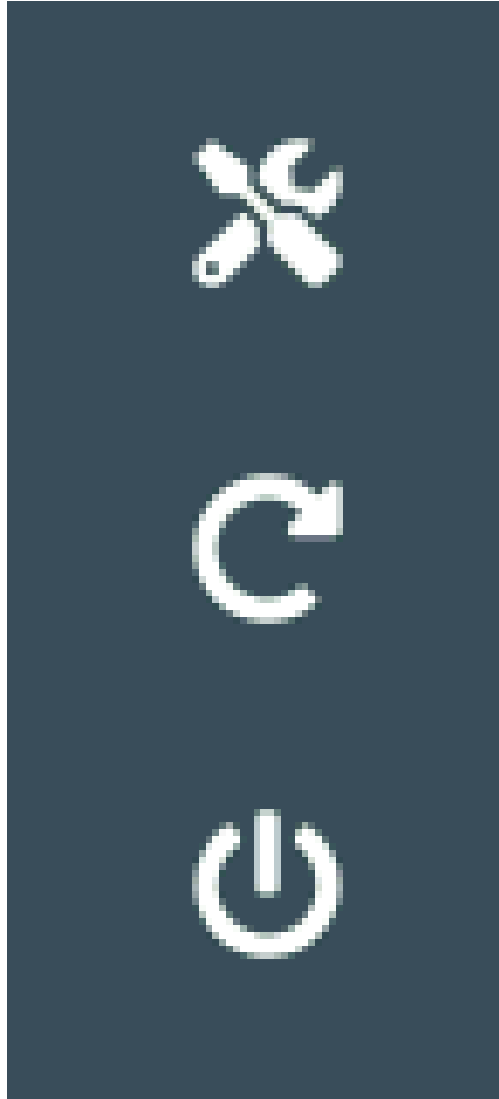


Abb. 305: Werkzeugleiste

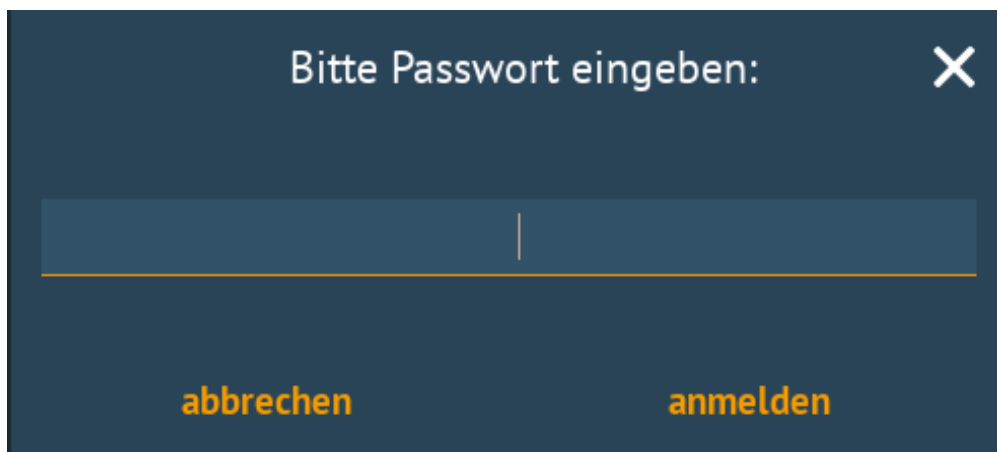


Abb. 306: LINBO Kennwort eingeben



Abb. 307: Menü Werkzeugleiste

Gibt es das Image noch nicht, so wird ein neues Image mit dem zuvor in der WebUI festgelegten Namen erstellt. Ansonsten wird das bestehende Image überschrieben.

Während des Vorgangs siehst Du nachstehenden Bildschirm:

Zum Abschluss erscheint die Meldung, dass das Image erfolgreich hochgeladen wurde.

Gehe durch einen Klick auf das Zeichen < zurück und melde Dich ab.

Rufst Du mit der WebUI den Menüpunkt **Geräteverwaltung** --> **LINB04** auf, siehst Du Deine HWK. Klickst Du hier auf die Reiterkarte **Abbilder**, wird das soeben erstellte Image angezeigt.

Klickst Du hier auf das Zahnrad-Symbol siehst Du weitere Informationen zu dem erstellten Image.

Wichtige Hinweise

pop!os versucht während der Installation für die EFI-Partition und für die SWAP-Partition diese mithilfe von UUIDs einzubinden. Startest Du das synchronisierte Image, so wird es einige Zeit bei einem grauen Bildschirm hängen bleiben. Danach erscheinen Fehlerhinweise und eine Notfallkonsole.

In der Notfallkonsole musst Du nun folgende Dateien

```
/etc/fstab
/etc/crypttab
```

auf dem Client korrigieren.

Die Datei `/etc/fstab` sollte folgende Einträge aufweisen:

```
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
```

(Fortsetzung auf der nächsten Seite)

Image erstellen

Auszuführende Aktion:

☒ Neues Basisimage erstellen

☐ Neues differentielles Image erstellen

Image Beschreibung:

pop!os 22.04 LTS

Aktualisiertes Image mit Domänenbeitritt

Was soll nach dem Ende des Prozesses passieren?

☒ nichts

☐ herunterfahren

☐ neu starten

☐ abmelden

erstellen

erstellen + hochladen

abbrechen

Abb. 308: Image erstellen

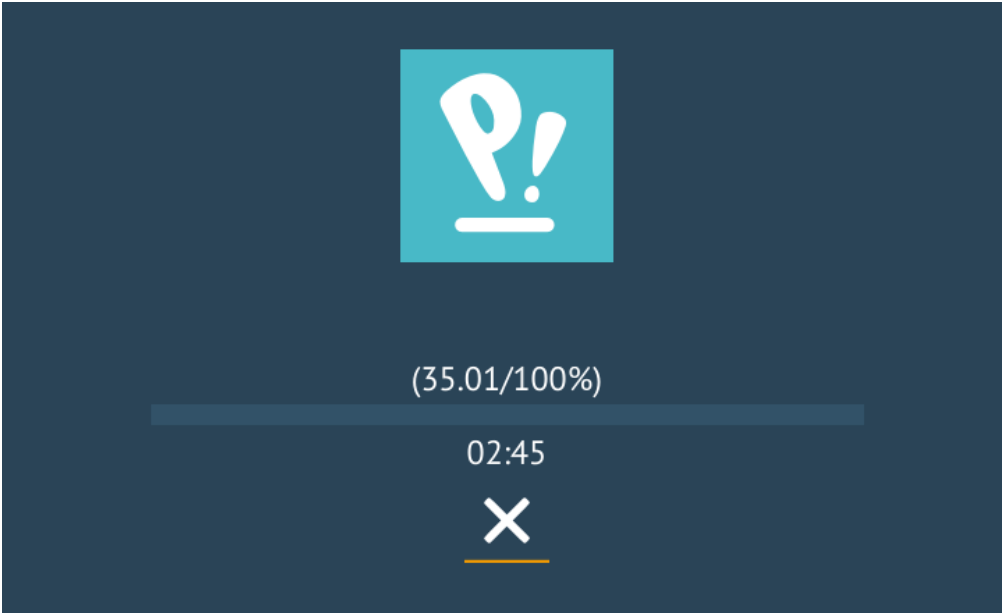


Abb. 309: Uploading Image



Abb. 310: Image erfolgreich hochgeladen

Gruppen		Abbilder	
Name	Differentielles Image	In Gruppe verwendet ...	Aktionen
<input type="checkbox"/> popos2202 3.6 GB	popos2202 1.4 GB	pop-os-22-04-lts	  
<input type="checkbox"/> ubuntu 3.5 GB	-	my-ubuntu-22-04-lts-muster-client	  

Abb. 311: Schulkonsole Abbilder

popos2202



Allgemein

Registry Patch

Postsync-Skript

Prestart Skript

Beschreibung

pop!os 22.04 LTS, aktualisiertes Image mit Domänenbeitritt

Info

```
["popos2202.qcow2" Info File]
timestamp="202310131652"
image="popos2202.qcow2"
imagesize="3881277440"
partition="/dev/sda2"
partitionsizesize="31457280"
```

Größe

3.6 GB

SPEICHERN

SCHLIESSEN

Abb. 312: Informationen zum Image

(Fortsetzung der vorherigen Seite)

```
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point> <type> <options> <dump> <pass>
/dev/sda1 /boot/efi vfat umask=0077 0 0
/dev/sda2 / ext4 noatime,errors=remount-ro 0 0
/dev/mapper/cryptswap none swap defaults 0 0
```

Ersetze hierbei Einträge wie PARTUUID=61bb910e-54ce-45e3-bd81-18f6f445d1d0 durch den Partitionseintrag /dev/sda1.

Die Datei /etc/crypttab sollte folgende Einträge aufweisen:

```
cryptswap /dev/sda4 /dev/urandom swap,plain,offset=1024,cipher=aes-xts-plain64,size=512
```

Hier musst Du ebenfalls UUID-Einträge durch die Angabe der SWAP-Partition ersetzen.

Fahre das System herunter. Starte den Client und starte diesen mithilfe der grünen Pfeiltaste, so dass nur das lokale System mit den soeben durchgeführten Anpassungen gestartet wird.

Danach solltest Du bis zum Login-Bildschirm kommen.

Paket linuxmuster-linuxclient7 installieren

Melde Dich an dem gestarteten pop!os 22.04 als Benutzer linuxadmin an.

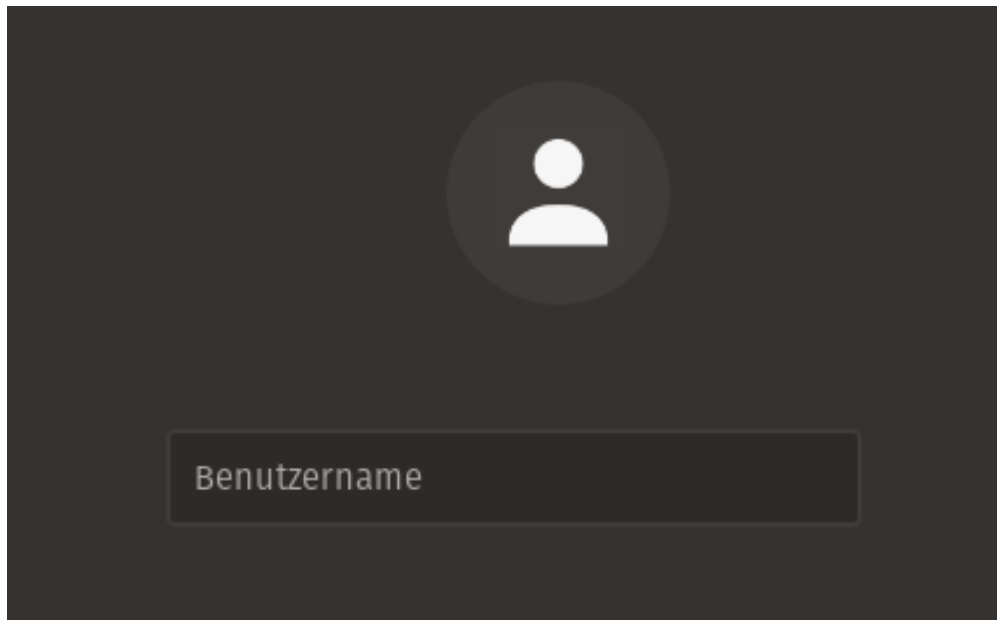


Abb. 313: Anmelden als Benutzer linuxadmin

Installiere das Paket linuxmuster-linuxclient7 wie folgt:

1. Importiere den GPG-Schlüssel des linuxmuster.net Respository.
2. Trage das linuxmuster.net Repository ein.
3. Installiere eine Library und das Paket

1. Schritt

Öffne ein Terminal unter Ubuntu mit `strg + T` oder klicke unten links auf die Kacheln und gib in der Suchzeile als Anwendung Terminal ein.

Importiere nun den GPG-Schlüssel des linuxmuster.net Repository:

```
sudo sh -c 'wget -qO- "https://deb.linuxmuster.net/pub.gpg" | gpg --dearmor -o /usr/share/keyrings/linuxmuster.net.gpg'
```

2. Schritt

Trage das linuxmuster.net Repository in die Paketquellen des Clients ein:

```
sudo sh -c 'echo "deb [arch=amd64 signed-by=/usr/share/keyrings/linuxmuster.net.gpg] https://deb.linuxmuster.net/ lmn71 main" > /etc/apt/sources.list.d/lmn71.list'
```

Aktualisiere die Paketinformationen mit `sudo apt update`.

3. Schritt

Installiere vorab eine Library mit `sudo apt install libsss-sudo -y`. Führe danach die Installation des Pakets mit `sudo apt install linuxmuster-linuxclient7 -y` durch.

Setup

Um den Domänenbeitritt auszuführen, rufe das Setup des linuxmuster-linuxclient7 auf:

```
sudo linuxmuster-linuxclient7 setup
```

Für den Domänenbeitritt wird das Kennwort des Domänen-Admins `global-admin` abgefragt.

Am Ende des Domänenbeitritts erfolgt eine Bestätigung, dass dieser erfolgreich durchgeführt wurde. Falls nicht, musst Du das Setup für den linuxmuster-linuxclient7 erneut durchlaufen.

Image vorbereiten

Der Linux-Client muss nun für die Erstellung des Images vorbereitet werden. Rufe hierzu den Befehl auf:

```
sudo linuxmuster-linuxclient7 prepare-image -y
```

Der Client erhält dadurch Aktualisierungen und es werden einige Dateien (`journalctl` & `apt-caches`) aufgeräumt, um Speicherplatz im Image zu sparen.

Achtung: Danach unbedingt **S O F O R T** ein neues Image mit Linbo erstellen. Beim Neustart via PXE darf Ubuntu **N I C H T** gestartet werden.

Image erstellen

Führe einen Neustart des Linux-Client durch, sodass die VM via PXE in Linbo bootet.

Nun erstellst Du in Linbo - genauso wie zuvor unter **Erstimage erstellen** beschrieben - das Image des neuen Muster-Clients für Linux.

Wurde der Vorgang erfolgreich beendet, kannst Du Dich wieder abmelden und den vorbereiteten Linux-Client synchronisiert starten. Nun sollte die Anmeldung mit jedem in der Schulkonsole eingetragenen Benutzer funktionieren.

Eigene Anpassungen im Image

Um den Linux-Client als Mustervorlage zu aktualisieren und Anpassungen vorzunehmen, startest Du den Client synchronisiert und meldest Dich mit dem Benutzer `linuxadmin` an.

Danach installierst Du die benötigte Software und nimmst die gewünschten Einstellungen vor.

Beispielsweise installierst Du auf dem Linux-Client zuerst Libre-Office:

```
sudo apt update
sudo apt install libreoffice
```

Hast Du alle Anpassungen vorgenommen, musst Du den Linux-Client noch zur Erstellung des Images vorbereiten.

Das machst Du mit folgendem Befehl:

```
sudo linuxmuster-linuxclient7 prepare-image
```

Achtung: Falls Du die history Deines Terminals nutzt um Befehle wieder zu nutzen, dann achte darauf das Du den Parameter `-y` entfernst.

Sollte während des Updates oder der Image-Vorbereitung die Meldung erscheinen, dass lokale Änderungen der PAM-Konfiguration außer Kraft gesetzt werden sollen, wähle hier immer **Nein** (siehe Abb.), da sonst der konfigurierte Login nicht mehr funktioniert.

Solltest Du versehentlich **ja** ausgewählt haben, kannst Du die Anmeldung mit folgendem Befehl reparieren:

```
sudo linuxmuster-linuxclient7 upgrade
```

Im Anschluss startest Du Deinen Linux-Client neu und erstellst wiederum, wie zuvor beschrieben, ein neues Image.

Serverseitige Anpassungen

Damit der Linux-Client die Drucker automatisch ermittelt und der Proxy korrekt eingerichtet wird, ist es erforderlich, dass auf dem linuxmuster.net Server einige Anpassungen vorgenommen werden.

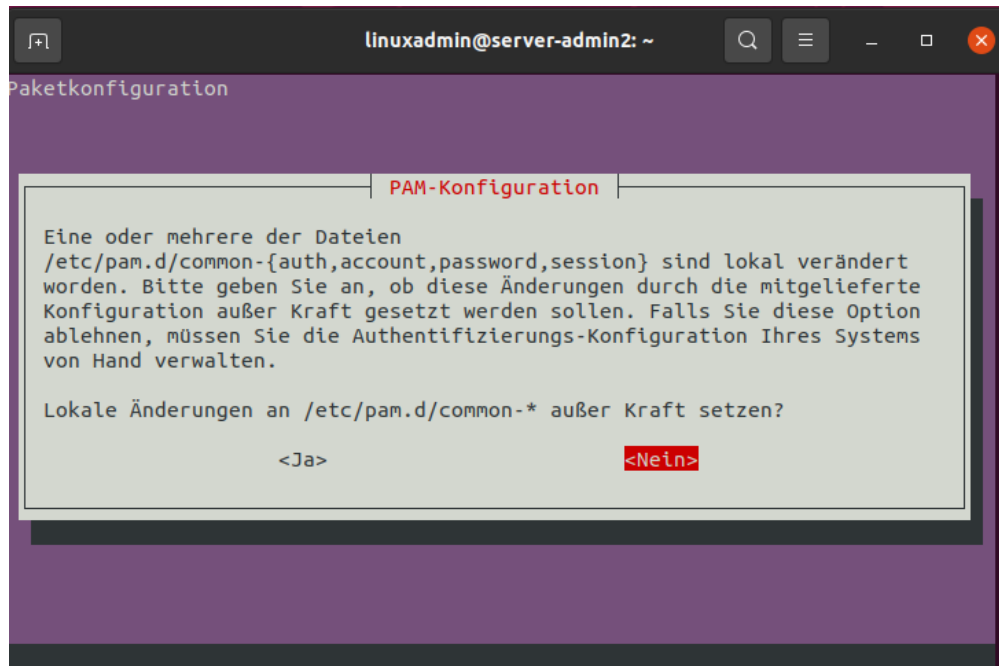


Abb. 314: PAM-Settings

Proxy-Einstellungen

Bei der Anmeldung vom Linux-Client werden sog. Hook-Skripte ausgeführt.

Diese finden sich auf dem linuxmuster.net Server im Verzeichnis: `/var/lib/samba/sysvol/gshoenningen.linuxmuster.lan/scripts/default-school/custom/linux/`.

Hinweis: Ersetze `gshoenningen.linuxmuster.lan` durch den von Dir beim Setup festgelegten Domänennamen.

Hier findet sich das Logon-Skript (`logon.sh`). Es wird immer dann ausgeführt, wenn sich ein Benutzer am Linux-Client anmeldet.

In diesem Logon-Skript musst Du die Einstellungen für den zu verwenden Proxy-Server festlegen, sofern dieser von den Linux-Clients verwendet werden soll.

Editiere die Datei `/var/lib/samba/sysvol/gshoenningen.linuxmuster.lan/scripts/default-school/custom/linux/logon.sh` und füge folgende Zeilen hinzu. Passe die `PROXY_DOMAIN` für Dein Einsatzszenario an.

```

PROXY_DOMAIN=gshoenningen.linuxmuster.lan #change it to your DOMAIN
PROXY_HOST=http://firewall.$PROXY_DOMAIN
PROXY_PORT=3128

# set proxy via env (for Firefox)
lmm-export no_proxy=127.0.0.0/8,10.0.0.0/8,192.168.0.0/16,172.16.0.0/12,localhost,.local,
↪ . $PROXY_DOMAIN
lmm-export http_proxy=$PROXY_HOST:$PROXY_PORT
lmm-export ftp_proxy=$PROXY_HOST:$PROXY_PORT
lmm-export https_proxy=$PROXY_HOST:$PROXY_PORT

```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
# set proxy gconf (for Chrome)
gsettings set org.gnome.system.proxy ignore-hosts "['127.0.0.0/8','10.0.0.0/8','192.168.
↪0.0/16','172.16.0.0/12','localhost','.local','.$PROXY_DOMAIN']"
gsettings set org.gnome.system.proxy mode "manual"
gsettings set org.gnome.system.proxy.http port "$PROXY_PORT"
gsettings set org.gnome.system.proxy.http host "$PROXY_HOST"
gsettings set org.gnome.system.proxy.https port "$PROXY_PORT"
gsettings set org.gnome.system.proxy.https host "$PROXY_HOST"
gsettings set org.gnome.system.proxy.ftp port "$PROXY_PORT"
gsettings set org.gnome.system.proxy.ftp host "$PROXY_HOST"
```

Drucker vorbereiten

Hinweis: Dies sind nur kurze allgemeine Hinweise. Im Kapitel *Drucker einbinden* findet sich eine ausführliche Anleitung.

Damit die Drucker richtig gefunden und via GPO administriert werden können, ist es erforderlich, dass jeder Drucker im CUPS-Server als Namen exakt seinen Hostnamen aus der Geräteverwaltung bekommt.

Die Zuordnung von Druckern zu Computern geschieht auf Basis von Gruppen im Active Directory. Im Kapitel *Drucker einbinden* gibt es weitere Informationen dazu.

Damit auf jedem Rechner nur die Drucker angezeigt werden, die ihm auch zugeordnet wurden, muss auf dem Server in der Datei `/etc/cups/cupsd.conf` der Eintrag `Browsing On` auf `Browsing Off` umgestellt werden. Andernfalls werden auf jedem Rechner ALLE Drucker angezeigt, nicht nur die ihm zugeteilt.

Appendix

Die HWK wird auf dem Server unter `/srv/linbo/start.conf.pop-os-22-04-lts` (Name für die hier dargestellte HWK) abgelegt.

Für die dargestellte Beispiel-HWK weist diese folgenden Inhalt auf:

```
[LINBO]
Server = 10.0.0.1
Group = pop-os-22-04-lts
Cache = /dev/sda3
RootTimeout = 600
AutoPartition = no
AutoFormat = no
AutoInitCache = no
GuiDisabled = no
UseMinimalLayout = no
Locale = de-DE
DownloadType = torrent
SystemType = efi64
KernelOptions = quiet splash
clientDetailsVisibleByDefault = yes

[Partition]
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
Dev = /dev/sda1
Label = efi
Size = 1G
Id = ef
FSType = vfat
Bootable = yes

[Partition]
Dev = /dev/sda2
Label = popos
Size = 30G
Id = 83
FSType = ext4
Bootable = no

[Partition]
Dev = /dev/sda3
Label = cache
Size = 30G
Id = 83
FSType = ext4
Bootable = no

[Partition]
Dev = /dev/sda4
Label = swap
Size = 8G
Id = 82
FSType = swap
Bootable = no

[OS]
Name = Pop!OS
Version = 22.04 LTS
Description = Ubuntu 20.04
IconName = debian.svg
Image =
BaseImage = popos2204.qcow2
Boot = /dev/sda2
Root = /dev/sda2
Kernel = boot/vmlinuz
Initrd = boot/initrd.img
Append = ro splash
StartEnabled = yes
SyncEnabled = yes
NewEnabled = yes
Autostart = no
AutostartTimeout = 5
DefaultAction = sync
Hidden = yes
```

In der WebUI kannst Du unter Geräteverwaltung --> Linbo-Synchronisierung die PC und die HWK Gruppen einsehen und hier sog. linbo-remote Befehle vom Server aus absetzen, die z.B. bewirken, dass der PC a00101

ausgeschaltet (Halt) wird.

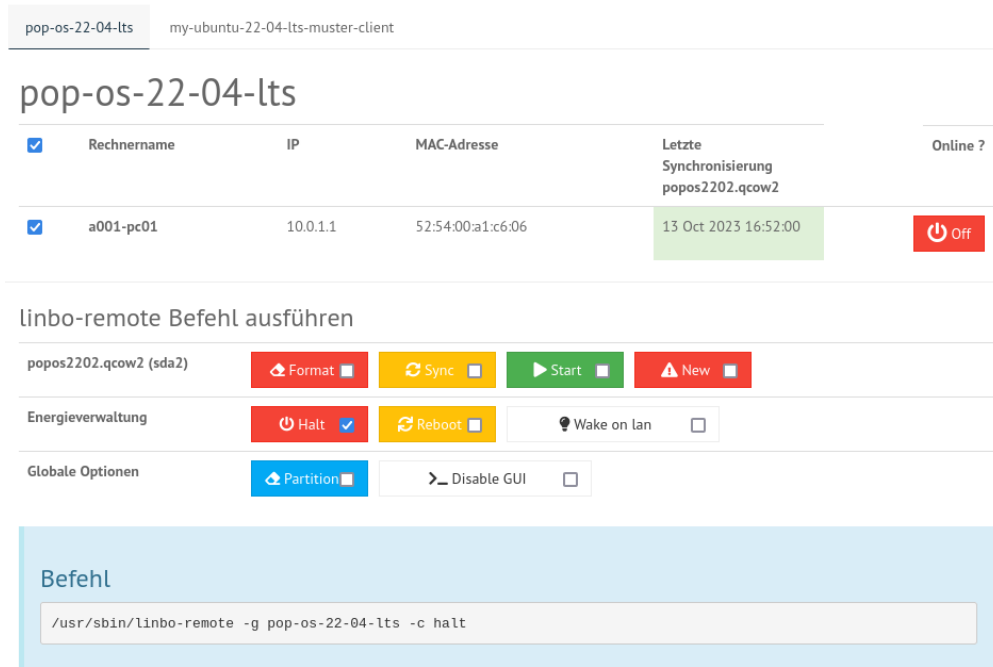


Abb. 315: WebUI LINBO-Synchronisierung

Windows 10 Clients

Autor des Abschnitts: @cweikl, @MachtDochNix (pics)

Betriebssystem Windows 10 installieren

1. Du hast den PC wie zuvor beschrieben mit LINBO partitioniert und formatiert. Danach hast Du den PC / die VM über CD/USB-Stick gebootet.
2. Drücke während des Boot-Vorgangs nach Aufforderung eine Taste, damit von dem Windows-Installationsmedium tatsächlich gebootet wird.
3. Danach siehst Du zu Beginn der Installation die Spracheinstellungen. Wähle die gewünschten Einstellungen aus und klicke auf Weiter:
4. Jetzt installieren wählen.
5. Es wird das Setup gestartet. Es erscheint zuerst der Hinweis auf die Windows-Aktivierung. Hier kannst Du zum jetzigen Zeitpunkt die Option Ich habe keinen Product Key wählen. Die Aktivierung mit der vorhandenen Lizenz erfolgt dann später in anderer Form.
6. Wähle dann das gewünschte Betriebssystem aus, für das die Lizenz vorliegt, z.B. Windows 10 Pro Education N.
6. Haken zum Akzeptieren der Lizenzbedingungen setzen und auf Weiter.
7. Benutzerdefinierte Installation wählen.
8. Im Menü der Festplattenauswahl sollte nun eine Partition vorhanden sein, die von LINBO vorbereitet wurde und auf welcher Windows 10 installiert werden soll.



Abb. 316: Wähle die Sprache und das Tastaturlayout



Abb. 317: Wähle Jetzt installieren

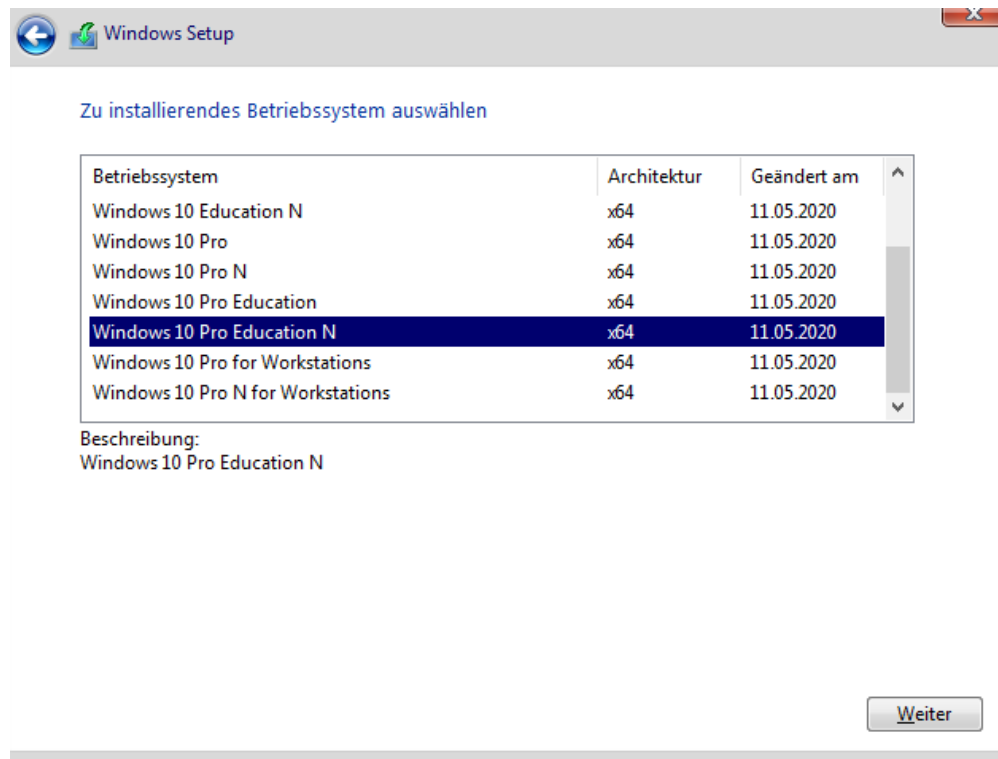


Abb. 318: Wähle das gewünschte Betriebssystem aus

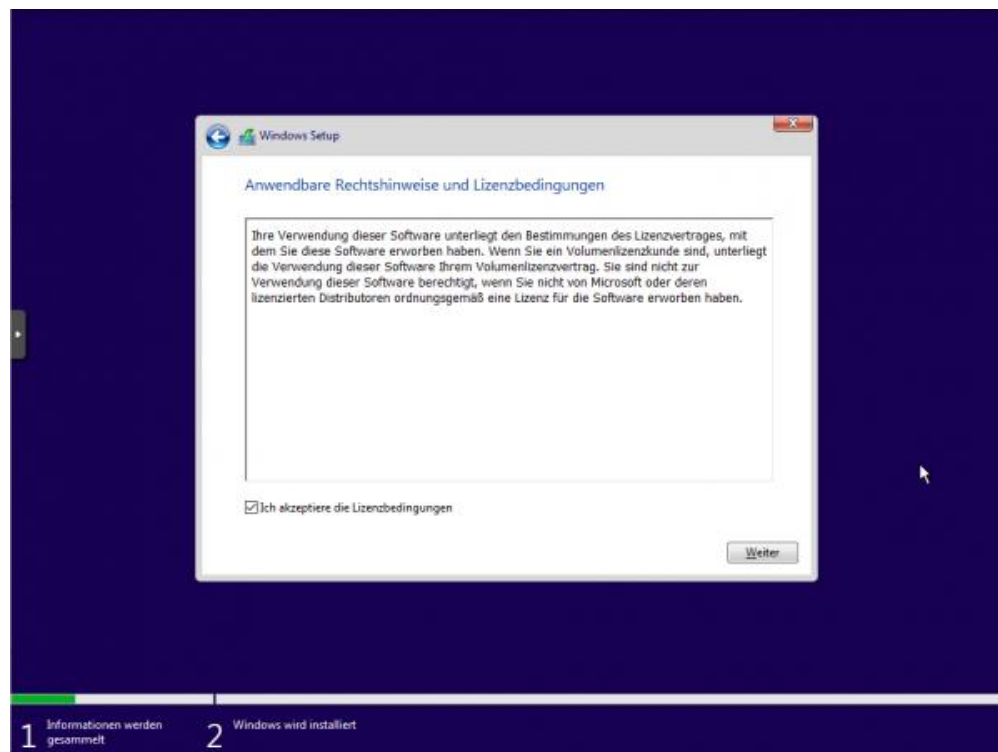


Abb. 319: Akzeptiere die Lizenzbedingungen

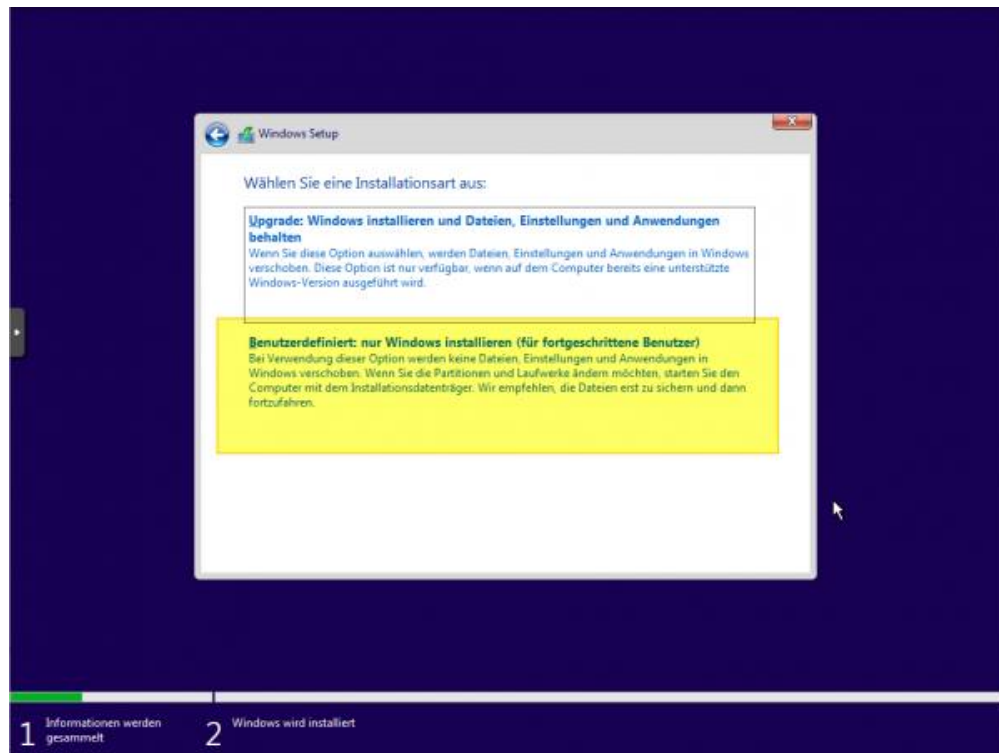


Abb. 320: Wähle die benutzerdefinierte Installation

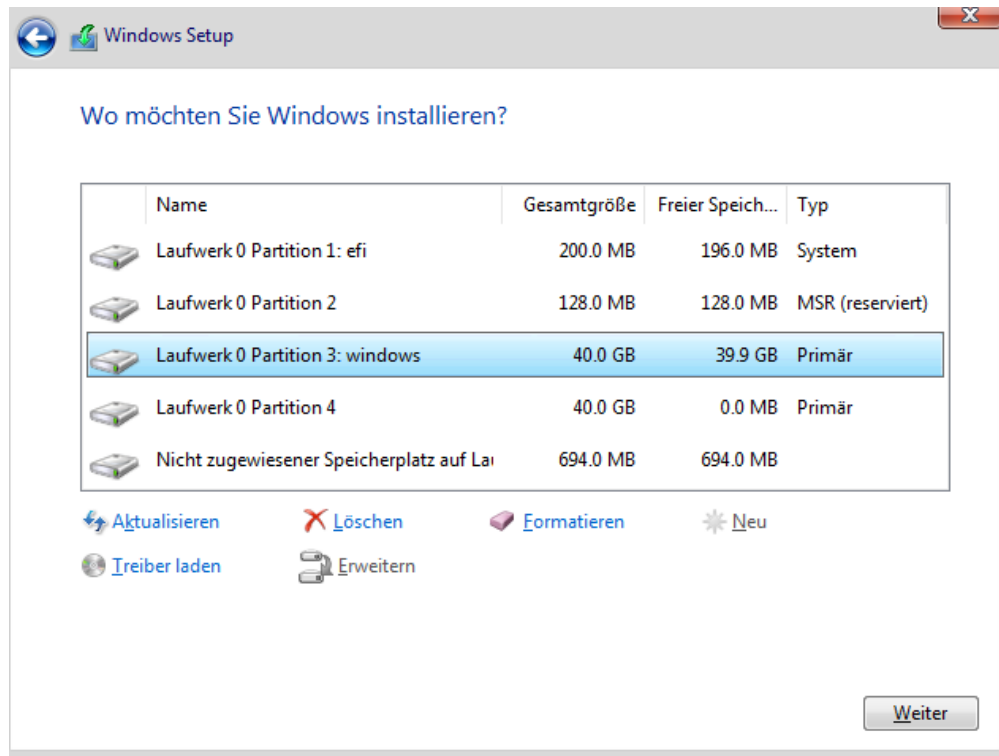


Abb. 321: Wähle die Partition für die Installation von Windows

In der Abb. wurde ein UEFI-System vorbereitet. Partition 3 wurde für Windows 10 vorbereitet und Partition 4 ist die Cache-Partition. Wähle nun die richtige Partition (hier: Partition 3: windows) aus und klicke auf Weiter.

9. Warte bis die Installation von Windows abgeschlossen wurde.

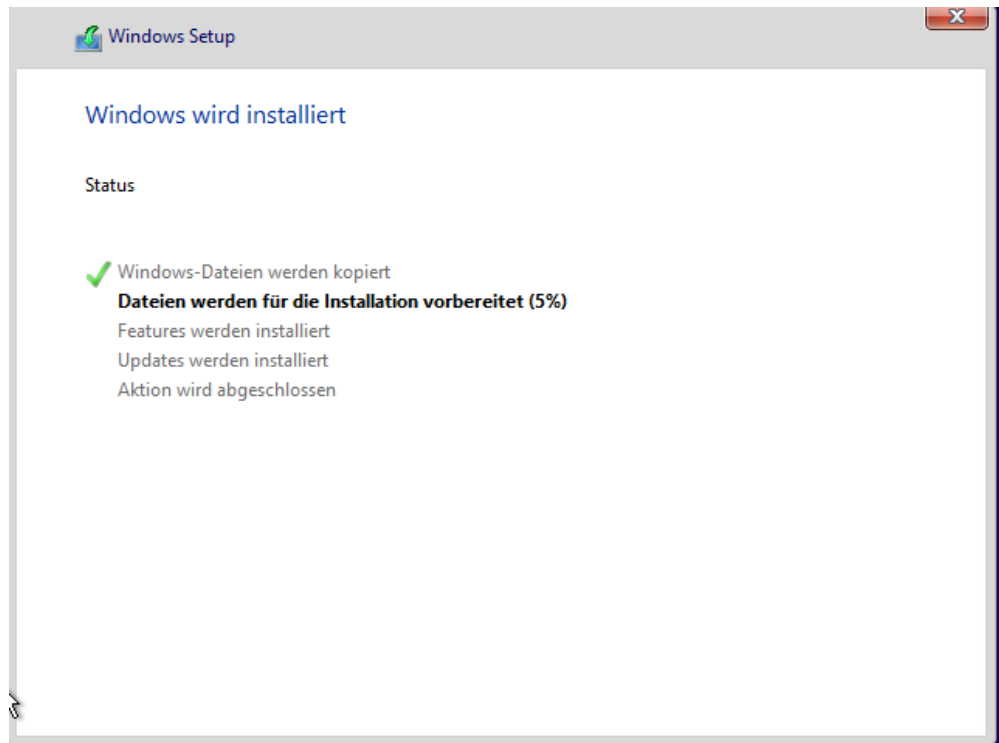


Abb. 322: Fortschritt der Installation von Windows

10. Starte Windows neu.

Hinweis: Es ist jetzt wichtig, dass der PC in LINBO gebootet wird. Stelle daher die Boot-Reihenfolge wieder so um, dass via PXE LINBO gebootet wird. Du gelangst dann wieder wie zuvor in den Linbo Startbildschirm.

11. Starte im LINBO-Menü nun Windows unsynchronisiert über den kleinen GRÜNEN Startknopf neu (!!!nicht rot oder orange!!!):



Abb. 323: Starte Windows 10 unsynchronisiert

Hinweis: Solltest Du hier Probleme haben und ein UEFI-System als Client eingerichtet haben, so versuche, den Client auf den Legacy-Modus umzustellen und die Hardwareklasse in der Schulkonsole ebenfalls so anzupassen, dass BIOS64 genutzt wird. Importiere die Geräte neu, formatiere den Client mit LINBO neu, installiere Windows erneut und boote das installierte Windows aus dem lokalen Cache - wie zuvor beschrieben.

12. Nachdem Windows nun aus dem lokalen LINBO-Cache bootet, wird die Installation fortgeführt. Windows richtet Dienste ein und startet dann erneut. Du gelangst wieder in LINBO und startest Windows wieder unsynchronisiert mit der grünen Pfeiltaste.

Nach dem erneuten Start von Windows wählst Du Deine Region aus.

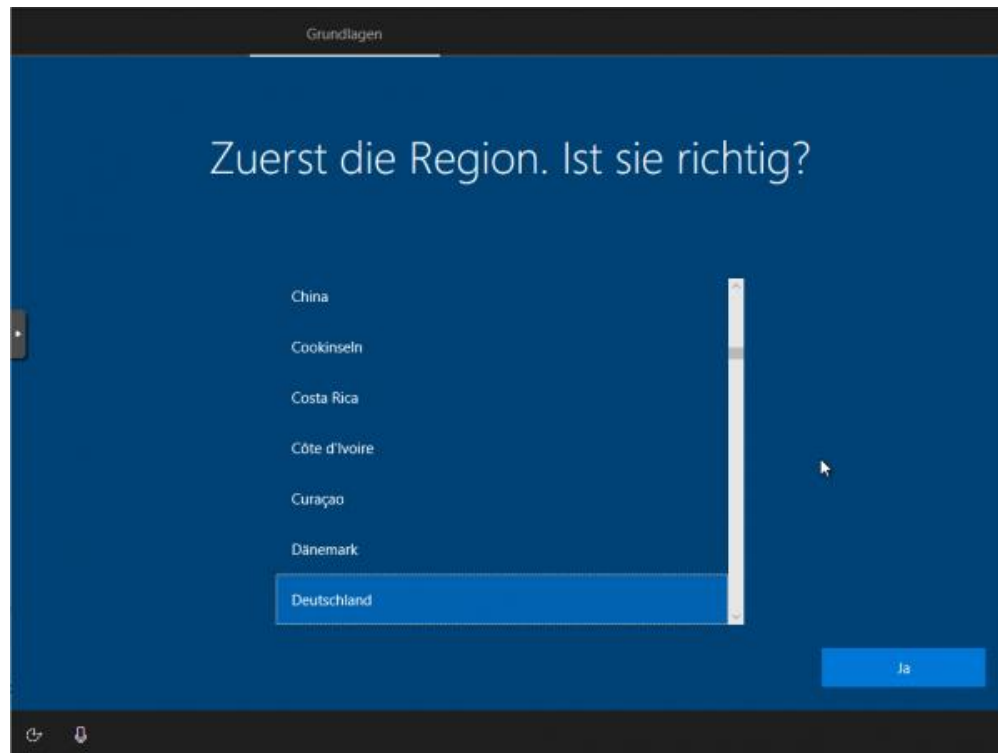


Abb. 324: Wähle die Region aus

13. Tastaturlayout wählen.
14. Zweites Tastaturlayout ggf. wählen.
15. Mit Netzwerk verbinden.
16. Internet-Verbindung herstellen.
17. Admin-Benutzer festlegen.
18. Kennwort festlegen und die Sicherheitsfragen beantworten.
19. Aktivitätenverlauf deaktivieren.
20. Assistenten deaktivieren.
21. Spracherkennung deaktivieren.
22. Standortdienste deaktivieren.
23. Gerätesuche deaktivieren

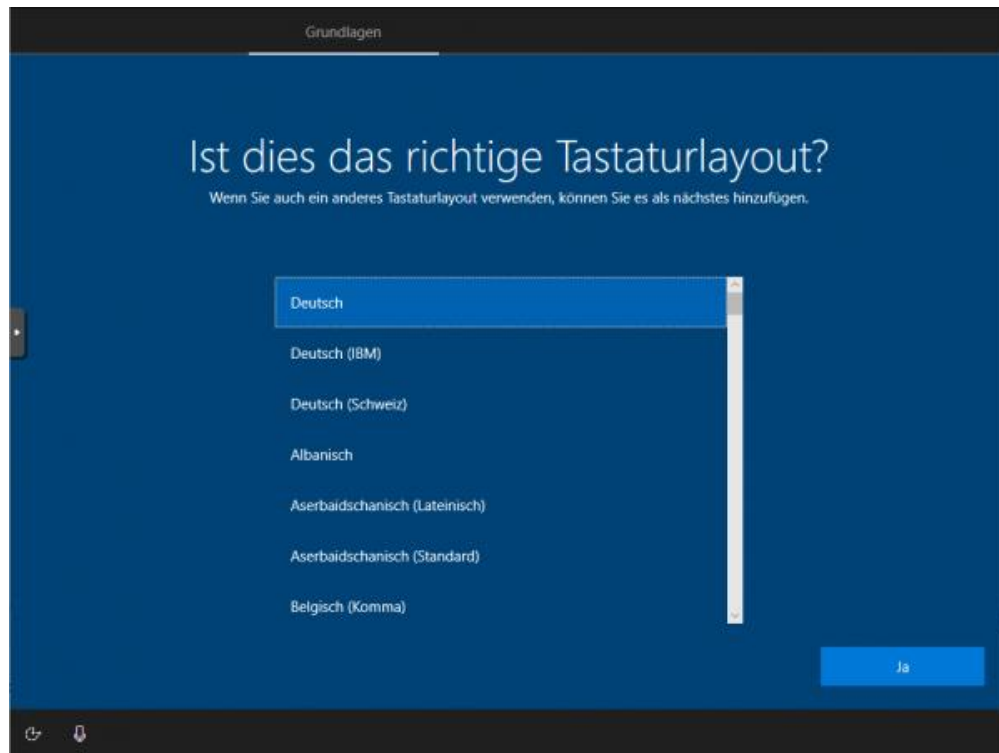


Abb. 325: Wähle das Tastaturlayout aus

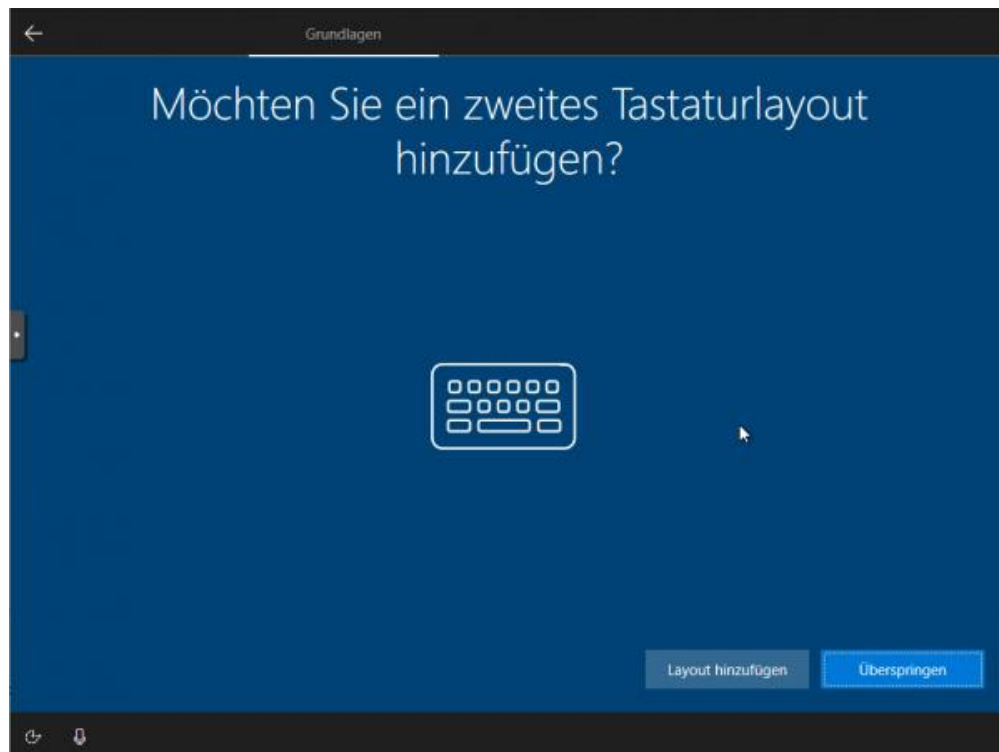


Abb. 326: Wähle ggf. ein zweites Tastaturlayout aus

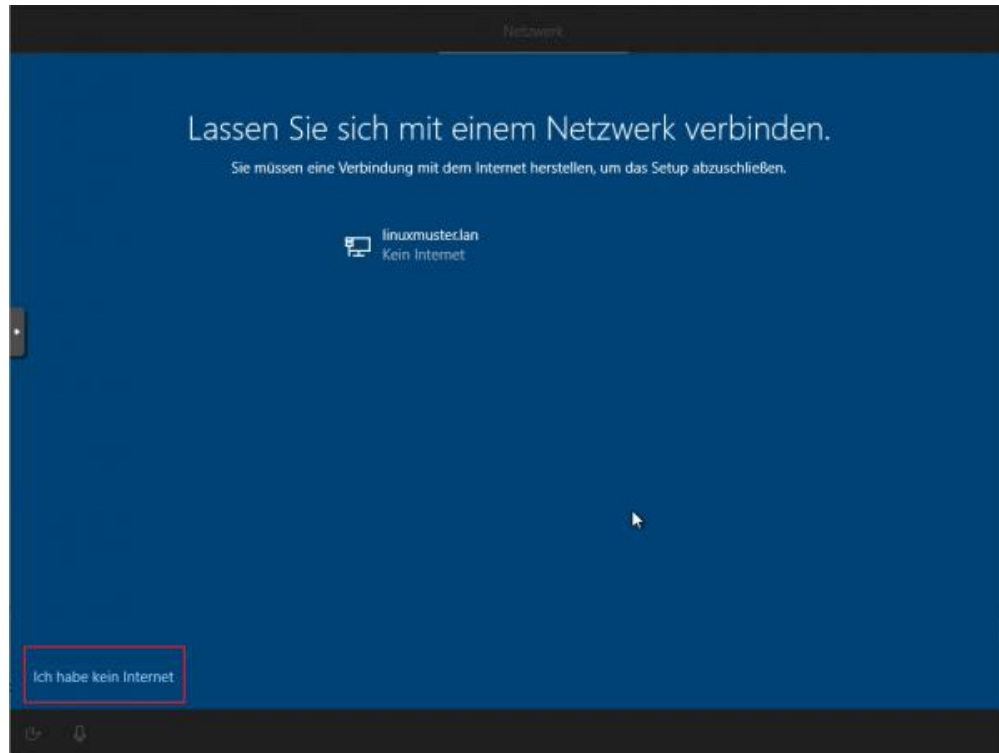


Abb. 327: Ohne Internet-verbinding installieren

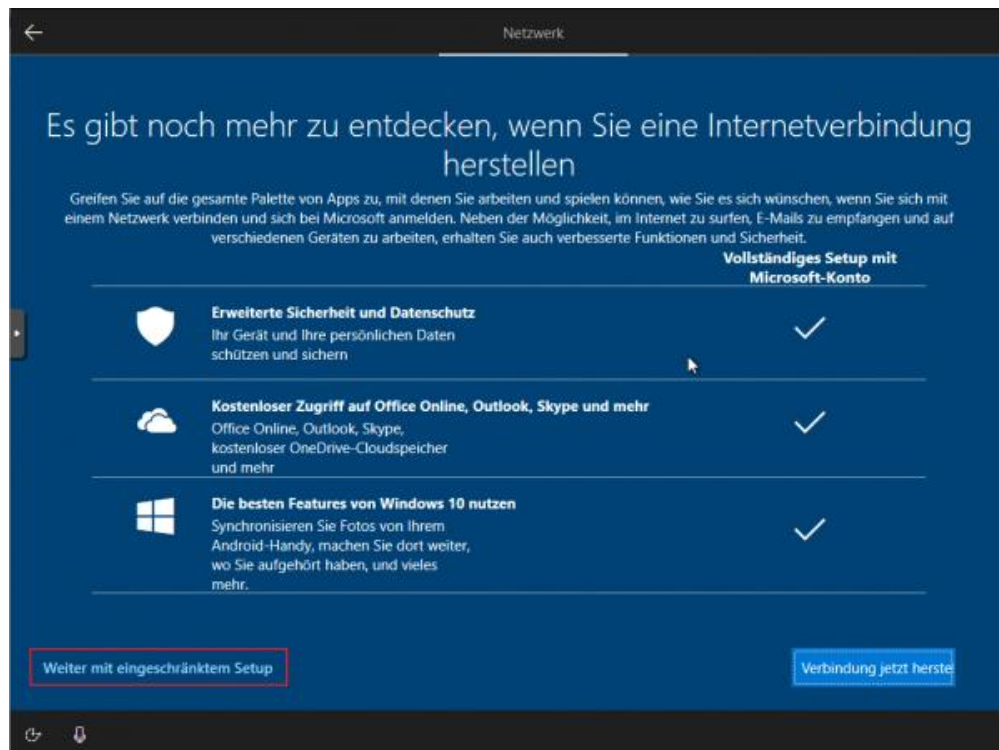


Abb. 328: Weiter mit eingeschränktem Setup

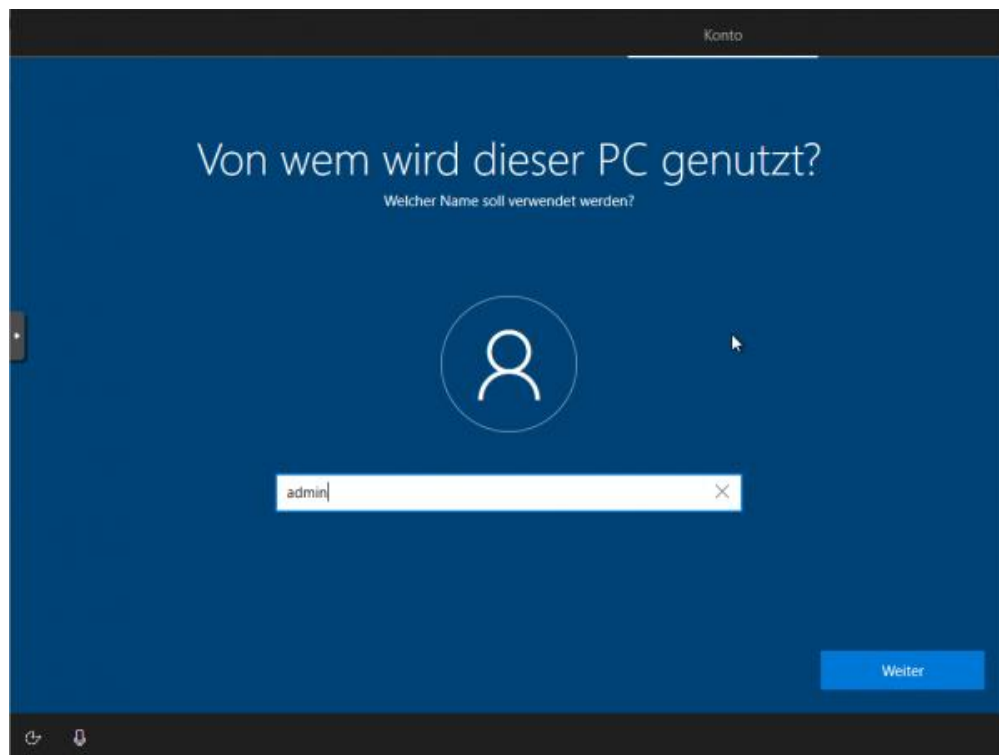


Abb. 329: Lege den Benutzer admin an

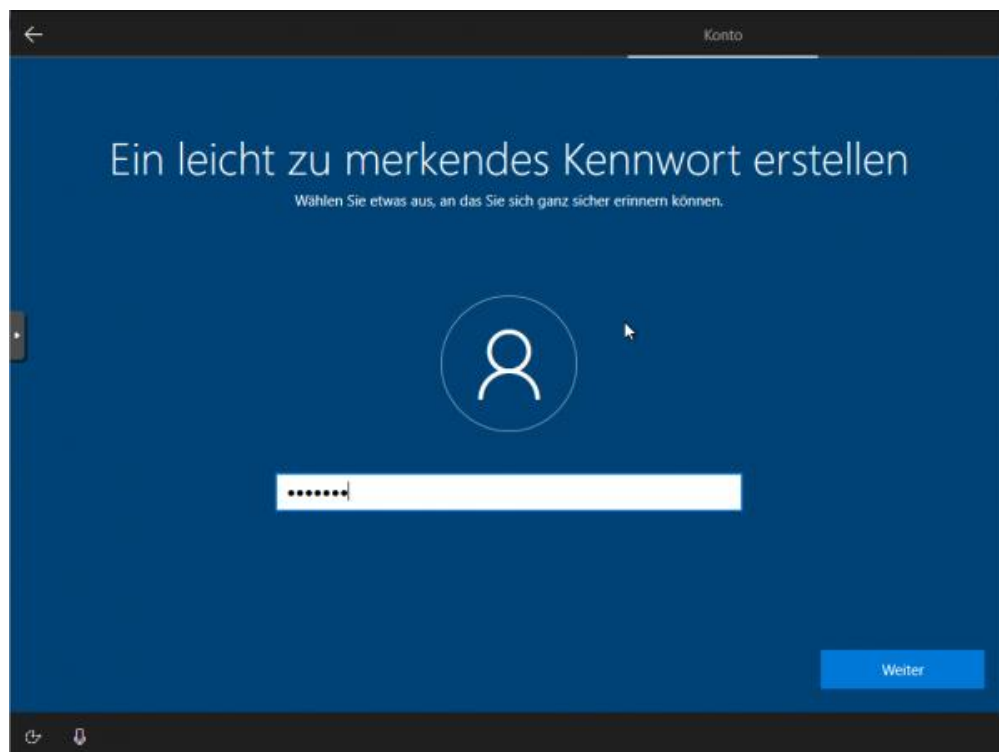


Abb. 330: Lege das Kennwort für den lokalen Benutzer admin fest

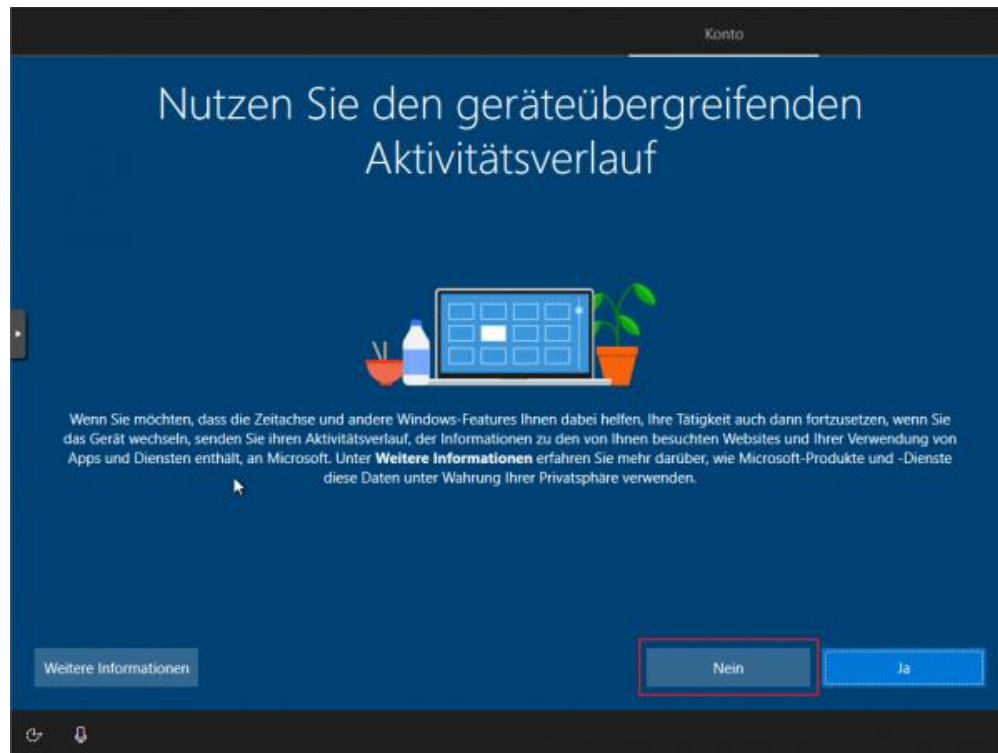


Abb. 331: Deaktiviere das Tracking

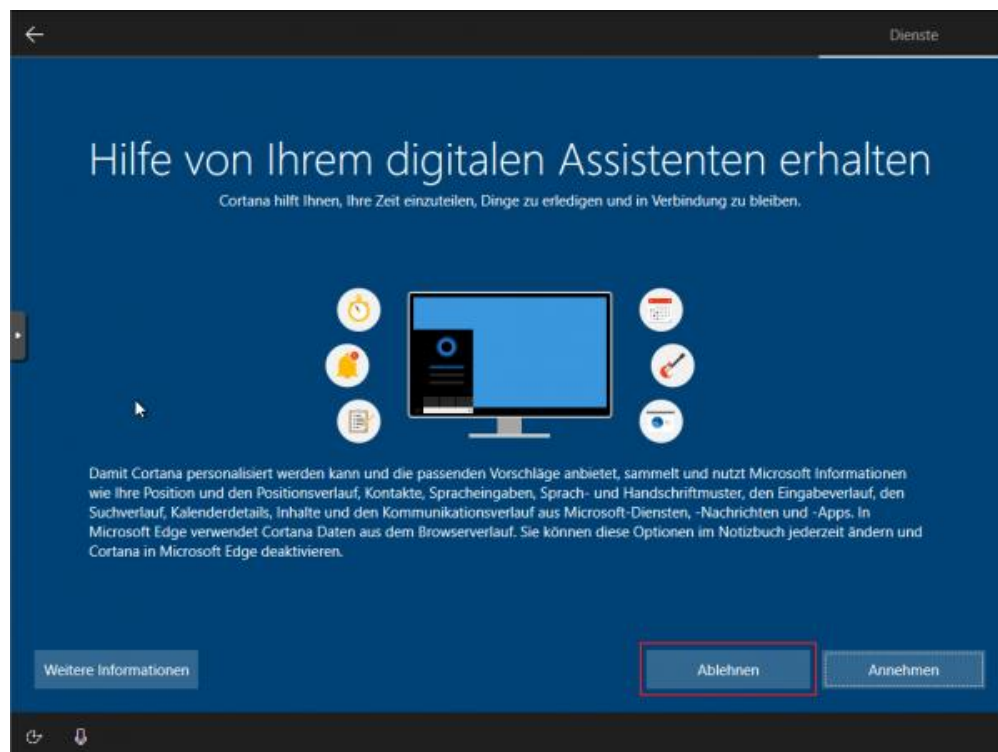


Abb. 332: Deaktiviere Assistenten

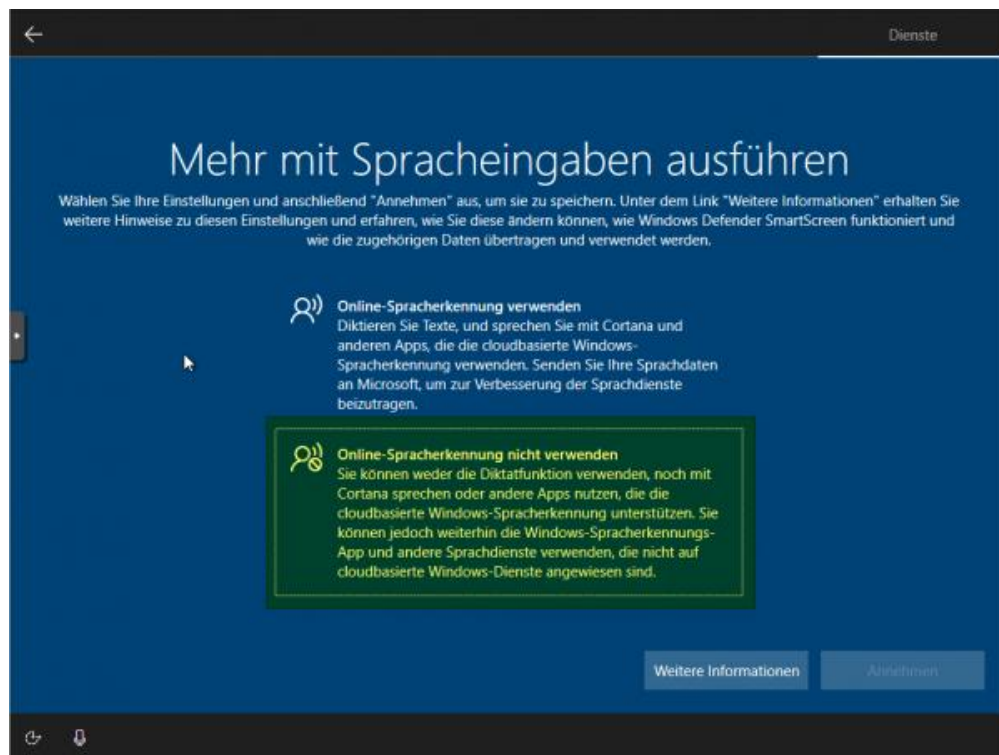


Abb. 333: Deaktiviere die Spracherkennung



Abb. 334: Deaktiviere den Ortungsdienst

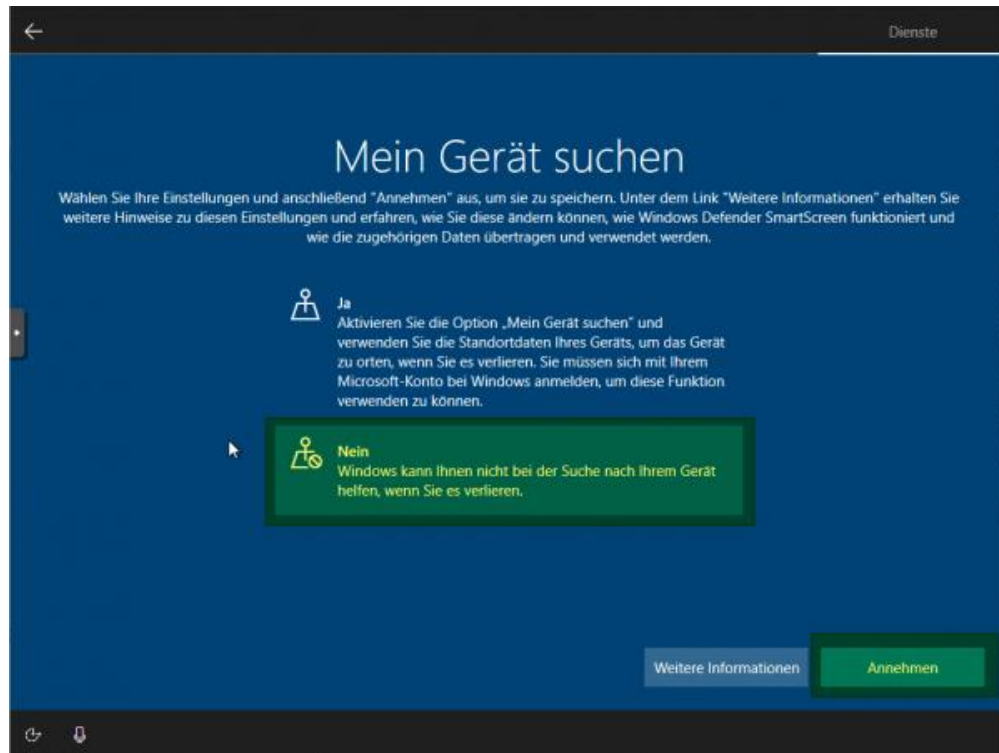


Abb. 335: Deaktiviere die Gerätesuche

24. Übermittlung der Diagnosedaten deaktivieren.
25. Verbesserung der Eingabe / Freihand deaktivieren
26. Restliche Einrichtungsschritte vornehmen.
27. Als Nutzer `admin` anlegen und Kennwort leer lassen oder ein bestimmtes setzen. Die nächsten Einstellungen ablehnen.
28. Weitere gewünschte Einrichtungen ausführen (Programme, Hintergründe, usw.).
29. Alle Updates installieren. Hierbei muss Windows immer wieder neu gestartet werden. Darauf achten, dass Windows aus LINBO heraus immer nur mit der GRÜNEN Pfeiltaste gestartet wird.
30. Gewünschte Einstellungen am Client vornehmen und Installation abschließen.

Global-Registry Patch für Windows 10

Achtung: Vor der Aufnahme des Rechners in die Domäne muss der sog. Global-Registry-Patch eingespielt werden, da es ansonsten zu einer Änderung des Kennworts für das Computerkonto kommen kann.

1. Starte auf dem Client Windows in LINBO mit der grünen Pfeiltaste.
2. Melde Dich als lokaler Administrator am Windows-PC an.
3. Öffne den Explorer und gehe auf Dieser PC -> Geräte und Laufwerke -> windows (C:) -> `linuxmuster-win`
4. Bestätige die Nachfrage zur Berechtigung zum Zugriff auf diesen Ordner mit Fortsetzen.

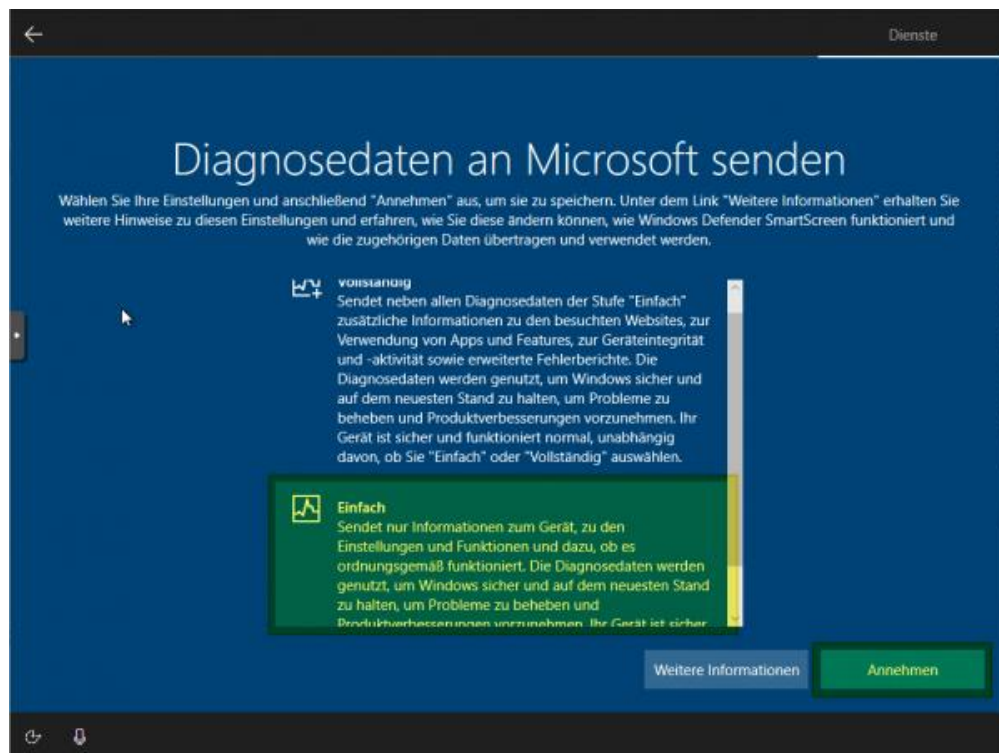


Abb. 336: Deaktiviere die Übermittlung von Diagnosedaten

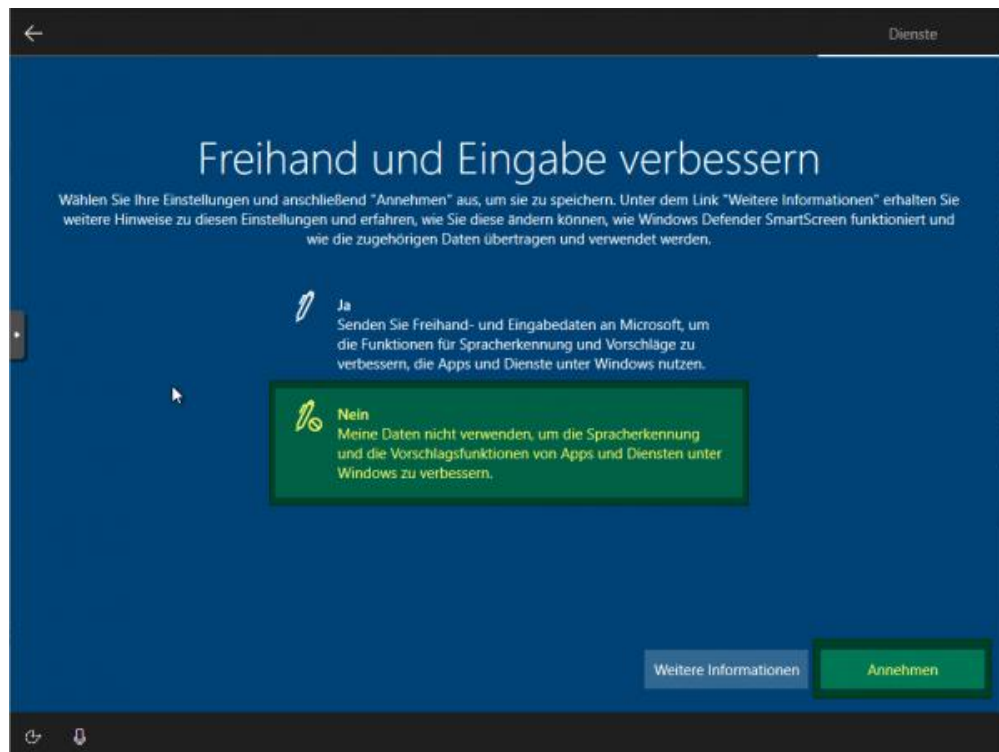


Abb. 337: Deaktiviere die Freihandeingabe

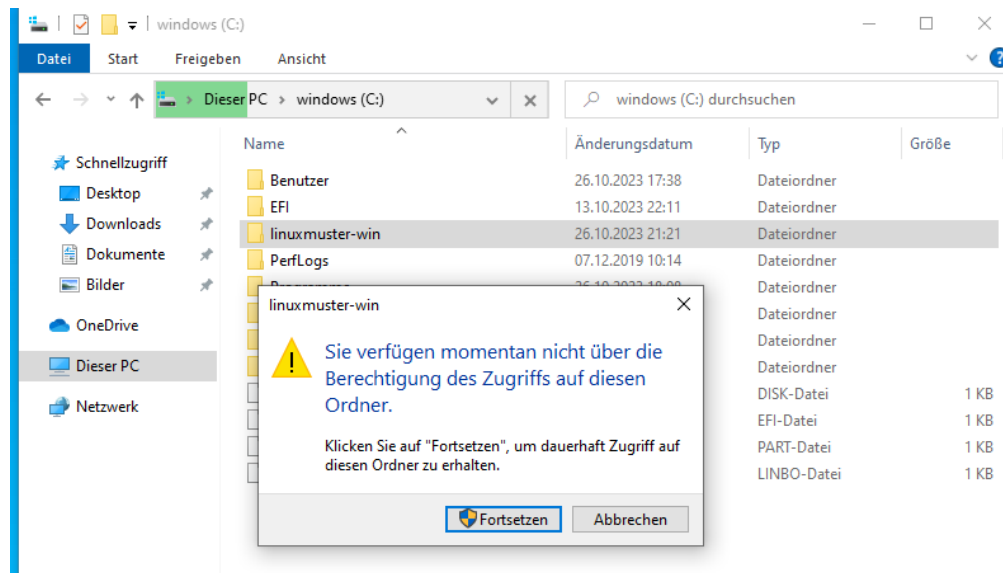
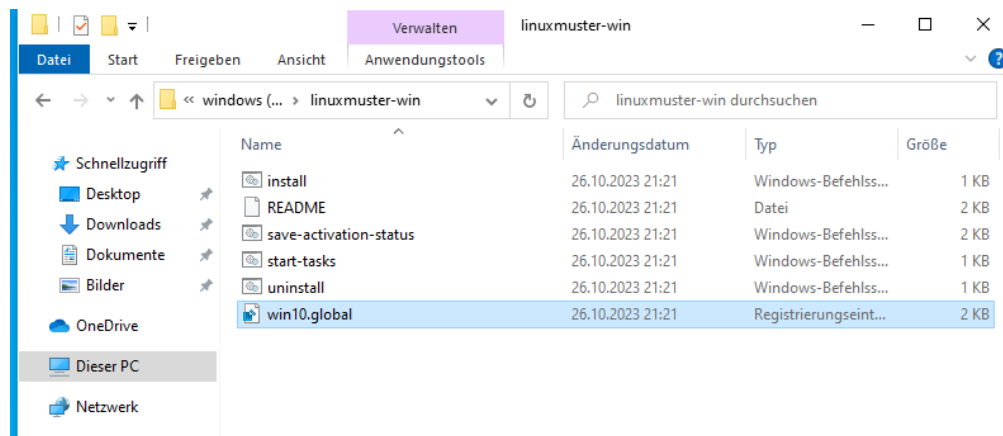


Abb. 338: Öffne den Ordner c:\linuxmuster-win\

5. Kopiere die Datei `win10.global` auf den Desktop, indem Du diese mit der linken Maustaste markierst und auf den Desktop ziehst.

Abb. 339: Kopiere die Datei `win10.global` auf den Desktop

Danach setzt Du die Installation mit dem Abschnitt *win10.global.reg einspielen* einspielen fort.

Im Fehlerfall gehst Du zu dem Abschnitt *im Fehlerfall*

win10.global.reg einspielen

Führe nun einen Doppelklick auf die Datei `win10.global.reg` auf dem Desktop aus. Lasse Änderungen durch diese App zu.

Nehme ggf. weitere gewünschte System-Einrichtungen vor.

Zum Herunterfahren vorsichtshalber über das Windows-Startmenü in der Suche `cmd` eingeben und die Eingabeaufforderung öffnen.

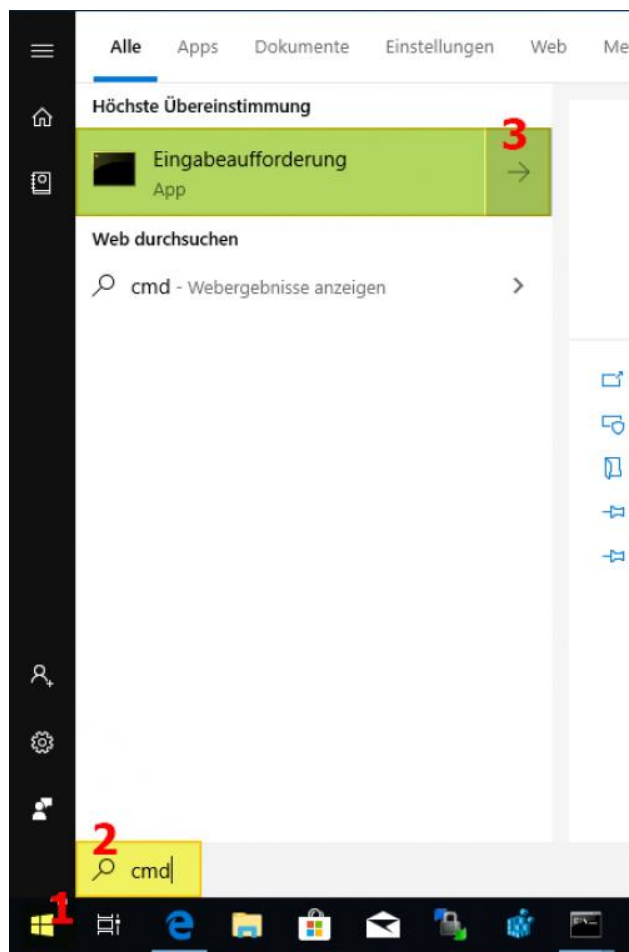


Abb. 340: Öffne das Windows-Terminal

In der Console `shutdown -s -t 1` eingeben und mit **Enter** bestätigen:

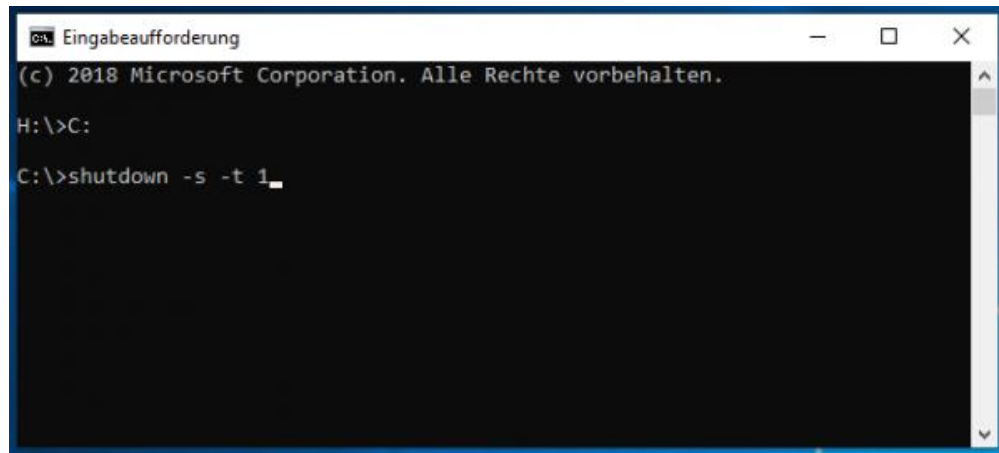


Abb. 341: Fahre das Gerät herunter

Domänenanbindung

Geräte die dauerhaft mit den Ressourcen der linuxmuster.net Umgebung arbeiten sollen, sind nach dem Einspielen des `win10-global.reg` Patches in der Domäne aufzunehmen.

Starte den Muster-Client wieder via LINBO, indem Du Win10 mit dem GRÜNEN Start-Button aus dem lokalen Cache startest.

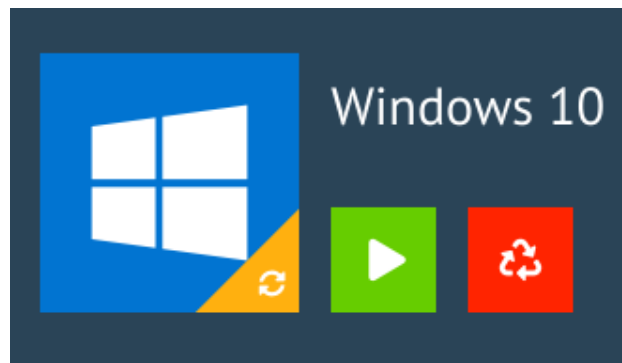


Abb. 342: Starte Windows 10 mit der grünen Taste

Manueller Domänen Join für Windows

Über **System** → **Info** → **Diesen PC umbenennen** einen Hostname vergeben, der *übereinstimmend* mit dem Hostnamen in der Geräteliste ist.

Um den neuen Hostname anzuwenden, muss Windows neu gestartet werden.

Starte in LINBO Windows mit der grünen Taste neu.

Nach dem Neustart meldest Du Dich wieder als Benutzer **admin** an und rufst **System** --> **Info** --> **Diesen PC umbenennen** (fortgeschritten) auf.

Klicke auf der Reiterkarte **Computernamen** auf **Ändern**.

Trage unter **Mitglied von** -> **Domäne** Deine Domäne ein. Bestätige dies mit **OK**.

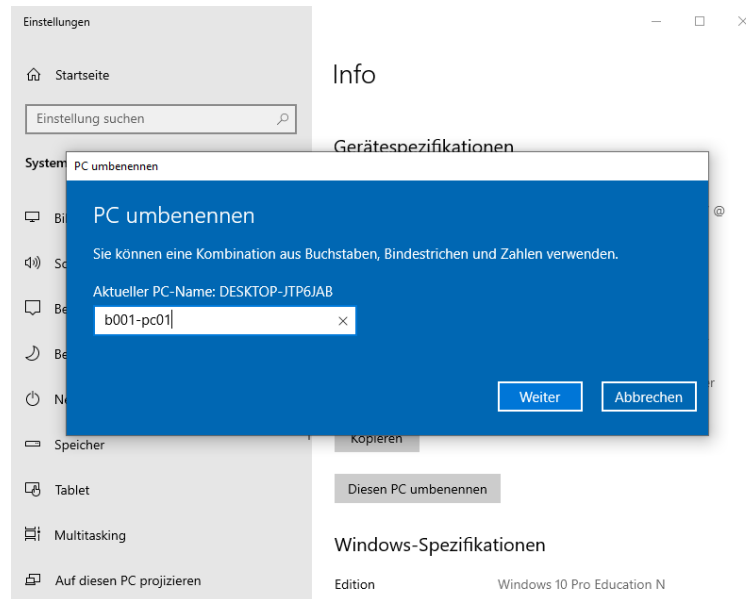


Abb. 343: Client umbenennen

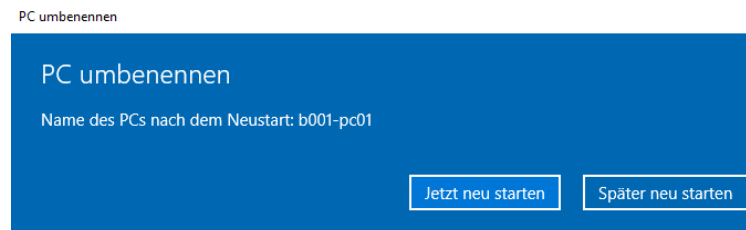


Abb. 344: Starte Windows neu

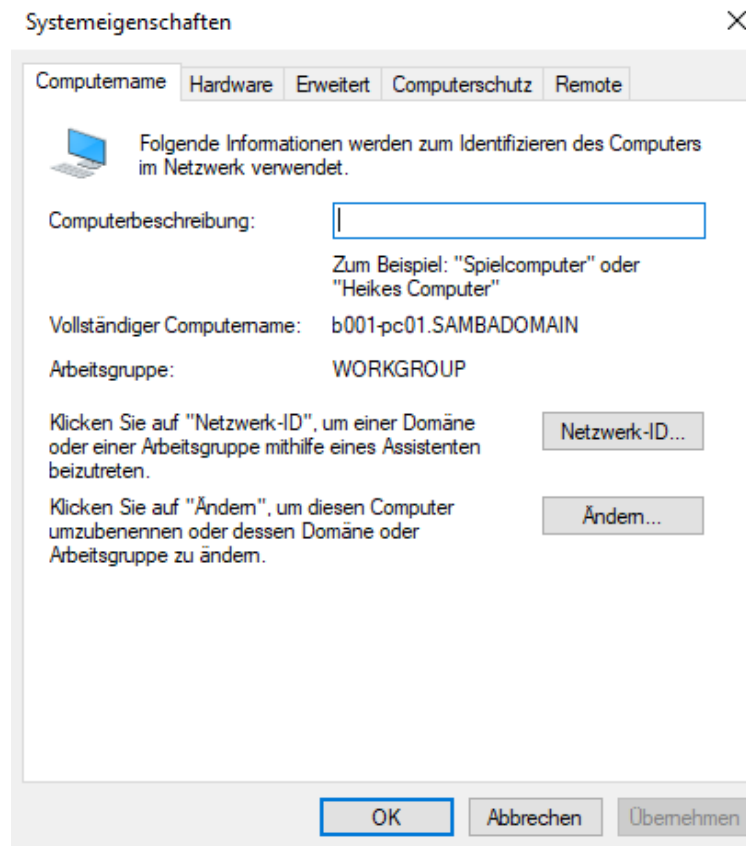


Abb. 345: Erweiterte Systemeinstellungen

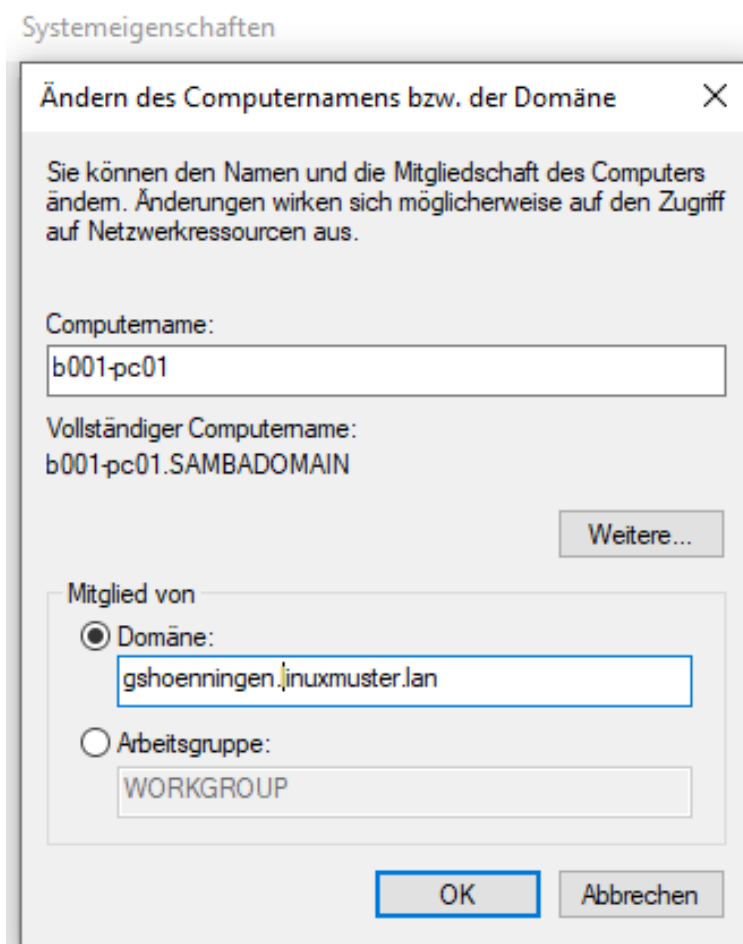


Abb. 346: Ändere die Domänenzugehörigkeit

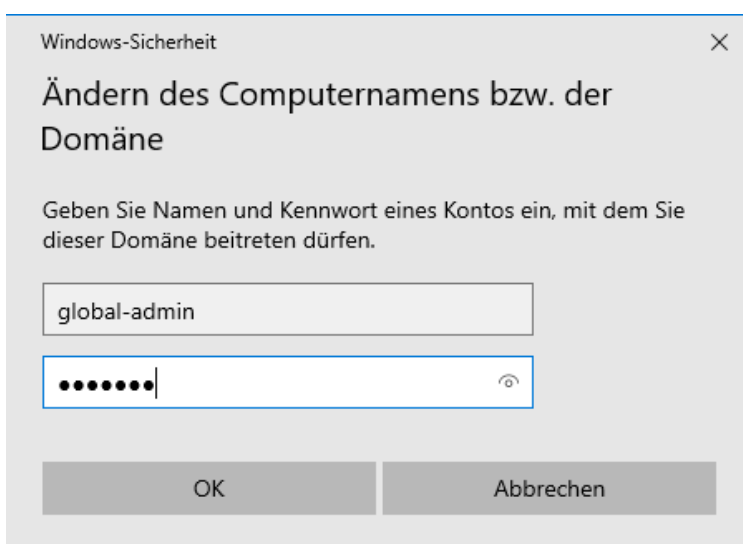


Abb. 347: Melde Dich als Benutzer global-admin an

Bei einem erfolgreichen Beitritt zur Windows-Domäne wird dies mit folgendem Fenster bestätigt.

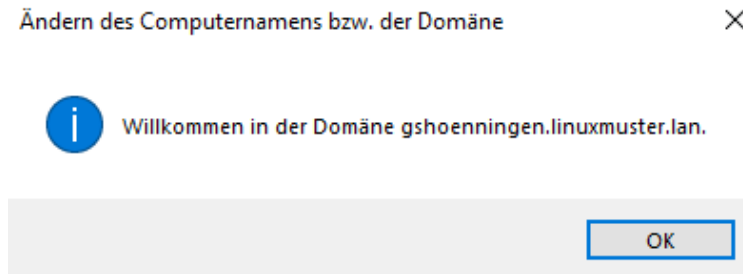


Abb. 348: Willkommen in der Domäne

Beendest Du die Systemeinstellungen erscheint der Hinweis, dass der PC neu zu starten ist.

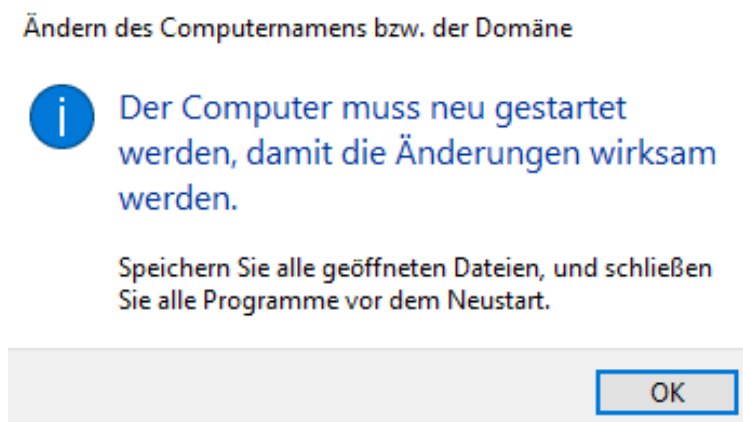


Abb. 349: Der Computer muss neu gestartet werden

Bestätige dies im nächsten Fenster mit **Jetzt neu starten**.

Der PC bootet nun wieder in LINBO.

Achtung: Starte Windows 10 nun **NICHT** neu ! Nach dem Start in LINBO erstellst Du jetzt Muster-Image

LINBO Muster-Image mit Domänenbeitritt

Nachdem der Muster-Client mit Windows 10 - wie zuvor beschrieben - der Domäne hinzugefügt wurde, erstellst Du **jetzt** ein Image für den Muster-Client. Wird dieses Image auf andere Maschinen übertragen, so sind diese bereits in der Domäne aufgenommen.

Hinweis: Nachdem eine Template-Maschine frisch der Domain gejoined ist, darf diese vor dem Upload nicht neu gestartet werden, da sonst das durch den DomainJoin neu erstellte Maschinenpasswort in der AD für diese Maschine mit einem falschen Maschinenpasswort ersetzt werden würde. Durch den Image-Upload wird das neue Passwort ausgelesen und in die macct-Datei geschrieben, die zu dem Image gehört.

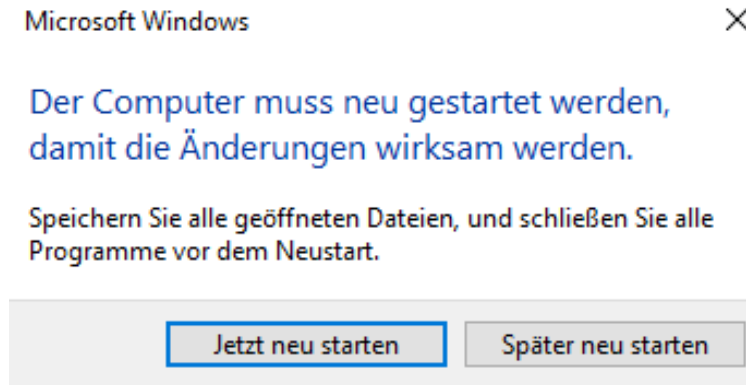


Abb. 350: PC neu starten

Image in LINBO erstellen

1. Jetzt wieder in LINBO starten und von dem aktuellem Stand ein Image erstellen. Klicke rechts auf das Werkzeug-Symbol. Gib das LINBO-Passwort ein, dann siehst Du folgende Einträge:

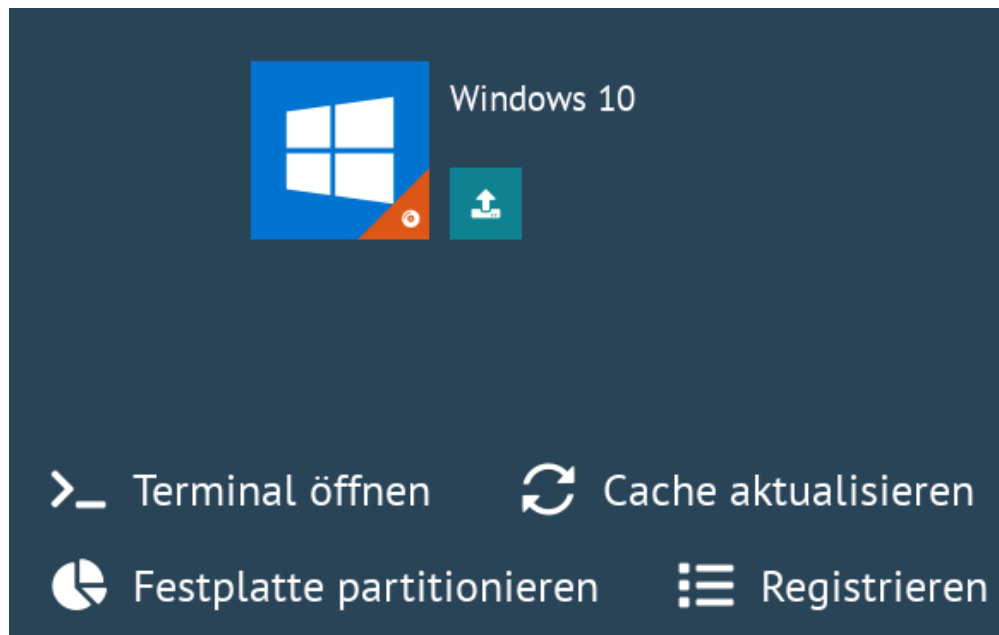


Abb. 351: Werkzeug-Symbol - Untermenü

2. Klicke nun das grosse Windows-Symbol, um das Image zu erstellen. Es öffnet sich folgender Dialog:

Gib eine Beschreibung an, die Dir Hinweise zum Konfigurationsstand des Images gibt. Da Du das erste Image erstellst, klickst Du nun **erstellen** + **hochladen**.

Nach dem erfolgreichen Upload siehst Du folgende Statusmeldung:

3. Nach dem erfolgreichem Upload sollte das Image auf der linuxmuster.net Schulkonsole unter LINBO4 → Gruppen angezeigt werden.

Zudem finden sich die Abbilder selbst unter LINBO4 → Gruppen → Abbilder aufgelistet.

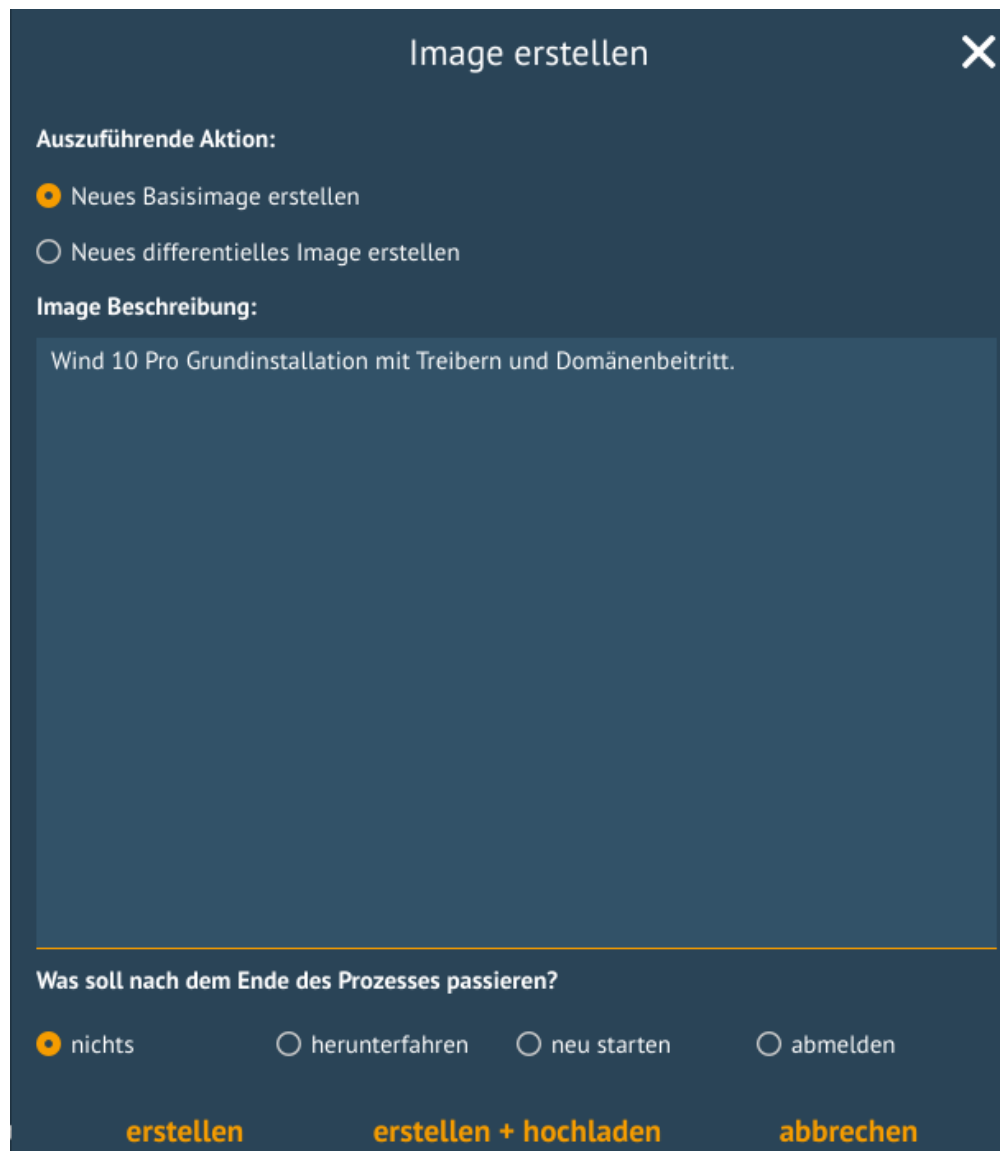


Image erstellen

Auszuführende Aktion:

☒ Neues Basisimage erstellen

☐ Neues differentielles Image erstellen

Image Beschreibung:

Wind 10 Pro Grundinstallation mit Treibern und Domänenbeitritt.

Was soll nach dem Ende des Prozesses passieren?

☒ nichts ☐ herunterfahren ☐ neu starten ☐ abmelden

erstellen erstellen + hochladen abbrechen

Abb. 352: Image erstellen

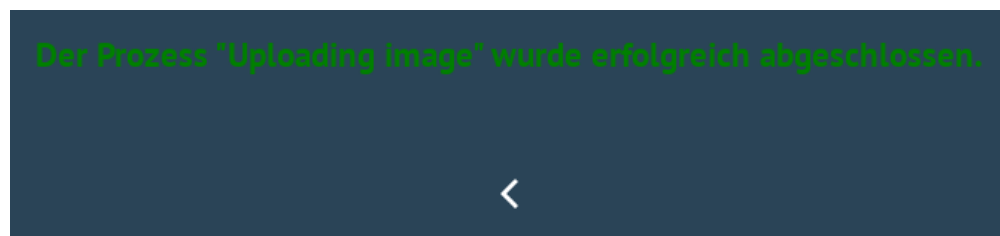


Abb. 353: Image erfolgreich hochgeladen

Gruppen	Abbilder	
Gruppenname	Verwendete Images	Aktionen
my-ubuntu-22-04-lts-muster-client	<div>ubuntu.qcow2</div>	<div></div>
pop-os-22-04-lts	<div>popos2202.qcow2</div>	<div></div>
win10-muster-client	<div>win10.qcow2</div>	<div></div>

Abb. 354: Verwendete Images

Gruppen	Abbilder	
Gruppenname	Verwendete Images	Aktionen
my-ubuntu-22-04-lts-muster-client	ubuntu.qcow2	  
pop-os-22-04-lts	popos2202.qcow2	  
win10-muster-client	win10.qcow2	  

Abb. 355: Übersicht der Abbilder

Falls der Gruppe anfangs kein Basisimage zugeordnet war, sollte das unter Groups → <gruppenname> → Partitionen → Windows 10 edit → OS → Basisimage nachgeholt werden. Speichern nicht vergessen.

4. Einem Image muss ein sog. Image-Registry-Patch angegeben werden: Wähle dazu das gewünschte Image aus. Klicke hierzu auf LINBO 4 --> Abbilder --> <Name des Images>. Klicke rechts neben dem Imagennamen auf das Zahnrad-Symbol. Gehe dort zur Reiterkarte Registry-Patch.

Klicke nun unten auf die Drop-down Liste Copy from. Es werden verschiedene Reg-Patches in der Dropdown-Liste dargestellt.

Klicke nun unten auf die Drop-down Liste Copy from -> win10.image.reg. Es wird die Reg-Datei in dem Fenster angezeigt.

Speichere diesen kopierten Registry-Patch für das Windows 10 Image, indem Du direkt auf **SPEICHERN** klickst.

5. *Alternativ* kannst Du in der Server-Shell aus /srv/linbo/examples die richtige Vorlage in /srv/linbo/ kopieren. Die Datei trägt dann den Namen <imagename>.reg - also in o.g. Beispiel win10.reg.

Imageübertragung auf den PC


1. Starte den PC, auf den das Image übertragen werden soll, über das Netzlaufwerk bis er in LINBO gebootet hat. Nun öffnest Du den Imaging-Reiter, wie im ersten Kapitel *Computer in linuxmuster.net aufnehmen* → Client lokal registrieren beschrieben wird.
2. Als nächstes partitionierst und formatierst Du den PC über den LINBO-Menüeintrag Partitionieren wie zuvor beschrieben.
3. Wechsel nun auf dem Imaging-Menü wieder in das Startmenü von LINBO. Klicke hier das ROTE Symbol (Windows neu installieren), um Windows neu zu installieren.
4. Wenn das Image vollständig heruntergeladen ist, startet Windows automatisch.

In der Datei /srv/linbo/start.conf.win10-muster-client (start.conf der HWK) könnten die Einstellungen für Windows wie folgt aussehen:

/dev/sda3

Partition OS

Name	Version
Windows 10	10

Standard Start	Symbol
Sync & start	

Basisimage

win10.qcow2


+

Start Optionen

- ☒ Start
- ☒ Sync & start
- ☒ New start
- ☐ Autostart

SPEICHERN ERWEITERT SCHLIESSEN

Abb. 356: Basisimage für die HWK festlegen

win10 

Allgemein Registry Patch Postsync-Skript Prestart Skript

1

Copy from

win10.image.reg Example

win10.global.reg Example

win11bypass.reg Example

SPEICHERN SCHLIESSEN

win10-muster-client

Abb. 357: Registry-Patch auswählen

win10



Allgemein

Registry Patch

Postsync-Skript

Prestart Skript

```

1 Windows Registry Editor Version 5.00
2
3 ; linuxmuster.net 7
4 ; thomas@linuxmuster.net
5 ; 20230510
6
7 ; patches hostname, to be applied after every image sync
8
9 [HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\ComputerName\Ac
   tiveComputerName\]
10 "ComputerName"="{${HostName$}"
11
12 [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ComputerNam
   e\ActiveComputerName\]
13 "ComputerName"="{${HostName$}"
14
15 [HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\ComputerName\Co
   mputerName\]
16 "ComputerName"="{${HostName$}"
17
18 [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ComputerNam
   e\ComputerName\]
19 "ComputerName"="{${HostName$}"
20
21 [HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Paramete
   rs\]
22 "Hostname"="{${HostName$}"
23 "NV Hostname"="{${HostName$}"
24
25 [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Para
   meters\]
26 "Hostname"="{${HostName$}"
27 "NV Hostname"="{${HostName$}"
28
29 ; add your custom registry patches below
30

```

Copy from ▼

SPEICHERN

SCHLIESSEN

Abb. 358: Kopiere und speichere den Registry-Patch



Abb. 359: Windows neu installieren

```
[OS]
Name = Windows 10
Version = 10
Description = Windows 10 1903
IconName = win10.svg
BaseImage = win10.qcow2
Boot = /dev/sda3
Root = /dev/sda3
Kernel = auto
Initrd =
Append =
StartEnabled = yes
SyncEnabled = no
NewEnabled = yes
Autostart = yes
AutostartTimeout = 5
DefaultAction = new
Hidden = yes
```

Abb. 360: LINBO Start.conf Einstellungen für Windows

Bei Änderungen in der start.conf der HWK muss erneut ein Import der Geräte ausgeführt werden. Dies kann entweder in der Schulkonsole unter Geräteverwaltung -> Geräte -> Speichern & importieren erfolgen.

Alternativ kann dies auf dem Server in der Konsole durchgeführt werden:

```
linuxmuster-import-devices
```

Programminstallation

Hast Du wie zuvor beschrieben, den Client synchronisiert gestartet, meldest Du Dich als Benutzer global-admin an der Domäne an.

Installiere die gewünschten Programme und konfiguriere die benötigten Programm- und Systemeinstellungen.

Starte den PC neu, ohne danach neu zu synchronisieren. Führe danach nachstehenden Abschnitt aus.

Default Profil kopieren

linuxmuster.net sieht vor, dass **Programminstallation von global-admin** durchgeführt werden. Damit alle User die bei der Installation vorgenommenen Änderungen bekommen, muss das Profil des global-admin als Default Profil kopiert werden.

Dies kann mit dem freien Tool DefProf durchgeführt werden. Das Tool kann hier heruntergeladen werden: <https://www.forensit.com/Downloads/DefProf.msi>

Das Ausführen der MSI-Datei entpackt das eigentliche Programm. Hast Du dies als Benutzer global-admin durchgeführt, siehst Du folgendes Fenster:

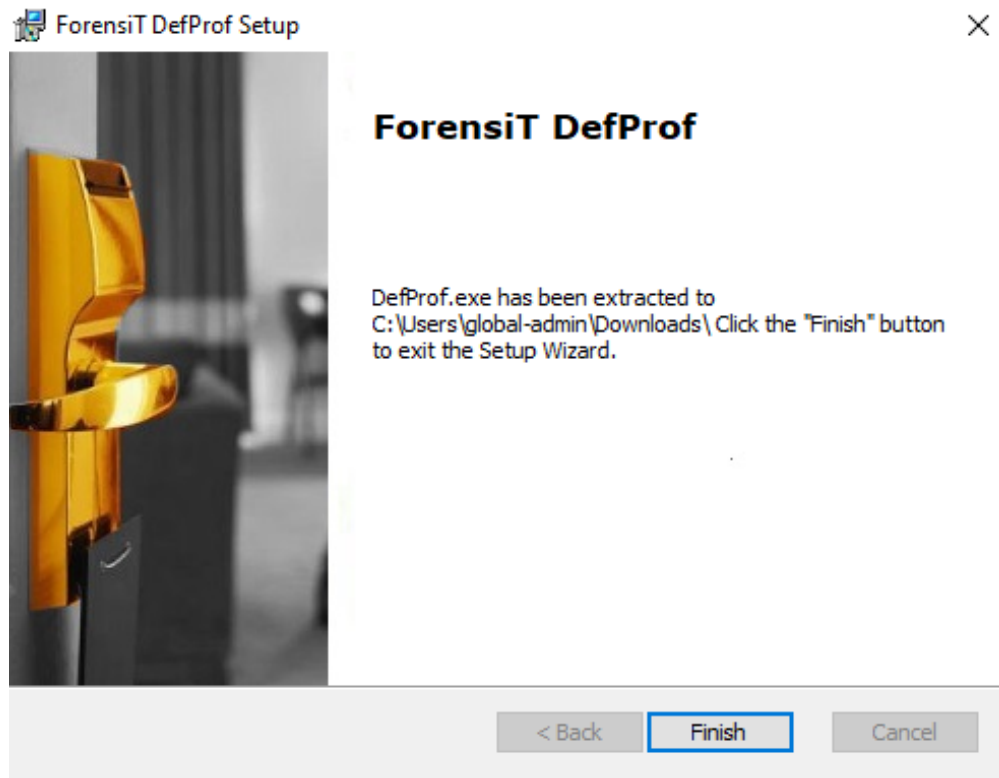


Abb. 361: Installiere DefProf

Das ausführbare Programm befindet sich nun unter `c:\Users\global-admin\downloads\Defprof.exe`. Kopiere diese Datei nun unter `c:\Windows\` als Benutzer `global-admin`.

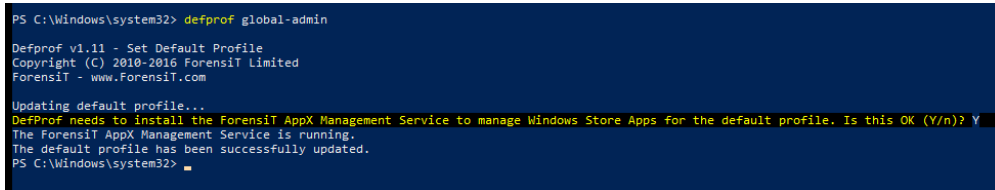
Hast Du alle Einstellungen als Benutzer `global-admin` für das Profil vorgenommen, kannst Du nun dieses Profil mithilfe des zuvor installierten Tools DefProf als Default-Profil kopieren.

Hierzu führst Du folgende Schritte aus:

1. Hierzu meldet Du Dich zuerst als Benutzer `global-admin` ab und lokal am PC als Benutzer `admin` wieder an.
2. Bist Du lokal als `admin` angemeldet, klickst Du mit der rechten Maustaste auf das Windows-Symbol unten links.
3. Wähle dann in dem Kontextmenü Windows `PowerShell(Administrator)` aus.
4. Es öffnet sich die PowerShell-Eingabekonzole von Windows mit Administrator-Berechtigungen.
5. Gebe nun in der Konsole den Befehl `defprof` gefolgt von dem als Default-Profil zu kopierenden Profil an.
6. Für den Windows 10 Muster-Client bedeutet dies, dass Du `defprof global-admin` angibst.

```
c:\defprof global-admin
```

7. Bei der Erstausführung müssen noch weitere Tools nachinstalliert werden. Bestätige dies mit `Y`.
8. Wurde das Profil erfolgreich als Default Profil kopiert, siehst Du folgende Meldungen:



```
PS C:\Windows\system32> defprof global-admin
DefProf v1.11 - Set Default Profile
Copyright (C) 2010-2016 ForensiT Limited
ForensiT - www.ForensiT.com

Updating default profile...
DefProf needs to install the ForensiT AppX Management Service to manage Windows Store Apps for the default profile. Is this OK (Y/n)? Y
The ForensiT AppX Management Service is running.
The default profile has been successfully updated.
PS C:\Windows\system32>
```

Abb. 362: DefProf: profil erfolgreich kopiert

9. Danach startest Du Windows neu und erstellst wie zuvor beschrieben ein neues Image für Windows.

im Fehlerfall

Zeitprobleme lösen

LINBO aktualisiert beim Systemstart die Zeit in LINBO. In Windows ist die Zeit damit allerdings noch nicht synchronisiert. Wurde, wie zuvor beschrieben, der Win10-PC der Domäne hinzugefügt, dann erfolgt automatisch die Zeitsynchronisation des Client mit dem AD-Server / Domaincontroller.

Bei der Synchronisation zwischen Client und Server kann es zu Beginn zu Zeitabweichungen kommen.

Hinweis: Die Systemzeit sollte möglichst synchron mit dem Server sein, um Probleme mit der Domänenanmeldung, dem Domänenbeitritt zu vermeiden! Auch andere Dienste (z.B. WSUS, KMS, ...) machen bei Zeitdifferenzen Probleme.

Achtung: Wurde der linuxmuster.net Server vor Oktober 2022 installiert und treten hier noch Fehler auf, dann ist ggf. die Samba-Konfiguration für die Zeitsynchronisation zu korrigieren. Hinweise finden sich hier: <https://github.com/linuxmuster/linuxmuster-base7/issues/144>

Domänenjoin verloren

Hast z.B. nicht daran gedacht, nach dem Domänenjoin ein Image zu erstellen, so kann die Vertrauensstellung zwischen Client und Server verloren gegangen sein.

Dies kannst Du wie folgt reparieren:

1. Melde Dich lokal am Windows-PC als admin an. Klicke mit der rechten Maustaste auf das Windows-Symbol unten links.
2. Wähle dann in dem Kontextmenü Windows PowerShell(Administrator) aus.
3. Es öffnet sich die PowerShell-Eingabekonsolle von Windows mit Administrator-Berechtigungen.
4. Gib in der Windows PowerShell(Administrator) folgenden Befehl an:

```
Reset-ComputerMachinePassword -Credential global-admin
```

5. Erstelle anschließend ein neues Image.

fehlendes Verzeichnis linuxmuster-win

1. Die Global-Registry-Patch-Datei liegt als Vorlage auf dem Server in \\server\srv\linbo\examples und heißt win10.global.reg. Diese muss auf den Client kopiert, angepasst und auf dem Client eingespielt werden.

Gehe wie folgt dabei vor:

a) Installiere Dir zuerst auf dem Windows-Client das freie Programm WinSCP (Freeware). Dieses kannst Du hier herunterladen: <https://winscp.net/download/WinSCP-6.1.2-Setup.exe>

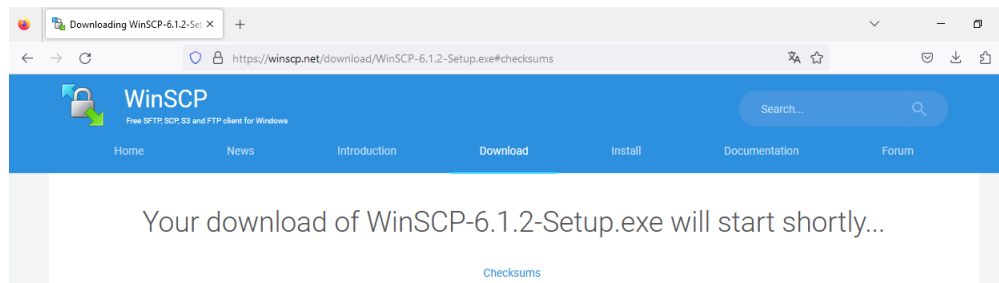


Abb. 363: WinSCP herunterladen

b) Überprüfe, ob die Prüfsumme des heruntergeladenen Programms korrekt ist, um sicherzustellen, dass Du keine kompromittierte Version heruntergeladen hast. Die korrekten SHA-Prüfsummen des Zertifikats für WinSCP sind:

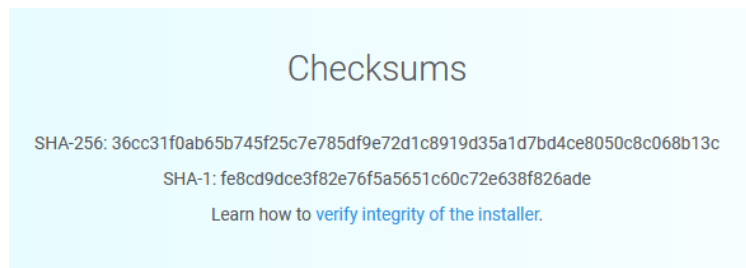


Abb. 364: Prüfsummen von WinSCP

Führe auf die heruntergeladene Datei einen Rechtsklick aus und klicke auf Eigenschaften.

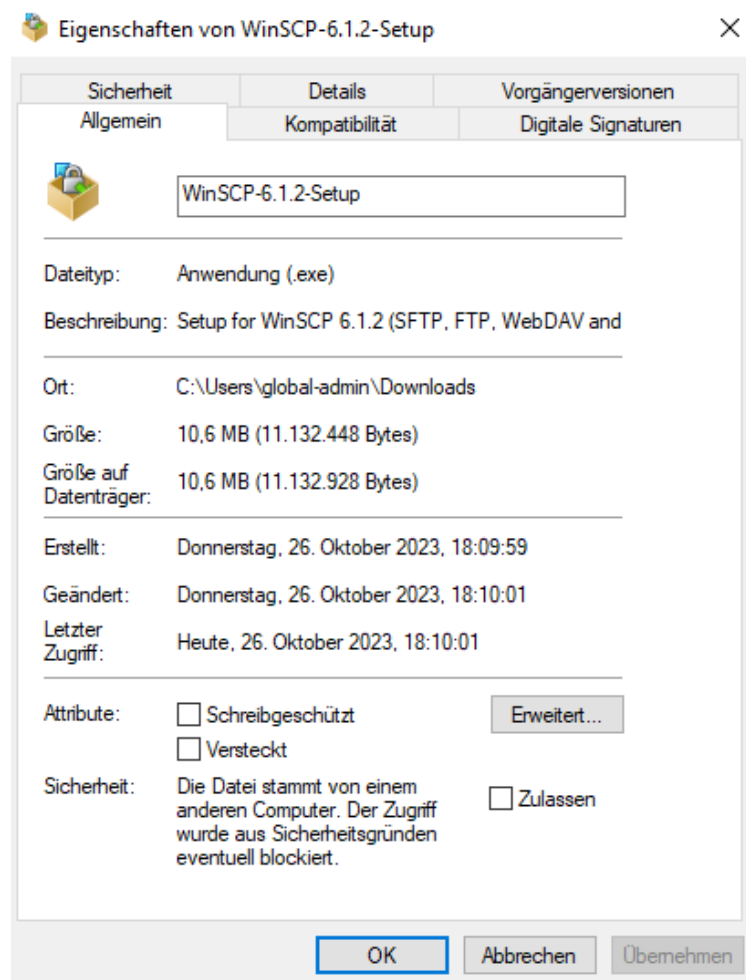


Abb. 365: WinSCP: Eigenschaften der heruntergeladenen Datei

Klicke nun auf die Reiterkarte **Digitale Signaturen**, markiere den Digestalgorithmus SHA-256 in der Signaturliste und klicke auf **Details**. Klicke dann auf **Zertifikat anzeigen** und im nächsten Fenster auf die Reiterkarte **Details**. Gehe in der Liste mit den Feldern bis zu dem Eintrag **Fingerabdruck**. Der hier angezeigte Wert muss mit dem auf dem Bild dargestellten übereinstimmen.

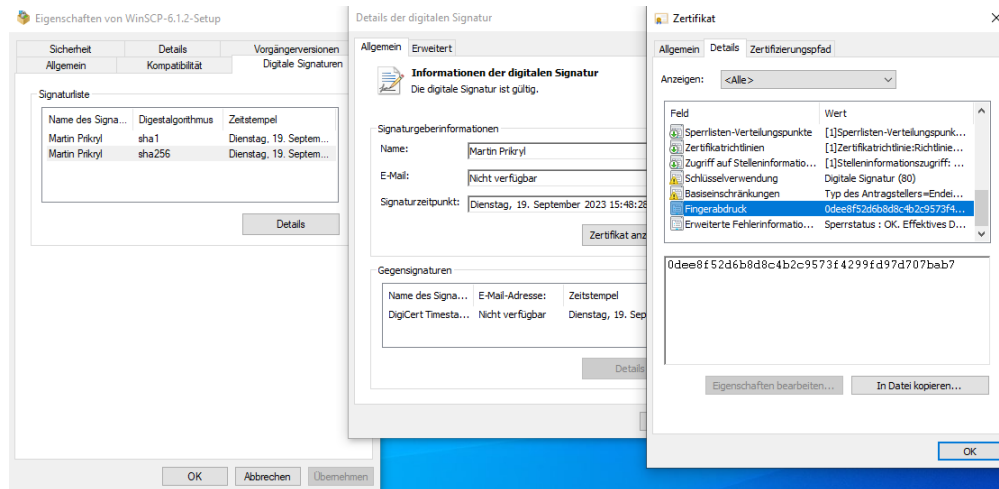


Abb. 366: WinSCP: Fingerprint der Signatur prüfen

Stimmt diese überein, so führe die Installation durch. Wähle während die Installation die Commander - Oberfläche aus.

c) Öffne nun das Programm WinSCP. Es erscheint direkt ein Anmeldefenster. Trage hier folgende Werte ein:

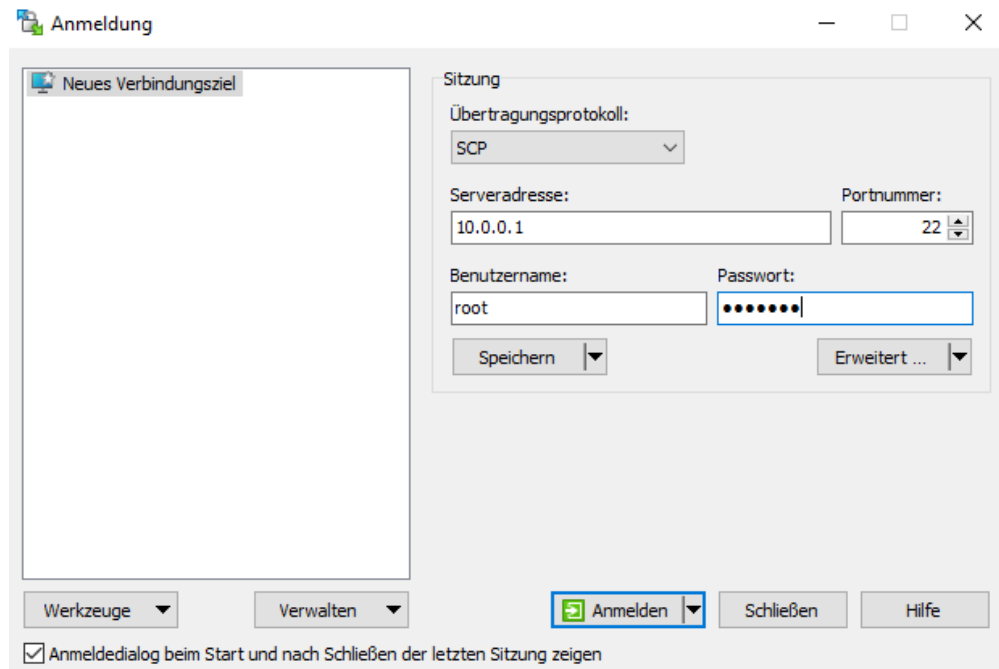


Abb. 367: WinSCP: Anmeldefenster

d) Klicke danach auf **anmelden**. Bei der ersten Anmeldung erhältst Du noch ein Hinweisfenster zu dem Hostschlüssel des Servers. Klicke hier auf **Ja**, um diesen im Speicher abzulegen.

e) Klicke nun im rechten Fenster, in dem der Inhalt des Servers dargestellt wird auf **/srv/linbo/examples/**.

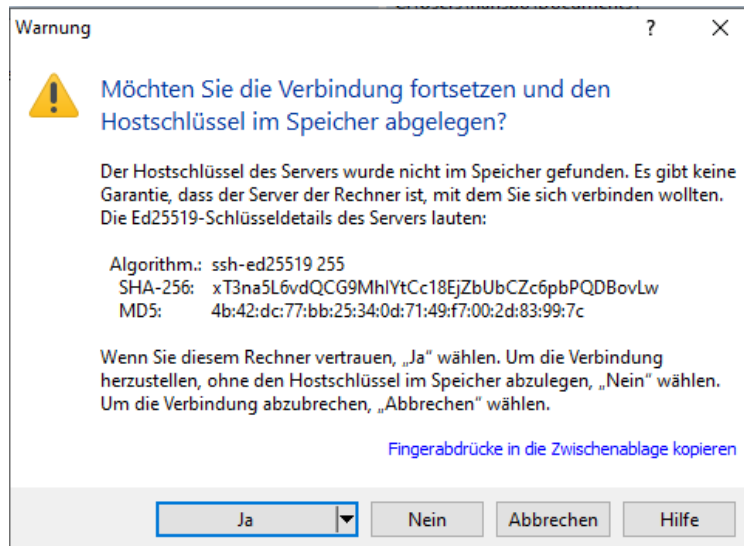


Abb. 368: Nehme den Hostschlüssel des Servers bei der ersten Anmeldung an

Wähle hier - wie in der Abb. markiert - die Datei `win10.global.reg` aus. Klicke links in dem Fenster, in dem der Inhalt Deines Win10-Clients dargestellt wird auf `c:\users\global-admin\Desktop\`.

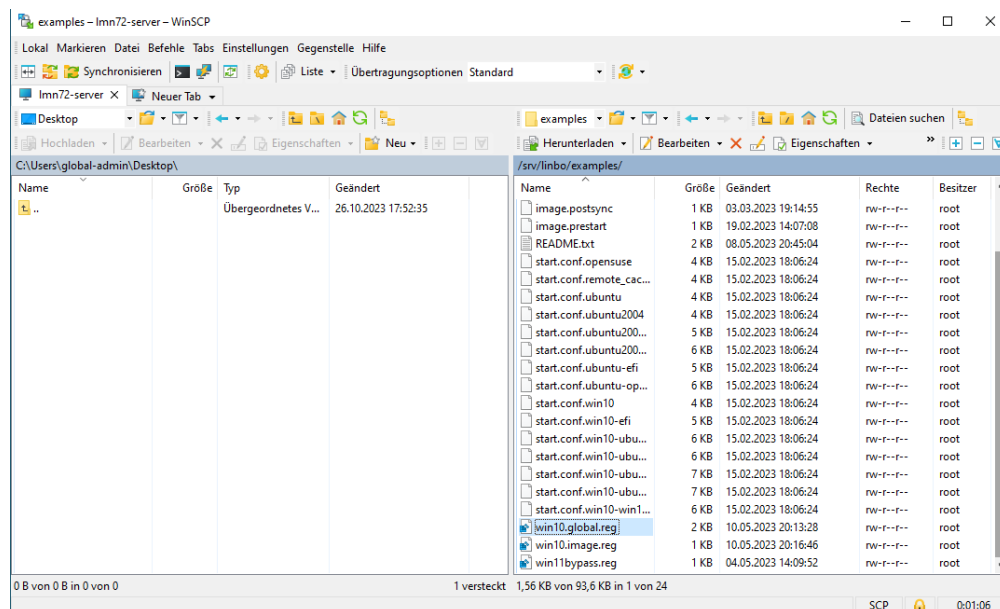


Abb. 369: WinSCP: Verzeichnisse auswählen

- Kopiere die Datei `win10.global.reg` auf den Desktop, in dem Du diese mit der linken Maustaste in WinSCP aus dem rechten Fenster in das linke Fenster ziehst. Danach erhältst Du die Rückfrage, ob Du die Datei wirklich herunterladen möchtest:
- Schließe WinSCP wieder.
- `Win10.global.reg` anpassen

Die Datei `win10.global.reg` befindet sich nun auf dem Desktop Deines Win10-Clients.

- Führe danach den einen Neustart aus und gehe zu *Manueller Domänen Join für Windows*

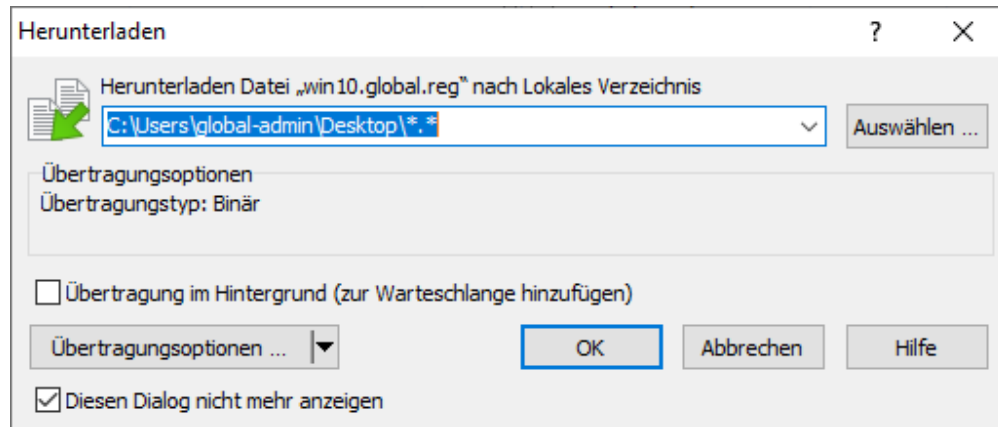


Abb. 370: Bestätige das Kopieren der Datei auf den Desktop mit OK

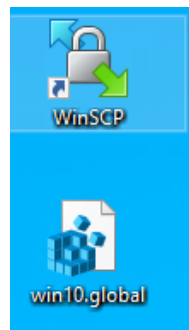


Abb. 371: Du findest nun die Datei win10.global.reg auf dem Desktop

Hinweis: Damit Clients in die Domäne aufgenommen werden können, muss auf dem Server vorher die Standard-GPO erzeugt werden. Dies ist auch notwendig, wenn ausschließlich Linux-Clients eingesetzt werden.

Die Standard-GPO wird auf dem Server erzeugt durch:

```
# sophomoric-school --gpo-create default-school
```

Anschließend den Samba-Dienst noch neu starten:

```
# systemctl restart samba-ad-dc.service
```

4.12 Upgrade v7.1 auf v7.2

1. Bringe zuerst den lmn7.1 Server auf den aktuellsten Paketstand.

Führe dazu in der Konsole folgende Befehle aus:

```
sudo apt update
sudo apt dist-upgrade
```

2. Aktualisiere danach das Betriebssystem auf dem Server von Ubuntu 18.04 LTS auf die Version Ubuntu 20.04 LTS. Nutze dazu den Befehl `do-release-upgrade`.

Gib dazu auf der Server-Konsole ein:

```
linuxadmin@server:~$ sudo -i
root@server:~$ do-release-upgrade
```

Nach der Überprüfung siehst Du, wieviele Pakete aktualisiert, neu installiert und gelöscht werden. Bestätige den Vorgang zur Durchführung des Upgrades mit `j`.

Während des Upgrades erhältst Du mehrere Nachfragen. Für einige Dienste (z.B. samba, ssh) wirst Du gefragt, ob die Konfigurationsdatei aktualisiert werden soll.

Achtung: Die Nachfrage zur Aktualisierung der Konfigurationsdateien für diese Dienste musst Du unbedingt mit `N` beantworten. Beispiele (keine Garantie auf Vollständigkeit) sind: `/etc/security/limits.conf`, `/etc/ntp.conf`, `/etc/system/system.conf`, `/etc/samba/smb.conf`, `/etc/ssh/sshd_config`

Zudem müssen während oder nach der Installation einiger neuerer Bibliotheken einige Dienste neu gestartet werden. Diese werden Dir in einer Liste angezeigt. Bestätige deren Neustart mit `OK`.

Danach wirst Du gefragt, ob Du die lokale Version bestimmter Dienste beibehalten möchtest. Beantworte dies jeweils mit `Ja/OK`.

Nach der Aktualisierung der Pakete wirst Du gefragt, ob die alten Pakete entfernt werden sollen. Bestätige dies mit `J`.

Danach wirst Du aufgefordert das System neu zu starten. Führe einen Reboot aus.

3. Aktualisiere danach das Betriebssystem auf dem Server von Ubuntu 20.04 LTS auf die nachfolgende Version Ubuntu 22.04 LTS. Nutze dazu den Befehl `do-release-upgrade`.

Der weitere Ablauf ist identisch zu den unter 2.) beschriebenen Schritten.

4. Führe die erneute Konfiguration der lmn-Pakete aus. Rufe dazu folgenden Befehl auf:

```
linuxadmin@server:~$ sudo -i
root@server:~$ dpkg-reconfigure sophomorix-samba linuxmuster-base7 linuxmuster-webui7
```

5. Aktiviere das lmn71-Repository wieder, indem Du die Datei `/etc/apt/sources.list.d/lmn71.list` editierst und dort das während des Upgrades automatisch eingefügte Kommentarzeichen `#` entfernst.

Zudem oder alternativ findest Du die Datei `/etc/apt/sources.list.d/lmn71.list.distUpgrade`, in der das Repository der lmn 7.1 auskommentiert ist.

6. Füge danach das Repository der lmn72 wie folgt hinzu:

Importiere zuerst die Schlüsseldatei:

```
root@server:~$ sudo sh -c 'wget -qO- "https://deb.linuxmuster.net/pub.gpg" | gpg --
↳dearmor -o /usr/share/keyrings/linuxmuster.net.gpg'
```

Hinweis: Bei `wget -qO-` ist der Großbuchstabe O zu verwenden - n i c h t die Zahl 0.

Füge danach das Linuxmuster 7.2 Testing-Repro hinzu:

```
root@server:~$ sh -c 'echo "deb [arch=amd64 signed-by=/usr/share/keyrings/linuxmuster.
↳net.gpg] https://deb.linuxmuster.net/ lmn72 main" > /etc/apt/sources.list.d/lmn72.list'
```

Aktualisiere nun die Paketquellen:

```
root@server:~$ apt update
```

7. Aktualisiere die installierten Pakete und führe anschließend ein Reboot durch:

Achtung: Die Nachfrage zur Aktualisierung der Konfigurationsdateien für Dienste musst du in diesem Schritt (im Gegensatz zur Systemaktualisierung in Schritt 2 und 3) mit `I` oder `Y` akzeptieren. Beispiele (keine Garantie auf Vollständigkeit) sind: `/etc/default/linbo-torrent`

```
root@server:~$ apt dist-upgrade
root@server:~$ reboot
```

8. Nach dem Neustart führe den Import der Geräte erneut aus:

```
sudo linuxmuster-import-devices
```

9. Starte nun die Clients neu. Du wirst zunächst noch die Version 4.0 von Linbo auf den Clients nach dem ersten Start sehen. Starte den Client ein zweites Mal und Linbo wird dann automatisch auf dem Client auf die Version 4.2 aktualisiert.

10. Synchronisiere das Betriebssystem und melde Dich danach mit einem Domänen-Benutzer an.

Achtung: Beim Upgrade von Ubuntu 18.04 über Ubuntu 20.04 zu 22.04 LTS werden die Einstellungen für CUPS zwar korrekt übernommen. Allerdings treten für einige Drucker Fehler auf. Es ist in diesen Fällen sinnvoll die Druckerinstallation erneut durchzuführen. Für viele HP-Drucker ist es hilfreich die Bibliothek `hplip` auf dem Server nachzuinstallieren - siehe zu den Druckern [Drucker einbinden](#).

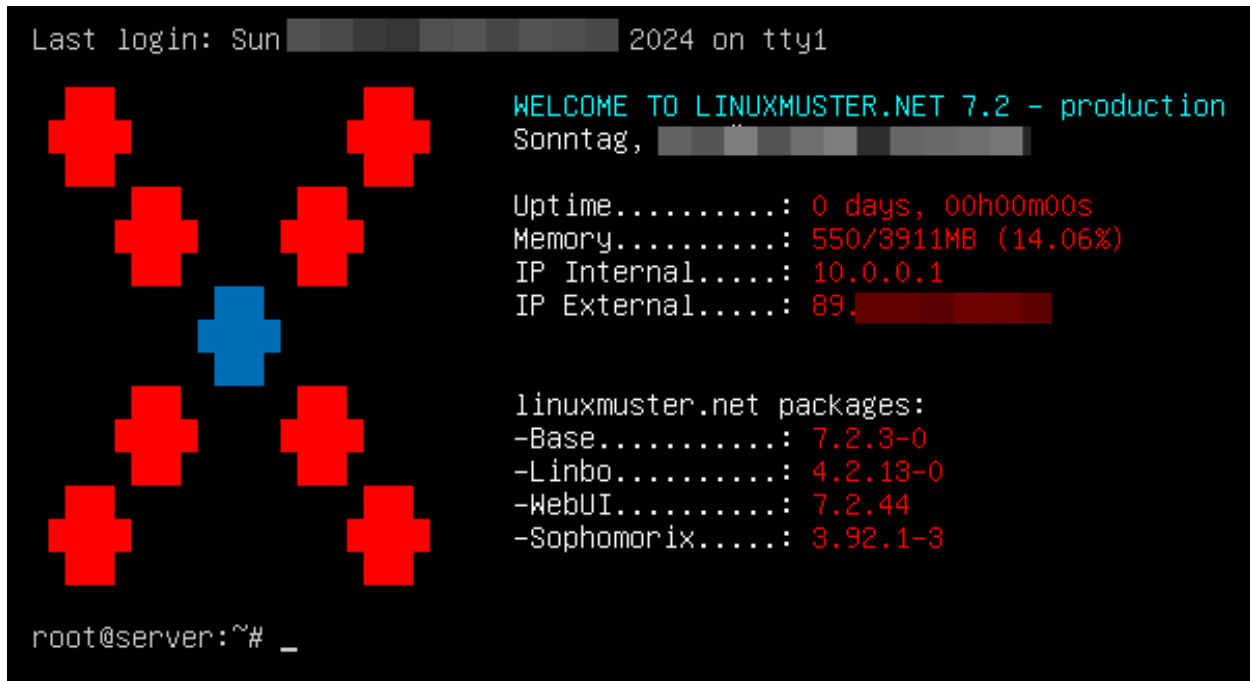


Abb. 372: Server-Infos nach dem Konsolen-Login

4.13 Migration LINBO 2.4 zu 4.2

Autor des Abschnitts: @cweikl

4.13.1 Hinweise zu LINBO 4.2

In der `linuxmuster` v7.2 löst LINBO 4.2 das bisherige LINBO 2.4 ab. Bereits ab v7.1 gibt es nur noch ein Debian-Paket für LINBO (`linuxmuster-linbo7`) und eines für die grafische Oberfläche (`linuxmuster-linbo-gui7`), die nur noch LINBO 4 und eine grafische Oberfläche enthalten.

Hast Du auf linuxmuster v7.2 umgestellt, ist es sinnvoll, die bisherigen LINBO 2.4 Cloop-Images zu konvertieren.

LINBO 4.2 weist einige Besonderheiten auf:

- Neues Image-Format mit Abwärtskompatibilität zum alten Format für eine einfache Migration
- Änderungen an der Namensgebung und des Speicherortes der zum Image zugehörigen Dateien
- Es wird nur noch 64-Bit Client-Hardware unterstützt.
- LINBO 4.2 kann nicht mit linuxmuster v6.2 und kleiner verwendet werden.
- Es werden differentielle Images ab LINBO >= 4.1 unterstützt.
- Erweiterte LINBO-Client Shell
- WLAN-Unterstützung
- Unterstützung eigener Boot-Skripte
- Einbindung des aktuellsten Linux-Kernels (z.B. > 6.6) - alternativ kann auch ein LTS-Kernel (6.1.*), ein legacy Kernel (5.15.*) oder ein eigener Kernel eingebunden werden.

Neues Image-Format

Das neue Image-Format heißt *qcow2*. *qemu-img* wird nun genutzt, um die Erstellung und Wiederherstellung der *qcow2*-Images durchzuführen.

- Für neue Images wird nur noch das Format *qcow2* unterstützt.
- Images im *cloop*-Format werden aber weiterhin an Clients ausgeliefert.
- Bisherige Images im *cloop*-Format können in das neue *qcow2*-Format einfach konvertiert werden.

Folgende Änderungen sollte man auch beachten:

- Der Name des Basis-Images muss aufgrund des Formatwechsels in der übernommenen *start.conf* angepasst werden (z.B. *image.qcow2* statt *image.cloop*).
- Die Benennung der zusätzlichen Image-Dateien **.postsync*, **.prestart* and **.reg* ändern sich, so dass das Image-Format nicht mehr in den Dateinamen mit angegeben wird (z.B. *image.postsync* statt *image.cloop.postsync* oder *image.prestart* statt *image.cloop.prestart*).
- Der Ablageort der neuen Images und der zugehörigen zusätzlichen Dateien ist */srv/linbo/images/<imagename>/*. Diese Verzeichnisstruktur wird aber nicht in der *start.conf* angegeben.
- Backups von Images werden jetzt nach */srv/linbo/images/<imagename>/backups/<timestamp>* verschoben.

4.13.2 Konvertieren der LINBO 2.4 Images

1. Konvertiere Deine Cloop-Images in das *qcow2* Format mithilfe von *linbo-cloop2qcow2*. Wechsle dazu in das Linbo-Verzeichnis und rufe den Befehl mit dem zu konvertierenden Dateinamen auf:

```
cd /srv/linbo
linbo-cloop2qcow2 ubu22.cloop
```

Das Cloop-Image wird dadurch in das *qcow2*-Format konvertiert und im Verzeichnis */srv/linbo/images/ubu22/* als Datei *ubu22.qcow2* abgelegt.

Hinweis: Images von Windows-Systemen könnten nach der Konvertierung ggf. nicht so funktionieren wie vorgesehen - dies gilt insbesondere für UEFI-Systeme. In diesem Fall ist es notwendig, ein neues Image zu erstellen.

2. Ändere den Dateinamen des Images in the *start.conf* der jeweiligen Hardwareklasse/Gruppe. Das Ablageverzeichnis des Images wird dabei nicht genannt, obiges Beispiel: *BaseImage = ubu22.qcow2*
 3. Starte die Dienste zur Image-Verteilung neu mit: `systemctl restart linbo-torrent.service`.
-

Wichtig: Starte alle Clients zweimal, um sicherzustellen, dass LINBO v2 auf v4 aktualisiert wurde.

4. Zum Schluss starte das Skript *linuxmuster-import-devices*. Dieses löscht die nun nicht mehr benötigten *start.conf*-Links.
5. Ab jetzt kannst Du Images wieder wie gewohnt erstellen und verteilen.

4.13.3 Widerspenstige LINBO-Clients

Möchtest Du, bestehende LINBO-Clients zu LINBO 4 migrieren und hast dabei Probleme, obwohl Du - wie zuvor beschrieben - den Befehl `linuxmuster-import-devices` ausgeführt hast, solltest Du nachstehend beschriebene Schritte ausführen.

Wichtig ist, dass vor dem Upgrade alle Clients das aktuelle LINBO im Cache haben. Falls es nach dem Upgrade beim Booten von LINBO trotzdem zu Fehlern kommt, kannst Du so vorgehen:

1. Auf dem Server temporär den LINBO-Netboot erzwingen:

```
# cd /srv/linbo/boot/grub/  
# cp grub.cfg grub.cfg.bak  
# cp /usr/share/linuxmuster/linbo/templates/grub.cfg.forced_netboot grub.cfg
```

2. Clients per PXE booten.
3. Prüfe, ob die Clients wirklich via PXE Network Boot starten, damit hierdurch die Clients auf die letzte LINBO-Version aktualisiert werden.
4. Nehme die Änderungen nun wieder zurück.

```
# cd /srv/linbo/boot/grub/  
# cp grub.cfg.bak grub.cfg
```

5. Starte die Clients erneut.

4.14 Migration auf linuxmuster 7.2

Autor des Abschnitts: @cweikl

Um auf die linuxmuster 7.2 zu migrieren, können zwei Wege genutzt werden:

1. Sollte noch eine linuxmuster 6.2 genutzt werden, so ist eine vollständige Migration durchzuführen. Diese ist deutlich aufwändiger. Gehe zum Kapitel: *Migration lmn 6.2 -> lmn 7.2*
2. Wird bereits linuxmuster 7.1 eingesetzt, besteht die Migration auf linuxmuster 7.2 in einem einfachen Upgrade des Servers und einer anschließenden Migration der bisherigen Linbo 2.4 Images auf Linbo 4. Gehe zum Kapitel: *Upgrade v7.1 auf v7.2*

4.14.1 Migration lmn 6.2 -> lmn 7.2

Autor des Abschnitts: @jeffbeck, @Tobias, @cweikl (Voraussetzungen) @MachtDochNix (Review)

Es wird eine Migration der

- Benutzerinformationen (Namen, Passwort, Projekte),
- Computerinformationen (`workstations`),
- der Benutzerdaten (`/home`),
- Tausch- und Projektverzeichnisse und der
- Geräte-Abbilder (`/var/linbo`) unterstützt.

Nicht migriert werden

- Beschreibungen von Projekten,

- Quota-Tabellen und
- Rollen, die Geräte bekommen.

Diese müssen von Hand angepasst werden.

Ebenso werden die Dienste mrbs, openSchulPortfolio und der Mail-Server nicht migriert, da diese - wenn benötigt - zur Installation in einem Dockercontainer übernommen werden müssen.

Voraussetzungen

Bestehendes System

Es muss als Quellsystem linuxmuster.net in der Version 6.2 installiert sein.

Es ist möglich, dass auch ab Version 6.1 und 6.0 eine Migration funktioniert. Dies wurde nicht offiziell getestet.

Neues v7.2 System

Es wird davon ausgegangen, dass ...

- der Server der Version 7.2 und eine Firewall (Standard OPNSense®) zur Verfügung stehen.
- das Setup wie zuvor beschrieben ausgeführt wurde und ohne Fehler durchgelaufen ist.
- nach der Installation keine zusätzlichen Benutzer, Gruppen und Projekte angelegt wurden.

In dieser Beschreibung wird als Schulinstanz, wie beim Erstsetup vorgegeben, `default-school` beibehalten.

Achtung: Solltest Du in der linuxmuster.net v6.2 bereits Netzsegmente gebildet und/oder Netzbereiche geändert haben, dann beachte nachstehendes Unterkapitel mit Hinweisen zum korrekten Vorgehen.

Hinweis: Dieser Teil kommt aus der Dokumentation der Version 7, und dient der Übernahme. Die einzelnen Schritte können so übernommen werden, allerdings der Workflow und die Beschreibung der Kommando-Parameter sind zu überarbeiten.

System mit Netzanpassungen .. —————

Solltest Du in der linuxmuster.net v6.2 andere Netzbereiche konfiguriert haben, die jetzt weiter genutzt werden sollen, oder hast Du das Netz in Subnetze aufgeteilt und möchtest bei der Migration diese Subnetze mit umstellen, dann ist nachstehendes Vorgehen unbedingt bereits beim Erstsetup der VMs der v7.2 zu beachten.

Ablauf .. ———

1. VMs erstellen (*Install-from-Scratch*)
2. VMs starten
3. IPs der OPNSense® auf die bisher verwendeten IPs/Netze anpassen
4. ServerVM mit netplan die IPs so ändern, dass diese die korrekte IP im internen (grünen) Netz haben wie bisher
5. VMs vor dem Setup auf die neue Netzstruktur vorbereiten (*Netzbereich anpassen*)
6. Erreichbarkeit der VMs im internen Netz testen.
7. Update der VMs durchführen
8. Erstsetup durchführen (*Setup v7.2*)

IPs OPNsense® anpassen .. —————

Die IP der externen Schnittstelle (WAN) der OPNsense® ist ggf. anzupassen. Diese ist in der Erstausslieferung so konfiguriert, dass diese eine IP via DHCP erhalten würde. Sollte die OPNsense® Firewall hinter einem Router arbeiten, so kann eine Anpassung für eine statische IP erforderlich sein.

Hierzu rufst Du auf der Konsole in der OPNsense®, nachdem Du Dich als `root` angemeldet hast, den Punkt 2) `Set interface IP address` auf. Sollte eine DHCP-Konfiguration in Deinem Netz hier nicht möglich sein, wählst Du zunächst die WAN-Schnittstelle aus und trägst die IP Adresse aus Deinem lokalen Netz mit korrekter Subnetzmaske, Gateway und DNS ein.

Danach wählst Du die *LAN-Schnittstelle* aus und konfigurierst die bisherige IP, die im IPFire bereits genutzt wurde. Hast Du z.B. ein Subnetting für das Server-Netz in der v6.2 genutzt, das im „grünen“ Netz den Bereich 10.16.1.0/24 vorsieht, so vergibst Du hier auf der LAN-Schnittstelle der OPNsense® die IP 10.16.1.254/24 (Subnetmask 255.255.255.0 = 24 Bit).

Bei vorhandener Subnettierung dürfte für o.g. Beispiel der L3-Switch im Server - VLAN die IP 10.16.1.253 haben. Zudem ist darauf zu achten, dass auf der Virtualisierungsumgebung die korrekten Bridges für das jeweilige VLAN den Schnittstellen der VMs korrekt zugeordnet wurden.

VMs vorbereiten .. ^^^^^^^^^^^^^^^

netplan .. " " " " " " " " " " " "

Die Server-VM muss nun vorbereitet werden.

In der Datei `/etc/netplan/01-meine-netzconfig.yaml` - Name bitte auf Dein System anpassen - sind die Netzwerkeinstellungen wie folgt zu ändern (**Hinweis:** nachstehende Angaben greifen o.g. Beispiel hier nur für die Server-VM auf):

```
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: no
      dhcp6: no
      addresses: [10.16.1.1/24]
      gateway4: 10.16.1.254
      nameservers:
        addresses: [10.16.1.254, 10.16.1.1]
```

Danach speicherst Du die Änderungen und wendest diese mit folgendem Befehl an und testest, ob die Firewall im internen Netz erreichbar ist:

```
netplan apply
ping 10.16.1.254
```

Erhältst Du erfolgreich Pakete zurück, so kannst Du die Firewall erreichen.

Können alle VMs im internen Netz sich untereinander via ping erreichen, bereitest Du die VMs mit `linuxmuster-prepare` vor. siehe: [Netzbereich anpassen](#)

linuxmuster-prepare .. " " " " " " " " " " " "

Jetzt meldest Du Dich auf der Eingabekonsolle an der Server-VM an.

Du bereitest diese VMs für der Erstsetup vor, indem Du die korrekten Angaben zur gewünschten IP der VM und der Firewall mit `linuxmuster-prepare` (siehe: [Netzbereich anpassen](#)) angibst.

Gehen wir davon aus, dass Du für die Server VM im vorangegangenen Schritt die IP *10.16.1.1/24* und für die OPNsense® als Firewall die IP *10.16.1.254/24* zugeordnet hast. Zudem nehmen wir an, dass Deine zukünftige Schuldomäne den Namen *schuldomaene* erhalten wird und Deine Domain *meineschule.de* lautet.

Mit diesen Vorgaben bereitest Du die Server-VM nun mit folgendem Befehl auf das Setup vor:

```
./lmn-appliance -s -u -d schuldomaene.meineschule.de -n 10.16.1.1/24 -f 10.16.1.254
```

Starte nach den Anpassungen die VM neu mit `reboot`.

Tests & Setup ..

Teste nun die Erreichbarkeit der VMs im internen Netz mit folgenden Befehlen (angepasst auf o.g. Bsp.):

```
ping 10.16.1.254
ping 10.16.1.1
```

Funktioniert dies korrekt, so kann jetzt die Aktualisierung der VM erfolgen.

Aktualisiere die VM mit folgendem Befehl:

```
apt update
apt dist-upgrade
```

Starte danach die VM neu.

Nach dem Neustart meldest Du Dich an der Server-VM als Benutzer *root* an und ruft das Setup mit folgendem Befehl auf:

```
linuxmuster-setup
```

Nach erfolgreichem Setup *Setup v7.2* durchläufst Du die nachstehend dargestellten Schritte zur Migration.

Vorgehen zur Migration ..

1. Zunächst installiert man auf dem Quellsystem (Version 6.x) das Paket *sophomorix-dump* und exportiert die Daten (ca. 15MByte).
2. Danach importiert man diese Daten auf einem Zielsystem (Version 7.x) und rekonstruiert dort Benutzer, Passwörter, Projekte und Geräte, etc.
3. Es müssen manuell die Verzeichnisse */home/share*, */home/teachers* und */home/students* im Zielsystem gemountet werden (z.B. über eine externe Festplatte und *bind-mount*, *Netzwerk-mount*, etc.) und importiert werden.
4. Die Daten von LINBO können ebenso wie Benutzerdaten synchronisiert werden.

Export der Daten unter linuxmuster.net 6.x ..

Der Server 6.x muss sich in einem synchronisierten Zustand befinden, d.h. der Befehl auf der Konsole *sophomorix-check* darf keine hinzuzufügenden oder zu verändernden Benutzer anzeigen. Dafür führt man folgende Schritte als *root* nacheinander aus:

```
# sophomorix-check
...
# sophomorix-add
...
# sophomorix-move
...
# sophomorix-kill
...
```

Jetzt sollte ein `sophomorix-check` keine Benutzer mehr verändern wollen.

`sophomorix-dump` installieren .. _____

Installiere jetzt `sophomorix-dump` aus dem babo-Repository oder lade das entsprechende Debian-Paket von der Webseite herunter

```
server ~ # apt-get update
server ~ # apt-get install sophomorix-dump
...
sophomorix-dump (3.63.2-1) wird eingerichtet ...
```

Alternativ kannst Du (z.B. wenn Du das babo-Repository nicht einbinden kannst) unter <http://pkg.linuxmuster.net/babo/> die neueste Version `sophomorix-dump_u.v.w-z_all.deb` herausfinden, herunterladen und installieren:

```
server ~ # wget http://pkg.linuxmuster.net/babo/sophomorix-dump_3.63.2-1_all.deb
server ~ # dpkg -i sophomorix-dump_3.63.2-1_all.deb
...
sophomorix-dump (3.63.2-1) wird eingerichtet ...
```

Daten exportieren .. _____

Führe das Skript `sophomorix-dump` aus

```
server ~ # sophomorix-dump
...
* Dump OK: /root/sophomorix-dump/data/etc/linuxmuster/subnets
##### End: Results of dump #####
WARNINGS in Results of dump are OK:

/etc/sophomorix/virusscan/sophomorix-virusscan-excludes.conf
/etc/sophomorix/virusscan/sophomorix-virusscan.conf
/var/lib/sophomorix/virusscan/penalty.db
are only needed, if you had configured sophomorix for scanning viruses
```

Die Zusammenfassung zeigt Fehler und Warnungen an. Warnungen und der folgende Fehler: `ERROR dumping: /root/sophomorix-dump/data/etc/sophomorix/user/mail/*` können ignoriert werden.

Die exportierten Daten (bis zu 15MByte) liegen jetzt in `/root/sophomorix-dump`. Kopiere dieses Verzeichnis auf den Server mit Version 7.x. Um die exportierten Daten wieder zu löschen, führe `sophomorix-dump.. --clean` aus.

Import der Daten unter linuxmuster.net 7.x .. =====

Installiere die `sophomorix-vampire`-Skripte über

```
server ~ # apt update
server ~ # apt install sophomorix-vampire
...
```

Das Skript `sophomorix-vampire -h` zeigt Optionen und Schritte an, die im folgenden durchgeführt werden.

Kompletter Import mit `sophomorix-vampire-example` .. _____

Beispielhaft führt das Skript `sophomorix-vampire-example` alle Schritte für eine typische Schule durch. Es empfiehlt sich das Skript in den übertragenen Ordner `sophomorix-dump` zu kopieren und an die eigenen Bedürfnisse anzupassen. Besonders der Import der Nutzerdaten sollte in der folgenden Schritt-für-Schritt Anleitung genau geprüft werden.

1. Analyse der exportierten Daten .. _____

Die folgende Analyse zeigt

```
server ~ # sophomorph-vampire.. --datadir /path/to/dir/sophomorph-dump --analyze
```

ERROR:

z.B. fehlende Dateien (/etc/sophomorph/user/mail/* wird dagegen nicht in jeder Installation verwendet)

INFO:

z.B. Gruppen, die während der Migration umbenannt werden

WARNING:

z.B. Warnungen, welche Dateien überschrieben werden

2. Migration der Klassen .. —————

Alle Klassen werden vor den Benutzern migriert, inklusive eventueller Umbenennungen der Klassennamen wie in der Analyse angezeigt. Dafür erstellt man zunächst das Klassenskript und führt es danach aus

```
server ~ # sophomorph-vampire.. --datadir /path/to/dir/sophomorph-dump --create-class-
↪script
server ~ # /root/sophomorph-vampire/sophomorph-vampire-classes.sh
```

Jetzt können die neu erstellten Klassen überprüft werden, beispielsweise

```
server ~ # sophomorph-class -i
server ~ # sophomorph-class -i.. --class teachers
```

3. Migration der Benutzer .. —————

Zunächst muss die Passwortlängen und -komplexitätsüberprüfung von Samba 4 so eingestellt werden, dass bisherige einfache Passwörter erlaubt sind.

```
server ~ # samba-tool domain passwordsettings set.. --complexity=off
server ~ # samba-tool domain passwordsettings set.. --min-pwd-length=1
```

Jetzt wird aus den exportierten Daten eine Datei `sophomorph.add` erzeugt, die an die richtige Stelle im System kopiert werden muss, um danach die Benutzer regulär aufzunehmen.

```
server ~ # sophomorph-vampire.. --datadir /path/to/dir/sophomorph-dump --create-add-file
server ~ # cp /root/sophomorph-vampire/sophomorph.add /var/lib/sophomorph/check-result/
↪sophomorph.add
```

Folgender Schritt informiert vorab mit **ERRORS** und **WARNINGS** über mögliche Fehlermeldungen bei der geplanten Aufnahme. Diese Fehler sollten manuell in der Datei `/var/lib/sophomorph/check-result/sophomorph.add` korrigiert werden.

```
server ~ # sophomorph-add -i
...
WARNING:
ERROR:
...
```

Die Aufnahme der Benutzer wird ca. 1 Sekunde Zeit pro Benutzer in Anspruch nehmen, Zeit einen Tee zu trinken.

```
server ~ # sophomorph-add
...
```

Die Aufnahme

- nimmt die Benutzer mit ihren Erstpasswörtern auf, dies kann mit

```
server ~ # sophomorphix-passwd.. --test-firstpassword
...
```

getestet werden, was hier zu 100% funktionieren sollte. Im nächsten Schritt folgt der Import der aktuellen Passworthashes.

- gibt den Benutzern zunächst keine Rechte für die WebUI/Schulkonsole. Dies folgt in einem späteren Schritt.

4. Passworthashes importieren .. —————

Die mit Hash codierten Passwörter werden mit folgendem Befehl importiert und sollte keine Fehler erzeugen

```
server ~ # sophomorphix-vampire.. --datadir /path/to/dir/sophomorphix-dump --import-user-
↳ password-hashes
...
0 ERRORS:
```

Jetzt müssen die standardmäßig komplexen Passwörter wieder aktiviert werden

```
server ~ # samba-tool domain passwordsettings set.. --complexity=default
server ~ # samba-tool domain passwordsettings set.. --min-pwd-length=default
```

Tests .. ^^^^

Jetzt sollten für Konten bei denen nicht mehr das Erstpasswort gilt, der folgende Test fehlschlagen. Für alle Konten mit Erstpasswörtern sollte er noch funktionieren.

```
server ~ # sophomorphix-passwd.. --test-firstpassword
```

Zeige einen oder mehrere Benutzer an

```
server ~ # sophomorphix-user -i
server ~ # sophomorphix-user -i.. --user name
server ~ # sophomorphix-user -i.. --user na*
```

5. Klassenadministratoren importieren .. —————

Wie bisher

```
server ~ # sophomorphix-vampire.. --datadir /path/to/dir/sophomorphix-dump --create-class-
↳ adminadd-script
server ~ # /root/sophomorphix-vampire/sophomorphix-vampire-classes-adminadd.sh
```

6. Projekte importieren .. —————

Im nachfolgenden Schritt werden alle Projekte importiert.

```
server ~ # sophomorphix-vampire.. --datadir /path/to/dir/sophomorphix-dump --create-project-
↳ script
server ~ # /root/sophomorphix-vampire/sophomorphix-vampire-projects.sh
```

Tests .. ^^^^

Zeige ein oder mehrere Projekte an


```
server ~ # sophomorix-project -i
server ~ # sophomorix-project -i -p name | p_name
server ~ # sophomorix-project -i -p p_na*
```

7. Konfigurationsdateien importieren .. —————

Mit folgendem Schritt werden wichtige Konfigurationsdateien verändert.

Das Skript muss zwei Mal ausgeführt werden.

```
server ~ # sophomorix-vampire.. --datadir /path/to/dir/sophomorix-dump --restore-config-
↪files
...
server ~ # sophomorix-vampire.. --datadir /path/to/dir/sophomorix-dump --restore-config-
↪files
```

Hinweis: Jetzt solltest Du noch die Datei `school.conf` bearbeiten, denn das wird nicht automatisch gemacht.

8. Updates diverser Einstellungen .. —————

Grundsätzlicher Durchlauf von `sophomorix-check` muss funktionieren:

```
server ~ # sophomorix-check
```

Stelle sicher, dass keine weiteren Benutzer hinzugefügt werden müssen:

```
server ~ # sophomorix-add -i
```

Mit folgendem Schritt werden

- Benutzernamen in UTF-8 konvertiert (ab jetzt sind Umlaute und Sonderzeichen in Namen möglich),
- Zugriffsrechte in der Schulkonsole gesetzt

```
server ~ # sophomorix-update
```

Lösche die Benutzer, die nach Deinen Einstellungen in `school.conf` fällig werden.

```
server ~ # sophomorix-kill
```

Tests .. ^^^^

So kann man überprüfen, ob Sonderzeichen in `students.csv` oder `teachers.csv` in das System übernommen wurden:

```
server ~ # sophomorix-user -i -u <user_with_umlaut>
```

9. Rechner importieren .. —————

```
.. --dryrun ohne funktion
server ~ # linuxmuster-import-devices.. --dry-run
```

```
server ~ # linuxmuster-import-devices
```

Tests .. ^^^^

Überprüfe, ob einzelne Rechner vorhanden sind:

```
server ~ # sophomorph-device -d firewall -i  
server ~ # sophomorph-device -r no-pxe -i
```

Überprüfe ob die Namensauflösung funktioniert:

```
server ~ # sophomorph-device.. --dns-test
```

10. Überprüfung von Benutzern und Gruppen .. _____

Benutzer und Gruppen können mit folgendem Skript getestet werden:

```
server ~ # sophomorph-vampire.. --datadir /path/to/dir/sophomorph-dump --verify-uidi
```

Fehler: Kommando liefert

Unknown option: verify-uid Command line:

You have made a mistake, when specifying options. See error message above.

... sophomorph-vampire is terminating

11. Synchronisiere Benutzerdaten .. _____

Zunächst müssen über irgendein Verfahren die Verzeichnisse `/home/share`, `/home/teachers` und `/home/students` vom Quellsystem im Zielsystem unter einem Pfad (hier im Beispiel: `/mnt`) erscheinen.

```
/mnt/home/share  
/mnt/home/students  
/mnt/home/teachers
```

Der Pfad im Zielsystem wird über das Kommandozeilenargument `--path-oldserver /mnt` an nachfolgende Skripte übergeben und erwartet dann die obige Ordnerstruktur unterhalb von `/mnt`.

Für einzelne Schüler, Lehrer, Klassen und Projekte sollte man eine Synchronisation testen:

```
server ~ # sophomorph-vampire.. --rsync-student-home <studentname> --path-oldserver /mnt  
server ~ # sophomorph-vampire.. --rsync-teacher-home <teachername> --path-oldserver /mnt  
server ~ # sophomorph-vampire.. --rsync-class-share <classname> --path-oldserver /mnt  
server ~ # sophomorph-vampire.. --rsync-project-share <projectname> --path-oldserver /mnt
```

Jetzt können alle Schüler, Lehrer, Klassen und Projekte in einem Schritt importiert werden

```
server ~ # sophomorph-vampire.. --rsync-all-student-homes --path-oldserver /mnt  
server ~ # sophomorph-vampire.. --rsync-all-teacher-homes --path-oldserver /mnt  
server ~ # sophomorph-vampire.. --rsync-all-class-shares --path-oldserver /mnt  
server ~ # sophomorph-vampire.. --rsync-all-project-shares --path-oldserver /mnt
```

12. Synchronisiere LINBO-Daten .. _____

Alle Daten von LINBO können ebenso wie die Benutzerdaten aus dem früheren Verzeichnis `/var/linbo` importiert werden.

```
/mnt/var/linbo
```

Auch hier wird beispielsweise der Inhalt von `/var/linbo` in das Zielsystem nach `/mnt` eingebunden. Das Skript erwartet dann die obige Ordnerstruktur unterhalb von `/mnt`.

```
server ~ # sophomorix-vampire.. --rsync-linbo --path-oldserver /mnt
```

Jetzt muss LINBO erneut installiert werden, um Änderungen, die nur unter linuxmuster.net v7 existieren, importiert werden

```
server ~ # apt-get.. --reinstall install linuxmuster-linbo7 linuxmuster-linbo-common7
```

13. Dinge, die manuell gemacht werden müssen .. _____

- Beschreibungen zu Projekten hinzufügen
- Die Rolle von Geräten festlegen
- Quota für die Benutzer (neu) festlegen
- Bei migrierten Subnetzen: Es muss in `/etc/linuxmuster/subnets.csv` das Gateway für das Servernetz eingetragen werden, z.B. 10.0.0.253 für einen L3-Switch. Danach muss `linuxmuster-import-subnets` ausgeführt werden.

4.15 Migration eines bestehenden Linux-Clients

Autor des Abschnitts: @cweikl, @dorian

Wird ein Ubuntu 20.04 Linux-Client eingesetzt, so kann dieser vorbereitete Client migriert werden, so dass die aktuell gepflegten Pakete für `linuxmuster-linuxclient7` genutzt werden können.

4.15.1 Vorgehen

1. VM anlegen und vorbereiten wie unter *Rechneraufnahme* beschrieben.
2. Für Linbo die `start.conf` der Hardwareklasse anpassen, so dass das bisherige Image angegeben wird.
3. Start der VM via PXE
4. Anmelden als Benutzer `linuxadmin`
5. ggf. Backup der eigenen Skripte unter `/etc/linuxmuster-client` - diese werden automatisch gelöscht!
6. Entferne den alten Linux-Client vollständig
7. Entferne das alte Proxy-Skript auf dem Client
8. Entferne `lightdm` als Anmeldemanager
9. Installiere `gdm3` als Anmeldemanager
10. Führe das Setup des neuen Pakets `linuxmuster-linuxclient7` aus (*Linux-Client*)
11. Erstelle ein neues Image.

Achtung: Du musst als Benutzer `linuxadmin` angemeldet bleiben, solange bis das Setup des neuen Pakets `linuxmuster-linuxclient7` vollständig abgeschlossen ist!

Zu den Schritten 6. bis 10. findest Du nachstehend Hinweise zur Umsetzung.

4.15.2 Entferne die alten Linux-Client Pakete

Hast Du den alten Linux-Client in der VM erfolgreich gestartet, meldest Du Dich als Benutzer `linuxadmin` an. Entferne danach die alten Linux-Client Pakete mit folgendem Befehl:

```
sudo apt purge linuxmuster-client-adsso
```

4.15.3 Anmeldemanager wechseln

Das neue Paket `linuxmuster-linuxclient7` benötigt als Anmeldemanager `gdm3` und `Gnome`, so dass zuerst der bisherige Anmeldemanager zu deinstallieren ist. Die Dokumentation geht hier dabei davon aus, dass `lightdm` zu deinstallieren ist. Ggf. musst Du das auf Deinen genutzten Anmeldemanager anpassen.

Lösche den Anmeldemanager `lightdm` mit dem Befehl:

```
sudo apt purge lightdm
```

Danach installierst Du `gdm3` mit:

```
sudo apt install --reinstall gdm3
```

Räume danach die Pakete im apt-cache auf:

```
sudo apt autoremove
```

Achtung: Bleibe weiterhin als Benutzer `linuxadmin` angemeldet, solange bis Du das Setup des neuen Paketes `linuxmuster-linuxclient7` abgeschlossen hast.

Führe nun alle Schritte zur Installation und zum Setup des neuen `linuxmuster-linuxclient7` Pakets aus wie diese im Kapitel *Linux-Client* beschrieben sind.

Nach Abschluss des Setups erstellst Du ein neues Image.

4.16 Clients in der linuxmuster.net

Autor des Abschnitts: @cweikl, @MachtDochNix

Die Bereitstellung und Pflege der schulischen Rechner für die Nutzer in einer `linuxmuster.net` Umgebung erfolgt mittels LINBO.

LINBO steht für GNU/ LI nux N etwork BO ot.

Es wurde ursprünglich im Auftrag des Landesmedienzentrums Baden-Württemberg von der Firma KNOPPER.NET in Zusammenarbeit mit den damaligen `paedML-Linux`- und heutigen `linuxmuster.net`-Entwickler realisiert.

Durch die letztgenannten ist es nun in der Version 4 erschienen. Der Sourcecode ist unter GNU General Public License 3.0 auf GitHub veröffentlicht. <https://github.com/linuxmuster/linuxmuster-linbo7>

4.16.1 Funktionsweise

Zum Verständnis erklären wir Dir einen

Start eines Arbeitsplatzrechners

Über das Transport-Protokoll TFTP wird vom linuxmuster.net-Server und die PXE-Implementierung von Grub bootet es ein kleines Linux-System (linbofs) auf den Clients. Diese zeigen dann eine Benutzeroberfläche, mit der dann alle Imaging-Aufgaben auf dem Client gesteuert werden.

Die steuerbaren Funktionen unterscheiden sich anhand der Berechtigungen der Nutzer und Nutzerinnen.

Konsolen-Tools sind ebenfalls verfügbar, um Clients und Imaging aus der Ferne über den Server zu verwalten.

Auswahl eines Betriebssystems

Die Funktionsweise wird am Beispiel eines Clients (rechts im Bild) beschrieben. Auf dem Server (links im Bild) sind zwei Betriebssysteme für Clients dieses Typs komprimiert gespeichert.

- Der Benutzer wählt das erste Betriebssystem zum synchronisierten Start aus.
- Der Client überprüft, ob sein lokal gespeichertes Systemabbild identisch ist mit dem auf dem Server (1.).
- Ist dieses der Fall und entpackt der Client das erste Betriebssystem auf die eigentliche System-Partition und startet das System anschließend (3.). Wäre das nicht der Fall gewesen, hätte dieser zuerst das Systemabbild vom Server heruntergeladen (2.), um dann mit (3.) fortzufahren.

Der hier aufgezeigte Ablauf eines synchronisierten Startes ist einer von vielen und dient der Veranschaulichung.

- Start wie in der vorherigen Sitzung
- Start mit erzwungener Formatierung der Betriebssystem-Partition
- Offline-Boot
- u. a.

Deren Beschreibung ist im Unterkapitel *LINBO4 nutzen* zu finden.

In dem gezeigten Ablauf eines synchronisierten Betriebssystem-Starts wurde ersichtlich, das sich auf dem Server mindestens ein Client-Image befinden muss. Dabei ist folgendes von entscheidender Wichtigkeit:

In der linuxmuster.net 7 ist es für Clients, denen alle pädagogischen Funktionen im Netz zur Verfügung stehen sollen, erforderlich, dass diese im Active Directory (AD) des Servers (samba 4) einen sog. Domänenbeitritt ausführen. Hierbei werden Schlüssel erzeugt und ausgetauscht. Diese stellen sicher, dass der Client als berechtigtes Gerät erkannt wird.

Ziel ist es, dass alle PCs mit einem vordefinierten Muster-Image für Linux oder Windows genutzt werden, sodass nach Möglichkeit nur ein Image oder wenige raumbezogene Images gepflegt werden.

Hierzu ist zunächst ein Rechner mit dem gewünschten Client-Betriebssystem und den gewünschten Programmen zu installieren und vorzukonfigurieren. Dieser Muster-Client muss dann mit dem jeweiligen Betriebssystem einen Domänenbeitritt ausführen, auch dieser wird im Image gespeichert. Erst danach kann dieses Image ebenfalls für alle anderen PCs genutzt werden.

Das Vorgehen wird Dir detailliert unter *Muster-Client aufsetzen* beschrieben.

4.17 LINBO4 nutzen

LINBO steht für GNU/Linux Network **B**oot. Es wurde ursprünglich im Auftrag des Landesmedienzentrums Baden-Württemberg von der Firma KNOPPER.NET in Zusammenarbeit mit den damaligen paedML-Linux- und heutigen linuxmuster.net-Entwicklern realisiert. Der Sourcecode ist unter GNU General Public License Version 2 veröffentlicht.

LINBO bietet

- Vollautomatisches Ausrollen von Client-Installationen im Netzwerk
- Verwaltung mehrerer Betriebssystem-Installationen auf einem Client (Multiboot)
- Minutenschnelle automatische Reparatur des Betriebssystems (Sheila-Prinzip)
- Konfigurierbarer Autostart
- Grafische Client-Oberfläche zur einfachen Bedienung durch Anwender und Netzwerkbetreuer
- Vollständige Integration in linuxmuster.net

LINBO4, das von linuxmuster.net entwickelt wurde, weist einige Neuerungen auf:

- Für neue Images wird nur noch das Format qcow2 unterstützt. Der Name des Basis-Images muss daher in der übernommenen start.conf angepasst werden (z.B. image.qcow2).
- Die Benennung der zusätzlichen Image-Dateien postsync, prestart and reg ändert sich, so dass diese nur noch ohne dem Image-Format angegeben werden (z.B. image.postsync, image.prestart and image.reg, früher: image.cloop.postsync etc.).
- qemu-img wird nun genutzt, um die Erstellung und Wiederherstellung der qcow2-Images durchzuführen.
- Es wird nur noch 64 Bit Client-Hardware unterstützt.
- linuxmuster.net <=6.2 wird nicht mehr unterstützt.
- Ab LINBO v4.1 stehen differentielle Images zur Verfügung.
- Bisherige Images im cloop Format sind direkt in das neue qcow2 Format zu konvertieren.
- AB LINBO v4.1.36 wird Kernel 6.5.3 verwendet und es können qcow2-Images mit Torrent verteilt werden, die > 52 GiB sind. Für ctorrent kann hierzu die sog. piece length konfiguriert werden.

Dieses Kapitel führt Dich in die Nutzung von LINBO4 ein und erklärt die wesentlichen Schritte zur Imageverwaltung.

Hinweis: Die meisten PC mit UEFI verwenden standardmäßig „SecureBoot“. Dies muss deaktiviert werden, um Linbo booten zu können!

4.17.1 Der LINBO Startbildschirm

Wird der Arbeitsplatzrechner (Client-PC) über das Netzwerk gebootet, startet LINBO und zeigt folgenden Bildschirm, wenn der PC noch nicht aufgenommen / registriert wurde.

Sobald der Client registriert wurde, zeigt der Startbildschirm weitere Optionen an.

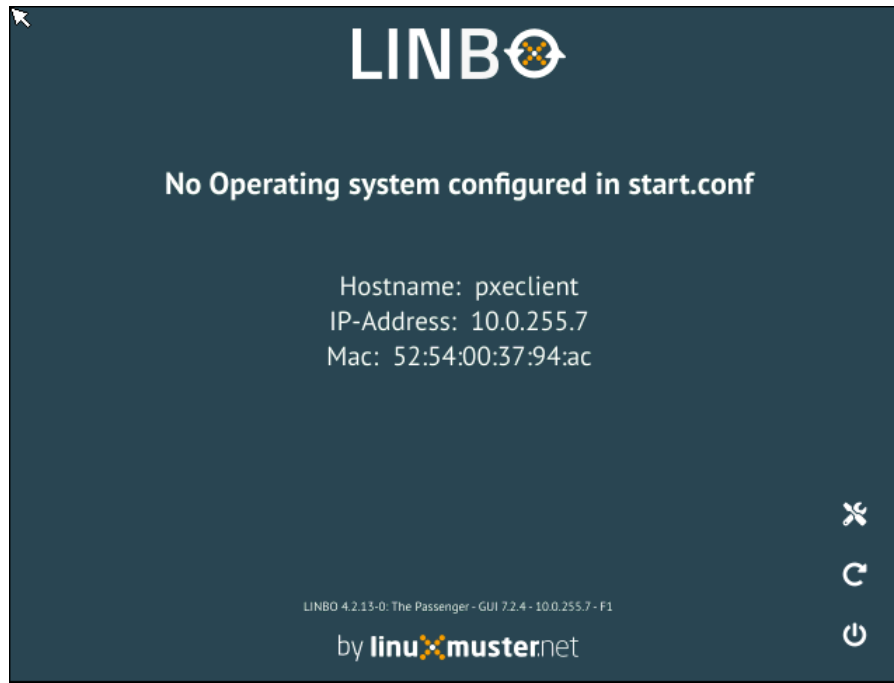


Abb. 373: Linbo Startbildschirm

Informationen

Drückst Du im Startbildschirm die Funktionstaste F1, dann werden Dir Informationen zum Client angezeigt.

Host

Der festgelegte Hostname oder „pxeclient“, wenn der Client nicht registriert ist.

Gruppe

Die festgelegte Hardwareklasse

IP-Address

Die festgelegte Netzwerkadresse oder „OFFLINE“, wenn der Client ohne Netzwerkverbindung zum Server gestartet wurde.

Mac

Die Hardware-Adresse des Clients.

HD, CPU, RAM

Zeigt die entsprechend verbaute Hardware des Clients an: Festplattengröße, Prozessor und Hauptspeicherinformationen

Cache

Zeigt die freie/gesamte Partitionsgröße der Cache-Partition an.



Abb. 374: Linbo Startbildschirm eines aufgenommenen Clients



Abb. 375: Client Informationen - F1

Reboot



Erzwingt einen Neustart.

Neustart



Lässt den Client herunterfahren.

Start-Icons

Pro festgelegter Partition (mit Betriebssystem oder ohne) erscheinen nach dem Start von Linbo ein großer Knopf und mehrere kleinere Knöpfe mit folgenden Bedeutungen



Abb. 376: Sync+Start Icon

Synchronisiert das System mit dem letzten aktuellen Image (hier Ubuntu). Bei Windows-Systemen wird eine bereitgestellte Registry-Patch-Datei angewendet. Bei Linux-Systemen werden Hostname und Rootpartition gepatcht. Falls ein neueres Image auf dem Server liegt, wird dies zunächst heruntergeladen.

Startet das System im aktuellen Zustand, unsynchronisiert. Es werden keine Patches angewendet.

Bemerkung: Die einzelnen Schaltflächen für die Startmechanismen können auch ausgegraut sein, wenn der Administrator den jeweiligen Mechanismus deaktiviert hat.

Tools-Icon

Um Images zu verwalten, klickst Du zunächst auf das Werkzeug-Icon.

Der Bereich ist mit dem Passwort von LINBO abgesichert. Dies entspricht dem LINBO-Administrator Kennwort. Dies ist nach dem Setup zunächst identisch mit dem festgelegten root / global-admin Kennwort.

Achtung: Bei der Eingabe des LINBO-Passwortes werden keine Zeichen angezeigt, weder das Passwort selbst, noch Sterne.



Abb. 377: Start Icon



Abb. 378: Neu+Start Knopf

Formatiert die relevante Partition neu, synchronisiert das System von Grund auf mit dem aktuellen Image und startet das System wie bei „Sync+Start“.



Abb. 379: Werkzeug-Icon



Abb. 380: LINBO Passwort

Passwort für „LINBO“ ändern

Das Passwort steht im Klartext auf dem Server in der Datei `/etc/rsyncd.secrets` und kann einfach mit einem Editor geändert werden.

```
# modified by linuxmuster-setup
# /etc/rsyncd.secrets
```

```
linbo:MeinKennwort
```

Nach Änderung des Passwortes musst Du auf dem Server noch die `linbofs.lz` neu erstellen, damit der Hash-Wert des aktuellen Linbo-Passwortes integriert wird. Dazu führst Du folgenden Befehl auf dem Server aus:

```
update-linbofs
```

4.17.2 LINBO Imageverwaltung am Client

Über den Tab Tools erhält der Administrator neue Funktionen.

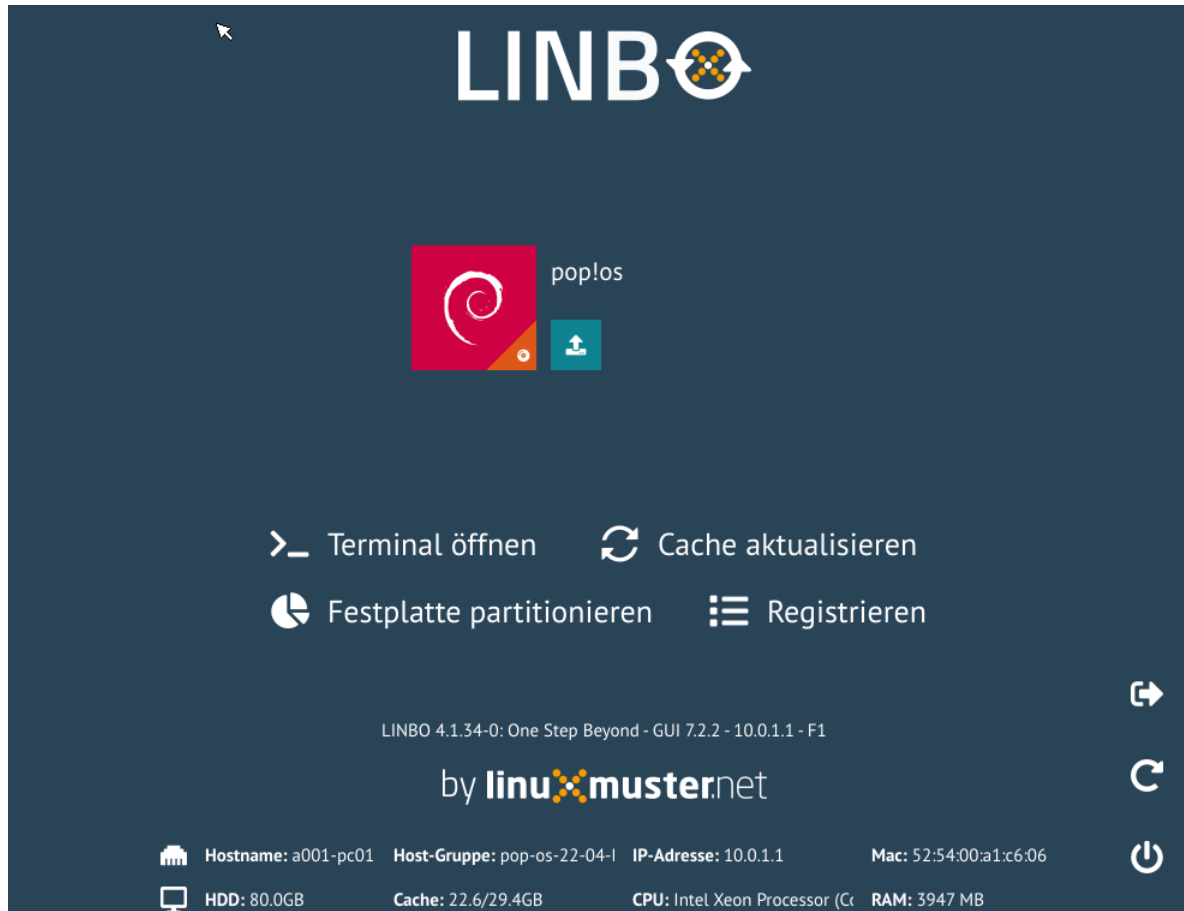


Abb. 381: LINBO Tools

Für jedes definierte Betriebssystem gibt es Schaltflächen für die Funktionen

Es öffnet sich ein neues Dialogfenster, über das man ein neues Image erstellen (und hochladen) kann.



Abb. 382: Image erstellen



Abb. 383: Image hochladen

Es öffnet sich ein neues Dialogfenster, über das man das aktuelle Image auf den Server hochladen kann.

Daneben gibt es Schaltflächen für folgende administrative Funktionen:



Abb. 384: Console

Du kannst eine (rudimentäre) Console öffnen, um Shell-Befehle abzusetzen und Fehler zu diagnostizieren.

Üblicherweise wird eine Partition auf dem Client als Cache festgelegt. Mit dieser Schaltfläche kann der Cache aktualisiert werden, d.h. alle für diesen Client nötigen Images und postsync-Dateien werden gegebenenfalls heruntergeladen.

Partitioniert die gesamte Festplatte gemäß der Vorgabe der Hardwareklasse.

Öffnet den Registrierungsdialog zur erstmaligen Aufnahme dieses Rechners.

Rufe zur Imageerstellung die entsprechende Schaltfläche auf:

Dialog: Image erstellen

Ab der LINBO Version 4.1 kannst Du wählen, ob Du ein neues Basisimage oder ein differentielles Image erstellen möchtest. Sollte bereits ein Basisimage existieren, so wird dieses mit überschrieben. Es erfolgt keine weitere Rückfrage.

Lokal im Cache wird das aktuelle Image beim Erstellen überschrieben. Beim Hochladen des aktuellen Images mit demselben Namen wird auf dem Server zuvor ein Backup des vorherigen Images erstellt.

Auf dem Server finden sich die Images im Verzeichnis `/srv/linbo/images/<hardwareklasse>/`. Die Backups der Images finden sich auf dem Server im Verzeichnis `/srv/linbo/images/<hardwareklasse>/backups`.

In der WebUI können die LINBO-Images komfortabel verwaltet werden (*LINBO-Imageverwaltung*).

Warnung: Vergibt man einen neuen Dateinamen, sollte man sicher stellen, dass die Cache-Partition über ausreichend Platz verfügt, da das alte Image ebenfalls im Cache gespeichert bleibt. Ist nicht genügend Platz vorhanden, dann schlägt das Erstellen des Images fehl. Hier ist vor der Erstellung eines neuen Images sicherzustellen, dass die lokale Cache-Partition vorab geleert wird.

Siehe hierzu das Unterkapitel zum Linbo4-Cache am Ende dieses Hauptkapitels.

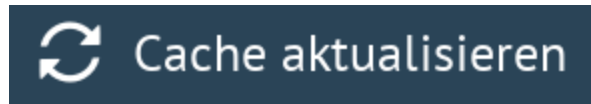


Abb. 385: Cache aktualisieren



Abb. 386: Partitionieren

Es gibt die Optionen `erstellen`, `erstellen+hochladen`. Mit der Option `erstellen` wird das neue Image nur lokal im LINBO-Cache erstellt. Die Option `erstellen + hochladen` erstellt zuerst das Image lokal im LINBO-Cache und lädt danach das Image auf den Server.

Dialog: Image hochladen

Wie beim Dialog zum Erstellen des Images, kann hier explizit nur ein ausgewähltes Image hochgeladen werden und der Rechner zum Abschluss neu gestartet oder heruntergefahren werden. In der Drop-down Liste werden nur dann Images angezeigt, wenn diese bereits im Cache vorhanden sind.

Dialog: Console

Der einfache Konsolendialog erlaubt die Eingabe einzelner Befehle in die untere Zeile.

Dialog: Cache aktualisieren

Der lokale Cache wird aktualisiert. Es werden die drei Möglichkeiten der Synchronisation zur Auswahl gegeben: Rsync, Multicast oder Torrent.

Dialog: Partitionieren

Es wird noch einmal gefragt, ob man wirklich alle Daten auf der Festplatte löschen will. Danach kann man mit „Cache aktualisieren“ auch wieder die Images vom Server in den Cache kopieren.



Abb. 387: Registrieren



Abb. 388: Image erstellen

Image erstellen

Auszuführende Aktion:

☒ Neues Basisimage erstellen

☐ Neues differentielles Image erstellen

Image Beschreibung:

Pop!OS 22.04 LTS konsolidiertes Image mit allen Anpassungen

Was soll nach dem Ende des Prozesses passieren?

☒ nichts

☐ herunterfahren

☐ neu starten

☐ abmelden

erstellen

erstellen + hochladen

abbrechen

Abb. 389: LINBO - Image erstellen



Abb. 390: LINBO Image hochladen

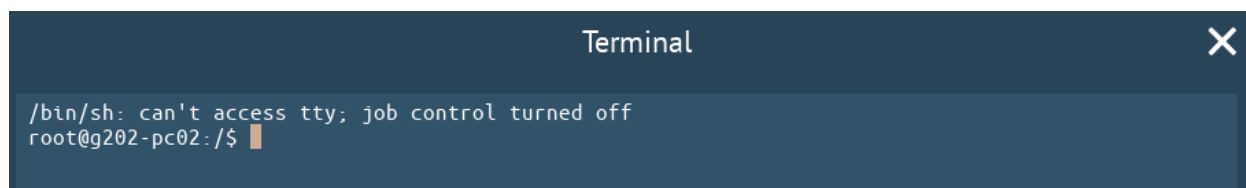


Abb. 391: LINBO Konsole

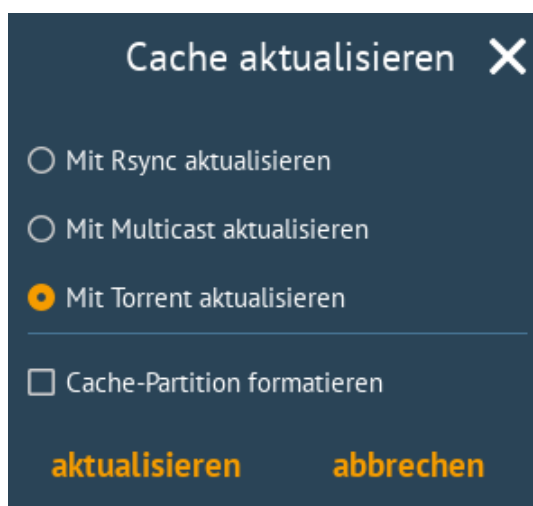
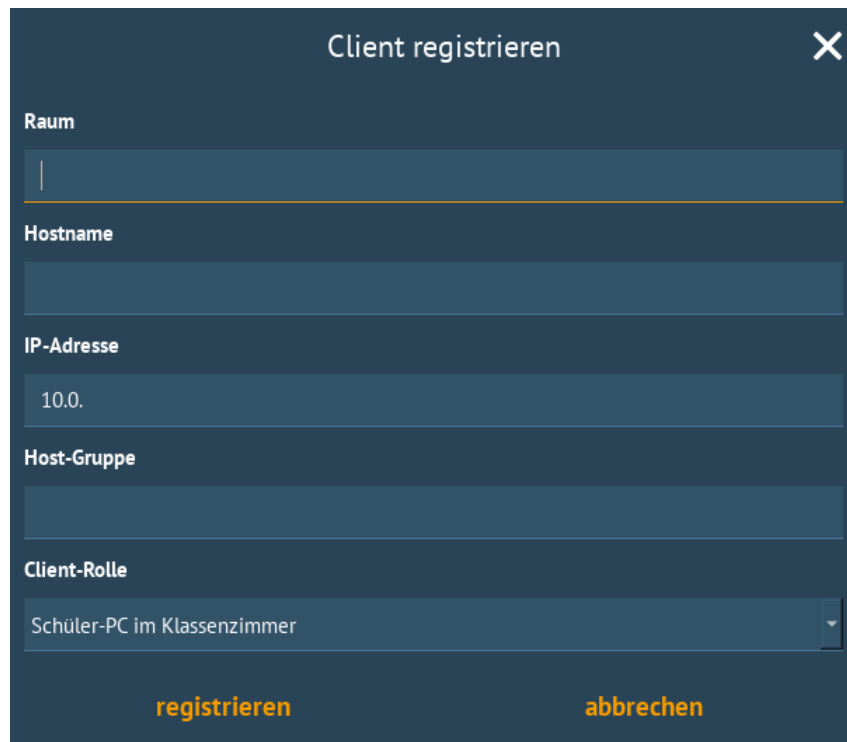


Abb. 392: LINBO Update Cache

Dialog: Registrieren

Client registrieren

Raum

Hostname

IP-Adresse

10.0.

Host-Gruppe

Client-Rolle

Schüler-PC im Klassenzimmer

registrieren abbrechen

Abb. 393: LINBO Client registrieren

Mit diesem Dialog kann ein erstmalig genutzter Rechner registriert werden. Dafür müssen alle Eingabefelder entsprechend ausgefüllt werden.

Bemerkung: Bitte trage für die Rechnergruppe einen Namen ohne Bindestriche `` - `` ein.

4.17.3 LINBO Differenzielle Images

Hinweis: Seit der Version LINBO 4.1 ist es möglich, differentielle Images zu erstellen.

Differentielle Images bauen auf einem vollständigen Image eines Client-Betriebssystems auf und legen alle Änderungen / Ergänzungen seit dem letzten Image ab. Diese werden dann bei einer Synchronisation des Clients vollständig angewendet.

Werden nur kleine Ergänzungen auf dem Client vorgenommen, kann ein differenzielles Image erstellt werden, um das Verteilen der Änderungen möglichst schnell für alle Clients einer Hardware-Klasse durchzuführen. Für die Aktualisierung der Clients werden so, deutlich weniger Daten via Netzwerk übertragen.

Sollten für ein Basisimage bereits mehrere differenzielle Images erstellt worden sein, so kann es sinnvoll sein, wenn viel neue Software installiert wurde, diese wieder durch Erstellung eines Vollimages zu konsolidieren.

Vorbereitungen

Der betreffende Muster-Client wurde entsprechend angepasst und alle erforderlichen Schritte zur Erstellung eines Images auf Client-Seite durchgeführt.

Für Linux-Clients ist z.B. der Befehl

```
sudo linuxmuster-linuxclient7 prepare-image
```

auszuführen.

Danach ist der Client neu zu starten.

Image erstellen

Erscheint die LINBO GUI:



Abb. 394: LINBO GUI

Wähle rechts das Werkzeug-Icon



Abb. 395: Tools Icon

aus.

Es erscheint ein neues Fenster, in dem Du das Passwort des Linbo-Admins eingeben musst, um dich zu authentifizieren.

Das Kennwort ist bei Eingabe nicht sichtbar. Klicke auf **anmelden**. Es erscheint das Werkzeug-Menü.

Zur Erstellung eines differenziellen Images klicke nun auf das große Icon zur Erstellung eines Images.

Es erscheint das Menü zur Erstellung neuer oder differenzieller Images.

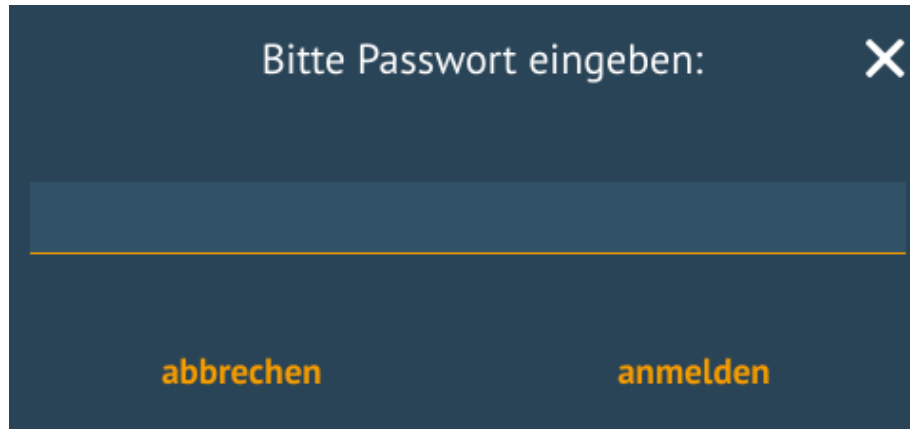


Abb. 396: LINBO Passwort



Abb. 397: LINBO Image Menü



Abb. 398: Icon neues Image

Image erstellen

Auszuführende Aktion:

☐ Neues Basisimage erstellen

☒ Neues differentielles Image erstellen

Image Beschreibung:

Differentielles Image: Neues Screenshot - Programm

Was soll nach dem Ende des Prozesses passieren?

☒ nichts

☐ herunterfahren

☐ neu starten

☐ abmelden

erstellen

erstellen + hochladen

abbrechen

Abb. 399: LINBO Image erstellen

Wähle die Option **Neues differenzielles Image erstellen** aus, trage eine nachvollziehbare Beschreibung für das Image als Text ein.

Wähle zur Erstellung des differenziellen Images den Eintrag **erstellen + hochladen** aus, damit zuerst auf dem Client das Image erstellt und dieses im Anschluss auf den Server geladen wird.



Abb. 400: Image erstellen + hochladen

Es werden bei der Erstellung des Images in der Linbo-GUI weitere Status-Meldungen angezeigt. Ist der Prozess der Erstellung und das Hochladen des differenziellen Images auf den Server abgeschlossen, siehst Du folgende Meldung:



Abb. 401: LINBO Image erstellt

Starte im Anschluss LINBO neu, indem Du das entsprechende Icon auswählst:



Abb. 402: Icon neu starten

Image synchronisieren

Nachdem LINBO neu gestartet wurde, erscheint wieder die LINBO-GUI.

Wende nun das differenzielle Image auf den Client an, indem Du das grosse Icon zur Synchronisation des Images klickst. Während der lokale Cache aktualisiert wird, siehst Du eine entsprechende Status-Leiste mit dem Fortschritt.

Das differenzielle Image wird vom Server geholt und lokal im Cache des Clients angewendet. Danach wird der Client gestartet.

4.17.4 WebUI: LINBO-Imageverwaltung

Alle LINBO-Images werden mit der Zuordnung zu den Hardwaregruppen in der WebUI übersichtlich dargestellt und können hier einfach verwaltet werden.

Neben den Informationen zu den Images wie z.B. Dateigröße und Imagebeschreibungen, lassen sich Images beispielsweise löschen oder anpassen.

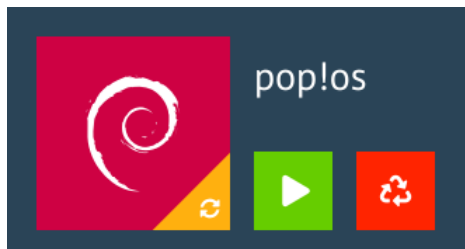


Abb. 403: LINBO-GUI: Boot-Icons

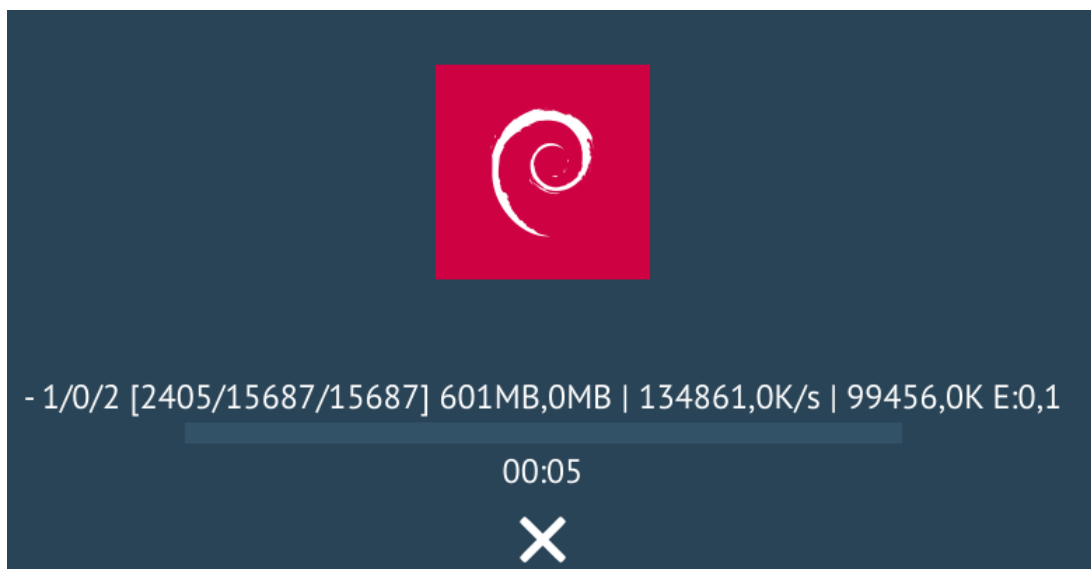


Abb. 404: Fortschrittsbalken

Imageverwaltung aufrufen



Abb. 405: LINBO4 Menü

Um zur Umageverwaltung in der WebUI zu gelangen, meldest Du Dich in der WebUI als `global-admin` an. Danach rufst Du links in der Menüspalte Geräteverwaltung -> LINBO4 auf.

Abb. 406: LINBO Hardwaregruppen

Rechts erscheinen im Fenster zunächst die Hardwaregruppen mit den zugeordneten Basis-Images als **Verwendete Images**. In nachstehender Abbildung ist das Basis-Image blau hervorgehoben. Es nutzt die Dateieindung `.qcow2`. In der Abbildung ist nur eine Hardwareklasse mit dem zugeordneten Basis-Image dargestellt.

Images verwalten

Klicke oben in dem Fenster auf den Tab **Abbilder** / **Images**, so siehst Du eine Gesamtliste aller Images, die mit LINBO erstellt wurden und hier verwaltet werden können.

Gruppen		Abbilder	
Name	Differentielles Image	In Gruppe verwendet ...	Aktionen
<input type="checkbox"/> popos2202 3.8 GB	popos2202 1.4 GB	pop-os-22-04-lts	

Abb. 407: Überblick der LINBO-Images

Unter der Spaltenüberschrift **Name** ist der Name und die Dateigröße des Basis-Images abgelegt. Daneben findest Du in der Spalte **Differentielles Image** das dem Basis-Image zugeordnete differentielle Image inkl. Angabe der Dateigröße. Zudem wird dargestellt, in welcher Gruppe diese Images verwendet werden. In der Spalte **Aktionen** befinden sich Symbole, die Aktionen für das Basis-Image ausführen.

Basis-Image

Gruppen		Abbilder	
Name	Differentielles Image	In Gruppe verwendet ...	Aktionen
<input type="checkbox"/> popos2202 3.8 GB	popos2202 1.4 GB  	pop-os-22-04-lts	  

Abb. 408: LINBO Images

Um das Basis-Image zu verwalten, das in der Image-Übersicht in der Spalte Namen angegeben wird, findest Du die Aktions-Icons in der Übersicht ganz rechts als etwas größere Symbole.

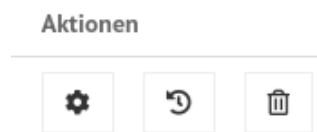


Abb. 409: Aktionen

Klicke auf das Zahnradsymbol. Es erscheint ein Fenster mit Informationen zu dem Basis-Image.

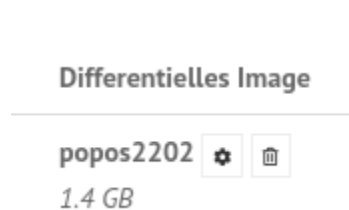
Hier finden Sie Informationen zum Dateinamen, dem Zeitstempel der Erstellung, der Dateigröße und weiterer Parameter. Die Dateiergung `.qcow2` steht für ein Basis-Image.

Hier kannst Du Änderungen bzw. Ergänzungen vornehmen und diese mithilfe des Buttons **SPEICHERN** dauerhaft anwenden.

Klicke auf mittlere Icon, um die Sicherungen des Basis-Images im Zeitablauf anzuzeigen.

Das aktuell gültige Basis-Image wird mit dem Status Basis-Image und einem grünen Haken symbolisiert. Im Zeitablauf werden die vorangegangenen Basis-Images dargestellt. Diese können entweder gelöscht (Papierkorb), wiederhergestellt (Pfeil gegen den Uhrzeigersinn) oder deren Besonderheiten eingesehen werden (Zahnrad-Icon).

Differentielle Images



Die beiden kleinen Icons neben dem Namen für das differentielle Image bieten die Möglichkeit, das differentielle Image entweder zu löschen (Papierkorb), oder mit dem Zahnrad weitere Informationen zu dem differentiellen Image aufzurufen.

Klickst Du auf das Zahnrad neben dem Namen für das differentielle Image, dann erscheint folgendes Fenster:

Unter der Reiterkarte **Allgemein** findest Du Informationen zu dem differentiellen Image wie z.B. den Zeitstempel oder den Imagenamen. Die Dateiergung `.qdiff`

steht für ein differentielles Image.

Hier kannst Du Änderungen bzw. Ergänzungen vornehmen und diese mithilfe des Buttons **SPEICHERN** dauerhaft anwenden.

popos2202

Allgemein

Registry Patch

Postsync-Skript

Prestart Skript

Beschreibung

Aktualisiertes Image mit Domänenbeitritt

Info

[“popos2202.qcow2“ Info File]

timestamp=“202307200551“

image=“popos2202.qcow2“

imagesize=“4112084992“

partition=“/dev/sda2“

partitionsizesize=“31457280“

Größe

3.8 GB

SPEICHERN

SCHLIESSEN

Abb. 410: Informationen zum Image

popos2202 - Sicherungen

Status	Name / Größe	Kommentar	Aktionen
<div>Basisimage</div> <div>✓</div>	<div>popos2202</div> <div>20/07/2023 05:51</div> <div>3.8 GB</div>	Aktualisiertes Image mit Domänenbeitritt	
<div>Sicherungen</div> <div>🔄</div>	<div>20/07/2023 05:51</div> <div>3.3 GB</div>	Erstes Image mit Domänenbeitritt	<div>⚙️</div> <div>↺</div> <div>🗑️</div>
<div>Sicherungen</div> <div>🔄</div>	<div>04/01/2023 17:04</div> <div>3.3 GB</div>		<div>⚙️</div> <div>↺</div> <div>🗑️</div>

SCHLIESSEN

Abb. 411: Image-Sicherungen

popos2202 - Differentielles Image

Allgemein
Registry Patch
Prestart Skript

Beschreibung

Info

```
[*popos2202.qdiff* Info File]
timestamp="202308012001"
image="popos2202.qdiff"
imagesize="1496645632"
partition="/dev/sda2"
partitionsizesize="31457280"
backingfile_timestamp="202307200551"
```

Größe

1.4 GB

SPEICHERN
SCHLIESSEN

Abb. 412: Informationen zum diff. Image

4.17.5 Boot-Bildschirme in LINBO

Beim Booten in LINBO sind folgende Bildschirme sichtbar:

Bootvorgang via Netzwerk

Egal ob über die lokale Festplatte gebootet wurde oder nach dem Bootvorgang via Netzwerkkarte (PXE) wird mit der Gruppenkonfiguration der Kernel geladen.

Der gebootete LINBO-Kernel erscheint als ASCII-Art.

Die Grub-Konfiguration wird ggf aktualisiert, danach erscheint der reguläre LINBO Startbildschirm.

4.17.6 LINBO-Image für USB-Sticks und CD/DVD

Zum Erstellen einer Boot-CD/DVD oder zum Kopieren auf einen USB-Stick lädst Du zuerst das aktuelle LINBO - Image als `linbo.iso` herunter. Dies ermöglicht es, dass ein Client lokal via CD/DVD oder USB-Stick als Boot-Medium startet. Dies kann dann hilfreich sein, wenn das Booten von LINBO via Netzwerk Probleme bereitet.

Melde Dich zuerst an der Schulkonsole an:

`https://10.0.0.1/`

Melde Dich an der Schulkonsole als Benutzer `global-admin` an.

Wähle danach links den Menüpunkt LINBO4 aus.

```
Machine UUID 250e893c-6508-45f1-9a5e-ece88c344948
Booting from ROM...
iPXE (PCI 00:12.0) starting execution...ok
iPXE initialising devices...ok

iPXE 1.20.1+ (g4bd0) -- Open Source Network Boot Firmware -- http://ipxe.org
Features: DNS HTTP iSCSI TFTP AoE ELF MB00T PXE bzImage Menu PXEXT
net0: 72:7e:b1:f5:4d:9c using virtio-net on 0000:00:12.0 (open)
[Link:up, TX:0 TXE:0 RX:0 RXE:0]
Configuring (net0 72:7e:b1:f5:4d:9c).....
```

Abb. 413: Initialmeldungen beim Bootvorgang via Netzwerk (PXE)

```
LINBO netboot in failsafe mode
Loading /linbo64 .. [ linbo64 3.82MiB 100% 1.87MiB/s ]
Loading /linbofs64.lz .. [ linbofs64.lz 13.55MiB 59% 5.09MiB/s ]
```

Abb. 414: Bootbildschirm: Laden des Kernels

```
Welcome to
LINBO
v4.0.8-0: Subterranean Homesick Blues
Linux 5.10.89 #1 SMP Fri Jan 28 16:03:31 UTC 2022 x86_64 GNU/Linux
Initializing hardware ...
```

Abb. 415: LINBO-Kernelboot ASCII-Art



Abb. 416: Login WebUI



Abb. 417: LINBO4 Menüeintrag

Rechts im Fenster erscheinen ganz unten zwei Buttons. Klicke nun den Button **Linbo Boot herunterladen**. Es erscheint ein Fenster zum Download des ISO-Images.

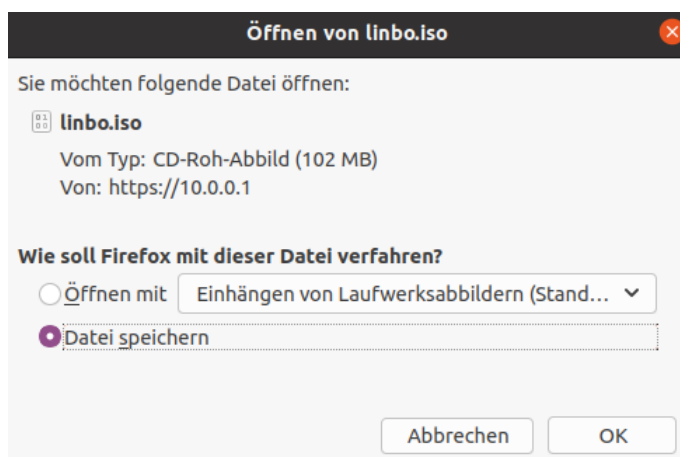


Abb. 418: Download des LINBO-Images

Das Booten eines Rechners mit einem LINBO-USB-Stick oder einer LINBO-CD/DVD kann nötig werden, wenn - in seltenen Fällen - LINBO nicht per PXE installiert wird.

Bootes Du einen Rechner via Stick oder von einer CD/DVD, dann siehst Du folgendes Bild:

Mit **Enter** wird der Client gebootet

Mit der Auswahl durch die Pfeiltasten der Tastatur **Ersteinrichtung + Neustart** wird Linbo eingerichtet und der Rechner mit Linbo gestartet. Nach dem Neustart stehen alle Linbo-Funktionen zur Verfügung.

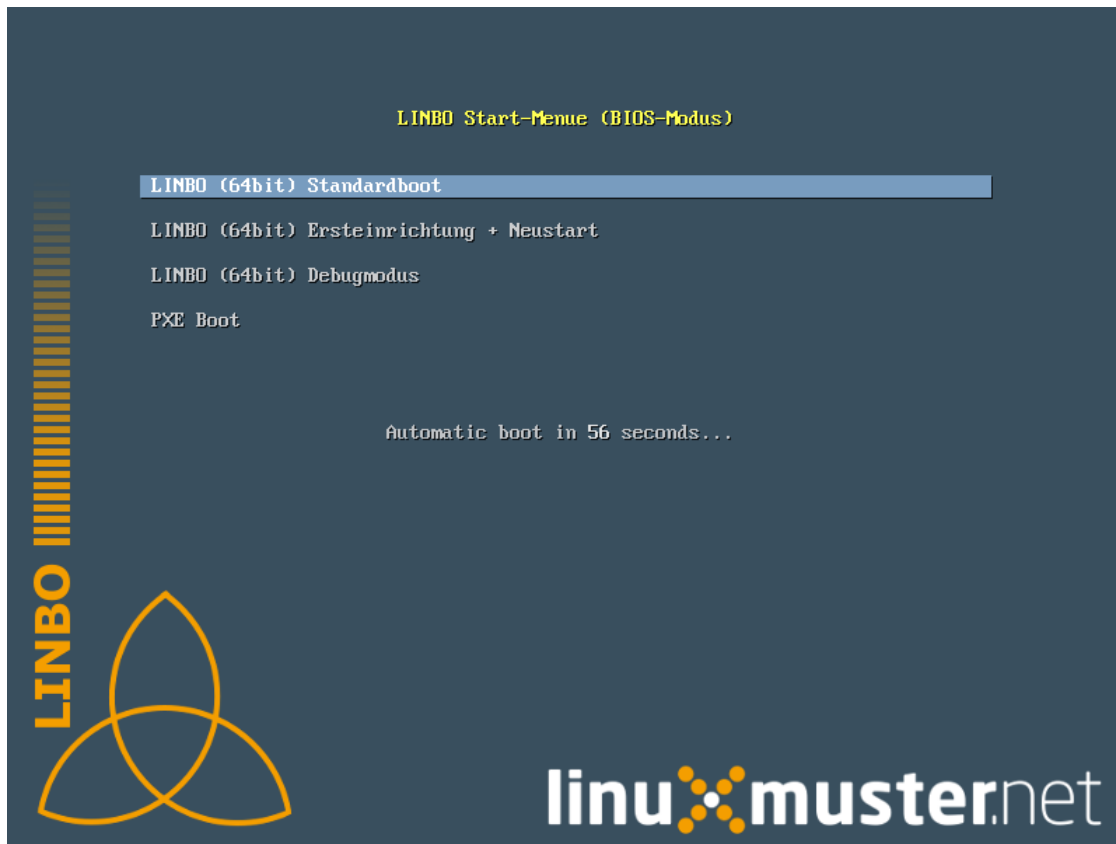


Abb. 419: LINBO Screen

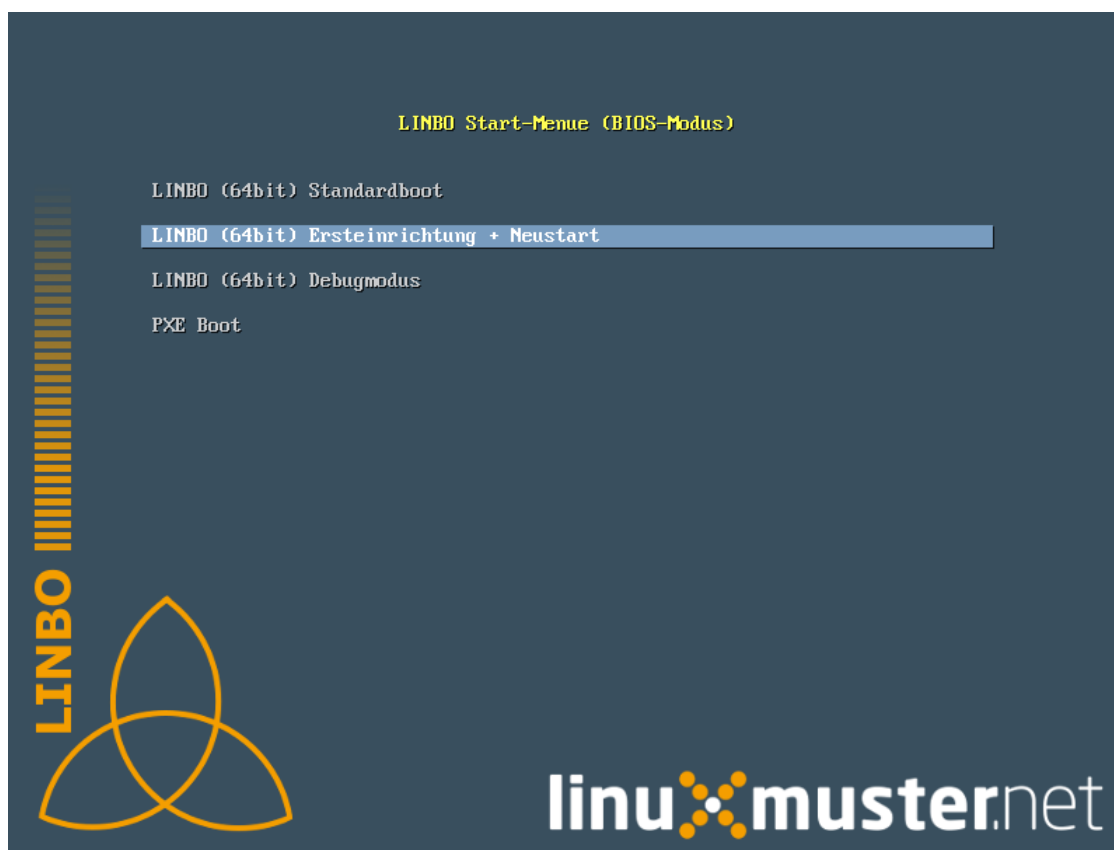


Abb. 420: LINBO Start-Menü

4.17.7 LINBO4-Cache: Hinweise

Linbo4 nutzt auf jedem Client eine lokale Cache-Partition, um ein oder mehrere Image/s eines Betriebssystems lokal vorzuhalten. Es lassen sich so unterschiedliche Verhaltensweisen eines Clients entweder via start.conf Datei oder via linbo-remote steuern.

Cache-Verhalten

Ausgangszustände des Linbo-Caches können sein:

1. Cache ist leer.
2. Cache beinhaltet ein altes, aber gewünschtes Image.
3. Cache beinhaltet ein aktuelles Image.
4. Cache beinhaltet ein altes, aber nicht mehr gewünschtes Image.
5. Cache beinhaltet zwei alte, aber gewünschte Images.
6. Cache beinhaltet zwei aktuelle Images.
7. Cache beinhaltet zwei alte, aber nicht mehr gewünschte Images.

Weitere Fälle sind denkbar.

- Welches Verhalten stellt sich dar?
 - Welche Wirkung hat in Linbo der Befehl initcache - also eine vorherige Bereinigung / neue Befüllung des Linbo-Caches?
1. Fall 1, das Image wird geladen ohne „initcache“.
 2. Fall 2, das neue Image wird geladen ohne „initcache“, das alte wird gelöscht.
 3. Fall 3, nichts passiert, ob mit oder ohne „initcache“.
 4. Fall 4, ohne „initcache“ läuft man Gefahr, dass der Cache voll läuft, mit „initcache“ wird das überflüssige Image gelöscht.
 5. Fall 5, die Images werden geladen (ohne „initcache“), die alten Images werden gelöscht.
 6. Fall 6, nichts passiert, ob mit oder ohne „initcache“.
 7. Fall 7, ohne „initcache“ läuft man Gefahr, dass der Cache voll läuft; mit „initcache“ werden die Images gelöscht und die neuen Images geladen.

Grundsätzlich gilt:

- `initcache` ist dann hilfreich, wenn
- `initcache` ist überflüssig, wenn nur ein Betriebssystem mit einem neuen Image gesynct werden soll und es keinen Grund gibt den Cache aufzuräumen. Das Image wird auch mit `sync` heruntergeladen.
- `initcache` ist kontraproduktiv, wenn der Client mehrere Images vorhält und beim Sync dann u.U. länger als nötig unbenutzbar ist, weil zuerst alle neuen Images (nicht nur das zu syncende) heruntergeladen werden.

Initcache anwenden

Option 1

In der Hardwareklasse (HWK) besteht für Linbo in der start.conf die Möglichkeit die Option

```
[LINBO]                                # globale Konfiguration
Cache = /dev/sda6                      # lokale Cache Partition
Server = 10.0.0.1                     # IP des Linbo-Servers, der das Linbo-Repository vorhaelt
Group = r101                          # Name der Rechnergruppe fuer die diese
↳ Konfigurationsdatei gilt
SystemType = efi64                    # moeglich ist bios/bios64/efi32/efi64 (Standard: bios
↳ fuer bios 32bit)
RootTimeout = 600                     # automatischer Rootlogout nach 600 Sek.
AutoPartition = no                    # automatische Partitionsreparatur beim LINBO-Start
AutoFormat = no                       # kein automatisches Formatieren aller Partitionen beim
↳ LINBO-Start
AutoInitCache = no                    # kein automatisches Befuellen des Caches beim LINBO-Start
DownloadType = torrent                # Image-Download per torrent/multicast/rsync, default ist
↳ rsync
KernelOptions = quiet splash #
```

Wird der Parameter AutoInitCache=yes gesetzt, so wird der lokale Cache jedesmal vollständig neu befüllt. Das ist entsprechend der oben beschriebenen Fälle allerdings nicht immer sinnvoll.

Option 2

Vom linuxmuster.net Server aus wird mit `linbo-remote` das Verhalten für initcache bei Bedarf gezielt gesteuert. In der start.conf der Linbo-HWK ist die Option `AutoInitCache=no` gesetzt.

Mit folgendem Befehl, der auf dem Server abgesetzt wird, lässt sich der Cache beim nächsten Boot-Vorgang des betreffenden PCs neu befüllen:

```
linbo-remote -i r100-pc01 -w 45 -p initcache,sync:1,sync:2,sync:3,start:2
```

Es werden WOL-Pakete an den PC r100-pc01 gesendet, um diesen „aufzuwecken“. Nach einer Wartezeit von 45 Sekunden werden die angegebenen Befehle an den Client weitergegeben. Es wird der Cache neu befüllt, das 1., 2. und 3. Betriebssystem synchronisiert und das 2. Betriebssystem gestartet.

Dies kann ebenfalls für eine ganze Rechnergruppe angewendet werden:

```
linbo-remote -g r101 -w 60 -p initcache,sync:1;sync:2,sync:3,start:2
```

Es werden ein WOL-Pakete an alle PCs der Gruppe r101 gesendet, um diese „aufzuwecken“. Nach einer Wartezeit von 60 Sekunden werden die angegebenen Befehle an die Clients weitergegeben. Es wird der Cache neu befüllt, das 1., 2. und 3. Betriebssystem synchronisiert und das 2. Betriebssystem gestartet.

Zudem kann mit `linbo-remote` auch gezielt eine Partition formatiert werden und danach die Synchronisation sowie der Start eines gewünschten Betriebssystems erfolgen:

```
linbo-remote -i win10-client1 -p format:3,sync:1,start:1
```

Dabei ist zu beachten:

- `format:<#>`: Schreibt die Partitionstabelle und formatiert nur die Partition mit der angegebenen Nummer aus der Partitionstabelle. Achtung: Bei UEFI-System ist EFI immer die erste Partition
- `sync:<#>`: Synchronisiert das Betriebssystem, das in der start.conf an der angegebenen <#> Position eingetragen wurde.

- `start:<#>`: Startet das Betriebssystem, das in der `start.conf` an der angegebenen `<#>` Position eingetragen wurde.

4.17.8 LINBO4 mit WLAN nutzen

Linbo4 unterstützt ab der Version 4.2 die Nutzung von LINBO via WLAN-Netzwerk. Hierzu wurde das Programm `wpa_supplicant` in LINBO integriert.

Vor der Nutzung solltest Du zuerst prüfen, ob LINBO für den eingebauten WLAN-Adapter die benötigte Firmware aufweist. Hierzu gehst Du wie folgt vor:

Firmware prüfen

1. Überprüfe die Ausgabe von `dmesg`

```
nb-01: ~ # dmesg | grep firmware
i915 0000:00:02.0: Direct firmware load for i915/kbl_dmc_ver1_04.bin failed with error -2
i915 0000:00:02.0: [drm] Failed to load DMC firmware i915/kbl_dmc_ver1_04.bin. Disabling
runtime power management.
i915 0000:00:02.0: [drm] DMC firmware homepage: https://git.kernel.org/pub/scm/linux/
kernel/git/firmware/linux-firmware.git/tree/i915
```

2. In obiger Ausgabe fehlt die Firmware für i915 DMC. Um die Firmware zu laden, findest Du unter `/etc/linuxmuster/linbo/firmware` eine Konfigurationsdatei, in der Du die benötigte Firmware einträgst.

```
# /etc/linuxmuster/linbo/firmware

# Realtek r8168 ethernet adapters firmware (whole directory)
rtl_nic

# Realtek RTL8821AE wifi firmware (single file)
rtlwifi/rtl8821aefw.bin

# Intel Wi-Fi 6 AX200 firmware (single file)
iwlwifi-cc-a0-77.ucode

# i915 DMC firmware
i915/kbl_dmc_ver1_04.bin
```

Zu o.g. Beispiel fügst Du die Zeile `i915/kbl_dmc_ver1_04.bin` in die Konfigurationsdatei für die LINBO-Firmware ein. Das Linux-Firmware Package ist auf dem linuxmuster.net Server bereits zusammen mit LINBO installiert. Der Pfad für die zu ladende Firmware-Datei muss relativ zum Verzeichnis `/lib/firmware` angegeben werden.

3. Um die Firmware für linbofs bereitzustellen, musst Du noch auf dem Server den Befehl

```
update-linbofs
```

ausführen.

Hinweis: Wenn die geladene WLAN-Firmware dazu führt, dass der WLAN Adapter nach einem Warmstart nicht funktioniert, kannst Du den `warmstart` in der `start.conf` mit `nowarmstart` als Kernel-Option abschalten.

WLAN definieren

Hat der Client die benötigte Firmware, bearbeitest Du die Datei `/etc/linuxmuster/linbo/wpa_supplicant.conf` auf dem Server. In dieser definierst Du das WLAN, das der Client verwenden soll.

Nachstehend findest Du zwei Beispiele hierzu:

```
# /etc/linuxmuster/linbo/wpa_supplicant.conf

# wpa-psk secured
network={
    ssid="LINBO_MGMT"
    scan_ssid=1
    key_mgmt=WPA-PSK
    psk="My Secret Passphrase"
}

# open
network={
    ssid="LINBO_MGMT"
    key_mgmt=NONE
}
```

Weitere Konfigurationsbeispiele findest Du unter: https://linux.die.net/man/5/wpa_supplicant.conf

Nachdem Du die Konfigurationsdatei mit den WLAN-Einstellungen bereitgestellt hast, müssen diese Informationen noch auf `linbofs` angewendet werden. Hierzu gibst Du auf dem Server den Befehl

```
update-linbofs
```

an.

WLAN-Gerät anlegen

Zuletzt musst Du noch für das Gerät, das via WLAN mit LINBO arbeiten soll, einen Geräteintrag erstellen. In der Datei `/etc/linuxmuster/devices.csv` oder in der Schulkonsole unter **Geräte** erstellst Du einen Eintrag für den WLAN-Adapter des zu importierenden Gerätes wie in nachstehendem Beispiel gezeigt:

```
notebooks;nb-01;nbclass;4d:b6:a7:12:45:79;10.0.100.1;;;classroom-studentcomputer;;1
notebooks;nb-01w;nbclass;b2:5f:5e:32:12:65;10.0.250.1;;;classroom-studentcomputer;;1
```

Achte darauf, dass Du bei zwei Eintragungen für ein Gerät (LAN und WLAN) jeweils voneinander abweichende Gerätenamen verwendest. In o.g. Beispiel ist der erste Eintrag für ein Notebook, das via Kabel mit LINBO arbeitet. Der zweite Eintrag ist für das identische Notebook (WLAN). Hier wird nun aber ein abweichender Hostname `nb-01w` genutzt und die MAC-Adresse des WLAN-Adapters eingetragen. Als IP-Adresse wird dem WLAN-Adapter eine eigene zugewiesen. DHCP-Einträge sollten vermieden werden, da sonst auch nicht bekannte Geräte, ggf. das WLAN nutzen können.

Hast Du die Eintragungen in der `devices.csv` auf dem Server vorgenommen, importierst Du diese mit:

```
linuxmuster-import-devices
```

Hast Du die Eintragungen hingegen in der Schulkonsole vorgenommen, so must Du nur auf **Save & import** klicken.

Hinweis: Für WLAN-Verbindungen gelten für LINBO einige Einschränkungen.

- Wireless pxe boot ist nicht möglich. LINBO stellt die WLAN-Verbindung nur während des Boot-Prozesses her.
- Die Erstinstallation von LINBO auf dem Client ist zuerst über ein kabelgebundenes LAN durchzuführen.
- Der Download großer Betriebssystem-Images beeinträchtigt Deine WLAN-Performance. Dies solltest Du vermeiden werden.
- Du solltest zudem überlegen, ob Du ein gesichertes WLAN für das LINBO-Management einrichtest, um den Zugriff auf das WLAN zu beschränken.

4.17.9 LINBO4: Hook-Skripte

Achtung: Ab der Version LINBO 4.1.31 linuxmuster-linbo7 4.1.31 stehen sogenannte Hook-Skripte zur Verfügung, um vor oder nach `update-linbofs` auf dem Server kleine Programme auszuführen, die durch definierte Ereignisse ausgelöst werden.

Pre-Hook-Skripte

Mit dem Befehl `update-linbofs` wird die Erstellung von `linbofs` auf dem Server angestoßen.

Pre-Hook-Skripte, werden hierbei vor der Erstellung von `linbofs64.lz` ausgeführt. Dies bietet die Möglichkeit, im Dateisystem vorher eigene Anpassungen vornehmen.

Was passiert bei Ausführung des Befehls `update-linbofs`?

- Das Template (`/var/lib/linuxmuster/linbo/linbofs64.cpio`) wird in ein Verzeichnis (`/var/cache/linuxmuster/linbo/linbofs64`) entpackt.
- Dort wird das Template angepasst: `passwort-hash`, `dropbear-key`, `permissions`, `default-start.conf` (`/srv/linbo/start.conf`), `Zeitzone`.
- Zum Schluss werden die Pre-Hook Skripte ausgeführt. Dies geschieht ebenfalls innerhalb des Verzeichnisses - man kann also über relative Bezüge auf die `linbofs`-Dateien zugreifen.
- Abschließend wird das Verzeichnis wieder gepackt (z.B. nach `/srv/linbo/linbofs64.lz`), bevor danach die Posthook-Skripte angepasst werden.

Hinweis: Die Linbo bekannten Variable können in den Hook-Skripten nicht verwendet werden, ohne sie vorher zu importieren.

Mit Pre-Hook-Skripten können so z.B. angepasste Dateien für `.ssh/authorized_keys` oder `.env` bereitgestellt werden.

Diese Skripte sind in folgendem Verzeichnis abzulegen:

```
/var/lib/linuxmuster/hooks/update-linbofs.pre.d/
```

Ein Hook-Skript muss ausführbar sein und mit einem `shebang` beginnen.

Nachstehendes Pre-Hook-Skript zeigt hierzu einige Möglichkeiten auf.

```
#!/bin/sh
# /var/lib/linuxmuster/hooks/update-linbofs.pre.d/pre-hook1.sh

# Ausgabe der Linbo-Version (wird beim Ablauf des update-linbofs-Skripts ausgegeben)
echo "Linbo-Version: $(cat etc/linbo-version)"

# Hinzufügen eigener Dateien, damit sie in Linbo zur Verfügung stehen
mkdir myfiles && echo /etc/linuxmuster/sophomorix/default-school/devices.csv myfiles

# Kopieren des Linbo-Verzeichnisses (z.B. zum Testen mit eigenen Skripten) nach /tmp/
↳ linbofs:
mkdir /tmp/linbofs && cp -R . /tmp/linbofs

# Einfügen einer Wartezeit von 2 Sekunden vor der Netzwerkeinrichtung, Ausgabe von Text
↳ in der Konsole
sed -i '/^network\(\).*\/a \ \ echo "Warte auf Netzwerk..." && sleep 2' init.sh

exit 0
```

Das Skript muss in dem o.g. Verzeichnis als ausführbar definiert werden:

```
chmod +x /var/lib/linuxmuster/hooks/update-linbofs.pre.d/pre-hook1.sh
```

Post-Hook-Skripte

Post-Hook-Skripte werden nach der Erstellung von update-linbofs auf dem Server ausgeführt. Es können so nachdem der Befehl update-linbofs durchgelaufen ist, z.B. Programme auf dem Server gestartet werden.

Diese Skripte sind in folgendem Verzeichnis abzulegen:

```
/var/lib/linuxmuster/hooks/update-linbofs.post.d/
```

Hook-Skripte müssen ausführbar sein und mit einem shebang beginnen. Es sind die zuvor genannten Hinweise zu beachten.

4.17.10 LINBO4: Linux-Kernel

Linbo ab v4.2 nutzt als Standard den aktuellsten Linux-Kernel. Manchmal gibt es aber dennoch Probleme mit Hardware, die nicht richtig erkannt wird. Dann kann es sein, dass z.B. LINBO per PXE nicht korrekt startet oder das System *scheinbar hängen bleibt*. Solche Fälle widerspenstiger Hardware können mit LINBO 4.2 mit einigen Handgriffen vielfach erfolgreich gelöst werden.

Mit LINBO 4.2 wird auf dem Client ein aktueller Linux-Kernel $\geq 6.6.x$ installiert und gestartet. Bei neuerer Hardware funktioniert dies i.d.R. problemlos. Bei einigen älteren Hardware-Modellen oder Modellen mit besonderer Hardware-Bestückung kann es vorkommen, dass der Client nicht startet. Dies kann schrittweise wie nachstehend beschrieben, zuerst eingegrenzt und dann behoben werden:

1. LINBO-Kernel wechseln

Auf dem Server befindet sich unter `/etc/linuxmuster/linbo/custom_kernel.ex` eine Beispieldatei, wie man den LINBO-Kernel wechselt. Die Kernel befinden sich unterhalb von `/var/lib/linuxmuster/linbo/`. Es stehen drei verschiedene Versionen zu Verfügung: *legacy*, *longterm*, *stable*

2. Netzwerkkarten-Treiber ersetzen

Erkennt der Client Hardware nicht richtig, kann mit `linbo-ssh` geprüft werden, welcher Treiber Probleme bereitet. Hierzu wechselst Du mit `linbo-ssh <IP des Clients>` auf die LINBO-Konsole auf dem Client.

```
dmesg |grep firmware      # listet evtl Probleme mit fehlenden Treiber auf
```

Danach die benötigte Firmware mit Pfad so unter `/etc/linuxmuster/linbo/firmware` eintragen - siehe hierzu auch die *Beispieldatei* `firmware.ex`.

Führe anschließend den Befehl `update-linbofs` auf dem linuxmuster Server aus.

3. Kernel-Options verwenden

Auf dem Server findet sich pro Hardwareklasse eine `start.conf` Datei unter: `/srv/linbo/start.conf.<Hardwareklasse>`

Setze den Eintrag `KernOptions` und gebe Optionen an, die für Deine Hardware dem Kernel wichtige Infos mitgeben.

```
KernelOptions =  
#unterschiedliche Einträge ausprobieren.  
  
KernelOptions = loadmodules=r8168 modprobe.blacklist=r8169  
  
oder auch  
  
KernelOptions = nomodeset
```

Anschließend musst Du auf dem Sever den Befehl `linuxmuster-import-devices` ausführen, damit die Änderungen auf den Clients übernommen werden.

4. LINBO-Befehle

Unter LINBO können sämtliche Befehle auch direkt am Client eingegeben werden. Dies ist sehr hilfreich, um Log-Dateien auszulesen, Hardware-Probleme und ihre mögliche Lösung schrittweise auszutesten.

Dazu wechselst Du wieder mit `linbo-ssh <IP des Clients>` auf die LINBO-Konsole des Clients. Dort kannst Du dann direkt LINBO-Befehle wie z.B. `linbo_partition_format` oder `linbo_sync 1` angeben.

Sämtliche Befehle, die `linuxmuster-linbo7` (next generation) beherrscht, werden hier aufgelistet: <https://github.com/linuxmuster/linuxmuster-linbo7/issues/72#issuecomment-1156633508>

4.17.11 im Fehlerfall

Torrent-Fehler

Nutzt Du sehr große Images, so kann es passieren, dass bei der Verteilung der qcow2-Images mit Torrent-Fehler auftreten und die Synchronisation auf `rsync` zurückfällt. Hierbei kommt es zum Einbruch bei den Datenübertragungsraten.

Ab LINBO v4.1.36 können für `ctorrent` Parameter angepasst werden, um dies zu verhindern.

Die Konfigurationsdatei für `ctorrent` befindet sich

```
/etc/default/linbo-torrent
```

Die Paketgrößen können nun als Parameter `piece length` angepasst werden. Dazu kannst Du in o.g. Konfigurationsdatei den Parameter wie folgt setzen:

```
# Piece length (torrent file option)
PIECELEN="524288"
```

Hast Du den Wert angepasst, musst Du Torrent neu starten:

```
linbo-torrent restart
```

Wurde die Option in der Konfigurationsdatei nicht explizit gesetzt, so wird ein Standardwert (default value) von 262144 verwendet.

Mit der Erhöhung des Wertes können o.g. Probleme behoben werden.

Zum Vergleich findet sich nachstehende Konfigurationsdatei `/etc/default/linbi-torrent`:

```
# default values for linbo-torrent helper service provided by ctorrent
# thomas@linuxmuster.net
# 20230918
#
# note: you have to invoke 'linbo-torrent restart' after you have changed any values
#

# Exit while seed <SEEDHOURS> hours later (default 72 hours)
SEEDHOURS="100000"

# Max peers count (default 100)
MAXPEERS="100"

# Min peers count (default 1)
MINPEERS="1"

# Download slice/block size, unit KB (default 16, max 128)
SLICESIZE="128"

# Max bandwidth down (unit KB/s, default unlimited)
MAXDOWN=""

# Max bandwidth up (unit KB/s, default unlimited)
MAXUP=""

# Supplemental ctorrent options, separated by space (-v: Verbose output for debugging)
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
#OPTIONS="-v"

# Timeout in seconds until rsync fallback (client only)
TIMEOUT="300"

# user to run ctorrent (server only)
CTUSER="nobody"

# Piece length (torrent file option)
PIECELEN="524288"
```

4.18 Linux-Client - Anpassungen mit Postsync-Skripten

Linux-Clients können in linuxmuster.net mithilfe sogenannter Postsync-Skripte an besondere Nutzungssituationen sehr variabel angepasst werden.

Nach erfolgreicher Synchronisation mit dem Client-Image, das auf dem Server liegt, werden weitere Skripte auf dem Client ausgeführt. Es können so z.B. bestimmte Dateien vom Server auf den Client gespielt werden, oder auf dem Lehrer-PC spezifische Anpassungen vorgenommen werden, die andere Schüler-PCs nicht erhalten.

Inhalt:

4.18.1 Funktionsweise und Grundlagen der Postsync-Skripte

Allgemeines

Nachdem mit Hilfe von LINBO der Linux-Client die Imagedatei (qcow2-Datei) vom Server geholt und auf den Client synchronisiert hat, kann ein für dieses Image definiertes Postsync-Skript angewendet werden. Dieses ermöglicht es, spezifische Anpassungen (sogenannte Patches) vorzunehmen und die PCs somit auf deren Einsatzumgebung anzupassen. Hierdurch können z.B. spezielle Anpassungen für Lehrer-PCs, für PCs in speziellen Räumen, oder für alle zu nutzenden Drucker bereitgestellt werden.

Wo liegt das Postsync-Skript ?

Ein Beispiel für ein universelles Postsync-Skript liegt im Verzeichnis `/srv/linbo/examples/postsync`.

Das Postsync-Skript ist in dem Verzeichnis abzulegen, in dem sich das Image befindet, auf das das Skript angewendet werden soll. Der Name für das Postsync-Skript wird dann zusammengesetzt aus

```
# dem Namen der qcow2-Image-Datei, mit welchem das Skript zusammen arbeitet
#. gefolgt von der Endung ``.postsync``:

/srv/linbo/images/<LinuxImageVerzeichnis>/<LinuxImageName>.postsync

# für das Image focalfossa also
# /srv/linbo/images/focalfossa/focalfossa.postsync
```

Es weist folgende Rechte auf:

```
-rw-rw-r-- 1 root root
```

Anwendung des Postsync-Skriptes

Soll das sogenannte universelle Postsync-Script angewendet werden, so ist dieses zuerst als Vorlage in das gewünschte Image-Verzeichnis zu kopieren:

```
cp /srv/linbo/examples/postsync/generic.postsync /srv/linbo/<LinuxImageVerzeichnis>/
↪<LinuxImageName>.postsync
```

Für das Image focalfossa wäre der Befehl also:

```
cp /srv/linbo/examples/postsync/generic.postsync /srv/linbo/focalfossa/focalfossa.
↪postsync
```

Achtung: Dieses Script wird also auf das jeweilige qcow2 Image angewendet.

4.18.2 Patchklassen für Postsync-Skripte

Die Bereiche, für die Anpassungen vorgenommen werden sollen, heißen Patchklassen.

Ablage der Patches

Zunächst ist das Verzeichnis `/srv/linbo/linuxmuster-client/` anzulegen:

```
mkdir -p /srv/linbo/linuxmuster-client/
```

Unter `/srv/linbo/linuxmuster-client/` sind weitere Unterverzeichnisse für die sog. Patchklassen anzulegen.

In der ersten Ebene wird nach dem verwendeten Imagennamen (qcow2-Datei) unterschieden. Bei Linuxmuster-Clients 20.04 (Focal Fossa) wäre dies z.B. das Verzeichnis `focalfossa`, oder bei Einsatz von Pop! OS 22.04 `popos2204`:

```
/srv/linbo/linuxmuster-client/focalfossa/
/srv/linbo/linuxmuster-client/popos2204/
```

In der nächsten Ebene können weitere Unterscheidungen nach folgendem Schema angewendet werden:

```
im Unterverzeichnis ../common liegende Patches erhalten alle Rechner, die dieses Image
↪nutzen.
im Unterverzeichnis ../r100 liegende Patches erhalten nur die Rechner in Raum r100.
im Unterverzeichnis ../r100-pc01 liegende Patches erhält nur der PC01 in Raum r100.
```

Hinweis: In der Geräteverwaltung muss der Rechnername nach dem Schema `RaumName-PCName` benannt worden sein. Beispiel: Raum: r100 Rechnername: r100-pc01

Unterhalb dieser Verzeichnisse sind alle Anpassungen so abzulegen, dass sie mit der Verzeichnisstruktur der betreffenden Clients identisch sind. So wird z.B. beim Anlegen der Datei auf dem Server:

```
../common/etc/cups/cups.conf
```

Die `cups.conf` im Verzeichnis `/etc/cups` auf allen Clients der Patchklasse entsprechend angepasst.

In der Patchklasse `focalfossa` würde eine Änderung der Datei `rc.local` auf allen Rechnern in folgendem Server-Verzeichnis abgelegt werden:

```
/srv/linbo/linuxmuster-client/focalfossa/common/etc/rc.local
```

Weitere Skripte ausführen

Das universelle Postsync-Script ist so aufgebaut, dass auch noch weitere Skripte ausgeführt werden können.

So können z.B. spezielle Anpassungen von PCs in einem bestimmten Raum vorgenommen werden. Alle abzuarbeitenden Skripte müssen im Verzeichnis `postsync.d` liegen.

Sollen Skripte für die Patchklasse `focalfossa` und dann nur auf PCs im Raum `r100` angewendet werden, so müssen die Skripte in folgendem Verzeichnis liegen:

```
/srv/linbo/linuxmuster-client/focalfossa/r100/postsync.d/
```

Die Skripte müssen sh-Skripte sein, da Linbo keine BASH als Shell kennt. In diesen Skripten ist der Shebang `#!/bin/sh` voranzustellen. Diese Skripte müssen zur Anwendung für die gewünschte Patchklasse in das jeweilige Verzeichnis kopiert und angepasst werden. Diese Skripte werden entsprechend ihrer lexikalischen Reihenfolge ausgeführt, also hier beginnend mit der niedrigsten Ziffer.

Beispiel

Nachstehender Verzeichnisbaum verdeutlicht, dass für Linuxmuster-Clients für alle PCs der Patchklasse `focalfossa` alles unterhalb von `./common` angewendet wird. Modulare Postsync-Skripte finden sich unter `./common/postsync.d/` und werden in lexikalischer Reihenfolge abgearbeitet. Zudem wird für den Raum `raum1` alles unterhalb von `./raum1` angewendet und schließlich wird für den Lehrer-PC in `raum1` alles unterhalb von `./raum1-lehrer-pc` angewendet.

```
root@server:/srv/linbo/linuxmuster-client/focalfossa # ls -ld $(find .)
drwxr-xr-x 7 root root 4096 Nov 20 10:25 .
drwxr-xr-x 3 root root 4096 Apr 22 2016 ./common
drwxr-xr-x 3 root root 4096 Mär 17 12:54 ./common/etc
drwxrwxr-x 2 root root 4096 Mai 9 2016 ./common/etc/cups
-rw-r--r-- 1 root root 21 Mai 9 2016 ./common/etc/cups/client.conf
-rw-r--r-- 1 root root 797 Mär 31 09:16 ./common/etc/fstab
-rw-r--r-- 1 root root 443 Mai 9 2016 ./common/etc/hosts
drwxr-xr-x 3 root root 4096 Mär 17 12:54 ./common/postsync.d
-rw-r--r-- 1 root root 21 Mai 9 2016 ./common/postsync.d/00-lcst-fix-initrd.sh
-rw-r--r-- 1 root root 797 Mär 31 09:16 ./common/postsync.d/01-lcst-setlocalpasswords.sh
drwxr-xr-x 4 root root 4096 Mär 26 2015 ./raum1
drwxr-xr-x 7 root root 4096 Nov 20 10:10 ./raum1/etc
drwxr-xr-x 2 root root 4096 Apr 14 10:38 ./raum1/etc/cups
-rw----- 1 root root 3588 Apr 14 10:40 ./raum1/etc/cups/printers.conf
drwxr-xr-x 2 root root 4096 Mär 26 2015 ./raum1/etc/default
-rw-r--r-- 1 root root 369 Nov 5 2011 ./raum1/etc/default/epoptes
-rw-r--r-- 1 root root 668 Nov 20 10:01 ./raum1/etc/default/epoptes-client
drwxr-xr-x 2 root root 4096 Mär 26 2015 ./raum1/etc/epoptes
-rw-r--r-- 1 root root 875 Mär 26 2015 ./raum1/etc/epoptes/server.crt
-rw----- 1 root root 916 Mär 26 2015 ./raum1/etc/epoptes/server.key
-rw-r--r-- 1 root root 984 Nov 20 10:18 ./raum1/etc/hosts
drwxr-xr-x 2 root root 4096 Mär 26 2015 ./raum1/etc/init.d
-rwxr-xr-x 1 root root 1645 Apr 8 2012 ./raum1/etc/init.d/epoptes
-rwxr-xr-x 1 root root 1124 Apr 8 2012 ./raum1/etc/init.d/epoptes-client
drwxr-xr-x 3 root root 4096 Mär 26 2015 ./raum1/etc/xdg
drwxr-xr-x 2 root root 4096 Mär 26 2015 ./raum1/etc/xdg/autostart
-rw-r--r-- 1 root root 428 Nov 20 10:45 ./raum1/etc/xdg/autostart/epoptes-client.desktop
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```

drwxr-xr-x 5 root root 4096 Jan 22 18:23 ./raum1-lehrer-pc
drwxr-xr-x 7 root root 4096 Nov 20 10:10 ./raum1-lehrer-pc/etc
drwxr-xr-x 2 root root 4096 Okt 23 2014 ./raum1-lehrer-pc/etc/cups
-rw----- 1 root root 3588 Apr 14 10:40 ./raum1-lehrer-pc/etc/cups/printers.conf
drwxr-xr-x 2 root root 4096 Mär 26 2015 ./raum1-lehrer-pc/etc/default
-rw-r--r-- 1 root root 370 Nov 20 10:14 ./raum1-lehrer-pc/etc/default/epoptes
-rw-r--r-- 1 root root 0 Nov 20 10:21 ./raum1-lehrer-pc/etc/default/epoptes-client
drwxr-xr-x 2 root root 4096 Mär 26 2015 ./raum1-lehrer-pc/etc/epoptes
-rw-r--r-- 1 root root 875 Mär 26 2015 ./raum1-lehrer-pc/etc/epoptes/server.crt
-rw-r--r-- 1 root root 916 Mär 26 2015 ./raum1-lehrer-pc/etc/epoptes/server.key
-rw-r--r-- 1 root root 983 Nov 20 10:17 ./raum1-lehrer-pc/etc/hosts
drwxr-xr-x 2 root root 4096 Mär 26 2015 ./raum1-lehrer-pc/etc/init.d
-rwxr-xr-x 1 root root 1645 Apr 8 2012 ./raum1-lehrer-pc/etc/init.d/epoptes
-rwxr-xr-x 1 root root 0 Nov 20 10:22 ./raum1-lehrer-pc/etc/init.d/epoptes-client

```

Universelles Postsync-Script

Das universelle Postsync-Script ist unter `/srv/linbo/images/<LinuxImageVerzeichnis>/<LinuxImageName>.postsync` mit folgendem Inhalt anzulegen bzw. wie zuvor beschrieben zu kopieren und gemäß der eigenen Anforderungen anzupassen:

```

echo "##### POSTSYNC BEGIN #####"
LOG=/mnt/var/log/postsync.log
echo "##### POSTSYNC BEGIN #####" > $LOG
NOW=$(date +%Y%m%d-%H%M)
echo $NOW | tee -a $LOG

# IP-Adresse des Servers für LINBO 4.1
SERVERIP=$LINBOSERVER

# Die Hostgruppe des aktuellen Rechners wird mit $HOSTGROUP abgerufen

# Raum feststellen. Dieses Skript geht davon aus
# dass die Rechner Namen der Form
# raumname-hostname haben, also z.B. cr01-pc18
RAUM=${HOSTNAME%%-*}

# wenn der string leer ist, Raum auf unknown setzen
if [ "x${RAUM}" == "x" ]; then
    RAUM="unknown"
fi

# UVZ für die Patches auf dem Server. Mit dieser Variablen
# kann man verschiedene Patches, z.B. für unterschiedliche
# Linux-Versionen bereitstellen.
# Wenn man hier $HOSTGROUP einträgt, erhält jede Rechnerklasse
# ein eigenes Patchklassenverzeichnis auf dem Server.
# Damit kann man verschiedene Patchklassen mit derselben cloop-Datei
# bedienen, wenn man das benötigt.
PATCHCLASS="focalfossa" #Name der Patchklasse anpassen

```

(Fortsetzung auf der nächsten Seite)

```

# Das Verzeichnis, in dem die Serverpatches
# im lokalen Clientcache synchronisiert werden.
PATCHCACHE=/linuxmuster-client/serverpatches

echo "" | tee -a $LOG
echo "Hostname:      ${HOSTNAME}" | tee -a $LOG
echo "Raum:          ${RAUM}" | tee -a $LOG
echo "Patchcache:     ${PATCHCACHE}" | tee -a $LOG
echo "Hostgruppe:     ${HOSTGROUP}" | tee -a $LOG
echo "Patchclass:     ${PATCHCLASS}" | tee -a $LOG
echo "" | tee -a $LOG

# -----
# Patchdateien auf das lokale Image rsyncen
# -----
echo " - getting patchfiles" | tee -a $LOG

# RAUM      -> Raumname
# HOSTNAME  -> Rechnername
# Verzeichnis anlegen, damit es sicher existiert
mkdir -p /cache/${PATCHCACHE}
rsync --delete --progress -r "${SERVERIP}::linbo/linuxmuster-client/${PATCHCLASS}" "/
→cache/${PATCHCACHE}" | tee -a $LOG

echo " - patching local files" | tee -a $LOG

# common: Bekommen alle clients der Patchklasse
# files
if [ -d /cache/${PATCHCACHE}/${PATCHCLASS}/common ]; then
    echo " - patching common to /mnt" | tee -a $LOG
    cp -ar /cache/${PATCHCACHE}/${PATCHCLASS}/common/* /mnt/ | tee -a $LOG
fi

# tarpacks
if [ -d /cache/${PATCHCACHE}/${PATCHCLASS}/common/tarpacks ]; then
    echo " - unpacking tarpacks from common/tarpacks to /mnt" | tee -a $LOG
    for pack in /cache/${PATCHCACHE}/${PATCHCLASS}/common/tarpacks/*; do
        echo " - unpacking: $pack" | tee -a $LOG
        tar xvzf $pack -C /mnt | tee -a $LOG
    done
fi

# Raum: Nur die Clients des Raums
# files
if [ -d /cache/${PATCHCACHE}/${PATCHCLASS}/${RAUM} ]; then
    echo " - patching ${RAUM} to /mnt" | tee -a $LOG
    cp -ar /cache/${PATCHCACHE}/${PATCHCLASS}/${RAUM}/* /mnt/ | tee -a $LOG
fi

# tarpacks
if [ -d /cache/${PATCHCACHE}/${PATCHCLASS}/${RAUM}/tarpacks ]; then
    echo " - unpacking tarpacks from ${RAUM}/tarpacks to /mnt" | tee -a $LOG

```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```

for pack in /cache/${PATCHCACHE}/${PATCHCLASS}/${RAUM}/tarpacks/*; do
    echo "    - unpacking: $pack" | tee -a $LOG
    tar xvzf $pack -C /mnt | tee -a $LOG
done
fi

# Host: Nur der Rechner
# files
if [ -d /cache/${PATCHCACHE}/${PATCHCLASS}/${HOSTNAME} ]; then
    echo "    - patching ${HOSTNAME} to /mnt" | tee -a $LOG
    cp -ar /cache/${PATCHCACHE}/${PATCHCLASS}/${HOSTNAME}/* /mnt/ | tee -a $LOG
fi

# tarpacks
if [ -d /cache/${PATCHCACHE}/${PATCHCLASS}/${HOSTNAME}/tarpacks ]; then
    echo "    - unpacking tarpacks from ${HOSTNAME}/tarpacks to /mnt" | tee -a $LOG
    for pack in /cache/${PATCHCACHE}/${PATCHCLASS}/${HOSTNAME}/tarpacks/*; do
        echo "        - unpacking: $pack" | tee -a $LOG
        tar xvzf $pack -C /mnt | tee -a $LOG
    done
fi

# Hook, um eigene Skripte auszuführen
if [ -d /mnt/postsync.d ]; then
    for SCRIPT in /mnt/postsync.d/*
    do
        chmod 755 $SCRIPT
        echo "Executing: $SCRIPT" | tee -a $LOG
        $$SCRIPT > /dev/null 2>&1
        $SCRIPT | tee -a $LOG
        echo " ...done." | tee -a $LOG
    done
    rm -rf /mnt/postsync.d
fi

# wenn es /mnt/tarpacks gibt - löschen
rm -rf /mnt/tarpacks

# hostname in /etc/hosts patchen
# es muss eine Datei hosts im Verzeichnis
# /srv/linbo/linuxmuster-client/$HOSTGROUP/common/raum/hostname/etc/
# geben, die den HOSTNAME anpasst. Zudem muss dort die SERVERIP angepasst werden.
# Fehlt diese Datei werden der Hostname und die SERVERIP nicht ersetzt.
sed -i "s/HOSTNAME/$HOSTNAME/g" /mnt/etc/hosts
sed -i "s/#SERVERIP/$SERVERIP/g" /mnt/etc/hosts

# Zeitstempel letzter sync hinterlegen
echo $NOW > /mnt/lastsync

echo "##### POSTSYNC END #####" | tee -a $LOG

# Folgende Zeile stellt sicher, dass bei Änderungen des Postsync-Scriptes auf dem Server

```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
# diese auch auf den Client übertragen werden.
# Achtung: Imageverzeichnis und Image name sind anzupassen
rsync --progress -r $LINBOSERVER::linbo/images/focalfossa/focalfossa.postsync /cache/
```

Achtung: Um Komplikationen vorzubeugen, verwende das Kommando `exit` in keinem Deiner Postsync-Scripte!

Variablen im Postsync-Script

In LINBO 4.1 stehen für die Postsync-Scripte bereits Variablen zum Abruf bereit. Nachstehende Übersicht mit Bildschirmausgaben nach dem Schema `Text -> Variablenwert` veranschaulicht dies:

```
echo "# postsync script example"
echo "os partition  : $root"
echo "os name       : $name"
echo "os description: $description"
echo "cache device  : $cache"
echo "baseimage     : $baseimage"
echo "kernel        : $kernel"
echo "initrd        : $initrd"
echo "append        : $append"
echo "hostgroup      : $HOSTGROUP"
echo "hostname       : $HOSTNAME"
echo "domain        : $DOMAIN"
echo "ip             : $IP"
echo "netmask        : $SUBNET"
echo "bitmask        : $MASK"
echo "server ip      : $LINBOSERVER"
echo "server name    : $SNAME"
```

4.18.3 Anwendung des Postsync

Wurden alle Patchklassen und Scripte definiert, die Dateiberechtigungen wie angegeben kontrolliert und das Postsync-Script in dem Image-Verzeichnis hinterlegt, fehlt noch ein wesentlicher Schritt, um das Postsync Script anzuwenden.

Achtung: Das Postsync-Script wird erst angewendet, wenn die betreffenden Clients partitioniert, formatiert und synchronisiert wurden. Erst hierbei wird das Postsync-Script auf den Client übertragen !

4.18.4 Troubleshooting

Welche Möglichkeiten der Fehlersuche gibt es ?

Vom linuxmuster.net Server aus kann man sich auf dem Client mithilfe von `linbo_ssh` anmelden. Es lassen sich so dann die Postsync-Ausgaben / Fehlermeldungen auf dem Client einsehen.

Das Postsync-Script schreibt eine LOG-Datei, die auf dem Client unter

```
/var/log/postsync.log
```

abgelegt wird.

Auf dem linuxmuster.net Server gibt man hierzu folgendes an, um den Client zu starten, zu synchronisieren und dann in den Linbo-Bildschirm zu gelangen, um die Log-Datei einzusehen:

```
linbo-remote -i <IP-Adresse des Clients> -b 5 -w 130 -c sync:1
linbo-ssh <client-name / oder IP-Adresse>
less /var/log/postsync.log
```

Herunterfahren der Clients mit:

```
linbo-remote -i <Client-name / IP-Adresse> -c halt
```

Bei Einsatz des universellen Postsync-Scriptes stehen am Anfang der LOG-Datei z.B. folgende Angaben, die die Infos zu Raum, Rechnername etc. ausgeben:

```
##### POSTSYNC BEGIN #####
20230303-2030

Hostname: a001-pc01
Raum: a001
Patchcache: /linuxmuster-client/serverpatches
Hostgruppe: pop-os-22-04-lts
Patchclass: popos2202

- getting patchfiles
receiving incremental file list
popos2202/
popos2202/common/
popos2202/common/home/
popos2202/common/home/test.txt
  0  0%  0.00kB/s  0:00:00  87 100%  84.96kB/s  0:00:00 (xfr#1,
to-chk=6/11)
popos2202/common/home/linuxadmin/
popos2202/postsync.d/
popos2202/postsync.d/00-lcst-fix-initrd
  0  0%  0.00kB/s  0:00:00 269 100% 262.70kB/s  0:00:00 (xfr#2,
to-chk=4/11)
```

Hier kann kontrolliert werden, ob der gewünschte Rechner, Raum, die korrekte Patchklasse und Hostgruppe ausgewählt wurden. Zudem werden die übertragenen Dateien / Scripte dargestellt.

4.19 Leoclient 2 - Windows im Linuxclient

Leoclient2 bietet die Möglichkeit auf einem Linuxclient verschiedene virtuelle Maschinen, beispielsweise mit Windows-Betriebssystem, einzurichten und zu starten.

Inhalt:

4.19.1 Funktionsprinzip

Durch das Programmpaket leoclient2 ist es möglich auf einem Linuxclient virtuelle Maschinen (VM), beispielsweise mit Windows-Betriebssystem, parallel zu nutzen.

Dabei können auf einfache Weise verschiedene Zustände der virtuellen Maschine erzeugt und den Benutzern angeboten werden.

Zur Auswahl der virtuellen Maschinen als Benutzer wurde eine grafische Oberfläche programmiert, auf der man zuerst die zu nutzende VM auswählt und dann den gewünschten Zustand startet.

Durch die Virtualisierung reduziert sich der administrative Aufwand auf ein Minimum, wogegen die Möglichkeit der Bereitstellung verschiedener Installationszustände extreme Flexibilität und ungeahnte Möglichkeiten bietet.

4.19.2 Installation von leoclient2

Software-Pakete installieren

Die leoclient2-Pakete liegen auf dem linuxmuster.net-Paketserver <https://deb.linuxmuster.net/>, der im Linuxclient eventuell schon zur Einrichtung der Anmeldung am Server (Domänenanmeldung) eingetragen wurde. Dann ist der Schlüssel schon als linuxmuster.net.gpg vorhanden.

```
# cd /etc/apt/trusted.gpg.d
# wget https://deb.linuxmuster.net/pub.gpg
```

In /etc/apt/sources.list Paketquellen eintragen:

```
deb https://deb.linuxmuster.net/ lmn71 main          (von Domänenanmeldung schon vorhanden)
deb https://deb.linuxmuster.net/ lmn71-testing main  (leoclient2 aus testing!!!)
```

Installation der Pakete auf dem Linuxclient mit folgenden Befehlen:

```
# sudo apt update
# sudo apt install leoclient2-leovirtstarter-client leoclient2-vm-printer
```

Virtualbox installieren/updates

Es wird empfohlen unter Ubuntu 22.04 die aktuelle Version von Virtualbox zu installieren.

```
# sudo apt update
# sudo apt install virtualbox virtualbox-guest-additions-iso
```

Zugehöriges Erweiterungspaket von VirtualBox installieren. Dazu mit dpkg die Versionsnummer von VirtualBox auffindig machen und den Downloadlink entsprechend anpassen.

```
# dpkg -l | grep virtualbox
ii virtualbox                    6.1.38-dfsg-3~ubuntu1.22.04.1
↳ amd64 x86 virtualization solution - base binaries
# cd /tmp
# wget https://download.virtualbox.org/virtualbox/6.1.38/Oracle_VM_VirtualBox_Extension_Pack-6.1.38.vbox-extpack
↳ Pack-6.1.38.vbox-extpack
```

als linuxadmin anmelden und virtualbox starten. Unter Datei -> Einstellungen -> Zusatzpakete: mit + hinzufügen und heruntergeladene Datei in /tmp auswählen und installieren.

Gruppenzugehörigkeiten anpassen

Lokale Benutzer

Lokale Benutzer am Linuxclient (z.B. linuxadmin) müssen der Gruppe vboxusers hinzugefügt werden. Für den lokalen Benutzer linuxadmin erfolgt das mit:

```
# sudo adduser linuxadmin vboxusers
```

Weitere lokale Benutzer können entsprechend hinzugefügt werden. Diese Änderung wird erst bei einer erneuten Anmeldung des Nutzers wirksam.

Domänenbenutzer

Anpassen der Datei `/etc/group` über ein Anmeldescript `/etc/linuxmuster-linuxclient7/onLoginAsRoot.d/10_vboxusers-group.sh`. Dabei wird den Gruppen `vboxusers` und `lpadmin` der sich anmeldende Benutzer `$USER` hinzugefügt. Der Eintrag in `lpadmin` berechtigt zur Anpassung der Druckerkonfiguration (z.B. Standarddrucker), die Mitgliedschaft in `vboxusers` ermöglicht die umfangreiche Nutzung von Virtualbox. Die Anpassungen in der Datei `/etc/group` zeigen sofort Wirkung und nicht erst nach einer erneuten Anmeldung.

```
#!/bin/bash
# mit diesem Script sollen zusätzliche Gruppenzugehörigkeiten
# eingerichtet werden, da dies über PAM aktuell nicht funktioniert

# Aktuellen Benutzer in Gruppe vboxusers und lpadmin in /etc/group eintragen
# vboxusers:x:136:linuxadmin ersetzen mit vboxusers:x:136:linuxadmin,$USER
# lpadmin:x:122:linuxadmin ersetzen mit lpadmin:x:122:linuxadmin,$USER
# wenn vboxusers vorhanden und $USER dort nicht enthalten

USER=`echo $USER | tr [:upper:] [:lower:]`

if [ 'grep vboxusers /etc/group' != "" ];
then
    if [ "`grep vboxusers /etc/group | grep $USER`" = "" ];
    then
        sed -i "s|vboxusers:x:136:linuxadmin|vboxusers:x:136:linuxadmin,$USER|g" /etc/
↪group
    fi
fi

if [ 'grep lpadmin /etc/group' != "" ];
then
    if [ "`grep lpadmin /etc/group | grep $USER`" = "" ];
    then
        sed -i "s|lpadmin:x:122:linuxadmin|lpadmin:x:122:linuxadmin,$USER|g" /etc/group
    fi
fi
```

Benutzerrechte erweitern mit sudo

Einträge in `/etc/sudoers.d/80-leoclient2` sind vorzunehmen, um die notwendigen Rechte für das `leovirtstarter2`-Skript zu erweitern. Die lokalen Benutzer (`linuxadmin`, `localuser`) und Domänenbenutzer (`%schools`) erhalten sudo-Rechte ohne Passwortabfrage. Änderungen über `# sudoedit /etc/sudoers.d/80-leoclient2`

```
# leoclient2 needs to make a VM of other users usable
# option --set-permissions allows to do this
# option --register-machine allows to do this
%schools ALL=NOPASSWD: /usr/bin/leovirtstarter2 --set-permissions, /usr/bin/
↪leovirtstarter2 --register-machine *
linuxadmin ALL=NOPASSWD: /usr/bin/leovirtstarter2 --set-permissions, /usr/bin/
↪leovirtstarter2 --register-machine *
localuser ALL=NOPASSWD: /usr/bin/leovirtstarter2 --set-permissions, /usr/bin/
↪leovirtstarter2 --register-machine *
```

Weitere sudo-Rechte setzen mit `sudoedit /etc/sudoers.d/60-mkdir`, um notwendige Berechtigungen für das Snapshot-Verzeichnis `/media/localdisk/cache` zu erhalten (dazu später mehr).

```
# leoclient2 needs to make a directory /media/localdisk/cache
%schools ALL=NOPASSWD: /bin/mkdir
%schools ALL=NOPASSWD: /bin/chmod
linuxadmin ALL=NOPASSWD: /bin/mkdir
linuxadmin ALL=NOPASSWD: /bin/chmod
localuser ALL=NOPASSWD: /bin/mkdir
localuser ALL=NOPASSWD: /bin/chmod
```

Dateien unter /etc/sudoers.d müssen Rechte 440 haben:

```
# sudo chmod 440 /etc/sudoers.d/80-leoclient2
# sudo chmod 440 /etc/sudoers.d/60-mkdir
```

Startskripte

Damit alle Benutzer im Verzeichnis /media Schreibrechte erhalten, um verschiedene Links einrichten zu können, werden die Berechtigungen über das Skript /etc/linuxmuster-linuxclient7/onLoginAsRoot.d/03_media-rechte.sh angepasst.

```
#!/bin/bash

chmod 777 /media
```

Für den leovirtstarter2 sollen die Snapshots vom Server in einem lokalen Verzeichnis gecacht werden. Dieses kann eine separate Partition (Datenpartition) sein und ist erreichbar über /media/localdisk. Eine separate Partition ist hilfreich, denn dann wird der cache beim Synchronisieren des Betriebssystems nicht gelöscht.

```
# sudo mkdir /media/localdisk
bzw. passender Eintrag für ``/media/localdisk`` in ``/etc/fstab``.
```

Die notwendigen Schreibrechte werden in /etc/linuxmuster-linuxclient7/onLoginAsRoot.d/40_localdisk.sh eingerichtet.

```
#!/bin/bash
# Schreibrechte auf Datenpartition setzen
sudo chmod 777 /media/localdisk
```

Hat ein anderer Benutzer einen Snapshot vom Server im lokalen Verzeichnis /media/localdisk/cache/ gecacht, muss der Snapshot für andere Benutzer freigegeben werden. Dazu werden in /etc/linuxmuster-linuxclient7/onLoginAsRoot.d/50_leoclient2.sh die notwendigen Rechte gesetzt. Außerdem werden die virtuellen Maschinen, die unter /virtual/leoclient2-vm/ liegen, für alle Benutzer lesbar gemacht (Hintergrund: Bei der Nutzung einer VM durch einen Benutzer werden die Berechtigungen für andere entfernt.)

Es bietet sich an den Ort für die virtuellen Maschinen /virtual/leoclient2-vm in eine separate Partition unter /virtual zu legen, dann kann man die virtuellen Maschinen unabhängig vom Betriebssystem.

/etc/linuxmuster-linuxclient7/onLoginAsRoot.d/50_leoclient2.sh

```
#!/bin/bash
# Schreibrechte auf alle gecachten Snapshots
chmod -R 777 /media/localdisk/cache/*
# Zugriffsrechte auf alle VMs setzen beim Anmelden
chmod -R 755 /virtual/leoclient2-vm/*
```


Links von früheren Benutzeranmeldungen müssen entfernen werden. Dazu das Skript `/etc/linuxmuster-linuxclient7/onLoginAsRoot.d/01_links-entfernen.sh` erstellen.

```
#!/bin/bash

# Link von /home/$USER/media/ISO für Virtuelle Maschinen auf /virtual/server
# muss vorher als root gelöscht werden
rm /virtual/server

# Link von /media/Tausch_auf_Server auf /home/$USER/Tausch_auf_Server
# muss vorher als root gelöscht werden
rm /media/Tausch_auf_Server

# Link zu Schülerhomes Schueler_auf_Server in /media, wenn vorhanden (nur für Lehrkräfte)
# muss vorher als root gelöscht werden
rm /media/Schueler_auf_Server
```

Zum Säubern von Einträgen von anderen Benutzern `/etc/linuxmuster-linuxclient7/onLoginAsRoot.d/02_leoclient2-log-heimat-entfernen.sh` anlegen.

```
#!/bin/bash
# leovirtstarter2-log-Dateien entfernen
rm /tmp/leovirtstarter2*.log
# Eintrag des bisher angemeldeten Benutzers entfernen
rm /tmp/heimatverzeichnis
```

Skripte für Login im User-Kontext

Für den einfachen Zugriff auf die Servershares werden verschiedene Links angelegt mit `/etc/linuxmuster-linuxclient7/onLogin.d/10_links.sh`.

```
#!/bin/bash

USER=`echo $USER | tr [:upper:] [:lower:]`

# Link von Home_auf_Server in lokales Home, wenn noch nicht vorhanden
if [ ! -L /home/$USER/Home_auf_Server ] && [ ! -f /home/$USER/Home_auf_Server ]; then
    ln -s "/home/$USER/media/$USER (H:)" "/home/$USER/Home_auf_Server"
fi

# Link von Tauschverzeichnissen in lokales Home
# mit Unterverzeichnis "Tausch_auf_Server" für deutsche Bezeichnungen darunter
# Verzeichnis Tausch_auf_Server mit Inhalten, wenn noch nicht vorhanden
if [ ! -L /home/$USER/Tausch_auf_Server ] && [ ! -d /home/$USER/Tausch_auf_Server ]; then
    mkdir /home/$USER/Tausch_auf_Server
    ln -s "/home/$USER/media/Shares/projects" "/home/$USER/Tausch_auf_Server/Projekte"
    ln -s "/home/$USER/media/Shares/classes" "/home/$USER/Tausch_auf_Server/Klassen"
    ln -s "/home/$USER/media/Shares/school" "/home/$USER/Tausch_auf_Server/Schule"
    ln -s "/home/$USER/media/Shares/teachers" "/home/$USER/Tausch_auf_Server/Kollegium"
fi

# Link von /media/Tausch_auf_Server auf /home/$USER/Tausch_auf_Server
# muss vorher als root gelöscht werden /etc/linuxmuster-linuxclient7/onLoginAsRoot.d/03_
↪ link-media-tausch.sh
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```

if [ -d /home/$USER/Tausch_auf_Server ]; then
    ln -s /home/$USER/Tausch_auf_Server /media/Tausch_auf_Server
fi

# Link zu Schülerhomes in lokales Home, wenn vorhanden (nur für Lehrkräfte)
if [ ! -L /home/$USER/Schueler_auf_Server ] && [ ! -d /home/$USER/Schueler_auf_Server ] &
  ↪& [ -d /home/$USER/media/Students-Home ]; then
    ln -s "/home/$USER/media/Students-Home" "/home/$USER/Schueler_auf_Server"
fi
# Link zu Schülerhomes Schueler_auf_Server in /media, wenn vorhanden (nur für ↪
  ↪Lehrkräfte)
# muss vorher als root gelöscht werden /etc/linuxmuster-linuxclient7/onLoginAsRoot.d/03_
  ↪link-media-tausch.sh
if [ -L /home/$USER/Schueler_auf_Server ]; then
    ln -s /home/$USER/Schueler_auf_Server /media/Schueler_auf_Server
fi

# Link für Virtuelle Maschinen auf /virtual/server
# muss vorher als root gelöscht worden sein
ln -s "/home/$USER/media/ISO" "/virtual/server"

```

Skript /etc/linuxmuster-linuxclient7/onLogin.d/50_leoclient2-printer.sh zum Starten der Druckskripte. Damit werden pdf-Dateien, die in der VM erzeugt werden und unter Home_auf_Server abgelegt werden zum Standarddrucker übertragen. Somit kann man aus der VM heraus ohne direkte Netzverbindung auf Netzwerkdrucker ausdrucken.

```

#!/bin/bash

# Die Skripte run-vm-printer2-spooler und run-vm-printer2-splitter
# überprüfen ständig, ob der angemeldete Benutzer
# (Eintrag in /tmp/heimatverzeichnis) noch mit dem Benutzer
# übereinstimmt, der das Skript gestartet hat.
# Ist dies nicht der Fall, wird das Skript beendet.

USER=`echo $USER | tr [:upper:] [:lower:]`

# Anlegen der Datei /tmp/heimatverzeichnis mit dem lokalen USER-home

echo /home/$USER > /tmp/heimatverzeichnis
chmod 777 /tmp/heimatverzeichnis

# kurze Pause, damit eventuell noch laufende printer-Skripte
# durch anderes /tmp/heimatverzeichnis beendet werden können
sleep 5

# Starten der Skripte für das Ausdrucken aus der VM
run-vm-printer2-spooler &
run-vm-printer2-splitter &

```

Eintrag in /etc/leoclient2/leoclient-vm-printer2.conf anpassen in welcher Datei das Ausdruck aus der VM abgelegt wird -> \$print_file_user="ausdruck-winxp.pdf";. Damit wird die Datei ausdruck-winxp.pdf unter Home_auf_Server auf dem Standarddrucker des Ubuntu-Rechners ausgedruckt.

Sicherungen der Skripte löschen (mit „~“ am Ende), die durch Änderungen entstehen. Diese würden sonst ebenso ausgeführt werden!!!

```
# sudo rm /etc/linuxmuster-linuxclient7/onLogin.d/*~
# sudo rm /etc/linuxmuster-linuxclient7/onLoginAsRoot.d/*~
```

Rechte der oben neu erstellten Dateien unter `/etc/linuxmuster-linuxclient7/onLogin.d/` bzw. `/etc/linuxmuster-linuxclient7/onLoginAsRoot.d/` anpassen, die bei der Anmeldung ausgeführt werden sollen, damit diese ausgeführt werden können.

```
# chmod +x /etc/linuxmuster-linuxclient7/onLoginAsRoot.d/*
# chmod +x /etc/linuxmuster-linuxclient7/onLogin.d/*
```

Abschließend muss man die Standard-VM in `/etc/leoclient2/servers.conf` eintragen (hier: „win7“), außerdem den Pfad zu den Snapshots für die VMs auf dem Server. Die Snapshots mit der folgenden Einstellung liegen für die VM „win7“ auf dem Server im Verzeichnis `/virtual/server/leoclient2-vm/win7`. Lokal liegen die VMs unter `/virtual/leoclient2-vm`.

```
# common configuration for the machines
#
# which machine is the default
DEFAULT=win7-64
# where is/are the mounted server dir for snapshots
SERVERDIR=/virtual/server/leoclient2-vm
```

Fehleranalyse

Zur Fehlerbehebung werden Log-Dateien in `/tmp/run-vm-printer2-spooler.log-USERNAME` und `/tmp/run-vm-printer2-splitter.log-USERNAME` abgelegt. Dort sieht man nach welcher Datei der Drucker-Splitter sucht.

Die log-Datei für den leovirtstarter2 liegt ebenfalls unter `/tmp`.

4.19.3 Virtuelle Maschine erzeugen

Das Script `leoclient2-init` bereitet eine virtuelle Maschine (VM) vor, die später mit dem Programm `leovirtstarter2` gestartet werden kann.

Die VM kann nur in einem Verzeichnis erstellt werden das der aufrufende User anlegen darf. Üblicherweise muss das Script also mit root-Rechten gestartet werden:

```
# sudo leoclient2-init
[sudo] Passwort für linuxadmin:

Geben Sie den Namen der neuen virtuellen Maschine ein
(Keine Leerzeichen - bestätigen mit der Enter-Taste):
winxp
...
Soll die virtuelle Maschine jetzt erzeugt und VirtualBox gestartet werden?
(j/n - Bestätigen mit der Enter-Taste):
j

Virtual machine 'winxp' is created and registered.
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
UUID: d96f7ee1-3c82-4bef-aa04-c9d39140cede
Settings file: '/virtual/winxp/winxp.vbox'
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
Medium created. UUID: 4da77206-3edf-41d6-84ec-1509cfb92441
```

Es werden folgende Parameter abgefragt und auf Nachfrage VirtualBox gestartet.

- der MASCHINENAME für die VM (keine Leerzeichen verwenden)
- der PFAD für den Speicherort der VM (Standardpfad `/var/virtual/`)
- die Größe der dynamisch wachsenden virtuellen Festplatte für die VM in MB

Man sollte unter VirtualBox die Konfiguration der VM noch an die eigenen Bedürfnisse anpassen (Die Arbeitsspeichergröße für die VM wird beim Starten an die Gegebenheiten der vorhandenen Maschine angepasst).

Betriebssystemeinstellungen

Unter Allgemein, Reiter Basis muss der Betriebssystemtyp und Version angepasst werden.

Systemanforderungen/Ressourcen

Unter System, wird konfiguriert, welche Hardware-Ressourcen die VM zur Verfügung gestellt bekommt. Je nach Gast sind hier Mindestwerte zu beachten:

Win10 (Beispielhaft):

- Hauptspeicher 2048 MB (System -> Hauptplatine)
- 2 CPU's (System -> Prozessor)
- 64 MB Grafikspeicher (System -> Bildschirm)

DVD-Laufwerk

Ein CD-/DVD-Laufwerk kann man ebenso einbinden wie iso-Dateien (→ CD-/DVD-Laufwerk hinzufügen → kein Medium (Laufwerk) → über das CD-Symbol rechts das Laufwerk auswählen bzw. → CD-/DVD-Laufwerk hinzufügen → Medium auswählen (iso-Datei)).

USB verwenden

Sollte man, wie voreingestellt, USB2 verwenden wollen, muss man das zur Version von VirtualBox passende Extension Pack installieren.

Netzwerk offline

Eine Netzwerkkarte ist in der Standardkonfiguration nicht aktiviert, dadurch bietet die VM keine Angriffsfläche und man kann auf zeitraubende Updates verzichten.

Wenn sie aktiviert wird, gilt das nur vorübergehend.

Trotzdem ist es möglich auf die Netzlaufwerke auf dem Server zuzugreifen und Netzwerkdrucker zu verwenden.

Betriebssystem installieren

Sind die Einstellungen wunschgemäß, startet man die VM und installiert das Betriebssystem über eine verbundene Installations-CD-/DVD oder eine entsprechende iso-Datei.

Ist die Installation abgeschlossen, fährt man die VM herunter. Bevor VirtualBox beendet wird, sollte man eventuell verbundene CD-/DVD-Laufwerke trennen.

Nach Beenden von Virtualbox wird die VM für den Start mit dem Programm `leovirtstarter2` fertiggestellt.

```
...
Für diese Maschine wird ein Sicherungspunkt erzeugt.
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
Snapshot taken. UUID: 3df3f4f2-38e8-4747-9934-533648e60d3f
...
Die Konfigurationsdateien und der Snapshot wurden gesichert.
Die Rechte der Dateien wurden angepasst.
Die virtuelle Maschine kann nun mit dem Snapshotstarter benutzt werden.

Wenn Sie die Basis für die virtuelle Maschine und den Snapshot neu
erzeugen wollen, starten Sie das Script 'leoclient2-base-snapshot-renew'.

Wenn Sie die vollständige virtuelle Maschine in ein anderes Verzeichnis
umziehen wollen, starten Sie das Script 'leoclient2-vm-move'.
```

Weitere Schritte

Nachdem das Betriebssystem installiert ist, ist es sinnvoll in der Basis der VM noch folgende Anpassungen vorzunehmen:

- Installation der Gasterweiterungen in der VM
- Verbinden der Netzlaufwerke in der VM
- Einrichten eines PDF-Druckers in der VM
- (Schrumpfen ???)

Diese Anpassungen unterscheiden sich je nach verwendeten Betriebssystem. Anleitungen finden sie bei „Weitere Informationen zu leoclient2“ und dem jeweiligen Gastbetriebssystem unter Tipps und Tricks.

Danach muss die Basis aktualisiert werden (Siehe folgendes Kapitel: Basis und Snapshots verwalten).

4.19.4 Virtuelle Maschinen starten

Das Script `leovirtstarter2` findet automatisch jede verfügbare VM (Eintrag in `/etc/leoclient2/machines`) und bietet diese zum Starten an. Es kann im Ubuntu Dash (Virtualbox Snapshotstarter) oder über die Konsole gestartet werden:

```
$ leovirtstarter2
```

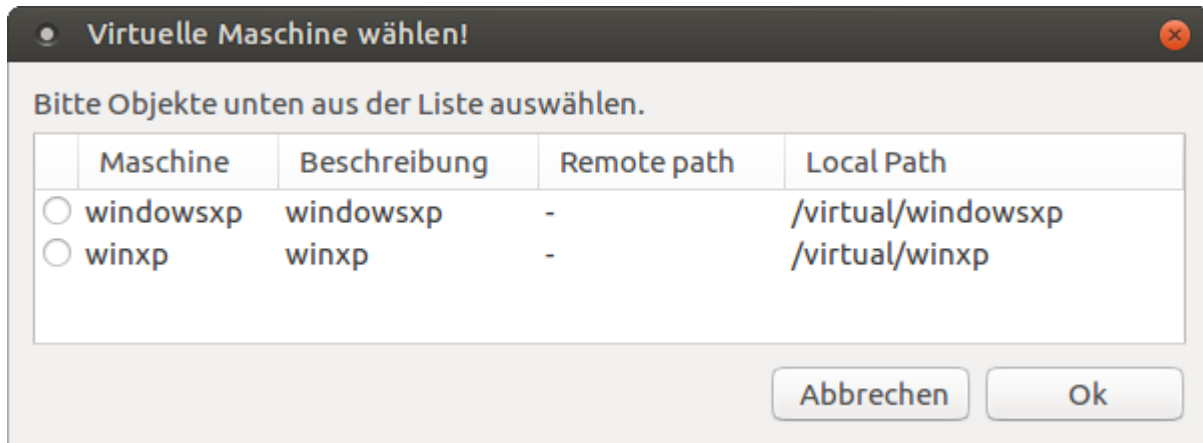


Abb. 421: Wählen Sie eine virtuelle Maschine

Nachdem eine VM gewählt wurde, werden mehrere Optionen angeboten

<VM> wie vorgefunden startet den aktuellen, unveränderten Zustand
der VM

<VM> Standard verwendet den Standard-Snapshot und startet die VM,
d.h. die virtuelle Maschine wird auf den Zustand des Snapshots zurückgesetzt.

optional weitere Snapshots wenn konfiguriert, tauchen weitere lokal
oder auf einem Serverlaufwerk gespeicherte Snapshots auf

Virtuelle Grafik Diese Optionen sind bisher ohne Funktion

Virtueller Arbeitsspeicher (RAM) Arbeitsspeicherzuweisung an die
VM - vorausgewählt ist ein automatisch an den vorhandenen realen Hauptspeicher angepasster Wert. Mit der Auswahl kann man den Hauptspeicher der VM etwas erhöhen oder vermindern.

Nach Auswahl wird die VM mit dem Button **Starten!** gestartet.

4.19.5 Basis und Snapshots verwalten

Jede virtuelle Maschine besitzt neben der Basis `/PFAD/MASCHINENNAME/MASCHINENNAME.vdi` einen Standard-Snapshot.

Zuerst sollte man eine solide VM-Basis erstellt haben. Da alle darauf basierenden weiteren Snapshots unbrauchbar werden, wenn die Basis aktualisiert werden muss.

Aufbauend auf diese Basis können dann weitere Snapshots erzeugt werden.

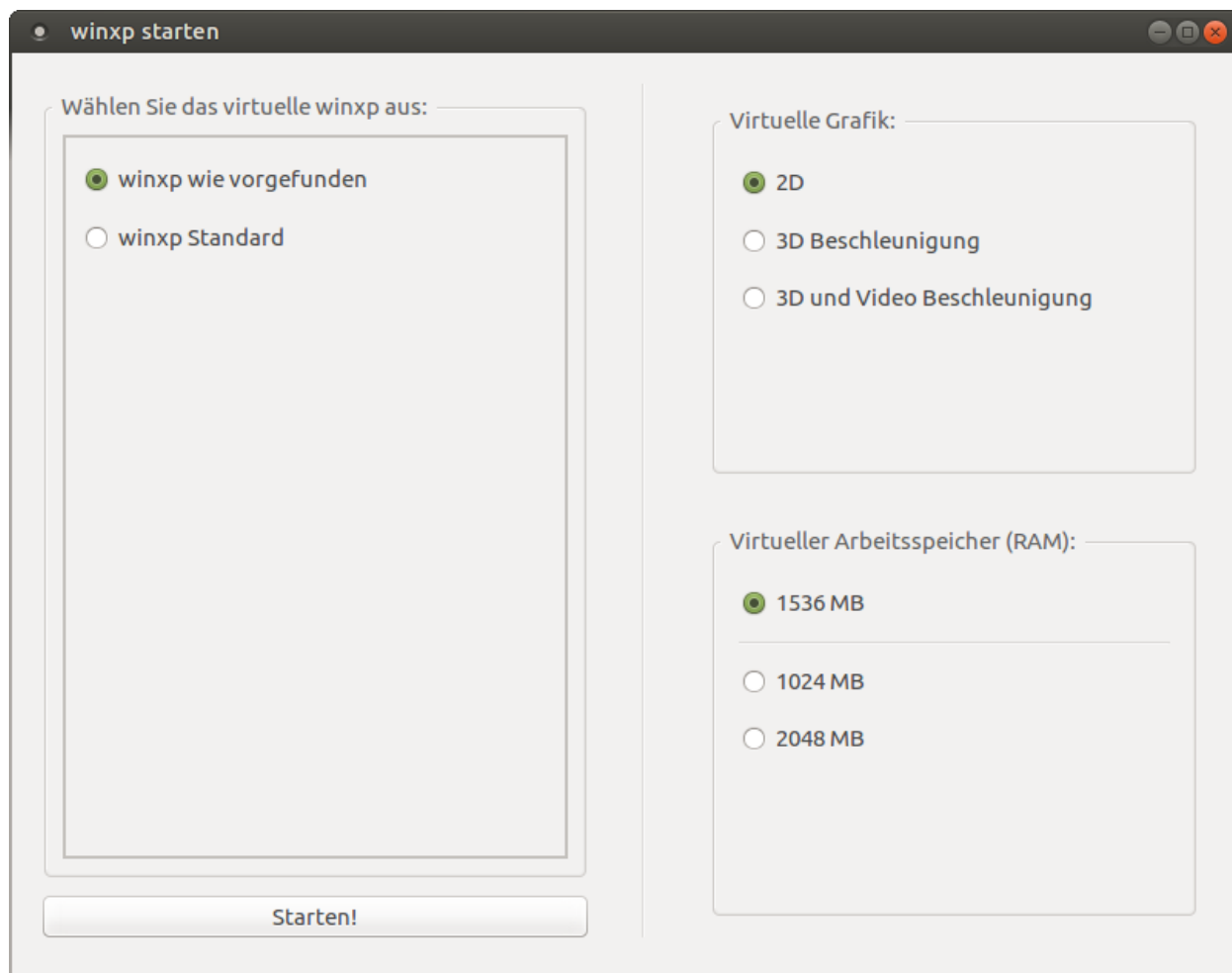


Abb. 422: Optionen zum Starten der virtuellen Maschine

VM-Basis aktualisieren

Mit Hilfe des Skripts `leoclient2-base-snapshot-renew` wird der aktuelle Zustand der virtuellen Maschine zur neuen Basis.

Hinweis: Durch eine Erneuerung der Basis werden alle (anderen) darauf aufbauenden Snapshots unbrauchbar.

Nach dem Aufruf des Skripts `leoclient2-base-snapshot-renew` mit root-Rechten

```
$ sudo leoclient2-base-snapshot-renew
```

sind einige selbsterklärende Fragen zu beantworten.

- Soll der Vorgang abgebrochen werden? (J/N)
- Name der virtuellen Maschine? (VM, die erneuert werden soll)
- Speicherort der virtuellen Maschine? (VM, die erneuert werden soll)

Das Skript startet dann zunächst VirtualBox, um die Sicherungspunkte zu löschen. Eine eventuelle Warnung, die aufgrund fehlender Verbindungen erscheint, kann ignoriert werden. Die Ursache ist z.B. bei dem vorkonfigurierten Ubuntu von linuxmuster.net die fehlende Verbindung zu den Homes als linuxadmin.

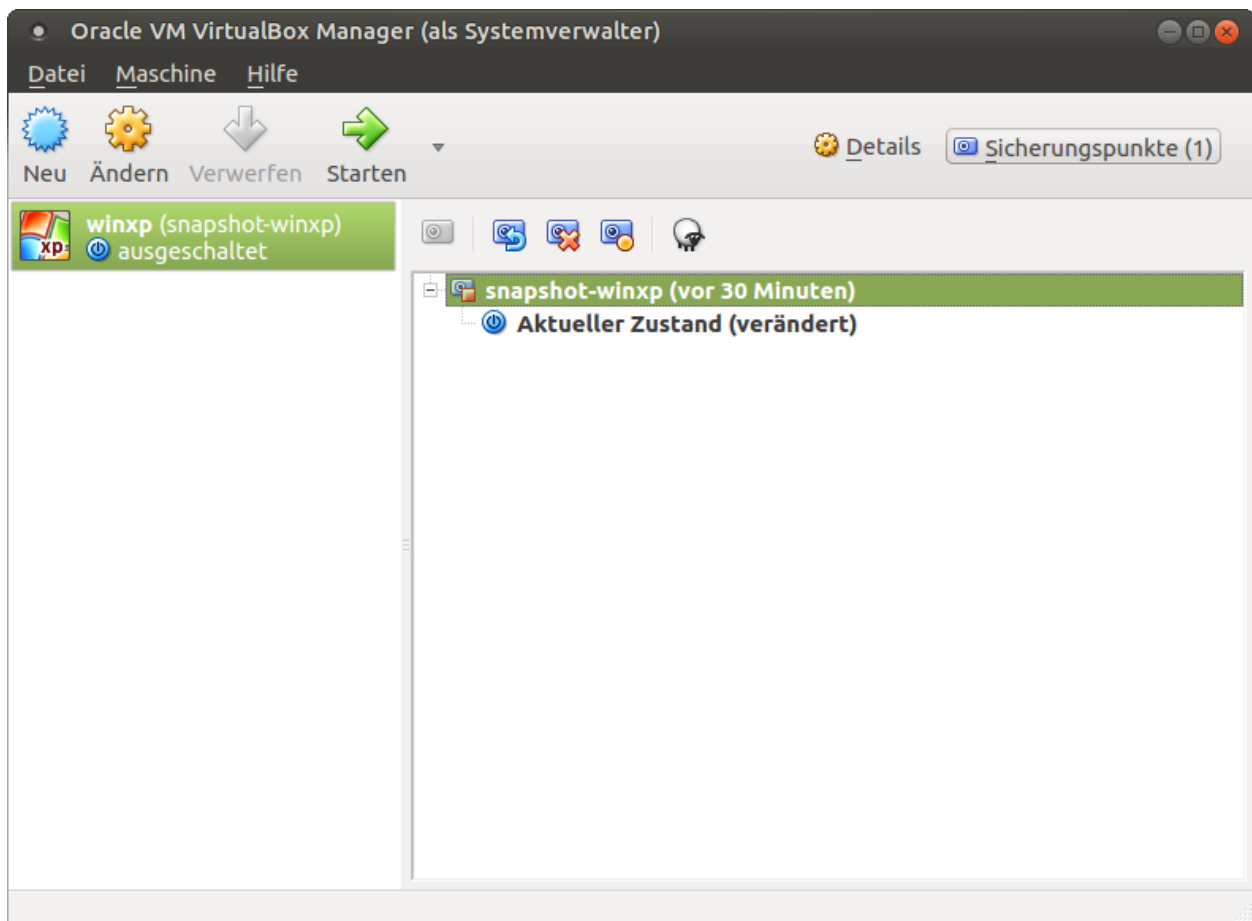


Abb. 423: VirtualBox-Optionen für Snapshots

- Klicken Sie rechts oben auf die Schaltfläche „Sicherungspunkte (1)“.

- Klicken Sie auf den Snapshot, löschen Sie diesen mit einem Rechtsklick oder mit dem entsprechenden Icon und bestätigen Sie mit „Löschen“ den nächsten Dialog.

Haben Sie im aktuellen Zustand bereits Änderungen vorgenommen, so kann das Löschen des Snapshots eine Weile dauern. Im Anschluss kann die VM gestartet werden und (weitere) gewünschte Änderungen durchgeführt werden.

- Schalten Sie die VM aus und beenden Sie VirtualBox

Das Skript erzeugt eine neue Basisfestplatte unter `/PFAD/MASCHINENAME/MASCHINENAME.vdi` und komprimiert sie (Das dauert einige Minuten). Darüber hinaus wird noch ein neuer Standard-Snapshot erzeugt und gezippt. Der Name des neuen Snapshots, hier: `{c81442ac-4e03-487c-a05a-e82b8918c834}.vdi`, erscheint in der Konsolenausgabe.

```
...
#### Processing snapshot: standard ####
* Zipping standard:
  * Image:  /virtual/winxp/snapshot-store/standard/{c81442ac-4e03-487c-a05a-
↪e82b8918c834}.vdi
  * Dir:    /virtual/winxp/snapshot-store/standard
  * File:   {c81442ac-4e03-487c-a05a-e82b8918c834}.vdi
...
```

- Vergleichen Sie den neuen Snapshot-Dateinamen und löschen Sie den alten Standard-Snapshot entsprechend dem Muster `sudo rm /PFAD/MASCHINENAME/{..alterSnapshot..}.vdi*`

```
$ ls -l /virtual/winxp/snapshot-store/standard/
{4a895e9c-a6e9-416d-b612-b643035c0103}.vdi
{4a895e9c-a6e9-416d-b612-b643035c0103}.vdi.zip
{c81442ac-4e03-487c-a05a-e82b8918c834}.vdi
{c81442ac-4e03-487c-a05a-e82b8918c834}.vdi.zip
filesize.vdi
filesize.vdi.zipped
$ sudo rm /virtual/winxp/snapshot-store/standard/{4a895e9c-a6e9-416d-b612-
↪b643035c0103}.vdi*
```

- Sollten Sie weitere Snapshots zur virtuellen Maschine haben, haben diese ihre Basis verloren. Löschen Sie diese Snapshots (als root) oder erzeugen Sie sie erneut aus dem bestehenden neuen Standard-Snapshot.

```
$ ls -l /virtual/winxp/snapshot-store/Software2016
{4a895e9c-a6e9-416d-b612-b643035c0103}.vdi
{4a895e9c-a6e9-416d-b612-b643035c0103}.vdi.zip
filesize.vdi
filesize.vdi.zipped
$ sudo leoclient2-snapshot-create -m winxp -s Software2016
adding: {c81442ac-4e03-487c-a05a-e82b8918c834}.vdi (deflated 100%)
OK: Snapshot {c81442ac-4e03-487c-a05a-e82b8918c834}.vdi wurde als Software2016.
↪gesetzt.
```

Neue Snapshots erzeugen

Das Skript `leoclient2-snapshot-create` legt mit dem aktuellen Zustand der VM einen neuen auswählbaren Snapshot an oder den Standard-Snapshot neu.

Hinweis: Die Basis, d.h. die zugrundeliegende Basisfestplatte wird dabei nicht verändert. Eine veränderte Hardwarekonfiguration speichert das Skript auch nicht.

Vorgehensweise:

- Laden Sie das Skript herunter: `leoclient2-snapshot-create`
- Legen Sie es unter `/usr/bin/leoclient2-snapshot-create` ab und machen Sie es ausführbar.

```
$ sudo mv leoclient2-snapshot-create /usr/bin/
$ sudo chmod 755 /usr/bin/leoclient2-snapshot-create
```

- Starten Sie als Benutzer die VM (z.B. hier `winxp`)

```
$ leovirtstarter2
```

- Installieren Sie Software nehmen Sie die Änderungen vor, fahren Sie die VM herunter.
- Rufen Sie das Skript (als root) ohne Argument `-s` auf, um den Standard-Snapshot neu zu setzen,

```
$ sudo leoclient2-snapshot-create -m winxp
```

- oder mit einem Argument `-s`, um einen neuen Snapshot zu erzeugen.

```
$ sudo leoclient2-snapshot-create -m winxp -s Software2016
```

Jetzt erscheint im Auswahlmenü von `leovirtstarter2` ein neuer Snapshot mit dem Namen `Software2016`.

4.19.6 Umzug von Leoclient1 nach Leoclient2

Für den Umzug benötigen Sie die alte virtuelle Festplatte `old.vdi` und den alten Standard-Snapshot `old-snapshot.vdi` der `leoclient1`-VM.

- Ermitteln Sie die Größe und UUID der alten Festplatte

```
# vboxmanage showmediuminfo /media/old/old.vdi | grep -E 'UUID|MBytes'
UUID:          22df228d-ecb2-44ba-a281-7c73a02d26bc
Parent UUID:    base
Capacity:       16384 MBytes
Size on disk:   1921 MBytes
```

- Erzeugen Sie eine neue virtuelle Maschine nach [Anleitung](#) (mindestens) mit der ermittelten Größe. Im Beispiel wird die neue VM „win-migrate“ genannt. Auf die Installation des Betriebssystems kann verzichtet werden. Ändern Sie Typ und Version des Betriebssystems und schließen Sie VirtualBox.
- Ermitteln Sie die UUID der neuen Festplatte:

```
# VBOX_USER_HOME=/var/virtual/win-migrate vboxmanage showmediuminfo /var/virtual/
↳ win-migrate/win-migrate.vdi | grep ^UUID
UUID:          1fbc6a0c-d9c9-48bf-ad1c-e94c4d7da406
```

- Kopieren Sie die alte virtuelle Festplatte auf die neue Festplatten-Datei

```
# cp /media/old/old.vdi /var/virtual/win-migrate/win-migrate.vdi
```

- Korrigieren Sie die UUID an den entsprechenden Stellen mit dem Schema `sed -i "s@neue UUID@alte UUID@"` Datei

```
# sed -i "s@1fbc6a0c-d9c9-48bf-ad1c-e94c4d7da406@22df228d-ecb2-44ba-a281-7c73a02d26bc@" /var/virtual/win-migrate/win-migrate.vbox
# sed -i "s@1fbc6a0c-d9c9-48bf-ad1c-e94c4d7da406@22df228d-ecb2-44ba-a281-7c73a02d26bc@" /var/virtual/win-migrate/defaults/win-migrate.vbox
```

- Kopieren Sie den alten Standard-Snapshot in das Unterverzeichnis `Snapshots` unter Verwendung des bestehenden Dateinamens der Snapshot-Datei der neuen virtuellen Maschine (bestehende Datei ersetzen).

```
# cp /media/old/old-snapshot.vdi /var/virtual/win-migrate/Snapshots/{08b01eb0-2f5b-4091-acf7-cd5f8cbfcef7}.vdi
```

- Aus folgender Fehlermeldung kann man die UUIDs des alten (`ef8629ce-c7c1-424b-8089-0e1d526b0c2c`) und des neuen (`08b01eb0-2f5b-4091-acf7-cd5f8cbfcef7`) Snapshots herauslesen

```
# VBox_USER_HOME=/var/virtual/win-migrate vboxmanage showmediuminfo /var/virtual/win-migrate/Snapshots/*.vdi | grep Error

Access Error: UUID {ef8629ce-c7c1-424b-8089-0e1d526b0c2c} of the
medium
'/var/virtual/win-migrate/Snapshots/{08b01eb0-2f5b-4091-acf7-cd5f8cbfcef7}.vdi'
does not match the value {08b01eb0-2f5b-4091-acf7-cd5f8cbfcef7}
stored in the media registry
('/var/virtual/win-migrate/VirtualBox.xml')
```

- Korrigieren Sie die UUID des Snapshots in den folgenden Dateien wiederum mit dem Schema `sed -i "s@neue UUID@alte UUID@"` Datei

```
# sed -i "s@08b01eb0-2f5b-4091-acf7-cd5f8cbfcef7@ef8629ce-c7c1-424b-8089-0e1d526b0c2c@" /var/virtual/win-migrate/win-migrate.vbox
# sed -i "s@08b01eb0-2f5b-4091-acf7-cd5f8cbfcef7@ef8629ce-c7c1-424b-8089-0e1d526b0c2c@" /var/virtual/win-migrate/defaults/win-migrate.vbox
```

- Setzen Sie den Standard-Snapshot neu (Skript siehe *Neue Snapshots erzeugen*)

```
# leoclient2-snapshot-create -m win-migrate
adding: {08b01eb0-2f5b-4091-acf7-cd5f8cbfcef7}.vdi (deflated 57%)
OK: Snapshot {08b01eb0-2f5b-4091-acf7-cd5f8cbfcef7}.vdi wurde als standard gesetzt.
```

- Starten Sie `leovirtstarter2` mit normalen Benutzerrechten über die Konsole, eventuelle Fehlermeldungen können so gesehen werden.

Alte Dateien von leoclient1 entfernen

Die Pakete des alten Leoclient müssen von Hand entfernt werden:

```
# apt-get purge leoclient-leovirtstarter-client leoclient-leovirtstarter-common
# apt-get purge leoclient-leovirtstarter-server leoclient-tools leoclient-virtualbox
↪ leoclient-vm-printer
```

Evtl. alte Daten von leoclient (Version 1) entfernen:

```
# rm -rf /etc/leoclient
```

4.19.7 Weitere Informationen zu leoclient2

Speicherort der virtuellen Maschinen

Virtuelle Maschinen auf einer zusätzlichen Partition

Standardmäßig werden die Dateien einer lokalen VM unter `/var/virtual/` abgelegt. Dieses Verzeichnis liegt im normalen Dateisystem des Linuxclients. Es wird empfohlen, diesen Speicherort auf eine zusätzliche Partition auszulagern und nach `/var/virtual` per `fstab` mounten.

Gründe für diese Empfehlung:

- Eine Partition dynamisch unter `/media` dafür zu verwenden ist ungeeignet, da sich deren Namen und Zugriffsberechtigung je nach User ändern kann.
- Mit der Auslagerung erfolgt die Synchronisation der Installation des Linuxclients deutlich schneller.
- Die virtuellen Maschinen können über das Synchronisieren der zugehörigen Partition unabhängig von der Linuxinstallation zurückgesetzt werden.

Vorgehensweise:

Es existiert eine Partition `/dev/sda3` (wie z.B. bei der `start.conf` zum `default-cloop`), die mit `ext4` formatiert ist.

- Zunächst das Verzeichnis `/var/virtual/` leeren bzw. den Inhalt wegsichern.
- Die Datei `/etc/fstab` als root editieren und letzte Zeile ergänzen:

```
# /etc/fstab: static file system information.
#
/dev/sda3    /var/virtual    ext4    defaults    0    0
```

- Danach als root die Partition mounten und das ganze dann noch mit `df` überprüfen:

```
# mount -a
# df -h
```

- Nun ggf. die weggesicherten Dateien wieder nach `/var/virtual/` zurückspielen und von beiden Partitionen mit Hilfe von LINBO ein Image erstellen.

Achtung: Nach dem Anlegen einer neuen VM müssen beide Partitionen geimaged werden da beim Anlegen einer neuen VM diese unter `/etc/leoclient2/machines` registriert wird. Nach dem Verändern einer VM muss nur die zusätzliche VM-Partition geimaged werden.

Virtuelle Maschinen auf dem Server

Remote virtuelle Maschine erzeugen

Eine lokale VM wird zur remoten VM, indem

- die in `/etc/leoclient2/servers.conf` konfigurierbare Variable `SERVERDIR` auf ein Verzeichnis gesetzt wird, in das im Verlauf des Bootprozesses oder der Anmeldung ein Netzwerk-Share gemountet wird
- das Datenverzeichnis der VM auf den Server kopiert wird, z.B. das Verzeichnis `/var/virtual/winxp` in das vom Server gemountete Netzlaufwerk `/media/leoclient2-vm` kopiert wird.

```
$ sudo cp -R /var/virtual/winxp /media/leoclient2-vm
```

Prinzipiell kann die VM danach lokal gelöscht werden.

Dann wird die VM vor dem Starten vom Server nach lokal synchronisiert/kopiert. Da dabei beträchtliche Datenmengen übertragen werden, sollte man das nur bei kleinen, wenig genutzten VM's machen (z.B. einem Linux-MySQL-Server o.ä.).

VM Windows XP – Tipps und Tricks

- Zur Installation in VirtualBox ein CD-Rom-Laufwerk hinzufügen und dann darin das Installations-ISO einlegen, die NTFS-Schellformatierung genügt.
- Die Gasterweiterungen installieren, mit Hilfe der Menüleiste des VBox-Fensters bei „Geräte“. Dadurch wird auch die Maus nicht mehr gefangen und das Fenster der VM ist beliebig skalierbar.

Verbindung zu Home_auf_Server einrichten:

- Windows Explorer → Menü Extras → Netzlaufwerk verbinden
- einen Laufwerksbuchstabe auswählen (z.B. H:) und Ordner angeben: `\\vboxsrv\home`
- ggf. Verknüpfung auf Desktop ziehen und umbenennen

Verbindung zu Tausch-Ordner und USB-Sticks einrichten:

- Windows Explorer → Menü Extras → Netzlaufwerk verbinden
- einen Laufwerksbuchstabe und Ordner angeben: `\\vboxsrv\media`
- ggf. Verknüpfungen auf Desktop ziehen und umbenennen

PDF-Drucker in der VM einrichten

- Siehe FreePDF-Webseite: http://freepdfxp.de/download_de.html
- ghostscript Installieren
- Free-PDF Installieren (Version 4.08 bei mir ging 4.14 NICHT(Eigener Drucker anlegen bei 32bit Windows 7))
- FreePDF Config starten → admin Config starten
- Profile neu : Profil ausdrucken anlegen
- Button: Für das aktuelle Profil einen eigenen Drucker anlegen
- Profil ausdrucken bearbeiten: FreePDF Dialog
 - Als festen Dateinamen speichern
 - H:ausdruck.pdf (anpassen, entsprechend `/etc/leoclient2/leoclient-vm-printer2.conf`)

- Speichern
- Den Drucker FreePDF als Standard Drucker anlegen
- Äquivalent funktioniert das Programm PDF24

VM Windows 7 – Tipps und Tricks

Bei der Installation bricht die 64bit Version ab, wenn nur 1 GB RAM da ist.

Verbindung zu Home_auf_Server einrichten:

- **Windows Explorer** → **Rechte Maustaste auf Netzwerk** → **Netzlaufwerk verbinden**
- Laufwerksbuchstabe (Üblicherweise H:) und Pfad nennen: \\vboxsrv\home
- Verknüpfung auf Desktop ziehen und umbenennen

Verbindung zu Tausch-Ordern und USB-Sticks einrichten:

- **Windows Explorer** → **Rechte Maustaste auf Netzwerk** → **Netzlaufwerk verbinden**
- Laufwerksbuchstabe (Üblicherweise M:) und Pfad nennen: \\vboxsrv\media
- Verknüpfung auf Desktop ziehen und umbenennen

VM Windows 10 - Tipps und Tricks

Bei der Installation kommen komische Fehlermeldungen, wenn nicht mindestens 2 CPU und 2096MB RAM vorhanden sind.

Verbindung zu Home_auf_Server (im Homeverzeichnis) einrichten:

- **Windows Explorer** → **Rechte Maustaste auf Dieser PC** → **Netzlaufwerk verbinden**
- Laufwerksbuchstabe (Üblicherweise H:) und Pfad nennen: \\vboxsrv\home sowie Haken bei „Verbindung bei Anmeldung wiederherstellen“.
- Verknüpfung auf Desktop ziehen und umbenennen in z.B. Home_auf_Server

Verbindung zu Tausch-Ordern und USB-Sticks einrichten:

- **Windows Explorer** → **Rechte Maustaste auf Dieser PC** → **Netzlaufwerk verbinden**
- Laufwerksbuchstabe (Üblicherweise M:) und Pfad nennen: \\vboxsrv\media sowie Haken bei „Verbindung bei Anmeldung wiederherstellen“.
- Verknüpfung auf Desktop ziehen und umbenennen in z.B. Medien

PDF-Drucker in der VM einrichten

- PDFX Lite Home9 installieren
- PDFXChange 9.0.354.0 - complete
- Druckerverwaltung
- Benutzerdefinierte Filter → Alle Drucker → Rechtsklick auf PDF-XChange Lite
- Eigenschaften → Allgemein → Einstellungen

- Speichern: Pfad: H:
- Name: ausdruck-winxp (.pdf wird ergänzt)
- Dialog zeigen: Aus
- Ausführen: Aus
- Drucker entfernen: alle außer PDFX Lite9 (OneNote, Microsoft XPS, ...)

VM schrumpfen – Tipps und Tricks

Die virtuellen dynamischen Festplattendateien werden im Laufe des Betriebes immer größer, nie kleiner, auch wenn man Dateien löscht. Zum Verkleinern muss man vierschrittig vorgehen:

- Alles überflüssige in der VM löschen
- Unbenutzte Festplattenbereiche in der VM nullen
- Mit dem Tool VBoxManage die .vdi-Festplattendatei kompakter machen
- Die kompakte Festplattendatei als neuen base-Snapshot setzen

Windows XP kompakter machen

Vorgehensweise (am Beispiel einer virtuellen Maschine mit Namen „winxp“):

- Die leoclient-VM booten und sdelete und CCleaner in der VM installieren:
 - download → sdelete (Microsoft-Tool), kopieren nach C:\Windows
 - download → CCleaner von heise.de
- Auslagerungsdatei abschalten, reboot der VM und dann die versteckte Datei C:\pagefile.sys löschen
- CCleaner ausführen und alles Wesentliche löschen lassen
- Ggf. Defragmentieren von c: (Auswirkung unklar)
- In der Windows Eingabeaufforderung ausführen: `sdelete.exe -z c:` (dauert etwas)
- Auslagerungsdatei wieder anschalten, Herunterfahren der VM
- Als linuxadmin im Terminal ausführen und den Anweisungen folgen:

```
# sudo leoclient2-base-snapshot-renew
```

Der aktuelle Snapshot `Snapshots/{...}.vdi` wird dadurch zur Basisfestplatte `winxp.vdi` „gemerged“ und ist diese danach wieder sehr klein.

- Als linuxadmin im Terminal ausführen um die Basisfestplatte zu schrumpfen:

```
# sudo VBoxManage modifymedium --compact /var/virtual/winxp/winxp.vdi
```

- Nun Basis nochmals neu erstellen, um die kompaktere Festplatte zu zippen und nach `snapshot-store/` zu kopieren:

```
# sudo leoclient2-base-snapshot-renew
```

Linux-VM kompakter machen

Zuerst alles Überflüssige in der laufenden VM löschen, u.a. auch der apt-Cache. Die anschließend beste Vorgehensweise ist das Einbinden der .vdi-Festplatte in ein anderes System, z.B. in ein live-Linux-System, um das „Nullen“ durchzuführen:

- das Tool „zerofree“ nullt die unbenutzten Festplatteninhalte
- auch Swap-Partition nullen per dd-Befehl
- Schließlich die 3 Punkte wie oben bei WinXP durchführen.
 - leoclient2-base-snapshot-renew
 - vboxmanage modifymedium
 - leoclient2-base-snapshot-renew

Das Tool VBoxManage kann nur .vdi-Dateien schrumpfen. Dateien vom Typ .vmdk müssen zuerst in .vdi-Dateien umgewandelt werden und danach ge-shrunked werden:

```
# VBoxManage clonehd disk1.vmdk disk1.vdi --format vdi
# VBoxManage modifyhd --compact disk1.vdi
```

Virtuelle Maschine direkt starten

Das zusätzliche Skript leoclient2-directstart startet direkt ohne Dialog eine VM.

Vorgehensweise:

- Laden Sie das Skript herunter leoclient2-directstart
- Legen Sie das Skript unter /usr/bin ab und machen es ausführbar.

```
$ sudo mv leoclient2-directstart /usr/bin/
$ sudo chmod 755 /usr/bin/leoclient2-directstart
```

- Das Skript kann mit folgenden Parameter gestartet werden:

```
# /usr/bin/leoclient2-directstart -m <VM> [-s <Snapshot>] -r <RAM>

m: Name der lokalen VM, zwingend notwendig
s: Name des lokalen Snapshots, ohne wird "wie vorgefunden" verwendet
r: RAM in MB, zwingend notwendig
```

- Starten Sie das Skript

```
$ leoclient2-directstart -m winxp -r 1024 -s standard
```

Hinweis: Einschränkungen des Skriptes:

- Eine Datei network.conf wird von dem Skript nicht ausgewertet.
- Bei den Berechtigungen wird nur der Snapshot und die primäre Gruppe des Users überprüft.
- Bei Angabe ohne Snapshot, kann „wie vorgefunden“ nicht einen gespeicherten Zustand starten.

Zum bequemen Starten kann man einen Desktop-Starter anlegen, z.B. für die VM „winxp“ mit 1024 MB RAM und „standard“-Snapshot:

Quellcode 1: /usr/share/applications/leoclient2-directstart.desktop

```
[Desktop Entry]
Version=1.0
Type=Application
Name=VirtualBox Direktstart
Comment=Starting Snapshots of VirtualBox
Comment[de]=Starten von VirtualBox Snapshots
Exec=/usr/bin/leoclient2-directstart -m winxp -r 1024 -s standard
Icon=leovirtstarter2
Categories=Graphics;Engineering;
Categories=Emulator;System;Application;
Terminal=false
```

Netzwerkeinstellungen einer VM

Die Netzwerkkonfiguration der VM erfolgt durch eine Datei `network.conf`, die zusätzlich im Verzeichnis der VM angelegt werden muss. Fehlt diese Datei oder treten Fehler bei der Konfiguration auf, werden beim Snapshot-Start des `leovirtstarters2` immer alle Netzwerkkarten deaktiviert.

Möchte man eine Netzwerkkarte aktivieren, so muss im Maschinenverzeichnis der VM eine Datei `<MASCHINENPFAD>/network.conf` angelegt werden, die 5 Einträge in einer Zeile, durch Strichpunkt getrennt, enthält. Diese Konfiguration gilt dann für alle lokalen Snapshots dieser VM.

- hostname (Name des Linux-Clients auf dem VirtualBox installiert ist)
- vm-nic (1-4)
- mode (none|null|nat|bridged|intnet|hostonly|generic|natnetwork)
- macaddress
- devicename (eth0,eth1,...) oder (auto-unused-nic|auto-used-nic)

Z.B. `/var/virtual/winxp/network.conf`

```
# Beispiel einer NAT-Netzwerkkarte
r100-pclehrer;1;nat;080011223344;auto-used-nic
```

Folgendes typische Netzwezeinstellungen können bisher (Version 0.5.4-1, Juli 2015) umgesetzt werden:

- nat - NAT auf die NIC des pädagogischen Netzes (VM kann ins Internet)
- bridged + auto-used-nic - Bridge auf die Karte ins pädagogische Netz
- bridged + auto-unused-nic - Bridge auf eine zweite Karte (nicht ins pädagogische Netz verbunden -> unused)

Mit Hilfe des `hostname` kann man z.B. auf verschiedenen Clients verschiedene MAC-Adressen in der VM für den Bridged-Modus verwenden.

Es gibt insgesamt 4 Möglichkeiten eine `network.conf` -Datei abzulegen: zweimal lokal und zweimal im `SERVERDIR`. Für die Priorität der Möglichkeiten gilt folgende Reihenfolge:

- **Ist auf dem Server speziell für einen Snapshot der VM eine eigene**
Datei `<SERVERDIR>/<MACHINE_NAME>/snapshot-store/<SNAPSHOT>/network.conf` vorhanden, so wird diese benutzt.
- Danach wird die Datei auf dem Server für die VM `<SERVERDIR>/<MACHINE_NAME>/network.conf` ausgewertet (falls vorhanden).
- Anschließend wird die lokale Datei für den Snapshot der VM `<lokaler Maschinenpfad>/network.conf` ausgewertet (falls vorhanden).
- **Abschließend wird die lokale Datei für die VM `<lokaler Maschinenpfad>/snapshot-store/<SNAPSHOT>/network.conf` ausgewertet (falls vorhanden).**
- Ist keine Datei `network.conf` vorhanden, werden alle Netzwerkkarten für die VM deaktiviert.

Fehlersuche - Fehlerbehebung

Log-Datei `````` Am Client findet man unter `/tmp/leovirtstarter2.log` die aktuelle log-Datei des `leovirtstarters2` zur Fehlersuche.

Endlosschleife bei `leoclient2-base-snapshot-renew` ``````
Problem: Das Script `leoclient2-base-snapshot-renew` läuft in eine Endlosschleife, wenn im Verzeichnis `<lokaler Maschinenpfad>/Snapshots/` eine verweiste Snapshot-Datei übrig bleibt.

Lösung: Die verweiste Snapshot-Datei manuell löschen, dann `leoclient2-base-snapshot-renew` nochmals ausführen.

Snapshot passt nicht zur Basisfestplatte

Nach einem `leoclient2-base-snapshot-renew` werden bisherige Snapshots unbrauchbar und sollten auch nicht mehr verwendet werden. Der Snapshotname wird dabei auch geändert. In der Datei `<Maschinennamen>.vbox` wird der aktuell gültige Snapshotname `{...}.vdi` aufgeführt.

Problem: Unter `<Maschinenpfad>/Snapshots` liegt ein alter Snapshot, der Name passt nicht. VirtualBox startet deshalb nicht.

Lösung: Den Snapshot in `<Maschinenpfad>/Snapshots` manuell löschen und dann einen Snapshot mit dem aktuellen Namen aus `<Maschinenpfad>/snapshot-store/standard/` in das Verzeichnis `<Maschinenpfad>/Snapshots` kopieren.

network.conf für lokalen Snapshot bereitstellen

Problem: Aktuell wertet der `leovirtstarter2` eine `network.conf` im Verzeichnis des lokalen Snapshots nicht aus. (leoclient2-Version: 0.5.4-1)

Lösung: Wenn man jedoch eine `network.conf` im remote-Pfad des Snapshots ablegt, wird diese ausgewertet. Weitere Dateien müssen im remote-Pfad nicht vorhanden sein. Der remote-Pfad muss nicht zwingend remote liegen! Z.B. mit den voreingestellten Standard-Pfaden des Snapshots „physik“:

- lokaler Snapshot-Pfad: `/var/virtual/winxp1/snapshot-store/physik/...`
- ergibt `network.conf`-Pfad: `/media/leoclient2-vm/winxp1/snapshot-store/physik/network.conf`

leovirtstarter2 zeigt „wie vorgefunden“ nicht an

Problem: Im Auswahlmenü wird „wie vorgefunden“ nicht angezeigt oder kann nicht gestartet werden.

Ursache 1: Die VM wurde nicht ausgeschaltet sondern befindet sich in einem gespeicherten Zustand. Im Verzeichnis `.../Snapshots` befindet sich eine `*.sav`-Datei.

Lösung 1: Den „Standard“-Snapshot starten oder die Maschine direkt mit VirtualBox starten und dann herunterfahren.

Ursache 2: Im Verzeichnis `Maschinenpfad>/Snapshots/` befinden sich überflüssige Dateien.

Lösung 2: Alle Dateien löschen bis auf den aktuellen Snapshot: `{...}.vdi`. Der Name/die UUID des aktuellen Snapshots kann man (falls unklar) aus der `<Maschinenname>.vbox`-Datei ermitteln.

Hintergrundinformationen

Virtuelle Maschine erzeugen

Beim Anlegen einer virtuellen Maschine mit `leoclient2-init` wird der Pfad zur Maschine in `/etc/leoclient2/machines/MASCHINENNAME.conf` gespeichert.

Nach Beenden von Virtualbox werden folgende Aktionen vom Script ausgeführt:

- Ein Snapshot wird erzeugt (in `/PFAD/MASCHINENNAME/Snapshot/`) und dieser als Standard-Snapshot nach `PFAD/MASCHINENNAME/snapshot-store/standard/` gesichert.
- Außerdem werden die Konfigurationsdateien (`compreg.dat`, `VirtualBox.xml`, `xpti.dat` und `MASCHINENNAME.vbox`) gesichert nach `/PFAD/MASCHINENNAME/defaults/`.
- Abschließend werden alle Dateirechte für den Einsatz gesetzt (z.B. `/PFAD/MASCHINENNAME/MASCHINENNAME.vdi` nur lesbar, da diese Datei nicht verändert werden darf)

Jede VM ist vollständig in ihrem Maschinenverzeichnis gespeichert.

Serverbasierte VM kopieren, lokaler cache

Die auf dem Server liegenden gezippten Basisimages und Snapshots werden (falls lokal nicht vorhanden oder verändert) beim Start in den lokalen cache kopiert und dann lokal an die Stelle entpackt, wo sie genutzt werden. Der Cache hat eine maximale Größe, die in `SERVERDIR/caches.conf` definiert wird. Es empfiehlt sich dafür ein lokales Datenlaufwerk zu verwenden. Falls das nicht vorhanden ist, ein Verzeichnis auf der Partition mit den virtuellen Maschinen.

Virtuelle Maschine starten

VirtualBox startet mit der Umgebungsvariablen `VBOX_USER_HOME` (`$ export VBOX_USER_HOME=/PFAD/MASCHINENNAME`) und mit der Einstellung für den Standardort für die VM für Virtualbox (`$ VBoxManage setproperty machinefolder /PFAD/MASCHINENNAME`). Mit diesen Anpassungen und anschließendem Starten von Virtualbox (`$ VirtualBox`) kann eine VM auch von Hand gestartet werden.

Damit `leovirtstarter2` eine lokale Maschine findet, muss in `/etc/leoclient2/machines/MASCHINENNAME.conf` ihr Pfad eingetragen sein. (`leoclient2-init` erzeugt diese Datei automatisch). Der Standard-Pfad für die lokalen VM ist dabei `/var/virtual/`.

Außer den lokal vorhandenen Maschinen wird auch in allen in `SERVERDIR` konfigurierten Pfaden nach Maschinen gesucht. (Der Pfad MUSS NICHT remote liegen, allerdings geht `leovirtstarter2` davon aus und holt diese Maschinen in gezippter Form (Netzwerk-Bandbreitenschonend) zu den lokalen Maschinen und startet Sie dort). Der Standard-Pfad für die remote VM ist dabei `/media/leoclient2-vm`.

Auflisten kann man alle sichtbaren VM's mit:

```
$ leovirtstarter2 -i
$ leovirtstarter2 --info
```

Wird mit dem leovirtstarter2 ein Snapshot einer VM zum Starten ausgewählt, wird folgendes abgearbeitet:

- Kopieren der Standard-Konfigurationsdateien aus /PFAD/MASCHINENNAME/defaults/ nach /PFAD/MASCHINENNAME/
- Anpassen folgender Angaben:
 - Shared Folder verbinden ins Heimatverzeichnis des angemeldeten Benutzers
 - Netzwerkeinstellungen (verschiedene Möglichkeiten stehen zur Verfügung)
- Starten der Maschine

Gibt es die Maschine auch Remote, können zusätzlich folgende Dinge erfolgen:

- Snapshots wird gegebenenfalls vom Server in den lokalen Cache kopiert.
- Reparatur des Basisimages, falls notwendig
- Update der lokalen VM durch die Remote-VM, falls verschieden.
- Der Snapshot wird aus dem Cache bzw. aus /PFAD/MASCHINENNAME/snapshot-store/default/ nach /PFAD/MASCHINENNAME/Snapshots/{...}.vdi entzippt

Berechtigungen zum Starten einer VM bzw. eines Snapshots

An welchen Rechnern (Hosts) welcher User eine VM starten darf wird in /PFAD/MASCHINENNAME/image.conf konfiguriert.

Es werden USER, GROUP, HOST, ROOM gelistet, die Zugriff erhalten sollen (Positivliste). Wenn nichts konfiguriert wird, haben alle User von allen Hosts Zugriff. Es gibt 2 Arten des Zugriffs:

USER-LEVEL Zugriff:

Zeile mit user=user1,user2 für den Zugriff eines Users Zeile mit group=group1,group2 für den Zugriff eines in der primären/sekundären Gruppe group1,group2 befindlichen Users (z.B. teachers)

HOST-LEVEL Zugriff:

Zeile mit host=host1,host2 für den Zugriff eines Hosts Zeile mit room=raum1,raum2 für den Zugriff eines in der primären Gruppe raum1,raum2 befindlichen Hosts

Um eine Maschine starten zu können, müssen BEIDE Level erfüllt sein (logische UND-Verknüpfung): Der User muss auf die VM zugreifen dürfen UND der Host muss die VM starten dürfen. Die Dateirechte der VM- bzw. Snapshot-Verzeichnisse müssen so eingestellt sein (z.B. Zugriff für alle), das die Konfigurierten USER, GROUP, HOST, ROOM Zugriff auf die VM/den Snapshot besitzen.

Beispieldatei image.conf

```
# Berechtigungen eine VM zu starten.
group=teachers
host=
room=lehrerzimmer
```

Hinweis: Die Berechtigung für einen einzelnen Snapshot wird nur dann korrekt ausgewertet, wenn beim HOST-LEVEL beide Optionen host und room auftauchen. Fehlt z.B. die „room“-Option ist jeder Raum und damit auch jeder Host zugelassen!

Stand Version 0.5.4-1 Juli 2015: Die Gruppen- und User-Beschränkung auf VM-Ebene wird z.Z. nicht korrekt ausgelesen → ‚group‘ und ‚user‘ damit ohne Funktion

Datenstruktur einer VM

Virtualbox-Dateien

In der obersten Verzeichnisebene im Verzeichnis der VM verwaltet VirtualBox die aktuell verwendete Maschine:

- Die Basisdatei ist `MASCHINENAME.vdi`, sie enthält den Basis-Zustand der Festplatte und ist meist mehrere GB groß
- Konfigurationsdateien
- Logdateien
- usw. ...
- Im Unterverzeichnis `Snapshots` verwaltet VirtualBox den aktuell verwendeten Snapshot `{*}.vdi`.

leoclient2-Dateien

- `MASCHINENAME.conf` beinhaltet den Pfad in dem die VM erstellt wurde. Dorthin wird sie im Fall einer remoten Maschine auch wieder entpackt (funktioniert nur in diesem Pfad)
- `network.conf` ist optional. Konfiguriert die Netzwerkkarten der Virtuellen Maschine (falls keine `network.conf` speziell für den Snapshot existiert)
- `image.conf` ist optional.
- Das Unterverzeichnis `snapshot-store` enthält in Unterverzeichnissen weitere Snapshots. (Bei einer lokalen VM ist meist nur das Verzeichnis `standard` vorhanden):
- `{*}.vdi` ist die Snapshot-Datei.
- `{*}.vdi.zip` ist die gezippte Snapshot-Datei (nur etwa 1/3 so groß wie `{*}.vdi`).
- `filesize.vdi` ist eine Textdatei und enthält die Größe von `{*}.vdi`.
- `filesize.vdi.zipped` ist eine Textdatei und enthält die Größe von `{*}.vdi.zip`.
- `network.conf` ist optional. Konfiguriert die Netzwerkkarten für diesen Snapshot.
- Das Unterverzeichnis `defaults` enthält ein Backup der Konfigurationsdateien. Vor dem Start der Maschine kann mit diesen Dateien die Maschine zurückgesetzt werden (Kopieren auf eine Verzeichnisebene höher).

Übersicht der Skripte/Befehle zum leoclient2

leoclient2-init:

legt eine neue lokale VM an

leovirtstarter2

startet das grafische Auswahl Fenster und anschließend die VM mit Optionen

```
--info      listet alle VMs auf der Konsole auf
--vbox      startet das grafische Auswahl Fenster und VirtualBox ohne die VM zu
↳ starten
-h          Hilfe anzeigen
--local-snapshots  nur lokale Snapshots listen
--ignore-virtualbox  startet den leovirtstarter auch wenn gerade VirtualBox
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
↪ausgeführt wird  
--serverdir <abs path> verwendet anderen Pfad statt SERVERDIR zu den remote VMs
```

leoclient2-base-snapshot-renew

Erstellt eine neue Basisfestplatte mit dem aktuellen Snapshot der zur bisherigen Basisfestplatte ge-„merged“ wird. Der „Aktuelle Zustand“ wird somit gesichert/festgeschrieben.

leoclient2-vm-move

Importiert eine VM (z.B. vom externen Speichermedium) oder verschiebt ein VM

VBoxManage

mit vielen Optionen Konsolen-Tool zum Bearbeiten von VMs

Entwicklungsdokumentation des leoclient2

siehe <http://www.linuxmuster.net/wiki/entwicklung:linuxclient:leoclient2>

4.20 Ändern des eigenen Passwortes

Autor des Abschnitts: @Tobias,

Melde Dich an der Schulkonsole an, d.h. besuche mit dem Browser die Webseite <https://server.linuxmuster.net> oder die an Deiner Schule äquivalent vom Administrator eingerichtete Seite und melde Dich mit den Schulkontodaten an.

Hinweis: Dein Benutzername besteht nur aus Kleinbuchstaben und eventuell Zahlen.

linuXmuster.net



max



Anmelden

Klicke auf der Hauptseite auf „Passwort ändern“

The screenshot shows the Linuxmuster.net web interface. The top navigation bar includes the logo, 'Hauptseite', a server URL, and a user profile icon. The left sidebar has a menu with 'ALLGEMEIN' (containing 'Hauptseite') and 'KLASSENZIMMER' (containing 'Unterricht', 'Einschreiben', and 'Passwörter drucken'). The main content area displays a welcome message for 'Max Mustermann' and a 'Konto Informationen' box. This box lists user details: Name (Max, Mustermann), E-Mail (max@humboldt-ka.de), Schule (default-school), and Rolle (teachers). A 'Passwort ändern' button is located at the bottom right of this box. Below the account information is a 'Quotas' section.

Gib das aktuelle und zweimal ein neues Passwort ein. Beachte die Anforderungen an das neue Passwort, die von Schule zu Schule abweichen können. Informiere dafür Dich bei deinem Netzwerkberater. Standardmäßig gibt es folgende Regeln

- Folgende Zeichen sind erlaubt:

a-z A-Z 0-9 ! § + - @ # \$ % & * () [] { }

(D.h. Umlaute oder diakritische Zeichen sind nicht erlaubt)

- Die Mindestlänge des Passwortes sind 7 Zeichen.
- Das Passwort muss aus Großbuchstaben, Kleinbuchstaben und entweder Zahlen oder Sonderzeichen (oder beidem) bestehen.

Beispiele sind: Muster! oder HundKatzeMau5



Das erfolgreiche Ändern des Passwortes wird mit einer Meldung bestätigt.

Falls die Änderung nicht erfolgreich war, erhalten Sie eine Fehlermeldung mit einem Hinweis auf den Fehler.

In dieser Beispielfehlermeldung bestand das Passwort nur aus Kleinbuchstaben, Zahlen und Sonderzeichen. Es enthielt keine Großbuchstaben.

Jetzt kannst Du Dich ausloggen. Rechts oben, wo in einem Kreis dein Bild oder Buchstabe steht erreicht man das persönliche Menü.

Mit dem neuen Passwort kannst Du Dich an allen Diensten anmelden, die im Schulnetzwerk mit dem Schulkonto verbunden sind, z.B. auch die Anmeldung an PCs.


Passwort ändern
server.linuxmuster.humboldt-gymnasium.ka.schule-bw.de
✓ Passwort geändert


ALLGEMEIN
[Hauptseite](#)
KLASSENZIMMER
[Unterricht](#)
[Einschreiben](#)
[Passwörter drucken](#)


! Minimale Passwortlänge ist 7 Zeichen. Verwenden Sie Großbuchstaben, Kleinbuchstaben und Sonderzeichen oder Zahlen. (z.B. Muster!)

Valid characters are: a-z A-Z 0-9 !\$+~@#\$%&*()'[]{}


Aktuelles Passwort

Neues Passwort


Passwort wiederholen


linuxmuster.humboldt-gymnasium.ka.schule-bw.de
! Passwort ist zu schwach



Großbuchstaben, Kleinbuchstaben und Sonderzeichen

linuxmuster.humboldt-gymnasium.ka.schule-bw.de


net 7!

 max UID 0

 Change password

 Ausloggen

u navigieren. Sie könnten damit beginnen, sich mit Hilfe des

4.21 Schülerverwaltung als Lehrer

Autor des Abschnitts: @Tobias,

Als Lehrer hat man in der Schulkonsole mehrere pädagogische und verwaltungstechnische Funktionen zur Verfügung.

Melde Dich an der Schulkonsole an, d.h. besuche mit dem Browser die Webseite <https://server.linuxmuster.net> oder die an Deiner Schule äquivalent vom Administrator eingerichtete Seite und melde Dich mit den Schulkontodaten an.

4.21.1 Klassen, Projekte, Kurse - Einführung

In der linuxmuster.net v7 gibt es zwei Kategorien von Gruppierungen. Klassen und Projekte sind Gruppierungen,

- denen Schüler automatisch angehören (Klassen) oder denen sie angehören durch Anlegen eines Lehrers (Projekte)
- die einen Tauschordner besitzen
- über die eine Zuordnung auch außerhalb der Imn7 möglich ist (z.B. Nextcloud, Moodle)

Kurse dagegen sind Gruppierungen,

- die jeder Lehrer selbst anlegt
- die für Unterrichtsfunktionen wie Teilen/Einsammeln/Klassenarbeit verwendet werden
- die zum Zurücksetzen der Passwörter durch Lehrer verwendet werden

Es werden meist beide Kategorien für den täglichen Umgang benötigt.

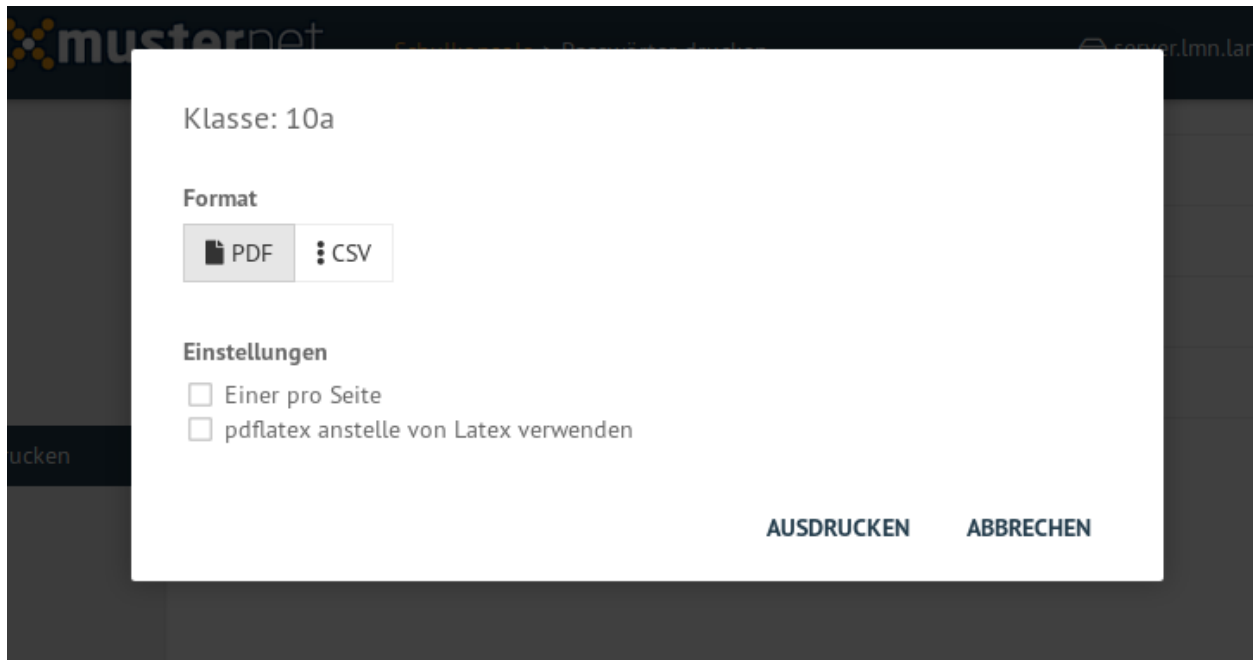


Solange ein Lehrer nur den automatisch angelegten Tauschordner der Klasse verwenden will, muss er keine Kurse einrichten. Die Konfiguration findet sich unter *KLASSENZIMMER/Einschreiben*.

Sobald ein Lehrer die Unterrichtsfunktionen verwenden will, die über einen Tauschordner hinausgehen, muss er einen Kurs anlegen und die gewünschten Schüler hinzufügen. Die Konfiguration findet sich unter *KLASSENZIMMER/Unterricht*.

4.21.2 Passwörter der Schüler ausdrucken

Für ein klassenweises Ausdrucken der Erstpasswörter gibt es einen zusätzlichen Menüpunkt in der Schulkonsole. Unter dem Menüpunkt *KLASSENZIMMER/Passwörter drucken* wähle aus der Liste aller Klassen die entsprechende aus.



Das resultierende PDF enthält Benutzername und Erstpasswort aller Schülerinnen und Schüler der Klasse und kann so ausgeteilt werden.

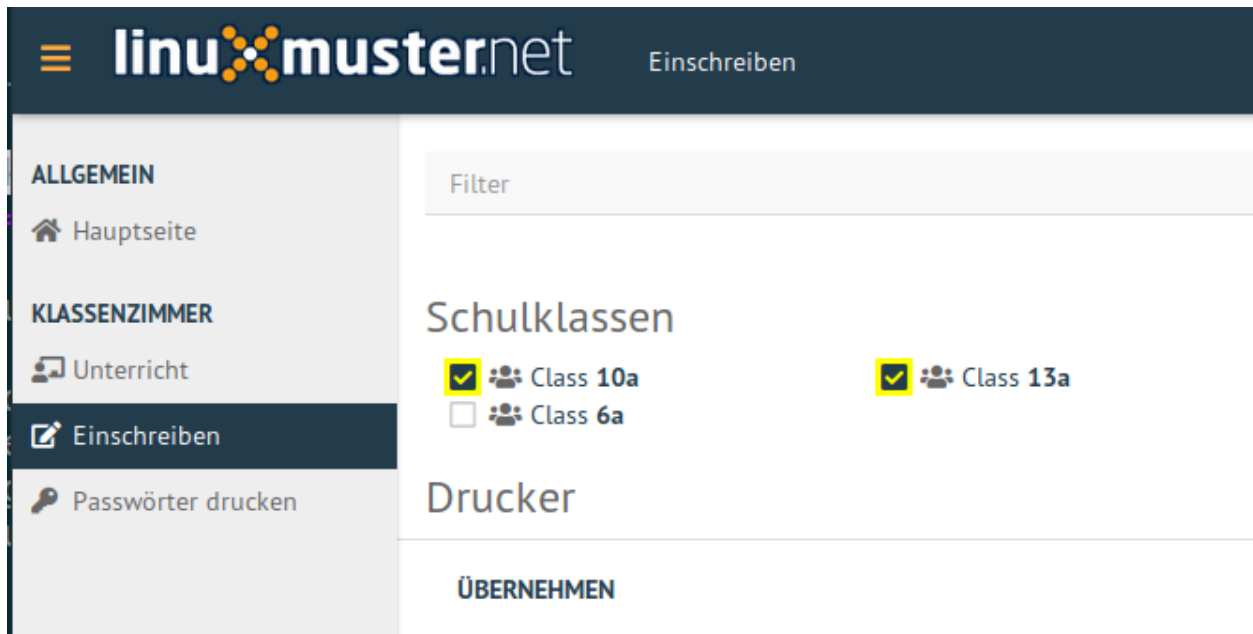
Zugangsdatenliste		10a
Fray, Katrin Klasse: 10a Passwort: g7Htvf\$9 Login: frayka	Gengler, Felix Klasse: 10a Passwort: S&2FeFys Login: genglefe	
Krüger, Richard Klasse: 10a Passwort: U(F3fZdc Login: kruegeri		

4.21.3 In Klassen einschreiben und Projekte anlegen

Die folgende Anleitung brauchst Du dann, wenn Du mit einer gesamten Schulklasse oder einem Teilnehmer einer Teilgruppe von Schülern Dateien über einen gemeinsamen Ordner bearbeiten willst oder diese Gruppierung in einer externen Anwendung gemeinsam ansprechen willst (z.B. Nextcloudgruppe oder Moodlegruppe). Für alle Unterrichtsfunktionen benötigst Du dagegen einen Kurs, siehe nächsten Abschnitt.

In Klassen einschreiben

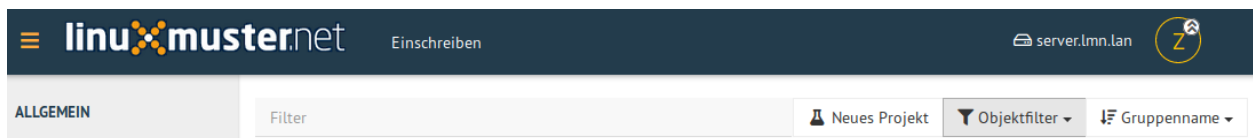
Unter KLASSENZIMMER/Einschreiben klicke auf die Klasse, der du angehören willst. Die Veränderung wird gelb hinterlegt angezeigt. Bestätige alle Änderungen mit ÜBERNEHMEN, das sich am unteren Ende der Seite befindet.



Das Austragen aus einer Klasse funktioniert analog mit Entfernen des Hakens und Übernehmen der Änderung.

Projekte erstellen und beitreten

Unter KLASSENZIMMER/Einschreiben klicke in der oberen Leiste auf Neues Projekt.



In dem sich öffnenden Eingabefeld kann der Projektname mit kleinen Buchstaben (a-z, keine Umlaute oder Sonderzeichen) und Zahlen (0-9) festgelegt werden. Die Schulkonsole meldet zurück, wenn das Projekt erfolgreich erstellt wurde und es erscheint in der Liste der Projekte.

fixme

Rest der Erstellung der Projekte

Projektname

kraeuterkunde12|

OK

ABBRECHEN

4.21.4 Unterrichtskurs einrichten

Die folgende Anleitung brauchst Du für alle Unterrichtsfunktionen (außer dem Tauschordner) und dafür musst Du nicht in der Klasse eingeschrieben sein.

Unter **KLASSENZIMMER/Unterricht** klicke auf **Neuer Kurs** und gib dem Kurs einen Namen. Im Kurs können sowohl Schülerinnen und Schüler einer Klasse als auch verschiedener Klassen zusammengestellt werden. Der Kurs ist auch nur für Dich sichtbar und verwendbar.

Der Kurs taucht nun in der Auflistung mittig auf. Klicke ihn an, er ist zunächst leer. In der ersten Zeile kannst Du nun bei *Schüler hinzufügen* einzelne Schülernamen eingeben oder bei *Klasse hinzufügen* Klassennamen eingeben.

Die Schulkonsole beschränkt während der Eingabe die möglichen Benutzer oder Gruppen des Systems und zeigt sie an. Klicke auf die angebotene Gruppe (z.B. hier: *10a*) um die entsprechenden Benutzer hinzuzufügen.

Die Schüler werden nun aufgelistet und können bei Bedarf über das Symbol des Mülleimers einzeln aus der Liste wieder entfernt werden.

Ist die Liste vollständig klicke unten rechts auf **SPEICHERN & ÜBERNEHMEN**.

Rechts oben wird das erfolgreiche Speichern mit einem grünen Haken zurückgemeldet.

Der Kurs kann später an dieser Stelle auch umbenannt oder gelöscht werden.

Folgende Unterrichtsfunktionen können jetzt genutzt werden:

- *Prüfungsmodus*

Add Student

Add Class

Lastname

Kurs bearbeiten

Kurse

10a_Jungs2019-10-04_13-06-18

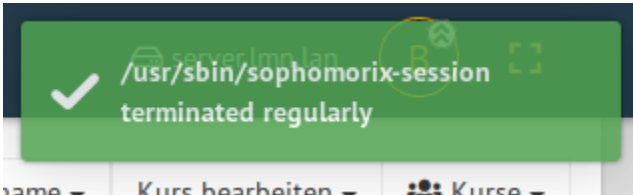
Userdata	Transfer	Exam-Supervisor						
Gengler, Felix 10a, genglefe	TeilenEinsammeln	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Ilkes, Judith 10a, ilkesju	TeilenEinsammeln	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Krüger, Richard 10a, kruegeri	TeilenEinsammeln	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

TEILEN

EINSAMMELN

SCHLIESSEN

SPEICHERN & ÜBERNEHMEN

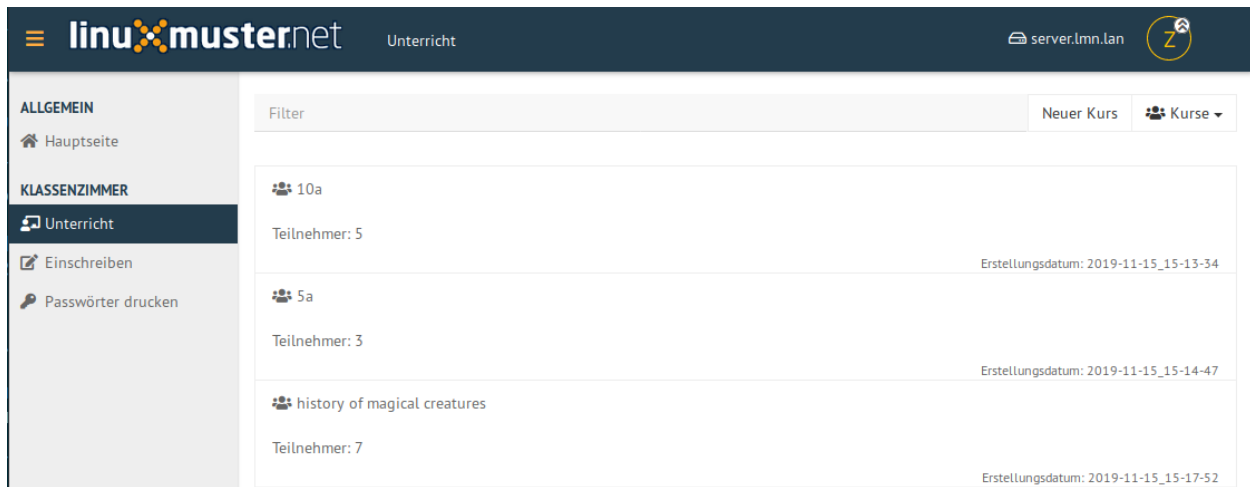


- *Zugriff auf WLAN, Internet und Drucker regeln*

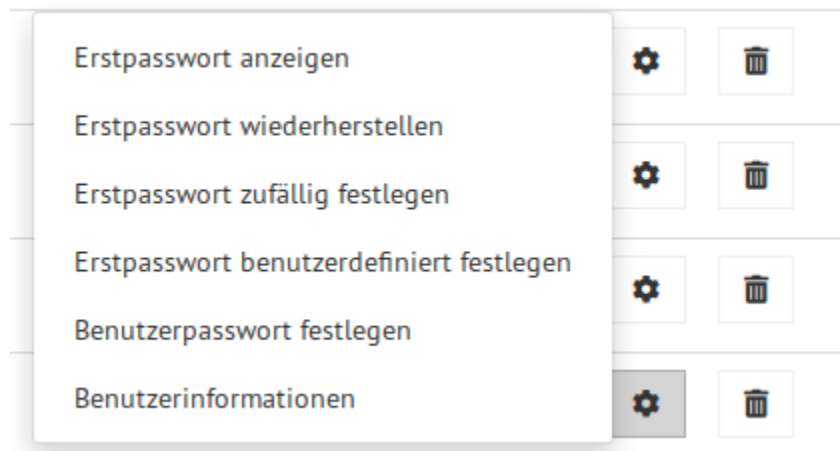
Passwörter zurücksetzen

Vergisst ein Schüler sein Passwort, kann jede Lehrkraft das Passwort des Schülers über die Schulkonsole auf das Erstpasswort zurücksetzen und dies dem Schüler mitteilen. Voraussetzung für die Passwortänderung ist die Aufnahme des Schülers in einen Kurs.

Öffne in der Schulkonsole unter **KLASSENZIMMER/Unterricht** den angelegten Kurs.



Die Liste mit Schülern des Kurses wird angezeigt. Klickst Du auf das Zahnradsymbol in der Zeile des Schülers im Kurs, erscheinen die Möglichkeiten



Wichtig: Das **Erstpasswort** ist ein Passwort, dass beim Anlegen des Schülers durch den Administrator oder durch eine Lehrperson in der Schulkonsole gesetzt wurde. Das Erstpasswort wird auch im Klartext gespeichert und ist daher nicht für die dauerhafte Verwendung geeignet. Die Schüler müssen es selbst ändern.

Das **Benutzerpasswort** also das geheime vom Schüler geänderte Passwort kann weder von Lehrer noch Administrator eingesehen werden. Diese Passwörter werden grundsätzlich nur verschlüsselt gespeichert.

Klicke auf

Erstpasswort anzeigen

um das aktuelle Erstpasswort anzuzeigen

Erstpasswort wiederherstellen

um das Passwort des Schülers (wieder) auf das Erstpasswort zurückzusetzen

Erstpasswort zufällig festlegen

um dem Schüler ein zufälliges neues Erstpasswort zu erzeugen und zu setzen

Erstpasswort benutzerdefiniert festlegen

um dem Schüler ein selbstgewähltes neues Erstpasswort zu erzeugen und zu setzen. Der folgende Dialog enthält einen Hinweis auf die Komplexitätsregeln des Passworts.

Benutzerpasswort festlegen

um direkt das Passwort des Schülers festzulegen. Das Erstpasswort wird dabei nicht geändert. Diese Option bietet sich an, wenn der Schüler selbst hier sein geheimes Passwort eingeben kann. Der folgende Dialog enthält einen Hinweis auf die Komplexitätsregeln des Passworts.

Nach Setzen des Erst- oder Benutzerpasswortes muss *nicht* mit *SPEICHERN & ÜBERNEHMEN* abgeschlossen werden.

4.22 Benutzer verwalten mit der Schulkonsole

Autor des Abschnitts: @cweikl

In dieser Dokumentation erhalten Sie einen Überblick über den workflow zur Benutzerverwaltung in der aktuellen linuxmuster.net. Neben den Möglichkeiten zur Konfiguration der Benutzereinstellungen, über das Einlesen der Benutzer via CSV-Datei und die Änderung einzelner Nutzer werden die wichtigsten Tätigkeiten zur Benutzerverwaltung erläutert.

Die Benutzerverwaltung in der aktuellen linuxmuster.net Version erfolgt auf dem Server mithilfe von sophomorix4. Sophomorix stellt eine Vielzahl an Befehlen und einen speziellen Workflow bereit, arbeitet aber vollständig konsolenorientiert. Es können somit alle Befehle zur Benutzerverwaltung auch auf der CLI am Server direkt abgesetzt werden. Siehe hierzu die Hinweise im letzten Unterkapitel dieses Abschnitts.

Um eine grafisch unterstützte, einfache und bequeme Möglichkeit zur Benutzerverwaltung bereitzustellen, verfügt linuxmuster.net über die sog. Schulkonsole, einem grafischen Hilfsmittel, das im Browser aufgerufen wird. Die Schulkonsole führt die Vielzahl an pädagogischen Funktionen und Funktionen zur Verwaltung und zum Betrieb des Schulungsnetzes unter einer einfach zu nutzenden, grafischen Oberfläche zusammen.

In der Schulkonsole (WebUI) werden grundlegende Einstellungen vorgenommen, die für die Benutzerverwaltung relevant sind, wie z.B. die Mindestanzahl an Zeichen für Nach- und Vorname. Zudem werden hier die Benutzerlisten gepflegt, geprüft sowie Benutzer angelegt, versetzt und gelöscht. Die Passwörter und der Plattenplatz (Quotas) werden hier für alle Benutzer, Klassen und Gruppen verwaltet.

Grundsätzlich nimmt der Benutzer `global-admin` die Einstellungen für die Benutzerverwaltung vor. Benutzer mit Lehrer-Rechten können danach Passwörter für Schüler und Schülerinnen sowie Projekte verwalten.

4.22.1 Workflow zur Benutzerverwaltung

Autor des Abschnitts: @cweikl

Die Benutzerverwaltung erfolgt in der aktuellen linuxmuster.net Version mithilfe der Schulkonsole. Diese wiederum greift auf dem Server auf die Benutzerverwaltung *sophomorix4* zu, die konsolenorientiert das Benutzermanagement mithilfe von geeigneten Befehlen durchführt. Das Zusammenspiel folgt einem ausgearbeiteten Workflow. Dieser kann unter nachstehendem Link mit allen Details nachvollzogen werden: <https://github.com/linuxmuster/sophomorix4/wiki/Workflows>

Nachfolgend beschränken sich die Ausführungen auf die Grundlagen, die zum Verständnis und Durchführung der Benutzerverwaltung mithilfe der Schulkonsole erforderlich sind.

Der Ablauf zur Einrichtung von Benutzern verläuft wie folgt:

- 1) Hochladen einer CSV-Datei mit den Benutzern via Schulkonsole.
- 2) Speichern & prüfen der CSV-Datei.
- 3) Die Schulkonsole legt eine temporäre CSV-Datei an, die dann anhand von Kriterien geprüft wird.
- 4) Verläuft der Prüfungsvorgang erfolgreich, so werden die Benutzer übernommen und es wird eine CSV-Datei geschrieben, die danach in der Schulkonsole im Editor aufgerufen und geändert werden kann. Schritte 2 - 4 sind nach den Änderungen erneut auszuführen.

4.22.2 Benutzergruppen in der linuxmuster.net

Autor des Abschnitts: @cweikl

Wenn man auf Dienste und Dateien des Servers zugreifen möchte, muss man sich mit einem Benutzernamen (Loginname) und einem Kennwort (Passwort) am Server anmelden (authentifizieren). Dabei sollen nicht alle Benutzer am System auf die gleichen Dateien und Drucker zugreifen oder an Dateien die selben Rechte haben können.

Es ist üblich, Benutzer, die gleiche Rechte haben sollen, zu Benutzergruppen zusammenzufassen. In der *linuxmuster.net* gibt es, angepasst auf Schulbedürfnisse, die folgenden Hauptbenutzergruppen (Schulkonsole):

Schüler: Schüler sind Benutzer mit (halb)privatem Datenbereich. Es dürfen keinerlei Systemdateien modifiziert werden.

Lehrer: Lehrer sind Benutzer mit privatem Datenbereich. Es dürfen keine Systemdateien modifiziert werden. Zusätzlich hat der Lehrer Zugriff auf alle Klassentauschverzeichnisse und lesenden Zugriff auf die Schüler-Homeverzeichnisse. Alle Lehrer können über die Schulkonsole pädagogisch notwendige Aufgaben auf dem Server ausführen (z. B. Dateien austeilen, Internetzugang abschalten)

Schul-Administratoren: Dürfen alle für den reinen Schulbetrieb wichtigen Aufgaben am Server durchführen. Diese Gruppe ist dann relevant, wenn ein Mehr-Schulbetrieb erfolgt, da es dann pro Schule einen oder mehrere Administratoren gibt, die Vorgaben bzw. administrative Aufgaben getrennt nach Schule wahrnehmen.

Globale Administratoren: Dürfen ohne Einschränkungen alle Aufgaben am Server via Schulkonsole durchführen. Erfolgt kein Mehr-Schulbetrieb, so ist dies der eigentliche Administrator, der alle Einstellungen und administrative Tätigkeiten durchführt.

4.22.3 Konfigurationseinstellungen vor der Benutzeraufnahme

Autor des Abschnitts: @cweikl

Nach Installation des Servers solltest Du einige Konfigurationseinstellungen für Deine Schule festlegen.

Melde Dich an der *Schulkonsole* durch Eingabe von <https://10.0.0.1> in einen Browser als `global-admin` an.



4.22.4 Listenimport

Die für das Benutzermanagement relevanten Einstellungen können in der *Schulkonsole* im Menü unter *Einstellungen* -> *Schuleinstellungen* vorgenommen werden.

BENUTZERVERWALTUNG

Schüler

Lehrer

Schul-Administratoren

Globale Administratoren

Listenverwaltung

GERÄTEVERWALTUNG

Geräte

LINBO

KLASSENZIMMER

Einschreiben

Passwörter drucken

EINSTELLUNGEN

Extraquota

Schuleinstellungen

Globale Einstellungen

Benutzername und Passwörter

Nachname und Vorname im Benutzernamen umkehren

☐

Nachname Zeichen

Schüler

6

Vornamen Zeichen

Schüler

2

Passwortlänge

Schüler

10

Zufallspasswort

Schüler

☒

Tage bis zum Deaktivieren nach Austreten

Schüler

30

Tage bis zum endgültigen Löschen

Schüler

60

Ersetze Schrägstrich(/) in Klassenname durch Bindestrich(-)

☐

Lehrer

Nachname und Vorname im Benutzernamen umkehren

☐

Nachname Zeichen

Lehrer

0

Vornamen Zeichen

Lehrer

0

Passwortlänge

Lehrer

12

Zufallspasswort

Lehrer

☒

Tage bis zum Deaktivieren nach Austreten

Lehrer

60

Tage bis zum endgültigen Löschen

Lehrer

90

Extraschüler

Nachname und Vorname im Benutzernamen umkehren

☐

Nachname Zeichen

Extraschüler

6

Vornamen Zeichen

Extraschüler

2

Passwortlänge

Extraschüler

10

Zufallspasswort

Extraschüler

☒

Tage bis zum Deaktivieren nach Austreten

Extraschüler

40

Tage bis zum endgültigen Löschen

Extraschüler

80

Zeichenkodierung

students.csv Kodierung

auto

teachers.csv Kodierung

auto

extrastudents.csv Kodierung

auto

Erkannter Zeichensatz

students.csv Kodierung

UTF8

teachers.csv Kodierung

UTF8

extrastudents.csv Kodierung

UTF8

SPEICHERN

Hier legst Du fest, welche Vorgaben für den Listenimport von Benutzern mithilfe von CSV-Dateien angewendet werden sollen.

Für Schüler, Lehrer und Extra-Schüler können die Vorgaben getrennt eingestellt werden. So können die Mindestanzahl an Zeichen für den Nachnamen, Vornamen und das Passwort vorgegeben werden.

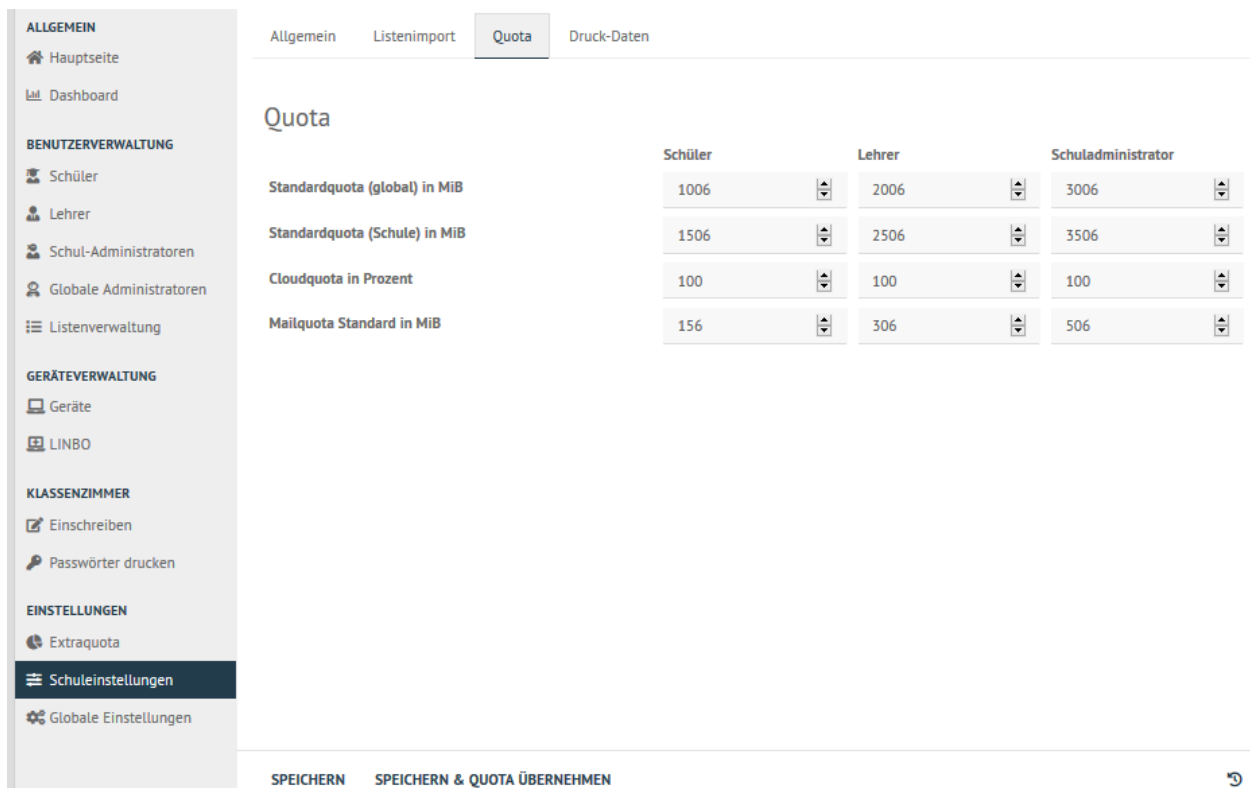
Es kann festgelegt werden, ob beim Import ein Zufallskennwort pro Benutzer erstellt wird, oder ob ein Kennwort später in der Schulkonsole gesetzt wird. Zudem wird hier festgeschrieben, wie mit Benutzern verfahren wird, die gelöscht werden sollen. Es wird hier mit einem Duldungszeitraum gearbeitet, so dass für eine Übergangszeit diese Benutzer noch in dem System in gesonderten Gruppen geführt und falls notwendig auch wieder reaktiviert werden können.

Zudem kann hier die Listenkodierung für die drei CSV-Dateien festgelegt werden, die genutzt werden, um die Benutzer Schüler, Lehrer und Extra-Schüler aufzunehmen. Mit der Einstellung `auto` ist es möglich, dass die Schulkonsole das Kodierung (*encoding*) der Datei ermittelt und entsprechend anwendet. Eine Änderung der Voreinstellung ist nur in besonderen Fällen erforderlich.

4.22.5 Quota

In der Schulkonsole können im Menü **Einstellungen** -> **Schuleinstellungen** -> **Quota** Vorgaben zur zulässigen Festplattenbelegung getrennt nach den Gruppen Schüler, Lehrer und Extra-Schüler vorgenommen werden. Hierdurch wird definiert, bis zu welcher Obergrenze ein Benutzer der jeweiligen Gruppen Dateien auf dem Server ablegen darf. Sollte diese Obergrenze erreicht werden, so werden weitere Speichervorgänge des Benutzers verhindert. Erst nachdem dieser Dateien und Verzeichnisse gelöscht hat, kann dieser weiter Daten auf dem Server ablegen.

Zur Ermittlung des belegten Speicherplatzes werden alle Dateien des Benutzers über alle sog. Partitionen hinweg gezählt. Dies bedeutet, dass der belegte Speicherplatz aller Dateien des Benutzers im Verzeichnis der Klasse oder Schule als auch Dateien in seinem eigenen Home-Laufwerk, das ebenfalls auf dem Server liegt, ermittelt wird.



	Schüler	Lehrer	Schuladministrator
Standardquota (global) in MiB	1006	2006	3006
Standardquota (Schule) in MiB	1506	2506	3506
Cloudquota in Prozent	100	100	100
Mailquota Standard in MiB	156	306	506

Buttons: **SPEICHERN** **SPEICHERN & QUOTA ÜBERNEHMEN**

Werden die Quota-Einstellungen geändert, so sind diese mit **Speichern & Quota übernehmen** anzuwenden.

4.22.6 Druck-Daten

Für Klassen können PDF-Drucker erstellt werden, um den Schülerinnen und Schülern Login-Karteikarten ausgeben zu können. Um festzulegen, welche Rahmendaten der Schule mitgedruckt werden sollen, können diese im Menü **Einstellungen -> Schuleinstellungen -> Druck-Daten** gesetzt werden.

Die Anpassungen sind mit **Speichern** zu übernehmen.

4.22.7 Anlegen, Versetzen und Löschen von Benutzern

Autor des Abschnitts: @cweikl

Normalerweise werden an einem Linux-Server die Benutzer durch Aufruf eines Programms angelegt, dem man den Benutzernamen des anzulegenden Benutzers und die Gruppe mitteilt, in welche der Benutzer zugeordnet werden soll.

Für eine Schule ist dieses Vorgehen nicht praktikabel, da meist mehrere hundert bis einige tausend Schüler als Benutzer angelegt werden müssen. Deshalb übernimmt bei der *linuxmuster.net* das Programm *sophomorix4* diese Aufgabe.

Sophomorix4 liest alle Schüler aus Text-Dateien ein, die aus dem Schulverwaltungsprogramm der Schule bezogen oder von Hand mit Hilfe eines Editors erstellt wurden. Anschließend werden alle Schüler dieser Liste, die im System noch nicht vorhanden sind, *angelegt*, solche mit einer neuen Klasse *versetzt* und nicht mehr aufgeführte Schüler im System *gelöscht*.

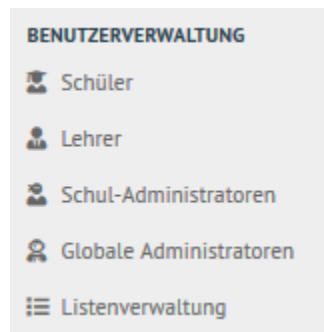
Mit der *Schulkonsole* gibt es für den Netzwerkbetreuer ein webbasiertes Werkzeug, das ihm die Bedienung von *sophomorix4* sehr erleichtert. Die einzelnen Schritte werden im Folgenden erläutert. Der Netzwerkbetreuer muss nur noch in Ausnahmefällen mit der Kommandozeile arbeiten.

Um Benutzer neu aufzunehmen, zu versetzen oder zu löschen müssen die folgenden Schritte nacheinander ausgeführt werden:

- 1) Schüler und Lehrerliste aus dem Schulverwaltungsprogramm exportieren.
- 2) Die Benutzerlisten auf dem Server aktualisieren. Dazu gehört im Einzelnen:
 - a) die Listen getrennt nach Schülern und Lehrern in das System übertragen,
 - b) evtl. eine Extraliste für Gast- und Kooperationsschüler, die nicht in das Schulverwaltungsprogramm aufgenommen werden, pflegen,
 - c) evtl. eine Extraliste für Kurse mit schulfremden Teilnehmern pflegen.
- 3) Alle Benutzerlisten auf Fehleingaben, oder Ähnlichkeiten mit vorhandenen Benutzern prüfen.
- 4) Danach evtl. die Benutzerlisten entsprechend korrigieren.
- 5) Benutzerdaten übernehmen, d.h. Benutzer jetzt tatsächlich anlegen, versetzen oder löschen
- 6) Passwortlisten bzw. Anmeldekärtchen ausdrucken

Änderung von Benutzerdaten

Sind Sie an der *Schulkonsole* als *global-admin* angemeldet, erhalten Sie unter der Rubrik *Benutzerverwaltung* die folgenden Menüpunkte:



Export von Schüler- und Lehrerliste aus dem Schulverwaltungsprogramm

Die meisten Schulverwaltungsprogramme bieten die Möglichkeit, eine Schüler- und eine Lehrerliste für die *linuxmuster.net* zu exportieren. Dabei werden die Daten mit dem benötigten Datensatzformat untereinander in eine Textdatei geschrieben. Für die Schülerliste gilt folgendes Format:

```
Klasse;Nachname;Vorname;Geburtsdatum;Nr;
```

```
Class;Last name;First name;Birthday;ID;
```

Dabei ist das letzte Feld optional. Es enthält die im Schulverwaltungsprogramm eindeutig vergebene Schülernummer. Ist sie vorhanden, sollte man sie unbedingt mit übernehmen, das sie die Identifikation des richtigen Datensatzes bei Versetzungen, Namensänderungen usw. erheblich erleichtert. Falls die Nummer nicht vorhanden ist, besteht jede Zeile nur aus den 4 Feldern

```
Klasse;Nachname;Vorname;Geburtsdatum;
```

```
Class;Last name;First name;Birthday;
```

Auch wenn Ihr Schulverwaltungsprogramm keine direkte Ausgabe für die Musterlösung vorsieht, können die Daten meist unter Angabe der benötigten Felder und mit dem Semikolon als Trennzeichen exportiert werden.

Für die CSV-Dateien sollte eine UTF-8 Kodierung verwendet werden. In den Voreinstellungen der Schulkonsole ist üblicherweise eine automatische Erkennung der Kodierung festgelegt.

Hinweis: Die nachstehend dargestellten Benutzer sind alles *fiktive Testnutzer*, die nur zur Illustration eingetragen und auf den Screenshots dargestellt werden. Es handelt um keine lebenden Personen. Die Daten dienen nur zu Test- und Dokumentationszwecken.

Pflege der Schülerdatei

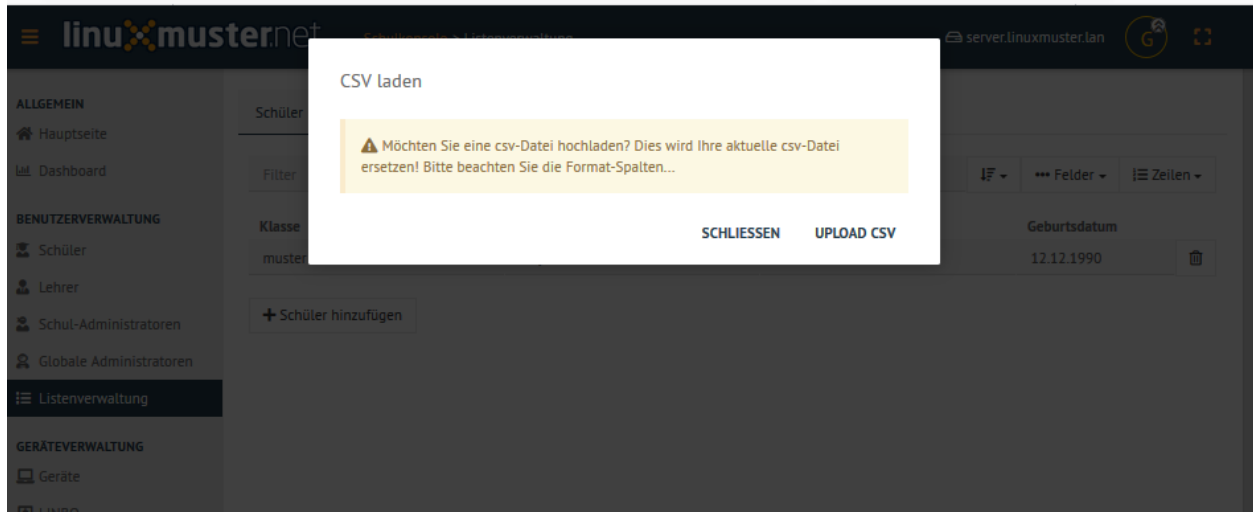
Die Schüler können Sie erstmals in das System aufnehmen, in dem Sie die vorbereitete students.csv Datei mithilfe der Schulkonsole hochladen.

Gehen Sie hierzu in der Schulkonsole unter **Benutzerverwaltung** in das Menü **Listenverwaltung** und klicken Sie auf die obere Reiterkarte **Schüler** und dann unten auf den Eintrag **CSV Laden**.

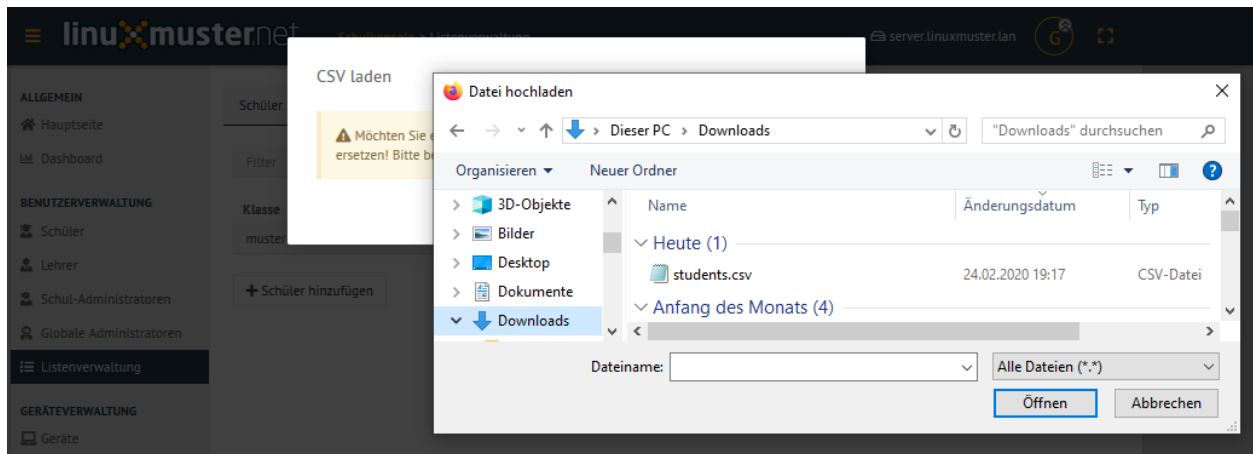
Es erscheinen dann schrittweise folgende Eingabefenster:

The screenshot displays the 'linuxmuster.net' Schulkonsole interface. The left sidebar shows the 'BENUTZERVERWALTUNG' (User Management) menu with 'Listenverwaltung' (List Management) selected. The main area shows the 'Schüler' (Students) tab with a table of student data. The table has columns for 'Klasse' (Class), 'Nachname' (Surname), and 'Vorname' (First Name). The first entry is 'muster', 'Meyer', and 'Ferdinand'. Below the table is a '+ Schüler hinzufügen' (Add student) button. At the bottom of the interface are four buttons: 'SPEICHERN' (Save), 'SPEICHERN & PRÜFEN' (Save & Check), 'IM EDITOR ÖFFNEN' (Open in Editor), and 'CSV LADEN' (Load CSV).

Es erscheint eine Warnmeldung, da der Upload einer neuen students.csv die bisherige Datei und damit deren Einträge überschreibt.



Nachdem Sie dies bestätigt haben, müssen Sie den Ort der hochzuladenden CSV-Datei angeben.



Haben Sie den Vorgang bestätigt, so wird nun die CSV-Datei überprüft und Sie sehen dann zur Kontrolle die ermittelten Klassen und Schüler:

Falls erforderlich kann hier die Reihenfolge der Spalteneinträge noch angepasst werden. Zudem kann angegeben werden, ob die Datei eine Schüler-ID verwendet.

Nach der Bestätigung der Sortierreihenfolge werden die Benutzer temporär importiert. Das Ergebnis wird Ihnen wie in der nachstehenden Abbildung angezeigt.

Entspricht dies dem gewünschten Import, so müssen Sie die Benutzer nun mithilfe des Eintrags **Speichern & prüfen** übernehmen. Das Prüfergebnis wird Ihnen angezeigt und Sie müssen nun die Übernahme der neuen Benutzer bestätigen.

Nach der Bestätigung zur Übernahme der neuen Benutzer werden diese auf dem Server angelegt und eingerichtet. Nach Abschluss des Imports sehen Sie im dargestellten Konsolenfenster einen Eintrag wie `4 users added` - wir in der Abbildung zu erkennen ist.

Die CSV-Dateien finden sich auf dem Server in folgendem Verzeichnis: `/etc/linuxmuster/sophomorix/default-school`

Es gibt dort drei verschiedene CSV-Dateien:

Liste sortieren

Linuxmuster muss wissen, welche Spalte welche Benutzerdaten enthält. Dies ist obligatorisch für den Import der CSV-Liste.
Bitte setzen Sie die Spalte in die richtige Reihenfolge.

Customizations
CSV contains custom student ID attribute (optional) ☐

ABBRECHEN SORTIERUNG AKZEPTIEREN

Klasse	Nachname	Vorname	Geburtsdatum	nicht verwendet
muster	Meyer	Ferdi	12.12.1990	
8a	Müller	Manfred	12.12.2005	
8a	Meyer	Luise	13.01.2005	
10b	Meier	Toto	22.04.2003	
10b	Matherni	Paul	11.07.2003	

ABBRECHEN SORTIERUNG AKZEPTIEREN

linuXmuster.net Schulkonsole > Listenverwaltung server.linuxmuster.lan

ALLGEMEIN
Hauptseite
Dashboard

BENUTZERVERWALTUNG
Schüler
Lehrer
Schul-Administratoren
Globale Administratoren
Listenverwaltung

GERÄTEVERWALTUNG
Geräte

Schüler Lehrer Extra-Schüler

Filter

Class	Last Name	First Name	Birthday	
muster	Meyer	Ferdi	12.12.1990	
8a	Müller	Manfred	12.12.2005	
8a	Meyer	Luise	13.01.2005	
10b	Meier	Toto	22.04.2003	
10b	Matherni	Paul	11.07.2003	

+ Schüler hinzufügen

Prüfergebnis

Übersicht Hinzufügen

Benutzer werden hinzugefügt: 4

10b	matherpa	Matherni Paul	student	default-school
8a	meyerlu	Meyer Luise	student	default-school
8a	muellema	Müller Manfred	student	default-school
10b	meiertoto	Meier Toto	student	default-school

Benutzer werden aktualisiert: 0

Benutzer werden gelöscht: 0

☒ Neue Benutzer hinzufügen

ÜBERNEHMEN ABBRECHEN

Änderungen werden übernommen

```

DONE with 1) Line 4: S/B::@SCHOOL@/$directory_students/@@ADMINCLASS@/@@USER@/::root::root::0755::student.home.ntacl:: ---
-----
2) Line 9: S/B::@SCHOOL@/$directory_students/@@ADMINCLASS@/@@USER@/@TRANSFER_DIR_HOME@/::root::root::0755::student.transf
OK (0): /usr/bin/smbclient -U administrator%***** //server/default-school -c 'mkdir "students/10b/matherpa/transfer"'
OK (0): smbcacls-NTACL on //server/default-school students/10b/matherpa/transfer
DONE with 2) Line 9: S/B::@SCHOOL@/$directory_students/@@ADMINCLASS@/@@USER@/@TRANSFER_DIR_HOME@/::root::root::0755::studi
#### Repairing from file: repdir.student_home (end) ####
#### Creating user 4: matherpa (end) ####

#### Running hook scripts ADD_HOOK_DIR: ####
#### Removing lock in /var/lib/sophomnix/lock/sophomnix.lock ####
#### /usr/sbin/sophomnix-add terminated regularly ####
Calling console printout
LOG : /usr/sbin/sophomnix-add terminated regularly
4 users added
  
```

Einstellungen

☒ Autoscroll

SCHLIESSEN

- Schülerinnen und Schüler: students.csv
- Lehrerinnen und Lehrer: teachers.csv
- zusätzliche Nutzer: extrastudents.csv

Haben Sie die Benutzer angelegt, so können Sie später Änderungen auch direkt via Schulkonsole in der CSV-Datei vornehmen. Wählen Sie hierzu im Menü **Benutzerverwaltung** -> **Listenverwaltung** -> **Schüler** -> **Im Editor öffnen**

Es erscheint dann im Browser die CSV-Datei im Editiermodus, so dass Sie Ihre Anpassungen vornehmen können, diese speichern und danach auf **speichern & prüfen** gehen.



Pflege der Lehrerdatei

Für die Lehrer besteht die Möglichkeit, einen Wunschlogin-Namen anzugeben. Der Datensatz aus dem Schulverwaltungsprogramm wird also um ein Feld ergänzt. In der CSV-Datei muss kein Klassenname angegeben, dafür jedoch bei jedem Lehrer *teachers* vorangestellt werden. Es wird automatisch ein Import in die Gruppe *Lehrer* vorgenommen.

Das Format der Datei *teachers.csv* stellt sich wie folgt dar:

```
teachers;Last name;First name;Birthday;Login;;;;
```

```
Lehrer;Nachname;Vorname;Geburtsdatum;Wunschlogin;;;;
```

Von *sophomorix* werden noch die für einzelne Lehrer gesondert eingegebenen Quotas angehängt.

Aus diesem Grund macht es keinen Sinn, eine vorhandene Lehrerdatei mit derjenigen aus dem Schulverwaltungsprogramm zu überspielen, da Sie dann für alle Lehrer *Wunschlogin* und *Sonderquota* wieder neu eingeben müssten.

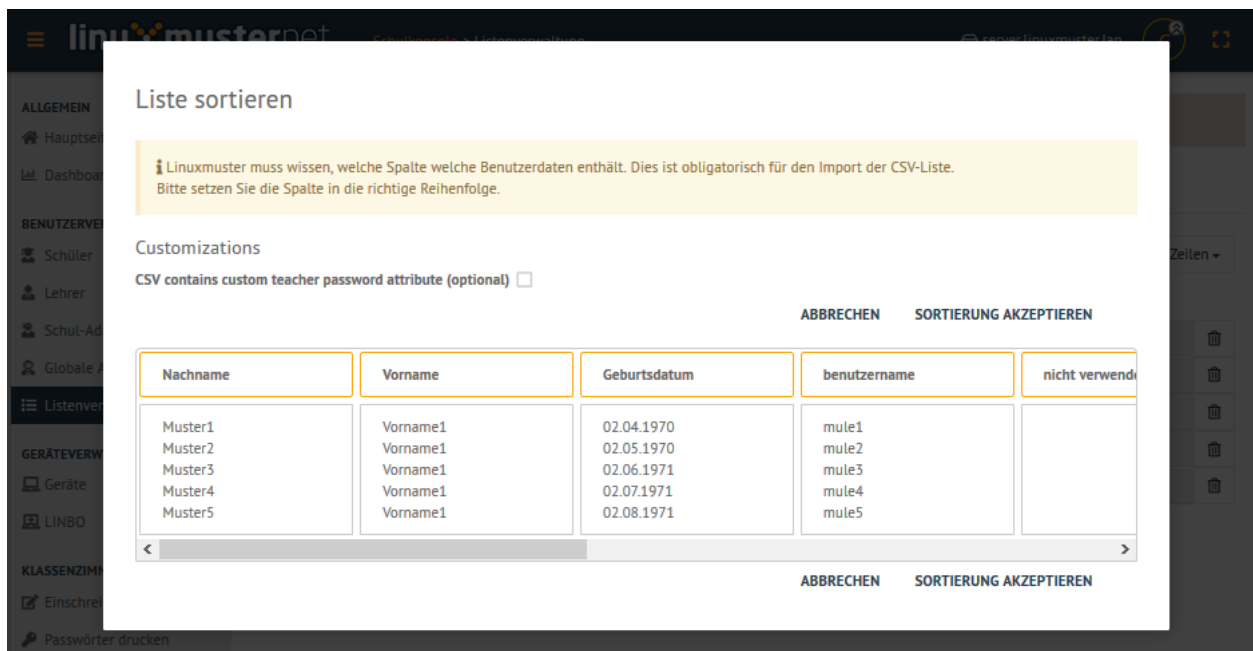
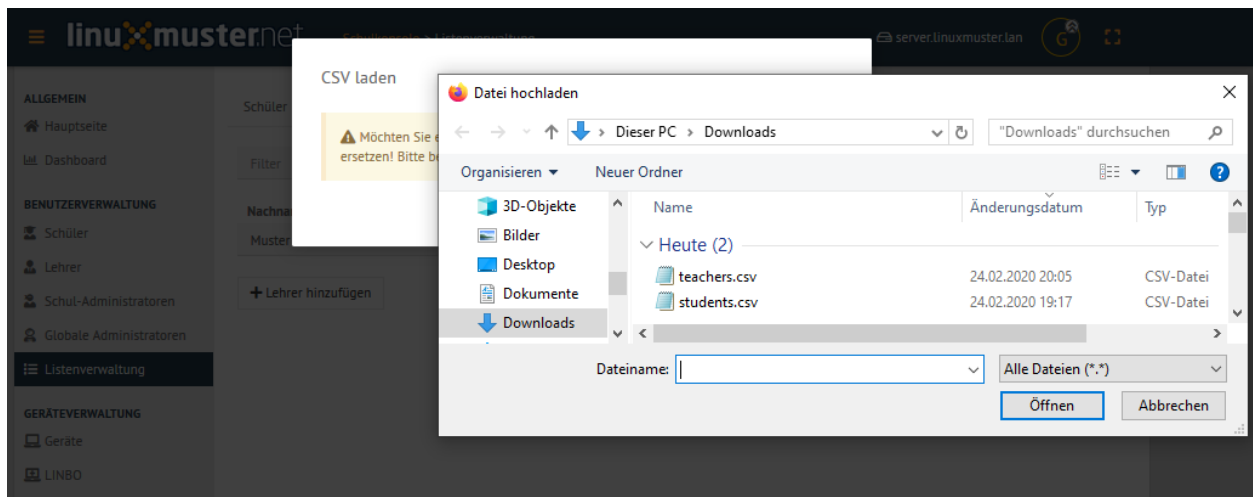
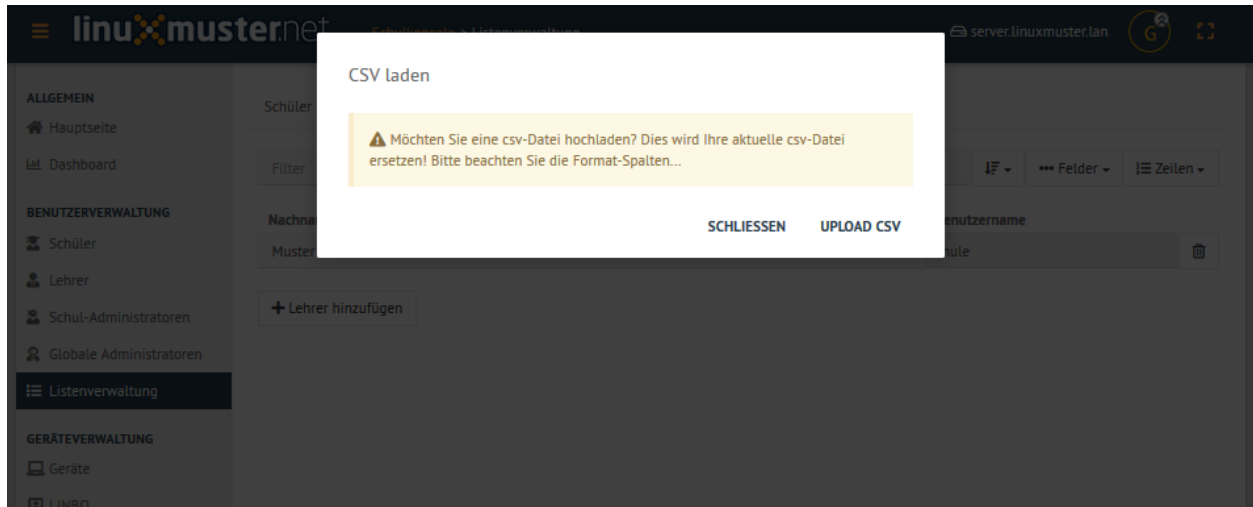
Der Import der *teachers.csv* erfolgt analog zu dem Vorgehen wie es zuvor bereits für die *students.csv* beschrieben wurde.

Rufen Sie im Menü unter der Benutzerverwaltung den Eintrag **Listenverwaltung** -> **Lehrer** -> **CSV Laden** auf.

Danach wählen Sie dort den Dateinamen der hochzuladenden CSV-Datei aus.

Die Einträge werden nun geprüft und das Prüfergebnis wird Ihnen angezeigt. Hier können Sie bereits falsche Spaltenzuordnungen oder eine abweichende Spaltenreihenfolge erkennen. Stimmt das dargestellte Ergebnis, so übernehmen Sie die Sortierreihenfolge.

Nach dem Import der CSV-Datei werden die zu importierenden Lehrer wie folgt dargestellt:



The screenshot shows the 'linuxmuster.net' Schulkonsole interface. The top navigation bar includes the logo, 'Schulkonsole > Listenverwaltung', and a server status indicator. The left sidebar lists various management functions. The main area displays the 'Lehrer' (Teachers) tab, which contains a table of user data and a button to add new teachers.

Last Name	First Name	Birthday	Login
Muster1	Vorname1	02.04.1970	mule1
Muster2	Vorname1	02.05.1970	mule2
Muster3	Vorname1	02.06.1971	mule3
Muster4	Vorname1	02.07.1971	mule4
Muster5	Vorname1	02.08.1971	mule5

Klicken Sie nun auf **Speichern & Prüfen**, um die importierten Lehrer dauerhaft in das System zu übernehmen. Es wird Ihnen dann vor der endgültigen Übernahme nochmals das Prüfergebnis dargestellt, aus dem hervorgeht, welche Lehrer hinzugefügt, versetzt oder gelöscht werden.

Nach der Bestätigung finden sich die Lehrer nun dauerhaft im System und werden wie folgt dargestellt:

Pflege der Extraschüler

Zur Verwaltung von Schülern, die nicht im Schulverwaltungsprogramm aufgenommen sind, gibt es in der *Schulkonsole* unter der Rubrik *Benutzerverwaltung* in der *Listenverwaltung* die Reiterkarte *Extra-Schüler*:

Im Bereich *Im Editor öffnen* können Schüler von Kooperationsschulen oder Austausch- bzw. Gast Schüler eingegeben werden. Die Syntax ist wie bei der Schülerdatei, ergänzt um ein Feld für einen Wunschanmeldenamen:

```
Class;Last name;First name;Birthday;Login;
```

```
Klasse;Nachname;Vorname;Geburtsdatum;Wunschlogin;
```

Der Name für die Klasse ist frei wählbar, z.B: *koop* (für Kooperation) oder *at* (für Austausch). Es können aber, gerade auch bei Kooperationsschülern, die **bestehenden** Klassennamen verwendet werden. Dies ist wichtig, falls der Zugriff auf das Klassentauschverzeichnis der Klasse ermöglicht werden soll. Bei neuen Gruppennamen, wird auch ein neues Klassentauschverzeichnis angelegt.

Analog zu dem Import der CSV-Dateien für die Schüler und Lehrer erfolgt auch für die Extra-Schüler der Upload bzw. die Bearbeitung der Datei *extrastudents.csv*.

Die Benutzer werden wiederum mit **Speichern & prüfen** übernommen. Hierbei wird Ihnen wiederum das Prüfergebnis angezeigt:

Nach dem Import sehen Sie in der dargestellten Konsole Hinweise wie `1 users added`.

Die Extra-Schüler werden im System dann wie folgt dargestellt:

server.linuxmuster.lan

Prüfergebnis

Übersicht Hinzufügen Zu versetzen

1 Benutzer werden hinzugefügt: 5

teachers	mule4	Muster4 Vorname1	teacher	default-school
teachers	mule5	Muster5 Vorname1	teacher	default-school
teachers	mule1	Muster1 Vorname1	teacher	default-school
teachers	mule2	Muster2 Vorname1	teacher	default-school
teachers	mule3	Muster3 Vorname1	teacher	default-school

1 Benutzer werden aktualisiert: 1

mule	<ul style="list-style-type: none"> • Role : teacher --> student • Status : Usable (U) --> Tolerated (T) • AdminClass : teachers --> attic
------	---

1 Benutzer werden gelöscht: 0

Änderungen werden übernommen

```

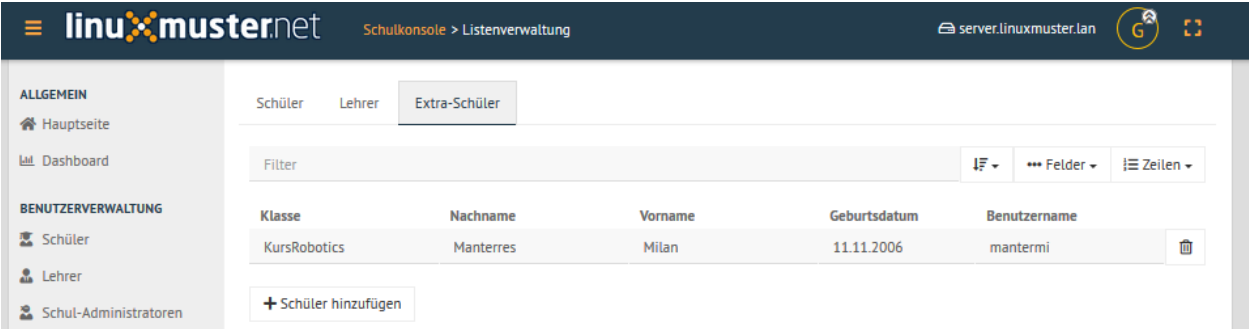
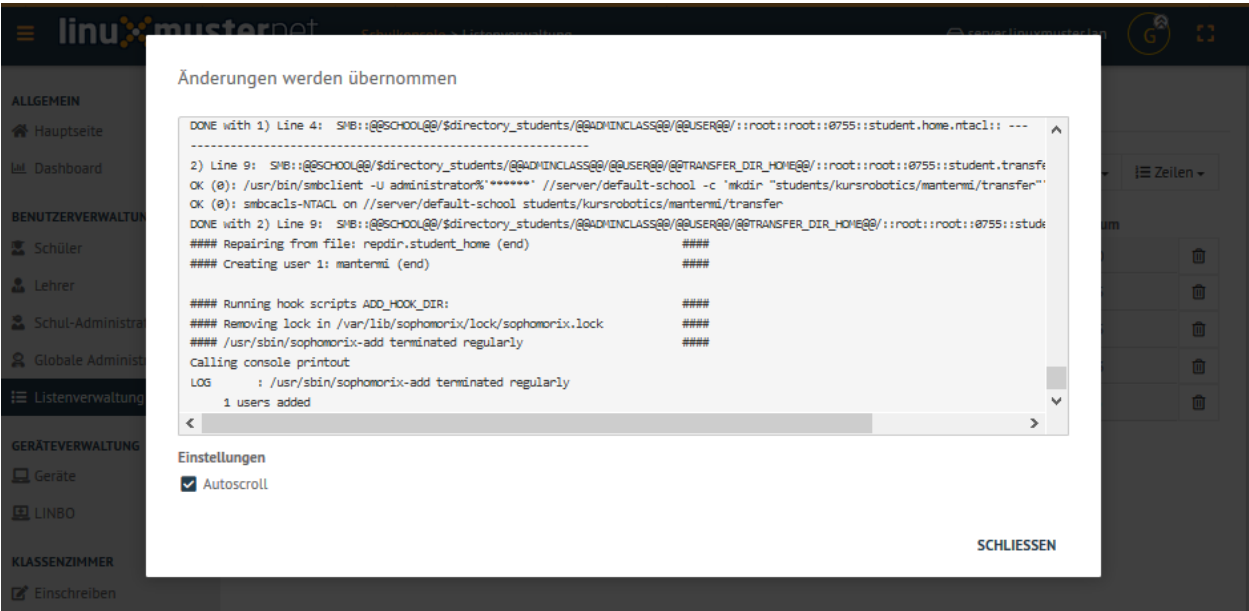
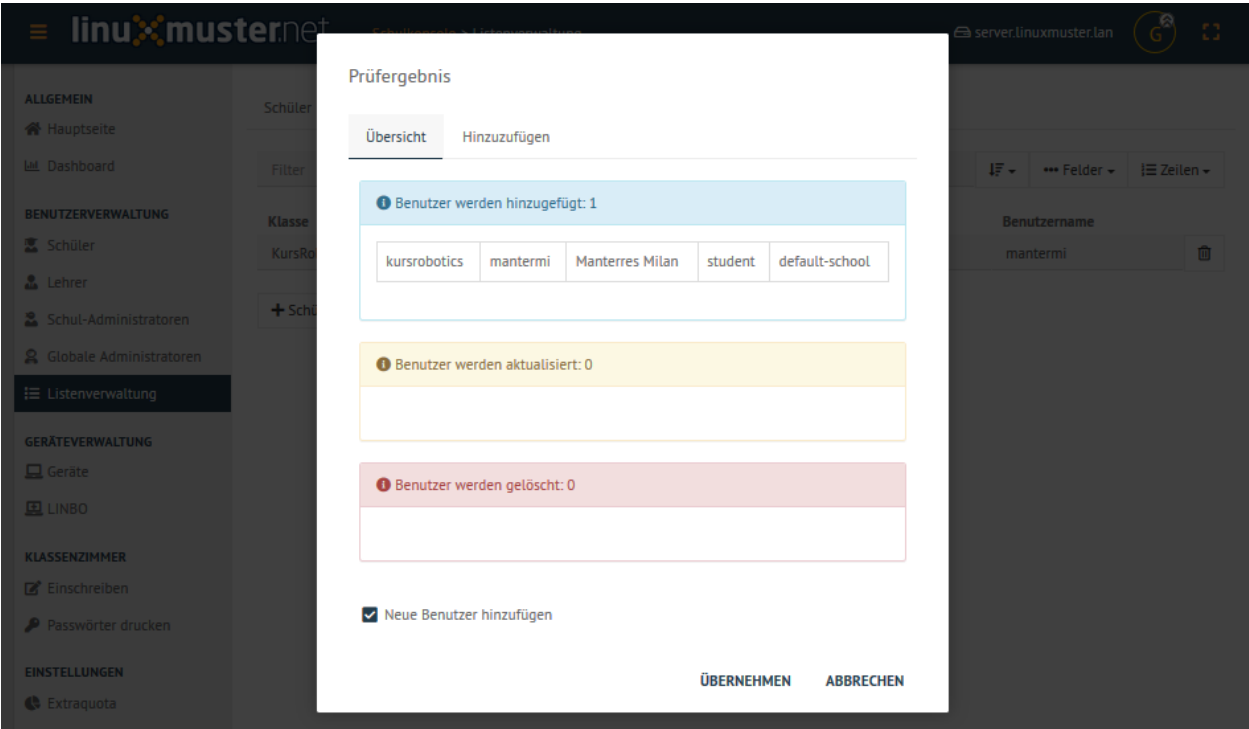
OK (0): smbcacls-NTACL on //server/default-school students/attic/mule
DONE with 1) Line 4: S\B:@@SCHOOL@@/$directory_students/@@ADMINCLASS@@/@USER@@/:root::root::0755::student.home.ntacl:: ---
-----
2) Line 9: S\B:@@SCHOOL@@/$directory_students/@@ADMINCLASS@@/@USER@@/@TRANSFER_DIR_HOME@@/:root::root::0755::student.transfe
OK (0): /usr/bin/smbclient -U administrator%***** //server/default-school -c 'mkdir "students/attic/mule/transfer"'
OK (0): smbcacls-NTACL on //server/default-school students/attic/mule/transfer
DONE with 2) Line 9: S\B:@@SCHOOL@@/$directory_students/@@ADMINCLASS@@/@USER@@/@TRANSFER_DIR_HOME@@/:root::root::0755::stud
#### Repairing from file: repdir.student_home (end) ####
#### Moving user mule (1),(end) ####

#### Running hook scripts UPDATE_HOOK_DIR: ####
#### /usr/sbin/sophomox-update terminated regularly ####
Calling console printout
LOG : /usr/sbin/sophomox-update terminated regularly
1 users updated
  
```

Einstellungen

☒ Autoscroll

SCHLIESSEN



4.22.8 Weiterführendes zu Sophomorix4

In der aktuellen Version der *linuxmuster.net* wird die Benutzerverwaltung mit Hilfe des Programms *Sophomorix4* durchgeführt. Für alle zuvor beschriebenen Vorgänge zur Benutzerverwaltung mit der Schulkonsole stellt *sophomorix4* Konsolenbefehle auf dem *linuxmuster.net* Server bereit.

Optional besteht also die Möglichkeit, die Benutzerverwaltung in bestimmten Fällen auch auf der Konsole auf dem Server durchzuführen, oder bestimmte Vorgänge mithilfe von Skripten zu automatisieren.

Sophomorix4 bietet hierfür eine Schnittstelle, um eigene Skripte hieran anzubinden.

Für weitergehende Informationen sei an dieser Stelle auf die Entwicklerdokumentation verwiesen:

<https://github.com/linuxmuster/sophomorix4/wiki/>

und

https://github.com/linuxmuster/sophomorix4/wiki/Custom_Scripts

Auf dem Server lassen sich die Befehle wie folgt ausgeben:

```
sophomorix-<tab>
```

Die Optionn eines Befehls können dann anhand der Hilfsoption ausgegeben werden:

```
sophomorix-add --help
```

4.23 Lehrer-Passwörter zurücksetzen

Autor des Abschnitts: @cweikl

Im Schulalltag tritt für den Netzwerkbeauftragten häufiger die Anforderung auf, einem oder mehreren Lehrern ein neues Kennwort zuzuweisen, oder ggf. allen neu angelegten Lehrern ein identisches Erstkennwort zuzuweisen, das diese nach der Erstanmeldung wieder ändern müssen.

Um für Lehrer Kennwörter neu zu setzen, melden Sie sich an der Schulkonsole als `global-admin` an. Klicken Sie im Menü Benutzerverwaltung auf den Eintrag **Lehrer**. Sie sehen dann alle derzeit im System angelegten Lehrer-Accounts.

Bei der Ersteinrichtung der Lehrer erhalten diese i.d.R. ein Zufallskennwort als Erstkennwort. Um für Lehrer das Kennwort neu zu setzen, markieren Sie die gewünschten Lehrer, indem Sie die Checkbox der Betreffenden auswählen. Sollten alle Lehrer ein neues Kennwort bekommen, so können Sie unten den Eintrag **Alle auswählen** klicken, dann wird bei allen Lehrern ein Auswahlhäkchen gesetzt.

4.23.1 Optionen für das Zurücksetzen

Für die ausgewählten Lehrer haben Sie nun drei Optionen, um das Kennwort neu zu setzen:

- 1) **Setze Erstpasswort für Ausgewählte:** Diese Option setzt das Kennwort der ausgewählten Lehrer auf das Erstkennwort zurück, das diesen bei der Ersteinrichtung zugewiesen wurde. Von Lehrern geänderte Kennwörter werden so auf ein vom System gesetztes Erstkennwort zurückgesetzt.
- 2) **Setze Zufallspasswort für Ausgewählte:** Für die ausgewählten Lehrer wird per Zufallsverfahren ein neues Kennwort erstellt und diesen zugewiesen. Jeder Lehrer erhält so ein eigenes Zufallskennwort, was bisherige Kennworteinträge zurücksetzt.
- 3) **Benutzerdefiniertes Passwort für Ausgewählte:** Mit dieser Option kann für alle ausgewählten Lehrer ein vom Netzwerkbetreuer vorgegebenes Kennwort gesetzt werden, wodurch alle bisherigen Kennworteinträge auf das neu definierte Kennwort zurückgesetzt werden. Sollen alle neu eingerichteten Lehrer z.B. das Kennwort **Muster!**

Filter ↓ Vorname ▼ | ≡ Zeilen ▼

	Loginname	Name			
<input checked="" type="checkbox"/>	mule4	Vorname1 Muster4	Passwort ▼	Benutzereinstellungen	Usable
<input checked="" type="checkbox"/>	mule5	Vorname1 Muster5	Passwort ▼	Benutzereinstellungen	Usable
<input checked="" type="checkbox"/>	mule1	Vorname1 Muster1	Passwort ▼	Benutzereinstellungen	Usable
<input type="checkbox"/>	mule2	Vorname1 Muster2	Passwort ▼	Benutzereinstellungen	Usable
<input type="checkbox"/>	mule3	Vorname1 Muster3	Passwort ▼	Benutzereinstellungen	Usable

* ALLE AUSWÄHLEN
SETZE ZUFALLSPASSWORT FÜR AUSGEWÄHLTE
SETZE ERSTPASSWORT FÜR AUSGEWÄHLTE
BENUTZERDEFINIERTES PASSWORT FÜR AUSGEWÄHLTE

erhalten, was diese nach der Erstanmeldung ändern müssen, so hilft diese Option dabei für alle Lehrer ein identisches Kennwort vorzugeben.

4.23.2 Benutzerdefiniertes Passwort für Ausgewählte

Haben Sie die Option 1.) oder 2.) geklickt, so sehen Sie nun eine Statusmeldung mit grüner Schrift, dass das Erstpasswort gesetzt oder das Zufallspasswort festgelegt wurde.

Bei der Auswahl der Option **Benutzerdefiniertes Passwort für Ausgewählte** erscheint danach ein Kontrollfenster, in dem alle ausgewählten Lehrer angezeigt werden. Zudem finden Sie in diesem Fenster ganz unten eine Eingabezeile zur Definition des von Ihnen festzulegenden Kennwortes. Hier müssen Sie je nach Anzahl der Ausgewählten nach unten scrollen, um die Eingabezeile zu sehen.

Danach verfügen alle ausgewählten Lehrer über das angegebene Kennwort.

Dies können Sie auch über den Aufruf einzelner Lehrer, wie nachstehend beschrieben, kontrollieren.

4.23.3 Einzelne Lehrer

In der Schulkonsole können Sie in der Benutzerverwaltung im Menü **Lehrer** als **global-admin** alle im System eingerichteten Lehrer-Accounts einsehen.

Um nun einzelne Kennwörter zurückzusetzen, Benutzerinformationen zu erhalten, oder stichprobenartig einzelne Kennwörter zu prüfen (z.B. nach dem Zurücksetzen vieler ausgewählter Lehrer) nutzen Sie hier pro Lehrer die Untermenüs des Eintrags **Passwort** oder das Untermenü zu dem Eintrag **Benutzereinstellungen**.

Klicken Sie auf den Eintrag **Passwort**, erscheint ein Untermenü bei dem Sie mehrere Optionen für das Erstpasswort haben. Zudem gibt es die Option, ein **benutzerdefiniertes Passwort** festzulegen.

Passwort ändern

- Vorname1 Muster5 **mule5** teachers
- Vorname1 Muster1 **mule1** teachers
- Vorname1 Muster2 **mule2** teachers
- Vorname1 Muster3 **mule3** teachers

••••••••

Hinweis: Minimale Passwortlänge ist 7 Zeichen. Verwenden Sie Großbuchstaben

ABBRECHEN

ANNEHMEN

Schulkonsole > Lehrer

server.linuxmuster.lan

ALLGEMEIN

- Hauptseite
- Dashboard

BENUTZERVERWALTUNG

- Schüler
- Lehrer**
- Schul-Administratoren

Filter

	Loginname	Name		
<input checked="" type="checkbox"/>	mule4	Vorname1 Muster4		
<input checked="" type="checkbox"/>	mule5	Vorname1 Muster5	Passwort	Benutzereinstellungen Usable
<input checked="" type="checkbox"/>	mule1	Vorname1 Muster1	Passwort	Benutzereinstellungen Usable

Erstpasswort anzeigen
Erstpasswort wiederherstellen
Erstpasswort zufällig festlegen
Erstpasswort benutzerdefiniert festlegen
Benutzerpasswort festlegen

Vorname

Zeilen

Benutzereinstellungen

Usable

Wählen Sie den Eintrag Erstpasswort anzeigen aus, so erscheinen nachfolgende Informationen für den jeweiligen Lehrer:

Password Information - Initial password

Password :

Loginname: mule3

Password: LFnTv32Gae(Q

Initial password Status: Still Set

Die weiteren Einträge sind analog zu o.g. Erklärungen zu nutzen.

Für jeden Benutzer gibt es bei der Einrichtung des Benutzer-Accounts immer ein Erstkennwort und später zusätzlich ein vom Benutzer festgelegtes Kennwort. Entsprechend müssen Sie für das Zurücksetzen der Kennwörter die hierfür gewünschten Optionen auswählen.

Für jeden Benutzer können Sie die Benutzerinformationen anzeigen lassen.

Klicken Sie auf Benutzereinstellungen.

The screenshot shows a web interface for user management. On the left is a sidebar with a menu. The main area displays a table of users. For the user 'mule3', a dropdown menu is open under the 'Benutzereinstellungen' button, showing the option 'Benutzerinformationen'.

BENUTZERVERWALTUNG		Muster4			
<input checked="" type="checkbox"/>	mule5	Vorname1 Muster5	Passwort	Benutzereinstellungen	Usable
<input checked="" type="checkbox"/>	mule1	Vorname1 Muster1	Passwort	Benutzereinstellungen	Usable
<input type="checkbox"/>	mule2	Vorname1 Muster2	Passwort	Benutzereinstellungen	Usable
<input type="checkbox"/>	mule3	Vorname1 Muster3	Passwort	Benutzereinstellungen Benutzerinformationen	Usable

GERÄTEVERWALTUNG

- Geräte
- LINBO

Wähle dann das Untermenü **Benutzerinformationen** aus. Es erscheinen dann für den jeweiligen Benutzer die zugehörigen Informationen, die im System erfasst sind. Hierzu gehören auch seine Gruppenzugehörigkeiten.

Es ist u.a. ersichtlich, ob der Account aktiviert ist, oder ob ein Duldungszeitraum für den Benutzer greift.

Benutzerdetails - Vorname1 Muster3

Eigenschaften

Loginname:	mule3
Klasse:	teachers
Geburtsdatum:	02.06.1971
Sophomorix-Status:	Usable
Rolle:	teacher
Schulname:	default-school
Deaktivierungsdatum:	Nie
Duldungsdatum:	Nie
Erstellungsdatum:	24 Feb 2020 - 20:16:58

Gruppenmitgliedschaft:

AUSBLENDEN

teachers	Teachers	webfilter	Management
internet	Management	intranet	Management
wifi	Management	printing	Management

Cloudquota berechnet in MiB: ---

Mailquota berechnet in MiB: 1

SCHLIESSEN

4.24 Festplattenplatz für Benutzer einschränken (Quota)

Autor des Abschnitts: @cweikl

Alle Benutzer im System dürfen Daten auf dem Server abspeichern. Es kann also vorkommen, dass Schüler und Lehrer so viele Daten abspeichern, dass der Festplattenplatz des Servers aufgebraucht ist, was bis zur Einstellung des Betriebes führen kann. Außerdem kann eine übermäßige Beanspruchung des Plattenplatzes des Servers auch via Internet z.B. durch E-Mail-Bombing erfolgen.

Um dies zu verhindern, sollten Sie als Netzwerkbetreuer die Nutzung des Festplattenplatzes durch einzelne Nutzer oder Gruppen kontrollieren und beschränken.

Hierzu werden auf dem linuxmuster.net Server die sog. Quotas aktiviert. Dies erfolgt bei der Ersteinrichtung automatisch. Für jede Partition auf die Quotas angewendet werden, finden sich folgende Dateien:

```
-rw----- 1 root root 7.0K Feb 24 15:18 aquota.group
-rw----- 1 root root 8.0K Feb 24 15:18 aquota.user
```

Zunächst ist zu prüfen, welcher Festplattenplatz - verteilt über die verschiedenen Partitionen - zur Verfügung steht. Danach ist zu planen, welche Obergrenzen zur Belegung des Festplattenplatzes pro Lehrer, Schüler und Schuladministrator festgelegt werden sollen. Danach kann ggf. eine individuelle Änderung der Quotas für einzelne Benutzer z.B. für einige Lehrer, die umfangreiches Material ablegen müssen, erfolgen.

Hinweis: Es ist darauf zu achten, dass die Summe der vergebenen „Quotas“ nicht die Kapazität der Festplatten des Servers übersteigt.

4.24.1 Quotavorgaben erstellen

Um die Quotas für alle Benutzer der Gruppen Lehrer, Schüler und Schuladministratoren in gleicher Weise vorzugeben, melden Sie sich an der Schulkonsole als `global-admin` an.

Gehen Sie im Menü der Schulkonsole unter dem Menüpunkt **Einstellungen auf Schuleinstellungen** -> **Reiterkarte Quota**.

Hier legen Sie nun die gewünschten Quotas für die Benutzer der Gruppen Schüler, Lehrer und Schuladministratoren fest. Die Angaben sind in der Einheit MiB vorzunehmen.

Danach müssen Sie die neuen Vorgaben anwenden, indem Sie die Option **Speichern & Quota übernehmen** auswählen. Es öffnet sich ein neues Konsolenfenster, das den Verlauf der Anwendung der neuen Quotas darstellt. Ist der Vorgang abgeschlossen, sehen Sie im Konsolenfenster einen Eintrag wie `12 users smbquotas updated`.

4.24.2 Quotas kontrollieren

Nachdem die Änderungen angewendet wurden, sehen Sie die neuen Quotas in der Übersicht **Schuleinstellungen** -> **Quota**.

Die Quotas können Sie nun pro Benutzer kontrollieren.

Hierzu wählen Sie im Menü der Schulkonsole im Bereich der Benutzerverwaltung die Gruppe der Benutzer, für die Sie Quotas kontrollieren möchten.

Haben Sie z.B. für die Lehrer eine neue Quota-Richtlinie angewendet, so wählen Sie das Menü **Lehrer** aus und klicken für einen exemplarischen Benutzer den Eintrag **Benutzereinstellungen** -> **Benutzerinformationen**. Es erscheint ein Fenster, in dem Informationen zum Benutzer dargestellt werden. Am unteren Rand des Fensters werden ebenfalls die Cloud- und die Mail-Quotas, die für diesen Benutzer greifen, dargestellt.

linuXmuster.net Schulkonsole > Einstellungen server.linuxmuster.lan

ALLGEMEIN
Hauptseite
Dashboard

BENUTZERVERWALTUNG
Schüler
Lehrer
Schul-Administratoren
Globale Administratoren
Listenverwaltung

GERÄTEVERWALTUNG
Geräte
LINBO

KLASSENZIMMER
Einschreiben
Passwörter drucken

EINSTELLUNGEN
Extraquota
Schuleinstellungen

Allgemein Listenimport **Quota** Druck-Daten

Quota

	Schüler	Lehrer	Schuladministrator
Standardquota (global) in MiB	1006	2006	3006
Standardquota (Schule) in MiB	1506	2506	3506
Cloudquota in Prozent	100	100	100
Mailquota Standard in MiB	156	306	506

SPEICHERN SPEICHERN & QUOTA ÜBERNEHMEN

linuXmuster.net Schulkonsole > Einstellungen server.linuxmuster.lan

ALLGEMEIN
Hauptseite
Dashboard

BENUTZERVERWALTUNG
Schüler
Lehrer
Schul-Administratoren
Globale Administratoren
Listenverwaltung

GERÄTEVERWALTUNG
Geräte
LINBO

KLASSENZIMMER
Einschreiben
Passwörter drucken

EINSTELLUNGEN
Extraquota
Schuleinstellungen

Allgemein Listenimport **Quota** Druck-Daten

Quota

	Schüler	Lehrer	Schuladministrator
Standardquota (global) in MiB	1006	2006	3006
Standardquota (Schule) in MiB	1506	2506	3506
Cloudquota in Prozent	100	100	100
Mailquota Standard in MiB	156	306	506

SPEICHERN SPEICHERN & QUOTA ÜBERNEHMEN

Änderungen werden übernommen

```

#### Updating User 1/-: mule5 (start)
DN: CN=mule5,OU=Teachers,OU=default-school,OU=SCHOOLS,DC=linux
sophomorixCloudQuotaCalculated: 4506 MB
Logging user update
#### Updating User 1/-: mule5 (end)

#### 0 ERRORS, 0 WARNINGS -> let's go
#### Creating lock in /var/lib/sophomorix/lock/sophomorix.lock
#### /usr/sbin/sophomorix-quota started ...
#### Removing lock in /var/lib/sophomorix/lock/sophomorix.lock
#### /usr/sbin/sophomorix-quota terminated regularly
Calling console printout
LOG      : /usr/sbin/sophomorix-quota terminated regularly
          12 users mailquota updated
          12 users smbquota updated

```

Einstellungen
☒ Autoscroll

DETAILS AUSBLENDEN SCHLIESSEN

The screenshot shows the 'Quota' settings page in the linuxmuster.net Schulkonsole. The sidebar on the left contains navigation links under categories like ALLGEMEIN, BENUTZERVERWALTUNG, GERÄTEVERWALTUNG, KLASSENZIMMER, and EINSTELLUNGEN. The main content area has tabs for 'Allgemein', 'Listenimport', 'Quota', and 'Druck-Daten'. The 'Quota' tab is selected, showing a table with quota settings for three user groups: Schüler, Lehrer, and Schuladministrator. The table has four rows of settings, each with a value and a spinner control.

	Schüler	Lehrer	Schuladministrator
Standardquota (global) in MiB	1006	2006	5006
Standardquota (Schule) in MiB	506	4506	5506
Cloudquota in Prozent	100	100	100
Mailquota Standard in MiB	156	306	506

At the bottom of the page, there are buttons for 'SPEICHERN' and 'SPEICHERN & QUOTA ÜBERNEHMEN'.

Gleiches können Sie auch für die Schüler durchführen, so dass Sie identische Informationen sehen.

4.24.3 Quotas für einzelne Benutzer und Klassen anpassen

Haben Sie Quota-Vorgaben für die gesamte Schule vorgenommen, so können Sie nun diese für Sonderfälle oder erforderliche Abweichungen anpassen.

Sind Sie als global-admin in der Schulkonsole angemeldet, so rufen Sie unter dem Punkt Einstellungen den Menüeintrag Extraquota auf.

Hier stehen zu Beginn i.d.R. keine Einträge. Sie können nun getrennt für einzelne Lehrer, Schüler, Schul-Administratoren, Klassen und Projekte gesonderte Quota-Vorgaben vornehmen, die die allgemeinen Vorgaben für diese Benutzer überschreiben.

Lehrer

Haben Sie die Reiterkarte Lehrer gewählt, klicken Sie unten auf Search & add user. Es erscheint ein Konsolenfenster, in dem Sie einen Suchbegriff eingeben sollen, so dass passende Lehrer gefunden werden.

Wählen Sie aus der angezeigten Liste den gewünschten Benutzer aus und bestätigen Sie dies mit Schliessen.

Danach sehen Sie in der Quota-Übersicht für Lehrer den Benutzer mit seinen bisherigen Quota-Eintragungen.

Passen Sie nun für die jeweiligen Benutzer, die Quotas wie gewünscht an. Änderungen gegenüber den bisherigen Vorgaben werden farblich abgesetzt.

Benutzerdetails - Vorname1 Muster4

Eigenschaften

Loginname:	mule4
Klasse:	teachers
Geburtsdatum:	02.07.1971
Sophomorix-Status:	Usable
Rolle:	teacher
Schulname:	default-school
Deaktivierungsdatum:	Nie
Duldungsdatum:	Nie
Erstellungsdatum:	24 Feb 2020 - 20:16:58

Gruppenmitgliedschaft:

AUSBLENDEN

teachers	Teachers	webfilter	Management
internet	Management	intranet	Management
wifi	Management	printing	Management

Cloudquota berechnet in MiB: 4506 MB

Mailquota berechnet in MiB: 306

SCHLIESSEN

Benutzerdetails - Manfred Müller

Eigenschaften

Loginname:	muellema
Klasse:	8a
Sophomorix-Status:	Useable
Rolle:	student
Schulname:	default-school
Deaktivierungsdatum:	Nie
Duldungsdatum:	Nie
Erstellungsdatum:	24 Feb 2020 - 19:32:15

Gruppenmitgliedschaft:

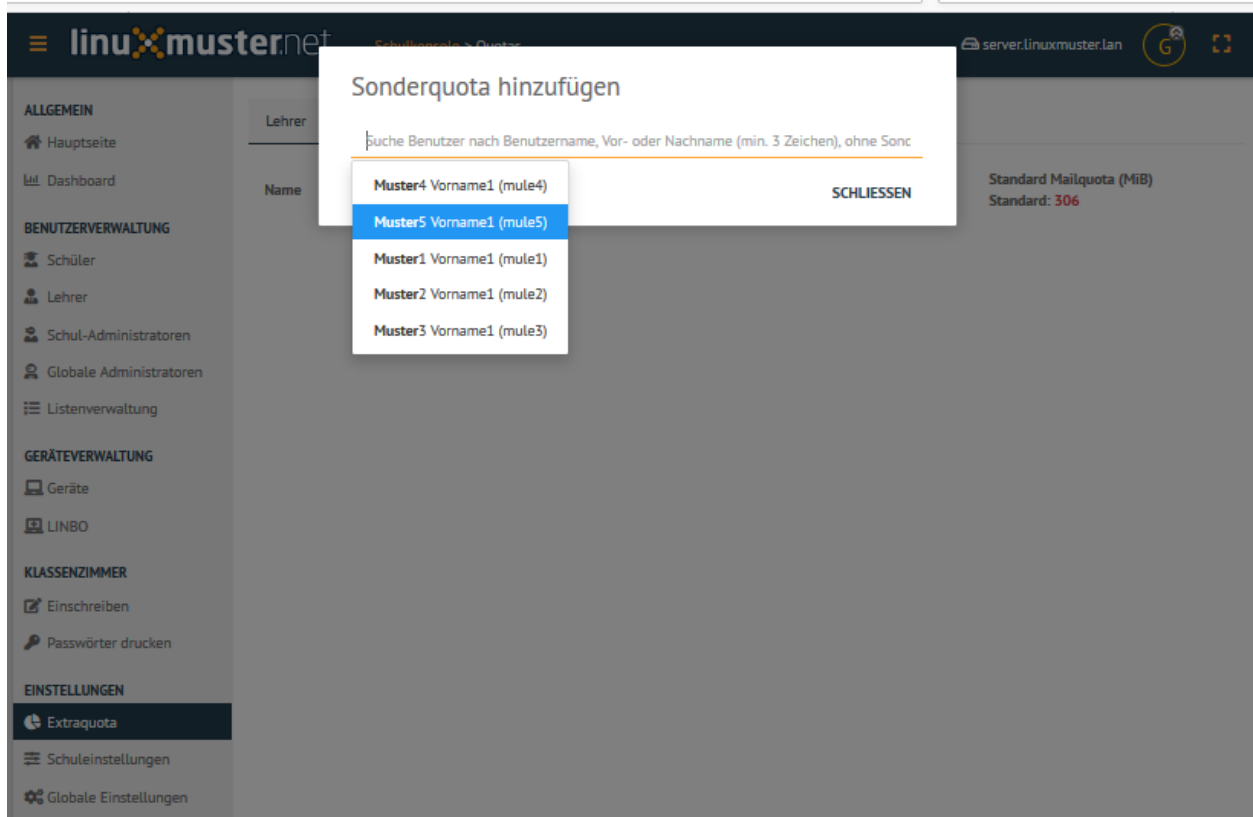
[AUSBLENDEN](#)

8a	8a	webfilter	Management
internet	Management	intranet	Management
wifi	Management	printing	Management

Cloudquota berechnet in MiB: 506 MB

Mailquota berechnet in MiB: 156

[SCHLIESSEN](#)



linuXmaster.net

Schulkonsole > Quotas

server.linuxmaster.lan

G

ALLGEMEIN

Hauptseite

Dashboard

BENUTZERVERWALTUNG

Schüler

Lehrer

Schul-Administratoren

Lehrer

Schüler

Schul-Administratoren

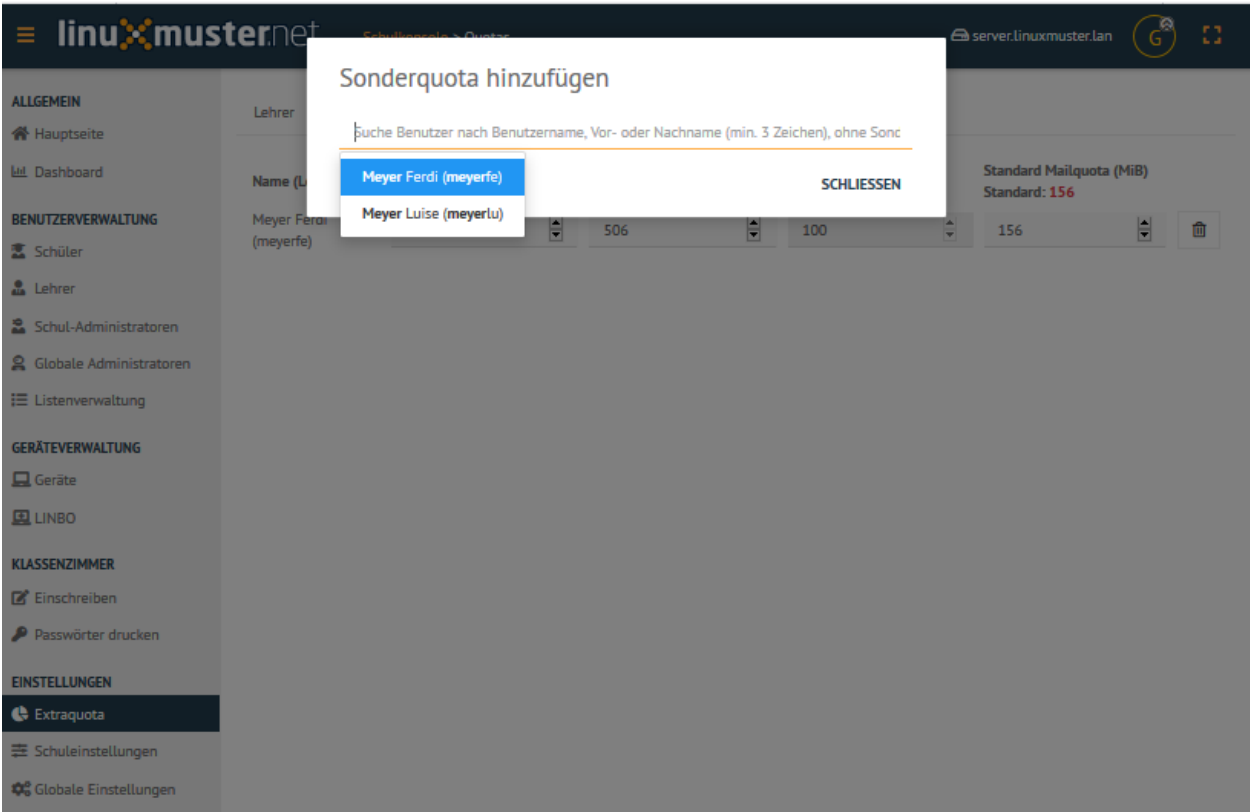
Klassen

Projekte

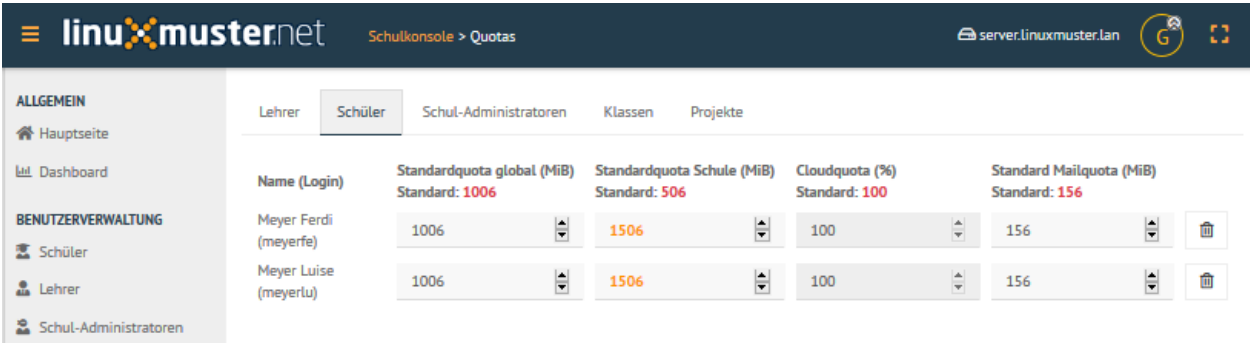
Name	Standardquota global (MiB) Standard: 2006	Standardquota Schule (MiB) Standard: 4506	Cloudquota (%) Standard: 100	Standard Mailquota (MiB) Standard: 306	
Muster4 Vorname1	<div>2006</div>	<div>406</div>	<div>100</div>	<div>306</div>	<div></div>
Muster5 Vorname1	<div>2006</div>	<div>406</div>	<div>100</div>	<div>306</div>	<div></div>

Schüler

Haben Sie die Reiterkarte Schüler gewählt, klicken Sie unten auf Search & add user. Es erscheint ein Konsolenfenster, in dem Sie einen Suchbegriff eingeben sollen, so dass passende Schüler gefunden werden.



Wählen Sie aus der angezeigten Liste den gewünschten Benutzer aus und bestätigen Sie dies mit Schliessen. Danach sehen Sie in der Quota-Übersicht für Schüler den Benutzer bzw. die Benutzer mit seinen/ihren bisherigen Quota-Eintragungen.



Passen Sie nun für die jeweiligen Benutzer, die Quotas wie gewünscht an. Änderungen gegenüber den bisherigen Vorgaben werden farblich abgesetzt.

Klassen

Um für Klassen Quota-Vorgaben zu erstellen bzw. klassenweise anzupassen, gehen Sie in der Schulkonsole unter Einstellungen auf Extraquota -> Klassen.

Es wird Ihnen dann eine Übersicht der im System vorhandenen Klassen angezeigt.

The screenshot shows the 'Klassen' tab in the 'Einstellungen' (Settings) section of the linuxmuster.net Schulkonsole. The table displays the following data:

Name	Standardquota global (MiB)	Standardquota Schule (MiB)	Standard Mailquota (MiB)
attic	0	0	0
10b	0	0	0
8a	0	0	0
kursrobotics	0	0	0
muster	0	0	0

Nehmen Sie hier nun wie gewünscht die neuen Eintragungen für die Quotas der Klassen vor. Änderungen gegenüber den bisherigen Vorgaben werden farblich abgesetzt.

Extraquotas anwenden

Um nun alle individuellen Anpassungen für Quota-Vorgaben von Lehrern, Schülern, Schul-Administratoren, Klassen und Projekten vorzunehmen, wählen Sie unter Extraquota -> Reiterkarte -> Speichern & übernehmen.

Danach erscheint ein Konsolenfenster, in dem die Anwendung der neuen Quotavorgaben dargestellt wird. Ist der Vorgang abgeschlossen, so erkennen Sie dies z.B. an Einträgen wie `8 user smbquota updated`

linuXmuster.net

Schulkonsole > Quotas

server.linuxmuster.lan

ALLGEMEIN

Hauptseite

Dashboard

BENUTZERVERWALTUNG

Schüler

Lehrer

Schul-Administratoren

Globale Administratoren

Listenverwaltung

GERÄTEVERWALTUNG

Geräte

LINBO

KLASSENZIMMER

Einschreiben

Passwörter drucken

EINSTELLUNGEN

Extraquota

Schuleinstellungen

Globale Einstellungen

Lehrer

Schüler

Schul-Administratoren

Klassen

Projekte

Name	Standardquota global (MiB)	Standardquota Schule (MiB)	Standard Mailquota (MiB)
attic	0	0	0
10b	0	0	0
8a	0	0	0
kursrobotics	0	0	0
muster	0	0	0

linuXmuster.net

Schulkonsole > Quotas

server.linuxmuster.lan

ALLGEMEIN

Hauptseite

Dashboard

BENUTZERVERWALTUNG

Schüler

Lehrer

Schul-Administratoren

Globale Administratoren

Listenverwaltung

GERÄTEVERWALTUNG

Geräte

LINBO

KLASSENZIMMER

Einschreiben

Passwörter drucken

EINSTELLUNGEN

Extraquota

Schuleinstellungen

Globale Einstellungen

Lehrer

Schüler

Schul-Administratoren

Klassen

Projekte

Name	Standardquota global (MiB)	Standardquota Schule (MiB)	Standard Mailquota (MiB)
attic	0	0	0
10b	0	0	0
8a	0	0	0
kursrobotics	0	0	0
muster	0	0	0

Änderungen werden übernommen

Updating User 1/-: mule5 (start)
DN: CN=mule5,OU=Teachers,OU=default-school,OU=SCHOOLS,DC=linuxmuster
sophomorixCloudQuotaCalculated: 406 MB
Logging user update
Updating User 1/-: mule5 (end)

0 ERRORS, 0 WARNINGS -> let's go
Creating lock in /var/lib/sophomorix/lock/sophomorix.lock
/usr/sbin/sophomorix-quota started ...
Removing lock in /var/lib/sophomorix/lock/sophomorix.lock
/usr/sbin/sophomorix-quota terminated regularly
Calling console printout
LOG : /usr/sbin/sophomorix-quota terminated regularly
0 users mailquota updated
8 users smbquota updated

Einstellungen

☒ Autoscroll

DETAILS AUSBLENDEN

SCHLIESSEN

4.25 Vorbereitung am Schuljahresanfang

Autor des Abschnitts: @cweikl

4.25.1 Klassenliste aktualisieren

Zu Schuljahresbeginn muss jeder Lehrer seine Klassenliste aktualisieren. Neu zu unterrichtende Klassen sind hinzuzufügen und nicht mehr unterrichtete Klassen sind auszutragen. Voraussetzung für die Zuordnung neuer Klassen ist, dass diese im linuxmuster.net System bereits existieren. Ihr Schuladministrator muss daher alle neuen Klassen- und Schülerdaten bereits aus der Schulverwaltung exportiert und in linuxmuster.net importiert haben.

Um die Klassenliste als Lehrer zu aktualisieren, erfolgt zunächst die Anmeldung in der Schulkonsole als Lehrer.

The screenshot shows the Linuxmuster.net login page. The header includes the logo and navigation links. The left sidebar contains a menu with 'ALLGEMEIN' and 'KLASSENZIMMER'. The main content area displays a welcome message and three panels: 'Konto Informationen', 'Quotas', and 'Gruppen'.

Konto Informationen

Name:	Vorname1, Muster4
E-Mail:	mule4@linuxmuster.net
Schule:	default-school
Rolle:	teachers

[Passwort ändern](#)

Quotas

default-school	0 MiB / 3006 MiB
linuxmuster-global	0 MiB / 2006 MiB

Cloudquota berechnet in MB: 3006 MB
Mailquota berechnet in MB: 306 MB

Gruppen

10b	Klasse
8a	Klasse
kursrobotics	Klasse
teachers	Lehrer

4.25.2 Klassenliste auswählen

Um Klassenlisten zu aktualisieren, ist nach erfolgreicher Anmeldung als Lehrer das Menü Klassenzimmer -> Einschreiben auszuwählen.

The screenshot shows the 'Einschreiben' (Enrollment) page in the Linuxmuster.net interface. The header and sidebar are consistent with the previous screenshot. The main content area displays a list of classes and projects.

Schulklassen

<input checked="" type="checkbox"/> Class 10b	<input checked="" type="checkbox"/> Class 8a	<input type="checkbox"/> Class attic	<input checked="" type="checkbox"/> Class kursrobotics	<input type="checkbox"/> Class muster
---	--	--------------------------------------	--	---------------------------------------

Drucker

<input type="checkbox"/> Printer r200hp-tj-2055dn

Projekte

Es gibt noch keine Projekte. Sie können über die Menüleiste ein neues erstellen.

Jede Klasse, die dem Lehrer zugeordnet ist, ist mit einem Auswahlhäkchen markiert. Für Klassen, die nun dem Lehrer neu hinzugefügt werden sollen, ist das Häkchen vor der betreffenden Klasse zu setzen. Für Klassen, die im neuen Schuljahr nicht mehr dem Lehrer zugeordnet sein sollen, ist das Häkchen zu deaktivieren.

Schulklassen

☒ Class 10b ☒ Class 8a ☐ Class attic ☒ Class kursrobotics ☒ Class muster

Danach sind die Änderungen unten auf der Seite mit **Übernehmen** dauerhaft anzuwenden.

Dies Änderungen stellen sich dann wie folgt dar:

4.25.3 Neue Anmeldung

Abschließend müssen Sie sich von Ihrem Client abmelden und wieder neu anmelden, damit die Netzlaufwerke korrekt zugeordnet werden.

Dies können Sie kontrollieren, indem Sie nach der erneuten Anmeldung mit dem Dateimanager prüfen, ob für die neue Klasse ein Tauschverzeichnis vorhanden ist.

4.26 Schulkonsole des Lehrers

Autor des Abschnitts: @cweikl, @MachtDochNix (pics)

Hast Du auf dem Server einen Lehrer-Account, so kannst Du die Steuerung des Unterrichts web-basiert mithilfe der Schulkonsole in einem Browser vornehmen.

Abb. 424: Schulkonsole als Lehrer nach der Anmeldung

Die Schulkonsole wird im Browser über `https://10.0.0.1` aufgerufen. Je nachdem welcher Benutzer angemeldet ist, erscheinen zugehörige Menüpunkte.

Die Icons haben folgende Bedeutung:

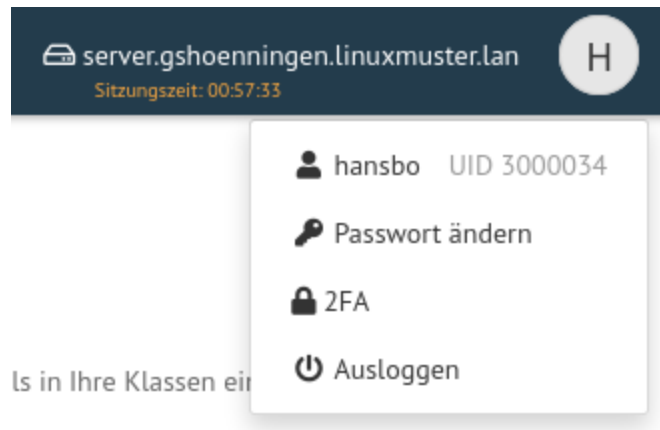


Abb. 425: Profil nach erfolgter Anmeldung

Das Menü kannst Du durch Anklicken der drei Striche links neben dem linuxmuster.net-Symbol ein- und ausblenden.



Abb. 426: oben links: Menü ein- und ausklappen



Abb. 427: angemeldeter Benutzer

Hinweis: Bei Vergabe von Kurs- oder Projektnamen solltest Du auf Umlaute und ß verzichten.

Das Menü der Schulkonsole des Lehrers teilt sich in die Bereiche **Allgemein** und **Klassenzimmer** auf.

4.26.1 Allgemein

Hauptseite

Hier findest Du Informationen zu Deinem Konto, Deinen zugeordneten Benutzergruppen sowie dem Verbrauch Deines Festplattenkontingents (Quota).

 Passwort ändern

Abb. 428: Kennwort ändern

 2FA

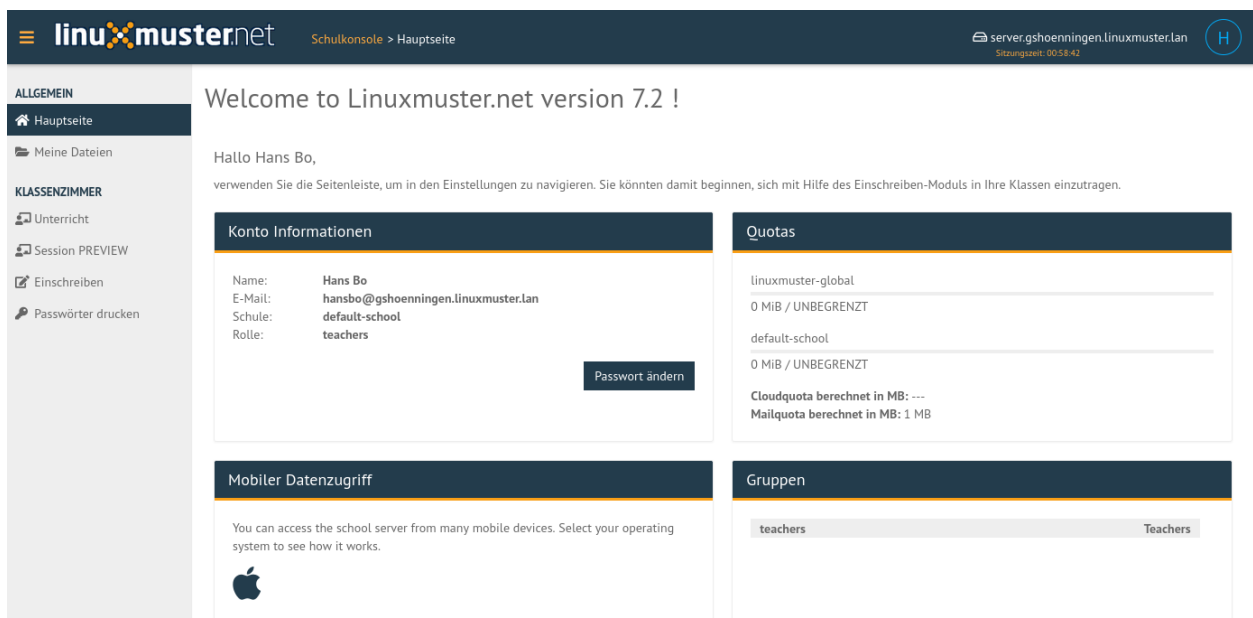
Abb. 429: Aktiviere die Zwei-Faktor-Authentifizierung

 Ausloggen

Abb. 430: Abmelden



Abb. 431: Seitenverhältnis skalieren



The screenshot shows the main interface of the Linuxmuster.net teacher console. At the top, there is a dark header with the 'linuxmuster.net' logo, the current page 'Schulkonsole > Hauptseite', and user information 'server.gshoenningen.linuxmuster.lan' with a session time of '00:58:42'. A sidebar on the left contains navigation links under 'ALLGEMEIN' (Hauptseite, Meine Dateien) and 'KLASSENZIMMER' (Unterricht, Session PREVIEW, Einschreiben, Passwörter drucken). The main content area is titled 'Welcome to Linuxmuster.net version 7.2 !' and greets the user 'Hans Bo'. It provides instructions on using the sidebar and includes four panels: 'Konto Informationen' (showing user details and a 'Passwort ändern' button), 'Quotas' (showing storage and mail quotas), 'Mobiler Datenzugriff' (with an Apple logo and instructions for mobile access), and 'Gruppen' (showing the 'teachers' group).

Abb. 432: Hauptseite als angemeldeter Lehrer

Meine Dateien

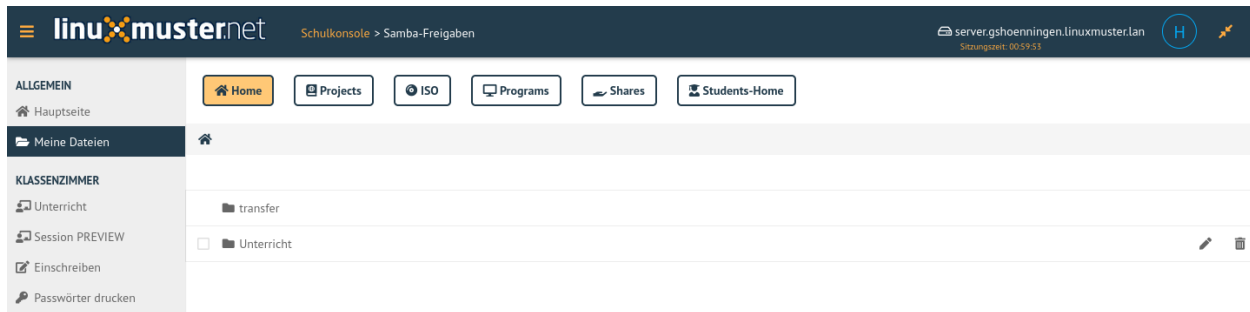


Abb. 433: Meine Dateien als angemeldeter Lehrer

Hier findest Du die Ordner und Dateien, die z.B. im Unterverzeichnis **Unterricht** abgelegt hast und im Unterricht an die Schüler der Klassen verteilen kannst. Das Verzeichnis **transfer** wird u.a. für den Klassenarbeitsmodus benötigt, um Dateien für Klassenarbeiten auszuteilen und die Ergebnisse auch wieder einzusammeln.

4.26.2 Klassenzimmer

Unterricht

Klassen / Kurse, in denen Du Mitglied bist, werden hier aufgelistet.

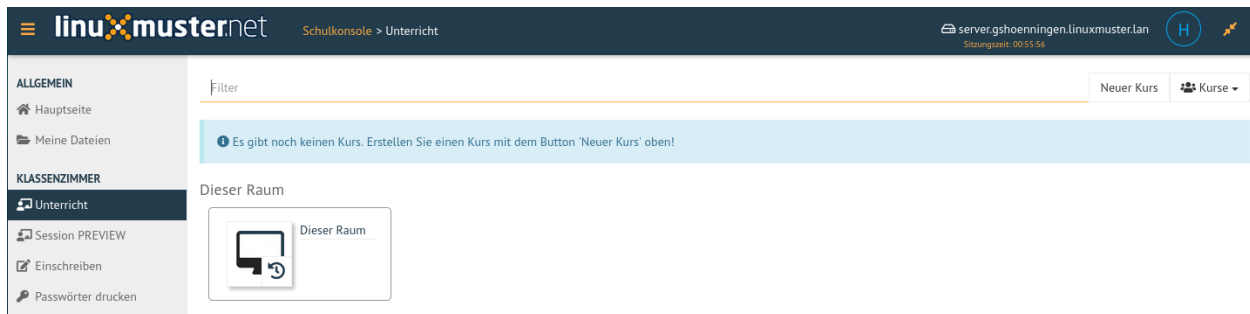


Abb. 434: Unterricht nach der Erstanmeldung als Lehrer

Zu Beginn bist Du noch in keinen Klassen / Kursen oder Projekten eingeschrieben. Schreibe Dich als Lehrer zuerst in den gewünschten Klassen / Kursen ein. Hierzu klickst Du links im Menü auf **Einschreiben** -> **Schulklassen**. Bei den angezeigten Schulklassen setzt Du für diejenigen Klassen einen Haken, in denen Du Dich einschreiben möchtest.

Oben erscheint ein blau hinterlegter Hinweis. Um die Die Einschreibung abzuschließen, musst Du auf **Jetzt ausführen** in dem blauen Hinweissfeld klicken. Verließ die Einschreibung erfolgreich, siehst Du nun im Menüpunkt **Unterricht** Deine Dir zugewiesenen Klassen / Kurse.

Klickst Du nun auf eine Klasse, so wird diese mit den eingetragenen Benutzern zusammengestellt. Es werden alle Benutzer der Klasse dargestellt.

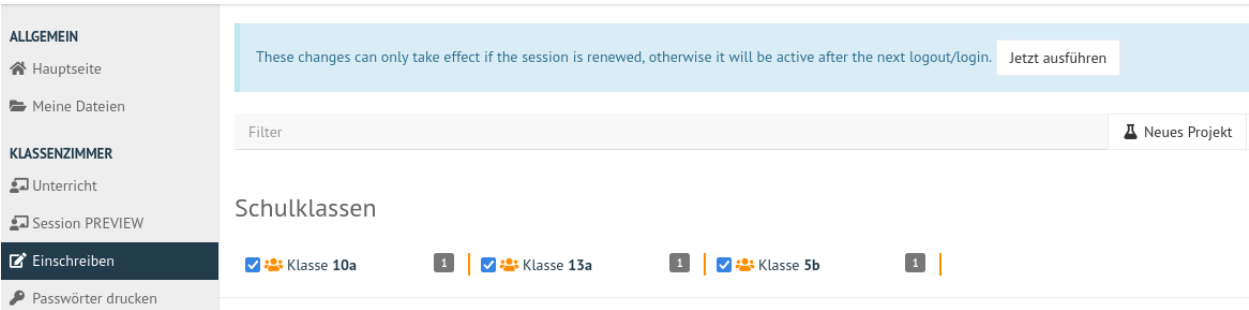


Abb. 435: Einschreibung in Klassen

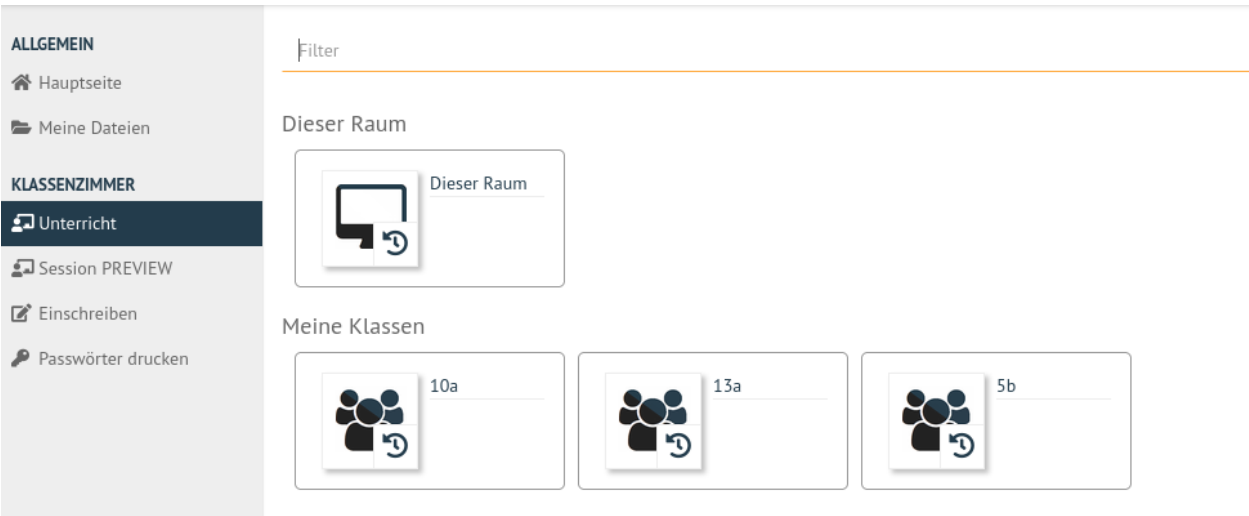


Abb. 436: Eingeschriebene Klassen

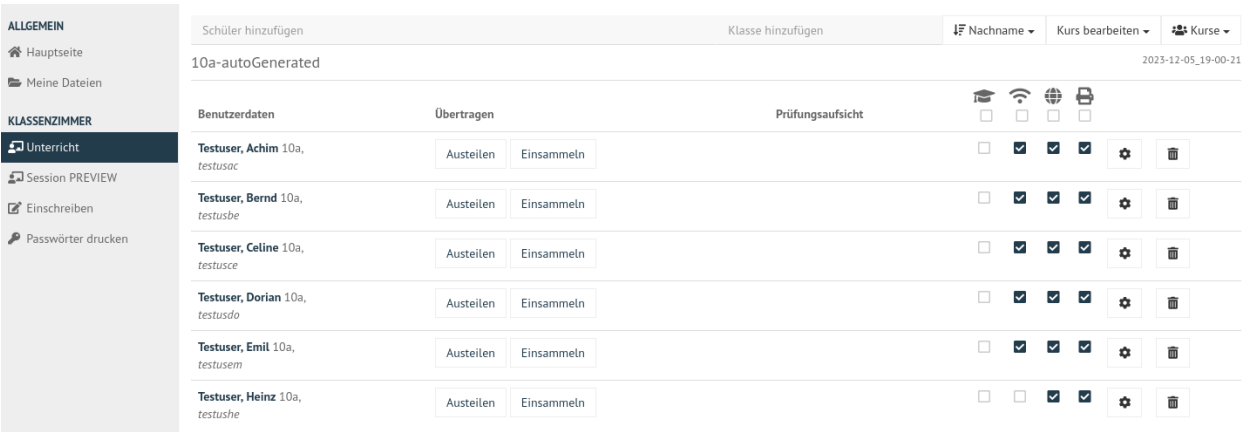


Abb. 437: Ausgewählte Klassen und deren Benutzer

Kurse erstellen

Du kannst über die Funktion oben rechts **Neuer Kurs** einen neuen Kurs anlegen.



Abb. 438: Wähle den Eintrag Neuer Kurs

Gib in dem sich öffnenden Fenster den neuen Kursnamen ein und bestätige diesen mit OK.

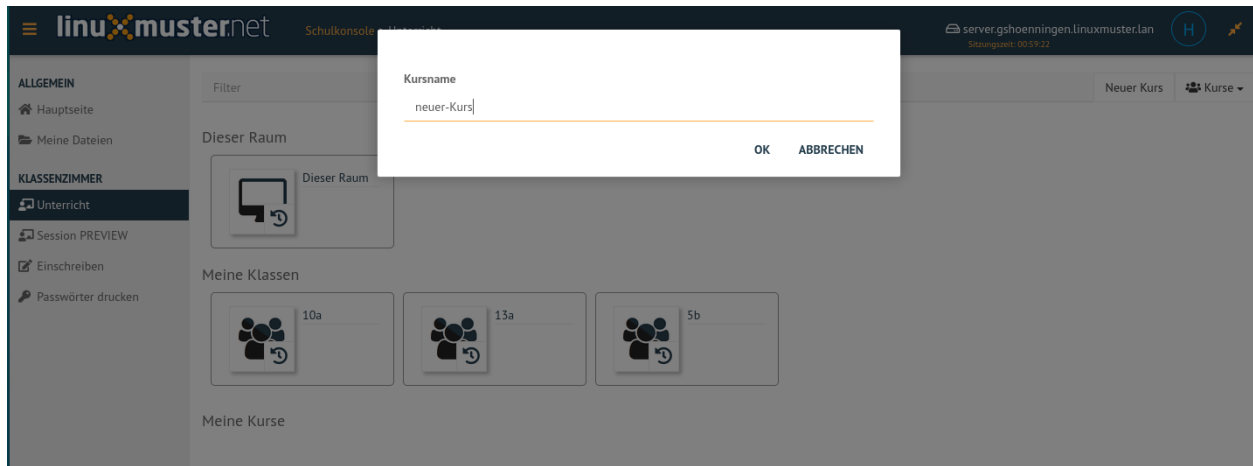


Abb. 439: Neuen Kurs erstellen

Der neu angelegte Kurs erscheint im Menü **Unterricht** -> unter der Rubrik **Meine Kurse**.

Meine Kurse

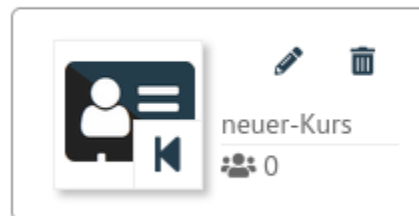


Abb. 440: Meine Kurse

In obiger Abbildung siehst Du, dass in dem neu angelegten Kurs noch keine Schüler zugewiesen wurden.

Schüler einem Kurs hinzufügen

Um Schüler einem Kurs hinzuzufügen, wählst Du den gewünschten Kurse via Klick auf das Icon des Kurses aus.

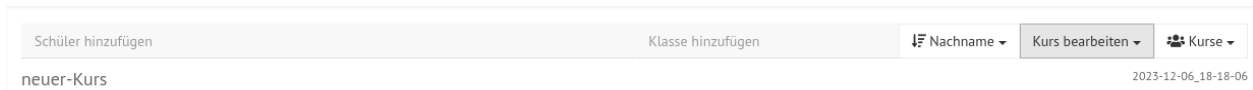


Abb. 441: Ausgewählter Kurs

In den oberen Zeilen gibt es nun die Möglichkeit über **Schüler hinzufügen** einzelne Schüler hinzuzufügen oder über **Klasse hinzufügen** eine ganze Schulklassen dem Kurs hinzuzufügen. Klickst Du in das Feld **Schüler hinzufügen** und gibst dort die **ersten beiden Buchstaben des Schülernamens** ein, erscheint eine Liste mit Schülern, deren Nachnamen mit diesen Buchstaben beginnen.

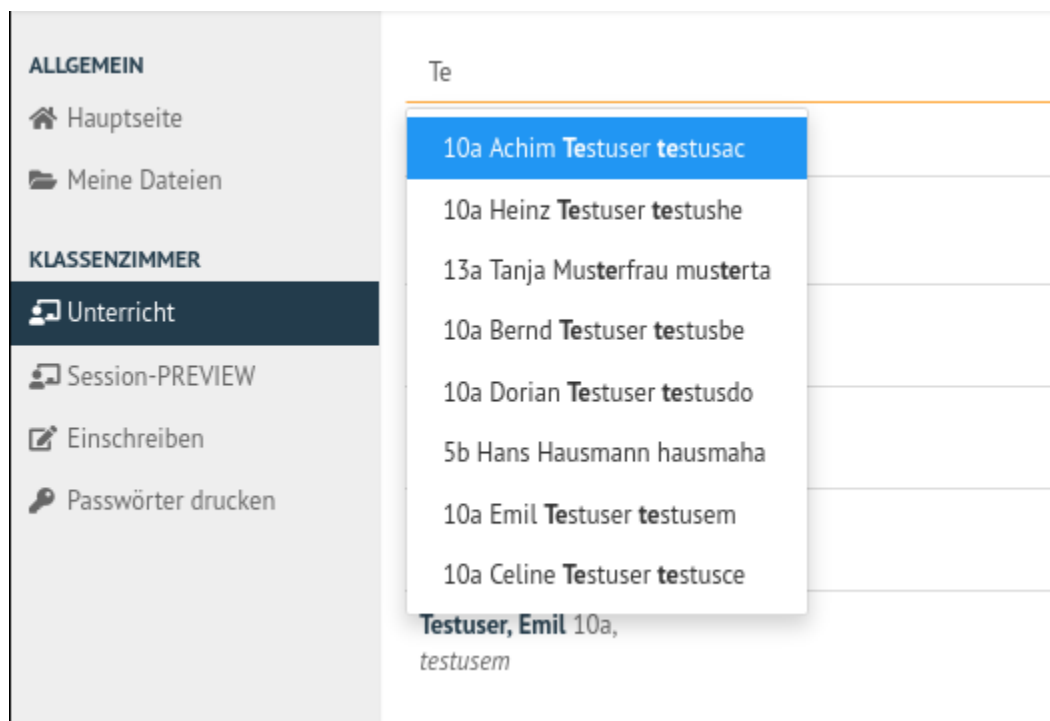


Abb. 442: Ausgewählter Kurs: Schüler hinzufügen

Hast Du alle gewünschten Schüler nacheinander ausgewählt, siehst Du eine Liste mit allen Schülern des Kurses. Um diese in den Kurs zu übernehmen, klickst Du abschließend unten rechts auf **Speichern & übernehmen**.

Wählst Du einen bestimmten Kurs oder eine bestimmte Klasse aus, findest Du folgende Ansicht vor.

In dieser Übersicht können die pädagogischen Funktionen WLAN-, Internet- & Drucker-Freigabe, Dateien-Übertragungs-Funktion und Prüfungsmodus genutzt werden.

Schüler hinzufügen

Klasse hinzufügen

🔍 Nachname ▾

Kurs bearbeiten ▾

👤 Kurse ▾

neuer-Kurs

2023-12-06_18-18-06

Benutzerdaten	Übertragen	Prüfungsaufsicht				
Hausmann, Hans 5b, <i>hausmaha</i>	<div>Austeilen</div> <div>Einsammeln</div>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Musterfrau, Tanja 13a, <i>musterta</i>	<div>Austeilen</div> <div>Einsammeln</div>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Testuser, Bernd 10a, <i>testusbe</i>	<div>Austeilen</div> <div>Einsammeln</div>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Testuser, Emil 10a, <i>testusem</i>	<div>Austeilen</div> <div>Einsammeln</div>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

📄 Teilen ▾

📄 Einsammeln ▾

Schließen

Speichern & übernehmen

WLAN-, Internet-Freigabe & Drucker-Freigabe

- WLAN-Freigabe



Abb. 444: WLAN Icon

- Internet-Freigabe



Abb. 445: Internet Icon

- Drucker-Freigabe



Abb. 446: Drucker Icon

- Prüfungsmodus

Freigaben zu den jeweiligen Diensten können über **Haken setzen oder entfernen** für die jeweiligen Benutzer freigegeben oder gesperrt werden. Über das Kästchen direkt unter einem Dienstsymbol kann die Freigabe oder Sperrung zu dem jeweiligen Dienst auf alle Benutzer angewendet werden.

Beispielsweise wurde hier mit einem Klick unter das WLAN-Symbol für jeden Benutzer des aktuellen Kurses der WLAN-Zugang freigegeben. Dieses muss nur noch unten rechts mit **Speichern & übernehmen** angewendet werden.

- Einstellungen (Zahnrad)

Unter Einstellungen sind verschiedene Optionen zum Passwort des Benutzers zu finden.

- Löschen (Mülleimer)

Mit Hilfe des Mülleiners können einzelne Schüler aus dem Kurs entfernt werden. Dies gilt, bis die Sitzung neu erstellt wird.

Sämtliche Änderungen müssen mit **Speichern & Übernehmen** angewendet werden.

Dateien austeilen & einsammeln

Dateien können für die Unterrichtsarbeit mithilfe der Funktion **Teilen & Einsammeln** an Schüler ausgeteilt und wieder eingesammelt werden.

Auf der Kursseite findest Du im unteren Bereich die Buttons **Teilen** und **Einsammeln**, welche sich auf alle Kursteilnehmer beziehen.

Neben jedem Benutzer selbst gibt es **Austeilen** und **Einsammeln** Funktionen, welche nur auf die einzelnen Benutzer angewendet werden.

Weitere Erläuterungen hierzu findest Du im Abschnitt *Prüfungsmodus*.



Abb. 447: Prüfungs Icon

Benutzerdaten	Übertragen	Prüfungsaufsicht	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Hausmann, Hans 5b, <i>hausmaha</i>	<input type="button" value="Austeilen"/> <input type="button" value="Einsammeln"/>	<input type="checkbox"/>	<input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="button" value="⚙️"/> <input type="button" value="🗑️"/>
Musterfrau, Tanja 13a, <i>musterta</i>	<input type="button" value="Austeilen"/> <input type="button" value="Einsammeln"/>	<input type="checkbox"/>	<input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="button" value="⚙️"/> <input type="button" value="🗑️"/>
Testuser, Bernd 10a, <i>testusbe</i>	<input type="button" value="Austeilen"/> <input type="button" value="Einsammeln"/>	<input type="checkbox"/>	<input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="button" value="⚙️"/> <input type="button" value="🗑️"/>
Testuser, Emil 10a, <i>testusem</i>	<input type="button" value="Austeilen"/> <input type="button" value="Einsammeln"/>	<input type="checkbox"/>	<input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="button" value="⚙️"/> <input type="button" value="🗑️"/>

Abb. 448: WLAN Zugang für alle Kursteilnehmer freigeben



Abb. 449: Einstellungen



Abb. 450: Mülleimer

Datei(en) aus dem Transfer-Verzeichnis dem gesamten Kurs austeilen



Abb. 451: Teilen

Kopiere Transfer-Verzeichnisse des gesamten Kurses
Sammle Transfer-Verzeichnisse des gesamten Kurses ein



Abb. 452: Einsammeln

Benutzerdaten	Übertragen
Testuser, Achim 10a, <i>testusac</i>	<div>Austeilen</div> <div>Einsammeln</div>

Abb. 453: Einsammeln

Prüfungsmodus

Das Absolventenkappen-Symbol



Abb. 454: Prüfungsmodus

stellt den Prüfungsmodus dar. Ausgewählte Schüler oder alle Schüler einer Klasse eines Kurses können dadurch in diesen Modus gesetzt werden (nach Klick auf **Speichern** & **Übernehmen** unten rechts). Im aktivierten Prüfungsmodus wird die Seite wie folgt angezeigt:








Benutzerdaten	Übertragen	Prüfungsaufsicht	
Testuser, Achim 10a-exam, <i>testusac-exam</i>	<div>Austeilen</div> <div>Einsammeln</div>	<div> hansbo</div>	<input checked="" type="checkbox"/>
Testuser, Bernd 10a-exam, <i>testusbe-exam</i>	<div>Austeilen</div> <div>Einsammeln</div>	<div> hansbo</div>	<input checked="" type="checkbox"/>
Testuser, Celine 10a-exam, <i>testusce-exam</i>	<div>Austeilen</div> <div>Einsammeln</div>	<div> hansbo</div>	<input checked="" type="checkbox"/>
Testuser, Dorian 10a-exam, <i>testusdo-exam</i>	<div>Austeilen</div> <div>Einsammeln</div>	<div> hansbo</div>	<input checked="" type="checkbox"/>
Testuser, Emil 10a-exam, <i>testusem-exam</i>	<div>Austeilen</div> <div>Einsammeln</div>	<div> hansbo</div>	<input checked="" type="checkbox"/>
Testuser, Heinz 10a-exam, <i>testushe-exam</i>	<div>Austeilen</div> <div>Einsammeln</div>	<div> hansbo</div>	<input checked="" type="checkbox"/>

Abb. 455: Aktiver Prüfungsmodus

Bei allen Schülern, die im Prüfungsmodus sind, wird unter Prüfungsaufsicht der Name des Lehrers, die den Modus aktiviert hat, mit rotem Hintergrund dargestellt. Schülern im Prüfungsmodus ist automatisch die WLAN-, Internet- & Drucker-Freigabe gesperrt. Dies kann jedoch individuell angepasst werden.

Um den Prüfungsmodus zu beenden, entfernst Du den Haken bei jedem Kursmitglied (Klick unter das Prüfungsmodus-Icon) und übernimmst die Einstellungen mit **Speichern** & **Übernehmen**.

Ausführliche Hinweise zum Prüfungsmodus findest Du im Abschnitt [Prüfungsmodus](#).

Einschreiben

Im Menü Einschreiben findest Du nachstehende drei Rubriken.

Schulklassen



Abb. 456: Schulklassen

Hier werden alle Schulklassen der Schule aufgelistet. Durch Klick auf den Klassennamen werden Dir weitere Informationen angezeigt, wie etwa alle Schüler der Klasse.

Drucker

Hier werden alle Drucker aufgelistet. Durch Anklicken werden weitere Informationen angezeigt.

Ein Auswählen ist nur erforderlich, wenn man den Drucker auch außerhalb des zugehörigen Raumes nutzen möchte.

Projekte

Hier werden alle Projekte aufgelistet. Zu Beginn ist die Liste leer. Du musst zuerst Projekte anlegen und diesen beitreten.

Projekte unterscheiden sich von Kursen:

- Mehrere Lehrer können in eine Projektgruppe aufgenommen werden.
- Projekte verfügen über eigene Tauschverzeichnisse
- Projekte können wiederverwendet werden.
- Unterrichtssteuerung (Passwörter ändern, Internet sperren, etc.) ist **nicht** möglich.

Projekt anlegen

Um ein Projekt anzulegen klickst Du im Menü **Klassenzimmer** -> **Einschreiben** -> **Neues Projekt**.

Es erscheint ein neues Fenster, in dem Du den Namen für das anzulegende Projekt einträgst.

Du darfst nur Kleinbuchstaben und Zahlen in dem Projektnamen verwenden. Bestätige das Anlegen des neuen Projektes mit OK.

Projektmitglieder verwalten

Durch Anklicken eines bestimmten Projekts, werden weitere Informationen angezeigt, wie etwa die Mitglieder und Administratoren des Projekts.

Über die Funktion **Beitretbar** kann die Beitrittmöglichkeit und über die Funktion **Nicht anzeigen** die Sichtbarkeit eingestellt werden. Klicke die Option **Beitretbar** an, damit Benutzer dem Projekt hinzugefügt werden können.

Mitglieder können nun über den Button **Benutzer** oder **Gruppe** hinzufügen dem Projekt zugeordnet werden. Danach erscheint ein Fenster, in dem Du nach Benutzer, Klassen oder Gruppen suchen kannst.

Gruppendetails - 10a

Eigenschaften

Erstellungsdatum:	03 Jan 2023 - 19:28:18
Typ:	adminclass
Schulname:	default-school
Sophomorix-Status:	P
Verteiler:	<input type="checkbox"/>

Gruppenmitglieder: 7 Benutzer und 0 Gruppe(n).

AUSBLENDEN

Mitglieder

Testuser Celine	10a	Testuser Bernd	10a
Testuser Emil	10a	Testuser Dorian	10a
Testuser Achim	10a	Bo Hans	teachers
Testuser Heinz	10a		

Gruppen

Keine Gruppe

Schließen

Abb. 457: Details der Schulklassen

Projekte

i Es gibt noch keine Projekte. Sie können über die Menüleiste ein neues erstellen.

Abb. 458: Projekte

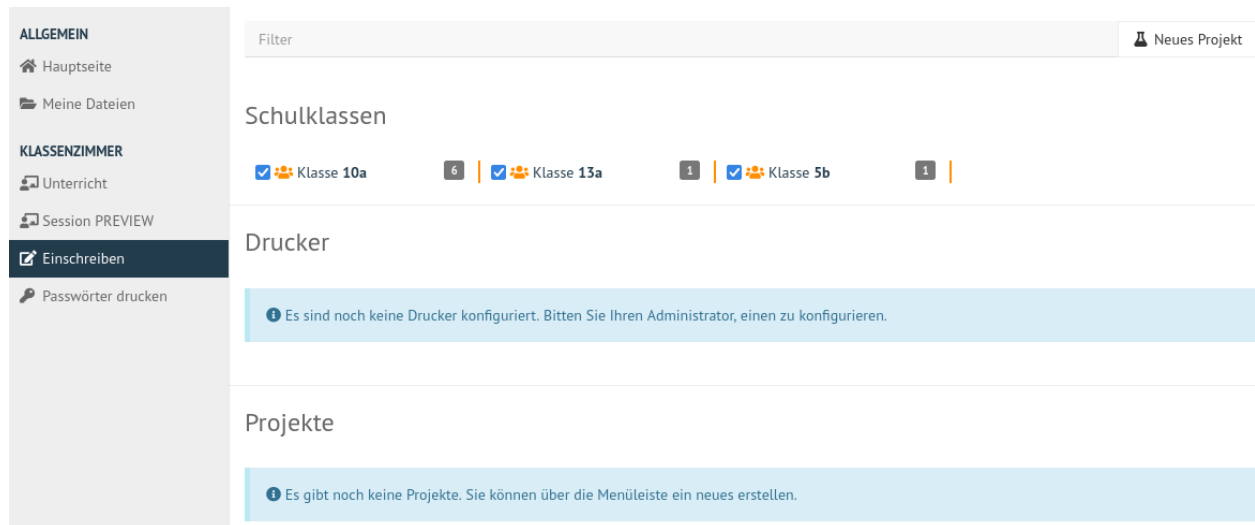


Abb. 459: Neues Projekt anlegen

Projektname

projektklasse10a

OK ABBRECHEN

Abb. 460: Namen für das Projekt festlegen

Gruppendetails - p_projektklasse10a

Eigenschaften

Erstellungsdatum:	07 Dec 2023 - 18:41:49
Typ:	project
Schulname:	default-school
Sophomorix-Status:	P
Beitretbar:	<input type="checkbox"/>
Nicht anzeigen:	<input type="checkbox"/>
Verteiler:	<input type="checkbox"/>

Gruppenadministratoren: 1 Benutzer und 0 Gruppe(n). AUSBLENDEN

Administratoren

Bo Hans

teachers

Gruppen

Keine Gruppe

Gruppenmitglieder: 1 Benutzer und 0 Gruppe(n). AUSBLENDEN

Mitglieder

Bo Hans

teachers

Gruppen

Keine Gruppe

Delete Project

Benutzer oder Gruppe hinzufügen

Schließen

Abb. 461: Weitere Projektinformationen

Beitretbar: ☒

Abb. 462: Projektoption „beitretbar“ setzen

Mitglieder und/oder Gruppen hinzufügen

Nach einem Benutzer suchen

Hans|

teachers Bo **Hans**

5b Hausmann **Hans**

er Klasse auswählen

Geben Sie die Klasse ein, z.B. 10a

Ganze Gruppe hinzufügen

Geben Sie den Gruppennamen ein, z.B. p_wifi

Hinzufügen

- Benutzer Testuser Emil 10a
- Benutzer Testuser Heinz 10a

☐ Add as admin

ÜBERNEHMEN

ABBRECHEN

Abb. 463: Projektmitglieder hinzufügen

Gebe in einer der Zeilen die ersten beiden Anfangsbuchstaben ein und es werden Dir unter Benutzer, Klasse oder Gruppe die bereits existierenden Einträge aufgelistet. Wähle aus der Liste die gewünschten aus. Wiederhole diesen Vorgang für weitere Benutzer oder Gruppen. Die bereits ausgewählten Benutzer oder Gruppen werden Dir unten links in dem Fenster unter der Überschrift **Hinzufügen** aufgelistet. Findest Du hier alle gewünschten Benutzer und Gruppen, klicke auf **Übernehmen**, um diese dem Projekt hinzuzufügen.

Projekt löschen

Klicken auf das jeweilige Projekt und wähle unten links **Projekt löschen**. Bestätige diesen Vorgang im nächsten Fenster mit **LÖSCHEN**.

Passwörter drucken

Hier gibt es die Möglichkeit, eine übersichtliche Liste von Benutzer- & Passwortinformationen im PDF- oder CSV-Format ausdrucken zu lassen bzw. als Datei herunterzuladen.

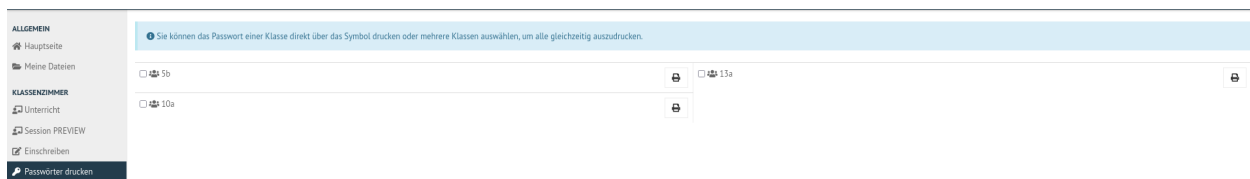


Abb. 464: Übersicht der Klassen zum Ausdruck der Passwörter

Der Druck der Passwörter kann durch Anklicken der jeweiligen Klasse klassenspezifisch erfolgen. Markiere die Klasse und klicke auf das Druckersymbol in der Zeile der Klasse. Es erscheint ein neues Fenster.



Abb. 465: Passwörter der Klasse als PDF ausdrucken

Wähle die gewünschten Einstellungen aus und es wird die erstellte Datei heruntergeladen und angezeigt.

Im PDF-Format werden die Benutzer neben dem zugehörigen Passwort in Kästchen angezeigt, wie in diesem Beispiel:

Zugangsdatenliste		10a	29. April 2019
Fray, Katrin Klasse: 10a Passwort: vdK4YciLx(Login: frayka	Gengler, Felix Klasse: 10a Passwort: ==7NjUcYnm Login: genglefe	Ilkes, Judith Klasse: 10a Passwort: (KA)P=KVb9 Login: ilkesju	Imbrogiana, Henriette Klasse: 10a Passwort: BMg&vMV!b3 Login: imbroghe
Krüger, Richard Klasse: 10a Passwort: p(uRKebk)9 Login: kruegeri	_____	_____	_____

Abb. 466: PDF-Datei mit den Passwörtern der Schüler der Klasse

4.27 Prüfungsmodus

Autor des Abschnitts: @cweikl, @MachtDochNix (pics)

In einem Kurs / einer Klasse können Schülerkonten in den Prüfungsmodus versetzt werden, ebenso kann man mit oder ohne Prüfungsmodus Schülern Dateien austeilen und von dort wieder einsammeln. Voraussetzung für diese Funktionen ist die *Aufnahme des Schülers* in einen Kurs.

Öffne in der Schulkonsole unter KLASSENZIMMER -> Session-PREVIEW den angelegten Kurs oder die gewünschte Klasse.

ALLGEMEIN
 🏠 Hauptseite
 📁 Meine Dateien
KLASSENZIMMER
 🗣️ Unterricht
Session-PREVIEW
 ✍️ Einschreiben
 🔑 Passwörter drucken


This plugin is actually under heavy development and only published for tests purpose.


Filter

Dieser Raum

Es konnte nicht ermittelt werden, in welchem Raum Sie sich befinden. Sind Sie an einem Schulrechner angemeldet ?

Meine Klassen


 5b
 👤 1


 10a
 👤 6



 13a
 👤 1

Abb. 467: Starte die Session für die Klasse

Die Liste mit Schülern des Kurses wird angezeigt.

Der Prüfungsmodus wird aktiviert, indem Du auf das Prüfungssymbol klickst. Du erhältst in einem neuen Fenster die

ALLGEMEIN

Hauptseite

Meine Dateien

KLASSENLEHRER

Unterricht

Session-PREVIEW

Einschreiben

Passwörter drucken

This plugin is actually under heavy development and only published for testing purposes.

Schüler hinzufügen

Klasse hinzufügen

IF Nachname

Gruppe speichern als

Benutzer	Übertragen	Arbeitsverzeichnis						
Testuser, Achim testuac	Teilen Einsammeln	transfer/hansbo/_collect						
Testuser, Bernd testuac	Teilen Einsammeln							
Testuser, Celine testuac	Teilen Einsammeln							
Testuser, Dorian testuac	Teilen Einsammeln							
Testuser, Emil testuac	Teilen Einsammeln							
Testuser, Heinz testuac	Teilen Einsammeln							

Abb. 468: Teilnehmer der ausgewählten

Rückfrage, ob Du den Prüfungsmodus wirklich starten möchtest. Bestätige dies mit einem Klick auf **PRÜFUNGSMODUS STARTEN**.

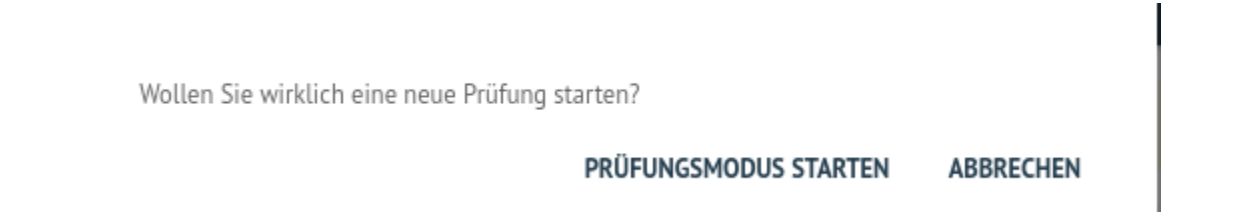


Abb. 469: Starte den Prüfungsmodus

Wurde der Prüfungsmodus aktiviert, so erkennst Du in der Spalte mit dem Prüfungssymbol pro Teilnehmer ein rotes Rechteck mit dem Prüfungssymbol und dem Namen des Lehrers, der für diese Teilnehmer den Prüfungsmodus aktiviert hat.

Benutzer	Übertragen	Arbeitsverzeichnis						
Testuser, Achim testuac-exam	Teilen Einsammeln	transfer/hansbo/_collect						
Testuser, Bernd testuac-exam	Teilen Einsammeln							
Testuser, Celine testuac-exam	Teilen Einsammeln							
Testuser, Dorian testuac-exam	Teilen Einsammeln							
Testuser, Emil testuac-exam	Teilen Einsammeln							
Testuser, Heinz testuac-exam	Teilen Einsammeln							

Abb. 470: Aktivierter Prüfungsmodus

4.27.1 Prüfungsmodus = Klassenarbeitsmodus

Bei Aktivierung des Prüfungsmodus wird für jedes Schülerkonto ein neues Konto angelegt mit dem bisherigen Kontonamen mit angehängter Zeichenkette `-exam`. Ebenso wird der Schüler in eine zugehörige Klasse „-exam“ gesetzt (siehe Abbildung). Das Passwort zur Anmeldung wird dabei übernommen.

In o.g. Abbildung müsste sich der Benutzer Achim Testuser nun mit dem Login `testuac-exam` und seinem bisherigen Kennwort am Client-PC anmelden. Zum Zeitpunkt des aktivierten Prüfungsmodus wurde die Klasse `10a-exam` angelegt.

Die Prüfungsaufsicht übernimmt der Lehrer, der den Prüfungsmodus aktiviert hat. Dies ist in den roten Rechtecken zu erkennen.

Benutzer	
6 Schüler	
Testuser, Achim <i>testusac-exam</i>	10a-exam
Testuser, Bernd <i>testusbe-exam</i>	10a-exam
Testuser, Celine <i>testusce-exam</i>	10a-exam
Testuser, Dorian <i>testusdo-exam</i>	10a-exam
Testuser, Emil <i>testusem-exam</i>	10a-exam
Testuser, Heinz <i>testushe-exam</i>	10a-exam

Abb. 471: Angelegte Schüleraccounts im Prüfungsmodus

Der Prüfungsmodus bleibt so lange erhalten, bis der Lehrer (oder auch ein anderer Lehrer) den Haken bei dem Schülerkonto entfernt.



Abb. 472: Beende den Prüfungsmodus

Klicke zum Beende des Prüfungsmodus auf der rot hinterlegte Prüfungssymbol.

Möchten Sie die aktuelle Prüfung wirklich beenden?

PRÜFUNGSMODUS BEENDEN **ABBRECHEN**

Abb. 473: Bestätige das Beendes Prüfungsmodus

Du erhältst ein Fenster mit der Nachfrage, ob die den Prüfungsmodus wirklich beenden möchtest. Hast Du alle gewünschten Daten der Prüflinge zuvor eingesammelt, bestätige diesen Vorgang mit **PRÜFUNGSMODUS BEENDEN**.

Benutzer		Übertragen	Arbeitsverzeichnis						
 Schüler			transfer/hansbo/_collect						
Testuser, Achim testusac	10a	 Teilen  Einsammeln				<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Testuser, Bernd testusbe	10a	 Teilen  Einsammeln				<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Testuser, Celine testusce	10a	 Teilen  Einsammeln				<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Testuser, Dorian testusdo	10a	 Teilen  Einsammeln				<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Testuser, Emil testusem	10a	 Teilen  Einsammeln				<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Testuser, Heinz testushe	10a	 Teilen  Einsammeln				<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Abb. 474: Prüfungsmodus beendet

Nachdem der Prüfungsmodus beendet wurde, werden alle Benutzer wie zuvor dargestellt und die Nutzung des Internet sowie der Drucker automatisch aktiviert.

Ablauf der Prüfung

- 1. Der Lehrer meldet sich an der Schulkonsole an.
- 2. Der Lehrer wählt unter Session-PREVIEW die gewünschte Klasse aus.
- 3. Der Lehrer aktiviert mit dem Prüfungssymbol den Prüfungsmodus.
- 4. Der Lehrer teilt den Prüflingen im Raum mit wie diese sich am PC für die Prüfung anmelden müssen (<bisherigsLogin>+“-exam“ & bisheriges Kennwort).
- 5. Der Lehrer teilt die Prüfungs und ggf. weitere Vorlagen an die Prüfungsteilnehmer aus.

6. Die Dateien liegen für die Prüfungsteilnehmer im Verzeichnis `transfer/LEHRER/_collect`.
7. Schüler nutzen die bereitgestellten Daten und erstellen ihre Lösungen.
8. Schüler speichern die bearbeiteten Daten unter einem vorher vom Lehrer mitgeteilten Namen bzw. Namensschema ab und lege diese zur Abgabe in das Verzeichnis `transfer/LEHRER/_collect`.
9. Der Lehrer sammelt zum Abschluss der Prüfung alle Abgaben mit dem Button `von allen einsammeln` ein.
10. Der Lehrer überprüft die eingesammelten Daten, die für diesen im Ordner `transfer/collected/` zu finden sind.
11. Liegen alle Daten wie gewünscht vor, beendet der Lehrer den Prüfungsmodus.

4.27.2 Austeilen und Einsammeln

Lehrer

Hast Du als Lehrer, wie zuvor beschrieben, für die gewünschte Klasse den Prüfungsmodus aktiviert, siehst Du folgende Anzeige:

Benutzer	Übertragen	Arbeitsverzeichnis	
6 Schüler		transfer/hansbo/_collect	
Testuser, Achim testusac-exam	10a-exam	Teilen Einsammeln	hansbo
Testuser, Bernd testusbe-exam	10a-exam	Teilen Einsammeln	hansbo
Testuser, Celine testusce-exam	10a-exam	Teilen Einsammeln	hansbo
Testuser, Dorian testusdo-exam	10a-exam	Teilen Einsammeln	hansbo
Testuser, Emil testusem-exam	10a-exam	Teilen Einsammeln	hansbo
Testuser, Heinz testushe-exam	10a-exam	Teilen Einsammeln	hansbo

Abb. 475: Prüfungsmodus aktiviert

Stellen nun den Prüflingen die Prüfung bzw. Vorlagendateien bereit. Klicke hierzu unten links auf den Button `Mit allen teilen`.



Abb. 476: Dateien bereitstellen

Es öffnet sich ein neues Fenster, in dem Dir der Inhalt Deines Home-Verzeichnisses dargestellt wird.

Sollten die gewünschten Dateien noch nicht in Deinem Ordner sein, klickst Du oben rechts auf das Wolkensymbol, um Dateien von Deinem USB-Stick oder dem lokalen PC in Dein Home-Verzeichnis hochzuladen.

Die hochgeladenen Dateien werden Dir ebenfalls hier angezeigt.

Aktiviere nun die gewünschten Dateien und /oder Verzeichniss, die Du den Prüflingen austeilen möchtest.

Um die Dateien auszuteilen, klickst Du nun unten rechts auf `TEILEN`.

Teile Dateien an alle Teilnehmer aus dem Verzeichnis transfer

Wählen Sie Dateien aus, die Sie teilen möchten



0 ausgewählte(s) Element(e)



 collected



TEILEN

ABBRECHEN

Abb. 477: Dateien bereitstellen: Verzeichnisansicht

Teile Dateien an alle Teilnehmer aus dem Verzeichnis transfer

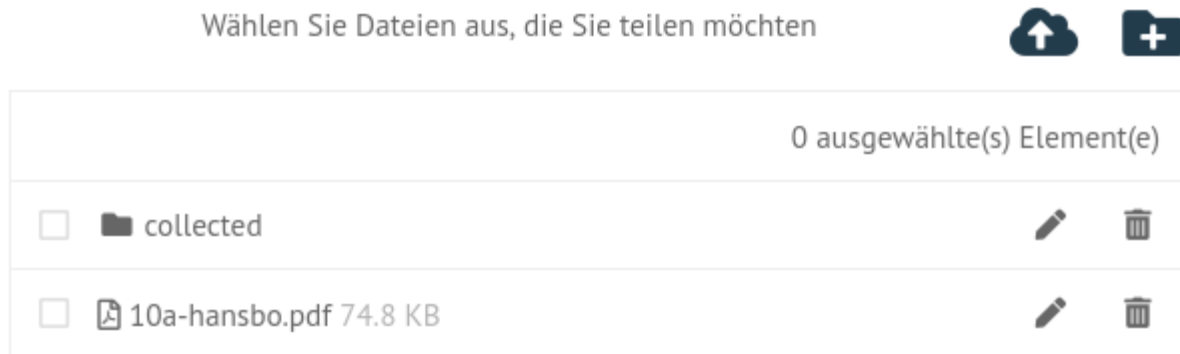


Abb. 478: Dateien bereitstellen: Auflistung der Dateien im Home-Verzeichnis

Bist Du als Lehrer an einem Client angemeldet, so findest Du die zu teilenden Daten unter Deinem Home-Laufwerk `H:\` im Unterverzeichnis `transfer`.

Prüflinge

1. Nachdem der Lehrer den Prüflingen ihre Prüfungs-Accounts mitgeteilt hat, melden diese sich mit den Daten an.
2. Der Prüfling geht im Dateiverzeichnis in sein Home-Laufwerk (`H:`) in den Transfer-Ordner, dort in den Ordner des Lehrers der Prüfung.
3. Im Ordner `H:transferLEHRER` werden die bereitgestellten Dateien in ein anderes Verzeichnis übernommen, dort bearbeitet und gespeichert.
4. Bei Abschluss der Prüfung kopiert der Prüfling zur Abgabe die bearbeiteten Dateien in das Verzeichnis `H:\transfer\LEHRER_collect\`.
5. Der Lehrer sammelt alle abgegebene Dateien ein und schließt die Prüfung.
6. Der Prüfling meldet sich ab.

Anmeldung

Jeder Prüfling meldet sich an dem Client an. Hierzu ist der bisherige Login + die Erweiterung `-exam` und das bisherige Kennwort anzugeben. Nachstehende Abbildungen verdeutlichen dies einmal für einen Windows-Client und für einen Ubuntu-Client:

Nach erfolgreicher Anmeldung am Client sieht der Prüfling die Einrichtung der Prüfungsumgebung.

An einem 22.04 Ubuntu-Client mit Gnome sieht die Anmeldung wie folgt aus:

Angabe des Kennworts.







Hat sich der Prüfling erfolgreich am Client angemeldet und ruft den Dateimanager auf, so sieht dieser folgende Netzlaufräume:

Die bereitgestellten Dateien findet der Prüfling nun im Verzeichnis `H:\transfer\LEHRER\`.

Teile Dateien an alle Teilnehmer aus dem Verzeichnis transfer

Wählen Sie Dateien aus, die Sie teilen möchten



1 ausgewählte(s) Element(e)		
<input type="checkbox"/>	 collected	 
<input checked="" type="checkbox"/>	 10a-hansbo.pdf 74.8 KB	 

TEILEN**ABBRECHEN**

Abb. 479: Dateien bereitstellen: Aktiviere die bereitzustellenden Dateien

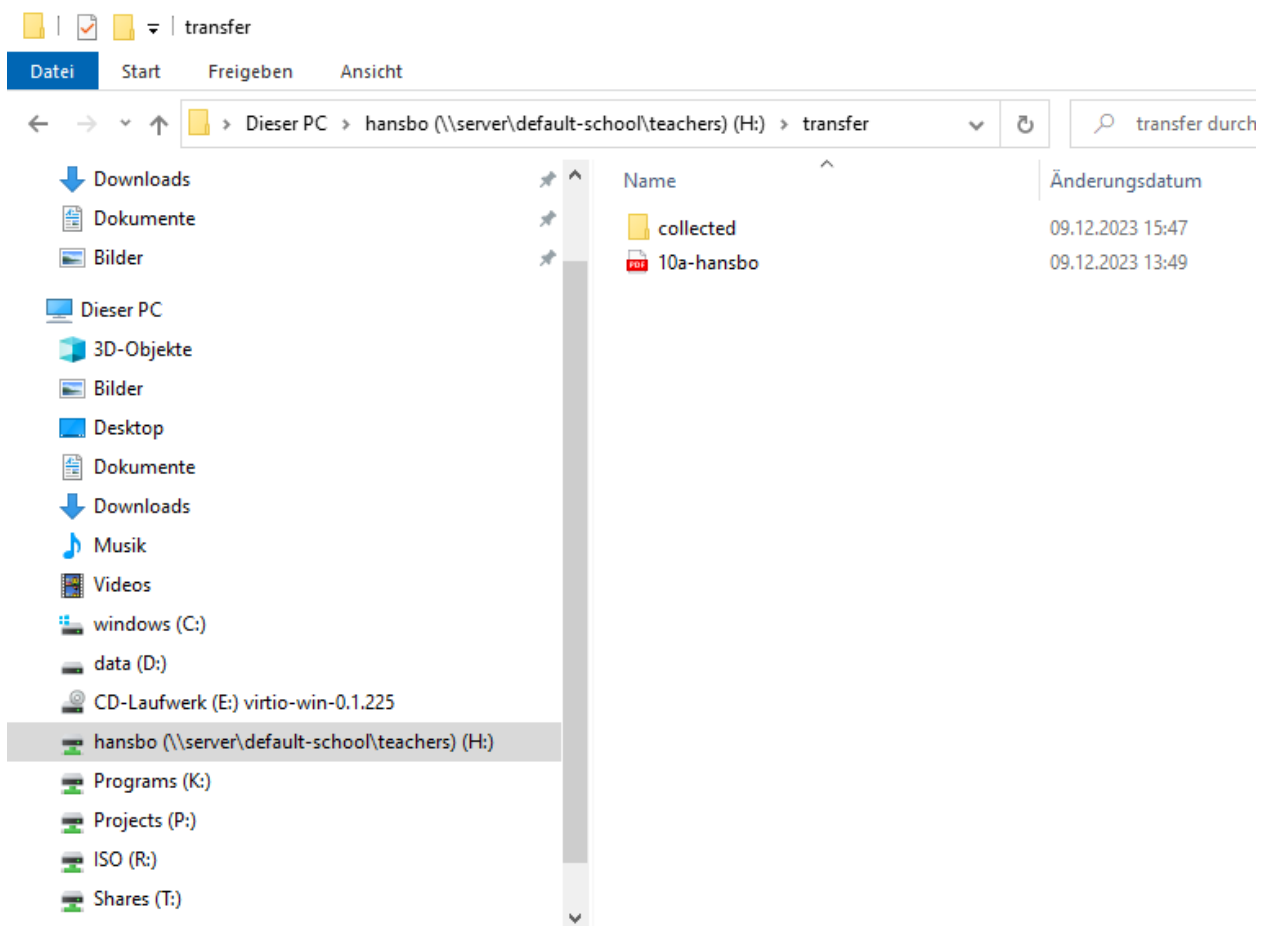


Abb. 480: Zu teilende Daten am Client

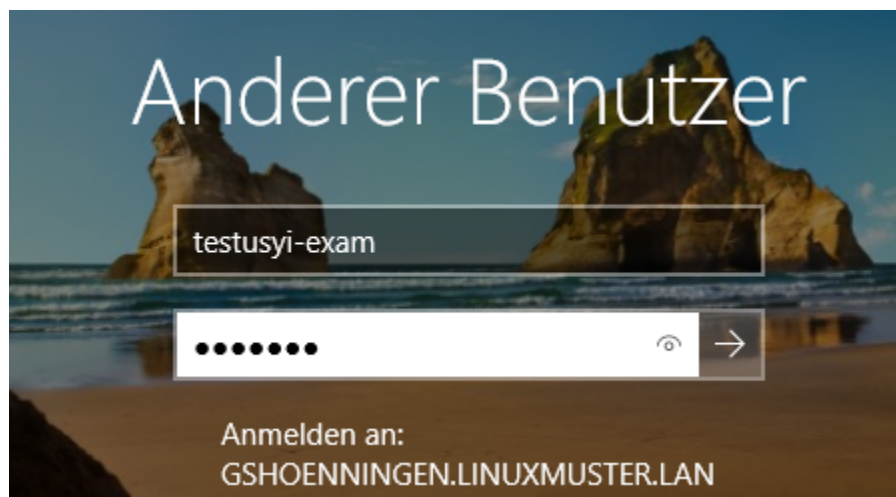


Abb. 481: Prüfungsanmeldung Windows-Client



Abb. 482: Prüfungsanmeldung Windows-Client - Setup

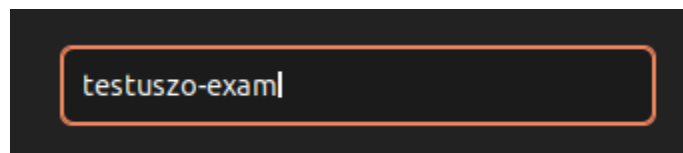


Abb. 483: Prüfungsanmeldung Ubuntu-Client

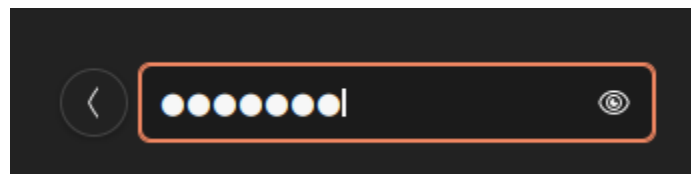


Abb. 484: Prüfungsanmeldung Ubuntu-Client - Eingabe des Kennworts

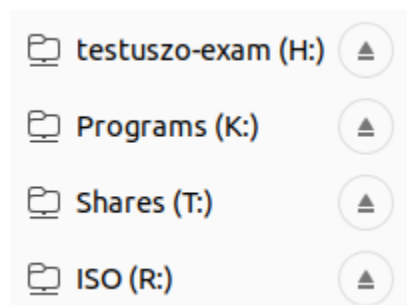


Abb. 485: Prüfungsanmeldung: Netzwerklaufwerke

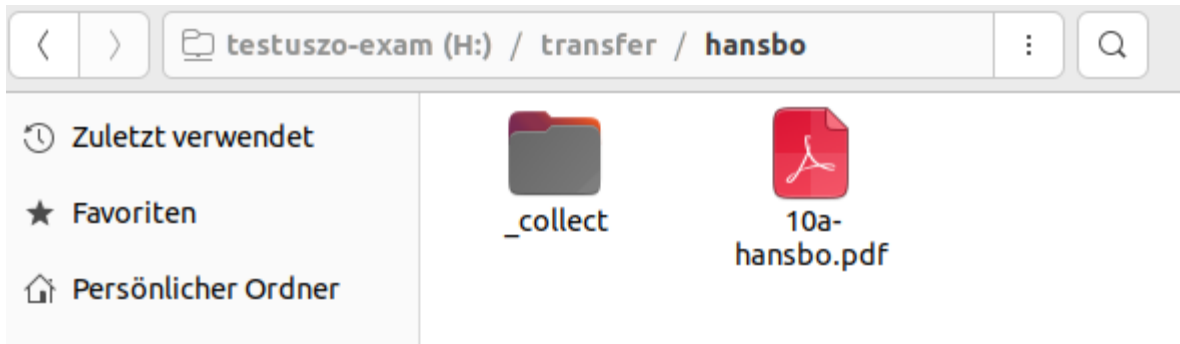


Abb. 486: Prüfung: Bereitgestellte Dateien

In der Prüfung bearbeitet der Prüfling die bereitgestellten Dateien und speichert seine Lösung zur Abgabe in dem Verzeichnis `H:\transfer\LEHRER_collect\`.

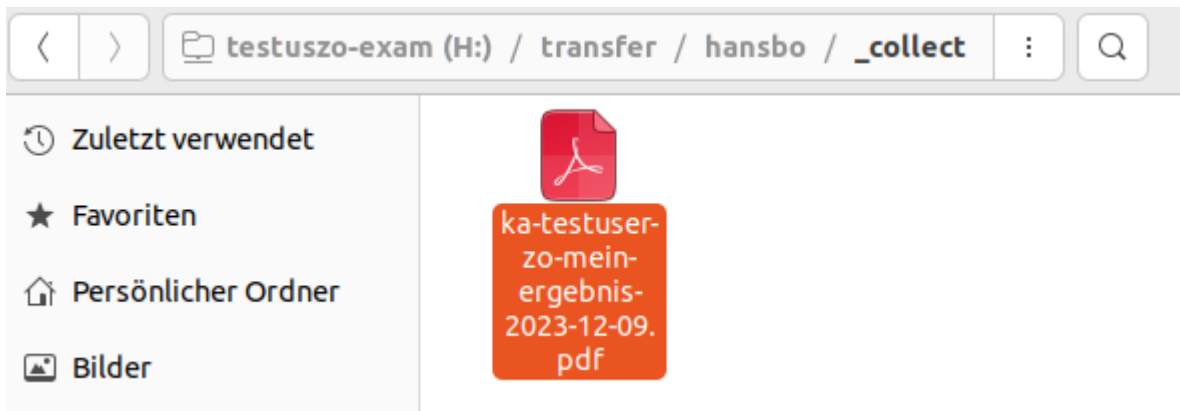


Abb. 487: Prüfung: Dateiabgabe

Unter Windows stellt sich dies für den Prüfling wie folgt dar:

Netzwerkfreigaben

Bereitgestellte Dateien

Abgabe unter `H:\transfer\LEHRER_collect\`

Abgaben einsammeln

Der Lehrer sieht in der Schulkonsole die abgegebenen Dateien.

Um vor Abschluss der Prüfung alle Abgaben einzusammeln, klickst Du unten links auf **Von allen einsammeln**. Klicke nun auf **Move _collect cirectory from all members**. Es werden nun alle Abgaben in das Verzeichnis des Lehrers zum Einsammeln der Dateien verschoben.

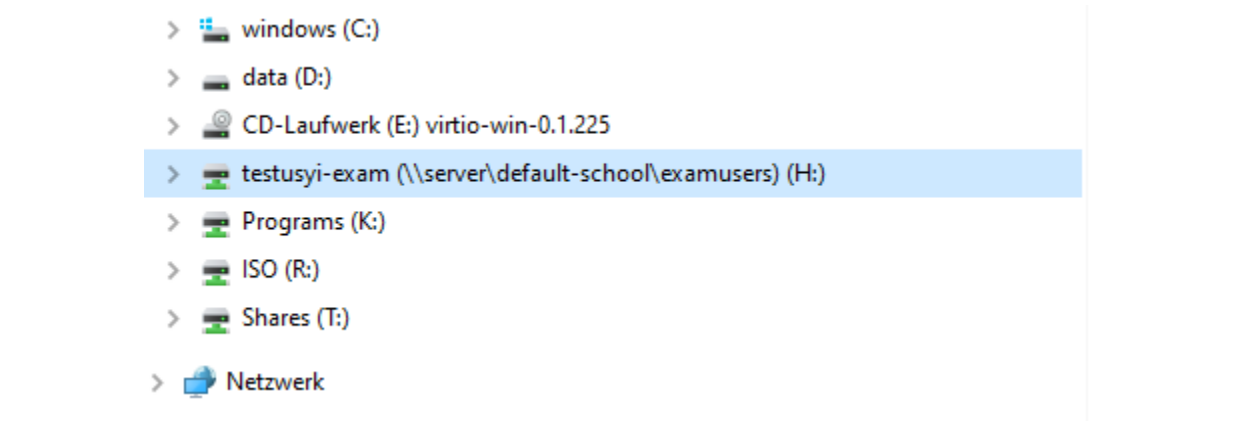


Abb. 488: Prüfung: Netzwerkfreigaben unter Windows

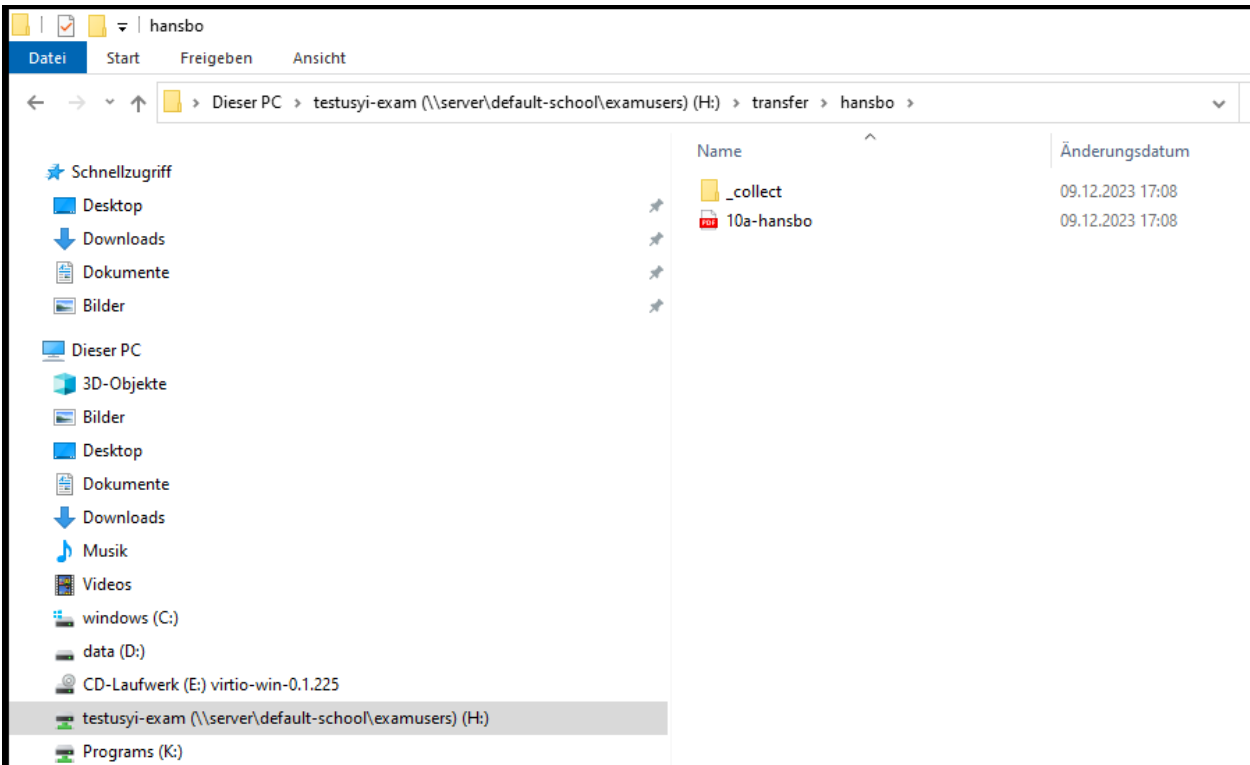


Abb. 489: Prüfung: Bereitgestellte Dateien unter Windows

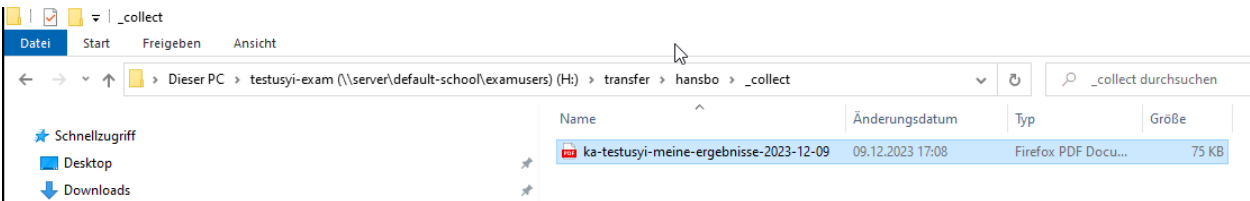


Abb. 490: Prüfung: Dateiabgabe unter Windows

Benutzer	Übertragen	Arbeitsverzeichnis	
<div>8 Schüler</div>		transfer/hansbo/_collect	
Testuser, Achim <i>testusac-exam</i>	<div>Teilen</div> <div>Einsammeln</div>		hansbo
Testuser, Bernd <i>testusbe-exam</i>	<div>Teilen</div> <div>Einsammeln</div>		hansbo
Testuser, Celine <i>testusce-exam</i>	<div>Teilen</div> <div>Einsammeln</div>		hansbo
Testuser, Dorian <i>testusdo-exam</i>	<div>Teilen</div> <div>Einsammeln</div>		hansbo
Testuser, Emil <i>testusem-exam</i>	<div>Teilen</div> <div>Einsammeln</div>		hansbo
Testuser, Heinz <i>testushe-exam</i>	<div>Teilen</div> <div>Einsammeln</div>		hansbo
Testuser, Yilzin <i>testusyi-exam</i>	<div>Teilen</div> <div>Einsammeln</div>	<div>ka-testusyi-meine-ergebnisse-2023-12-09.pdf 74.8 KB</div>	hansbo
Testuser, Zoran <i>testuszo-exam</i>	<div>Teilen</div> <div>Einsammeln</div>	<div>ka-testuser-zo-mein-ergebnis-2023-12-09.pdf 74.8 KB</div>	hansbo

Abb. 491: Prüfung: abgegebene Dateien einsehen

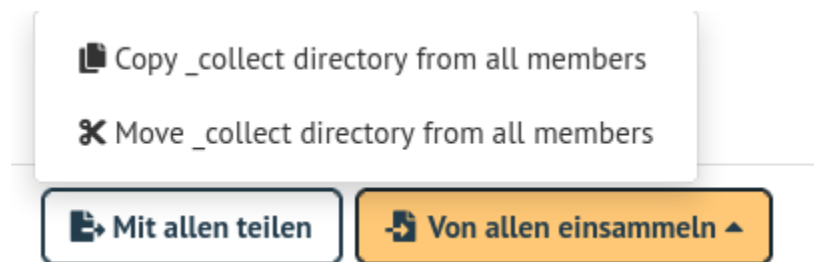


Abb. 492: Prüfung: Alle Dateien einsammeln

Prüfung beenden

Nachdem alle Dateien eingesammelt wurden, beendet der Lehrer den Prüfungsmodus.

Benutzer	Übertragen	Arbeitsverzeichnis	
8 Schüler		transfer/hansbo/_collect	
Testuser, Achim <i>testusac-exam</i>	10a-exam Teilen Einsammeln		hansbo
Testuser, Bernd <i>testusbe-exam</i>	10a-exam Teilen Einsammeln		hansbo
Testuser, Celine <i>testusce-exam</i>	10a-exam Teilen Einsammeln		hansbo
Testuser, Dorian <i>testusdo-exam</i>	10a-exam Teilen Einsammeln		hansbo
Testuser, Emil <i>testusem-exam</i>	10a-exam Teilen Einsammeln		hansbo
Testuser, Heinz <i>testushe-exam</i>	10a-exam Teilen Einsammeln		hansbo
Testuser, Yilzin <i>testusyi-exam</i>	10a-exam Teilen Einsammeln		hansbo
Testuser, Zoran <i>testuszo-exam</i>	10a-exam Teilen Einsammeln		hansbo

Abb. 493: Prüfung: beenden

Hierzu klickst Du auf das rot hinterlegte Prüfungssymbol.

Abgaben einsehen

Hast Du als Lehrer die Prüfung beendet, kannst Du nun in der Schulkonsole unter Allgemein -> Meine Dateien im Ordner transfer alle bislang eingesammelten Dateien finden.

Für die durchgeführte Prüfung gehst Du in den Ordner schoolclass_10a_20231209-171650 - also immer der Ordner mit dem aktuellen Prüfungsdatum.

Dort findest Du pro Prüfling einen Ordner, in dem sich die abgegebenen Dateien befinden.

Die Abgaben kannst Du markieren und herunterladen.

4.28 Zugriff auf WLAN, Internet und Drucker regeln

In einer Klasse und einem Kurs kann einzelnen Personen oder dem gesamten Kurs / der Klasse die Berechtigung zu Drucken oder der Zugriff auf WLAN und Internet gegeben oder genommen werden. Voraussetzung für diese Funktionen ist die *Aufnahme des Schülers* in einen Kurs.

Öffne in der Schulkonsole unter KLASSENZIMMER -> Session-PREVIEW wähle die gewünschte Klasse oder den gewünschten Kurs.

Es wird Liste mit Schülern des Kurses bzw. der Klasse angezeigt.

Für jeden einzelnen und für alle Schüler können folgende Funktionen aktiviert oder deaktiviert werden:

- den Prüfungsmodus (siehe *Prüfungsmodus*)
- WLAN-Zugang

ALLGEMEIN Hauptseite	Home Projects ISO Programs Shares Students-Home
Meine Dateien	/ transfer / collected
KLASSENZIMMER Unterricht Session-PREVIEW Einschreiben Passwörter drucken	<div> <input type="checkbox"/> <div>EXAM_10a-exam_testusac-exam_ENDED_FROM_hansbo_2023-12-07_19h22m21</div> </div> <div> <input type="checkbox"/> <div>EXAM_10a-exam_testusbe-exam_ENDED_FROM_hansbo_2023-12-07_19h22m21</div> </div> <div> <input type="checkbox"/> <div>EXAM_10a-exam_testusce-exam_ENDED_FROM_hansbo_2023-12-07_19h22m21</div> </div> <div> <input type="checkbox"/> <div>EXAM_10a-exam_testusdo-exam_ENDED_FROM_hansbo_2023-12-07_19h22m21</div> </div> <div> <input type="checkbox"/> <div>EXAM_10a-exam_testusem-exam_ENDED_FROM_hansbo_2023-12-07_19h22m21</div> </div> <div> <input type="checkbox"/> <div>EXAM_10a-exam_testushe-exam_ENDED_FROM_hansbo_2023-12-07_19h22m21</div> </div> <div> <input type="checkbox"/> <div>EXAM_schoolclass_10a_2023-12-09_13h23m23</div> </div> <div> <input type="checkbox"/> <div>EXAM_schoolclass_10a_2023-12-09_15h47m37</div> </div> <div> <input type="checkbox"/> <div>schoolclass_10a_20231209-171650</div> </div>

Abb. 494: Prüfung: Prüfe Dateiabgaben

<input type="checkbox"/> <div>ka-testusyi-meine-ergebnisse-2023-12-09.pdf 74.8 KB</div>	Download Edit Delete
---	--

Abb. 495: Prüfung: Dateiabgaben herunterladen

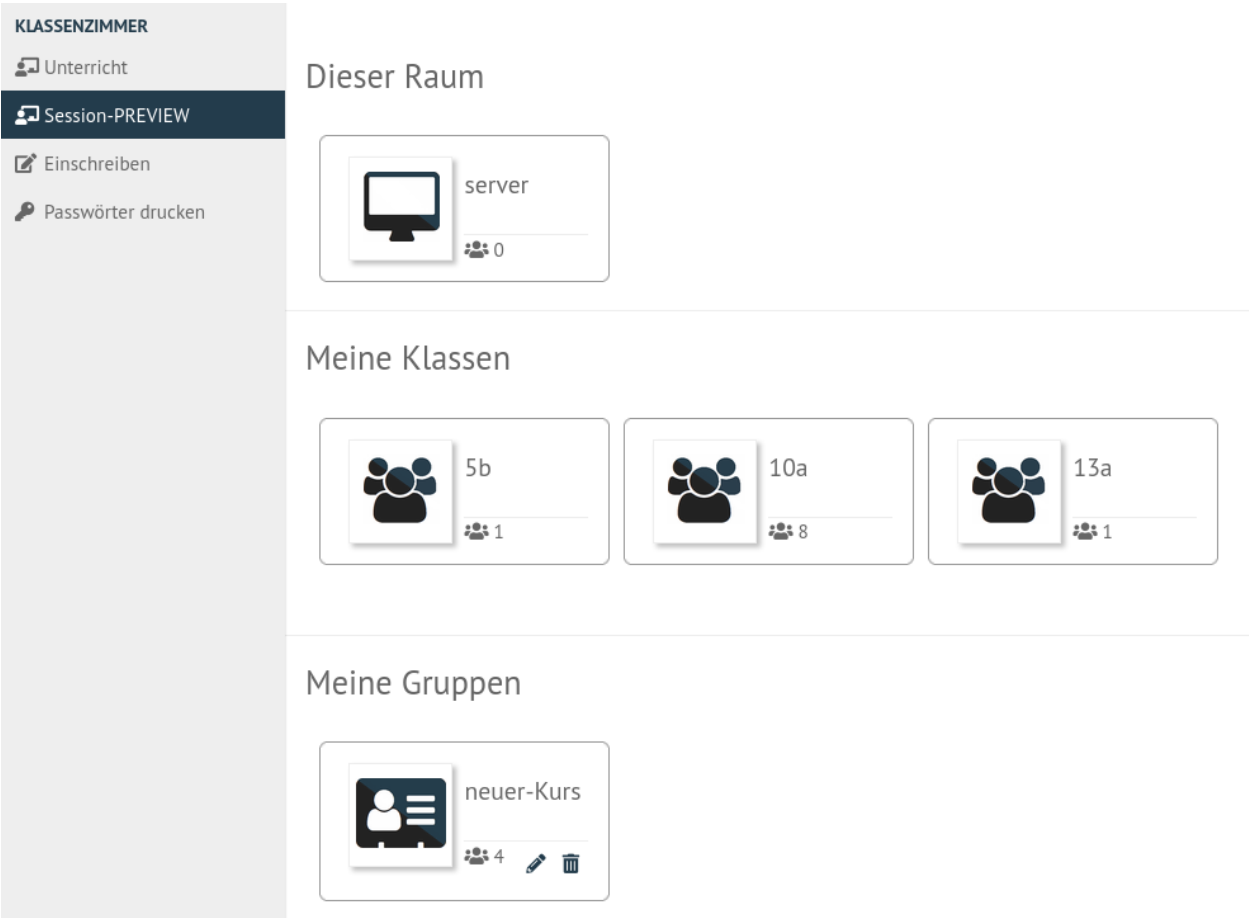


Abb. 496: Starte die Session für die Klasse

Benutzer	Übertragen	Arbeitsverzeichnis						
<div>8 Schüler</div>		transfer/hansbo/_collect						
Testuser, Achim testusac	10a <div>Teilen</div> <div>Einsammeln</div>				<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<div>⚙</div>
Testuser, Bernd testusbe	10a <div>Teilen</div> <div>Einsammeln</div>				<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<div>⚙</div>
Testuser, Celine testusce	10a <div>Teilen</div> <div>Einsammeln</div>				<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<div>⚙</div>
Testuser, Dorian testusdo	10a <div>Teilen</div> <div>Einsammeln</div>				<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<div>⚙</div>
Testuser, Emil testusem	10a <div>Teilen</div> <div>Einsammeln</div>				<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<div>⚙</div>
Testuser, Heinz testushe	10a <div>Teilen</div> <div>Einsammeln</div>				<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<div>⚙</div>
Testuser, Yilzin testusyl	10a <div>Teilen</div> <div>Einsammeln</div>				<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<div>⚙</div>
Testuser, Zoran testuszo	10a <div>Teilen</div> <div>Einsammeln</div>				<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<div>⚙</div>

Abb. 497: Liste aller Schüler der Klasse / des Kurses

- Internetzugang
- Druckerzugriff







					
		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Abb. 498: Spalten mit den zu-/abschaltbaren Funktionen pro Schüler

Soll eine Funktion für alle Schüler aktiviert werden, klickst Du nur auf das Symbol des Spaltenkopfen (z.B. WLAN). Die Änderungen werden direkt angewendet.

4.29 Anzeigen des eigenen Plattenplatzes

Autor des Abschnitts: @cweikl

Jeder Benutzer kann sich auf der Startseite der *Schulkonsole* über den verbrauchten Speicherplatz und die ihnen zugewiesenen Speicherplatzbegrenzungen (Quota) informieren.

Lehrer: Prüfen der eigenen Quota

Melde Dich als Lehrer in der Schulkonsole an. Es erscheint zunächst die Hauptseite mit den Konto-Informationen, den Quotas und denjenigen Gruppen, denen Sie zugeordnet sind.

Es sind verschiedene Quotas voneinander abzugrenzen:

Wie in obiger Abbildung dargestellt, sind folgende Quota zu unterscheiden:

1. **default-school:** Dieser Plattenplatz in MiB wird auf dem Server auf dem share `/srv/samba/schools/default-school` geprüft. Diese Freigabe (share DFLT) ist für alle Benutzer der zugeordneten Schule relevant. In der eigenen Schule - hier `default-school` - können Daten bis zur definierten Obergrenze auf dieser Freigabe gespeichert werden.
2. **linuxmuster-global:** Dieser Plattenplatz in MiB wird auf dem Server auf dem share `/srv/samba/global` geprüft. Diese Freigabe (share GLOBAL) ist für alle Benutzer der beteiligten Schulen (Mehr-Schulbetrieb) relevant, um schulübergreifend Dateien zu tauschen (linuxmuster-global).
3. **Cloudquota:** Bezeichnet die Quota der eigenen Schule - ein anderer Name für die unter 1.) dargestellte Quota für `default-school`.
4. **Mailquota:** Zeigt den verfügbaren Plattenplatz zur Ablage von E-Mails an.

Beachte auch, dass die gesetzte Quota immer für eine ganze Festplattenpartition auf dem Linux-Server gilt. Dies bedeutet, dass auch Dateien auf den Tauschverzeichnissen zum verbrauchten Speicherplatz oder ausgeteilte Dateien für Prüfungen, die nicht wieder gelöscht wurden, diesen Plattenplatz belegen.

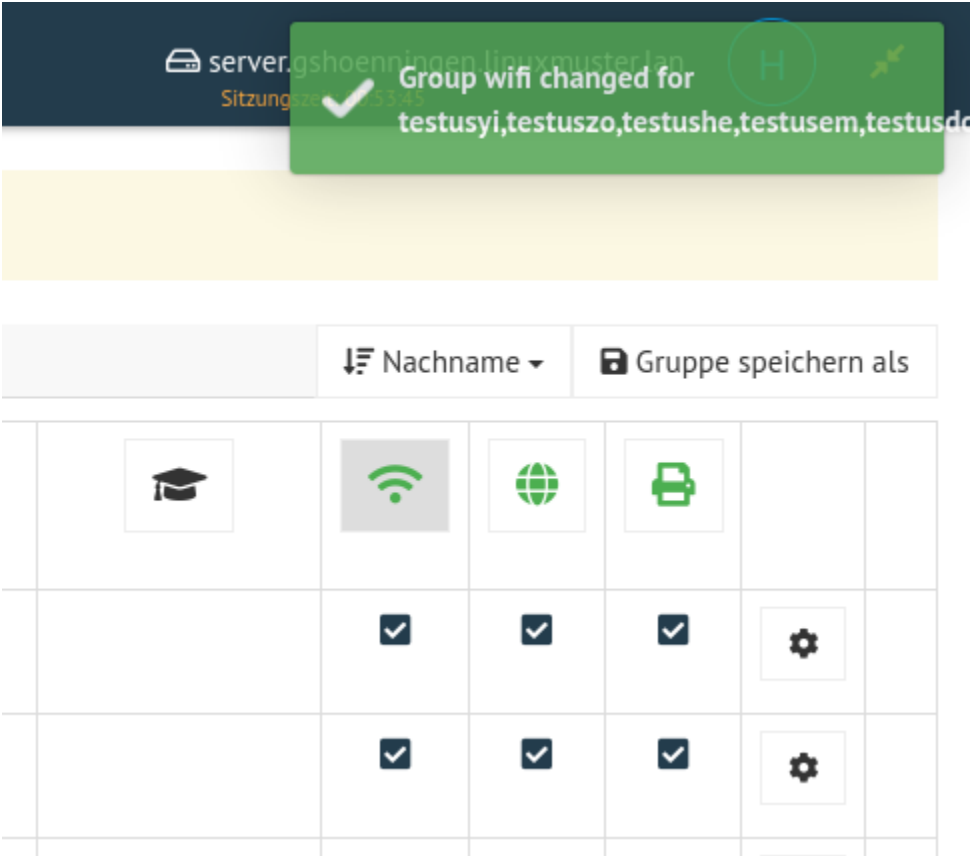


Abb. 499: WLAN für alle Schüler aktivieren



Abb. 500: Schulkonsole Übersicht

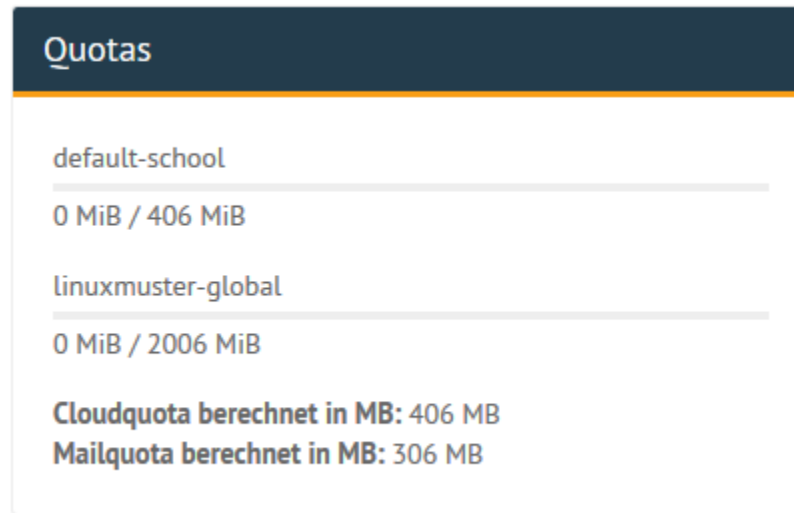


Abb. 501: Verschiedene Quota des Benutzers

4.30 linuxmuster.net aktuell halten

Autor des Abschnitts: @toheine

4.30.1 Update des Ubuntu Servers von linuxmuster.net

Um die linuxmuster.net 7.x zugrunde liegende Ubuntu Version (Ubuntu Server 22.04.x LTS 64bit) zu aktualisieren, beachte bitte nachstehende Hinweise.

Achtung: Für ein sicheres System muss regelmäßig ein Update durchgeführt werden!

4.30.2 Keine automatischen Updates

Es wird ausdrücklich davon abgeraten den Linuxmuster.net-Server die Option Automatische Updates zu aktivieren, so dass Paketaktualisierungen automatisch von den Ubuntu-Update-Servern heruntergeladen und installiert werden.

Automatische Updates sind in der Datei `/etc/apt/apt.conf.d/20auto-upgrades` konfiguriert. Sofern darin der Eintrag `APT::Periodic::Unattended-Upgrade "1";` existiert, muss die "1" in eine "0" geändert werden.

Melde Dich zusätzlich bei der entsprechenden [Mailingliste](#) an oder abonniere den entsprechenden [RSS-Feed](#). Alle Hinweise zu Sicherheitsupdates von Ubuntu erhält man unter <http://www.ubuntu.com/usn/>

4.30.3 Aktualisierungen einspielen

Um die Server-Installation auf den aktuellen Paketstand zu bringen, gehe folgendermaßen vor:

1. Logge Dich als Benutzer root auf einer Serverkonsole ein.
2. Aktualisiere die Paketlisten:

```
# apt update
```

3. Installiere nun Aktualisierungen und weitere Software-Pakete über das Internet:

```
# apt dist-upgrade
```

4. Es wird aufgelistet, welche Pakete aktualisiert werden. Bestätige die Aktualisierung mit der Eingabe von **Y**
5. Während des Aktualisierungsverlaufs fragen manchmal Pakete nach, ob eine neue Konfigurationsdatei installiert werden soll. Gib hier **N** oder **ENTER** für „Beibehalten“ an.

```
Konfigurationsdatei »/etc/cloud/cloud.cfg«
==> Geändert (von Ihnen oder von einem Skript) seit der Installation.
==> Paketverteiler hat eine aktualisierte Version herausgegeben.
Wie möchten Sie vorgehen? Ihre Wahlmöglichkeiten sind:
  Y oder I : Die Version des Paket-Betreuers installieren
  N oder O : Die momentan installierte Version beibehalten
  D        : Die Unterschiede zwischen den Versionen anzeigen
  Z        : Eine Shell starten, um die Situation zu begutachten
Der Standardweg ist das Beibehalten der momentanen Version.
*** cloud.cfg (Y/I/N/O/D/Z) [Vorgabe=N] ?
Fortschritt: [ 79%] [#####.....]
```

6. Insbesondere bei einem ersten Update innerhalb eines Ubuntu-Server-Releases, können Dienste die Nachfrage stellen, ob die jeweilige Konfigurationsdatei automatisch erstellen sollen. hier lautet die Antwort grundsätzlich „nein“ (z. B. Samba)

Samba-Server und Hilfsprogramme

Der Rest der Konfiguration von Samba betrifft Fragen über Parameter in /etc/samba/smb.conf (das ist die Datei, die genutzt wird, um die Samba-Programme (nmbd und smbd) zu konfigurieren). Ihre aktuelle smb.conf enthält eine »include«-Zeile oder eine mehrzeilige Option. Dies kann den automatischen Konfigurationsprozess stören, so dass Sie eventuell Ihre smb.conf-Datei manuell korrigieren müssen, um Samba wieder zum Laufen zu bekommen.

Wenn Sie diese Option nicht wählen, werden Sie jede Änderung an der Konfiguration manuell vornehmen müssen und können nicht den Vorteil von regelmäßigen Verbesserungen an der Konfiguration nutzen.

Soll smb.conf automatisch konfiguriert werden?

☐ <Yes> ☒ <No>

7. Zudem kann die Frage auftauchen, ob bei Bedarf Dienste neu gestartet werden dürfen. Sofern das Update eher zu Zeiten geringer Last ausgeführt werden sollten, kann diese Frage mit **y** beantwortet werden:

Konfiguriere libssl1.1:amd64

Auf Ihrem System sind Dienste installiert, die beim Upgrade bestimmter Bibliotheken, wie Libpam, Libc und Libssl, neu gestartet werden müssen. Da diese Neustarts zu Unterbrechungen der Dienste für dieses System führen können, werden Sie normalerweise bei jedem Upgrade über die Liste der neu zu startenden Dienste befragt. Sie können diese Option wählen, um diese Abfrage zu vermeiden; stattdessen werden alle notwendigen Dienste-Neustarts für Sie automatisch vorgenommen und die Beantwortung von Fragen bei jedem Upgrade von Bibliotheken vermieden.

Dienste bei Paket-Upgrades ohne Rückfrage neu starten?

☒ <Yes> ☐ <No>

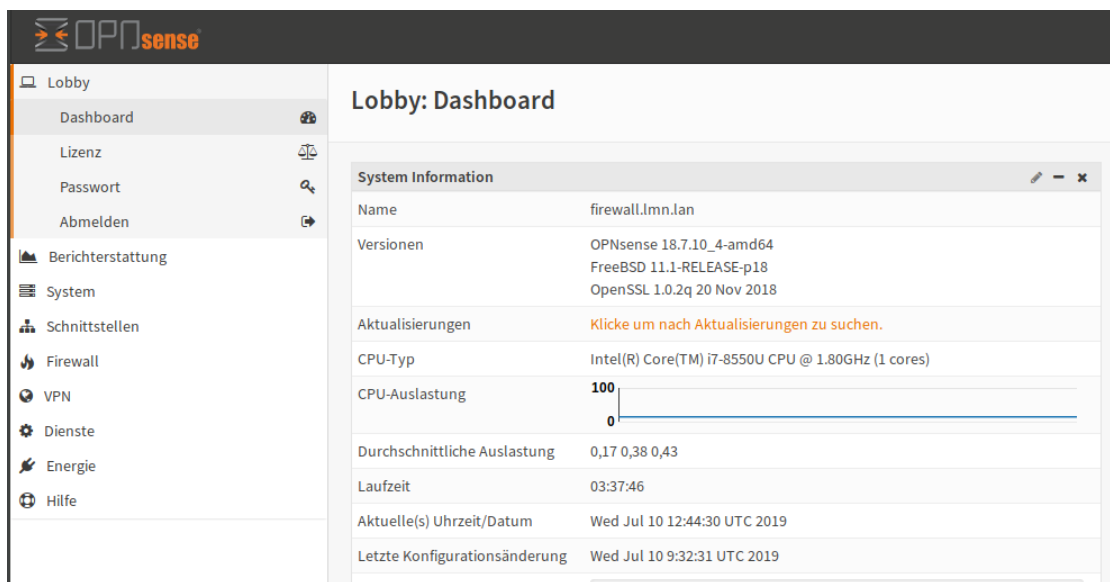
4.30.4 Aktualisierung der Firewall OPNsense®

Um die Firewall OPNsense® zu aktualisieren, beachte bitte Hinweise.

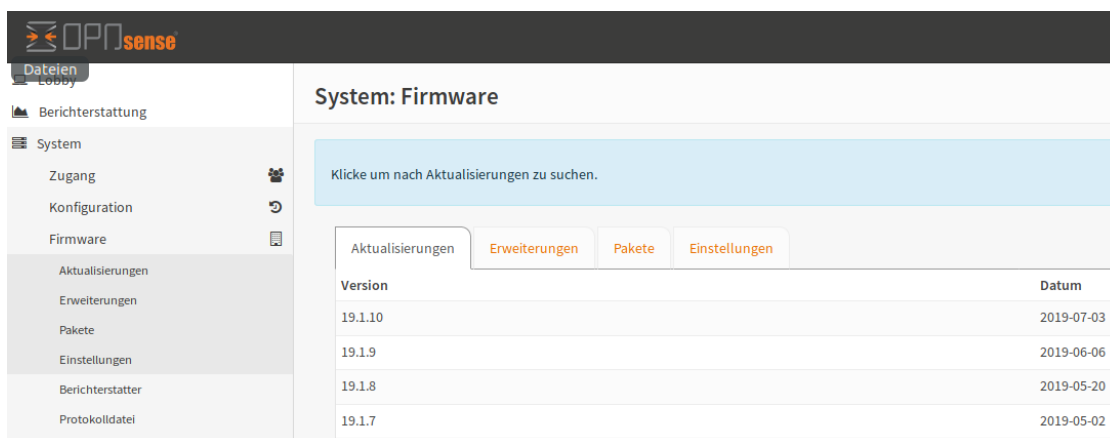
Achtung: Führe Updates bitte regelmäßig manuell durch.

Bei linuxmuster.net 7.2 ist die Firewall relativ unabhängig vom eigentlichen Server zu warten. Dementsprechend werden die Updates über die Weboberfläche der Firewall eingespielt.

Verbinde Dich hierzu mit der Firewall über einen Browser. Nach der Anmeldung erscheint das Dashboard (unter Lobby). Darin befindet sich ein Link um direkt Updates einzuspielen.



Eine etwas ausführlichere Übersicht ist unter System -> Firmware -> Aktualisierungen zu finden.



Normale Minor-Releases können so direkt eingespielt werden. Sobald allerdings das Patch-Level erhöht wird, muss hier zuerst das *Upgrade* entsperrt werden.

System: Firmware

Es sind auf dem ausgewählten Spiegelserver keine Aktualisierungen verfügbar. Auf Aktualisierungen prüfen Jetzt aktualisieren

Diese Softwareversion hat das Ende ihrer Lebensdauer erreicht. Die nächste Hauptversion ist: 19.7 Diese Aktualisierung entsperren Jetzt aktualisieren

Aktualisierungen Erweiterungen Pakete Changelog Einstellungen

Version	Datum	
19.7.1	2019-07-25	
19.7	2019-07-17	
19.1.10 (installiert)	2019-07-03	
19.1.9	2019-06-06	
19.1.8	2019-05-20	
19.1.7	2019-05-02	

Es ist zu empfehlen solche Upgrades außerhalb der regulären Einsatzzeiten der Schule zu betreiben. Bei einem Upgrade startet die Firewall mehrfach neu und unterbricht damit alle Verbindungen nach außen. Zudem kann es zu Problemen mit einzelnen Modulen kommen. Vor dem Update sollte also im Hypervisor (Proxmox, XenServer, ...) unbedingt ein Snapshot erstellt werden, so dass die Maschine im Fehlerfall wieder in den Ausgangszustand zurückgesetzt werden kann.

4.31 Zugriffsrechte im Netzwerk

Autor des Abschnitts: @Thomas, @Tobias, @michael_kohls

4.31.1 Zugriff über einen Proxy

Standardmäßig sollen die Benutzer der Schulgeräte nur dann Zugriff auf das Internet bekommen, wenn sie sich ausweisen können („authentication“). Dies geschieht über einen Webproxy, der in der Firewall läuft und der wiederum auf den Schulgeräten als Proxy eingetragen sein muss.

Hinweis: Der Proxy muss als FQDN angegeben werden! Z.B. `firewall.linuxmuster.lan`, Port: 3128

4.31.2 Single-Sign-On am Proxy

Eine Einmalanmeldung („Single-Sign-On“ oder kurz SSO) ist eine moderne Methode die Eingabe eines Passwortes auf ein einziges Mal zu reduzieren. Bei Schulgeräten ist das meist der Anmeldevorgang am Gerät. Danach meldet der Client dem Webproxy, wer hier angemeldet ist und kann so den Internetzugriff erfragen.

linuxmuster.net verwendet hier standardmäßig das Kerberos-Ticketsystem. Dieses SSO-Verfahren ist auf der Firewall OPNsense® aktiviert und muss auf den Arbeitsplatzrechnern eingerichtet werden.

4.31.3 Zugriff ohne Proxy

In manchen Fällen will man Geräten zeitweilig oder permanent den Zugriff auf das Internet geben.

Es gibt eine nicht aktivierte Regel „Allow entire LAN“ die bei Aktivierung aus dem LAN für alle Geräte uneingeschränkten Zugriff erlaubt.

Darüberhinaus ist unter Firewall | Aliase ein „NoProxy“-Alias angelegt, der die ersten zehn IP-Adressen des LAN-Netzwerks und diejenigen der Server enthält. Für die Adressen dieses Aliases ist eine aktive Regel „Allow NoProxy-Group“ angelegt, die unbeschränkten Zugriff auf das Internet erlaubt. Eine IP-Adresse aus diesem Pool kann z.B. für einen Admin-PC oder für einen Masterclient verwendet werden.

Edit Alias

☒
enabled

☒
 enable this alias

Name

NoProxy

Der name des Alias darf nur aus den Zeichen a-z, A-Z, 0-9 und _ bestehen. Alias können unter Verwendung des Namens verschachtelt werden.

Typ

Host(s)

Inhalt

10.0.0.1 ×

10.0.0.2 ×

10.0.0.3 ×

10.0.0.4 ×

10.0.0.5 ×


10.0.0.6 ×

10.0.0.7 ×

10.0.0.8 ×

10.0.0.9 ×

10.0.0.10 ×

✖ Alles entfernen
 

Beschreibung

NoProxy-Group

Die Beschreibung wird nicht als Parameter verwendet.

4.31.4 Entfernen nicht benötigter IP

Während der Installation wurde das „NoProxy“-Alias automatisch mit den IP-Adressen 10.0.0.1 – 10.0.0.10 bzw. bei do-it-like-babo mit den IP-Adressen 10.16.1.1 – 10.16.1.3 und 10.16.0.1 – 10.16.0.10 angelegt. Normalerweise werden nicht alle für den Server, die Dockerhosts und evtl. Admin-PC benötigt.

Als letzter Schritt vor dem Installationsende empfiehlt es sich, alle nicht dauerhaft benötigten IP-Adressen aus dem „NoProxy“-Alias zu entfernen. Hintergrund: Der Internetzugriff wird grundsätzlich über den Proxy geregelt. Gibt es unbenutzte IP-Adressen im „NoProxy“-Alias könnten diese unbefugt verwendet werden, um permanenten und ungefilterten Internetzugang zu erlangen.

4.32 Anpassen der Festplattengröße

Autor des Abschnitts: @toheine, @MachtDochNix, @cweikl

Must Du aufgrund geänderter Anforderungen die bereits eingerichteten Festplattengrößen in Deiner Virtualisierungs-umgebung ändern, dann ist es hilfreich, sich an nachstehend beschriebenen Ablauf und Hinweisen zu orientieren.

4.32.1 Übersicht zum Vorgehen

Folgender Ablauf zur Anpassung der Festplattengrößen ist einzuhalten:

1. In der Virtualisierungsumgebung ein Snapshot der VM ausführen. Auf diesen Stand kannst Du zurückkehren, sofern bei den nachfolgenden Schritten etwas nicht funktioniert.
2. In der Virtualisierungsumgebung die HDDs der VM erweitern.
3. Größenänderung in den VMs bekannt machen.

Hinweis: Die VM der OPNsense® benötigt bei der Anpassung ein etwas anderes Vorgehen, da hier ein BSD Linux zum Einsatz kommt. Die entsprechenden Hinweise finden sich im entsprechenden Abschnitt

4.32.2 Anpassung Hypervisor

Starte nun mit Punkt 1, indem Du nachstehend Deine eingesetzte Virtualisierungsumgebung auswählst und gemäß der Dokumentation die Festplattengröße Deiner VMs im Hypervisor anpasst.

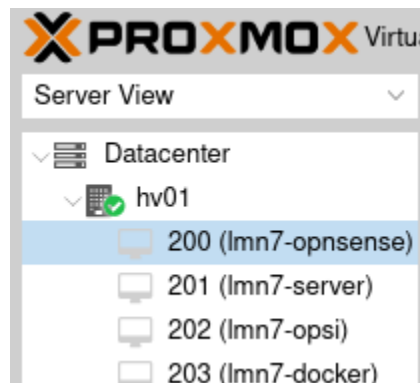
Vorbereiten der Proxmox Festplatten

1. Snapshots der VMs anfertigen

Autor des Abschnitts: @toheine, @MachtDochNix, @cweikl

Am Beispiel der OPNsense®-VM werden die Anpassungen nachstehend erläutert.

Wähle als Erstes die VM aus, die geklont werden soll.



Unter More findest Du den Button zum Starten des Klon-Vorganges



In dem sich öffnen Fenster siehst Du welche VM geklont werden wird und deren neuer ID.

Im Feld *Name* kannst Du einen eigenen angeben, ansonsten wird einer nach dem Muster „Copy of VM ...“ verwendet.

Clone VM 200

Target node:

hv01

Target Storage:

Same as source

VM ID:

100

Format:

QEMU image format (qc)

Name:

lmn7-opnsense-be4-hd-resi

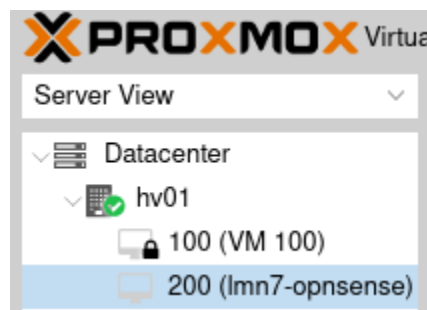
Resource Pool:

Help



Clone

Der Klon-Vorgang wird mit *Clone* gestartet.

Das wird sichtbar daran, dass die VM mit der neuen ID in der linken Übersicht mit einem Schloss erscheint.



Das Schloss zeigt an, dass das Kopieren der VM gestartet ist. Dieses siehst Du auch in den *Tasks* am unteren Bildschirmrand.

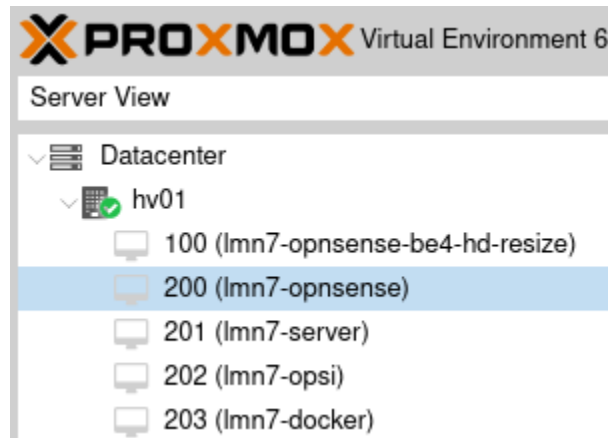
Tasks		Cluster log			
Start Time ↓	End Time	Node	User name	Description	Status
Dec 24 11:10:46		hv01	root@pam	VM 200 - Clone	

Dort erkennst Du, wann der Vorgang abgeschlossen ist.

Bei der neuen VM ist das Schloss verschwunden und der Name wird in der Übersicht der VMs angezeigt.

Hinweis: Diesen Ablauf musst Du für alle Virtuellen Maschinen, deren Festplatte Du vergrößern möchtest, wiederholen.

Tasks Cluster log					
Start Time ↓	End Time	Node	User name	Description	Status
Dec 24 11:10:46	Dec 24 11:12:05	hv01	root@pam	VM 200 - Clone	OK



2. Vorbereiten der PROXMOX Festplatten

Ausgangssituation:

Die OPNsense®-VM wurde mit dem Namen *lmn7-opnsense* und der *VM-ID: 200* angelegt. In der Übersicht erkennst Du, dass derzeit eine Festplatte mit einer Größe von 10 GiB eingerichtet wurde. Für den Einsatz in einem Produktivserver einer Schule dürfte dies zu klein sein. Die Festplattengröße kannst Du nun wie folgt anpassen:

1. Wähle links im Menü die gewünschte VM aus und dann in der Spalte daneben (Kontextmenü der VM) den Eintrag *Hardware* aus.
2. Rechts werden nun die Hardware-Komponenten der VM aufgelistet. Markiere den Eintrag *Hard disk*.
3. Klicke danach auf den Button *Resize Disk*, um die Festplatte der VM zu vergrößern.

Hinweis: Auf diesem Wege ist nur eine Vergrößerung des Plattenplatzes möglich, eine Verkleinerung hingegen nicht!

4. Es erscheint ein neues Fenster, in dem Du angeben must, um wieviel GiB Du die Festplatte vergrößern willst.
5. In dem Beispiel sind 10 GByte gegeben, um auf 50 GByte zu kommen, trägst Du nun 40 GByte ein. Danach siehst Du folgenden Eintrag:

Hinweis: Für die anderen VMs werden die Festplatten in gleicher Weise vergrößert.

Bei der Server-VM ist zu beachten, dass diese über zwei Festplatten verfügt. Die kleine Festplatte weist zu Beginn 25 GByte die größere 100 GByte auf. Beide sind zu vergrößern.

Hierbei ist auf eine ausreichende Größe zu achten, da auf dem Server neben den Nutzer- und Klassendaten auch die von Linbo gespeicherten Festplattenabbilder der Clients abgelegt werden. Siehe Einleitung dieses Abschnittes: [Anpassen der Festplattengröße](#)

Virtual Machine 200 (lmm7-opnsense) on node 'hv01' ▶ Start ⏻ Stop

- Summary
- Console
- Hardware
- Cloud-Init
- Options
- Task History
- Monitor
- Backup
- Replication
- Snapshots
- Firewall
- Permissions

lmm7-opnsense

Status	stopped
HA State	none
Node	hv01
CPU usage	0.00% of 4 CPU(s)
Memory usage	0.00% (0 B of 4.00 GiB)
Bootdisk size	10.00 GiB
IPs	No Guest Agent configured

PROXMOX Virtual Environment 6.2-10 Search Documentation Create VM Create

Server View ▼

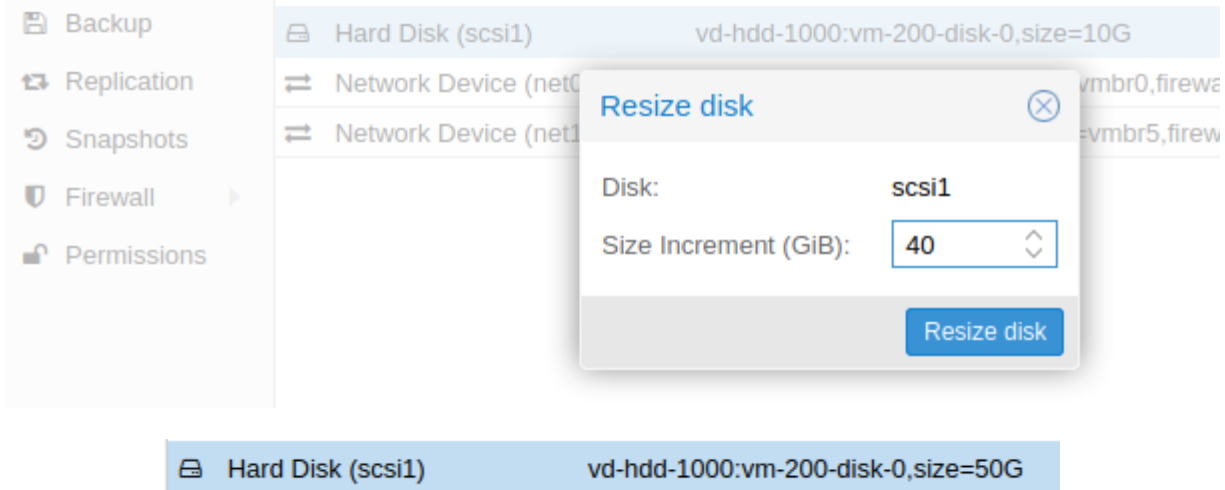
- ▼ Datacenter
 - ▼ hv01
 - 200 (lmm7-opnsense)
 - 201 (lmm7-server)
 - 202 (lmm7-opsi)
 - 203 (lmm7-docker)
 - local (hv01)
 - vd-hdd-1000 (hv01)

Virtual Machine 200 (lmm7-opnsense) on node 'hv01' ▶ Start ⏻ Shutdown Console

- Summary
- Console
- Hardware
- Cloud-Init
- Options
- Task History
- Monitor
- Backup
- Replication
- Snapshots
- Firewall
- Permissions

Add Detach Edit Resize disk Move disk Revert

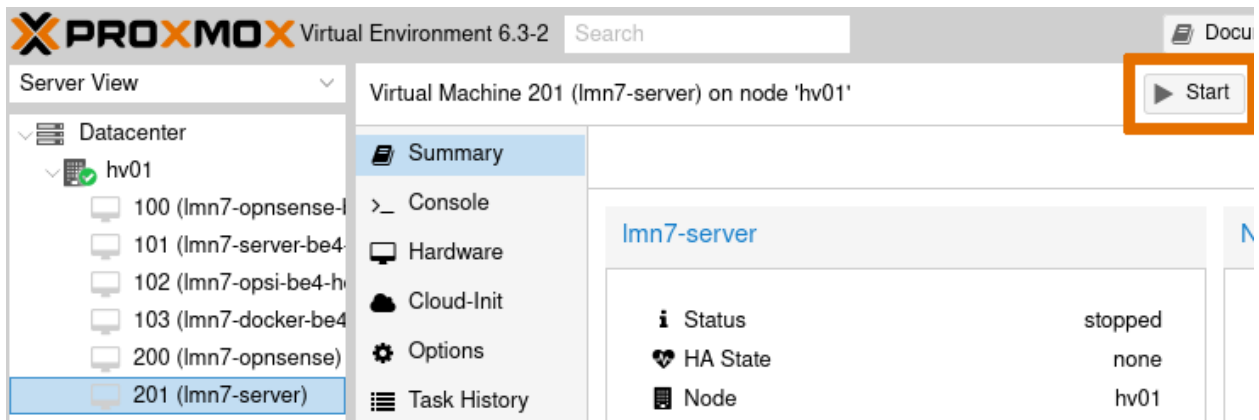
Memory	4.00 GiB
Processors	4 (2 sockets, 2 cores)
BIOS	Default (SeaBIOS)
Display	Default
Machine	Default (i440fx)
SCSI Controller	VirtIO SCSI
CD/DVD Drive (ide2)	none,media=cdrom
Hard Disk (scsi1)	vd-hdd-1000:vm-200-disk-0,size=10G
Network Device (net0)	virtio=42:C9:F7:76:90:59,bridge=vbr0,firewall=1
Network Device (net1)	virtio=5A:42:BC:9C:6E:77,bridge=vbr5,firewall=1



3. Schritt: HDD-Größen der Virtuellen Maschinen anpassen

Nachdem im Virtualisierungs-Host die HDD der VM vergrößert wurde, muss die tatsächlich genutzte Größe angepasst werden.

3.1 Virtuelle Maschinen starten



Wähle links im Menü die gewünschte VM aus. Exemplarisch ist der Start der Server-VM dargestellt.

Nach der Auswahl betätigst Du den Button *Start*.

Wiederhole dieses Vorgehen für alle VMs deren Festplatten Du angepasst hast.

3.2 Vergrößern der Server Festplatten

In der gestarteten VM musst Du nun den Festplattenplatz anpassen. Folge hierzu der Beschreibung mit nachstehendem Link.

Aktualisieren der Server-Festplattengrößen

Autor des Abschnitts: @toheine, @MachtDochNix, @cweikl

Hinweis: Achtung: Dies ist noch eine unvollständige Beschreibung. Findest Du Fehler oder kannst zur Verbesserung beitragen, dann wende Dich bitte an einen der Autoren des Abschnittes.

Überblick

1. Starten der VM wie zuvor beschrieben ist erfolgt.
2. Prüfen, ob die neuen HDD-Größen an die VM durchgereicht werden.
3. Partitionsgrößen prüfen.
4. HDD1 anpassen.
5. HDD2 mit dem LVM anpassen.
6. Reboot
7. Tests durchführen.

3.1 Starten der VM

Starte die VM wie zuvor beschrieben.

3.2 HDD-Größen überprüfen

Auf der Konsole der Server-VM prüfst Du zuerst, welche Festplatten des Hypervisor auch in der VM durchgereicht werden und welche Bezeichnung diese haben. Die im Hypervisor geänderten Größen werden hier bereits angezeigt, aber die Partitionen wurden noch nicht auf die neuen Größen angepasst.

Öffne die Konsole wie schon in einem vorherigen Abschnitt gezeigt, nachdem Du in der Übersicht links den Server *lmn-server* ausgewählt hast.

Für den Login benötigst Du folgende Informationen:

- Login: root
- Passwort: Muster!

Hinweis: Diese Daten dürfen bis zum Aufruf des Installationsskriptes nicht verändert werden!

In der geöffneten Konsole gib folgenden Befehl ein:

```
lsblk
```

Du solltest jetzt die geänderten Größen angezeigt bekommen.

```
root@server:~# lsblk
NAME                                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sr0                                11:0    1 1024M  0 rom
xvda                               202:0    0 155G  0 disk
├─xvda1                            202:1    0   1M  0 part
├─xvda2                            202:2    0  24G  0 part /
xvdb                               202:16   0 1000G  0 disk
├─vg_srv-var                       253:0    0  9,8G  0 lvm  /var
├─vg_srv-linbo                     253:1    0  40G  0 lvm  /srv/linbo
├─vg_srv-global                     253:2    0  9,8G  0 lvm  /srv/samba/global
└─vg_srv-default--school           253:3    0  40G  0 lvm  /srv/samba/schools/default-school
```

In Abhängigkeit Deiner Virtualisierungs-Umgebung werden die Festplatten unterschiedlich benannt. Wir zeigen das hier an einem Beispiel mittels mit XCP-ng. Es kann also in Deiner Konfiguration Abweichungen in der Bezeichnung geben. Passe diese bei den folgenden Befehlen dementsprechend an.

Die Bezeichnung *xvda* steht in XCP-ng für die 1. Festplatte der VM, *xvdb* für die 2. Festplatte der VM.

- *xvda1* ist dann die 1. Partition auf der 1. Festplatte der VM
- *xvda2* die 2. Partition auf der 1. Festplatte

*vg-** steht für ein LVM auf der jeweils zugeordneten Festplatte. Im obigen Beispiel befindet sich das LVM auf der 2. Festplatte (*xvdb*).

Hinweis: Unter Proxmox oder KVM werden in der VM hingegen die Festplattenbezeichnungen *sda* für die 1. HDD und *sdb* für die 2. HDD des Systems verwendet. Die Nummerierung für die Partitionen bleibt erhalten. Die angeben sind je nach eingesetztem System entsprechend anzupassen.

3.3 Dateisystem prüfen

Lasse Dir nun die aktuellen Größen des Dateisystems ausgeben.

```
df -h
```

```
root@server: ~# df
Dateisystem      Größe Benutzt Verf. Verw% Eingehängt auf
udev             5,9G      0  5,9G   0% /dev
tmpfs            1,2G    7,7M  1,2G   1% /run
/dev/xvda2       25G     5,7G  18G  25% /
tmpfs            5,9G      0  5,9G   0% /dev/shm
tmpfs            5,0M      0  5,0M   0% /run/lock
tmpfs            5,9G      0  5,9G   0% /sys/fs/cgroup
/dev/mapper/vg_srv-global  9,8G    37M  9,3G   1% /srv/samba/global
/dev/mapper/vg_srv-linbo   40G   347M  37G   1% /srv/linbo
/dev/mapper/vg_srv-default-school  40G    74M  38G   1% /srv/samba/schools/default-school
tmpfs            1,2G      0  1,2G   0% /run/user/0
```

Hier werden noch die alten Partitionsgrößen angegeben.

3.4 HDD1 anpassen

Partitionen auf der 1. HDD prüfen:

```
fdisk /dev/xvda
```

Sollte eine derartige Meldung

```
Warning: GPT - PMBR Größenunterschied (52428799 != 304087039) wird durch write
↳ korrigiert.
```

durch den Befehl ausgegeben werden, dann fdisk wieder ohne Schreibvorgang verlassen mit *q*.

Dieses Problem gilt es zunächst zu lösen.

Rufe dazu auf der Eingabekonsolle das Programm *parted* auf.

```
parted /dev/xvda
```

Das Programm wartet dann auf eine Eingabe von dir.

```
root@server: ~# parted /dev/xvda
GNU Parted 3.2
/dev/sda wird verwendet
Willkommen zu GNU Parted! Rufen Sie >>help<< auf, um eine Liste der verfügbaren Befehle
↳ zu erhalten.
(parted)
```

Gib *print* ein.

Es wird dann ein Größenproblem für die 1. HDD angezeigt und parted bietet eine Auswahloption an, um dieses Problem zu beheben.

Anmerkung zu den Platzhaltern *xx*, diese stehen für die ausgewählten Vorgaben Deiner Installation.

```
Warnung: Nicht der gesamte verfügbare Platz von /dev/xvda scheint belegt zu sein. Sie
↳ können die GPT reparieren, damit der gesamte Platz verwendet wird (zusätzlich xxx
↳ Blöcke) oder Sie können mit den aktuellen Einstellungen fortfahren.
Reparieren/Fix/Ignoren/Ignore?
```

Gib *Reparieren* ein, damit das Größenproblem gelöst wird und verlasse dann parted wieder durch Angabe des Befehls *quit*.

Danach erneut *fdisk* aufrufen, die 2. Partition löschen und neu mit neuer Größe anlegen. Die angegebenen Befehle musst Du der Reihe nach abarbeiten.

```
fdisk /dev/xvda
```

```
p
```

p (print) zeigt Dir die vorhandenen Partitionen an

```
d
```

d bietet Dir die Auswahl der zu löschen Partitionen durch die Angabe einer Nummer an. Hier also die 2

2

Nun gilt es die Partition neu anzulegen, das erreichst Du mit *n*:

n

Die folgenden 3 Vorgaben kannst Du einfach mit *Enter* übernehmen.

```
Partitionsnummer (2-128, Vorgabe 2): 2
Erster Sektor (4096-xxx, Vorgabe 4096):
Letzter Sektor, +Sektoren oder +Größe{K,M,G,T,P} (4096-xxx, Vorgabe xxx):
```

Dir wird darauf die folgende Frage gestellt:

```
Eine neue Partition 2 des Typs "Linux filesystem" und der Größe xxx GiB wurde erstellt
Partition #2 enthält eine ext4-Signatur.
```

```
Wollen Sie die Signatur entfernen? [J]a/[N]ein:
```

Gib ein *N* ein

Zum Beenden von *fdisk* verwendest Du nun *w* damit Deine Änderungen auf die Festplatte geschrieben werden.

```
Wollen Sie die Signatur entfernen? [J]a/[N]ein:
```

```
Befehl (m für Hilfe): w
```

```
Die Partitionstabelle wurde verändert.
Festplatten werden synchronisiert.
```

Nun muss die Partition noch auf die neue Größe erweitert werden. Gib in der Konsole nun an:

```
resize2fs /dev/xvda2
```

Ab nun wird die neue Größe für der 1. HDD genutzt.

3.5 HDD2 mit dem LVM anpassen

In o.g. VM auf XCP-ng befindet sich auf der 2. HDD */dev/xvdb* ein LVM.

Folgende Begriffe sind hierbei relevant:

- a) Physical Volume (PV)
- b) Volume Group (VG)
- c) Logical Volume (LV)
- a) Anpassen der PV - Größe auf die gesamte neue Festplattengröße

PV ermitteln

```
root@server:/srv/linbo# pvscan
PV /dev/xvdb VG vg_srv lvm2 [<100,00 GiB / 0 free]
```

PV Größenanpassung testen

```
pvresize /dev/xvdb
Physical volume „/dev/xvdb“ changed
1 physical volume(s) resized / 0 physical volume(s) not resized
```

b) LV-Größen anpassen

```
lvextend -L+100G /dev/mapper/vg_srv-var
```

Der Befehl liefert folgende Ausgabe:

```
lvextend -L+100G /dev/mapper/vg_srv-var
Size of logical volume vg_srv/var changed from 10,00 Gib (2560 extents) to xx,xx GiB
↳ (xxxxx extents).
Logical volume vg_srv/var successfully resized.
```

Diesen Befehl wiederholst Du für die anderen Logical Volumes

```
lvextend -L+200G /dev/mapper/vg_srv-linbo
lvextend -L+100G /dev/mapper/vg_srv-global
lvextend -l +100%FREE /dev/mapper/vg_srv-default--school
```

c) Dateisystem an die neuen Größen anpassen:

```
resize2fs /dev/mapper/vg_srv-var
```

Beispiel der Befehlsausgabe:

```
resize2fs 1.44.1 (24-Mar-2018)
Dateisystem bei /dev/mapper/vg_srv-var ist auf /var eingehängt; Online-Größenänderung ist
erforderlich
old_desc_blocks = 2, new_desc_blocks = 14
Das Dateisystem auf /dev/mapper/vg_srv-var is nun 28835840 (4k) Blöcke lang.
```

Wiederhole diesen Befehl für die anderen Logical Volumes.

```
resize2fs /dev/mapper/vg_srv-linbo
resize2fs /dev/mapper/vg_srv-global
resize2fs /dev/mapper/vg_srv-default--school
```

d) Ergebnis prüfen

```
root@server: ~# df -h
```

Dateisystem	Größe	Benutzt	Verf.	Verw%	Eingehängt auf
udev	5,9G	0	5,9G	0%	/dev
tmpfs	1,2G	7,7M	1,2G	1%	/run
/dev/xvda2	25G	5,7G	18G	25%	/
tmpfs	5,9G	0	5,9G	0%	/dev/shm
tmpfs	5,0M	0	5,0M	0%	/run/lock
tmpfs	5,9G	0	5,9G	0%	/sys/fs/cgroup
/dev/mapper/vg_srv-global	207G	59M	199G	1%	/srv/samba/global
/dev/mapper/vg_srv-linbo	433G	368M	415G	1%	/srv/linbo
/dev/mapper/vg_srv-default-school	236G	85M	226G	1%	/srv/samba/schools/default- ↳ school

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

/dev/mapper/vg_srv-var	109G	1,2G	103G	2%	/var
tmpfs	1,2G	0	1,2G	0%	/run/user/0

3.6 Reboot

Starte nun die Server-VM neu, um zu prüfen, ob die vorgenommenen Größenanpassungen funktionsfähig sind und der Reboot korrekt ausgeführt wird.

```
root@server: ~# reboot
```

3.7 Tests durchführen

Nachdem die VM wieder gestartet ist, melde Dich an der Konsole an und prüfe mithilfe nachstehender Befehle, ob die Platten- und Partitionsgrößen nun Deinen Wünschen tatsächlich entsprechen.

```
root@server:~# lsblk
```

NAME	MAJ:MIN	RM	SIZE	RO	TYPE	MOUNTPOINT
sr0	11:0	1	1024M	0	rom	
xvda	202:0	0	145G	0	disk	
├─xvda1	202:1	0	1M	0	part	
├─xvda2	202:2	0	145G	0	part	/
xvdb	202:16	0	1000G	0	disk	
├─vg_srv-var	253:0	0	110G	0	lvm	/var
├─vg_srv-linbo	253:1	0	440G	0	lvm	/srv/linbo
├─vg_srv-global	253:2	0	210G	0	lvm	/srv/samba/global
└─vg_srv-default--school	253:3	0	240G	0	lvm	/srv/samba/schools/default-school

```
root@server:~# df -h
```

Dateisystem	Größe	Benutzt	Verf.	Verw%	Eingehängt auf
udev	5,9G	0	5,9G	0%	/dev
tmpfs	1,2G	6,8M	1,2G	1%	/run
/dev/xvda2	143G	13G	125G	10%	/
tmpfs	5,9G	0	5,9G	0%	/dev/shm
tmpfs	5,0M	0	5,0M	0%	/run/lock
tmpfs	5,9G	0	5,9G	0%	/sys/fs/cgroup
/dev/mapper/vg_srv-global	207G	59M	199G	1%	/srv/samba/global
/dev/mapper/vg_srv-default--school	236G	43G	184G	19%	/srv/samba/schools/default-school
/dev/mapper/vg_srv-var	109G	3,5G	101G	4%	/var
/dev/mapper/vg_srv-linbo	433G	40G	376G	10%	/srv/linbo
tmpfs	1,2G	0	1,2G	0%	/run/user/0

Hinweis: Dieses Vorgehen musst Du für die optionalen Server *docker* und *opsi* wiederholen, wenn Du auch deren Festplattengröße verändert hast!

Im Folgenden wirst Du die Festplatten der OPNsense® anpassen.

Aktualisieren der Festplattengrößen der OPNsense®-VM

Autor des Abschnitts: @toheine, @MachtDochNix, @cweikl

Hinweis: Diesen Abschnitt musst Du nur ausführen, sofern Du in Deinem Hypervisor die HDD-Größe der OPNsense® bereits vergrößert hast.

Überblick

OPNsense® basiert auf FreeBSD, sodass die Erweiterung der Festplattengröße von dem Vorgehen der Server-VM abweicht.

Die Erweiterung der Festplattengröße folgt folgendem Ablauf:

1. Starten der VM.
2. Prüfen, ob die neue HDD-Größe an die VM durchgereicht wurde.
3. Partitionsgrößen prüfen.
4. Festplatte `ad0` anpassen.
5. Partition `ad0s1` anpassen.
6. Änderungen anwenden.
7. Tests durchführen.
8. Reboot

Gleich bleibt, dass zu Beginn ein Snapshot erstellt werden sollte und die Virtuelle Disk im Hypervisor wie beschrieben vergrößert sein muss.

4.1 Starten der VM

Starten der VM und öffnen einer Konsole für diese ist wie zuvor beschrieben erfolgt.

Anmeldung als `root` mit dem bekannten Passwort.

Öffnen einer Shell mit der Taste `8`.

4.2 HDD-Größe prüfen

Prüfen, ob die neue HDD-Größe an die VM durchgereicht wurde.

Nach der Vergrößerung der virtuellen Platte und dem Systemstart wird überprüft, ob die Änderung vom System erkannt wird.

```
gpart show
```

Ausgabe des Befehls liefert:

```
root@OPNsense:~ # gpart show
=>      63  104857537  da0  MBR   (50G)
        63    20964762    1  freebsd [active]  (10G)
        20964825  83892775    -  free   -   (40G)
```

(Fortsetzung auf der nächsten Seite)


```

Stopping syslog_ng.
Waiting for PIDS: 21462.
Starting syslog_ng.
>>> Invoking start script 'carp'
>>> Invoking start script 'cron'
Starting Cron: OK
>>> Invoking start script 'beep'
Root file system: /dev/ufs/OPNsense
n Dec 27 13:29:20 CET 2020

* OPNsense.linuxmuster.lan: OPNsense 20.7.7_1 (amd64/OpenSSL) ***

LAN (vtnet0)    -> v4: 10.0.0.254/16
WAN (vtnet1)    ->

HTTPS: SHA256 DC 4A 8C B4 50 A0 6E 2B C5 A6 01 74 C5 A7 48 8A
              79 67 5F 1E 81 39 FC 98 67 2D AD 37 6E A5 63 A7
SSH:   SHA256 5zinhXX0awj1Q2N0AxtZ+i5YDrIu3rI/j85pPILUy1c (ECDSA)
SSH:   SHA256 r2Ij7n3j1q1hRYSB+dEog/rUs0lwq+U2ugGUydduU5U (ED25519)
SSH:   SHA256 uRGfUm13RxPaSR+K0u0RuggDpLWRw9+ErQPRfycdJHQ (RSA)

FreeBSD/amd64 (OPNsense.linuxmuster.lan) (ttyv0)

login: root
Password:

```

```

! Forums:      https://forum.opnsense.org/   !      000///  \\\0000
! Lists:       https://lists.opnsense.org/   !      0000   0000
! Code:        https://github.com/opnsense   !      0000000000000000
-----

*** OPNsense.linuxmuster.lan: OPNsense 20.7.7_1 (amd64/OpenSSL) ***

LAN (vtnet0)    -> v4: 10.0.0.254/16
WAN (vtnet1)    ->

HTTPS: SHA256 DC 4A 8C B4 50 A0 6E 2B C5 A6 01 74 C5 A7 48 8A
              79 67 5F 1E 81 39 FC 98 67 2D AD 37 6E A5 63 A7
SSH:   SHA256 5zinhXX0awj1Q2N0AxtZ+i5YDrIu3rI/j85pPILUy1c (ECDSA)
SSH:   SHA256 r2Ij7n3j1q1hRYSB+dEog/rUs0lwq+U2ugGUydduU5U (ED25519)
SSH:   SHA256 uRGfUm13RxPaSR+K0u0RuggDpLWRw9+ErQPRfycdJHQ (RSA)

0) Logout                      7) Ping host
1) Assign interfaces           8) Shell
2) Set interface IP address    9) pfTop
3) Reset the root password     10) Firewall log
4) Reset to factory defaults   11) Reload all services
5) Power off system            12) Update from console
6) Reboot system               13) Restore a backup

Enter an option: 8

```

(Fortsetzung der vorherigen Seite)

```
=>      0  20964762  da0s1  BSD  (10G)
      0         16      - free - (8.0K)
      16  20964746      1  freebsd-ufs (10G)
```

4.3 Partitionsgrößen prüfen

```
df -h
```

Die Ausgabe zeigt Dir an, dass derzeit nur der bisher verwendete Platz zu Verfügung steht:

```
root@OPNsense:~ # df -h
Filesystem      Size  Used Avail Capacity  Mounted on
/dev/ufs/OPNsense 9.7G  1.8G   7.1G    20%    /
devfs           1.0K  1.0K    0B   100%    /dev
devfs           1.0K  1.0K    0B   100%    /var/dhcpd/dev
devfs           1.0K  1.0K    0B   100%    /var/unbound/dev
```

Es ist zu erkennen, dass die Platte *da0* nur 10 GByte nutzt. Aus 4.2. wurde ersichtlich das weitere 40 GByte zur Verfügung stehen.

4.4 Festplatte da0/ada0 anpassen

```
root@OPNsense:~ # growfs /dev/ufs/OPNsense
```

Ausgabe des Befehls:

```
growfs: requested size 10GB is not larger than the current filesystem size 10GB
```

4.5 Partition da0s1/ada0s1 anpassen

```
growfs /dev/da0s1
```

Ausgabe des Befehls:

```
growfs: superblock not recognized
```

4.6 Änderungen anwenden

```
service growfs onestart
```

```

root@OPNsense:~ # service growfs onestart
Growing root partition to fill device
da0s1: da0s1 was automatically resized.
▶ Use 'gpart commit da0s1' to save changes or 'gpart undo da0s1' to revert them.
da0s1 resized
da0s1a resized
gpart: arg0 'ufs/OPNsense': Invalid argument
super-block backups (for fsck_ffs -b #) at:
 21798272, 23080512, 24362752, 25644992, 26927232, 28209472, 29491712,
 30773952, 32056192, 33338432, 34620672, 35902912, 37185152, 38467392,
 39749632, 41031872, 42314112, 43596352, 44878592, 46160832, 47443072,
 48725312, 50007552, 51289792, 52572032, 53854272, 55136512, 56418752,
 57700992, 58983232, 60265472, 61547712, 62829952, 64112192, 65394432,
 66676672, 67958912, 69241152, 70523392, 71805632, 73087872, 74370112,
 75652352, 76934592, 78216832, 79499072, 80781312, 82063552, 83345792,
 84628032, 85910272, 87192512, 88474752, 89756992, 91039232, 92321472,
 93603712, 94885952, 96168192, 97450432, 98732672, 100014912, 101297152,
 102579392, 103861632
root@OPNsense:~ #

```

4.7 Tests durchführen

Mittels `df -h`, `gpart show` und `gpart status` kannst Du überprüfen, ob die von Dir gewünschte Größenänderung erfolgreich übernommen wurden.

```

root@OPNsense:~ # df -h

```

Filesystem	Size	Used	Avail	Capacity	Mounted on
/dev/gpt/rootfs	48G	1.8G	43G	4%	/
devfs	1.0K	1.0K	0B	100%	/dev
devfs	1.0K	1.0K	0B	100%	/var/dhcpd/dev
devfs	1.0K	1.0K	0B	100%	/var/unbound/dev

```

root@OPNsense:~ # gpart show
=>      63  104857537  da0  MBR  (50G)
        63  104857537   1  freebsd [active] (50G)

=>      0  104857537  da0s1  BSD  (50G)
        0           16      - free - (8.0K)
        16  104857521   1  freebsd-ufs (50G)

```

```

root@OPNsense:~ # gpart status

```

Name	Status	Components
da0s1	OK	da0
da0s1a	OK	da0s1

4.8 Reboot

Führe nun einen Reboot der VM aus.

Weiterführende Erklärungen zu FreeBSD zu diesem Thema findest Du hier:

<https://www.digitalocean.com/community/questions/freebsd-growfs-operation-not-permitted-aka-enlarge-your-partition>

4.33 Netzwerkzugriff über Radius

Autor des Abschnitts: @cweikl

RADIUS (Remote Authentication Dial-In User Service) ist ein Client-Server Protokoll, das zur Authentifizierung, Autorisierung und für das Accounting (Triple A - AAA) von Benutzern in einem Netzwerk dient.

Der RADIUS-Server dient als zentraler Authentifizierungsserver, an den sich verschiedene IT-Dienste für die Authentifizierung wenden können. RADIUS bietet sich an, um in grossen Netzen sicherzustellen, dass ausschließlich berechnete Nutzer Zugriff haben. Der Zugriff kann zudem auch auf bestimmte Endgeräte beschränkt werden. Um die Authentifizierungsdaten zu übertragen, wird oftmals das Protokoll EAP (Extensible Authentication Protocol) genutzt.

Viele Geräte und Anwendungen, wie z.B. Access Points, Captive Portals oder Wireless Controller bieten neben einer einfachen Benutzerauthentifizierung auch eine Überprüfung mit Hilfe eines RADIUS-Servers an (WPA-Enterprise, 802.1X). Werden die Geräte so konfiguriert, dass diese zur Authentifizierung den RADIUS-Server nutzen, so kann sichergestellt werden, dass nur berechnete Benutzer Zugriff auf z.B. das WLAN haben.

4.33.1 FreeRADIUS: Einsatz in linuxmuster.net

FreeRadius ist ein Open-Source RADIUS-Server, der in der linuxmuster.net v7 eingesetzt werden kann.

Hinweis: Es wird grundsätzlich empfohlen, zusätzliche Dienste **nicht** auf dem lmn-Server zu installieren.

Dieser RADIUS-Server kann prinzipiell auf der OPNsense®, dem lmn-Server oder auf einem Docker-Host genutzt werden.

Die Benutzerauthentifizierung erfolgt anhand der Daten im ActiveDirectory (AD) des lmn-Servers, die vom RADIUS-Server via LDAP oder direkt abgefragt werden.

Einsatz auf der OPNsense®

Derzeit unterstützt das OPNsense® - Plugin die Radius <-- --> AD Kommunikation mithilfe von auth_ntlm N I C H T.

Eine Dokumentation zur Einrichtung von Freeradius auf der OPNsense® kann daher derzeit nicht erstellt werden.

Einsatz auf dem Imn-Server

Führe nachstehende Schritte durch.

Zugehörigkeit zur Gruppe wifi

Der Zugriff soll über die Schulkonsole gesteuert werden. Dafür werden Benutzer einer speziellen Gruppe wifi hinzugefügt oder daraus entfernt.

Achtung: Das Standardverhalten der linuxmuster.net ist, dass ein neu angelegter Benutzer immer in der Gruppe wifi ist, d.h. auch alle Schüler dürfen zunächst in das WLAN, sobald ein WLAN-Zugriff auf Basis dieser Gruppe wifi erstellt wurde.

Zugehörigkeit zur Gruppe wifi einmalig festlegen

Die Steuerung der Gruppenzugehörigkeit kann auf der Konsole auf dem Imn-Server wie folgt gesetzt werden. Wenn Du z.B. nur die Gruppe der Lehrer und der Schüler der Oberstufenklassen „k1“ und „k2“ für den WLAN-Zugang konfigurieren willst, erstellst Du eine Vorlage und setzt die wifi-Gruppe dann wie folgt:

```
server ~ # cat << EOF > /etc/linuxmuster/sophomorix/default-school/wifi.teachers_and_
↪ oberstufe.conf
    MEMBER_ROLE=teacher,globaladministrator
    MEMBER_CLASS=teachers,k1,k2
    EOF

server ~ # sophomorix-managementgroup --set-wifi teachers_and_oberstufe
```

Um noch weitere einzelne Schüler hinzuzunehmen oder zu entfernen, nutzt Du danach die Funktion `--wifi` bzw. `--nowifi` mit von Komma getrennten Benutzernamen.

```
server ~ # sophomorix-managementgroup --nowifi lempel,fauli
server ~ # sophomorix-managementgroup --wifi schlaubi,torti
```

Freeradius installieren und aktivieren

```
apt install freeradius
```

```
systemctl enable freeradius.service
```

ntlm_auth in samba erlauben

In der Datei `/etc/samba/smb.conf` ist folgende Zeile einzufügen:

```
[global]
...
ntlm_auth = mschapv2-and-ntlmv2-only
```

Danach muss der `samba-ad-dc` Dienst neu gestartet werden:

```
systemctl restart samba-ad-dc.service
```

Radius konfigurieren

Dem Freeradius-Dient muss Zugriff auf `winbind` gegeben werden:

```
usermod -a -G winbindd_priv freerad
chown root:winbindd_priv /var/lib/samba/winbindd_privileged/
```

In dem Verzeichnis `/etc/freeradius/3.0/sites-enabled` in die Dateien `default` und `inner-tunnel` ganz am Anfang unter `authenticate` ist `ntlm_auth` einzufügen.

```
authenticate {
    ntlm_auth
    # ab hier geht es weiter
```

In der Datei `/etc/freeradius/3.0/mods-enabled/mschap` sind im Abschnitt `mschap` zwei Einträge zu ergänzen:

```
mschap {
    use_mppe = yes
    with_ntdomain_hack = yes
    # hier geht es weiter
```

Anpassen des Abschnitts `ntlm_auth` weiter unten. Zuerst das Kommentarzeichen `#` entfernen, dann die Zeile folgendermaßen anpassen:

```
# eine Zeile
ntlm_auth = "/usr/bin/ntlm_auth --allow-mschapv2 --request-nt-key --domain=DOMÄNE --
↪require-membership-of=DOMÄNE\wifi --username=%{%{Stripped-User-Name}:-%{%{User-Name}:-
↪None}} --challenge=%{%{mschap:Challenge}:-00} --nt-response=%{%{mschap:NT-Response}:-
↪00}"
```

Dabei muss `DOMÄNE` durch den eigenen Domänennamen ersetzt werden. Gebe den Inhalt der Datei `/etc/hosts` mit folgendem Befehl aus:

```
less /etc/hosts

Ausgabe:
127.0.0.1 localhost
10.0.0.1 server.linuxmuster.lan server
```

Hostname ist im o.g. Beispiel `server`. Danach folgen Domain und Top-Level-Domain, also: `.linuxmuster.lan`. `DOMÄNE` muss in o.g. `ntlm_auth` in diesem Beispiel durch `linuxmuster.lan` ersetzt werden.

Die Option `-require-membership-of=...` lässt nur Mitglieder der Gruppe `wifi` zu. So funktioniert die WLAN-Steuerung über die WebUI.

Danach ist die Datei `/etc/freeradius/3.0/mods-enabled/ntlm_auth` noch anzupassen. Zuerst ist das Kommentarzeichen `#` zu entfernen. Danach ist die Zeile wie folgt anzupassen:

```
exec ntlm_auth {
    wait = yes
    # eine Zeile
    program = "/usr/bin/ntlm_auth --allow-mschapv2 --request-nt-key --domain=DOMÄNE --
↪require-membership-of=DOMÄNE\wifi --username=%{mschap:User-Name} --password=%{User-
↪Password}"
}
```

DOMÄNE ist hierbei wieder wie zuvor zu ersetzen.

In der Datei `/etc/freeradius/3.0/users` ist ganz oben nachstehende Zeile einzufügen.

```
DEFAULT      Auth-Type = ntlm_auth
```

Nun ist der Freeradius-Dienst neuzustarten:

```
systemctl restart freeradius.service
```

Achtung: Das Defaultverhalten der `lmn7` ist, dass ein neu angelegter User immer in der Gruppe `wifi` ist, d.h. auch alle Schüler dürfen zunächst in das WLAN.

Die Steuerung der Gruppenzugehörigkeit kann auf der Konsole wie folgt gesetzt werden:

```
sophomorph-managementgroup --nowifi/--wifi user1,user2,...
```

Um alle Schüler aus der Gruppe `wifi` zu nehmen, listest Du alle User des Systems auf und schreibst diese in eine Datei. Dies kannst Du wie folgt erledigen:

```
samba-tool user list > user.txt
```

Jetzt entfernst Du alle User aus der Liste, die immer ins Wlan dürfen sollen. Danach baust Du die Liste zu einer Kommazeile um mit:

```
less user.txt | tr '\n' ',' > usermitkomma.txt
```

Die Datei kann jetzt an den o.g. Sophomorph-Befehl übergeben werden:

```
sophomorph-managementgroup --nowifi $(less usermitkomma.txt)
```

WLAN Zertifikate einrichten

Um allen Clients eine Anmeldung mit Zertifikat zu ermöglichen, ist es notwendig, dass der RADIUS-Server die vollständige Zertifikatskette ausliefert. Zu beachten ist, dass zudem für RADIUS bei Zertifikaten eine eigene CA hierfür zu nutzen ist. Es gilt das Prinzip des Organisationsvertrauens.

Der Server von linuxmuster.net verfügt bereits über eine eigene CA. Die Zertifikatsdateien finden sich unter `/etc/linuxmuster/ssl/`.

Mit folgendem Befehl lässt sich der CN des Zertifikats ermitteln:

```
openssl x509 -in /etc/linuxmuster/ssl/cacert.crt -text -noout |more
```

In der Ausgabe ist unter ISSUER nach dem Eintrag CN zu suchen. Dieser kann z.B. wie folgt aussehen:

CN = LINUXMUSTER.LAN

oder

CN=GSHOENNINGEN.LINUXMUSTER.LAN

Zunächst ist für RADIUS ein selbst signiertes Zertifikat zu erstellen. Grundlage ist immer ein privater Schlüssel:

```
cd /etc/linuxmuster/ssl/
openssl genrsa -out radius-key.pem 4096
chgrp ssl-cert radius-key.pem
```

Danach ist ein neues Zertifikat zu beantragen:

```
openssl req -new -key radius-key.pem -out radius.csr -sha512
```

Gebe hierbei die gewünschten Informationen an. Bei Common Name (e.g. server FQDN or YOUR name) []: muss die zuvor ermittelte CN eingetragen werden, die z.B. durch ein vorangestelltes radius ergänzt wird. Ein korrekter Eintrag wäre z.B.: `radius.gshoenningen.linuxmuster.lan`

Das Zertifikat ist nun noch auszustellen. Zuvor wird noch das Kennwort für den CA-Key (`/etc/linuxmuster/ssl/cakey.pem`) benötigt. Das Kennwort findet sich unter `/etc/linuxmuster/.secret/cakey`.

Zur Ausstellung ist folgender Befehl anzugeben und o.g. Kennwort zum Abschluss anzugeben:

```
openssl x509 -req -in radius.csr -CA /etc/linuxmuster/ssl/cacert.pem -CAkey /etc/
linuxmuster/ssl/cakey.pem -CAcreateserial -out radius.pem -days 365 -sha512
```

Die erstellten Dateien sowie die cacert-Dateien sind nun in das Freeradius Zertifikats-Verzeichnis zu kopieren sowie Gruppenzugehörigkeiten und Dateiberechtigungen wie folgt anzupassen:

```
cd /etc/linuxmuster/ssl/
cp cacert.crt cacert.pem radius.csr radius-key.pem radius.pem /etc/freeradius/3.0/certs/
cd /etc/freeradius/3.0/certs/
chgrp freerad cacert.crt cacert.pem radius.csr radius-key.pem radius.pem
chmod 640 cacert.crt cacert.pem radius.csr radius-key.pem radius.pem
```

Danach ist ein Zertifikat zu erstellen, das die gesamte Zertifizierungskette enthält:

```
cd /etc/freeradius/3.0/certs/
cat radius.pem cacert.pem > fullchain.pem
chgrp freerad fullchain.pem
chmod 640 fullchain.pem
```


Passe nun RADIUS so an, dass das Fullchain-Zertifikat genutzt wird.

```
nano /etc/freeradius/3.0/mods-enabled/eap

eap {
    [...]
    tls-config tls-common {
        [...]
        private_key_file = /etc/freeradius/3.0/certs/radius-key.pem
        certificate_file = /etc/freeradius/3.0/certs/fullchain.pem
        ca_file = /etc/freeradius/3.0/certs/cacert.pem
        [...]
    }
    [...]
}
```

Hinweis: Je nach Server-Distribution ist ggf. die Datei EAP unter /etc/raddb/mods-enabled/eap oder je nach Radius-Version unter /etc/freeradius/3.2/mods-enabled/eap anzupassen.

Danach den Dienst neu starten:

```
systemctl restart freeradius.service
```

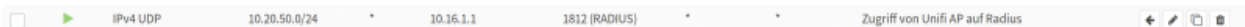
Melden die Clients sich nun im WLAN an, so liefert der RADIUS die Zertifikatskette aus und bei der ersten Herstellung der Verbindung muss das Zertifikat auf dem Client akzeptiert werden, so dass es dort dann importiert wird.

Auf diese Weise kann WPA-Enterprise auch mit neueren Client-Betriebssystemen genutzt werden.

Firewallregeln anpassen

Auf der Firewall OPNsense® muss je nach eigenen Voraussetzungen dafür gesorgt werden, dass die AP's aus dem Wlan-Netz den Server auf dem Port 1812 via udp erreichen können. Es ist darauf zu achten, dass die IP des Servers den eigenen Netzvorgaben entspricht (also z.B. 10.0.0.1/16 oder /24 oder 10.16.1.1/16 oder /24)

Die Regel auf der OPNsense® hierzu könnte, wie nachstehend abgebildet, eingetragen werden.



Jetzt sollte die Authentifizierung per WPA2-Enterprise funktionieren, sofern der Testuser in der Gruppe wifi ist. Ein Zertifikat ist nicht erforderlich.

Sollte das nicht funktionieren, hält man den Freeradius-Dienst an und startet ihn im Debugmodus.

```
service freeradius stop
service freeradius debug
```

Jetzt sieht man alle Vorgänge während man versucht, sich mit einem Device zu verbinden.

APs im Freeradius eintragen

Die APs müssen im Freeradius noch in der Datei `/etc/freeradius/3.0/clients.conf` eingetragen werden. Dies erfolgt wie in nachstehendem Schema dargestellt:

```
client server {
ipaddr = 10.0.0.1
secret = GeHeim
}

client opnsense {
ipaddr = 10.0.0.254
secret = GeHeim
}

client unifi {
ipaddr = 10.0.0.10
secret = GeHeim
}
```

Um den APs feste IPs zuzuweisen, sollten diese auf dem lmn-Server in der Datei `/etc/linuxmuster/sophomorix/default-school/devices.csv` eingetragen sein.

Je nachdem, ob in jedem (Sub)-netz die APs angeschlossen werden, ist die zuvor dargestellte Firewall-Regel anzupassen. Der Radius-Port in der OPNsense® müsste dann z.B. von Subnetz A (blau) zu Subnetz B (grün Servernetz) geöffnet werden, damit alle APs Zugriff auf den Radius-Dienst erhalten.

4.34 Netzwerksegmentierung

Autor des Abschnitts: @cweikl, @MachtDochNix (pics)

Im ersten Schritt erhältst Du Hinweise zur Anpassung der Netzwerkkonfiguration der Server mithilfe des Skript `lmn71-prepare`. Im zweiten Schritt wirst Du in das Thema Netzsegmentierung eingeführt. Wir geben Sie Hilfestellung zur Planung der neuen Netzstruktur und deren vollständigen Umsetzung.

4.34.1 Netzbereich anpassen

Autor des Abschnitts: @cweikl

Hinweis: Die Anpassung des Netzbereichs ist vor Aufruf des eigentlichen Setups auszuführen. Dies erfolgt mit dem Paket `lmn71-prepare`.

Vorgehen

Die OPNsense® ist im gewünschten Zielnetz einzurichten (z.B. 10.17.0.254/16). Diese muss für alle Server / Ubuntu-VMs als Gateway angegeben werden. Dies kann mithilfe des lmn71-prepare Skripts für den gewünschten neuen Netz-bereich (z.B. 10.17.0.0/16) vorbereitet werden.

Gleiches gilt für die Vorbereitung der from-scratch installierten Server.

Das Skript lmn71-prepare

Das Skript lmn71-prepare installiert für Dich das Paket linuxmuster-prepare mit all seinen Abhängigkeiten und es richtet die zweite Festplatte für den Serverbetrieb ein.

Achtung: Nachstehende Beschreibung muss für 7.1 noch überarbeitet werden !

- Vorbereitung: Lade das Skript hier herunter: `wget https://raw.githubusercontent.com/linuxmuster/linuxmuster-prepare/master/lmn71-appliance`.
- Mach das Skript nun ausführbar: `chmod +x lmn71-appliance` ausführbar
- Starte das Skript als Benutzer root mit: `./lmn71-appliance -p server -l /dev/sdb`. Hierbei wird auf dem angegebenen Device/ der HDD ein LVM eingerichtet.
- Für weitere Hinweise zum linuxmuster-prepare Skript siehe: <https://github.com/linuxmuster/linuxmuster-prepare>

Im Anschluss kann das Setup ausgeführt werden, das dann den Netzbereich ausliest und für die weitere Einrichtung verwendet.

Hinweise zum Skript

Das Skript lmn71-appliance bereitet eine Appliance (VM) für die linuxmuster v7.1 vor:

- Es bringt das Betriebssystem auf den aktuellen Stand,
- installiert das Paket linuxmuster-prepare und
- startet dann das Vorbereitungsskript linuxmuster-prepare, das die für das jeweilige Appliance-Profil benötigten Pakete installiert, das Netzwerk konfiguriert, das root-Passwort auf Muster! setzt und im Falle des Serverprofils LVM einrichtet.

Das Skript kennt beim Aufruf folgende Übergabeparameter:

Optionen

Parameter	Wert	Bedeutung
-t,	-hostname=<hostname>	Hostname der Appliance, falls weggelassen wird der Profilname verwendet.
-n,	-ipnet=<ip/bitmask>	IP-Adresse und Bitmaske des Hosts (Standardwert ist 10.0.0.[1,2,3]/16, abhängig vom Profil).
-p,	-profile=<server>	appliance-Profil, wurde -n nicht angegeben, wird die IP-Adresse automatisch gesetzt: server 10.0.0.1
-l,	-pvdevice=<device>	Pfad zum LVM-Device (nur bei Serverprofil).
-f,	-firewall=<ip>	Firewall-/Gateway-/Nameserver-Adresse (Standard x.x.x 254).
-d,	-domain=<domain>	Domänenname (Standard: linuxmuster.lan).
-h,	-help	Hilfe anzeigen.

Profilvorgaben

server:

Paket linuxmuster-base7 (v7.1) mit allen seinen Abhängigkeiten wird installiert. Ist eine zweite Festplatte definiert und wird der Parameter `-l, --pvdevice=<device>` angegeben, wird diese wie folgt mit LVM eingerichtet (Werte beziehen sich auf eine Festplattengröße von 100G. Für das LV default-school wird immer der verbleibende Rest genommen. Festplattengröße muss daher mindestens 70G betragen.):

LV Name	LV Pfad	Mountpoint	Größe
var	/dev/vg_srv/var	/var	10G
linbo	/dev/vg_srv/linbo	/srv/linbo	40G
global	/dev/vg_srv/global	/srv/samba/global	10G
default-school	/dev/vg_srv/default-school	/srv/samba/default-school	40G

Beispiele

```
./lmm71-appliance -p server -l /dev/sdb
```

Richtet Serverprofil mit LVM auf 2. Festplatte mit Standardwerten ein:

- Hostname server,
- IP/Bitmask 10.0.0.1/16,
- Domänenname linuxmuster.lan
- Gateway/DNS 10.0.0.254

Server-Appliance vorbereiten

Appliance mit 2 Festplatten einrichten, zum Beispiel:

- HD 1: 25G (Root-Dateisystem)
- HD 2: 100G (LVM)
- Ubuntu Server 18.04 Minimalinstallation durchführen.
- System in eine Partition auf HD 1 installieren (keine Swap-Partition),
- HD 2 unkonfiguriert lassen.
- Nach dem ersten Boot als root einloggen und Prepare-Skript herunterladen:

```
# wget https://raw.githubusercontent.com/linuxmuster/linuxmuster-prepare/master/lmn71-
↪appliance
```

* Skript ausführbar machen

```
# chmod +x lmn71-appliance
```

* und starten:

```
./lmn71-appliance -p server -l /dev/sdb
```

* Appliance herunterfahren und Snapshot erstellen.

Anwendung auf die Appliances

Zuerst ist die OPNsense® Firewall anzupassen.

OPNsense® Firewall

Nach dem ersten Start als Benutzer root mit dem Passwort **Muster!** anmelden. Danach erscheint nachstehendes Konsolenmenü der OPNsense®:

Zunächst müssen die Netzwerk-Interfaces unter Mneüpunkt 1 neu zugordnet werden. Je nach Hypervisor werden unterschiedliche Namen für die Netzwerkinterfaces verwendet - z.B. em0 / vtnet0

- em0/vtnet0 → LAN
- em1/vtnet1 → WAN
- em2/vtnet2 → OPT1

Um nun die vorgegebene Netzwerkkonfiguration anzupassen, ist das Menü 2 zu wählen. In nachstehendem Beispiel wird das LAN-Interface auf die IP-Adresse 10.16.1.254/12 geändert.

Der DHCP-Dient auf der OPNsense® sollte in jedem Fall ausgeschaltet bleiben. Sollte der Domänenname geändert werden, kann dies später via OPNsense®-GUI erfolgen.

Anschließend muss die OPNsense® neu gestartet werden.

Im zweiten Schritt muss der Netzbereich der Server-Appliance angepasst werden.

```

FreeBSD/amd64 (OPNsense.localdomain) (ttyv0)
login: root
Password:
Last login: Tue Aug 15 14:40:26 from 10.0.0.253
-----
:      Hello, this is OPNsense 17.7      :
:                                       :
: Website:      https://opnsense.org/   :
: Handbook:     https://docs.opnsense.org/ :
: Forums:       https://forum.opnsense.org/ :
: Lists:        https://lists.opnsense.org/ :
: Code:         https://github.com/opnsense :
:                                       :
-----
0) Logout                                7) Ping host
1) Assign interfaces                    8) Shell
2) Set interface IP address             9) pfTop
3) Reset the root password              10) Firewall log
4) Reset to factory defaults            11) Reload all services
5) Power off system                     12) Upgrade from console
6) Reboot system                        13) Restore a backup

Enter an option: 

```

```

Configure IPv4 address LAN interface via DHCP? [y/N]
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.16.1.254

Subnet masks are entered as bit counts (like CIDR notation).
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 12

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via WAN tracking? [Y/n] n
Configure IPv6 address LAN interface via DHCP6? [y/N] n

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? [y/N] 

```

Server-Appliance

Nach dem ersten Start der Server-Appliance als root einloggen (Passwort: Muster!). Danach ist die Netzwerkverbindung für den gewünschten Bereich anzupassen. Das Netzwerkinterface des Server muss sich im gleichen Netzsegment wie die LAN-Schnittstelle der OPNsense® befinden.

```
# ip -4 -br -a addr show | grep -v ^lo
```

der o.g. Befehl gibt einen Überblick über alle gefundenen Interfaces.

Das entsprechende Interface ist unter Ubuntu 18.04 nun anzupassen. Dies erfolgt in der Datei `/etc/netplan/01-netcfg.yaml` (z.B. ens33):

```
network:
  ethernets:
    ens33:
      ...
```

Hinweis: ggf. kann die YAML-Datei auch einen anderen Namen nach der Erstinstallation aufweisen. Zu Beginn findet sich nur eine YAML-Datei in dem Verzeichnis.

Änderungen in der Datei speichern und danach wie folgt übernehmen:

```
# netplan apply
```

Mithilfe eines Ping-Test wird zuerst geprüft, ob der Server das Gateway erreicht. Im o.g. Beispiel müsste dies wie folgt überprüft werden:

```
ping 10.0.0.254
```

Ist dies erfolgreich, muss die Appliance mit dem Skript `lmn71-appliance` für das Setup vorbereitet werden. Netzwerkadressen und Domänenname werden damit gesetzt.

Eine eigene IP-/Netzwerkconfiguration übergibt man mit dem Parameter `-n`:

```
./lmn71-appliance -n 192.168.0.1/16 oder
./lmn71-appliance -n 192.168.0.1/255.255.0.0
```

Einen eigenen Domänennamen übergibt man mit `-d`:

```
./lmn71-appliance -d schule.lan
```

Eine abweichende Firewall-IP setzt man mit `-f`:

```
./lmn71-appliance -f 192.168.0.10
```

Das alles kann **in einem Schritt** erfolgen:

```
./lmn71-appliance -d schule.lan -n 192.168.0.1/16 -f 192.168.0.10
```

Minimaler Aufruf, wenn die Standard-Netzwerkeinstellungen (10.0.0.0/16) verwendet werden sollen:

```
./lmn71-appliance --default -p <Profil>
```

Gesetzt wird damit:

- Server: IP 10.0.0.1, Hostname server
- Firewall-IP: 10.0.0.254, Hostname firewall
- Domänenname: linuxmuster.lan

Einen Überblick über alle Optionen erhält man mit dem Parameter -h.

Hinweis: Das Default-Rootpasswort **Muster!** darf nicht geändert werden, da die Setuproutine dieses voraussetzt. Nach der Vorbereitung mit linuxmuster-prepare muss die Appliance neu gestartet werden.

Im letzten Vorbereitungsschritt muss die Appliance noch aktualisiert werden:

```
# apt update && apt -y dist-upgrade
```

Danach kann das Setup mit der WebUI oder auf der Konsole auf dem Server aufgerufen werden.

4.34.2 Netzwerksegmentierung

Autor des Abschnitts: @cweikl, @MachtDochNix (pics)

Vorbemerkungen

Aus datenschutzrechtlichen Überlegungen ist ein schulisches Netzwerk in drei Bereiche mit unterschiedlichen Absicherungen und Berechtigungsstufen zur Verarbeitung und Speicherung von personenbezogenen Daten zu unterteilen:

- Verwaltungsnetz (Verwaltungsprogramme, dienstliche Beurteilungen etc.)
- Lehrernetz (Stundenplan, Kompetenzen, Noten, etc.)
- pädagogisches Netz (keine Verarbeitung personenbezogener Daten)

Wesentliches Ziel bei der Gestaltung der schulischen Netzinfrastruktur ist es, diese unterschiedlichen personenbezogenen Daten besonders zu schützen. Dabei ist sicherzustellen, dass nur diejenigen Personen auf solche personenbezogene Daten zugreifen können, die zur Erfüllung ihrer dienstlichen Aufgaben unbedingt erforderlich sind.

Es muss sichergestellt werden, dass ein **Zugriff auf das Lehrernetz und Verwaltungsnetz vom pädagogischen Netz aus wirksam verhindert** wird. Der Einsatz von VLANs und die Nutzung virtueller Maschinen wird hierzu explizit zugelassen.

Im **pädagogischen Schulnetz dürfen grundsätzlich keine personenbezogenen Daten von Schülern** verarbeitet und gespeichert werden, außer Name und Klassenzugehörigkeit des Schülers sowie die hierzu erforderlichen technischen Daten, die direkt für die Unterrichtsgestaltung erforderlich sind. Insbesondere dürfen grundsätzlich keinerlei personenbezogene Daten zu Verhalten oder Leistung (Bewertungen, Beurteilungen) eines Schülers verarbeitet werden. Insgesamt dürfen in diesem Netz nur die zur Aufgabenerfüllung unbedingt erforderlichen Daten verarbeitet werden.

In dieser Dokumentation geht es im Folgenden **ausschließlich um den Betrieb des pädagogischen Netzes**.

Es wird empfohlen, das **pädagogische Netz** wiederum in mindestens drei Bereiche / Subnetze zu unterteilen:

- Lehrernetz
- Schülernetz
- Servernetz

Hinweis: Das Lehrernetz im pädagogischen Netz besitzt aufgrund von Firewallregeln keine eingehenden Verbindungen vom Schülernetz aus. Es besteht aufgrund des Zugangsschutzes ein Sonderstatus. Eine Verarbeitung von **personenbezogenen Daten** in diesem Segment darf im pädagogischen Netz **nicht erfolgen!**

Sollte z.B. WLAN zum Einsatz kommen oder sollen weitere Anforderungen erfüllt werden, so werden weitere Subnetze empfohlen.

Diese Dokumentation greift den Fall einer **Unterteilung des pädagogischen Netzes in sieben Subnetze** auf. Eine Erweiterung/Anpassung um weitere Subnetzbereiche, ist später analog zu dem in dieser Dokumentation beschriebenen Vorgehen möglich. Die Umsetzung der Segmentierung erfordert managebare L2- und L3-Switches, die VLANs verwalten können. Hierzu können Switches beliebiger Hersteller genutzt werden.

Die Konfigurationsschritte für den L3-Switch werden anhand eines Cisco SG300-300-28 beispielhaft dargestellt. Für die Konfiguration der L2-Switches werden die Schritte anhand eines Cisco SF200-24 exemplarisch verdeutlicht. Bei dem Einsatz anderer Switches sind die dargestellten Konfigurationsschritte entsprechend anzupassen.

Am Ende des Kapitels findest Du weitere Konfigurationen für andere L3-Switches, die Du zur Anpassung auf Dein Netzszenario nutzen kannst.

Geplante Netzwerkstruktur

Bei dem Standard-Setup des linuxmuster.net Servers (v7.1) wird das Netz 10.0.0.0/16 zur Einrichtung vorgesehen. Eine Unterteilung kann bereits in der Form erfolgen, dass im 2. Oktett weitere Netzsegmente genutzt werden.

Beispiel:

- Servernetz, Netzwerkadressen 10.0.0.0/16
- Lehrernetz, Netzwerkadressen 10.1.0.0/16
- Schülernetz, Netzwerkadressen 10.2.0.0/16

Es wäre so eine Einteilung der Rechner eines Raumes im dritten Oktett problemlos möglich, z.B. alle Rechner in Raum 107 sind im Schülernetz und haben Adressen aus dem Bereich 10.2.107.x, alle Rechner des Lehrerzimmers sind im Lehrernetz und haben Adressen aus dem Bereich 10.1.120.x. Die Unterscheidung der Räume erfolgt so im 3. Oktett, die Unterscheidung der Subnetze im 2. Oktett.

Sollen weitere Segmente gebildet werden, die z.B. jeden Raum als eigenes Segment (VLAN) abbilden, so bietet es sich an, kleinere Segmente zu bilden.

Nachstehend soll daher das **Vorgehen zur Vorbereitung einer Segmentierung mit kleineren IP-Netzen** dokumentiert werden. Es sollen nachstehende sieben Segmente gebildet werden:

VLAN Name	Verwendung	Netzwerkadressen
Internet	alle Server an der WAN - Schnittstelle	IP-Netz der Firewall WAN
Server	alle Server/-VMs im LAN	10.0.0.0/24
WLAN-LuL	ein WLAN-Netz für Lehrerinnen und Lehrer	10.3.0.0/24
WLAN-SuS	ein WLAN-Netz für Schülerinnen und Schüler	10.4.0.0/24
Lehrer	Zugriff mit Lehrer PCs, Laptops	10.1.0.0/24
Raum100	Zugriff mit Schulungsgeräten im Raum 100	10.2.100.0/24
Raum200	Zugriff mit Schulungsgeräten im Raum 200	10.2.200.0/24

Für die Unterteilung sind auf **allen** Switches entsprechende VLANs in gleicher Weise einzurichten. Die Verbindungen zwischen den Switches werden als Trunks (bzw. Tagged-Ports) definiert, die über Gerätegrenzen hinweg die Daten der

VLANs weiterleiten. Die Ports auf den Switches sind i.d.R. als untagged ports zu konfigurieren und den gewünschten VLANs zuzuordnen (port-basierte VLANs), so dass die an den Ports angeschlossenen Geräte ihre Daten in das zugeordnete VLAN schicken.

Der L3-Switch erhält in jedem VLAN die letzte nutzbare IP-Adresse - also z.B. für das VLAN Lehrer die IP *10.1.0.254*, außer in den VLANs, in denen die Firewall im jeweiligen Subnetz bereits diese IP-Adresse nutzt.

VLAN IDs und Gateway-IPs

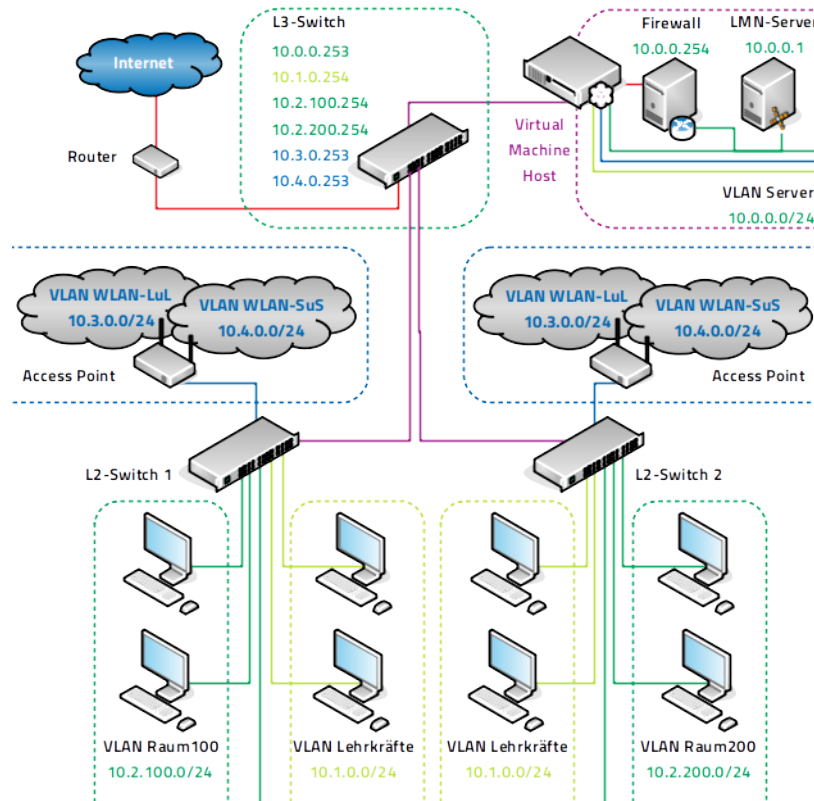
In dieser Dokumentation werden folgende VLAN-IDs und Gateway-IPs verwendet:

VLAN Name	VLAN ID	Gateway-IP (+ Firewall-IP)
VLAN Internet	5	IP aus dem Netz der Firewall an der Schnittstelle WAN
VLAN Server	10	10.0.0.253 (Firewall: 10.0.0.254)
VLAN WLAN LuL	20	10.3.0.253 (Firewall: 10.3.0.254)
VLAN WLAN SuS	30	10.4.0.253 (Firewall: 10.4.0.254)
VLAN Lehrer	40	10.1.0.254
VLAN Raum100	100	10.2.100.254
VLAN Raum200	200	10.2.200.254

Hinweis: Das VLAN 3 wird auf den Switchen zusätzlich eingerichtet und als Management VLAN für die Netzkomponenten genutzt. Das Default VLAN 1 wird hingegen deaktiviert. In diesem VLAN 3 wird das Netz 192.168.1.0/24 genutzt. Der L3-Switch erhält die Adresse 192.168.1.254/24, der L2-Switch die Adresse 192.168.1.250/24.

Damit DHCP-Anfragen der Clients aus dem internen Netz an den Server 10.0.0.1 weitergeleitet werden, muss auf dem L3-Switch ein DHCP-Relay-Agent konfiguriert werden. Entsprechende Hinweise finden sich hierzu bei der Dokumentation zur Konfiguration des L3-Switches.

Geplante Netzsegmentierung



In der Abbildung wird die Verbindung zwischen dem L3-Switch, dem VM-Host (Hypervisor) und zwei weiteren L2-Switchen dargestellt. Die Verbindungen zwischen dem L3-Switch und dem VM-Host sowie zwischen dem L3-Switch und den beiden L2-Switchen sind **lila als Trunk** (Cisco) bzw. tagged port (HP) gekennzeichnet. Dies bedeutet, dass die Uplinks zwischen den Switchen bzw. zwischen Switch und Hypervisor so zu konfigurieren sind, dass diese als Trunks arbeiten und o.g. VLANs als **allowed VLANs** aufweisen, so dass die Daten der VLANs über diese Verbindungen weitergereicht werden. An den L2-Switchen werden die benötigten Ports z.B. für die Computer in einem Fachraum als **untagged ports** definiert und dem jeweiligen VLAN zugeordnet (z.B. für Raum 200 dem VLAN 200).

Verfügt der VM-Server über mehrere Netzwerkschnittstellen, so sollten diese gebündelt werden (je nach Hersteller werden hierfür die Begriffe NIC Bonding, LinkAggregation, Etherchannel verwendet), um den Datendurchsatz zu verbessern. Zudem können so die VMs recht flexibel den einzelnen VLANs zugeordnet werden. Die Bündelung von Ports kann ebenfalls für die Verbindung zwischen den Switchen (Uplinks) genutzt werden. In dieser Dokumentation soll die LinkAggregation am Beispiel des L3-Switch verdeutlicht werden. Es werden für 12 Ethernet-Schnittstellen drei Link-Aggregation Ports bestehend aus jeweils vier Ethernet-Schnittstellen gebildet, die dann entsprechend konfiguriert werden.

Überblick zum Vorgehen

Nachstehende Auflistung gibt einen Überblick zu den erforderlichen Schritten zur Umsetzung der o.g. Netzsegmentierung bei einer neu zu installierenden linuxmuster v7.1.

- 1) L3-Switch und L2-Switches gemäß nachstehender Anleitung konfigurieren und testen.
- 2) Hypervisor: LACP-Bonds und VLAN Bridges konfigurieren.
- 3) VMs importieren.
- 4) Netzwerkkarten (NICs) der importierten VMs den korrekten VLAN Bridges zuordnen, ggf. weitere NICs hinzufügen und diese den korrekten VLAN Bridges zuordnen.

- 5) OPNsense®-VM starten und nach dem Login die Netzwerkkarten korrekt zuordnen (MAC-Adressen und VLAN Bridges helfen dabei die richtige Bezeichnung zu identifizieren).
- 6) OPSense VM: Korrekte IPs den NICs zuordnen (LAN: 10.0.0.254/24, WAN: DHCPv4, OPT1: 10.3.0.254/24, OPT2: 10.4.0.254/24, kein Upstream Gateway eintragen)
- 7) Update OPNsense®, danach Reboot.
- 8) lmn7 Server: NIC - VLAN Bridge für VLAN 10 zuordnen, VM starten, danach `apt update && apt dist-upgrade`, reboot.
- 9) lmn7 Server: Adressbereich anpassen: `linuxmuster-prepare -s -u -p server -n 10.0.0.1/24 -f 10.0.0.254`
- 10) wie unter 9) identisches Vorgehen für Opsi- und Docker-VM - Achtung: abweichende IPs und Profile
- 11) Zugriff vom Server zur Firewall, zu OPSI und Docker via SSH sicherstellen. Danach alle VMs herunterfahren.
- 12) Den Konfigurationsstand der vier VMs mithilfe von Snapshots sichern. Danach alle vier VMs starten.
- 13) linuxmuster-setup auf dem Server ausführen - muss erfolgreich durchlaufen, alle VMs werden neu gestartet.
- 14) Erreichbarkeit der VMs und Internet-Zugriff testen, danach wieder Snapshots erstellen.
- 15) In der Datei `subnets.csv` die Netzsegmentierung eintragen und speichern.
- 16) Die Segmentierung mithilfe des Befehls `linuxmuster-import-subnets` übernehmen.
- 17) Kontrolle der Eintragungen in der Datei `/etc/netplan/01-netcfg.yaml` (siehe Eintragungen später bei der detaillierten Beschreibung).
- 18) Tests zur Erreichbarkeit der VMs.
- 19) `devices.csv`: Weitere Computer aus den verschiedenen Netzsegmenten eintragen und mit `linuxmuster-import-devices` übernehmen.
- 20) PCs, die in der `devices.csv` definiert wurden, an die entsprechenden Ports anschliessen und prüfen, ob diese eine IP aus dem gewünschten Bereich erhalten. Erreichbarkeit des Servers, der Firewall und des Internets von den Clients aus testen.

Konfiguration des L3-Switches

Konfigurationsschritte auf dem Layer-3-Switch:

- VLANs für jedes Subnetz definieren
- VLANs den Ports zuordnen
- DHCP-Relaying einrichten (damit DHCP-Broadcasts in alle Subnetze geroutet werden)
- UDP-Relaying einrichten (damit WOL über Subnetzgrenzen hinweg funktioniert)
- Access Listen definieren (Zugriffe in Subnetze werden unterbunden mit Ausnahme des Servernetzes, das aus allen Subnetzen heraus erreicht werden muss)

Einspielen der vordefinierten Konfiguration

Hinweis: Die Firmware des Cisco L3 Switch SG300-28 ist vorab auf die aktuellste Version (hier: 1.4.8.6) zu aktualisieren. Für die Aktualisierung ist wesentlich, welche aktuelle FW-Version und welche Boot Version genutzt werden. Bei älteren Versionen ist eine Aktualisierung nur über Zwischenschritte möglich. So muss z.B. von FW 1.1.2.0 via 1.3.7.18 via 1.4.75 via 1.4.11.2 aktualisiert werden. Um die die Boot Version zu aktualisieren, ist via TFTP schrittweise die jeweilige rfb-Datei des FW-Images hochzuladen und danach ist das Gerät jeweils erneut zu starten. Hier der Link zur aktuellen Firmware - [FW](#)

Die Version der Firmware sowie die Boot Version lassen sich unter **Status** und **Statistics** im Untermenü **System Summary** anzeigen. Wie in nachstehender Abbildung:

System Summary			
System Information		Software Information	
System Operational Mode:	L3 Mode	Firmware Version (Active Image):	1.4.11.2
System Description:	SG300-28 28-Port Gigabit Managed Switch	Firmware MD5 Checksum (Active Image):	9cc30194a4d2a2fe9f8d3f2670a9f624
System Location:	Edit	Firmware Version (Non-active):	1.4.11.2
System Contact:	Edit	Firmware MD5 Checksum (Non-active):	9cc30194a4d2a2fe9f8d3f2670a9f624
Host Name:	SG300-24-L3 Edit	Boot Version:	1.3.5.06
System Object ID:	1.3.6.1.4.1.9.6.1.83.28.1	Boot MD5 Checksum:	da44c9c583e5a8a274f911c4d16f501e
System Uptime:	0 day(s), 2 hr(s), 22 min(s) and 0 sec(s)	Locale:	en-US
Current Time:	22:26:30;2019-Sep-26	Language Version:	1.4.11.2
Base MAC Address:	00:38:df:d8:3d:eb	Language MD5 Checksum:	N/A
Jumbo Frames:	Disabled		

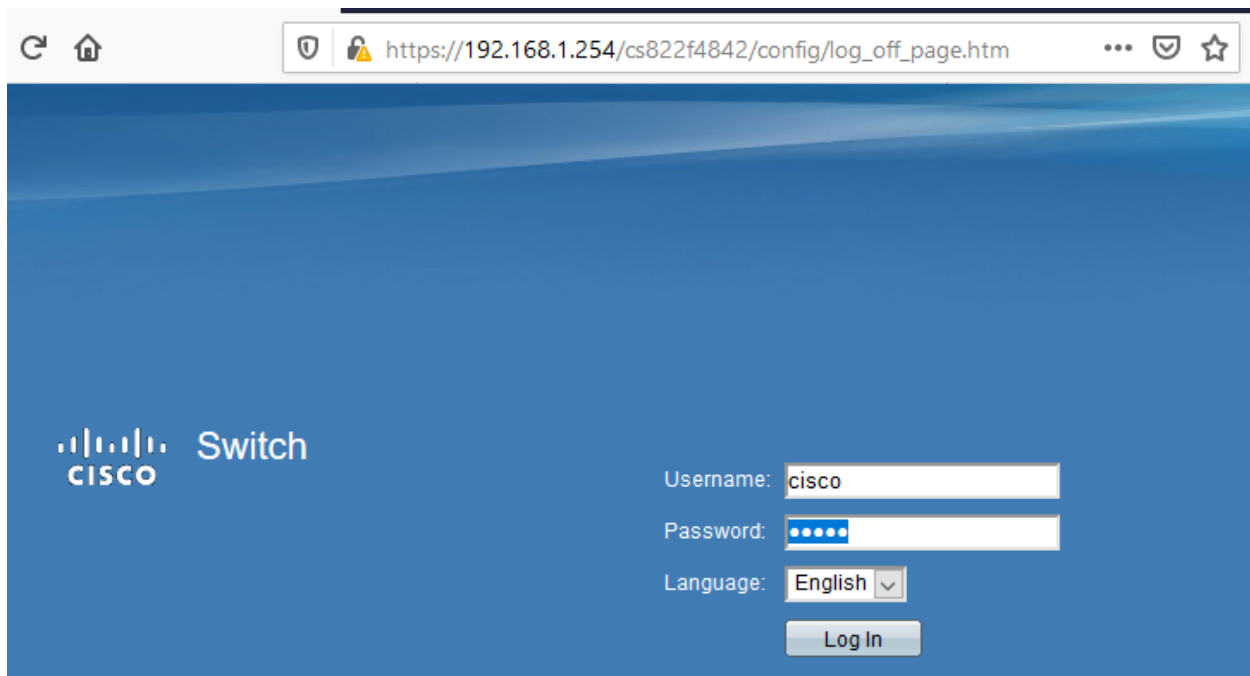
Für den L3-Switch Cisco SG300-28 steht die vorbereitete Konfigurationsdatei zur Verfügung, die die Konfiguration auf dem L3-Switch so einspielt, wie diese in dieser Dokumentation beschrieben wird.

Download

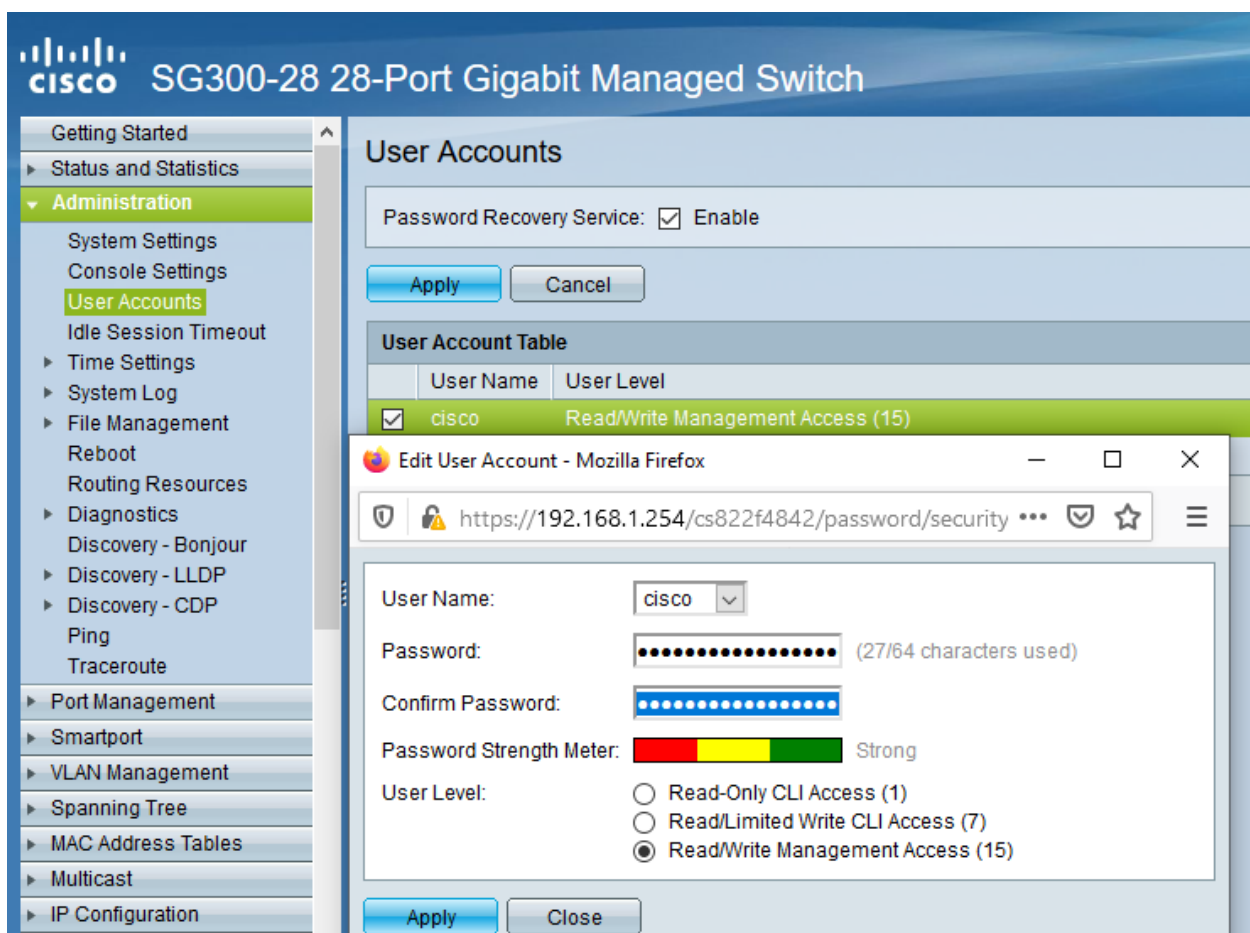
- Konfiguration für v7.1 mit Server-IP 10.0.0.1/24.

Upload der Konfiguration: Schritt für Schritt

Hinweis: Im Auslieferungszustand kann auf den Cisco Switch mit der IP 192.168.1.254/24 zugegriffen werden. Diese IP wird in dieser Konfiguration dem VLAN 3 (Management) zugewiesen, so dass nach Einspielen der Konfiguration und dem Reboot weiterhin mit dieser Adresse die Konfiguration über den access port 24 angepasst werden kann.



Meldest Du Dich als Benutzer cisco mit dem Kennwort cisco (Voreinstellungen) an.



Danach erfolgt der Wechsel in das Menü Administration --> User Accounts. Dort ist der betreffende Benutzer

zer auszuwählen, mit dem Menüpunkt Edit ist das Kennwort des Benutzers neu zu setzen. Die neueren Firmware-Versionen geben eine Kennwort-Komplexität vor.

The screenshot shows the Cisco SG300-28 28-Port Gigabit Managed Switch web interface. The left sidebar shows the navigation menu with 'Administration' expanded and 'System Settings' selected. The main content area is titled 'System Settings' and contains the following fields:

- System Description:** SG300-28 28-Port Gigabit Managed Switch
- System Location:** (0/160 characters used)
- System Contact:** (0/160 characters used)
- Host Name:**
 - ☐ Use Default
 - ☒ User Defined SG300-24-L3 (11/58 characters used; Default: switchd83deb)
- System Mode:**
 - ☐ L2
 - ☒ L3
- Custom Banner Settings:**
 - Login Banner:** (0/1000 characters used)

A 'Preview...' button is located at the bottom left of the Custom Banner Settings section.

Im Menü Administration --> System Settings ist der Name für den Switch zu vergeben und der System-Modus ist auf L3 zu ändern. Die Änderungen sind dann mit Apply zu übernehmen.

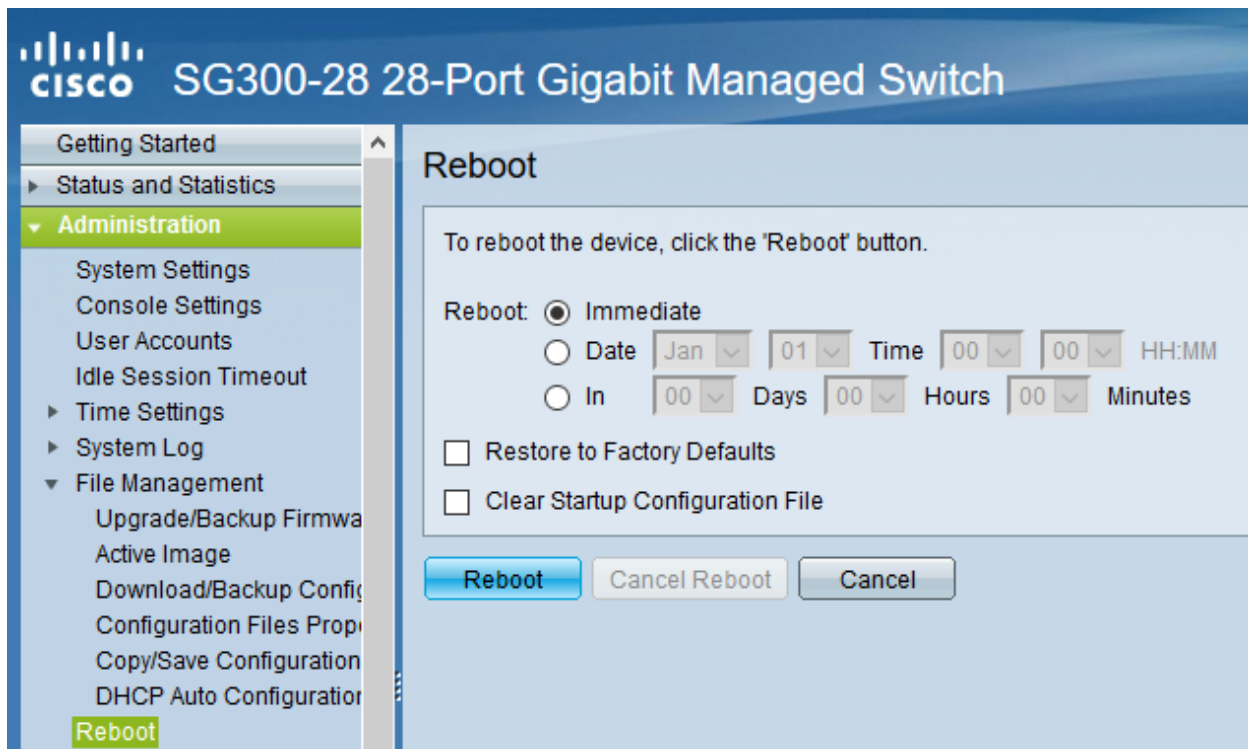
The screenshot shows the Cisco SG300-28 28-Port Gigabit Managed Switch web interface. The left sidebar shows the navigation menu with 'Administration' expanded and 'Download/Backup Configuration/Log' selected. The main content area is titled 'Download/Backup Configuration/Log' and contains the following fields:

- Transfer Method:**
 - ☐ via TFTP
 - ☒ via HTTP/HTTPS
 - ☐ via SCP (Over SSH)
- Save Action:**
 - ☒ Download
 - ☐ Backup
- Source File Name:** Durchsuchen... Keine Datei ausgewählt.
- Destination File Type:**
 - ☐ Running configuration file
 - ☒ Startup configuration file

Buttons for 'Apply' and 'Cancel' are located at the bottom.

Dies erfolgt im Menü Administration --> File Management --> Download/BackupConfig. Die hochzuladende Datei ist als sog. Startup configuration file hochzuladen. Mit Durchsuchen ist die heruntergeladene Konfigurationsdatei anzugeben.

Ist der Upload erfolgreich verlaufen, so muss der Switch neu gestartet werden, um die Konfiguration anzuwenden.



Der Neustart ist über das Menü Administration --> File Management --> Reboot durchzuführen.

Nach dem Neustart meldest Du Dich erneut an dem L3-Switch an und kontrollieren nochmals die Switch-Ports. Hierbei ist zwischen Access-Ports (port-basierte VLANs) und Trunk-Ports zu unterscheiden.

Hinweis: In der bereitgestellten Konfigurationsdatei ist der Login cisco mit dem Kennwort cisco für die weitere Konfiguration vorhanden - dies gilt ebenfalls für die IP 192.168.1.254/24 des Switches. Bei Verbindung via Port GE24 kann so eine Verbindung zur weiteren Anpassung der Konfiguration hergestellt werden.

Allgemeine Hinweise zur Konfiguration der Switch-Ports

Für jeden Switchport muss festgelegt werden, in welchem (VLAN-)Modus dieser arbeitet (Access, Trunk, allgemein u.a.) und welche Mitgliedschaft diese im VLAN X aufweist (verboten, aktuell ausgeschlossen, Mitglied tagged oder untagged). Bei der Mitgliedschaft werden die Daten mit oder ohne Tag weitergeleitet. Je nach Fall kann es also sein, dass ein Tag hinzugefügt oder gelöscht wird.

- **ausgeschlossen:** Datenpakete, die mit der VLAN-ID x getaggt sind, werden verworfen.
- **tagged:** Datenpakete, die mit der VLAN-ID x getaggt sind, werden weitergeleitet.
- **untagged:** Von Datenpaketen, die mit der VLAN-ID x getaggt sind, wird die VLAN-ID entfernt und zum Client weitergeleitet. Die meisten Clients können mit getaggtten Datenpaketen nichts anfangen.
- **PVID:** Bei einem Port, der mit der PVID x markiert ist, werden alle ungetaggtten Datenpakete des Clients mit der VLAN-ID x getaggt.

Anwendung auf das Ausgangsbeispiel

Nachstehende Ausführungen, dienen dazu, die eingespielte Konfiguration zu prüfen oder ggf. Anpassungen für abweichend eingesetzte Hardware zu erstellen.

Definition der Link Aggregation Ports

- LAG1: Ports 1,2,13,14 -> Verbindung zu VMs / Servern
- LAG2: Ports 3,4,15,16 -> Verbindung zu VMs / Servern
- LAG3: Ports 25-28 -> Uplink/Trunk zu L2-Switches

LAG Management

Load Balance Algorithm: ☒ MAC Address ☐ IP/MAC Address

LAG	Name	LACP	Link State	Active Member	Standby Member
<input type="radio"/> LAG 1	Port 1,2,13,14 Trunk-SRV, VLANs 3,5,10,20,30,40,100,200	Enabled	Link Up	GE2, GE13	GE1, GE14
<input type="radio"/> LAG 2	Port 3,4,15,16 als Trunk / Server, VLANs 3,5,10,20,30,40,100,200	Enabled	Link Down		GE3, GE4, GE15, GE16
<input type="radio"/> LAG 3	Ports 25-28 Uplink-Trunk / L2-SW, VLANs 3,5,10,20,30,40,100,200	Enabled	Link Up	GE25, GE26	GE27, GE28
<input type="radio"/> LAG 4			Link Not Present		
<input type="radio"/> LAG 5			Link Not Present		
<input type="radio"/> LAG 6			Link Not Present		
<input type="radio"/> LAG 7			Link Not Present		
<input type="radio"/> LAG 8			Link Not Present		

LAG Settings

Entry No.	LAG	Description	Type	Status	Link Status	SNMP Traps
<input type="radio"/> 1	LAG 1	Port 1,2,13,14 Trunk-SRV, VLANs 3,5,10,20,30,40,100,200	eth1000M	Up	Enabled	
<input type="radio"/> 2	LAG 2	Port 3,4,15,16 als Trunk / Server, VLANs 3,5,10,20,30,40,100,200		Down	Enabled	
<input type="radio"/> 3	LAG 3	Ports 25-28 Uplink-Trunk / L2-SW, VLANs 3,5,10,20,30,40,100,200	eth1000M	Up	Enabled	
<input type="radio"/> 4	LAG 4				Enabled	
<input type="radio"/> 5	LAG 5				Enabled	
<input type="radio"/> 6	LAG 6				Enabled	
<input type="radio"/> 7	LAG 7				Enabled	
<input type="radio"/> 8	LAG 8				Enabled	

Definition der Access Ports (port-based VLAN)

- Port 7: Port wird dem VLAN 5 (Internet VLAN) zugeordnet (untagged / PVID 5).
- Port 19: Port wird dem VLAN 5 (Internet VLAN) zugeordnet (untagged / PVID 5).
- Port 24: Port wird dem VLAN 3 (Management VLAN) zugeordnet (untagged / PVID 3).

Werden auf dem Switch weitere Ports z.B. für Testzwecke im Server VLAN benötigt, so sind diese unter VLAN Management --> Interface Settings als Access-Ports und unter Port-to-VLAN dem korrekten VLAN zuzordnen. Nachstehende Abbildungen stellen die Zuordnung zu VLAN 1 dar.

Port to VLAN

VLAN Membership Table

Filter: VLAN ID equals to

AND/Interface Type equals to


Interface Name	VLAN Mode	Membership Type	PVID
GE1	Trunk	Excluded	<input checked="" type="checkbox"/>
GE2	Trunk	Excluded	<input checked="" type="checkbox"/>
GE3	Trunk	Excluded	<input checked="" type="checkbox"/>
GE4	Trunk	Excluded	<input checked="" type="checkbox"/>
GE5	Trunk	Untagged	<input checked="" type="checkbox"/>
GE6	Trunk	Untagged	<input checked="" type="checkbox"/>
GE7	Access	Excluded	<input type="checkbox"/>
GE8	Trunk	Untagged	<input checked="" type="checkbox"/>
GE9	Trunk	Untagged	<input checked="" type="checkbox"/>
GE10	Trunk	Untagged	<input checked="" type="checkbox"/>
GE11	Trunk	Untagged	<input checked="" type="checkbox"/>
GE12	Trunk	Untagged	<input checked="" type="checkbox"/>
GE13	Trunk	Excluded	<input checked="" type="checkbox"/>
GE14	Trunk	Excluded	<input checked="" type="checkbox"/>
GE15	Trunk	Excluded	<input checked="" type="checkbox"/>
GE16	Trunk	Excluded	<input checked="" type="checkbox"/>

Port	Mode	VLAN Tagging	Check
GE6	Trunk	Untagged	<input checked="" type="checkbox"/>
GE7	Access	Excluded	<input type="checkbox"/>
GE8	Trunk	Untagged	<input checked="" type="checkbox"/>
GE9	Trunk	Untagged	<input checked="" type="checkbox"/>
GE10	Trunk	Untagged	<input checked="" type="checkbox"/>
GE11	Trunk	Untagged	<input checked="" type="checkbox"/>
GE12	Trunk	Untagged	<input checked="" type="checkbox"/>
GE13	Trunk	Excluded	<input checked="" type="checkbox"/>
GE14	Trunk	Excluded	<input checked="" type="checkbox"/>
GE15	Trunk	Excluded	<input checked="" type="checkbox"/>
GE16	Trunk	Excluded	<input checked="" type="checkbox"/>
GE17	Trunk	Untagged	<input checked="" type="checkbox"/>
GE18	Trunk	Untagged	<input checked="" type="checkbox"/>
GE19	Access	Excluded	<input type="checkbox"/>
GE20	Trunk	Untagged	<input checked="" type="checkbox"/>
GE21	Trunk	Untagged	<input checked="" type="checkbox"/>
GE22	Trunk	Untagged	<input checked="" type="checkbox"/>
GE23	Trunk	Untagged	<input checked="" type="checkbox"/>
GE24	Access	Untagged	<input checked="" type="checkbox"/>
GE25	Trunk		<input type="checkbox"/>
GE26	Trunk		<input type="checkbox"/>
GE27	Trunk		<input type="checkbox"/>
GE28	Trunk		<input type="checkbox"/>

Buttons: Apply, Cancel

Definition / Zuordnung der VLANs

- LAG1 (Port 1, 2, 13, 14): Der Hypervisor ist über vier Netzkabel mit Port 1,2,13,14 des Switches verbunden. Auf der Seite des Hypervisor sind ebenfalls vier Ports durch LinkAggregation definiert. LAG1 ist getaggt Mitglied der VLANs 3,5,10,20,30,40,100,200.
- LAG2 (Port 3, 4, 15, 16): Der zweite Hypervisor ist über vier Netzkabel mit Port 3,4,15,16 des Switches verbunden. Auf der Seite des Hypervisor sind ebenfalls vier Ports durch LinkAggregation definiert. LAG2 ist getaggt Mitglied der VLANs 3,5,10,20,30,40,100,200.
- LAG3 (Port 25 - 28): Uplink zu anderen L2-Switches via vier Ports. Auf den L2-Switches sind ebenfalls vier Ports durch LinkAggregation definiert. LAG3 ist getaggt Mitglied der VLANs 3,5,10,20,30,40,100,200.
- Port 7, 19: Ports werden dem VLAN 5 (Internet VLAN) zugeordnet (untagged / PVID 5).
- Port 24: Port wird dem VLAN 3 (Management VLAN) zugeordnet (untagged / PVID 3).



SG300-28 28-Port Gigabit Managed Switch

- Getting Started
- ▶ Status and Statistics
- ▶ Administration
- ▶ Port Management
- ▶ Smartport
- ▼ **VLAN Management**
 - Default VLAN Settings
 - VLAN Settings
 - Interface Settings
 - Port to VLAN
 - Port VLAN Membership**
 - Private VLAN Settings
 - GVRP Settings
 - ▶ Voice VLAN
 - ▶ Access Port Multicast TV VLAN
 - ▶ Customer Port Multicast TV VLAN
- ▶ Spanning Tree
- ▶ MAC Address Tables
- ▶ Multicast
- ▶ IP Configuration
- ▶ Security
- ▶ Access Control
- ▶ Quality of Service
- ▶ SNMP


Port VLAN Membership

F - Forbidden member T - Tagged member U - Untagged member

Port VLAN Membership Table

Filter: *Interface Type* equals to

	Interface	Mode	Administrative VLANs	Operational VLANs	LAG
<input type="radio"/>	GE1	Trunk	1P	1P	1
<input type="radio"/>	GE2	Trunk	1P	1P	1
<input type="radio"/>	GE3	Trunk	1P	1P	2
<input type="radio"/>	GE4	Trunk	1P	1P	2
<input type="radio"/>	GE5	Trunk	1UP	1UP	
<input type="radio"/>	GE6	Trunk	1UP	1UP	
<input type="radio"/>	GE7	Access	5UP	5UP	
<input type="radio"/>	GE8	Trunk	1UP	1UP	
<input type="radio"/>	GE9	Trunk	1UP	1UP	
<input type="radio"/>	GE10	Trunk	1UP	1UP	
<input type="radio"/>	GE11	Trunk	1UP	1UP	
<input type="radio"/>	GE12	Trunk	1UP	1UP	
<input type="radio"/>	GE13	Trunk	1P	1P	1
<input type="radio"/>	GE14	Trunk	1P	1P	1
<input type="radio"/>	GE15	Trunk	1P	1P	2
<input type="radio"/>	GE16	Trunk	1P	1P	2



SG300-28 28-Port Gigabit Managed Switch

- Getting Started
- ▶ Status and Statistics
- ▶ Administration
- ▶ Port Management
- ▶ Smartport
- ▼ **VLAN Management**
 - Default VLAN Settings
 - VLAN Settings
 - Interface Settings
 - Port to VLAN
 - Port VLAN Membership**
 - Private VLAN Settings
 - GVRP Settings
 - ▶ Voice VLAN
 - ▶ Access Port Multicast TV VLAN
 - ▶ Customer Port Multicast TV VLAN
- ▶ Spanning Tree
- ▶ MAC Address Tables
- ▶ Multicast
- ▶ IP Configuration
- ▶ Security
- ▶ Access Control
- ▶ Quality of Service
- ▶ SNMP

<input type="radio"/>	GE8	Trunk	1UP	1UP	
<input type="radio"/>	GE9	Trunk	1UP	1UP	
<input type="radio"/>	GE10	Trunk	1UP	1UP	
<input type="radio"/>	GE11	Trunk	1UP	1UP	
<input type="radio"/>	GE12	Trunk	1UP	1UP	
<input type="radio"/>	GE13	Trunk	1P	1P	1
<input type="radio"/>	GE14	Trunk	1P	1P	1
<input type="radio"/>	GE15	Trunk	1P	1P	2
<input type="radio"/>	GE16	Trunk	1P	1P	2
<input type="radio"/>	GE17	Trunk	1UP	1UP	
<input type="radio"/>	GE18	Trunk	1UP	1UP	
<input type="radio"/>	GE19	Access	5UP	5UP	
<input type="radio"/>	GE20	Trunk	1UP	1UP	
<input type="radio"/>	GE21	Trunk	1UP	1UP	
<input type="radio"/>	GE22	Trunk	1UP	1UP	
<input type="radio"/>	GE23	Trunk	1UP	1UP	
<input type="radio"/>	GE24	Access	1UP	1UP	
<input type="radio"/>	GE25	Trunk	1P	1P	3
<input type="radio"/>	GE26	Trunk	1P	1P	3
<input type="radio"/>	GE27	Trunk	1P	1P	3
<input type="radio"/>	GE28	Trunk	1P	1P	3

F - Forbidden member T - Tagged member U - Untagged member

cisco SG300-28 28-Port Gigabit Managed Switch

Getting Started
 ▶ Status and Statistics
 ▶ Administration
 ▶ Port Management
 ▶ Smartport
 ▼ **VLAN Management**
 Default VLAN Settings
 VLAN Settings
 Interface Settings
 Port to VLAN
 Port VLAN Membership
 Private VLAN Settings
 GVRP Settings
 ▶ Voice VLAN
 ▶ Access Port Multicast TV VLAN
 ▶ Customer Port Multicast TV VLAN
 ▶ Spanning Tree

VLAN Settings

<input type="checkbox"/>	VLAN ID	VLAN Name	Originators	VLAN Interface State	Link Status SNMP Traps
<input type="checkbox"/>	1		Default	Disabled	Disabled
<input type="checkbox"/>	3	Managgement VLAN	Static	Enabled	Enabled
<input type="checkbox"/>	5	Internet	Static	Enabled	Enabled
<input type="checkbox"/>	10	Server	Static	Enabled	Enabled
<input type="checkbox"/>	20	WLAN-LuL	Static	Enabled	Enabled
<input type="checkbox"/>	30	WLAN-SuS	Static	Enabled	Enabled
<input type="checkbox"/>	40	Lehrer	Static	Enabled	Enabled
<input type="checkbox"/>	100	Raum100	Static	Enabled	Enabled
<input type="checkbox"/>	200	Raum200	Static	Enabled	Enabled

Add... Edit... Delete


cisco SG300-28 28-Port Gigabit Managed Switch

Getting Started
 ▶ Status and Statistics
 ▶ Administration
 ▶ Port Management
 ▶ Smartport
 ▶ VLAN Management
 ▶ Spanning Tree
 ▶ MAC Address Tables
 ▶ Multicast
 ▼ **IP Configuration**
 ▼ IPv4 Management and Interface
 IPv4 Interface
 IPv4 Routes
 ARP

IPv4 Interface

<input type="checkbox"/>	Interface	IP Address Type	IP Address	Mask	Status
<input type="checkbox"/>	VLAN 10	Static	10.0.0.253	255.255.255.0	Valid
<input type="checkbox"/>	VLAN 40	Static	10.1.0.254	255.255.255.0	Valid
<input type="checkbox"/>	VLAN 100	Static	10.2.100.254	255.255.255.0	Valid
<input type="checkbox"/>	VLAN 200	Static	10.2.200.254	255.255.255.0	Valid
<input type="checkbox"/>	VLAN 20	Static	10.3.0.253	255.255.255.0	Valid
<input type="checkbox"/>	VLAN 30	Static	10.4.0.253	255.255.255.0	Valid
<input type="checkbox"/>	VLAN 1	Static	192.168.1.254	255.255.255.0	Valid

Add... Edit... Delete


SG300-28 28-Port Gigabit Managed Switch

- Getting Started
- ▶ Status and Statistics
- ▶ Administration
- ▶ Port Management
- ▶ Smartport
- ▼ **VLAN Management**
 - Default VLAN Settings
 - VLAN Settings
 - Interface Settings**
 - Port to VLAN
 - Port VLAN Membership
 - Private VLAN Settings
 - GVRP Settings
 - ▶ Voice VLAN
 - ▶ Access Port Multicast TV VLAN
 - ▶ Customer Port Multicast TV VLAN
- ▶ Spanning Tree
- ▶ MAC Address Tables
- ▶ Multicast
- ▶ IP Configuration
- ▶ Security
- ▶ Access Control
- ▶ Quality of Service
- ▶ SNMP

Interface Settings

Interface Settings Table

Filter: *Interface Type* equals to

	Entry No.	Interface	Interface VLAN Mode	Administrative PVID	Frame Type	Ingress Filtering	Primary VLAN
<input type="radio"/>	1	GE1	Trunk	1	Admit All	Enabled	
<input type="radio"/>	2	GE2	Trunk	1	Admit All	Enabled	
<input type="radio"/>	3	GE3	Trunk	1	Admit All	Enabled	
<input type="radio"/>	4	GE4	Trunk	1	Admit All	Enabled	
<input type="radio"/>	5	GE5	Trunk	1	Admit All	Enabled	
<input type="radio"/>	6	GE6	Trunk	1	Admit All	Enabled	
<input type="radio"/>	7	GE7	Access	5	Admit All	Enabled	
<input type="radio"/>	8	GE8	Trunk	1	Admit All	Enabled	
<input type="radio"/>	9	GE9	Trunk	1	Admit All	Enabled	
<input type="radio"/>	10	GE10	Trunk	1	Admit All	Enabled	
<input type="radio"/>	11	GE11	Trunk	1	Admit All	Enabled	
<input type="radio"/>	12	GE12	Trunk	1	Admit All	Enabled	
<input type="radio"/>	13	GE13	Trunk	1	Admit All	Enabled	
<input type="radio"/>	14	GE14	Trunk	1	Admit All	Enabled	
<input type="radio"/>	15	GE15	Trunk	1	Admit All	Enabled	
<input type="radio"/>	16	GE16	Trunk	1	Admit All	Enabled	

Port	Name	Mode	Value	Admit All	Enabled
6	GE6	Trunk	1	Admit All	Enabled
7	GE7	Access	5	Admit All	Enabled
8	GE8	Trunk	1	Admit All	Enabled
9	GE9	Trunk	1	Admit All	Enabled
10	GE10	Trunk	1	Admit All	Enabled
11	GE11	Trunk	1	Admit All	Enabled
12	GE12	Trunk	1	Admit All	Enabled
13	GE13	Trunk	1	Admit All	Enabled
14	GE14	Trunk	1	Admit All	Enabled
15	GE15	Trunk	1	Admit All	Enabled
16	GE16	Trunk	1	Admit All	Enabled
17	GE17	Trunk	1	Admit All	Enabled
18	GE18	Trunk	1	Admit All	Enabled
19	GE19	Access	5	Admit All	Enabled
20	GE20	Trunk	1	Admit All	Enabled
21	GE21	Trunk	1	Admit All	Enabled
22	GE22	Trunk	1	Admit All	Enabled
23	GE23	Trunk	1	Admit All	Enabled
24	GE24	Access	1	Admit All	Enabled
25	GE25	Trunk	1	Admit All	Enabled
26	GE26	Trunk	1	Admit All	Enabled
27	GE27	Trunk	1	Admit All	Enabled
28	GE28	Trunk	1	Admit All	Enabled

Access Listen definieren

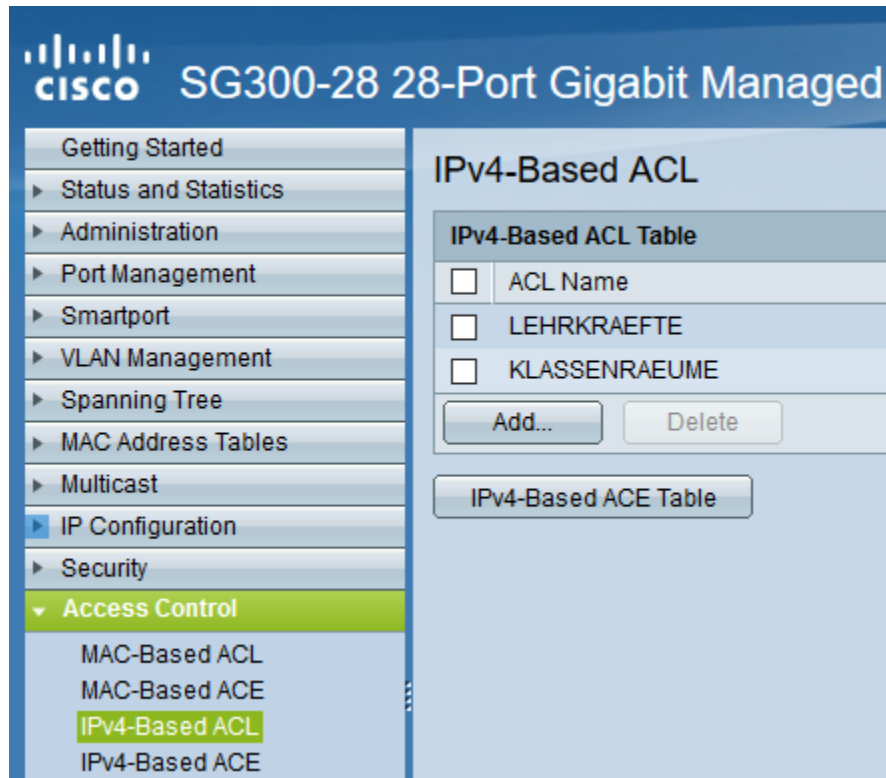
Hinweis: Der Cisco L3-Switch kann nur eingehenden Datenverkehr filtern. Dies ist relevant für die Definition und Anwendung der Listen für die Zugriffssteuerung (ACLs). **Achtung:** Die hier vorgestellten ACLs führen dazu, dass bsp. PCs aus zwei verschiedenen Klassenräumen sich untereinander via ping nicht mehr erreichen können. Wenn dies gewünscht ist, müsste in den ACEs eine weitere Regel erstellt werden, die Daten Zulassen → 10.(subnet).0 mit Netmask 0.0.0.255 - also z.B. 10.16.1.0 0.0.0.255. Diese Regel muss die niedrigste Priorität erhalten.

ACL: Lehrkrafte und Klassenraeume

Es sind Zwei ACL anzulegen: Lehrkrafte und Klassenraume. Dies erfolgt im Menü unter: Zugriffssteuerung → IPv4 basierte ACL → Hinzufügen → <Name der ACL>

ACEs hinzufügen

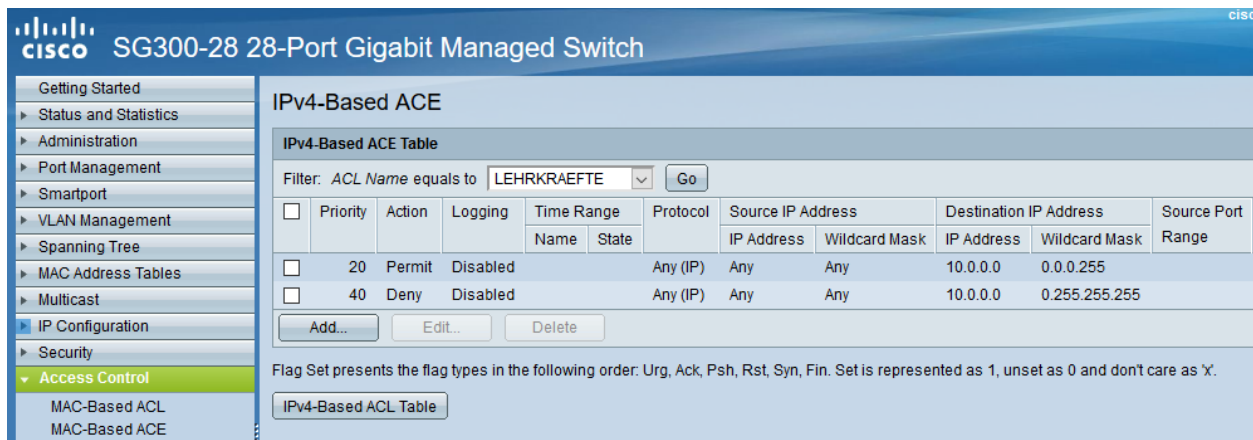
Für die zuvor genannten ACLs sind jetzt sog. Entries (Einträge) anzulegen. Hierfür wählst Du im Menü: Zugriffssteuerung → IPv4 basiertes ACE → <Name der ACL aus Liste auswählen - hier Lehrkrafte> → Hinzufügen



Du gibst dann folgende Werte an:

- Priorität: 20
- Aktion: Zulassen (permit)
- Protokoll: Beliebig (IP) (any)
- Quell-IP-Adresse: Beliebig (any)
- Ziel-IP-Adresse: Benutzerdefiniert (user defined)
- Wert der Ziel-IP-Adresse: 10.16.1.0 (Servernetz-IP)
- Ziel-IP-Platzhaltermaske: 0.0.0.255 (invertierte Netzmaske)

Danach legst Du eine zweite ACE für die ACL Lehrkraefte an. Im Ergebnis solltest Du für die Lehrkraefte dann nachstehenden Einträge haben:



Danach lest Du ACEs für die ACL Klassenraeume an. Danach solltest Du nachstehende Einträge haben:

The screenshot shows the configuration page for the IPv4-Based ACE on a Cisco SG300-28 switch. The left sidebar shows the navigation menu with 'Access Control' expanded and 'IPv4-Based ACE' selected. The main content area is titled 'IPv4-Based ACE' and contains a table with two entries.

IPv4-Based ACE Table

Filter: ACL Name equals to **KLASSENRAEUME**

<input type="checkbox"/>	Priority	Action	Logging	Time Range	Protocol	Source IP Address	Destination IP Address	Source Port
				Name State		IP Address Wildcard Mask	IP Address Wildcard Mask	Range
<input type="checkbox"/>	60	Permit	Disabled		Any (IP)	Any Any	10.0.0.0 0.0.0.255	
<input type="checkbox"/>	80	Deny	Disabled		Any (IP)	Any Any	10.0.0.0 0.255.255.255	

Flag Set presents the flag types in the following order: Urg, Ack, Psh, Rst, Syn, Fin. Set is represented as 1, unset as 0 and don't care as X.

Schliesslich müssen die definierten ACLs noch an die VLANs gebunden werden, damit diese korrekt angewendet werden. Die Zuordnung sollte für das hier gewählte Beispiel wie folgt aussehen:

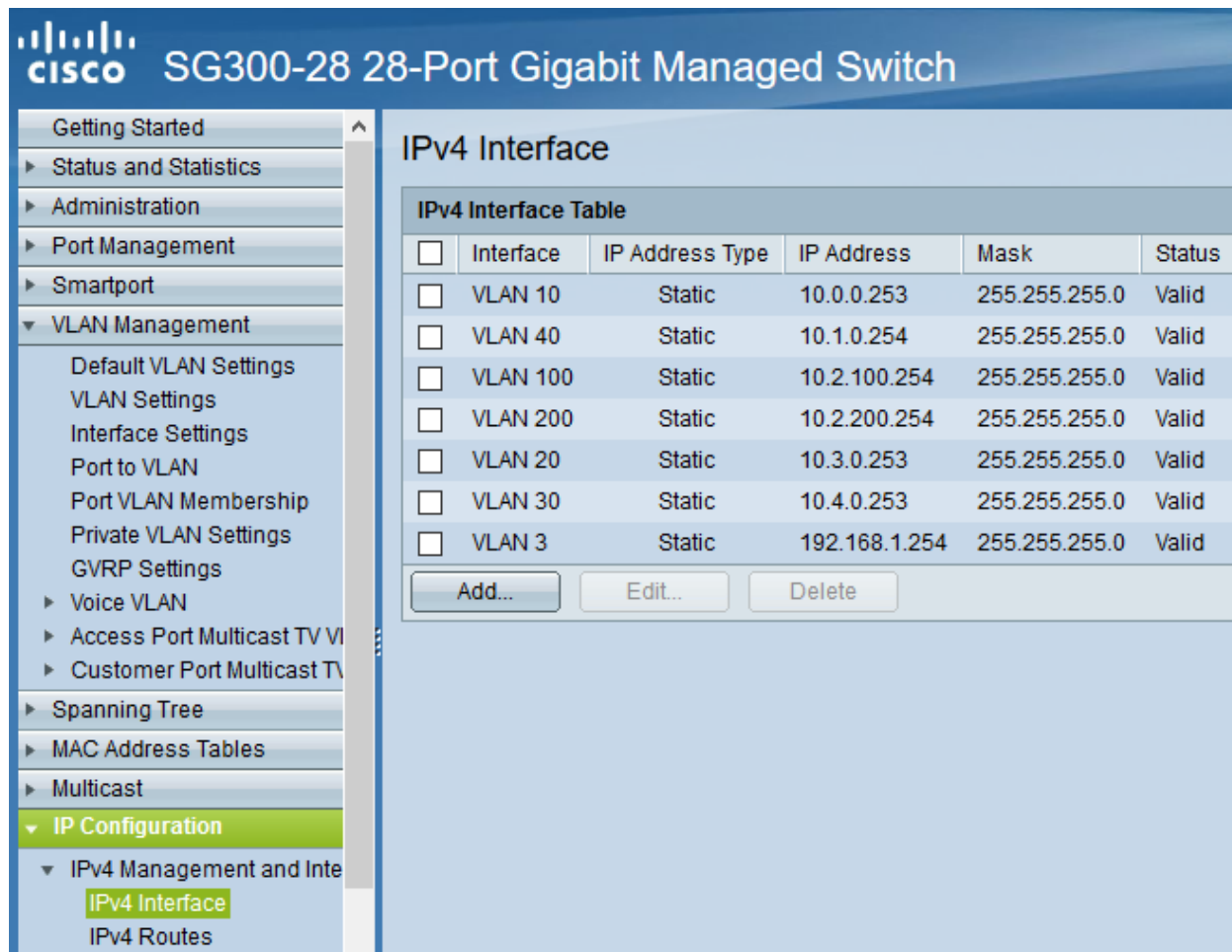
The screenshot shows the configuration page for ACL Binding (VLAN) on a Cisco SG300-28 switch. The left sidebar shows the navigation menu with 'Access Control' expanded and 'ACL Binding (VLAN)' selected. The main content area is titled 'ACL Binding (VLAN)' and contains a table with three entries.

ACL Binding Table

<input type="checkbox"/>	VLAN ID	MAC ACL	IPv4 ACL	IPv6 ACL	Default Action
<input type="checkbox"/>	40		LEHRKRAEFTE		Permit Any
<input type="checkbox"/>	100		KLASSENRAEUME		Permit Any
<input type="checkbox"/>	200		KLASSENRAEUME		Permit Any

DHCP-Relay konfigurieren

Die Einstellungen für das DHCP-Relaying sollten wie folgt aussehen:



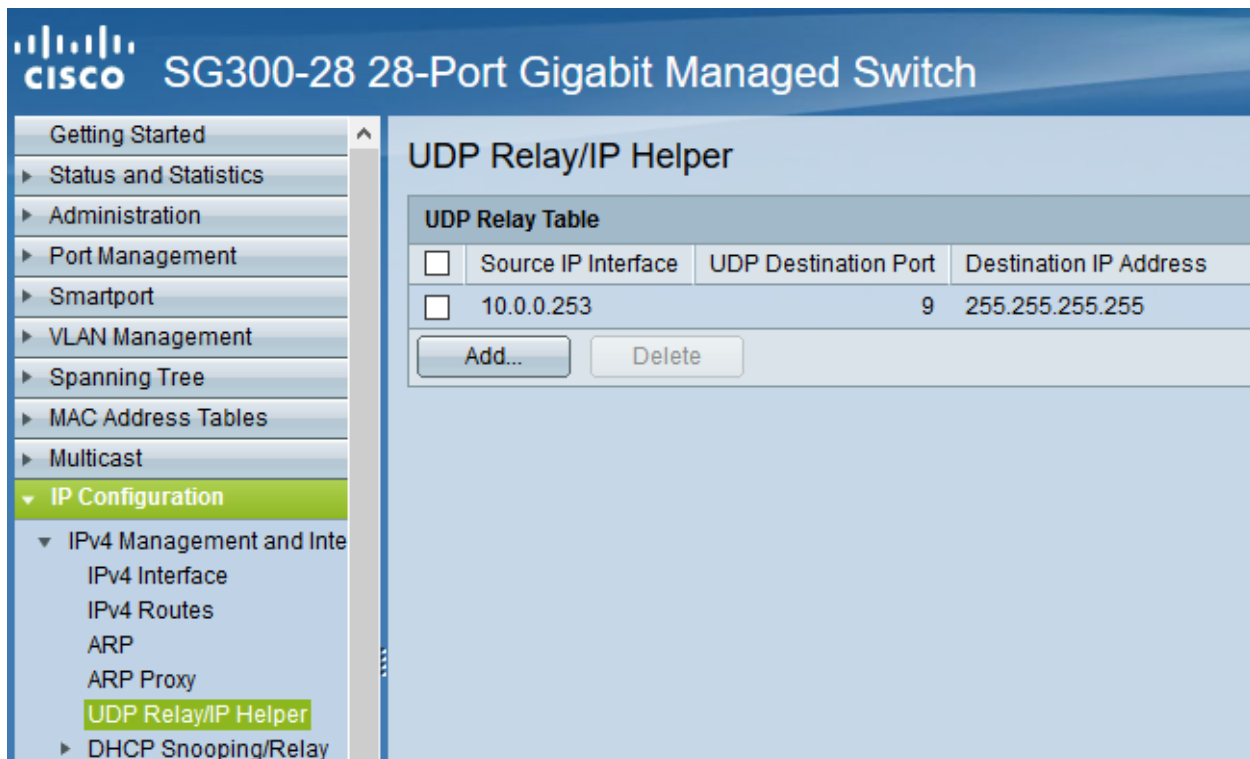
IPv4 Interface

<input type="checkbox"/>	Interface	IP Address Type	IP Address	Mask	Status
<input type="checkbox"/>	VLAN 10	Static	10.0.0.253	255.255.255.0	Valid
<input type="checkbox"/>	VLAN 40	Static	10.1.0.254	255.255.255.0	Valid
<input type="checkbox"/>	VLAN 100	Static	10.2.100.254	255.255.255.0	Valid
<input type="checkbox"/>	VLAN 200	Static	10.2.200.254	255.255.255.0	Valid
<input type="checkbox"/>	VLAN 20	Static	10.3.0.253	255.255.255.0	Valid
<input type="checkbox"/>	VLAN 30	Static	10.4.0.253	255.255.255.0	Valid
<input type="checkbox"/>	VLAN 3	Static	192.168.1.254	255.255.255.0	Valid

Buttons: Add... Edit... Delete

Hierdurch wird sichergestellt, dass DHCP-Anfragen aus den genannten VLANs auch beim linuxmuster.net Server ankommen und bedient werden können.

Um Wake-on-LAN über Subnetze hinweg zu nutzen, muss ein sog. UDP-Relaying eingerichtet werden. Hierdurch können dann z.B. Clients via linbo-remote aufgeweckt werden.



The screenshot shows the Cisco SG300-28 28-Port Gigabit Managed Switch web interface. The left sidebar contains a navigation menu with the following items: Getting Started, Status and Statistics, Administration, Port Management, Smartport, VLAN Management, Spanning Tree, MAC Address Tables, Multicast, IP Configuration (expanded), IPv4 Management and Inte, IPv4 Interface, IPv4 Routes, ARP, ARP Proxy, UDP Relay/IP Helper (highlighted), and DHCP Snooping/Relay. The main content area is titled "UDP Relay/IP Helper" and features a "UDP Relay Table" with the following columns: Source IP Interface, UDP Destination Port, and Destination IP Address. The table contains one entry: 10.0.0.253, 9, 255.255.255.255. Below the table are "Add..." and "Delete" buttons.

Source IP Interface	UDP Destination Port	Destination IP Address
10.0.0.253	9	255.255.255.255

Für das DHCP-Relaying/Snooping muss zudem die Option 82 aktiviert werden.

Properties

Option 82, if enabled, applies to DHCP Relay interface with IP address

Option 82: ☒ Enable

DHCP Relay: ☒ Enable

DHCP Snooping

DHCP Snooping Status: ☐ Enable

Option 82 Pass Through: ☐ Enable

Verify MAC Address: ☒ Enable

Backup Database: ☐ Enable

✱ Backup Database Update Interval: 1200

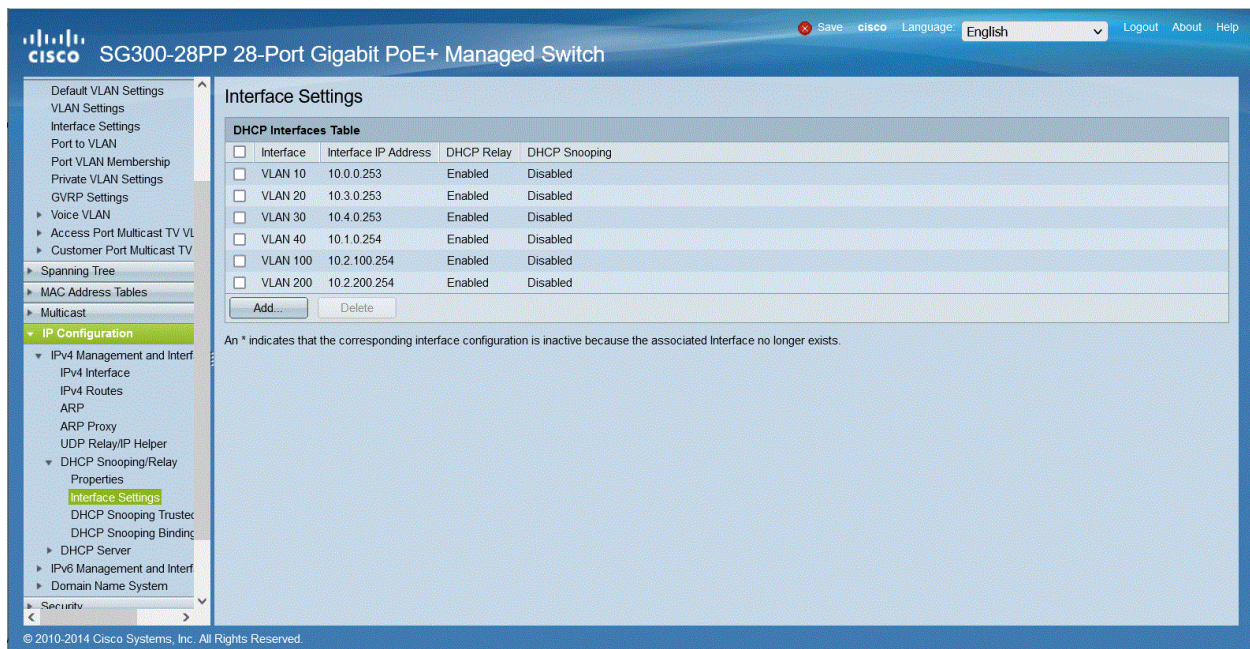
Apply Cancel

DHCP Relay Server Table

<input type="checkbox"/>	DHCP Server IP Address
<input type="checkbox"/>	10.0.0.1

Add... Delete

Abschliessend trägst Du noch die VLANs ein, die für das DHCP Relay aktiv sein sollen.



Nachdem Du alle Einstellungen kontrolliert und ggf. angepasst haben, speicherst Du die aktuelle Konfiguration. Dies erledigst Du bei dem Cisco-Switch dadurch, dass Du die Konfiguration aus dem RAM (running-config) auf die NVRAM-Konfiguration kopierst (startup-config).

Weitere L2-Switches mit VLANs anbinden

In Vorbereitung auf das Subnetting sind auf allen Switches im Netzwerk (in allen Gebäuden) die VLANs mit den IDs 3, 5, 10, 20, 30, 40, 100, und 200 anzulegen, damit später die Portkonfiguration aller Switches angepasst werden kann.

In der hier dargestellten Konfiguration des L3-Switches gibt es drei LAG-Ports. Ein LAG-Port (25-28) ist dazu gedacht, eine Anbindung zu weiteren L2-Switches zu ermöglichen, die ebenfalls für die Nutzung der VLANs zu konfigurieren sind. Dieser LAG-Port ist als Trunk konfiguriert.

Wesentlich ist, dass alle VLANs, die auf dem L3-Switch eingerichtet wurden, ebenfalls auf allen L2-Switches erstellt werden. Danach muss eine LinkAggregation mit vier Ports erstellt werden, die die Anbindung zum LAG-Port des L3-Switches zur Verfügung stellt. Dieser LAG-Port auf dem L2-Switch ist dann als Trunk zu definieren, der alle VLANs (3,5,10,20,40,100,200) tagged.

Danach werden die einzelnen Ports auf den jeweiligen L2-Switches als untagged ports einem der gewünschten VLANs zugeordnet (port-based VLANs). Die Clients sind dann entsprechend auf den gewünschten VLAN-Port anzuschliessen.

Ist ein Switch in einem PC-Raum, so ist der Uplink als LinkAggregation und Trunk mit den o.g. tagged VLANs zu definieren. Alle anderen Ports sind dann z.B. als access ports zu definieren, die dem VLAN 100 (Raum 100) zugeordnet sind, so dass alle angeschlossenen PCs in diesem VLAN sind.

Hinweis: Es sollten alle Switch Konfigurationen, VLANs und Port-Belegungen sehr genau pro Switch dokumentiert sein. Hierzu ist es hilfreich in jedem Verteilerschrank eine entsprechende Dokumentation zu hinterlegen. Als Hilfestellung zur Erstellung dieser Dokumentation kann folgende Datei dienen:

Einfache Dokumentation mit Calc.

Vorbereitung der Switches im Netzwerk

Das genaue Vorgehen kann hier nicht umfassend dokumentiert werden, da es auch von Art und Hersteller der Switches abhängt.

Exemplarisch erfolgt die Darstellung zur Einrichtung der VLANs auf L2-Switches anhand des Modells Cisco SF200-24. Für andere Modelle sind die Konfigurationsschritte entsprechend anzupassen.

SF200-24 Startup-Config

Für das hier dokumentierte Netzwerkszenario wurde ein Switch des o.g. Modells für Raum 200 vorkonfiguriert, um das Vorgehen zur Konfiguration der L2-Switches besser darstellen zu können. Die Konfiguration wird zur schnelleren Umsetzung des Szenarios unten bereitgestellt.

Startup-config-SF200-24-L2-Raum200.

Hinweis: Die Firmware des Cisco L2-Switches ist vorab auf die aktuellste Version (hier: 1.4.11.2) zu aktualisieren. Ist eine ältere FW-Version noch installiert, so kann es erforderlich sein, die Aktualisierung in Etappen vorzunehmen (z.B. 1.1.2.0 -> 1.3.7.18 -> 1.4.7.5 -> 1.4.11.2). Um die Boot Version zu aktualisieren, ist die RTB-Datei des FW-Images via TFTP auf den Switch zu laden und dieses jeweils neu zu starten. Im Auslieferungszustand ist der Switch via IP 192.168.1.254/24 erreichbar. Login ist im Auslieferungszustand cisco mit dem Kennwort cisco.

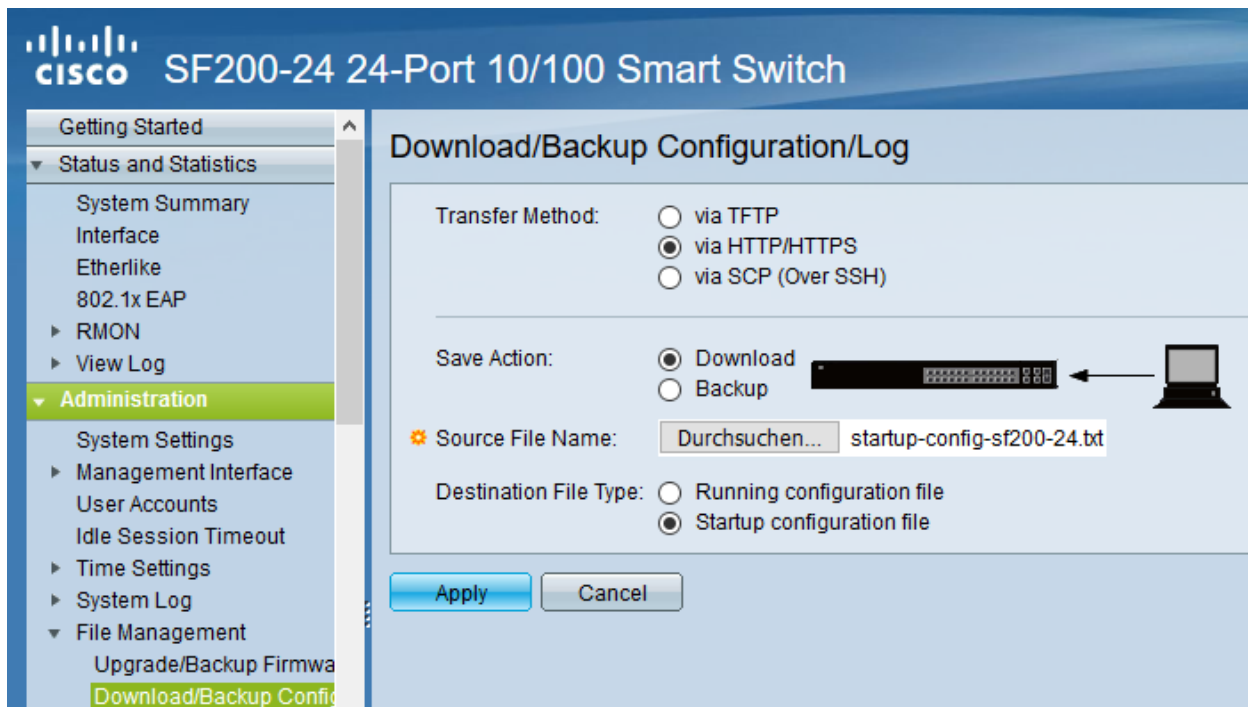
The screenshot shows the Cisco SF200-24 24-Port 10/100 Smart Switch web interface. The left sidebar contains a navigation menu with options like 'Getting Started', 'Status and Statistics', 'Administration', and 'System Settings'. The main content area displays the 'System Summary' page, which is divided into two columns: 'System Information' and 'Software Information'.

System Information		Software Information	
System Description:	SF200-24 24-Port 10/100 Smart Switch	Firmware Version:	1.4.11.2
System Location:	Edit	Firmware MD5 Checksum:	c86117e717b05c56f27740001cc1334b
System Contact:	Edit	Boot Version:	1.3.5.06
Host Name:	switch35ae02 Edit	Boot MD5 Checksum:	da8bcdbf216c7df1a3bcb41ec8669e76
System Object ID:	1.3.6.1.4.1.9.6.1.87.24.1	Locale:	en-US
System Uptime:	0 day(s), 0 hr(s), 25 min(s) and 33 sec(s)	Language Version:	1.4.11.2
Current Time:	20:32:26;2019-Sep-26	Language MD5 Checksum:	N/A
Base MAC Address:	58:8d:09:35:ae:02		
Jumbo Frames:	Disabled		

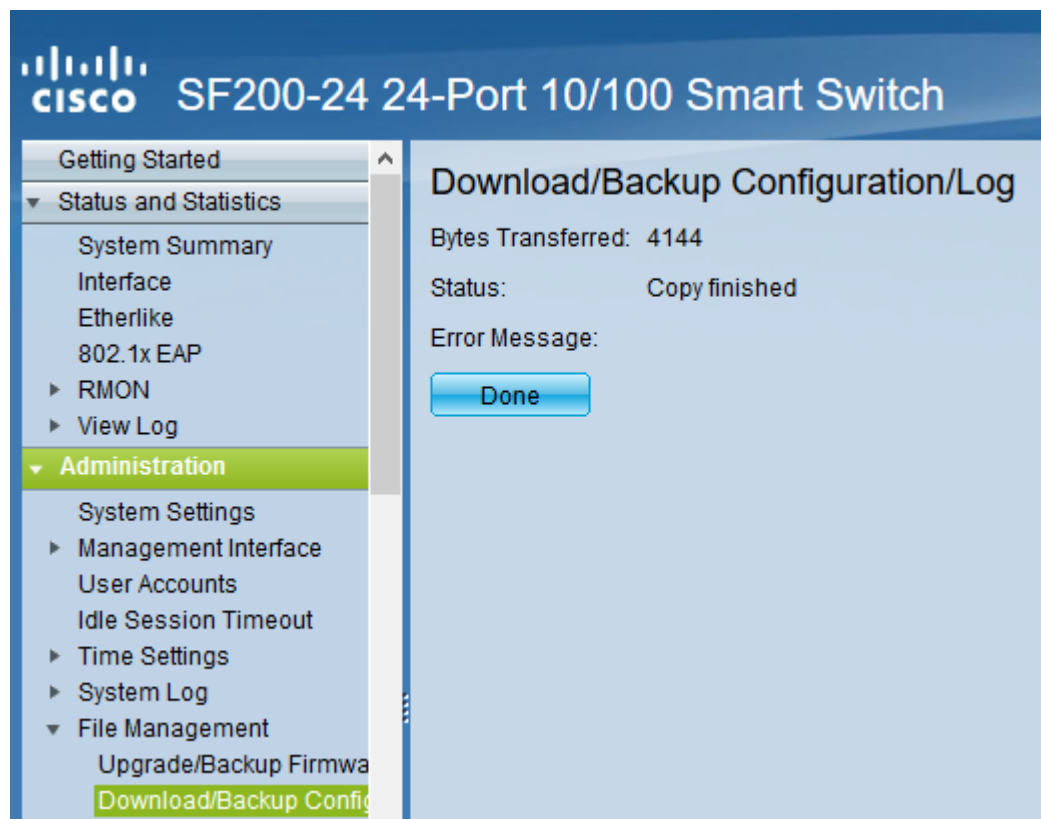
Die heruntergeladene Konfigurationsdatei ist nun auf den Switch zu laden und dieser ist dann neu zu starten.

Hinweis: Im Auslieferungszustand kann auf den Switch mit der IP 192.168.1.254/24 zugegriffen werden. Benutzer und Kennwort sind cisco.

Im Menü Administration --> File Management --> Download/Backup Config ist zu Konfigurationsdatei mit Durchsuchen auszuwählen. Als Ziel ist Startup Configuration file anzugeben.



Der erfolgreiche Upload der Konfigurationsdatei wird im Fenster bestätigt.



Danach ist der Switch neu zu starten (siehe Hinweise wie bei Cisco L3-Switch). Nach dem Neustart sind nachstehende Hinweise zur weiteren Konfiguration des Switches zu beachten.

Hinweis: Der Switch weist im VLAN 3 (access port 24) die IP 192.168.1.250/24 auf. Benutzer ist cisco und PW ist cisco. Die Ports 25 & 26 wurden als LACP-Bond konfiguriert. Dieser arbeitet als Trunk und tagged die Pakete für die VLANs 3, 5, 10, 20, 30, 40, 100, 200. In dem dokumentierten Szenario sind die Ports 25&26 des L3-Switches mit den Ports 25 & 26 des L2-Switches zu verbinden.

Durch den Import der Konfigurationsdatei sind bereits alle Konfigurationseinstellungen für den Switch eingetragen, der als Raum-Switch für Raum 200 (VLAN 200) für einen PC-Raum dienen soll.

Nachstehend dargestellte Konfigurationsschritte visualisieren die jeweiligen Einstellungen, die so auch manuell eingestellt werden können.

Zunächst sind die VLANs mit identischen IDs und Bezeichnungen auf allen L2 - Switchen analog zum L3-Switch anzulegen.

cisco SF200-24 24-Port 10/100 Smart Switch

VLAN Settings

<input type="checkbox"/>	VLAN ID	VLAN Name	Originators	VLAN Interface State	Link Status SNMP Traps
<input type="checkbox"/>	1		Default	Disabled	Enabled
<input type="checkbox"/>	3	Management VLAN	Static	Enabled	Enabled
<input type="checkbox"/>	5	Internet	Static	Enabled	Enabled
<input type="checkbox"/>	10	Server	Static	Enabled	Enabled
<input type="checkbox"/>	20	WLAN-LuL	Static	Enabled	Enabled
<input type="checkbox"/>	30	WLAN-SuS	Static	Enabled	Enabled
<input type="checkbox"/>	40	Lehrer	Static	Enabled	Enabled
<input type="checkbox"/>	100	Raum 100	Static	Enabled	Enabled
<input type="checkbox"/>	200	Raum 200	Static	Enabled	Enabled

Danach ist der LACP-Bond bestehend aus den Ports 25 & 26 zu definieren.

The screenshot shows the Cisco SF200-24 24-Port 10/100 Smart Switch web interface. The left sidebar contains a navigation menu with the following items: Getting Started, Status and Statistics, Administration (expanded), System Settings, Management Interface, User Accounts, Idle Session Timeout, Time Settings, System Log, File Management (expanded), Upgrade/Backup Firmware, Download/Backup Configuration, Configuration Files Properties, Copy/Save Configuration, DHCP Auto Configuration, Reboot, Diagnostics, Discovery - Bonjour, Discovery - LLDP, Discovery - CDP, Ping, Port Management (expanded), Port Settings, Error Recovery Settings, Loopback Detection Settings, Link Aggregation (expanded), LAG Management (highlighted), and LAG Settings.


The main content area is titled "LAG Management". It features a "Load Balance Algorithm" section with two radio buttons: "MAC Address" (selected) and "IP/MAC Address". Below this are "Apply" and "Cancel" buttons.

Below the buttons is a "LAG Management Table" with the following columns: LAG, Name, LACP, Link State, Active Member, and Standby Member. The table contains four rows of LAG configurations:

LAG	Name	LACP	Link State	Active Member	Standby Member
<input type="radio"/> LAG 1	Uplink Trunk	Enabled	Link Down		GE1, GE2
<input type="radio"/> LAG 2			Link Not Present		
<input type="radio"/> LAG 3			Link Not Present		
<input type="radio"/> LAG 4			Link Not Present		

Below the table is an "Edit..." button.

Die Nutzung der jeweiligen Ports wird in der Beschreibung pro Port dokumentiert.

 SF200-24 24-Port 10/100 Smart Switch									
Getting Started									
▼ Status and Statistics									
System Summary									
Interface									
Etherlike									
802.1x EAP									
► RMON									
► View Log									
▼ Administration									
System Settings									
► Management Interface									
User Accounts									
Idle Session Timeout									
► Time Settings									
► System Log									
► File Management									
Reboot									
► Diagnostics									
Discovery - Bonjour									
► Discovery - LLDP									
► Discovery - CDP									
Ping									
▼ Port Management									
Port Settings									
Error Recovery Settings									
Loopback Detection Settings									
▼ Link Aggregation									
LAG Management									
LAG Settings									

<input type="radio"/>	3	FE3	Port VLAN 200 - Raum200	100M-Copper	Up	Enabled	100M	Full	
<input type="radio"/>	4	FE4	Port VLAN 200 - Raum200	100M-Copper	Down	Enabled			
<input type="radio"/>	5	FE5	Port VLAN 200 - Raum200	100M-Copper	Down	Enabled			
<input type="radio"/>	6	FE6	Port VLAN 200 - Raum200	100M-Copper	Down	Enabled			
<input type="radio"/>	7	FE7	Port VLAN 200 - Raum200	100M-Copper	Down	Enabled			
<input type="radio"/>	8	FE8	Port VLAN 200 - Raum200	100M-Copper	Down	Enabled			
<input type="radio"/>	9	FE9	Port VLAN 200 - Raum200	100M-Copper	Down	Enabled			
<input type="radio"/>	10	FE10	Port VLAN 200 - Raum200	100M-Copper	Down	Enabled			
<input type="radio"/>	11	FE11	Port VLAN 200 - Raum200	100M-Copper	Down	Enabled			
<input type="radio"/>	12	FE12	Port VLAN 200 - Raum200	100M-Copper	Down	Enabled			
<input type="radio"/>	13	FE13	Port VLAN 200 - Raum200	100M-Copper	Down	Enabled			
<input type="radio"/>	14	FE14	Port VLAN 200 - Raum200	100M-Copper	Down	Enabled			
<input type="radio"/>	15	FE15	Port VLAN 200 - Raum200	100M-Copper	Down	Enabled			
<input type="radio"/>	16	FE16	Port VLAN 200 - Raum200	100M-Copper	Down	Enabled			
<input type="radio"/>	17	FE17	Port VLAN 200 - Raum200	100M-Copper	Down	Enabled			
<input type="radio"/>	18	FE18	Port VLAN 200 - Raum200	100M-Copper	Down	Enabled			
<input type="radio"/>	19	FE19	Port VLAN 200 - Raum200	100M-Copper	Down	Enabled			
<input type="radio"/>	20	FE20	Port VLAN 200 - Raum200	100M-Copper	Down	Enabled			
<input type="radio"/>	21	FE21		100M-Copper	Down	Enabled			
<input type="radio"/>	22	FE22	VLAN10 Server	100M-Copper	Down	Enabled			
<input type="radio"/>	23	FE23	VLAN 10 Server	100M-Copper	Down	Enabled			
<input type="radio"/>	24	FE24	Port VLAN 3 - Management	100M-Copper	Up	Enabled	100M	Full	
<input type="radio"/>	25	GE1	Uplink-Trunk within LAP1	1000M-ComboC	Up	Enabled	1000M	Full	1
<input type="radio"/>	26	GE2	Uplink-Trunk within LAP1	1000M-ComboC	Up	Enabled	1000M	Full	1

Die VLAN - Nutzung der Ports (Access, Trunk) ist festzulegen.

cisco SF200-24 24-Port 10/100 Smart Switch

Port	Port Name	Mode	VLAN	Trunk	Admit All	Enabled
1	FE1	Access	1	Admit All	Enabled	
2	FE2	Access	1	Admit All	Enabled	
3	FE3	Access	1	Admit All	Enabled	
4	FE4	Access	1	Admit All	Enabled	
5	FE5	Access	1	Admit All	Enabled	
6	FE6	Access	1	Admit All	Enabled	
7	FE7	Access	1	Admit All	Enabled	
8	FE8	Access	1	Admit All	Enabled	
9	FE9	Access	1	Admit All	Enabled	
10	FE10	Access	1	Admit All	Enabled	
11	FE11	Access	1	Admit All	Enabled	
12	FE12	Access	1	Admit All	Enabled	
13	FE13	Access	1	Admit All	Enabled	
14	FE14	Access	1	Admit All	Enabled	
15	FE15	Access	1	Admit All	Enabled	
16	FE16	Access	1	Admit All	Enabled	
17	FE17	Access	1	Admit All	Enabled	
18	FE18	Access	1	Admit All	Enabled	
19	FE19	Access	1	Admit All	Enabled	
20	FE20	Access	1	Admit All	Enabled	
21	FE21	Trunk	1	Admit All	Enabled	
22	FE22	Trunk	1	Admit All	Enabled	
23	FE23	Trunk	1	Admit All	Enabled	
24	FE24	Trunk	1	Admit All	Enabled	
25	GE1	Trunk	1	Admit All	Enabled	
26	GE2	Trunk	1	Admit All	Enabled	

Copy Settings... Edit...

Die Ports sind den VLANs zuzuordnen in denen diese arbeiten sollen. So soll der Switch die Ports 1-20 als Access Ports im VLAN 200 nutzen.

cisco SF200-24 24-Port 10/100 Smart Switch

System Log
 File Management
 Upgrade/Backup Firmware
 Download/Backup Configuration Files
 Configuration Files Properties
 Copy/Save Configuration
 DHCP Auto Configuration
 Reboot
 Diagnostics
 Discovery - Bonjour
 Discovery - LLDP
 Discovery - CDP
 Ping
 Port Management
 Port Settings
 Error Recovery Settings
 Loopback Detection Settings
 Link Aggregation
 LAG Management
 LAG Settings
 LACP
 Green Ethernet
 Smartport
 VLAN Management
 Default VLAN Settings
 VLAN Settings
 Interface Settings
 Port to VLAN
 Port VLAN Membership

Port to VLAN

VLAN Membership Table

Filter: VLAN ID equals to
 AND Interface Type equals to

Interface Name	VLAN Mode	Membership Type	PVID
FE1	Access	Untagged	<input checked="" type="checkbox"/>
FE2	Access	Untagged	<input checked="" type="checkbox"/>
FE3	Access	Untagged	<input checked="" type="checkbox"/>
FE4	Access	Untagged	<input checked="" type="checkbox"/>
FE5	Access	Untagged	<input checked="" type="checkbox"/>
FE6	Access	Untagged	<input checked="" type="checkbox"/>
FE7	Access	Untagged	<input checked="" type="checkbox"/>
FE8	Access	Untagged	<input checked="" type="checkbox"/>
FE9	Access	Untagged	<input checked="" type="checkbox"/>
FE10	Access	Untagged	<input checked="" type="checkbox"/>
FE11	Access	Untagged	<input checked="" type="checkbox"/>
FE12	Access	Untagged	<input checked="" type="checkbox"/>
FE13	Access	Untagged	<input checked="" type="checkbox"/>
FE14	Access	Untagged	<input checked="" type="checkbox"/>
FE15	Access	Untagged	<input checked="" type="checkbox"/>
FE16	Access	Untagged	<input checked="" type="checkbox"/>
FE17	Access	Untagged	<input checked="" type="checkbox"/>
FE18	Access	Untagged	<input checked="" type="checkbox"/>

Die Darstellung der Zuordnung kann pro VLAN kontrolliert werden. Hier als Beispiel die Darstellung für das VLAN 5.

Port to VLAN

VLAN Membership Table

Filter: VLAN ID equals to AND Interface Type equals to

Interface Name	VLAN Mode	Membership Type	PVID
LAG1	Trunk	<input type="text" value="Tagged"/>	<input type="checkbox"/>
LAG2	Trunk	<input type="text" value="Excluded"/>	<input type="checkbox"/>
LAG3	Trunk	<input type="text" value="Excluded"/>	<input type="checkbox"/>
LAG4	Trunk	<input type="text" value="Excluded"/>	<input type="checkbox"/>

Die Zuordnung der Ports zu den VLANs inkl. Darstellung deren Funktion ist im Menü VLAN Management --> Port VLAN Membership dargestellt.

The image shows the configuration interface of a Cisco SF200-24 24-Port 10/100 Smart Switch. The left sidebar contains a navigation menu with the following items: Getting Started, Status and Statistics, Administration, Port Management, Smartport, VLAN Management (highlighted), Default VLAN Settings, VLAN Settings, Interface Settings, Port to VLAN, Port VLAN Membership (highlighted), Voice VLAN, Spanning Tree, MAC Address Tables, Multicast, IP Configuration, Security, Quality of Service, and SNMP. The main content area displays a table of port configurations.

Port	Mode	Speed	Duplex	Flow Control
FE4	Access	200UP	200UP	
FE5	Access	200UP	200UP	
FE6	Access	200UP	200UP	
FE7	Access	200UP	200UP	
FE8	Access	200UP	200UP	
FE9	Access	200UP	200UP	
FE10	Access	200UP	200UP	
FE11	Access	200UP	200UP	
FE12	Access	200UP	200UP	
FE13	Access	200UP	200UP	
FE14	Access	200UP	200UP	
FE15	Access	200UP	200UP	
FE16	Access	200UP	200UP	
FE17	Access	200UP	200UP	
FE18	Access	200UP	200UP	
FE19	Access	200UP	200UP	
FE20	Access	200UP	200UP	
FE21	Access	1UP	1UP	
FE22	Access	10UP	10UP	
FE23	Access	10UP	10UP	
FE24	Access	3UP	3UP	
GE1	Trunk	1P	1P	1
GE2	Trunk	1P	1P	1

Sind alle Ports wie gewünscht konfiguriert, ist die Konfiguration zu speichern (Kopie der running-config auf die startup-config), eine Sicherungskopie anzulegen und abschliessend ist der Switch neu zu starten.

Wichtig: Es ist immer das Protokoll 802.1q für die Definition der VLANs anzuwenden. Dies ist ein genormtes Netzwerkprotokoll, das es ermöglicht, sog. tagged VLANs zu definieren.

Netzkonfiguration VM-Host

Bonds erstellen

Stehen auf dem VM-Host mehrere Netzwerkkarten zur Verfügung, so bietet es sich an, diese als Bonds (Link Aggregation) zu bündeln. Auf dem Hypervisor sind dann zudem VLAN Bridges anzulegen.

In dem hier dokumentierten Netzzenario werden vier Netzwerkkarten zu einem Bond zusammengefasst und dann die VLANs eingerichtet. Dies Abbildung der VLANs erfolgt auf dem Hypervisor mithilfe von VLAN Bridges. Eine Netzwerkkarte, die an ein VLAN Bridge angeschlossen wird, erhält den jeweiligen VLAN-TAG.

Auf diese Weise können VMs flexibel den VLANs zugeordnet werden.

Nachstehend wird die Konfiguration des Hypervisors in der Übersicht mithilfe von Proxmox v6 dargestellt. Für andere Hypervisor müssen die Einstellungen entsprechend angepasst werden.

Übersicht der VM-Host Netzwerkkonfiguration

Nachstehende Abb. zeigt die Netzwerkeinstellungen des Proxmox-Hosts in der Übersicht:

Name ↑	Type	Active	Autostart	VLAN a...	Ports/Slaves	Bond Mode	CIDR	Gateway	Comment
bond0	Linux Bond	Yes	Yes	No	enp4s0 en...	LACP (802...			4-port Bond for all VLANs - LACP-Modus
enp4s0	Network Device	Yes	No	No					
enp5s0	Network Device	Yes	No	No					
enp6s0	Network Device	Yes	No	No					
enp7s0	Network Device	Yes	No	No					
vmbr0	Linux Bridge	Yes	Yes	No	enp7s0		192.168.199.6...	192.168.199.1	VLAN 1 Management
vmbr1	Linux Bridge	Yes	Yes	No	bond0				Bridge für 4-fach Bond
vmbr10	Linux Bridge	Yes	Yes	No	bond0.10				VLAN 10 Server
vmbr100	Linux Bridge	Yes	Yes	No	bond0.100				VLAN 100 Raum 100
vmbr20	Linux Bridge	Yes	Yes	No	bond0.20				VLAN 20 WLAN LuL
vmbr200	Linux Bridge	Yes	Yes	No	bond0.200				VLAN 200 Raum 200
vmbr30	Linux Bridge	Yes	Yes	No	bond0.30				VLAN 30 WLAN SuS
vmbr40	Linux Bridge	Yes	Yes	No	bond0.40				VLAN 40 Lehrer
vmbr5	Linux Bridge	Yes	Yes	No	bond0.5				VLAN 5 Internet / WAN

Diese Konfiguration können entweder durch Eintragungen in der Proxmox-GUI erfolgen, oder durch Ergänzung der Datei /etc/network/interfaces

```

auto lo
iface lo inet loopback

iface enp7s0 inet manual

iface enp4s0 inet manual

iface enp5s0 inet manual

iface enp6s0 inet manual

auto bond0
iface bond0 inet manual
    bond-slaves enp4s0 enp5s0 enp6s0
    bond-miimon 100
    bond-mode 802.3ad
    bond-xmit-hash-policy layer2+3
# 3-port Bond for all VLANs - LACP-Modus

auto vmbr0
iface vmbr0 inet static
    address 192.168.1.10 # Managment IP Proxmox
    netmask 255.255.255.0
    gateway 192.168.1.254
    bridge-ports enp7s0
    bridge-stp off
    bridge-fd 0
    bridge_maxage 0
    brdige_ageing 0

```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
        bridge_maxwait 0
#Bridge für 3-fach Bond

auto vmbr5
iface vmbr5 inet manual
    bridge-ports bond0.5
    bridge-stp off
    bridge-fd 0
    bridge_maxage 0
    bridge_ageing 0
    bridge_maxwait 0
#VLAN 5 Internet / WAN

auto vmbr10
iface vmbr10 inet manual
    bridge-ports bond0.10
    bridge-stp off
    bridge-fd 0
    bridge_maxage 0
    bridge_ageing 0
    bridge_maxwait 0
#VLAN 10 Servernetz

auto vmbr20
iface vmbr20 inet manual
    bridge-ports bond0.20
    bridge-stp off
    bridge-fd 0
    bridge_maxage 0
    bridge_ageing 0
    bridge_maxwait 0
#VLAN 20 WLAN LuL

auto vmbr30
iface vmbr30 inet manual
    bridge-ports bond0.30
    bridge-stp off
    bridge-fd 0
    bridge_maxage 0
    bridge_ageing 0
    bridge_maxwait 0
#VLAN 30 WLAN SuS

auto vmbr40
iface vmbr40 inet manual
    bridge-ports bond0.40
    bridge-stp off
    bridge-fd 0
    bridge_maxage 0
    bridge_ageing 0
    bridge_maxwait 0
#VLAN 40 Lehrernetz
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```

auto vmbr100
iface vmbr100 inet manual
    bridge-ports bond0.100
    bridge-stp off
    bridge-fd 0
    bridge_maxage 0
    bridge_ageing 0
    bridge_maxwait 0
#VLAN 100 Raum 100

auto vmbr200
iface vmbr200 inet manual
    bridge-ports bond0.200
    bridge-stp off
    bridge-fd 0
    bridge_maxage 0
    bridge_ageing 0
    bridge_maxwait 0
#VLAN 200 Raum 200

```

Nach einem Neustart sind die VLAN Bridges nutzbar.

Nach dem Import der VMs sind nun deren Netzwerkkarten den richtigen VLAN Bridges zuzuordnen. Dies muss für alle VMs erfolgen.

Die Anpassung sieht unter Proxmox für OPSense wie folgt aus:

Virtual Machine 112 (lmm7-opsense-vlans) on node 'lmm7-testserver'

Summary	Add	Remove	Edit	Resize disk	Move disk	Revert
Console						
Hardware						
Cloud-Init						
Options						
Task History						
Monitor						
Backup						
Replication						
Snapshots						
Firewall						
Permissions						
Memory	2.00 GiB					
Processors	2 (1 sockets, 2 cores)					
BIOS	Default (SeaBIOS)					
Display	Default					
Machine	Default (i440fx)					
SCSI Controller	VirtIO SCSI					
CD/DVD Drive (ide2)	none,media=cdrom					
Hard Disk (scsi0)	zfspool:vm-112-disk-0,size=10G					
Network Device (net0)	e1000=4E:E0:AC:0B:97:28,bridge=vmbr30,firewall=1					
Network Device (net1)	e1000=E2:81:C1:AF:1D:9E,bridge=vmbr5,firewall=1					
Network Device (net2)	e1000=B6:92:EB:0A:62:E8,bridge=vmbr10,firewall=1					
Network Device (net3)	e1000=7A:55:D8:49:A1:D1,bridge=vmbr20,firewall=1					

Netzanpassung VMs

Zunächst sind in der OPNsense®-VM die Netzwerkkarten korrekt den VLAN Bridges des Hypervisors zuzuordnen. Danach sind den Netzwerkkarten die korrekten IPs (FW: 10.0.0.254/24, OPT1: 10.3.0.254/24, OPT2: 10.4.0.0/24, WAN: DHCPv4) zuzuordnen. Danach ist die VM neu zu starten.

Die virtuellen Maschinen (Server, Docker-Host, OPSI und ggf. XOA) sind mithilfe des Befehls `linuxmuster-prepare` auf die gewünschte Struktur anzupassen, so dass diese die korrekten Adressen aus dem Servernetz zugewiesen bekommen.

Hinweis: siehe zur ausführlichen Darstellung von `linuxmuster-prepare` [Netzbereich anpassen](#)

Als Bsp. zur Nutzung des Konsolenbefehls pro virtueller Maschine wird nachstehend die Anpassung des Servers erklärt:

```
linuxmuster-prepare -p server -n 10.0.0.1/24 -d meineschule.de -f 10.0.0.254
linuxmuster-prepare -p opsi -n 10.0.0.2/24 -d meineschule.de -f 10.0.0.254
linuxmuster-prepare -p docker -n 10.0.0.3/24 -d meineschule.de -f 10.0.0.254
```

Richtet das Server-Profil wie folgt ein (übersetzt für die erste Code-Zeile):

- Profil/Hostname server,
- IP/Bitmask 10.0.0.1/24,
- Domänenname meineschule.de,
- Gateway/DNS 10.0.0.254

Wurde dies für alle verwendeten VMs durchgeführt, ist zu prüfen, ob die VMs im Servernetz sich untereinander erreichen können.

Vom Server aus ist die Erreichbarkeit der Firewall, der Docker-, der OPSI- und ggf. der XOA-VM zu prüfen.

```
ping 10.0.0.254
ping 10.0.0.2
ping 10.0.0.3
ping 10.0.0.4
```

Sofern erfolgreich Antwortpakete zu sehen sind, kann mit dem nächsten Schritt die Einrichtung fortgesetzt werden.

Weitere Subnetze definieren

Weitere Subnetze ergänzt man nach dem Setup in der Datei `/etc/linuxmuster/subnets.csv`.

Für o.g. Netzstruktur müsste die Datei folgende Eintragungen aufweisen:

```
# Network/Prefix;Router-IP (last available IP);1. Range-IP;Last-Range-IP;SETUP-Flag
# Servernetz;VLAN-GW nicht FW IP
10.0.0.0/24;10.0.0.253;10.0.0.100;10.0.0.200;SETUP
# add your subnets below
# Lehrernetz
10.1.0.0/24;10.1.0.254;10.1.0.1;10.1.0.253;SETUP
# Schuelernetz Raum 100
10.2.100.0/24;10.2.100.254;10.2.100.1;10.2.100.253;SETUP
# Schuelernetz Raum 200
10.2.200.0/24;10.2.200.254;10.2.200.1;10.2.200.253;SETUP
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
# WLAN-Lehrer
10.3.0.0/24;10.3.0.253;10.3.0.1;10.3.0.252;SETUP
# WLAN-Schueler
10.4.0.0/24;10.4.0.253;10.4.0.1;10.4.0.252;SETUP
```

Hinweise:

- Im zweiten Feld der Zeile steht die IP-Adresse des Subnetz-Gateways, die auf dem Layer-3-Switch für das entsprechende VLAN-Interface konfiguriert werden muss (s.o. - bereits auf dem L3-Switch erfolgt).
- Optional können im dritten und vierten Feld Anfangs- und Endadressen für eine freie DHCP-Range angegeben werden.
- Wichtig ist darüberhinaus, dass auf dem Switch für das Servernetz ebenfalls ein VLAN-Interface mit einer IP-Adresse aus dem Subnetz (z.B. 10.0.0.253) als Gateway eingerichtet werden muss.
- Diese IP muss anstatt der Firewall-IP als Router-IP in die Servernetz-Zeile in subnets.csv eingetragen werden.

Subnetze importieren

Die geänderte Subnetz-Konfiguration wird mit dem Befehl `linuxmuster-import-subnets` übernommen. Dabei werden die Subnetze in die DHCP-Server-Konfiguration eingetragen. Außerdem richtet das Skript statische Routen in die Subnetze über die definierten Gateway-Adressen auf Server-, Firewall-, Opsi- und Docker-VMs ein.

Firewall-Beispiel

Disabled	Network	Gateway	Description
<input type="checkbox"/>	10.0.0.0/24	GW_LAN_2 - 10.0.0.253	Route for subnet 10.0.0.0/24
<input type="checkbox"/>	10.1.0.0/24	GW_LAN_2 - 10.0.0.253	Route for subnet 10.1.0.0/24
<input type="checkbox"/>	10.2.100.0/24	GW_LAN_2 - 10.0.0.253	Route for subnet 10.2.100.0/24
<input type="checkbox"/>	10.2.200.0/24	GW_LAN_2 - 10.0.0.253	Route for subnet 10.2.200.0/24
<input type="checkbox"/>	10.3.0.0/24	GW_OPT1 - 10.3.0.253	Route for subnet 10.3.0.0/24

Auf der Firewall werden zusätzlich ausgehende NAT-Regeln für jedes Subnetz angelegt:

System

Interfaces

Firewall

Aliases

Rules

NAT

Port Forward

One-to-One

Outbound

NPTv6

Shaper

Groups

Virtual IPs

Settings

Log Files

Diagnostics

Manual rules									
<input type="checkbox"/>	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
<input type="checkbox"/>	▶ WAN	10.0.0.0/24	*	*	*	Interface address	*	NO	Outbound NAT rule for subnet 10.0.0.0/24
<input type="checkbox"/>	▶ WAN	10.1.0.0/24	*	*	*	Interface address	*	NO	Outbound NAT rule for subnet 10.1.0.0/24
<input type="checkbox"/>	▶ WAN	10.2.100.0/24	*	*	*	Interface address	*	NO	Outbound NAT rule for subnet 10.2.100.0/24
<input type="checkbox"/>	▶ WAN	10.2.200.0/24	*	*	*	Interface address	*	NO	Outbound NAT rule for subnet 10.2.200.0/24
<input type="checkbox"/>	▶ WAN	10.3.0.0/24	*	*	*	Interface address	*	NO	Outbound NAT rule for subnet 10.3.0.0/24
<input type="checkbox"/>	▶ WAN	10.4.0.0/24	*	*	*	Interface address	*	NO	Outbound NAT rule for subnet 10.4.0.0/24

und das LAN-Gateway angepasst.

Lobby

Reporting

System

Access

Configuration

Firmware

Gateways

Single

Group

Log File

System: Gateways: Single

Add

	Name	Interface	Protocol	Priority	Gateway	Monitor IP	RTT	RTTd	Loss	Status	Description	
<input type="checkbox"/>	▶ GW_LAN_2 (active)	LAN	IPv4	255 (upstream)	10.0.0.253		~	~	~	Online	Interface LAN Gateway	<div></div>
<input type="checkbox"/>	▶ WAN_DHCP	WAN	IPv4	254	192.168.199.1		~	~	~	Online	Interface WAN_DHCP Gateway	<div></div>
<input type="checkbox"/>	▶ GW_OPT1	OPT1	IPv4	255	10.3.0.253		~	~	~	Online	Interface OPT1 Gateway	<div></div>
<input type="checkbox"/>	▶		IPv6	defunct			~	~	~	Offline		<div></div>

netplan auf VMs prüfen

Der Import ändert die Netzwerkeintragen der VMs. Nach einem Neustart der VMs ist für den Server-, OPSI- und Docker-VM zu prüfen, ob die Eintragungen in der Datei `/etc/netplan/01-netcfg.yaml` den nachstehenden Eintragungen entsprechen:

```

network:
  ethernet:
    eth0:
      addresses:
        - 10.0.0.1/24
      dhcp4: false
      dhcp6: false
      gateway4: 10.0.0.254
      nameservers:
        addresses:
          - 10.0.0.1
          - 10.0.0.254
        search:
          - linuxmuster.lan
      routes:
        - to: 10.0.0.0/24
          via: 10.0.0.253
        - to: 10.1.0.0/24
          via: 10.0.0.253
        - to: 10.2.100.0/24
          via: 10.0.0.253
        - to: 10.2.200.0/24
          via: 10.0.0.253
        - to: 10.3.0.0/24
          via: 10.0.0.253
root@server:~#

```

Wichtig ist, dass die Routen zu den jeweiligen Netzen via IP 10.0.0.253 (IP des VLAN 10 auf dem L3-Switch) geleitet werden. Das Standard-Gateway bleibt hingegen die Firewall 10.0.0.254.

Sollten hier Abweichungen festgestellt werden, so sind diese so anzupassen, dass die diese den o.g. Eintragungen entsprechen. Die Änderungen werden dann mit dem Befehl `netplan apply` angewendet.

Es sollte nun die Erreichbarkeit der Server im Servernetz und der Zugriff der Server-VMs auf das Internet getestet werden. Sollte dies funktionieren, so können nun die Geräte eingetragen werden.

Geräte den Subnetzen zuweisen

Auf dem linuxmuster.net Server sind in der Datei `/etc/linuxmuster/sophomox/default-school/devices.csv` alle Geräte eingetragen. Gemäß der neuen Netzstruktur sind die IP-Adressen entsprechend anzupassen und danach mit dem Import-Befehl zu übernehmen.

Nachstehende Eintragungen sollen verdeutlichen, wie Geräte den VLANs dieses hier dokumentierten Netzszenarios zugeordnet werden:

```

#Raum;Hostname;Linbo-Klasse;MAC-Adresse;IP-Adresse;;;Arte des Geraetes;;
# Servernetz;
server;server;nopxe;aa:bb:cc:dd:ee:11;10.0.0.1;;;server;;0;;;SETUP;
server;firewall;nopxe;11:11:11:22:22:22;10.0.0.254;;;server;;0;;;SETUP;
server;opsi;nopxe;33:22:11:AA:BB:CC;10.0.0.2;;;server;;0;;;SETUP;
server;docker;nopxe;D2:31:22:11:A1:22:33;10.0.0.3;;;server;;0;;;SETUP;
#Raum R200
r200;r200-pc01;win10-efi;00:50:56:3E:A5:7A;10.2.200.1;;;computer;;2
r200;r200-pc02;win10-efi;00:50:56:3E:A5:7B;10.2.200.2;;;computer;;2
r200;r200-pc03;win10-efi;00:50:56:3E:A5:7C;10.2.200.13;;;computer;;2

```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```

r200;r200-pc04;win10-efi;00:50:56:3E:A5:7D;10.2.200.1;4;;computer;;2
# PC im VLAN der Lehrer, PCs stehen im Raum L001
1001;1001-pc01;ubu18;01:60:66:3F:A6:1A;10.1.0.1;;;computer;;2
1001;1001-pc02;ubu18;01:60:66:3F:A6:1B;10.1.0.2;;;computer;;2
1001;1001-pc03;ubu18;01:60:66:3F:A6:1C;10.1.0.3;;;computer;;2

```

Die Anpassungen in der Datei sind nun zu speichern. Danach sind die so angepassten Geräte abschliessend mithilfe des nachstehenden Befehls in das System zu übernehmen:

```
linuxmuster-import-devices
```

Die Clients in Raum 200 und im Lehrernetz sind dann anzuschliessen. Diese Clients müssen o.g. IPs erhalten. Ist dies der Fall, kann ein Linbo-Image erstellt und weitere Tests (Anmeldung, Zugriff auf den Server, Internet-Zugriff etc.) ausgeführt werden.

Erhält ein Client die korrekte IP so ist dies unter Linbo wie folgt zu erkennen:



Testen der neuen Netzstruktur

Grundsätzlich gilt, dass die einzelnen konfigurierten Netzbereiche unmittelbar zu testen sind. Wurde der L3-Switch und der Hypervisor mit den VMs konfiguriert und wurde die geeignete Verkabelung hergestellt, so ist zunächst zu testen, ob sich alle VMs im Servernetz untereinander erreichen und ob diese Internet-Zugriff haben.

Die durchzuführenden Tests sind in folgende Bereiche zu unterteilen:

- Verbindung VMs untereinander via L3-Switch (Servernetz)
- Verbindung zwischen den Switchen über das Management VLAN - in diesem Beispiel VLAN 1
- Verbindung von Endgeräten eines VLANs auf L2-Switch1 / L2-Switch2 zum linuxmuster.net Server und Verbindung zum Internet
- Verbindung von Endgeräten von L2-Switch1 via L3 Switch zu Endgeräten des identischen VLANs auf L2-Switch2
- Linbo-Start der Clients in einem Fachraum. Prüfen, ob den Geräten eine IP über die Netzgrenzen hinweg - wie in der devices.csv angegeben - erfolgreich zugewiesen wird.
- vom Server aus sind WOL-Pakete an einen Client zu senden, um diesen aufzuwecken und mit Linbo zu synchronisieren.

Download L3-Configs

Nachstehend werden Dir einige Konfigurationsdateien für L3-Switches angeboten, die Du an Dein NetzszENARIO anpassen kannst.

Für den L3-Switch Cisco SG300-28 steht die vorbereitete Konfigurationsdatei zur Verfügung, die die Konfiguration auf dem L3-Switch so einspielt, wie diese in dieser Dokumentation beschrieben wird.

Hersteller	L3 - Switch Modell	Download
Cisco	SG-300-28	Config SG300-28
Cisco	3750G (IOS 12.2)	Config 3750G
D-Link	DGS-1510-28x	Config DGS1510-28x still missing

Hinweis: Die Liste wird schrittweise erweitert. D-Link fehlt noch.

4.35 Drucker einbinden

Autor des Abschnitts: @cweikl

Zur Einrichtung der Drucker sollte folgendes Vorgehen eingehalten werden:

1. Infos zu allen Druckern zusammentragen
2. Drucker via Schulkonsole als Geräte hinzufügen
3. Drucker auf dem Server mithilfe von CUPS einrichten
4. Drucker via AD-Gruppenzuweisung konfigurieren
5. Auf dem jeweiligen Linux- oder Windows-Client ggf. Anpassungen vornehmen

Sammle nun zuerst die Infos zu den Druckern, die Du im gesamten Netzwerk einrichten möchtest.

4.35.1 Drucker Informationen

Autor des Abschnitts: @cweikl

Um in linuxmuster.net mit Druckern zu arbeiten, ist es erforderlich, dass Netzwerkdrucker zur Verfügung stehen. Es können entweder Drucker mit eingebauten Netzwerkkarten (Printservern) eingesetzt, oder bisherige Drucker mit einer geeigneten sog. „Printserver-Box“ in das Netzwerk eingebunden werden.

Vor dem Hinzufügen und Einrichten von Druckern in linuxmuster.net ist es sehr hilfreich, vorab nachstehende Informationen zu erfassen:

- die genaue Bezeichnung des Druckersmodells
- mögliche Treiber für Linux, Windows und ggf. andere Clients
- MAC-Adresse des Druckers
- Raum / Standort des Druckers
- IP-Adresse gemäß des genutzten Adressschemas

Die meisten Netzwerkdrucker sind bei Auslieferung so eingestellt, dass diese eine IP-Adresse via DHCP beziehen. Die IP-Adresse für den Drucker muss daher in der Schulkonsole gesetzt werden.

Um eine Steuerung der Drucker via Schulkonsole zu ermöglichen, müssen die Drucker zentral auf dem Server als Geräte eingetragen und auf dem Server in CUPS konfiguriert werden.

CUPS arbeitet als „zentraler Printserver“ und hält für alle dort eingerichteten Drucker entsprechende Druckwarteschlangen vor.

4.35.2 Drucker via Schulkonsole hinzufügen

Autor des Abschnitts: @cweikl

Viele Printserver und Netzwerkdrucker sind in der Lage, Ihre IP-Adresse von einem DHCP-Server zu beziehen. Zuerst muss der Drucker am Server mithilfe der Schulkonsole hinzugefügt werden. Hierbei wird dem Drucker ein Name sowie eine IP-Adresse zugewiesen.

Für das folgende Beispiel nehmen wir an, der Drucker stehe in Raum „r200“, bekomme den Namen „r200-pr01“, habe die MAC-Adresse „00:11:22:33:44:55“ und bekomme entsprechend einem IP-Adressschema die IP-Adresse 10.2.200.101.

Melde Dich als `global-admin` in der [Schulkonsole \(https://10.0.0.1\)](https://10.0.0.1) an. Wähle dort links im Menü Geräteverwaltung das Untermenü Geräte aus.

Raum	Hostname	Gruppe	MAC	IP	Sophomore-Rolle	PXE
adminlap	adminlaptop	nopxe	F0DE:F170:88:4B	10.0.0.8	Lehrer-PC	Kein PXE
r100	r10001	ubu18-new	7E43:89:04:3D:C4	10.2.100.1	Schüler-PC im Klassenzimmer	Linbo-PXE
r200	r20001	nopxe	1A59:8F:5C:89:9A	10.2.200.1	Schüler-PC im Klassenzimmer	Kein PXE
r200	r20002	ubu18-std	60EB:69:02:EA:13	10.2.200.2	Lehrer-PC im Klassenzimmer	Linbo-PXE
r200	r20003	bionic	4C52:62:07:89:0B	10.2.200.3	Lehrer-PC im Klassenzimmer	Linbo-PXE
r200	r20005	bionic	00:23:24:9:26:CC	10.2.200.5	Lehrer-PC im Klassenzimmer	Linbo-PXE
r200	r20004	win10-vm	EE:5A:87:C4:9A:DE	10.2.200.4	Lehrer-PC im Klassenzimmer	Linbo-PXE
server	server	nopxe	4a72:02:f5:4c:43	10.0.0.1	Server	Kein PXE
server	firewall	nopxe	B6:92:EB:0A:62:E8	10.0.0.254	Server	Kein PXE
server	opsi	nopxe	6E:93:D3:47:21:12	10.0.0.2	Server	Kein PXE
server	dockier	nopxe	D2:86:F9:7C:F0:8B	10.0.0.3	Server	Kein PXE
testvm	testvm	nopxe	9A:4B:27:FE:89:97	10.0.0.9	Server	Kein PXE
wlanlul	ap01lul	nopxe	00:1E:5A:54:FE:09	10.3.0.1	Router	Kein PXE

Klicke unterhalb der Geräteliste auf den Eintrag `Gerät hinzufügen`.

Es wird eine leere Zeile zur Liste hinzugefügt.

Room	Hostname	Group	MAC	IP	Schüler-PC im Klassenzimmer	Linbo-PXE
+ Gerät hinzufügen						

Die Option PXE ist zu deaktivieren, da die Drucker nicht via PXE starten. Als Gruppe ist `nopxe` einzutragen.

Für o.g. Beispieldrucker stellt sich der Eintrag wie folgt dar:

r200	r200HP-LJ-2055dn	nopxe	00:11:22:33:44:55	10.2.200.101	Drucker	Kein PXE
+ Gerät hinzufügen						

Bestätige den Eintrag mit `speichern & importieren`.

Achtung: Den hier vergebenen Druckernamen musst Du später in identischer Schreibweise in CUPS angeben (siehe nächstes Unterkapitel).

Es erscheint ein Fenster, in dem der Vorgang bestätigt wird.

Gerät wird importiert

```

#### > Creating pxe configuration.          ####
#### * ubu18-std                          ####
#### > Creating pxe configuration.          ####
#### * bionic                             ####
#### > Creating pxe configuration.          ####
#### * win10-vm                           ####
#### > Creating pxe configuration.          ####

-----
#### Restarting services:                  ####
#### * isc-dhcp-server ..... OK!          ####
#### * linbo-bittorrent ..... OK!         ####
#### * linbo-multicast ..... OK!         ####

-----
#### linuxmuster-import-devices finished at 2020-03-08 10:00:40 ####
-----

```

Einstellungen
☒ Autoscroll

DETAILS AUSBLENDEN SCHLIESSEN

Danach ist ein Neustart des Druckers empfehlenswert, damit dieser die neue IP-Adresse übernimmt.

Die Erreichbarkeit des Druckers sollte nach dem Neustart des Druckers vom Server aus vorab mithilfe des ping-Befehl überprüft werden.

4.35.3 Drucker auf dem Server hinzufügen

Autor des Abschnitts: @cweikl

Um die als Geräte bereits importierten Netzwerkdrucker einzurichten, sind diese auf dem linuxmuster.net Server mithilfe von CUPS einzurichten und bereitzustellen. Die gesamte Druckersteuerung erfolgt via Active Directory für alle Betriebssysteme, so dass diese zunächst auf dem Server bereitgestellt, den AD-Gruppen zugewiesen und ggf. Anpassungen pro Client Betriebssystem vorgenommen werden müssen.

Für die Nutzung von HP-Druckern ist es hilfreich, auf dem Server die Bibliothek HPLIP zu installieren und dann die Drucker einzurichten.

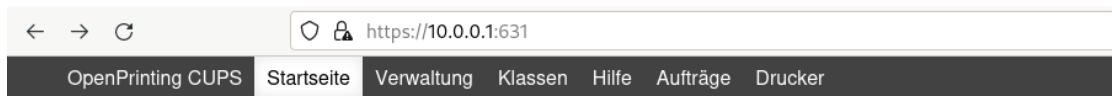
Zur Installation der HPLIP Bibliothek rufst Du unter Ubuntu 22.04 LTS Server folgenden Befehl auf dem Server auf:

```
sudo apt install hplip hplip-data hplip-gui hplip-doc
```

Starte auf einem Rechner einen Browser, um das sog. CUPS-Webinterface des Servers zur weiteren Einrichtung der Drucker aufzurufen. Hierzu füge nachstehende URL in der Adresszeile Deines Browsers ein:

```
https://10.0.0.1:631
```

Da meist nur ein selbst-signiertes Zertifikat auf dem Server installiert ist, ist es i.d.R. erforderlich, dem benutzten Browser die sichere Kommunikation ausnahmsweise zu erlauben (SSL-Zertifikat akzeptieren).



OpenPrinting CUPS 2.4.1

CUPS basiert auf Standards, Open Source Drucksystem entwickelt durch [OpenPrinting](#) für Linux® und andere UNIX®-artige I lokaler und Netzwerkdrucker.

CUPS für Benutzer

[Überblick über CUPS](#)

[Befehlszeilen-Druck und Optionen](#)

CUPS für Administratoren

[Drucker und Klassen hinzufügen](#)

[Betriebs-Richtlinie festlegen](#)

[Benutzung von Netzwerk-Druckern](#)

[Firewalls](#)


[cupsd.conf Referenz](#)

Drucker hinzufügen

Nach der Anmeldung an CUPS wähle den Menüpunkt **Verwaltung** aus.

Es erscheint die Login-Aufforderung von CUPS auf dem Server:

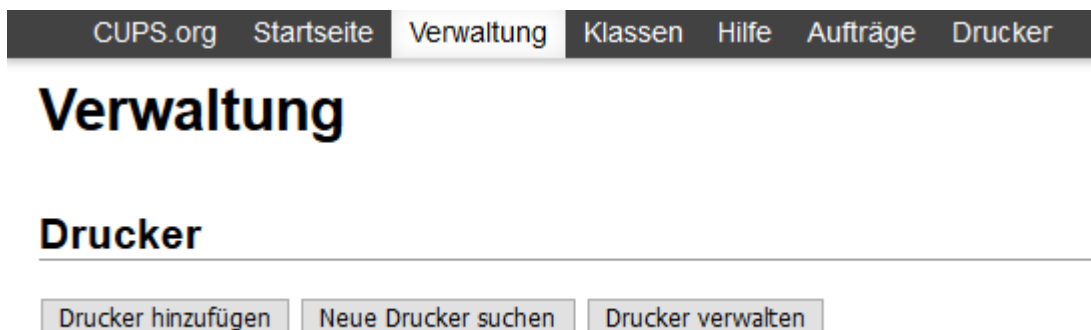
Authentifizierung erforderlich ✕

 https://10.0.0.1:631 verlangt einen Benutzernamen und ein Passwort. Ausgabe der Website: "CUPS"

Benutzername:

Passwort:

Melde Dich als root dort an. Nach erfolgreicher Anmeldung siehst Du folgende Einträge:



Rufe den Untermenüpunkt **Drucker hinzufügen** aus. Es erscheint nachstehende Maske. Wähle als Netzwerkdrucker i.d.R. LPD/LPR-Host aus und klicke auf **weiter**.

CUPS.org Startseite Verwaltung Klassen Hilfe Aufträge Drucker

Drucker hinzufügen

Drucker hinzufügen (Schritt 1/5)

Lokale Drucker: ☐ CUPS-BRF (Virtual Braille BRF Printer)
☐ CUPS-PDF (Virtual PDF Printer)

Gefundene Netzwerkdrucker:

Andere Netzwerkdrucker: ☐ AppSocket/HP JetDirect
☐ Backend Error Handler
☒ LPD/LPR-Host oder -Drucker
☐ Internet Printing Protocol (ipp)
☐ Internet Printing Protocol (ipps)
☐ Internet Printing Protocol (http)
☐ Internet Printing Protocol (https)
☐ Windows Printer via SAMBA

Weiter

Gib als Verbindung die IP-Adresse und den Port des LPD-Druckers wie in der Abb. an:

CUPS.org Startseite Verwaltung Klassen Hilfe Aufträge Drucker

Drucker hinzufügen

Drucker hinzufügen (Schritt 2/5)

Verbindung:

Beispiele:

```
http://hostname:631/ipp/
http://hostname:631/ipp/port1

ipp://hostname/ipp/
ipp://hostname/ipp/port1

lpd://hostname/queue

socket://hostname
socket://hostname:9100
```

Beispiele und gängige URIs finden sich in der Hilfe unter ["Netzwerkdrucker"](#).

Weiter

Klicke auf weiter. Wähle nun den geeigneten Druckertreiber für Deinen Drucker aus:

CUPS.org	Startseite	Verwaltung	Klassen	Hilfe	Aufträge	Drucker
----------	------------	------------	---------	-------	----------	---------

Drucker hinzufügen

Drucker hinzufügen (Schritt 3/5)

Name:
(Darf alle druckbaren Zeichen außer "/", "#", und Leerzeichen enthalten)

Beschreibung:
(Menschenlesbare Beschreibung wie etwa "HP LaserJet mit Duplexer")

Ort:
(Menschenlesbarer Ort wie etwa "Labor 1")

Verbindung: socket://10.2.200.101:9100

Freigabe: ☒ Drucker im Netzwerk freigeben

Wähle den Hersteller aus, dann erscheint eine Liste mit den verfügbaren Druckertreibern. Wähle in der Liste den korrekten Drucker aus. Sollte dieser in der Liste nicht enthalten sein, so klicke auf PPD-Datei bereitstellen -> Durchsuchen. Wähle nun die PPD-Datei mit dem korrekten Druckertreiber aus, den Du zuvor von der Website des Herstellers heruntergeladen hast.

Drucker hinzufügen

Drucker hinzufügen (Schritt 5/5)

Name: r200-HP-LJ-P2055DN

Beschreibung: Drucker JP Laser Jet P2055DN

Ort: Raum 200

Verbindung: socket://10.2.200.101:9100

Freigabe: Drucker im Netzwerk freigeben

Hersteller: HP

Modell:

- HP LaserJet 1220 - CUPS+Gutenprint v5.2.13 (en)
- HP LaserJet 1300 - CUPS+Gutenprint v5.2.13 (en)
- HP LaserJet 1320 - CUPS+Gutenprint v5.2.13 (en)
- HP LaserJet 2100 - CUPS+Gutenprint v5.2.13 (en)**
- HP LaserJet 2100M - CUPS+Gutenprint v5.2.13 (en)
- HP LaserJet 2200 - CUPS+Gutenprint v5.2.13 (en)
- HP LaserJet 2300 - CUPS+Gutenprint v5.2.13 (en)
- HP LaserJet 2410 - CUPS+Gutenprint v5.2.13 (en)
- HP LaserJet 2420 - CUPS+Gutenprint v5.2.13 (en)
- HP LaserJet 2430 - CUPS+Gutenprint v5.2.13 (en)

Oder PPD-Datei bereitstellen: Keine Datei ausgewählt.

Drucker konfigurieren

Danach erscheinen die Standardeinstellungen für den hinzugefügten Drucker. Wähle hier die gewünschten Einstellungen aus und speichere diese als **Standardeinstellungen** festlegen. Gib unter Fehlerbehandlung **abort-job** an, um sicherzustellen, dass CUPS im Fehlerfall den Druckjob löscht.

r200-HP-LJ-P2055DN

r200-HP-LJ-P2055DN (Leerlauf, Aufträge annehmen, Netzwerkfreigabe, Farbmanagement)

Wartung

Beschreibung: Drucker JP Laser Jet P2055DN

Ort: Raum 200

Treiber: HP LaserJet 2100 - CUPS+Gutenprint v5.2.13 (schwarz-weiß, 2-seitiges Drucken)

Verbindung: socket://10.2.200.101:9100

Standardeinstellungen: job-sheets=none, none media=iso_a4_210x297mm sides=two-sided-long-edge

Aufträge

Suche in r200-HP-LJ-P2055DN:

Jobs listed in print order; held jobs appear first.

Damit der Drucker nur von berechtigten Nutzern verwendet werden kann, muss noch der Kreis der erlaubten Benutzer festgelegt werden: Gib unter Erlaubte Benutzer festlegen die Gruppe @printing an. Lehrer sind standardmäßig in der Gruppe. Bei Schülern wird die Zugehörigkeit über die Spalte **Drucken** in der Schulkonsole gesteuert.



Danach findet sich der neue Drucker in der Druckerliste in CUPS.

CUPS.org Startseite Verwaltung Klassen Hilfe Aufträge Drucker				
Drucker				
Suche in Druckern: <input type="text"/> Suchen Leeren				
Zeige 2 von 2 Druckern.				
Warteschlange	Beschreibung	Ort	Hersteller und Modell	Status
PDF	PDF		Generic CUPS-PDF Printer (w/ options)	Leerlauf
r200-HP-LJ-P2055DN	Drucker JP Laser Jet P2055DN	Raum 200	HP LaserJet 2100 - CUPS+Gutenprint v5.2.13	Leerlauf

Nun wird Dein Netzwerkdrucker vom Server den Clients bereitgestellt.

Angesprochen wird obiger Drucker über folgende URL:

```
http://10.0.0.1:631/printers/r200-HP-LJ-P2055DN
```

4.35.4 Drucker einzelnen Räumen zuweisen

Autor des Abschnitts: @cweikl, @rettich

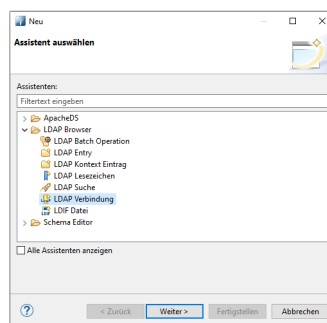
Achtung: Sobald diese Funktion in der Schulkonsole zur Verfügung steht, wird dieser Teil der Dokumentation ergänzt.

Für die Raumzuweisung von Druckern eignet sich am besten das *Apache Directory Studio*. Das *Apache Directory Studio* braucht das Java Development Kit. Lade dafür von www.oracle.com die Installationsdatei und installiere sie. Lade anschließend von directory.apache.org die aktuelle Version des *Apache Directory Studios* herunter und installiere sie ebenfalls.

Hinweis: Auf dem Ubuntu-Client kann das *Apache Directory Studio* direkt ausgeführt werden.

Schauen wir uns mit dem *Apache Directory Studio* die AD-Struktur etwas genauer an. Dazu müssen wir zunächst eine Verbindung zum Server aufbauen.

Starte das *Apache Directory Studio* und gehe in der Menü-Leiste auf Datei → Neu.



Wähle LDAP-Verbindung und klicke auf weiter.

Gib der Verbindung einen Namen und trage die Verbindungsdaten des Servers ein.

Klicke auf Netzwerkparameter überprüfen. Falls der Server nur ein selbst signiertes Zertifikat hat, erscheint der folgende Dialog:

Wähle **Diesem Zertifikat immer vertrauen** und klicke auf ok. Wenn Du jetzt auf Netzwerkparameterüberprüfen klickst, sollte die Verbindung erfolgreich aufgebaut werden.

Nachdem Du auf **weiter** geklickt hast, erscheint ein neues Dialogfenster in dem die Anmeldeinformationen abgefragt werden.

Als Bind DN trägst Du `CN=global-admin,OU=Management,OU=GLOBAL`, gefolgt von Deiner DN ein. In diesem Beispiel ist das `CN=global-admin,OU=Management,OU=GLOBAL,DC=linuxmuster,DC=lan`.

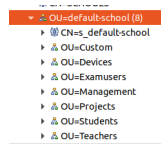
Hinweis: Du nutzt hier den global-admin, weil Du Schreibrechte brauchst. Sicherheitshalber solltest Du vor Deiner Arbeit einen Snapshot des Servers machen.

Klicke auf **Anwenden und Schließen**.

Der Baum des AD wird geladen und angezeigt.

Schreib Dich in der Schulkonsole bei den Druckern ein.

Im AD-Baum sieht das dann so aus:



In Devices findest Du Klassenräume und ihre Rechner. Und es gibt dort auch die printer-groups in der die Drucker zu finden sind. In Students sind die Klassen und ihre Schüler. Und in Teachers findest Du die Lehrer.

Im Eintrag des Benutzers sind die Drucker als memberOf eingetragen.

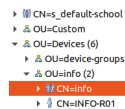
memberOf	CN=11a,OU=11a,OU=Students,OU=default-school,OU=SCHOOLS,DC=linuxmuster,DC=lan
memberOf	CN=infolaser,OU=printer-groups,OU=Devices,OU=default-school,OU=SCHOOLS,DC=linuxmuster,DC=lan
memberOf	CN=internet,OU=Management,OU=default-school,OU=SCHOOLS,DC=linuxmuster,DC=lan
memberOf	CN=intranet,OU=Management,OU=default-school,OU=SCHOOLS,DC=linuxmuster,DC=lan
memberOf	CN=itglaser,OU=printer-groups,OU=Devices,OU=default-school,OU=SCHOOLS,DC=linuxmuster,DC=lan
memberOf	CN=printing,OU=Management,OU=default-school,OU=SCHOOLS,DC=linuxmuster,DC=lan
memberOf	CN=role-teacher,OU=Groups,OU=GLOBAL,DC=linuxmuster,DC=lan
memberOf	CN=teachers,OU=Teachers,OU=default-school,OU=SCHOOLS,DC=linuxmuster,DC=lan
memberOf	CN=webfilter,OU=Management,OU=default-school,OU=SCHOOLS,DC=linuxmuster,DC=lan
memberOf	CN=wifi,OU=Management,OU=default-school,OU=SCHOOLS,DC=linuxmuster,DC=lan

Beim Eintrag des Druckers ist der Benutzer als member eingetragen.

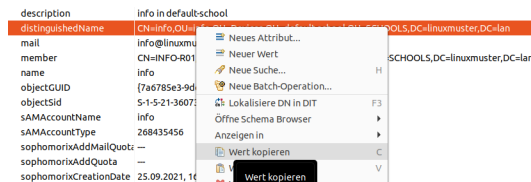
member	CN=retlich,OU=Teachers,OU=default-school,OU=SCHOOLS,DC=linuxmuster,DC=lan
name	infolaser

Genau so tragen wir die Gruppe eines Raums als Member in die Gruppe eines Druckers ein. Im Beispiel soll der Informatikraum in die Gruppe des InfoLasers eingetragen werden.

Navigiere zum Gruppeneintrag des Informatik-Raums.



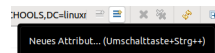
Im mittleren Fenster werden die Einträge der Gruppe info angezeigt. Kopiere mit einem Rechtsklick den distinguishedName.



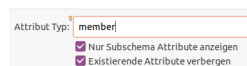
Navigiere zur Gruppe des Druckers.



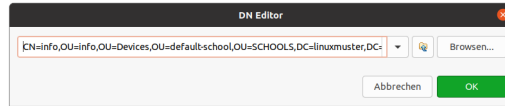
und klicke auf Neues Attribut...



Als Attribut-Typ gibst Du member ein und klickst anschließend auf Fertigstellen.



Jetzt Fügt Du mit <Strg>+V den vorher kopierten distinguishedName ein und klickst anschließend auf OK.



Alle Rechner die im Informatikraum stehen, werden ab „jetzt“ Zugriff auf den InfoLaser haben. Allerdings kann es eine ganze Weile dauern, bis sich dieser Eintrag auf die Druckerverteilung auswirkt. Starte am besten Deinen Client neu.

4.35.5 Drucker am Linux-Client

In dieser Dokumentation wird davon ausgegangen, dass der Linux-Client mithilfe des aktuellen Pakets `linuxmuster-linuxclient7` der Domäne hinzugefügt wurde.

Vorgehen

1. Drucker - wie zuvor dokumentiert - auf dem Server einrichten.
2. Linux-Client erstellen wie unter *ref:install-linux-clients-label* beschrieben
3. ggf. das CUPS Browsing auf dem Server anpassen, sofern nicht jeder Rechner alle Drucker anzeigen soll. (siehe: *ref:install-linux-clients-label*)
4. Auf dem Server cupsd neu starten.
5. Linux-Client neu synchronisieren.
6. Nach der Anmeldung prüfen, ob Drucker angezeigt werden und dann Drucker testen.

Drucker testen

Nachdem der Linux-Client neu gestartet und synchronisiert wurde, meldest Du Dich an und prüfst, ob unter **Drucker** alle zuvor auf dem Server eingerichteten Drucker angezeigt werden. Dies muss der Fall sein, sofern aus dem jeweiligen Raum oder von dem jeweiligen PC ein Zugriff auf dem Drucker überhaupt gewünscht ist und zuvor eingerichtet wurde.

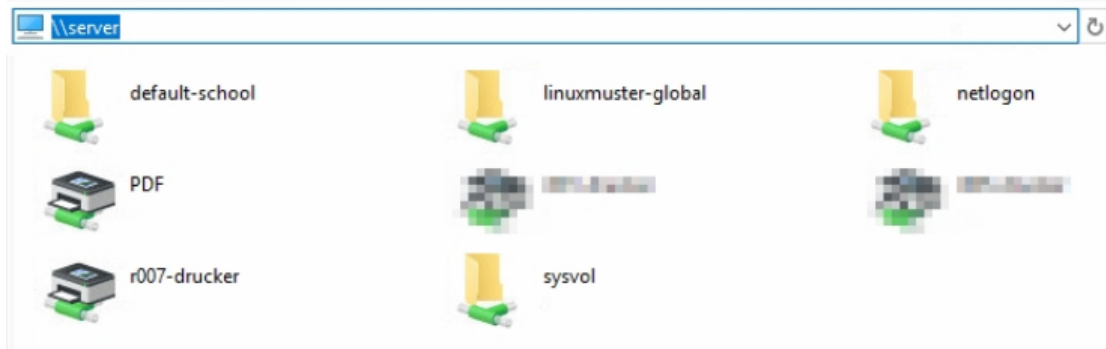
Markiere einen Drucker, klicke mit der rechten Maustaste und wähle im Kontextmenü den Punkt **Eigenschaften** aus. Klicke unterhalb von **Tests** und **Wartungen** den Button **Testseite drucken** aus.

Führe das Verfahren aus allen Räumen und von allen PCs durch.

4.35.6 Drucker am Windows - Client

Autor des Abschnitts: @cweikl, @rettich

Nachdem die Drucker auf dem Server eingerichtet wurden, sind diese auf Windows-Clients nun als Freigaben sichtbar.



Die Treiber sind nun über die Microsoft Management Console (MMC) hinzuzufügen.

Dem global-admin die nötigen Rechte einräumen

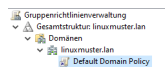
Bevor es losgehen kann, müssen wir dem *global-admin* noch die nötigen Rechte auf dem Server einräumen. Melde Dich dazu als *root* auf dem Server an und führen Sie die folgenden Befehle aus:

```
net rpc rights grant "LINUXMUSTER\Domain Admins" SePrintOperatorPrivilege -U
↪ "LINUXMUSTER\global-admin"
chgrp -R "LINUXMUSTER\Domain Admins" /var/lib/samba/printers/
chmod -R 2775 /var/lib/samba/printers/
```

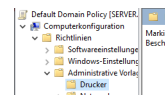
Dem Server vertrauen

Seit Juli 2016 hat Windows10 ein neues Sicherheitsfeature. Es muss über GPOs festgelegt werden, dass die Windows-Clients unserem Server vertrauen. Dazu gehen wir wie folgt vor:

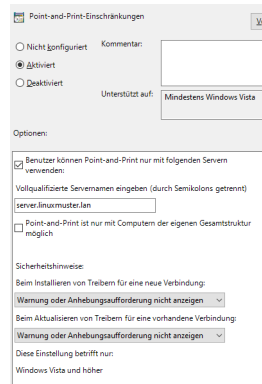
Melde Dich als *global-admin* am Windows-Client an und starte die Gruppenrichtlinienverwaltung (Wie Du sie installierst kannst Du [hier](#) nachlesen). Navigiere zur Default Domain Policy von linuxmuster.lan.



Wähle mit einem Rechtsklick **Bearbeiten**. Es öffnet sich der Gruppenrichtlinien-Editor. Navigiere zu **Computerkonfiguration** → **Richtlinien** → **Administrative Vorlagen** → **Drucker**.



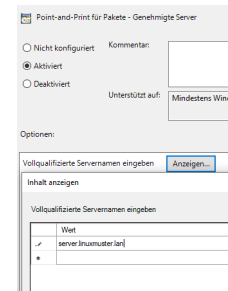
Doppelklicke auf **Point and Print Einschränkungen**, aktiviere die Richtlinie und setze folgende Einstellungen:



Setze einen Haken bei Benutzer können Point and Print für Pakete - Genehmigte Server verwenden. Gib die FQDN des Servers bei Vollqualifizierte Servernamen ein und wähle bei Beim Installieren von Treibern für eine neue Verbindung und bei Beim Aktualisieren von Treibern für eine vorhandene Verbindung die Einstellung Warnung oder Anhebungsaufforderung nicht anzeigen.

Bestätige mit OK.

Doppelklicke auf Point and Print für Pakete - Genehmigte Server und aktiviere die Richtlinie.



Aktiviere die Richtlinie, klicken auf Anzeigen... und gib den FQDN des Servers ein.

Bestätige zwei mal mit OK.

Schließe den Gruppenrichtlinien-Editor und die Gruppenrichtlinien-Verwaltung

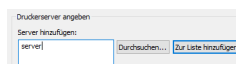
Starte den Rechner neu.

Druckertreiber auf dem Server installieren

Hinweis: Es können ausschließlich v3 Druckertreiber verwendet werden. V4 Druckertreiber werden Stand Samba 4.7 (September 2019) noch nicht unterstützt.

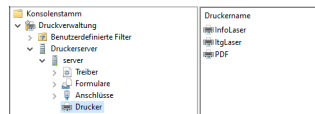
Jetzt können wir die Druckertreiber auf dem Server installieren.

Öffne als global-admin das Programm mmc.exe, wähle Datei → snapin hinzufügen/entfernen und füge die Druckverwaltung hinzu.



Trage den Server ein, klicke auf zur Liste hinzufügen und anschließend auf Fertigstellen und OK.

Wie man sieht, sind die Drucker dem Systems bekannt. Du musst nur noch die Druckertreiber installieren.



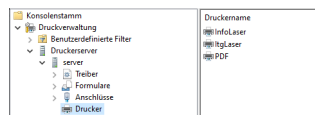
Mache einen Rechtsklick auf **Treiber** und wähle **Treiber hinzufügen**. Gehe zu **Weiter** → **Weiter** → **Datenträger...** **Durchsuchen** → **Ok** und wähle den richtigen Druckertreiber. Es werden nur Microsoft zertifizierte Treiber akzeptiert. Falls Du mit einem Treiber Probleme haben solltest, versuche es eventuell mit einem etwas älteren Treiber. Die werden sehr oft akzeptiert.

Klicke abschließend auf **Fertigstellen**.

Einem Drucker einen Druckertreiber zuweisen

Jetzt müssen wir nur noch den Druckern die Druckertreiber zuweisen.

Öffne als global-admin das Programm `mmc.exe` und navigiere zu **Drucker**.



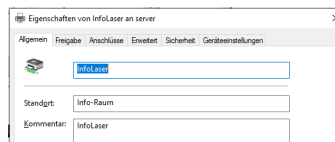
Mache einen Rechtsklick auf den Drucker, dem Du einen Druckertreiber zuweisen möchtest und wähle **Eigenschaften...** Falls Du gefragt wirst, ob Du einen Druckertreiber lokal installieren möchtest, antworte mit **Nein**.

Gehe zum Reiter **Erweitert**, wähle bei **Treiber** den passenden Treiber für den Drucker und bestätige mit **OK**.



Leider ändert Windows den Namen des Druckers in den Namen des Druckertreibers. Um wieder den richtigen Namen zu setzen, machst Du in `mmc.exe` einen Rechtsklick auf den Drucker und wählst **Eigenschaften...**

Ändere unter dem Reiter **Allgemein** den Namen des Druckers auf den Namen, den er in CUPS hat und bestätige mit **OK**.



Benutzern erlauben einen Druckertreiber zu installieren

Die Windows-Clients erlauben normalen Benutzern nicht, einen Druckertreiber zu installieren. Das müssen wir ändern, da sonst normale Benutzer nicht drucken können. Am einfachsten geht das mit folgendem Registry-Eintrag:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\
↳PointAndPrint
RestrictDriverInstallationToAdministrators=0 (DWORD)
```

Erzeuge den Eintrag mit dem Registrierungs-Editor direkt in die Registry oder lege Dir die Datei win10.printer.reg mit folgendem Inhalt an:

```
Windows Registry Editor Version 5.00
; linuxmuster.net 7 version
; notwendig, damit Druckertreiber installiert werden können
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\
↳PointAndPrint]
"RestrictDriverInstallationToAdministrators"=dword:00000000
```

Und doppelklicke als *global-admin* win10.printer.reg.

Jetzt muss nur noch ein neues Image erzeugt und verteilt werden, damit die Firewall-Einstellungen und der Registry-Eintrag auf die Windows-Clients verteilt werden.

Wenn alles geklappt hat, installieren sich die Druckertreiber auf den Windows-Clients sobald sich ein Benutzer anmeldet. Wie Du die Drucker-Raumzuweisung machst, kannst Du [hier](#) nachlesen.

Hat ein Lehrer in der Schulkonsole bei einem Drucker einen Haken gesetzt, wird der Drucker bei der Anmeldung des Lehrers zusätzlich installiert. Das ist dann sinnvoll, wenn beispielsweise ein Lehrer oft in der Nähe des Physik-Drucker unterrichtet. Dann kann er auch von jedem Laptop aus auf dem Physik-Drucker ausdrucken.

Falls o.g. Weg nicht funktionieren sollte, ist der Treiber manuell auf dem Windows Client zu installieren. Anschließend ist der Druckertreiber dem Drucker auf dem Server zuzuweisen.

Hierzu sind die eingerichteten Drucker auf dem Server zunächst auszugeben:

```
rpcclient 10.0.0.1 -U "LINUXMUSTER\global-admin" -c "enumdrivers 3"
```

LINUXMUSTER stellt den Namen der eigenen Samba-Domäne dar, global-admin ist der Administrator auf dem Server, 10.0.0.1 ist die IP des Server.

Danach ist der lokale Druckertreiber dem Drucker zuzuordnen - in nachstehendem Beispiel ist dies der Druckertreiber *HP Universal Printing PS*:

```
rpcclient 10.0.0.1 -U "LINUXMUSTER\global-admin" -c 'setdriver "DemoPrinter"
↳"HP Universal Printing PS"'
```

Das Ergebnis kann mit dem zuvor genannten Befehl kontrolliert werden:

```
rpcclient 10.0.0.1 -U "LINUXMUSTER\global-admin" -c "enumdrivers 3"
```

Danach ist der Druck zu testen. Funktioniert der Drucker wie gewünscht ist ein neues Image für den Windows-Client zu erstellen.

4.35.7 Hinweise Mac OS X - Clients

Für Mac OS X - Clients gibt es für linuxmuster.net keine Pakete zur Einbindung. Daher an dieser Stelle in der Dokumentation nur für diejenigen, die Mac OS X - Clients in einem linuxmuster.net Netzwerk einsetzen und mit diesen Clients drucken möchte, nachstehend nur kurz einige Hinweise zu Druckerproblemen:

Bei der Standardkonfiguration kann es passieren, dass die Kommunikation mit dem Drucker nicht funktioniert und zum Beispiel nach der Installation jeder Druck auf einen Fehler läuft:

Waiting **for** Authentication...

Wenn ein Drucker unter MacOS mit dem Drucker-Dialog hinzugefügt wird, kann nur das IPP-Protokoll ausgewählt (Reiter „IP“) werden. Bei „Address“ ist dann die Server-IP mit dem CUPS-Port 10.0.0.1:631 einzutragen. Bei „Queue“ /printers/printer-name ist der Druckername anzugeben (z.B. /printers/lz-drucker).

Hinweis: Sollte dies nicht funktionieren, ist zunächst die Web-Oberfläche von CUPS local auf dem Mac zu aktivieren (localhost:631) und anschließend dort der Drucker per IPP-Protokoll und <http://10.0.0.1:631/printers/printer-name> hinzuzufügen. Gibt es Treiberprobleme und der Drucker druckte nur Kauderwelsch, kann es helfen, statt den generischen Postscript-Treiber den generischen PCL-Treiber auszuwählen, oder ggf. die Installation der Originaltreiber (in dem Fall von Kyocera) auszuführen. Ein ähnliches Problem mit dem Drucker und MacOS X wird hier beschrieben: <https://ask.linuxmuster.net/t/mac-os-x-clients-an-cups/1176>

4.36 Schulkonsole des global-admin

Autor des Abschnitts: @maurice, @cweikl, @MachtDochNix (pics)

4.36.1 Allgemeine Bedienung

Die Schulkonsole wird im Browser über <https://10.0.0.1> aufgerufen. Je nachdem welcher Benutzer angemeldet ist, erscheinen zugehörige Menüpunkte. Alle verwaltungsspezifischen Menüpunkte stehen dem Benutzer ‚global-admin‘ bereit. Lehrer haben Zugriff auf alle pädagogischen Funktionen.

Die Icons haben folgende Bedeutung:


- Menü ein- und ausklappen
- Benutzericon
- angemeldeter Benutzername
- eigenes Passwort ändern
- Abmelden
- Seitenverhältnis skalieren

Das Menü können Sie durch Anklicken der drei Striche links neben dem linuxmuster.net-Symbol ein- und ausblenden.

Hinweis: Bei Namenvergaben, beispielsweise von Kursen oder Projekten, sollte auf Umlaute und ß verzichtet werden.

The screenshot shows the Linuxmuster.net 7! web interface. The top header includes the logo, navigation links like 'Schulkonsole > Hauptseite', and server information 'server.linuxmuster.net'. A left sidebar contains a menu with categories: ALLGEMEIN (Hauptseite, Dashboard, Support), BENUTZERVERWALTUNG (Schüler, Lehrer, Schul-Administratoren, Globale Administratoren, Listenverwaltung), GERÄTEVERWALTUNG (Geräte, LINBO), KLASSENZIMMER (Einschreiben, Passwörter drucken), and EINSTELLUNGEN (Quotas, Schuleinstellungen, Globale Einstellungen). The main content area is titled 'Willkommen zu Linuxmuster.net 7!' and greets the 'Global Admin'. It includes a warning: 'Benutzen Sie die Seitenleiste, um durch die Optionen zu navigieren. Aber denken Sie daran: Aus großer Macht folgt große Verantwortung!'. Below this are three panels: 'Konto Informationen' (Name: Global, Admin; E-Mail: global-admin@linuxmuster.net; Schule: global; Rolle: global-admins; Passwort ändern button), 'Quotas' (linuxmuster-global; 0 MiB / UNBEGRENZT; Cloudquota berechnet in MiB: ---; Mailquota berechnet in MiB: 1 MiB), and 'Gruppen'.

This screenshot is similar to the one above, showing the Linuxmuster.net 7! web interface. The top header and left sidebar are identical. The main content area is titled 'Willkommen zu Linuxmuster.net 7!' and greets the 'Global Admin'. It includes the same warning: 'Benutzen Sie die Seitenleiste, um durch die Optionen zu navigieren. Aber denken Sie daran: Aus großer Macht folgt große Verantwortung!'. Below this are three panels: 'Konto Informationen' (Name: Global, Admin; E-Mail: global-admin@linuxmuster.net; Schule: global; Rolle: global-admins; Passwort ändern button), 'Quotas' (linuxmuster-global; 0 MiB / NO LIMIT; Cloudquota berechnet in MiB: ---; Mailquota berechnet in MiB: 1), and 'Gruppen'.





4.36.2 Allgemein

Hauptseite

Eine Übersicht über Account- & Speicherinformationen des angemeldeten Benutzer. Möglichkeit zur Änderung des eigenen Passworts über Passwort ändern-Funktion.

Dashboard

Übersicht über aktive Serverkomponenten, wie CPU-Auslastung, Speicherauslastung und Laufzeit.

Benutzerverwaltung

Hier können bereits aufgenommene Benutzer in den jeweiligen Bereichen Schüler, Lehrer, Schul-Administratoren verwaltet werden, sowie diese in der Listenverwaltung hinzugefügt/entfernt werden. Im Bereich Globale Administratoren können globale Admins verwaltet und hinzugefügt/entfernt werden.

Schüler, Lehrer, Schul-Administratoren, Globale Administratoren: Funktionen

Suche

In den jeweiligen Benutzer-Bereichen kann in der intelligenten Filterleiste nach Benutzern mit Kriterien wie Namen, Klassen, Projekten gefiltert und gesucht werden.

Passwort-Verwaltung

Zu einzelnen Benutzern gibt es die Möglichkeiten über das Passwort-Menü rechts neben dem jeweiligen Namen.

- Erstpasswort anzeigen
- Erstpasswort wiederherstellen
- Erstpasswort zufällig festlegen
- Erstpasswort benutzerdefiniert festlegen
- Benutzerpasswort festlegen

Durch Auswählen von mehreren Benutzern über Anklicken des Quadrats links neben dem Loginnamen oder über die Funktion **Alle auswählen**, können Funktionen auf mehrere Benutzer gleichzeitig angewendet werden.

- Setze Zufallspasswort für Ausgewählte
- Setze Erstpasswort für Ausgewählte





linuXmuster.net Hauptseite server.linuxmuster.net

ALLGEMEIN
 Hauptseite
 Dashboard
 Support
BENUTZERVERWALTUNG
 Schüler
 Lehrer
 Schul-Administratoren
 Globale Administratoren
 Listenverwaltung
GERÄTEVERWALTUNG
 Geräte
 LINBO
KLASSENZIMMER
 Einschreiben
 Passwörter drucken
EINSTELLUNGEN
 Quotas
 Schuleinstellungen

Willkommen zu Linuxmuster.net 7!

Hallo Global Admin,

Benutzen Sie die Seitenleiste, um durch die Optionen zu navigieren.
Aber denken Sie daran:
Aus großer Macht folgt große Verantwortung!

Konto Informationen
Name: Global Admin
E-Mail: global-admin@linuxmuster.net
Schule: global
Rolle: global-admins
[Passwort ändern](#)

Quotas
linuxmuster-global
0 MiB / NO LIMIT
Cloudquota berechnet in MiB: ...
Mailquota berechnet in MiB: 1

Gruppen

linuXmuster.net Dashboard server.linuxmuster.net

ALLGEMEIN
 Hauptseite
 Dashboard
 Support
BENUTZERVERWALTUNG
 Schüler
 Lehrer
 Schul-Administratoren
 Globale Administratoren
 Listenverwaltung
GERÄTEVERWALTUNG
 Geräte
 LINBO

Home

Hostname
server.linuxmuster.net

Laufzeit
03:17:15

Aktive Kerne
1/4

CPU-Auslastung
0%

Insgesamt
3.9 GB

Speicherauslastung
14%

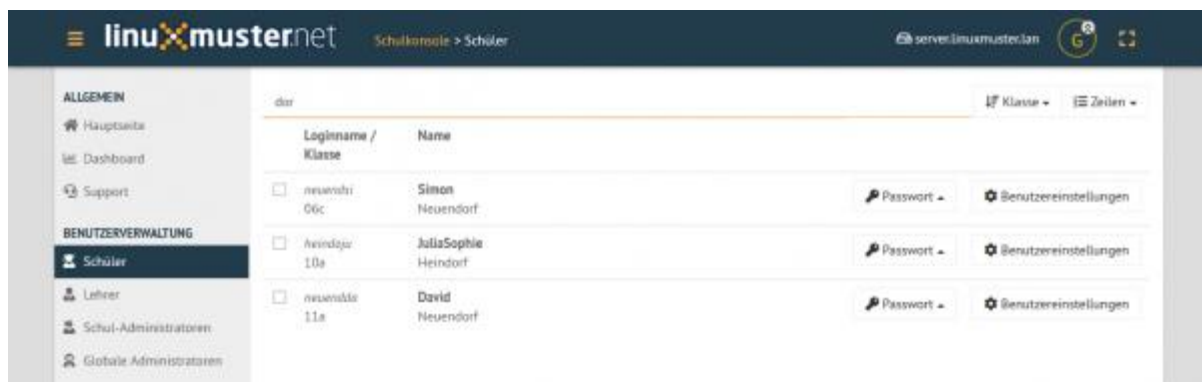
1 Min
0.02

5 Min
0.06

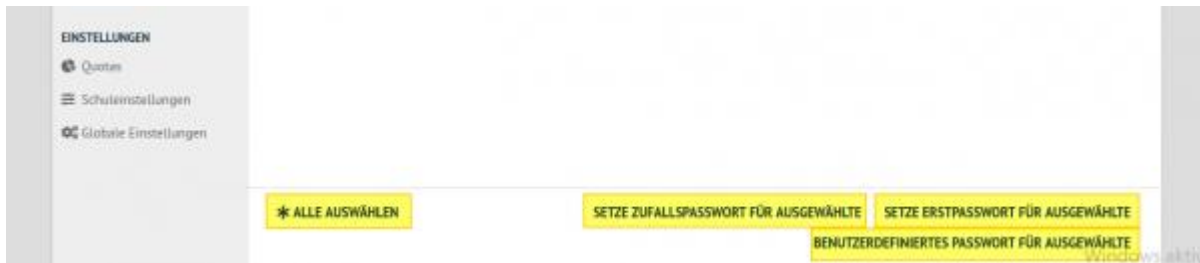
15 Min
0.08

482

Kapitel 4. Weitere Hilfe

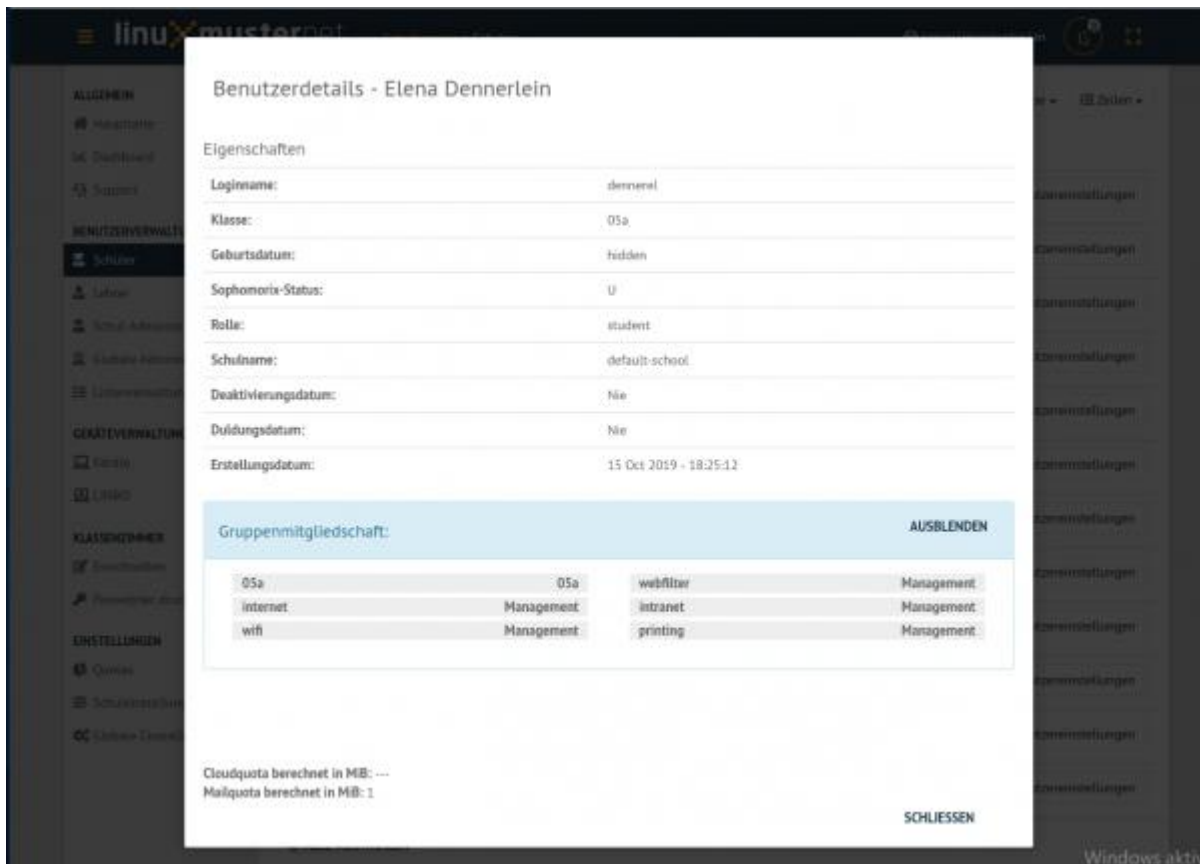


- Benutzerdefiniertes Passwort für Ausgewählte



Informationsübersicht

Über das Benutzereinstellungen-Menü rechts neben der jeweiligen Person können über die Funktion Benutzerinformationen benutzerbezogene Informationen angezeigt, wie Rolle und Gruppenzugehörigkeiten.



Listenverwaltung

In der Listenverwaltung können Benutzer von Schülern, Lehrern, und Extra-Schülern verwaltet werden, das bedeutet hinzugefügt, entfernt oder deren Daten und Zugehörigkeiten geändert werden. Benutzer können manuell über Eingabe von Vorname, Nachname und Geburtsdatum (und ggf. selbstdefinierten Benutzernamen für Lehrer) hinzugeügt werden und einzeln wiederum entfernt werden. Ebenso besteht die Möglichkeit auf schnellerem Wege eine vorhanden CSV-Liste mit Benutzerdaten in die Schulumgebung zu importieren.

Manuelle Benutzeraufnahme

Unter den 3 Bereichen Schüler, Lehrer, Extra Schüler gibt es jeweils unten links der Seite (ggf. runterscrollen) eine hinzufügen-Option drücken.

VKL	Last name	First name	Birthday	
VKL	Pajazitaj	Elvira	21.06.2005	
VKL	Prabakaran	Thilakshi	12.12.2002	
VKL	Salih	Nesaket	19.10.2004	
VKL	Salih	Sibiljam	26.08.2006	
VKL	Teterea	Adrian	10.10.2007	

+ Schüler hinzufügen

First Previous 1 2 3 4 5 **6** Next Last

SPEICHERN SPEICHERN & PRÜFEN IM EDITOR ÖFFNEN CSV LADEN

Drücken Sie dann **Speichern & Prüfen**.

Haben Sie alle Benutzerinformationen eingegeben und ist kein Feld leer, überprüfen Sie die Eingaben mit **Speichern & Überprüfen** in der Prüfergebnis-Ansicht.

Eventuelle Fehler in der Fehleransicht auslesen, die Prüfergebnis-Ansicht abbrechen und die fehlerhaften Daten korrigieren und nochmals mit **Speichern & Überprüfen** testen. Sind keine Fehler aufgetreten, über den Button **Übernehmen** die neuen Benutzer ins System übertragen.

Benutzeraufnahme über vorhandene CSV-Datei

Über die integrierte Funktion, Benutzer simpel über eine CSV-Datei zu übernehmen und anzupassen, können so zahlreiche Benutzer schnell aufgenommen werden. Dafür in einer bestimmten Benutzerliste über die Funktion in der unteren Menüleiste **CSV laden** auswählen und die CSV-Datei hochladen.

Falls die Spalten nicht in der richtigen Reihenfolge aufgelistet sind, gibt es die Möglichkeit diese graphisch per Ziehen mit der Maus umzuordnen, bevor sie mit Sortierung akzeptieren in die Liste übernommen werden.

Falls die Spalten nicht in der richtigen Reihenfolge aufgelistet sind, gibt es die Möglichkeit diese graphisch per Ziehen mit der Maus umzuordnen, bevor sie mit Sortierung akzeptieren in die Liste übernommen werden.

Anschließend **Speichern & Überprüfen** und ganz unten auf der Listenübersicht (gegebenfalls runterscrollen) **Übernehmen**.

linuXmuster.net Schulkontrolle > Listenverwaltung server.linuxmuster.net

VKL	Ilhaev	Said-Ibragim	10.09.2003	
VKL	JavadNiyaSoumehSarpei	SeyedehTina	27.11.2001	
VKL	Javil	Mohamad	01.01.2006	
VKL	Javil	Rasid	01.01.2004	
VKL	Jomaa	Rama	10.01.2006	
VKL	Kalaizidou	Sylliani	16.01.2006	
VKL	Karimi	Normohamad	01.02.2002	
VKL	KhalidAbdulla	Mahmoud	19.07.2006	
VKL	KhalidAbdulla	Sindis	30.09.2002	
VKL	Pajazitaj	Elvira	21.06.2005	
VKL	Prabakaran	Thilakshi	12.12.2002	
VKL	Salih	Nesaket	19.10.2004	
VKL	Salih	Sibijam	26.08.2006	
VKL	Teteroa	Adrian	10.10.2007	
VKL	Teer	Miranda	05.07.2005	
OSa	Pfaus	Vivienne	07.08.2009	
Class	Last name	First name	Birthday	

+ Schüler hinzufügen

First Previous 3 4 5 6 7 8 9 10 11 12 Next Last

SPEICHERN **SPEICHERN & PRÜFEN** IM EDITOR ÖFFNEN CSV LADEN

linuXmuster.net

Prüfergebnis

Übersicht Bericht Hinzufügen

Benutzer werden hinzugefügt: 1

teachers	netzint-teacherin	Netzint-Testteacherin	teacher	default-school
----------	-------------------	-----------------------	---------	----------------

Benutzer werden aktualisiert: 0

Benutzer werden gelöscht: 0

☒ Neue Benutzer hinzufügen

ÜBERNEHMEN ABBRECHEN

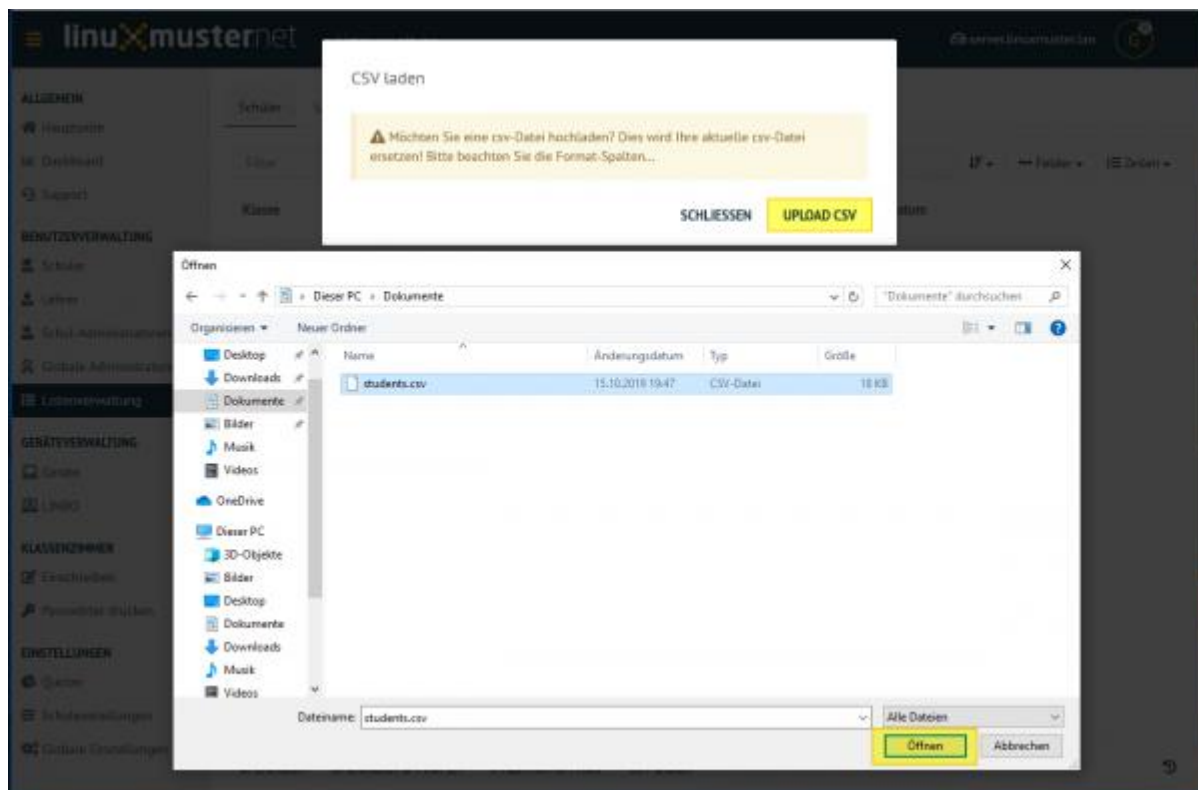
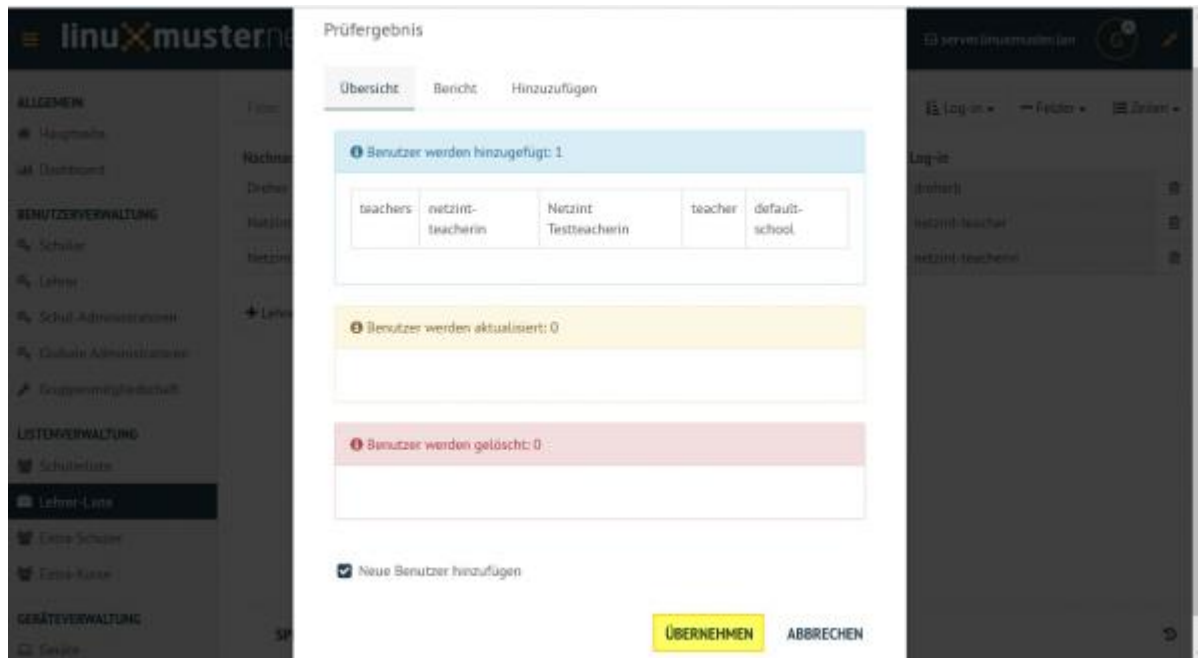
server.linuxmuster.net

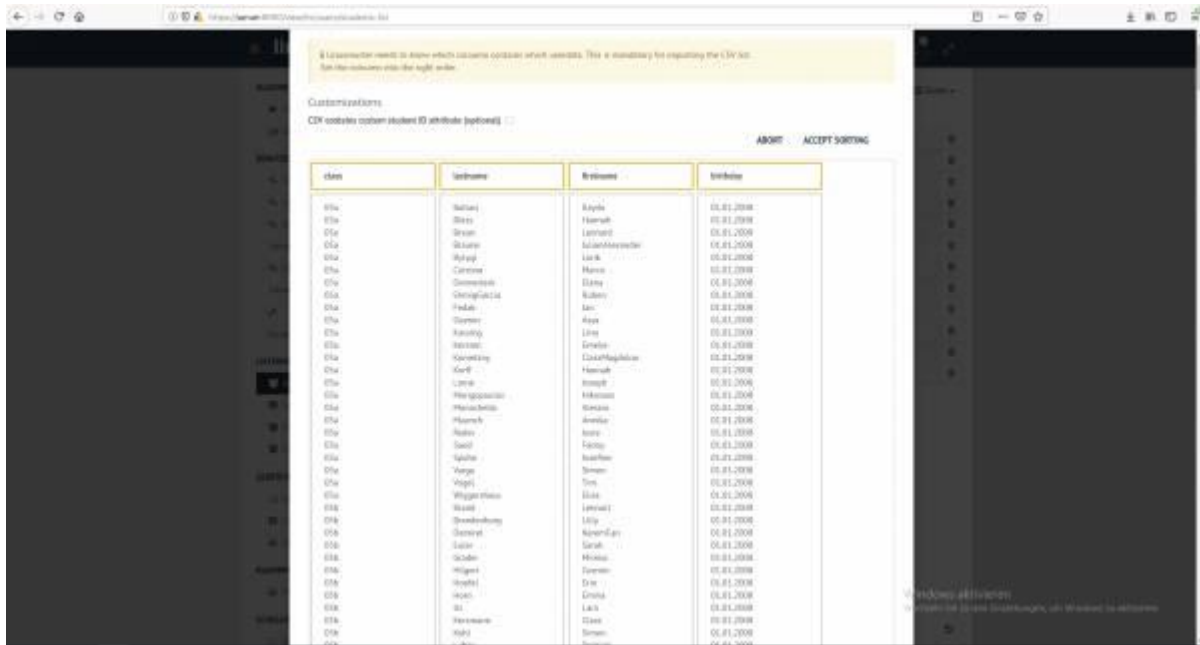
Log-in

Log-in (behalten)

netzint-teacher

netzint-teachern





Benutzer entfernen

Sollen Benutzer entfernt werden, kann dies in der Listenansicht über das Papierkorb-Symbol rechts in der Benutzerzeile gemacht werden. Jeweilige Liste (Schüler-, Lehrer-, Extra-Schüler oder Extra-Kurse) öffnen Benutzer über den Papierkorb aus dessen Zeile entfernen.

- Jeweilige Liste (Schüler-, Lehrer-, Extra-Schüler oder Extra-Kurse) öffnen
- Benutzer über den Papierkorb aus dessen Zeile entfernen



Hinweis: Die Listenänderungen werden erst übernommen, wenn Speichern & Überprüfen erfolgreich ausgeführt wurde. Mögliche unpassende Eingaben oder leere Felder werden rot gekennzeichnet und sollten korrigiert werden, um dann nochmal Speichern & Überprüfen auszuführen.

4.36.3 Geräteverwaltung

In der Geräteverwaltung gibt es unter Geräte eine Übersichtsseite aller angebundenen Geräte inklusiver Informationen und der Möglichkeit diese zu ändern, weitere Geräte hinzuzufügen oder zu entfernen. Weiter finden Sie das LINBO-Menü zu dessen Handhabung Sie die Anleitung LINBO & Domänenintegration verwenden können.



Geräte

Hier ist die graphische Gerätelistenverwaltung implementiert. Geräte können hier aufgenommen, bearbeitet oder entfernt werden. Jedem Gerät müssen die Informationen mitgegeben werden.

- Raum
- Hostname
- Gruppe (Hardwareklasse)
- MAC
- IP (jede IP nur einmal vergeben)
- Sophomorix-Rolle
- PXE (ermöglicht oder deaktiviert Netzwerkboot per LINBO)

Gerät hinzufügen

Über die Funktion Gerät hinzufügen unten links erscheint eine neue Zeile, in welcher die Informationen des neuen Gerätes eingegeben werden sollen.

Die Listenänderungen werden übernommen, wenn **Speichern & Importieren** erfolgreich ausgeführt wurde. Mögliche unpassende Eingaben oder leere Felder werden rot gekennzeichnet und sollten korrigiert werden, um dann nochmal **Speichern & Importieren** auszuführen.

Geräteansicht

- Mit der Filterfunktion in der oberen Leiste kann über Eigenschaften, wie Namen und MAC, nach Geräten gefiltert werden. Rechts gibt es die Möglichkeit die Sortierweise nach Standardspalten, wie Raum und Gruppe, anzupassen.
- Unter Felder können zusätzliche Spalten in der Geräteliste zur Anzeige ausgewählt werden.
- Die Anzahl der pro Seite aufgelisteten Geräte kann unter Zeilen angepasst werden.

linuXmuster.net Geräte server.linuxmuster.net

🔍 Schüler
 🔍 Lehrer
 🔍 Schul-Administratoren
 🔍 Globale Administratoren
 🛠 Gruppenmitgliedschaft

LISTENVERWALTUNG

📋 Schülerliste
 📋 Lehrer-Liste
 📋 Extra-Schüler
 📋 Extra-Kurse

GERÄTEVERWALTUNG

🖨 Geräte
 🖨 LINBO
 🖨 Drucker

KLASSENVERWALTUNG

🖨 Passwörter drucken

SCHULEINSTELLUNGEN

<https://10.0.0.1:8000/view/lin/users/teachers>
 🔍

Id	Gerätename	OS	MAC	IP	Benutzername	Linbo-Profile	Gruppen	Drucker	Linbo-Profile
r001	r001-pc16	win10neu	4C:52:62:0F	10.0.10.16	Schüler-PC im Kl	Linbo-P			
r001	r001-ueflpc	win10efl	BA:F1:DF:7F	10.0.0.200	Schüler-PC im Kl	Linbo-P			
r100	r100-pc01	win1809ausl	06:4C:00:5E	10.0.100.1	Lehrer-PC im Kl	Linbo-P			
r100	r100-pc02	win10TestOri	B6:49:24:8F	10.0.100.2	Schüler-PC im Kl	Linbo-P			
r100	r100-pc03	win10	12:11:34:0E	10.0.100.3	Schüler-PC im Kl	Linbo-P			
r200	r200-pc01	win101809	FA:3F:85:3E	10.0.200.1	Schüler-PC im Kl	Linbo-P			
r200	r200-pc02	win101809	AA:97:A4:8E	10.0.200.2	Schüler-PC im Kl	Linbo-P			
server	server	nopxe	6e:8c:87:8f	10.0.0.1	Server	Kein PXI			
server	firewall	nopxe	00:1A:8C:51	10.0.0.254	Server	Kein PXI			
server	opsi	nopxe	5A:5C:10:D	10.0.0.2	Server	Kein PXI			
server	admin-pc	nopxe	56:C5:D6:A1	10.0.0.9	Server	Kein PXI			
server	service01	nopxe	0A:33:31:E7	10.0.0.7	Server	Kein PXI			
test	test-pc1	win10TestOri	E6:0C:18:2F	10.0.0.201	Schüler-PC im Kl	Linbo-P			
test	test-pc2	win10	EE:F1:A4:EE	10.0.0.202	Schüler-PC im Kl	Linbo-P			
test	test-pc5	win10ausTen	92:82:C1:0E	10.0.0.205	Schüler-PC im Kl	Linbo-P			

+ Gerät hinzufügen

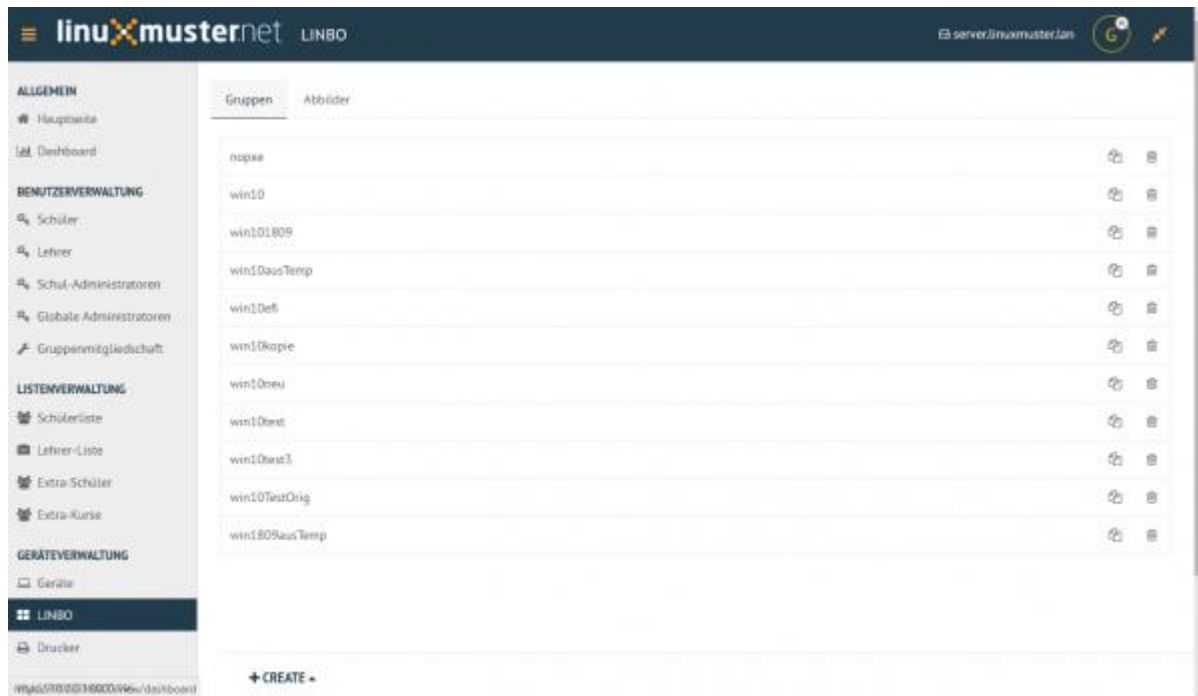
SPEICHERN SPEICHERN & IMPORTIEREN IM EDITOR ÖFFNEN

Filter

📄 Raum ▾ 📄 Felder ▾ 📄 Zeilen ▾

Raum	Hostname	Gruppe	MAC	IP	Sophomox-Rolle	PXE
admin	nb09	nopxe	E4:B9:7A:6C:6D	10.0.0.8	Server	Kein PXI ▾

4.36.4 Linbo



Unter dem Menü Gruppen können die Hardwareklassen bearbeitet werden, welche in der Gerätestenverwaltung den jeweiligen Geräten zugeordnet werden. Im Menü ‚Abbilder‘ werden die enthaltenen Images aufgelistet, welche wiederum einer Hardwareklasse zugeordnet werden können.

4.36.5 Klassenzimmer

Einschreiben

Dieser Abschnitt dient Lehrern oder global-admins dazu sich in Schulklassen, Projekte oder zu Druckern einzuschreiben. Der global-admin ist automatisch zu allen Klassen und Projekte sowie Druckern zugeteilt. Lehrer sollten sich den jeweiligen Klassen zuordnen.

Ein jeweiliges Objekt zum Einschreiben auswählen oder den Haken entfernen um daraus auszutreten. Geänderte Einstellungen werden gelb angezeigt. Um die Änderungen anzuwenden, auf **Übernehmen** klicken.

Passwörter drucken

Hier gibt es die Möglichkeit, eine übersichtliche Liste von Benutzer- & Passwortinformationen per PDF oder CSV-Format ausdrucken zu lassen.

Die kann über Anklicken der jeweiligen Klasse klassenspezifisch, über Klasse: teachers auf alle Lehrer oder über die Option Alle Benutzer auf alle Benutzer der Schule angewendet werden. Als PDF werden die Benutzer neben dem zugehörigen Passwort in Kästchen angezeigt, wie in diesem Beispiel:

Um nicht jedes Kästchen einzeln ausschneiden zu müssen, gibt es vor dem Drucken die Option One per page, um pro Seite nur eine Benutzerinformation auszugeben. Um zu Drucken Ausdrucken wählen.

linuxmuster.net Schulkarte > Einschreiben

server:linuxmuster.lan

Filter Neues Projekt Objektfiler Gruppennamen

Schulklassen

<input checked="" type="checkbox"/> Class 05a	<input checked="" type="checkbox"/> Class 05b	<input checked="" type="checkbox"/> Class 05c	<input checked="" type="checkbox"/> Class 06a
<input checked="" type="checkbox"/> Class 06b	<input checked="" type="checkbox"/> Class 06c	<input checked="" type="checkbox"/> Class 07a	<input checked="" type="checkbox"/> Class 07b
<input checked="" type="checkbox"/> Class 07c	<input checked="" type="checkbox"/> Class 08a	<input checked="" type="checkbox"/> Class 08b	<input checked="" type="checkbox"/> Class 09a
<input checked="" type="checkbox"/> Class 09b	<input checked="" type="checkbox"/> Class 09c	<input checked="" type="checkbox"/> Class 10a	<input checked="" type="checkbox"/> Class 11a
<input checked="" type="checkbox"/> Class 12a	<input checked="" type="checkbox"/> Class vkl		

Drucker

Es sind noch keine Drucker konfiguriert. Bitte Sie Ihren Administrator, einen zu konfigurieren.

Projekte

☒ Project p_fitformathematik

ÜBERNEHMEN

ALLGEMEIN

- Hauptseite
- Dashboard
- Support

BENUTZERVERWALTUNG

- Schüler
- Lehrer
- Schul-Administratoren
- Globale Administratoren
- Listenverwaltung

GERÄTEVERWALTUNG

- Geräte
- LINBO

KLASSENZIMMER

- Einschreiben

linuxmuster.net Schulkarte > Passwörter drucken

server:linuxmuster.lan

Alle Benutzer

Klasse: 05a
Klasse: 05b
Klasse: 05c
Klasse: 06a
Klasse: 06b
Klasse: 06c
Klasse: 07a
Klasse: 07b
Klasse: 07c
Klasse: 08a
Klasse: 08b
Klasse: 09a
Klasse: 09b
Klasse: 09c

ALLGEMEIN

- Hauptseite
- Dashboard
- Support

BENUTZERVERWALTUNG

- Schüler
- Lehrer
- Schul-Administratoren
- Globale Administratoren
- Listenverwaltung

GERÄTEVERWALTUNG

- Geräte
- LINBO

KLASSENZIMMER

- Einschreiben
- Passwörter drucken

EINSTELLUNGEN

Zugangsdatenliste		10a	29. April 2019
Fray, Katrin Klasse: 10a Passwort: vdK4YciLx(Login: frayka	Gengler, Felix Klasse: 10a Passwort: ==7NjUcYnm Login: genglefe	Ilkes, Judith Klasse: 10a Passwort: (KA)P=KVb9 Login: ilkesju	Imbrogiana, Henriette Klasse: 10a Passwort: BMg&vMV!b3 Login: imbroghe
Krüger, Richard Klasse: 10a Passwort: p(wRkebK)9 Login: kruegeri	_____	_____	_____

4.36.6 Einstellungen

Quotas

Unter Standardwerte werden standarmäßige Speichergrößen von Standardquota, Cloudquota und Mailquota für Schüler, Lehrer und Schuladministratoren festgelegt.

linuxmuster.net Schulkonsole > Quotas server.linuxmuster.lan

ALLGEMEIN

- Hauptseite
- Dashboard
- Support

BENUTZERVERWALTUNG

- Schüler
- Lehrer
- Schul-Administratoren
- Globale Administratoren
- Listenverwaltung

GERÄTEVERWALTUNG

- Geräte
- LINBO

KLASSENZIMMER

- Einschreiben
- Passwörter drucken

EINSTELLUNGEN

- Quotas**
- Schuleinstellungen
- Globale Einstellungen

Standardwerte Lehrer Schüler Klassen Projekte Spezielle

	Schüler	Lehrer	Schuladministrator
Standardquota (global) in MiB	1006	2006	3006
Standardquota (Schule) in MiB	1506	2506	3506
Cloudquota in Prozent	100	100	100
Mailquota Standard in MiB	156	306	506

Quota ist derzeit in ldap gesetzt
Quota ist derzeit nicht in ldap gesetzt

In den Bereichen **Lehrer** und **Schüler** daneben können von den Standwartwerten abweichend pro Benutzer eigene Werte eingestellt werden. Ebenso kann unter **Klassen** und **Projekte** einer jeweiligen Schulklasse/einem jeweiligen Projekt die Speichergröße festgelegt werden.

4.36.7 Schuleinstellungen

Allgemeine Informationen, Einstellungen zum Listenimport, Quotalimits und Druck-Daten-Werte können in der Schuleinstellungen verwaltet werden.

Unter Allgemein werden generelle Schuleinstellungen wie Namen oder E-Mail-Domänen für jeweilige Rollen angegeben und geändert.

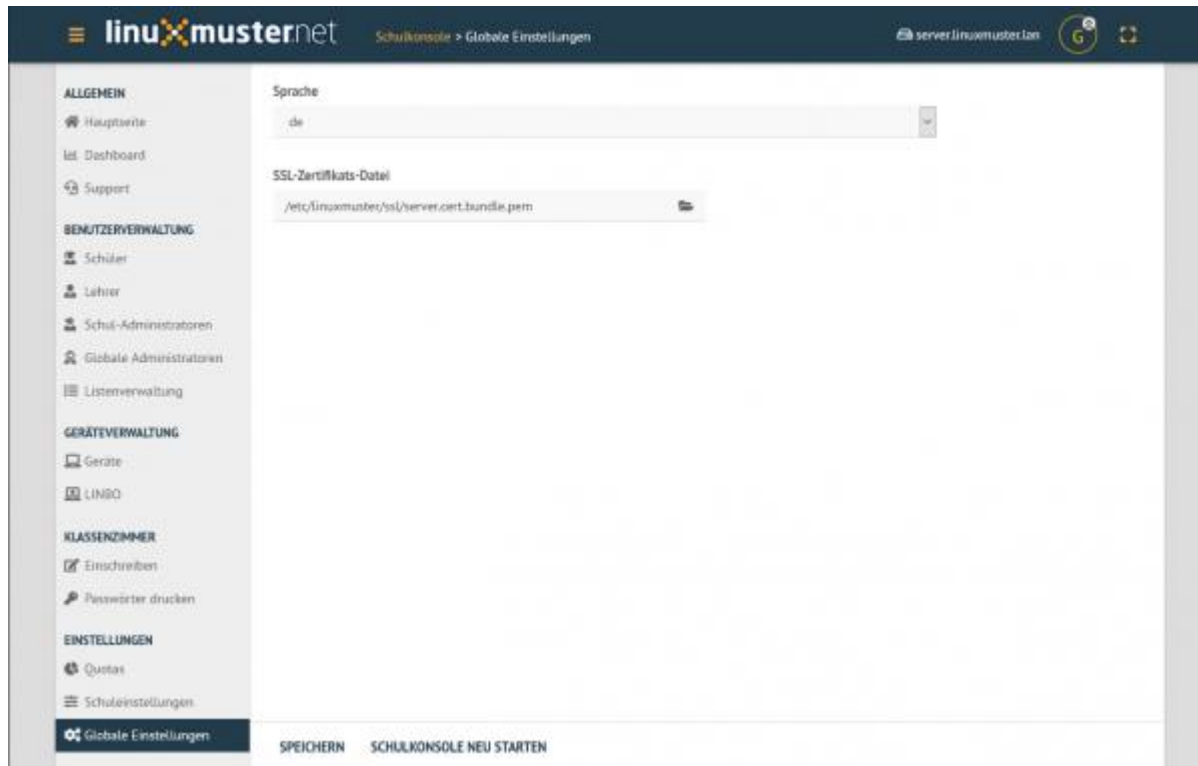
Änderungen über Speichern & Prüfen und anschließend Übernehmen anwenden. Unter Listenimport können Standardwerte festgelegt werden, die beim Import einer CSV-Datei angewendet werden. Wird ein Haken unter der Funktion Nachname und Vorname im Benutzernamen umkehren für eine jeweilige Rolle, werden die Benutzernamen zuerst aus dem Vornamen und dann aus Nachnamen generiert. Wie viele Zeichen aus den jeweiligen Namen genommen werden, wird in den unteren Werten Nachname Zeichen und Vornamen Zeichen angegeben. Ältere Sicherungen könne über das Symbol



unten rechts wiederhergestellt werden.

4.36.8 Globale Einstellungen

In diesem Bereich werden die globalen Einstellungen für die Schulkonsole der linuxmuster-Umgebung verwaltet, welche aber in der Regel nie geändert werden müssen.



Zu den globalen Einstellungen gehören die für die Schulkonsole Sprache, welche unter Sprache geändert werden kann. Auch die Zertifikatsdatei könnte hier unter SSL-Zertifikats-Datei geändert werden. Um die Änderungen wirksam zu machen, muss die Schulkonsole über `Schulkonsole neu starten` neu gestartet und initialisiert werden.

4.37 Nutzung der Remote Server Administration Tools zum Anpassen der GPO

Autor des Abschnitts: @michael_kohls

Das Anpassen der vom SAMBA-Server bereitgestellten GPO erfolgt von einem Windows-PC aus.

4.37.1 Installation der RSAT (Remote Server Administration Tools)

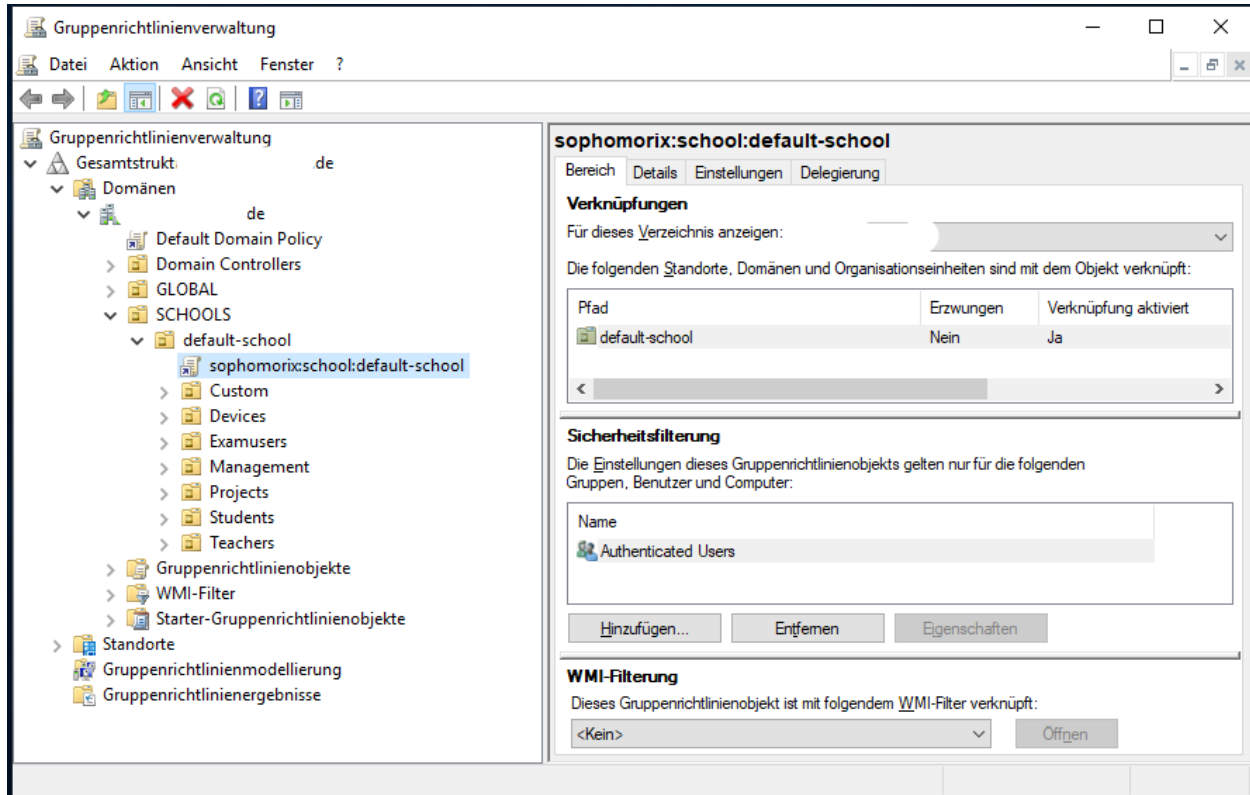
Zur Verwaltung des Active Directory (AD) benötigt man die Microsoft Remote Server Administration Tools (RSAT). Diese werden von Microsoft bereitgestellt. (Home-Versionen von Windows werden nicht unterstützt!)

Für Windows 10-Versionen vor 1809 müssen diese noch als separates Installationspaket heruntergeladen werden: <https://www.microsoft.com/en-us/download/details.aspx?id=45520>

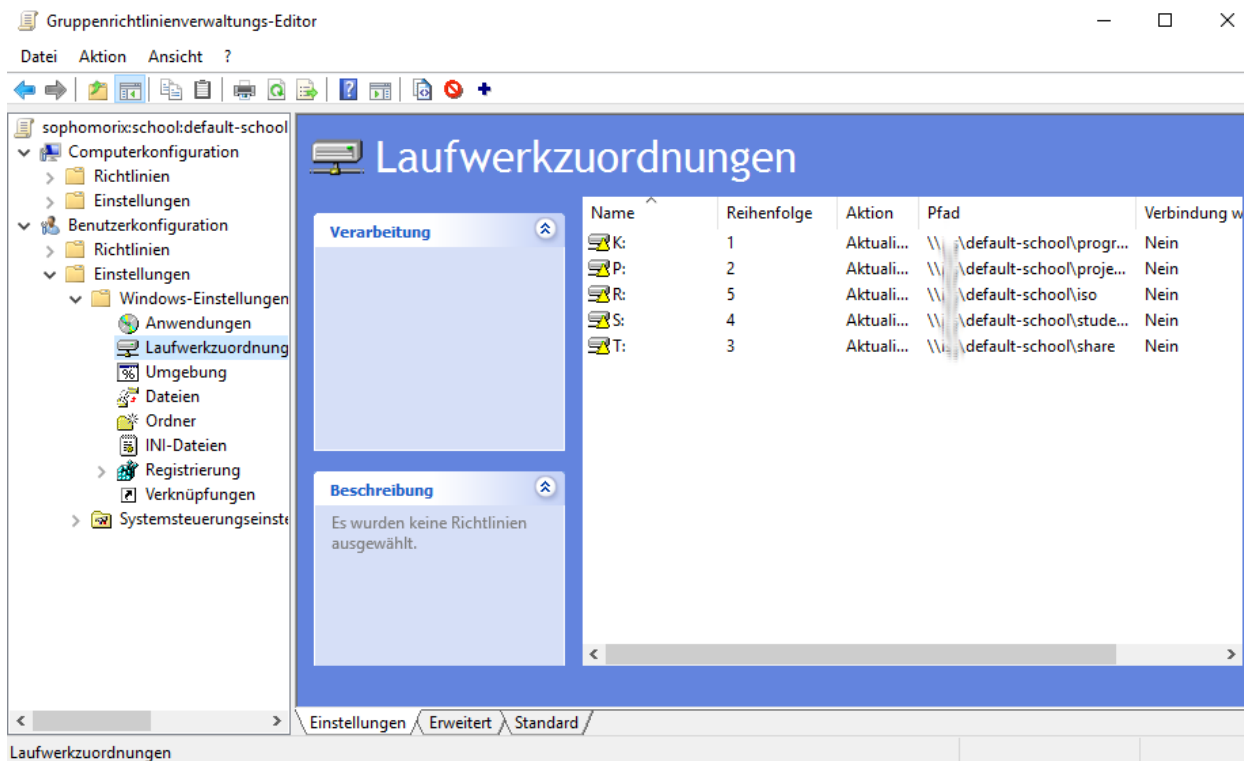
Ab Version 1809 sind die RSAT ein optionales Feature. Die Installation erfolgt über Start -> Apps und Features -> optionale Features -> Feature hinzufügen -> RSAT: Group Policy Management Tools.

4.37.2 Verwendung der Gruppenrichtlinienverwaltung

Falls noch nicht geschehen, melde Dich mit einem Domänenbenutzerkonto, welches zur Gruppe der Administratoren gehört, am Computer an. Zum Beispiel als global-admin. Starte die Gruppenrichtlinienverwaltung durch Eingabe von `gpmc.mmc`. Bei Windows ab Version 1809 starte die App Gruppenrichtlinienverwaltung.



Mittels Rechtsklick auf `sophomorix:school:default-school` und Bearbeiten öffnet sich der Gruppenrichtlinienverwaltungs-Editor:

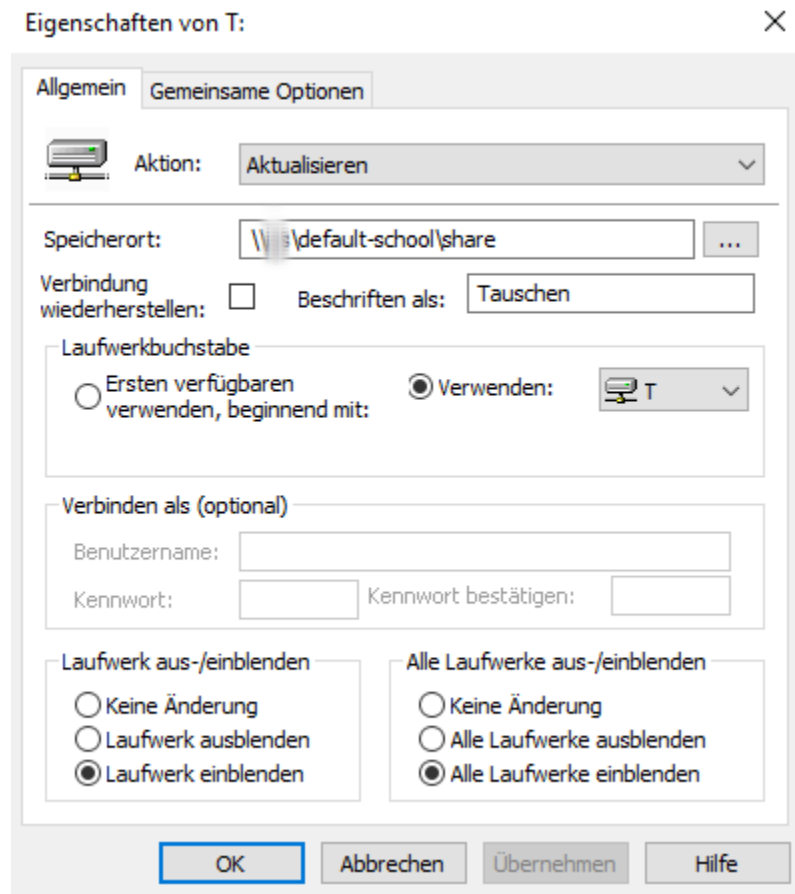


Hinweis: Sollte die Standard-GPO „sophomrix:school:default-school“ nicht vorhanden sein, dann kann diese auf dem Server erzeugt werden durch Eingabe von: `sophomrix-school --gpo-create default-school`.

Im Gruppenrichtlinienverwaltungs-Editor können nun Anpassungen der GPO vorgenommen werden:

4.37.3 Beispiel für Änderung der Laufwerksbeschriftung

Die Netzlaufwerke unter Windows werden mit Ausnahme des Homelaufwerks per GPO eingebunden. Wenn z.B. die Beschriftung deutsch statt englisch sein soll oder der Laufwerkbuchstabe geändert werden soll kann das unter Benutzerkonfiguration -> Einstellungen -> Laufwerkszuordnungen geändert werden:



4.38 Softwareinstallation via GPO

Autor des Abschnitts: @michael_kohls

Voraussetzung: Windows-PC mit installierten RSAT-Tools. Siehe: <https://docs.linuxmuster.net/de/latest/systemadministration/gpo/gpo.html#installation-der-rsat-remote-server-administration-tools>

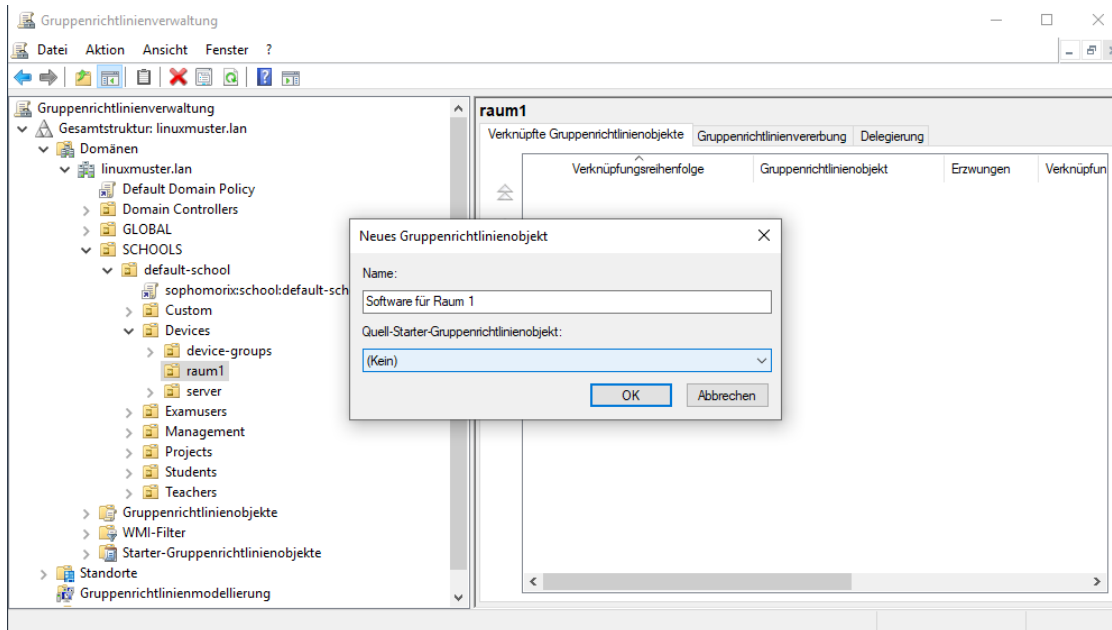
Über GPOs können drei Arten von Paketen installiert werden: Windows-Installationspakete mit der Dateierdung .MSI, Transformationsdateien mit der Dateierdung .MST und Patch-Dateien, die auf .MSP enden.

Software kann an Computer oder User verteilt werden. In diesem Beispiel erfolgt die Verteilung an die Computer in einem bestimmten Raum.

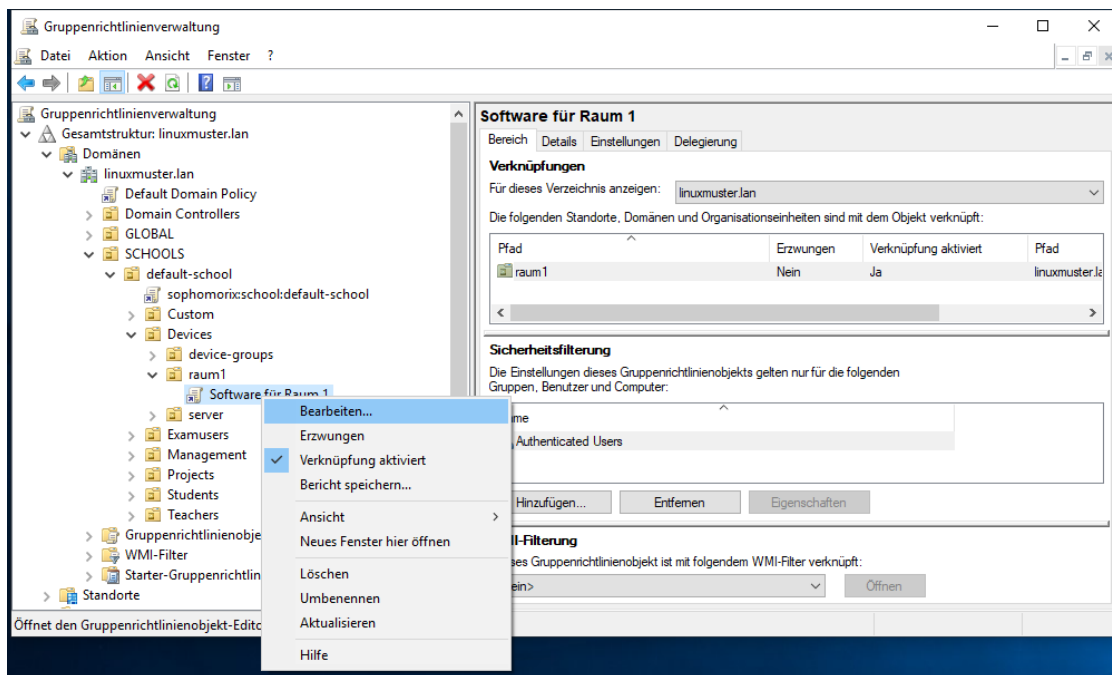
Zunächst sollte die Software auf einem UNC-Pfad abgelegt werden, von dem aus die Installation ausgeführt werden kann. Das Server-Share \\server\default-school\program ist ungeeignet. Besser: \\server\sysvol\domänenname\. Hier einen Unterordner Software erstellen und die MSI-Pakete ablegen.

4.38.1 Neue GPO erzeugen

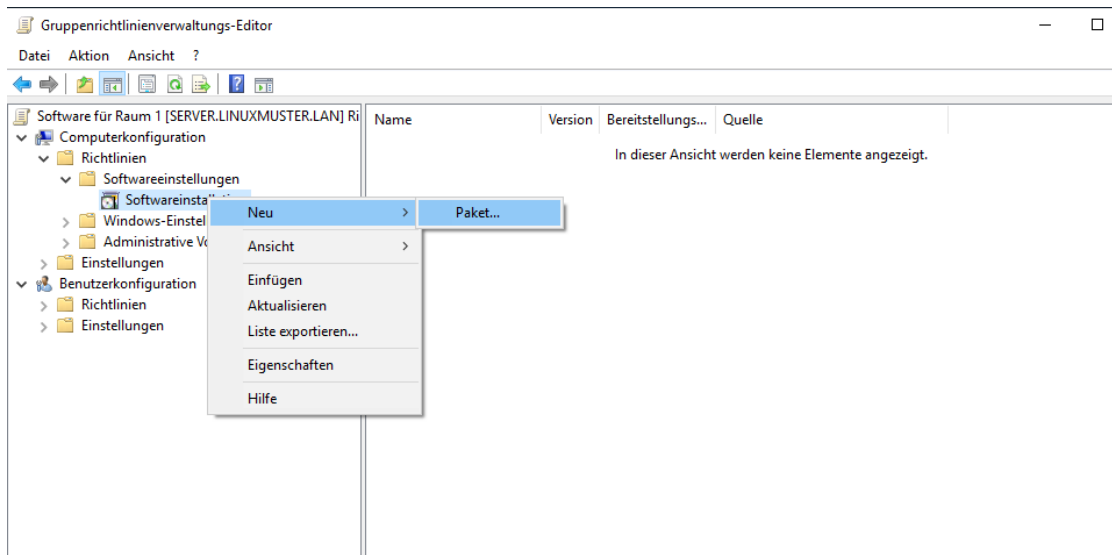
Melde Dich an einem PC mit global-admin an und starte die Gruppenrichtlinienverwaltung. Klappe den Baum auf bis zum gewünschten Raum. Mache einen Rechtsklick auf den gewünschten Raum und wähle Gruppenrichtlinienobjekt hier erstellen und verknüpfen. Im folgenden Fenster einen sinnvollen Namen vergeben (z.B. Software für Raum X) und mit OK bestätigen.



Nun muss die neue GPO noch bearbeitet werden. Mache dazu einen Rechtsklick darauf und wähle Bearbeiten.



Der Gruppenrichtlinienverwaltungs-Editor öffnet sich. Gehe zu: Computerkonfiguration -> Richtlinien -> Softwareeinstellungen -> Softwareinstallation



Mache einen Rechtsklick auf Softwareinstallation und wähle Neu -> Paket. Gib den UNC-Pfad zum Paket ein. Wichtig: Das Paket muss an einer Stelle liegen, auf die der Ziel-Computer Zugriff hat! Darauf weist der folgende Dialog auch nochmals hin.

Bei der Bereitstellungsmethode Zugewiesen auswählen und mit Okay bestätigen.

Damit die neue GPO am Ziel-PC greift, muss dieser neu gestartet werden.

4.38.2 bekannte Probleme:

- 1) Hibernate / Fastboot nicht deaktiviert
- 2) Die GPO wird nicht übernommen, weil die Verbindung zu schnell ist. In diesem Fall auf dem Ziel-PC mittels gpedit.msc die lokale GPO aktivieren: Computerkonfiguration\Administrative Vorlagen\System\Anmelden - Beim Neustarten des Computers und bei der Anmeldung immer auf das Netzwerk warten.

4.38.3 Software erneut verteilen

Wurde die Software absichtlich oder unabsichtlich mit einem lokalen Administrator auf dem Ziel-PC gelöscht, muss das Paket neu verteilt werden. Dazu im Gruppenrichtlinienverwaltungs-Editor unter Computerkonfiguration -> Richtlinien-> Softwareeinstellungen-> Softwareinstallation einen Rechtsklick auf die Software machen und Alle Aufgaben -> Entfernen wählen. Anschließend das Paket wieder neu hinzufügen.

4.39 OpenVPN konfigurieren

Autor des Abschnitts: @dorian, Ergänzungen @cweikl

Um Schülern und Lehrern die Möglichkeit zu geben, sich via VPN in das Schulnetz „einzuwählen“, beschreibt diese Dokumentation die Einrichtung des OpenVPN-Dienstes auf der Firewall OPNsense®. Sowie die Anmeldung via LDAP über den linuxmuster Server.

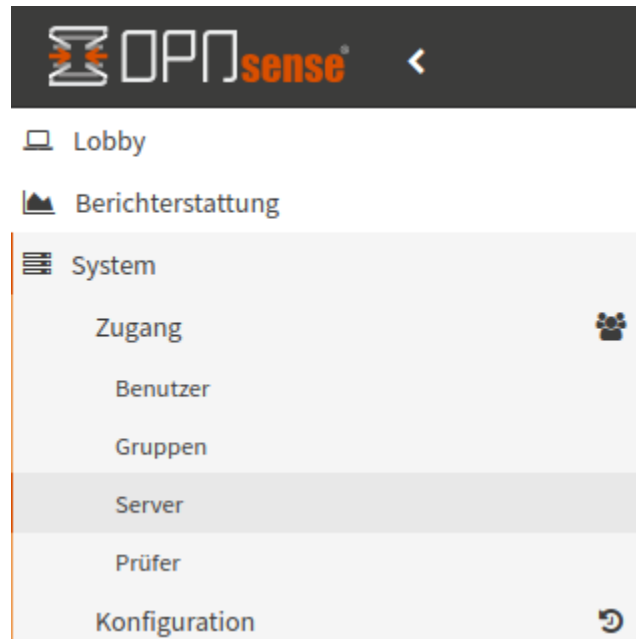
4.39.1 Voraussetzungen

Die Firewall OPNsense® wurde erfolgreich in Verbindung mit dem linuxmuster.net Server (v7) eingerichtet. Sofern „vor“ der OPNsense® ein Router zur Verwaltung der externen Verbindung eingesetzt wird, muss dieser ein Port - Forwarding ermöglichen, der Anfragen auf dem für VPN genutzten Port (z.B. 1194) auf die externe Schnittstelle der OPNsense® ermöglicht. Zudem muss die OPNsense® aus dem externen Netz via URL (DynDNS oder eigene Domain) erreichbar sein.

4.39.2 LDAP-Anbindung

Melde Dich an der GUI der OPNsense® als Benutzer root an.

Wähle links im Menü unter dem Eintrag System → Zugang → Server , um einen neuen Server-Eintrag für die LDAP-Authentifizierung hinzuzufügen.



Um die LDAP-Anbindung auf der OPNsense® für Schüler und Lehrer einzurichten, durchläufst Du folgende Schritte:

Server hinzufügen

Unter System → Zugang → Server einen Server hinzufügen (oben rechts). Es sind folgende Einträge vorzunehmen:

1. Beschreibender Name: Linuxmuster VPN Zugang
2. Typ: LDAP
3. Hostname oder IP-Adresse: server.linuxmuster.lan
4. Port-Wert: 636
5. Transport: SSL - Verschlüsselt
6. Protokollversion: 3
7. Bind-Zugangsdaten:

Benutzer DN: CN=**global**-binduser,OU=Management,OU=GLOBAL,DC=linuxmuster,DC=lan
Suchbereich: Kompletter Unterbaum

DC-Werte wie unter 8. auf den eigenen Bind anpassen.

8. Basis-DN: DC=linuxmuster,DC=lan
9. Authentifizierungscontainer: DC=linuxmuster,DC=lan

DC-Werte wie unter 8. auf den eigenen Bind anpassen.

Nachstehende Abb. verdeutlicht die Anwendung der o.g. Einstellungen:

System: Zugang: Server

i Beschreibender Name	<input type="text" value="Linuxmuster VPN Zugang"/>	
i Typ	<input type="text" value="LDAP"/>	
i Hostname oder IP-Adresse	<input type="text" value="server.linuxmuster.lan"/>	
i Port-Wert	<input type="text" value="636"/>	
i Transport	<input type="text" value="TCP - Standard"/>	
i Protokollversion	<input type="text" value="3"/>	
i Bind Zugangsdaten	Benutzer DN: <input type="text" value="CN=global-binduser,OU=Management,OU=GLOBAL, ..."/> Passwort: <input type="password" value="*****"/>	
i Suchbereich	<input type="text" value="Kompletter Unterbaum"/>	
i Basis DN	<input type="text" value="DC=linuxmuster,DC=lan"/>	
i Authentifizierungscontainer	<input type="text" value="DC=linuxmuster,DC=lan"/>	<input type="button" value="Auswählen"/>

10. Erweiterte Abfrage: Schüler und Lehrer:

```
(memberof=CN=role-student,OU=Groups,OU=GLOBAL,DC=linuxmuster,DC=lan)(memberof=CN=role-teacher,OU=Groups,OU=GLOBAL,DC=linuxmuster,DC=lan)
```








O D E R

Erweiterte Abfrage: Nur Lehrer:

```
(memberof=CN=role-teacher,OU=Groups,OU=GLOBAL,DC=linuxmuster,DC=lan)
```

11. Benutzerbenennungsattribut: sAMAccountName

Nachstehende Abb. verdeutlicht die Anwendung der o.g. Einstellungen:

 Erweiterte Abfrage	<input type="text" value=" (memberof=CN=role-student,OU=Groups,OU=GLOB ..."/>
 Initiale Vorlage	<input type="text" value="Microsoft AD"/>
 Benutzerbenennungsattribut	<input type="text" value="sAMAccountName"/>
 Read properties	<input type="checkbox"/>
 Synchronize groups	<input type="checkbox"/>
 Limit groups	<input type="text" value="Nothing selected"/>
 Match case insensitive	<input type="checkbox"/>
<input type="button" value="Speichern"/>	

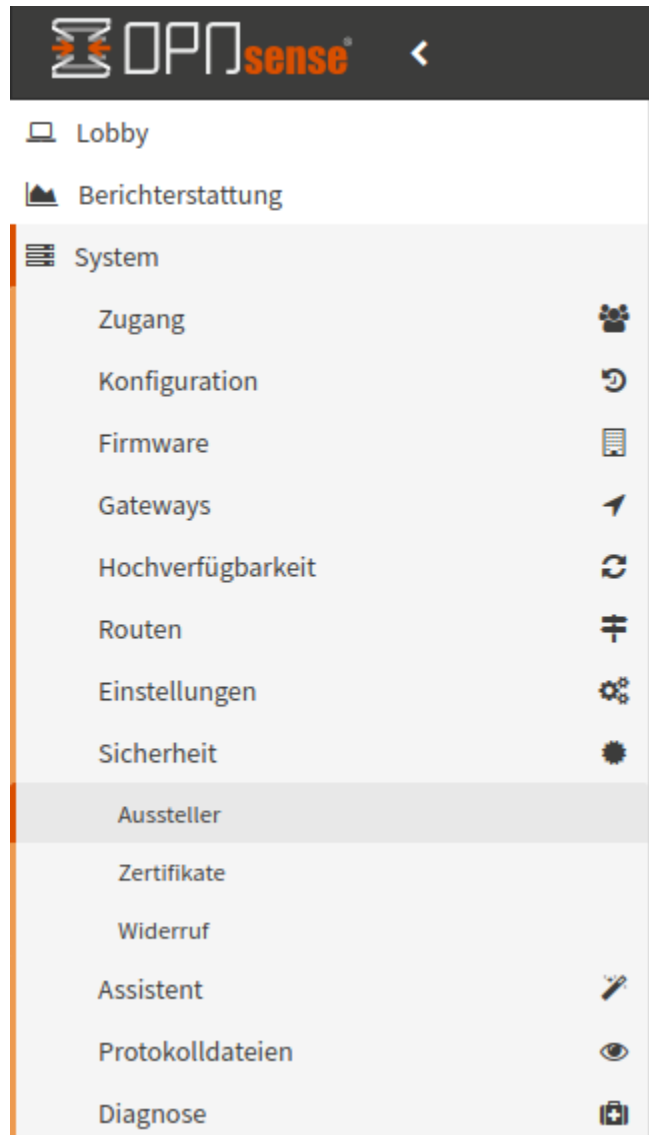
Danach sollte der Login mit beliebigen Nutzern getestet werden. Erst nachdem die Tests erfolgreich waren fortfahren. Dies kann unter System > Zugang > Prüfer und der Auswahl des vorhin angelegten Authentifizierungsservers für den Linuxmuster VPN-Zugang erfolgen.

4.39.3 Zertifikate erstellen

Der OpenVPN Server braucht eine CA, um das Serverzertifikat zu erstellen. Man kann entweder eine neue CA generieren, oder die vom linuxmuster Setup erzeugte CA verwenden. In dieser Dokumentation wird die Erstellung einer neuen CA dargestellt, die nur für das VPN verwendet werden soll.

CA erstellen

Unter System → Zugang → Sicherheit → Aussteller



ist ein Aussteller hinzuzufügen (oben rechts). Es sind folgende Einstellungen vorzunehmen:

1. Beschreibender Name: `Linuxmuster VPN CA` <eigener Name>
2. Vorgehen: Erstelle eine interne Zertifizierungsstelle
3. Key Type: RSA
4. Schlüssellänge: 4096
5. Hash-Algorithmus: SHA512
6. Lebenszeit (Tage): <frei wählbar>

System: Sicherheit: Aussteller

Beschreibender Name	Linuxmuster VPN CA
Vorgehen	Erstelle eine interne Zertifizierungsstelle ▼
Interne Zertifizierungsstelle	
Key Type	RSA ▼
Schlüssellänge (Bits)	4096 ▼
Hashalgorithmus	SHA256 ▼
Lebenszeit (Tage)	1095
Bedeutender Name	
Ländercode :	DE (Germany) ▲

7. Bedeutender Name: <dein bedeutender Name für die CA>

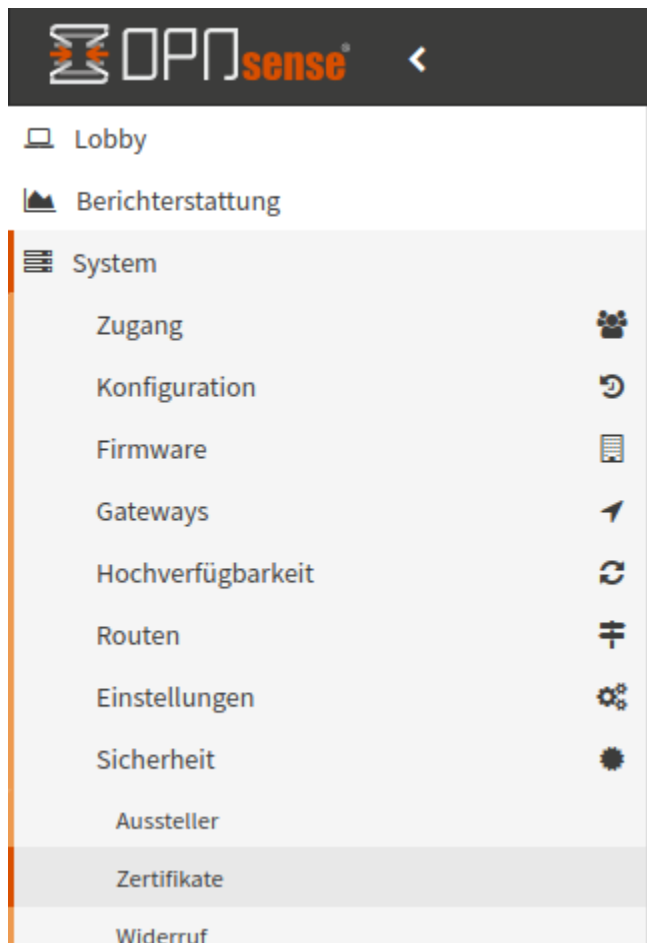
Die erstellte CA findet sich unter System → Zugang → Sicherheit → Aussteller wie in nachstehender Abb. dargestellt:

System: Sicherheit: Aussteller

Name	Intern	Herausgeber	Zertifikate
linuxmuster	NEIN	<i>selbstsigniert</i>	1
Linuxmuster VPN CA FLB	JA	<i>selbstsigniert</i>	0

Zertifikat hinzufügen

Danach ist unter System → Sicherheit → Zertifikate ein Zertifikat hinzuzufügen (oben rechts).



Folgende Eingaben sind zu treffen:

1. Vorgehen: Erstelle ein neues internes Zertifikat
2. Beschreibender Name: Linuxmuster VPN Server
3. Zertifizierungsstelle: Linuxmuster VPN CA
4. Type: Serverzertifikate
5. Key Type: RSA
6. Schlüssellänge: 4096
7. Hash-Algorithmus: SHA512
8. Lebenszeit (Tage): frei wählbar!
9. Private Key Location: Save on this firewall
10. Bedeutender Name: <dein bedeutender Name für das Zertifikat>

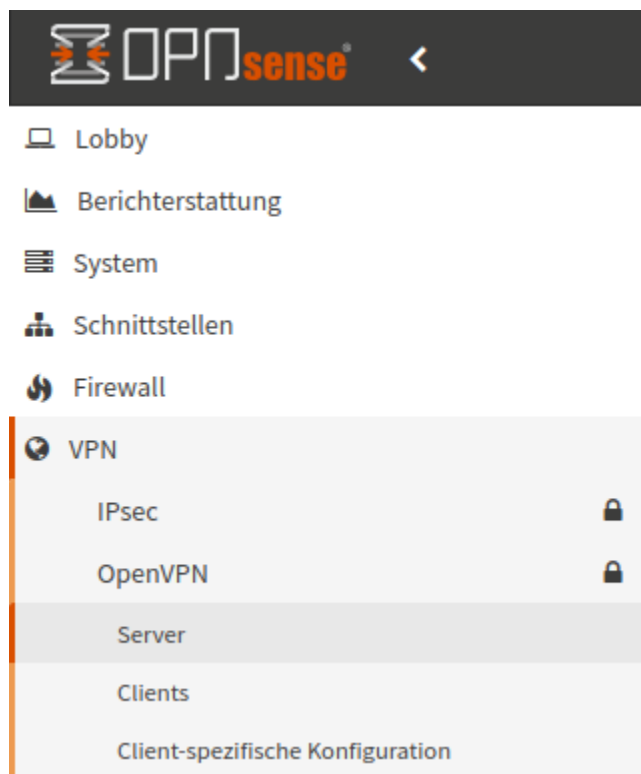
Folgende Abb. gibt diese Einstellungen wieder:

System: Sicherheit: Zertifikate

Vorgehen	Erstelle ein neues internes Zertifikat ▼
Beschreibender Name	Linuxmuster VPN Server
Interne Zertifikate	
Zertifizierungsstelle	Linuxmuster VPN CA FLB ▼
Typ	Serverzertifikate ▼
Key Type	RSA ▼
Schlüssellänge (Bits)	4096 ▼
Hashalgorithmus	SHA256 ▼
Lebenszeit (Tage)	1095
Private key location	Save on this firewall ▼
Bedeutender Name	
Ländercode :	DE (Germany) ▲

4.39.4 OpenVPN-Server erstellen

Unter VPN → OpenVPN → Server ist ein OpenVPN-Server zu erstellen (oben rechts).



Es sind folgende Eingaben sind zu treffen:

1. Beschreibender Name: Linuxmuster VPN
2. Servermodus: Remotezugriff (Benutzerauthentifizierung)
3. Backend Authentifizierung: Linuxmuster VPN Zugang
4. Lokale Gruppe erzwingen (keiner)
5. Protokoll: UDP
6. Gerätemodus: tun
7. Schnittstelle: WAN
8. Lokaler Port: (frei wählbar) 25008
9. TLS Authentifikation: Beides angehakt lassen
10. Peer-Zertifizierungsstelle: Linuxmuster VPN CA
11. Peerzertifikatsrückrufliste: Keine
12. Serverzertifikate: Linuxmuster VPN Server

Nachstehende Abb. verdeutlicht diese Einstellungen:

VPN: OpenVPN: Server

Allgemeine Information	
Deaktiviert	<input type="checkbox"/>
Beschreibung	Linuxmuster VPN FLB
Servermodus	Remotezugriff (Benutzerauthentifizierung)
Backend Authentifizierung	Linuxmuster VPN Zugang
Lokale Gruppe erzwingen	(keiner)
Protokoll	UDP
Gerätemodus	tun
Schnittstelle	WAN
Lokaler Port	1194
Kryptografische Einstellungen	
TLS Authentifikation	<input checked="" type="checkbox"/> Authentifizierung von TLS Paketen aktivieren. <input checked="" type="checkbox"/> Automatisch gemeinsamen Authentifizierungsschlüssel generieren.
Peer-Zertifizierungsstelle	Linuxmuster VPN CA FLB
Peerzertifikatsrückrufliste	None

13. DH Parameterlänge: 4096
14. Verschlüsselungsalgorithmus: AES-256-CBC (256-bit key, 128-bit block)
15. Authentifizierungs-Digestalgorithmus: SHA512 (512-bit)
16. Hardwarekryptografie: No Hardware Crypto Acceleration
17. Zertifikatstiefe: Eins (Client+Server)

i Serverzertifikate	Linuxmuster VPN Server (Linuxmuster VPN CA FLB) ▲
i DH Parameterlänge	4096 bit ▼
i Verschlüsselungsalgorithmus	AES-256-CBC (256 bit key, 128 bit block) ▲
i Authentifizierungs-Digestalgorithmus	SHA512 (512-bit) ▼
i Hardwarekryptografie	No Hardware Crypto Acceleration ▲
i Zertifikatstiefe	Eins (Client + Server) ▲

18. IPv4 Tunnelnetzwerk: Ein Netzbereich in dem die VPN Clients ihre IP bekommen z.B. 172.30.1.0/24 oder 192.168.100.0/24
19. IPv6 Tunnelnetzwerk:
20. Weiterleitungs Gateway:
21. Lokales IPv4-Netzwerk: 10.0.0.0/16 -> hier ist das beim Setup gewählte linuxmuster-Netz anzugeben
22. Lokales IPv6-Netzwerk:
23. Fernes IPv4-Netzwerk:
24. Fernes IPv6-Netzwerk:
25. Konkurrierende Verbindungen:
26. Komprimierung: Aktiviert mit adaptiver Kompression

i Komprimierung	Legacy - Enabled LZO algorithm with adaptive compri ▲
------------------------	---

27. Typ des Dienstes:
28. Inter-Client-Kommunikation:
29. Doppelte Verbindungen:
30. IPv6 deaktivieren:
31. Für den Rest: Standardwerte!

Hast Du den VPN-Server erfolgreich hinzugefügt, so wird dieser in der Übersicht angezeigt. Siehst Du vor der Angabe des Protokolls ein grünes Dreieck, dann läuft der VPN-Server.

VPN: OpenVPN: Server

Protokoll / Port	Tunnel Netzwerk	Beschreibung
▶ UDP / 1194	172.30.1.0/24	Linuxmuster VPN FLB

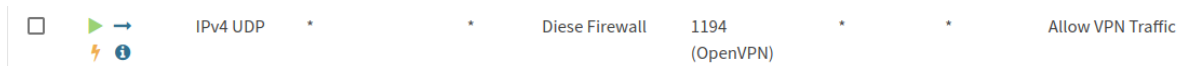
4.39.5 Firewall Regeln

Es müssen nun Regeln definiert werden, die die VPN-Anfragen an die Firewall weitergeben und nach erfolgreicher Authentifizierung den VPN-Datenverkehr zulassen.

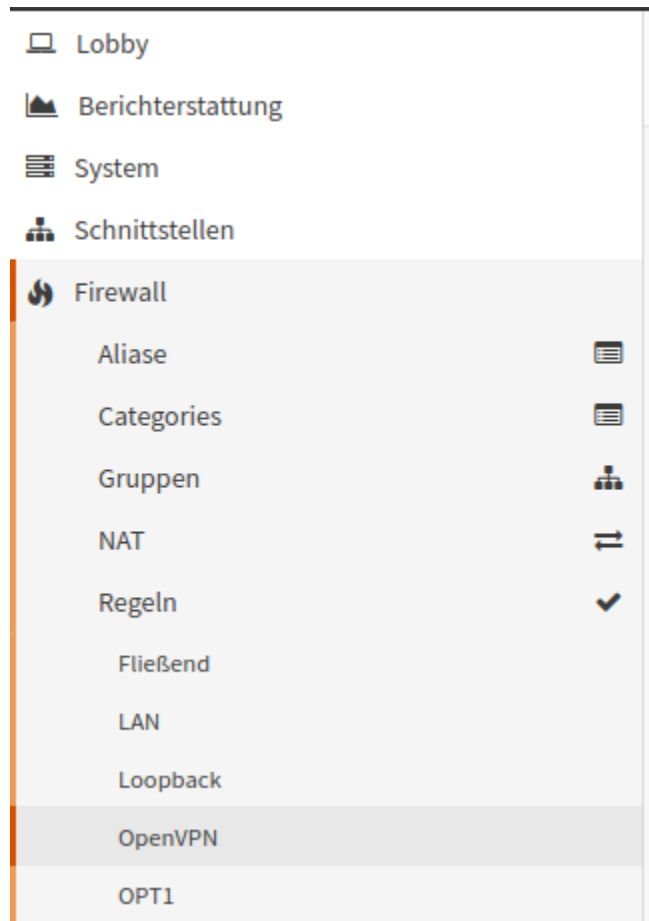
Unter Firewall → Regeln → WAN eine neue Regel anlegen (oben rechts). Folgende Eingaben sind zu treffen:

1. Protokoll: UDP
2. Ziel: Diese Firewall
3. Zielportbereich: von: 25008 bis: 25008 (ggf. anpassen an eigene Portwahl -> in der Abb. 1194)
4. Für den Rest: <Standardwerte>

In der Regelansicht stellt sich diese wie folgt dar:



Danach unter Firewall → Regeln → OpenVPN eine neue Regel anlegen (oben rechts). Hier findet sich jetzt nach der Anlage des VPN-Servers eine neuer Menüeintrag für OpenVPN:



Es sind folgende Eingaben vorzunehmen:

1. Quelle: 172.30.1.0/24 -> das VPN-Netz, das Du für den OpenVPN-Server zuvor eingerichtet hast.
2. Für den Rest: <Standardwerte>

Änderungen übernehmen (rechts im blauen Kasten).

Firewall: Regeln: OpenVPN

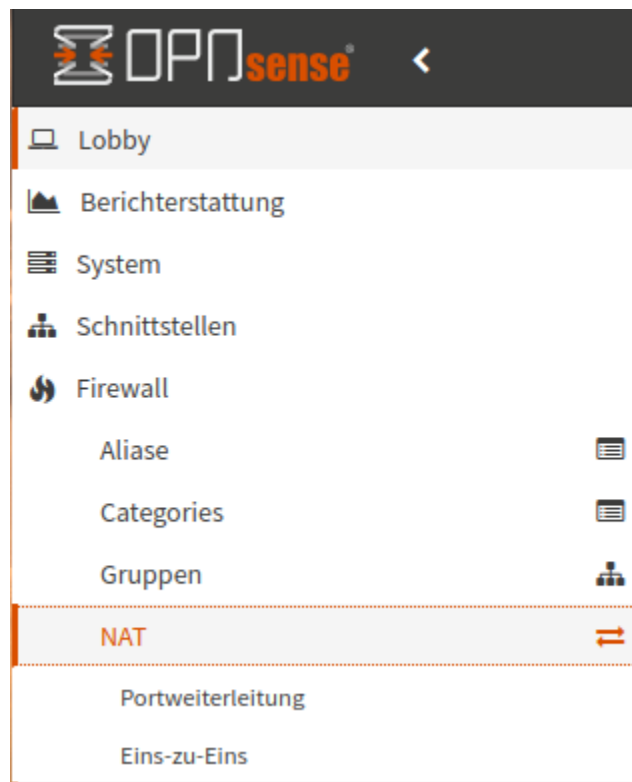
Kategorie auswählen

Die Änderungen wurden erfolgreich angewandt.

<input type="checkbox"/>	Protokoll	Quelle	Port	Ziel	Port	Gateway	Zeitplan	Beschreibung
<input type="checkbox"/>	IPv4 *	172.30.1.0/24	*	*	*	*	*	Allow OpenVPN Traffic

Sollte ein Router das externe Netz bedienen und befindet sich die OPNsense® „hinter“ dem Router, so muss auf dem Router eine Port-Forwarding Regeln für den gewünschten VPN-Port und das TCP-Protokoll eingerichtet werden, so dass alle externen Pakete auf diesem Port via UDP zur externen Schnittstelle der OPNsense® weitergeleitet werden.

In der OPNsense® ist dann unter Firewall -> NAT -> Portweiterleitung eine Regel hierzu anzulegen.



Hier legst Du nun eine Regel an, die UDP-Pakete, die an diese Firewall auf dem gewählten VPN-Port (hier in dem Beispiel Port 1194) ankommen, an die externe Schnittstelle (IP aus einem privaten Netz) der Firewall und den hier konfigurierten Port weitergegeben werden.

Nachstehende Abb. verdeutlicht diese Regel:

<input type="checkbox"/>	WAN	UDP	*	*	Diese Firewall	1194 (OpenVPN)	192.168.200.0/24	1194 (OpenVPN)	NAT 1194 -> 192.168.200.0/24
--------------------------	-----	-----	---	---	----------------	----------------	------------------	----------------	------------------------------

Zwischen dem Router, der die externe Verbindung bedient und der externen Schnittstelle der Firewall wird i.d.R. ein privates Netz (z.B. 192.168.200.0/24) verwendet. Daher muss hier eine Weiterleitungsregel für NAT angelegt werden, sonst werden die eingehenden Pakete vom Router nicht an die Firewall weitergegeben.

4.39.6 Konfiguration exportieren

Für die Verbindung mit den Clients muss nun ein Export des Profils für den Benutzer erfolgen.

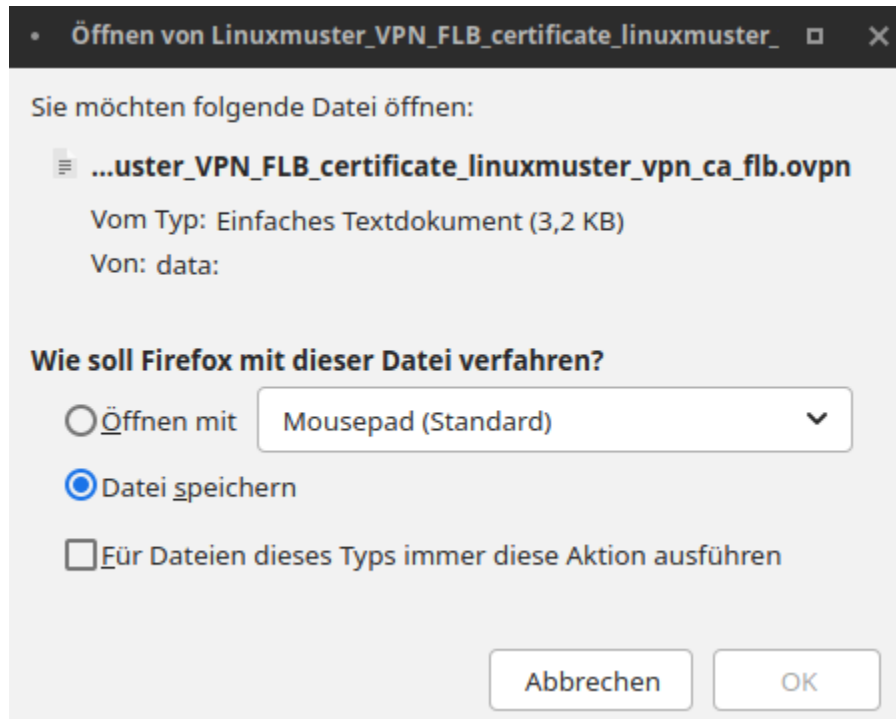
Dazu gehst Du zu VPN → OpenVPN → Clientexport. Dort gibst Du Folgendes an:

1. Ferner Zugriffsserver: Linuxmuster VPN UDP:25008 → Server aus der Liste auswählen, Port wie von Dir vorher angegeben.
2. Export type: Nur Datei
3. Hostname: URL unter dem die Firewall erreichbar ist, z.B: vpn.meineschule.de
4. Port: 25008 (ggf. anpassen an eigene Portwahl)
5. Für den Rest: <Standardwerte>

VPN: OpenVPN: Clientexport

i Ferner Zugriffsserver	Linuxmuster VPN FLB UDP:1194 ✖ Alles entfernen
i Export type	Nur Datei ✖ Alles entfernen
i Hostname	vpn.linuxmuster.lan
i Port	1194
i Use random local port	<input checked="" type="checkbox"/>
i Den Server-Subject überprüfen	<input checked="" type="checkbox"/>
i Windows Certificate System Store	<input type="checkbox"/>
i Disable password save	<input type="checkbox"/>
i Custom config	<div></div>

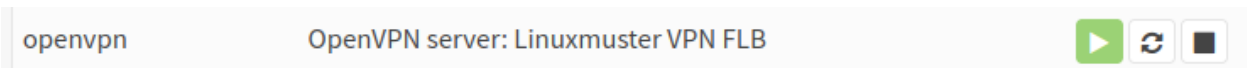
Danach drückst Du unter Accounts / certificates bei Linuxmuster VPN Server ganz rechts auf das Download-symbol.



Diese Konfigurationseinstellungen kannst Du nun allen Nutzern (z.B. Lehrern und Schülern), die Zugriff auf der Schulnetz via VPN haben sollen, im Intranet oder via Messenger zur Verfügung stellen.

4.39.7 mit VPN verbinden

Bevor Du nun die Verbindung mit einem Client zum VPN-Server testest, überprüfe zuerst, ob der Dienst läuft. In der GUI der OPNsense® klickst Du links auf den Menüeintrag Lobby und siehst rechts alle Dienste mit ihrem Status aufgelistet. Hier muss für OpenVPN Server ein grünes Dreieck zu sehen sein. Dies weist daraufhin, dass der Dienst läuft.



OpenVPN Client

Installiere Dir auf Deinem Gerät (PC, Tablet, Smartphone) den OpenVPN Client. Die heruntergeladene Datei muss nun auf das Endgerät heruntergeladen und dort in die App OpenVPN Connect (für alle Plattformen) importiert werden. Nach dem Import kann durch Eingabe von Benutzername und Passwort eine VPN-Verbindung hergestellt werden.

Auf der OPNsense® kannst Du den Verbindungsstatus der VPN-Verbindungen unter VPN -> OpenVPN -> Verbindungsstatus überprüfen.



Hier werden dann die Benutzer mit den zugeordneten VPN-Verbindungen angezeigt:

VPN: OpenVPN: Verbindungsstatus

Linuxmuster VPN FLB UDP:1194 Clientverbindungen			
Common Name	Reale Adresse	Virtuelle Adresse	Verbunden seit

Troubleshooting

Sollte die Verbindung nicht erfolgreich aufgebaut werden können, prüfe Folgendes ab:

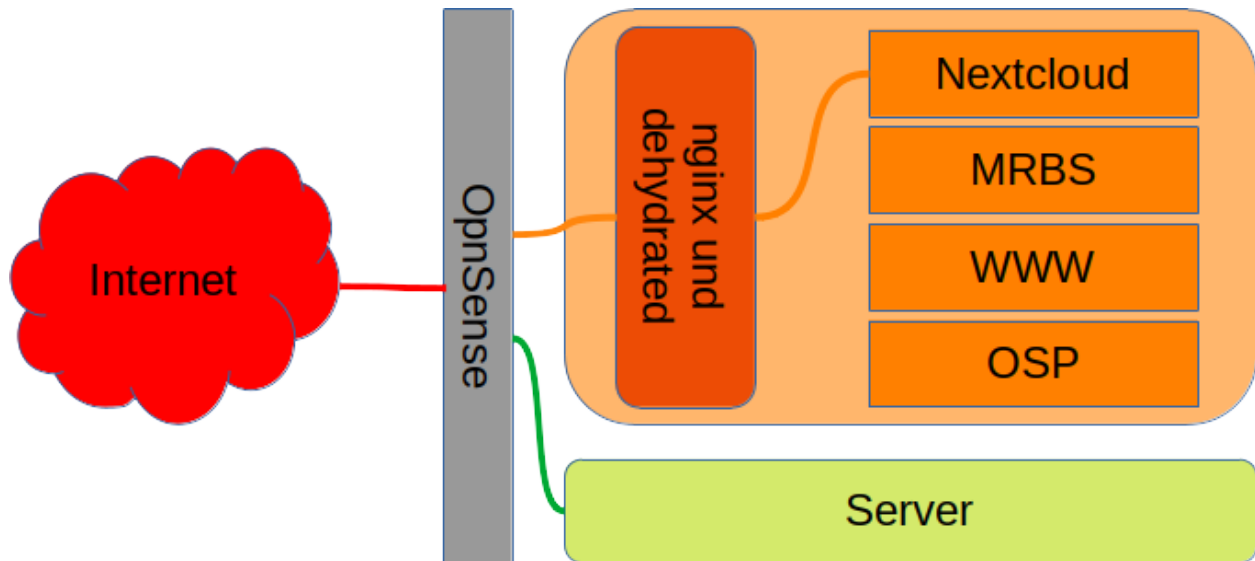
1. Ist die OPNsense® von extern via URL erreichbar ?
2. Antwortet die OPNsense® auf dem eingestellten VPN Port ?
3. Kommen die VPN - Pakete (ggf. Prot-Forwarding) auf der OPNsense® an?
4. Werden die VPN-Pakete auf der WAN-Schnittstelle zugelassen (siehe Live-Logs)?

4.40 Installation eines Dockerhosts

Autor des Abschnitts: @rettich

Ein Docker-Host vereinfacht die Bereitstellung von Anwendungen, weil Anwendungen virtualisiert in einem Container, der alle nötigen Pakete enthält, leicht als Datei transportiert und installiert werden können.

Angenommen wir möchten an einer Schule eine Nextcloud, ein MRBS, eine Website und eventuell noch ein Open-SchulPortfolio betreiben und jeder dieser Anwendungen soll eine Weboberfläche (Port 80 und 443) anbieten. Dann bräuchten wir entweder 5 öffentliche IP-Adressen oder einen Reverse Proxy, wie nginx, der alle Anfragen für verschiedene Domänen / Subdomänen über eine IP stellvertretend entgegennimmt und an die Anwendungen verteilt.



Das hier abgebildete System besteht aus der Firewall OpnSense einem Docker-Host und dem Server.

Alle Anfragen auf Port 80 oder 443 an `nextcloud.schulname.de`, `www.schulname.de`, `mrbs.schulname.de` oder `osp.schulname.de` kommen zunächst an der Firewall OpnSense an und werden direkt an den Dockerhost weiter geleitet. Der Reverse Proxy nginx schaut dann nach, mit welcher URL die Anfrage eigentlich verbunden werden möchte und stellt dann die Verbindung zum entsprechenden Service her.

Dehydrated nutzen wir, um Zertifikate mit Let's Encrypt zu signieren.

Wenn Du lediglich einen internen Service wie den Unifi-Controller benötigst, solltest Du auf nginx und dehydrated verzichten.

Installiere zunächst einen ubuntu 20.04 Server.

4.40.1 Installation des Ubuntu Servers

Lade die iso-Datei für den Ubuntu-Server von <https://ubuntu.com/download/server> herunter und starte Deinen Server vom Installationsmedium.

Im folgenden gehen wir davon aus, dass der Docker-Host in Deiner `/etc/linuxmuster/sophomorix/default-school/devices.csv` als `servername` bekannt ist. Dann bekommt der Dockerhost seine IP und seinen Namen über DHCP.

Wenn Du den Dockerhost nicht im Schulnetz sondern in der DMZ der OpnSense anlegen möchtest, bekommt er ebenfalls seine IP über DHCP.

```

Willkommen! Bienvenue! Welcome! Добро пожаловать! Welkom! [ Help ]

Use UP, DOWN and ENTER keys to select your language.

[ Asturianu                ▶ ]
[ Bahasa Indonesia         ▶ ]
[ Català                   ▶ ]
[ Deutsch                   ▶ ]
[ English                   ▶ ]
[ English (UK)              ▶ ]
  
```

Wähle Deine bevorzugte Sprache

Tastatur-Konfiguration	[Help]
Bitte wählen Sie unten Ihr Tastaturlayout aus oder wählen Sie »Tastatur identifizieren«, um Ihr Layout automatisch zu erkennen.	
Belegung: [Deutsch ▼]	
Variante: [Deutsch ▼]	
[Tastatur erkennen]	

und Tastatur.

Netzwerkverbindungen	[Help]												
Konfigurieren Sie mindestens eine Schnittstelle, über die dieser Server mit anderen Maschinen kommunizieren kann und die vorzugsweise ausreichend Zugriff für Aktualisierungen bietet.													
<table border="1"> <thead> <tr> <th>NAME</th> <th>TYPE</th> <th>NOTES</th> </tr> </thead> <tbody> <tr> <td>[enp0s3</td> <td>eth</td> <td>- ▶]</td> </tr> <tr> <td colspan="3">DHCPv4 10.0.0.2/16</td> </tr> <tr> <td colspan="3">08:00:27:f8:be:94 / Intel Corporation / 82540EM Gigabit Ethernet Controller (PRO/1000 MT Desktop Adapter)</td> </tr> </tbody> </table>		NAME	TYPE	NOTES	[enp0s3	eth	- ▶]	DHCPv4 10.0.0.2/16			08:00:27:f8:be:94 / Intel Corporation / 82540EM Gigabit Ethernet Controller (PRO/1000 MT Desktop Adapter)		
NAME	TYPE	NOTES											
[enp0s3	eth	- ▶]											
DHCPv4 10.0.0.2/16													
08:00:27:f8:be:94 / Intel Corporation / 82540EM Gigabit Ethernet Controller (PRO/1000 MT Desktop Adapter)													
[Erstelle Bond ▶]													

Da der neue Docker-Host per DHCP seine IP-Adresse bekommt, kannst Du die Vorgaben übernehmen.

Proxy konfigurieren	[Help]
Wenn dieses System einen Proxy erfordert, um mit dem Internet verbunden zu werden, geben Sie seine Details hier an.	
Proxy-Adresse:	<input type="text"/> Wenn Sie einen HTTP-Proxy verwenden müssen, um die Außenwelt zu erreichen, geben Sie die Proxy-Informationen hier an. Ansonsten lassen Sie dies leer. Die Proxy-Informationen sollten in der Standardform von "http://[[Benutzer][:Kennwort]@]Host[:Port]/" angegeben werden.

Die Proxy-Adresse und

Konfiguriere Ubuntu-Archiv-Mirror	[Help]
Wenn Sie einen alternativen Spiegelserver für Ubuntu verwenden, geben Sie dessen Details hier an.	
Mirror-Adresse:	<input type="text" value="http://de.archive.ubuntu.com/ubuntu"/> Sie können einen Archivspiegel angeben, der anstelle des Standardwertes verwendet wird.

die Mirror-Adresse übernimmst du.

Begleitete Speicherplatzkonfiguration	[Help]
Configure a guided storage layout, or create a custom one:	
(X) Eine ganze Festplatte verwenden	
[VBOX_HARDDISK_VB267cb299-911b6f56 local disk 40.000G ▼]	
[] Diese Festplatte als LVM-Gruppe konfigurieren	
[] Die LVM-Gruppe mit LUKS verschlüsseln	
Passphrase:	
Passphrase bestätigen:	
() Custom storage layout	

Die Speicherplatzkonfiguration

Speicherplatzkonfiguration	[Help]
ZUSAMMENFASSUNG DES DATEISYSTEMS	
EINHÄNGEPUNKT	GRÖSSE TYP GERÄTETYP
[/]	39.997G new ext4 neu partition of lokaler Datenträger ▶]
VERFÜGBARE GERÄTE	
Keine verfügbaren Geräte	
[Software-RAID (md) erstellen ▶]	
[Datenträgergruppe (LVM) anlegen ▶]	
GENUTZTE GERÄTE	
GERÄT	TYP GRÖSSE
[VBOX_HARDDISK_VB267cb299-911b6f56	lokaler Datenträger 40.000G ▶]
partition 1 neu, BIOS grub spacer	1.000M ▶
partition 2 neu, formatiert werden als ext4, Nach /	39.997G ▶
eingebunden	

kannst Du auch übernehmen.

Profileinrichtung		[Help]
Geben Sie den Benutzernamen und das Passwort ein, mit dem Sie sich am System anmelden möchten. Sie können den SSH-Zugang auf dem nächsten Bildschirm konfigurieren, aber für sudo wird weiterhin ein Passwort benötigt.		
Ihr Name:	<input type="text" value="Docker Admin"/>	
Name Ihres Servers:	<input type="text" value="unifi"/> Der Name, der bei der Kommunikation mit anderen Rechnern verwendet wird.	
Bitte Benutzernamen auswählen:	<input type="text" value="dockeradmin"/>	
Bitte Passwort auswählen:	<input type="password" value="kkkkkkkk"/>	
Passwort bestätigen:	<input type="password" value="kkkkkkkk"/>	

Der Name des Servers sollte so, wie in `/etc/linuxmuster/sophomorix/default-school/devices.csv` gewählt werden.

Der Benutzername ist frei wählbar.

SSH-Einrichtung		[Help]
Sie können auswählen das OpenSSH-Server-Paket zu installieren um sicheren Fernzugriff auf Ihren Server zu aktivieren.		
	<input checked="" type="checkbox"/> OpenSSH-Server installieren	
SSH-Identität importieren:	[Nein ▼] Sie können Ihre SSH-Schlüssel aus GitHub oder Launchpad importieren.	
Importiere Benutzername:	<input type="text"/>	
	<input checked="" type="checkbox"/> Kennwortauthentifizierung über SSH erlauben	

OpenSSH-Server solltest Du installieren, möchtest Du Dich vom lmn-Server auf dem Docker-Host anmelden können. Andere Pakete brauchst Du nicht zu installieren.

Wenn alles installiert ist, kannst Du Dich an Deinem frisch installiertem Docker-Host anmelden.

4.40.2 Installation ohne nginx und dehydrated

- Gib `sudo -i` ein um `root` zu werden.
- Update Dein System mit `apt update` und `apt dist-upgrade`.
- Installiere docker und docker-compose mit:

```
apt-get install docker-ce docker-ce-cli containerd.io docker-compose-plugin
```


4.40.3 Installation mit nginx und dehydrated

- Gib `sudo -i` ein um *root* zu werden.
- Update Dein System mit `apt update` und `apt dist-upgrade`.
- Installiere docker, docker-compose, nginx und dehydrated mit:

```
apt-get install docker-ce docker-ce-cli containerd.io docker-compose-plugin nginx_
↪ dehydrated
```

4.41 Externe Authentifizierung - Moodle

Autor des Abschnitts: @thomas, @cweikl

Das Active Directory (AD) der linuxmuster.net 7 dient als zentrale Authentifizierungsinstanz. Sollen Dienste wie z.B. das Lernmanagementsystem (LMS) Moodle oder das Raumbuchungssystem MRBS extern betrieben werden, so können diese so konfiguriert werden, dass eine Authentifizierung gegen das AD der lmn 7 erfolgt.

Hierzu sind einige Konfigurationsschritte erforderlich, die nachstehend beschrieben werden.

4.41.1 Firewall-Einstellungen

Die Firewall (OPNsense®) muss so konfiguriert werden, dass Anfragen über den LDAPS-Port 636 an den Server weitergeleitet werden.

In der Konfigurationsoberfläche ist unter **Firewall -> NAT -> Portweiterleitung** eine entsprechende Regel anzulegen. Wenn die von linuxmuster.net bereitgestellte Appliance verwendet wurde, ist die Regel schon vorbereitet. Anderfalls muss diese wie in der Abb. ersichtlich, noch erstellt werden.

Firewall: NAT: Portweiterleitung

		Quelle		Ziel		NAT			
<input type="checkbox"/>	Schnittstelle	Protokoll	Adresse	Ports	Adresse	Ports	IP	Ports	Beschreibung
<input checked="" type="checkbox"/>	LAN	TCP	*	*	LAN Adresse	22, 80, 443	*	*	Anti-Aussperrregel
<input type="checkbox"/>	↔ WAN	TCP	*	*	*	22 (SSH)	10.0.0.1	22 (SSH)	SSH -> Server
<input type="checkbox"/>	↔ WAN	TCP	*	*	*	636	10.0.0.1	636	LDAPS -> Server

Die Regel muss nun noch aktiviert



und anschliessend übernommen werden:

Die NAT Konfiguration hat sich geändert.
Sie müssen die Änderungen übernehmen, damit diese in Kraft treten.

Änderungen übernehmen

4.41.2 Moodle-Einstellungen

Im externen Moodle-System sind unter Website-Administration -> Plugins -> Authentifizierung -> LDAP-Server die folgenden Einstellungen vorzunehmen.

Nicht aufgeführte Optionen sollten auf der Standard-Einstellung bleiben bzw. leer gelassen werden.

LDAP-Server-Einstellungen

Host Url	ldaps://server.linuxmuster.lan
	Hier den vollständigen Namen des eigenen Servers oder die IP-Adresse verwenden.
Version	3
TLS benutzen	Nein
LDAP-Codierung	utf-8

Bind-Einstellungen

Achtung: Grundsätzlich sollten alle externen Dienste, die via LDAP an das AD angebunden werden, mit einem eigens dafür angelegten Bind-User genutzt werden. Für Moodle sollte so z.B. ein Benutzer `moodle-binduser` angelegt werden, der für die Verbindung zum AD genutzt wird. Hinweise hierzu findest Du unter <https://github.com/linuxmuster/sophomorph4/wiki/bindusers>

Vorgehen zur Anlage eines neuen Bind-Users

1. Auf dem linuxmuster.net Server folgenden Befehl in der Konsole als Benutzer root absetzen, um einen neuen Benutzer (`moodle-binduser`) für den Bind-Zugriff zu definieren. Das zufällig erzeugte Kennwort wird in einer Datei auf dem Server hinterlegt.

```
# sophomorph-admin --create-school-binduser moodle-binduser --school default-school --
  ↳ random-passwd-save
```

2. Gib für den neu angelegten Benutzer einen Kommentar an, um später einen Hinweis zu erhalten, für welchen Zweck der Benutzer genutzt wird.

```
# sophomorph-user -u moodle-binduser --comment "AD access from moodle"
```

3. Lasse nun die Daten für den neu angelegten Benutzer anzeigen, die dann in Moodle als bind-user einzutragen sind.

```
# sophomorix-admin -i -a moodle-binduser
```

4. Trage in Moodle die unter 3. angezeigten Daten in Moodle für den Bind-User nach dem nachstehenden Schema ein:

Anmeldename	CN=moodle-binduser,OU=Management,OU=default-school,OU=SCHOOLS,DC=linuxmuster,DC=lan
Kennwort	geheim (angezeigtes Kennwort, das in der datei hinterlegt wurde) Kennwort des Bind-Users wurde unter 1. in einer Datei auf dem Server abgelegt. zur Anzeige ist der Befehl unter 3. erforderlich
Nutzertyp	MS ActiveDirectory
Kontexte	OU=schools,DC=linuxmuster,DC=lan Die DC-Einträge sind durch die, der eigenen Domäne zu ersetzen.
Subkontexte	Ja

Weitere Einstellungen

Kennwortänderung fordern

Änderung fordern	Nein
Standardseite zur Änderung nutzen	Nein
Kennwortformat	Nein

Einstellungen zum Ablauf von LDAP-Kennwörtern

Ablauf	Nein
Ablaufwarnung	Leer
Ablaufmerkmal	Leer
GraceLogins	Nein
Merkmal für GraceLogin	Leer

Nutzererstellung aktivieren

Nutzer/innen extern anlegen	Nein
Kontext für neue Nutzer/innen	Leer

Zuordnung von Systemrollen

Kursersteller/in-Kontext	OU=teachers,OU=default-school,OU=schools,DC=linuxmuster,DC=lan DC-Einträge durch eigene Domäne ersetzen.
--------------------------	---

Synchronisierung von Nutzerkonten

Entfernte externe Nutzer	Intern löschen
Status von lokalen Nutzerkonten synchronisieren	Nein

NTLM-SSO

Aktivieren	Nein
Subnet	Nein
MS IE fast path?	NTLM mit allen Browsern versuchen

Datenzuordnung

Daten übernehmen (Vorname)	givenName
Daten übernehmen (Nachname)	sn
Daten übernehmen (E-Mail-Adresse)	Leer

Nutzersuche (user lookup)

ObjectClass (auth_ldap objectclass)	((!(sophomorixRole=teacher)(sophomorixRole=student)) Filter: Nur Lehrer und SuS, keine Maschinen-Accounts
-------------------------------------	--

Zum Testen, ob der Filter korrekt arbeitet, sollte zugleich die Einstellung zur Synchronisierung von Nutzerkonten wie folgt angepasst werden:

Synchronisierung von Nutzerkonten (user account synchronisation)

Entfernte externe Nutzer/innen (auth_ldap removeuser)	für Tests: intern sperren (suspend internal) danach: intern löschen (delete internal)
---	--

Die Änderungen sind abschließend über die Schaltfläche am Seitenende zu sichern. In der Übersicht der **Aktiven** Plugins ist der LDAP-Server zur Authentifizierung zu aktivieren.

Achtung: Nachdem alle Einstellungen getroffen sind, unbedingt alle Caches leeren!

4.41.3 Host-Einstellungen

Gegebenenfalls muss auf dem Moodle-Host sicher gestellt werden, dass das selbstsignierte Zertifikat des Servers bei der LDAP-Abfrage akzeptiert wird.

Auf dem Host selbst ist hierzu in der Datei `/etc/ldap/ldap.conf` folgender Eintrag zu ergänzen:

`TLS_REQCERT never`

Läuft die Moodle-Instanz in einem Docker-Container, reicht man diese Datei als `readonly` Volume an den Container durch. Der Eintrag in der Datei `docker-compose.yml` lautet dann:

`volumes:
- '/etc/ldap/ldap.conf:/etc/ldap/ldap.conf:ro'`

4.42 Nextcloud für linuxmuster.net

Autor des Abschnitts: @rettich, Ergänzungen: @cweikl

In diesem Teil der Dokumentation siehst Du, wie Du auf einem Docker-Host Nextcloud einrichtest, wie Du das Active Directory (AD) der linuxmuster.net 7 als Authentifizierungsinstanz nutzt und was Du einstellen musst, damit Deine Benutzer über die Nextcloud direkt auf ihre Daten zugreifen können.

Inhalt:

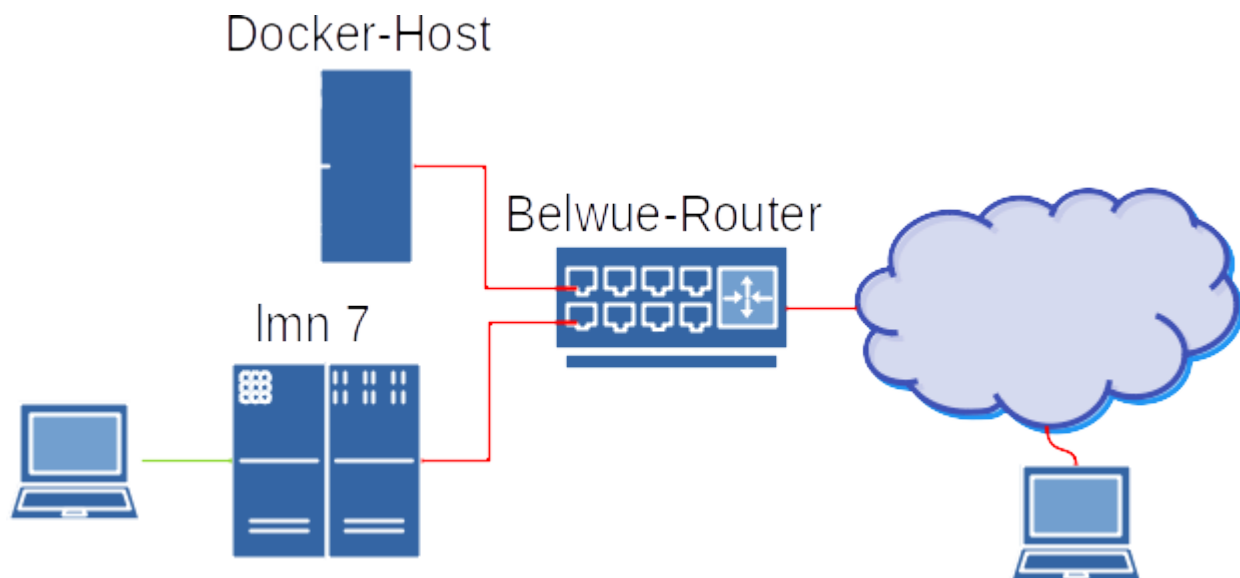
4.42.1 Vorüberlegungen zum Standort des Nextcloud-Services

Vor dem Einsatz einer Nextcloud ist zu überlegen, wie die Nutzung geplant ist und wie sich die technischen Voraussetzungen an der Schule darstellen.

Hierbei spielen auch Überlegungen eine Rolle, ob die Daten, die auf den internen Home-Laufwerken der lmn7 liegen, über die Nextcloud eingebunden und zur Verfügung gestellt werden sollen. Sollte dies der Fall sein, so bietet sich ein interner Docker-Host an (u.a. auch aus Sicherheitsüberlegungen). Kann darauf verzichtet werden und ist die Anbindung der Schule nur mit begrenzter Bandbreite gegeben, so könnte ein externer Docker-Host besser für die Schule geeignet sein.

Beide Szenarien werden nachstehend kurz dargestellt.

Nextcloud auf einem internen Docker-Host

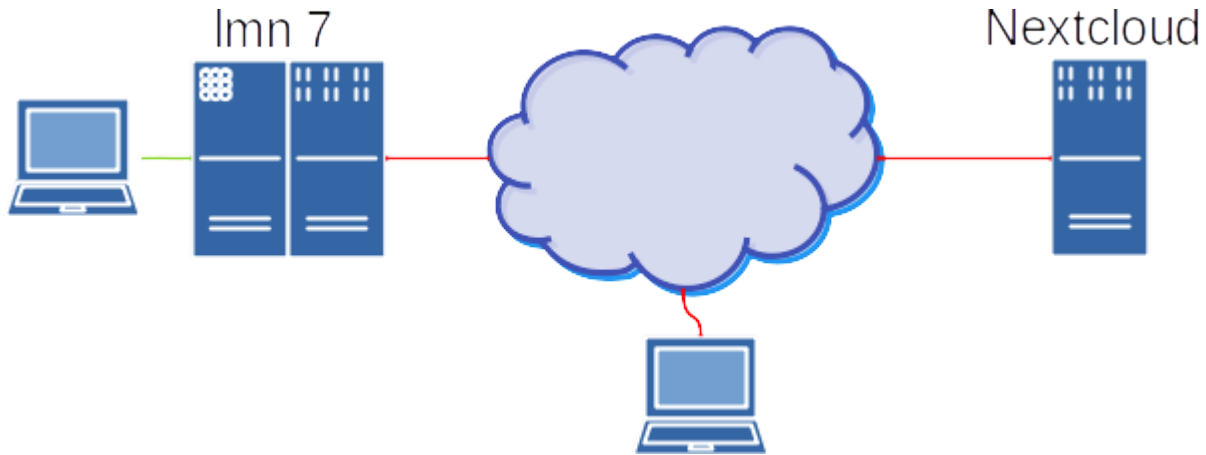


In der Grafik ist der Nextcloud-Service auf dem Docker-Host der Schule installiert. Da der Docker-Host Web-Services wie das Medien- und Raumbuchungssystem und die Nextcloud zur Verfügung stellt, ist er ein völlig eigenständiger Server, der außerhalb der linuxmuster.net steht. Er sollte also direkt an den Router angeschlossen sein und eine eigene IP-Adresse haben. Hier ist später darauf zu achten, dass die Portweiterleitungen am Router für den Docker-Host und die lmn7 korrekt gesetzt sind.

Greift ein Gerät in der Schule, z.B. ein Tablett oder ein Handy, über die Nextcloud auf Daten zu, die in den Home-Laufwerken der lmn7 liegen, müssen die Daten nicht über das Internet gesendet werden. Hier ist der Datenzugriff schnell.

Greift ein Gerät außerhalb der Schule über die Nextcloud auf Daten auf dem Schulserver zu, müssen die Daten vom Docker-Host über das Internet zum Gerät. Hier hängt die Geschwindigkeit von der Internetanbindung der Schule ab.

Nextcloud auf einem externen Docker-Host



In der Grafik ist ein externer Nextcloud-Service außerhalb der Schule dargestellt.

Greift ein Gerät in der Schule über die Nextcloud auf Daten auf dem Schulserver zu, müssen die Daten vom Schulserver über das Internet zum Nextcloud-Service und wieder zurück zum Schulserver. Hier ist der Datenzugriff erheblich langsamer als oben.

Greift ein Gerät außerhalb der Schule über die Nextcloud auf Daten auf dem Schulserver zu, müssen die Daten vom Schulserver über das Internet zum Nextcloud-Service und dann zum Gerät. Der Datenzugriff ist hier nicht schneller als oben.

Sollte ein Zugriff auf die Home-Laufwerke der lmn7 nicht vorgesehen sein, ist die externe Nextcloud, was die Rechenleistung angeht, leistungstärker als eine interne Nextcloud.

Falls Du bereits einen Nextcloud-Service hast, kannst Du das erste Kapitel überspringen.

4.42.2 Voraussetzung: Docker-Host

Um den Nextcloud-Service in der hier beschriebenen Form zu betreiben, ist die Installation eines Docker-Hosts erforderlich. Hierzu ist ein dedizierter oder als VM entsprechend leistungsstarker Linux-Server mit Ubuntu 20.04 LTS zu installieren. Auf dem Server ist dann der Docker-Host einzurichten. Wie das geht siehst Du im Kapitel *Installation eines Dockerhosts*

4.42.3 Firewall-Regeln

Damit die Nextcloud funktionieren kann, braucht Sie Zugriff auf das AD des Servers. Möchtest Du auch auf Verzeichnisse und Dateien zugreifen, muss die OpnSense auch Samba-Anfragen an den Server weiterleiten.

In beiden Fällen müssen Anfragen vom Docker-Host an den Server weitergeleitet werden

Hinweis: Jede Öffnung der Firewall birgt Sicherheitsrisiken. Insgesamt müssen diese vor der Einrichtung bewertet werden.

Firewallregel für den Zugriff auf das AD

Wenn ein Service, wie die Nextcloud oder Moodle auf das AD des Servers zugreifen möchte, wird er die Anfrage an die Firewall stellen. Die Firewall sollte dann diese Anfrage an den Server weiterleiten.

Die Firewallregel wird also eine Portweiterleitung des Ports 636 (ldaps) sein.

Melde Dich als root an der OpnSense an und navigiere zu Firewall -> NAT -> Portweiterleitung.



Klicke auf Hinzufügen um eine neue Firewallregel hinzuzufügen und trage die folgenden Werte ein.

Weiterleitungseintrag bearbeiten
vollständige Hilfe

☐ Deaktiviert
Dieser Regel deaktivieren

☐ Kein RDR (NICHT)

☐ Schnittstelle
WAN

☐ TCP/IP Version
IPv4

☐ Protokoll
TCP

Quelle
Erweitert

☐ Ziel / Umkehren

☐ Ziel
Diese Firewall

☐ Zielportbereich
von:
anz:

(anderer(r)s)
(anderer(r)s)

636
636

☐ Ziel-IP umleiten
Einzelner Host oder Netzwerk

10.0.0.1

☐ Pooloptionen:
Standard

☐ Protokoll

☐ Kategorie

☐ Beschreibung
LDAPs -> Server

☐ Setze lokal-Tag

☐ Prüfe auf die lokale Markierung

☐ Keine XMLRPC Synchronisation

☐ NAT reflection
Benutze Systemvorgabe

☐ Filter Regel Zuordnung
Erlauben

Regelinformation

Erstellt
11/30/18 23:06:09 (linuxmuster)

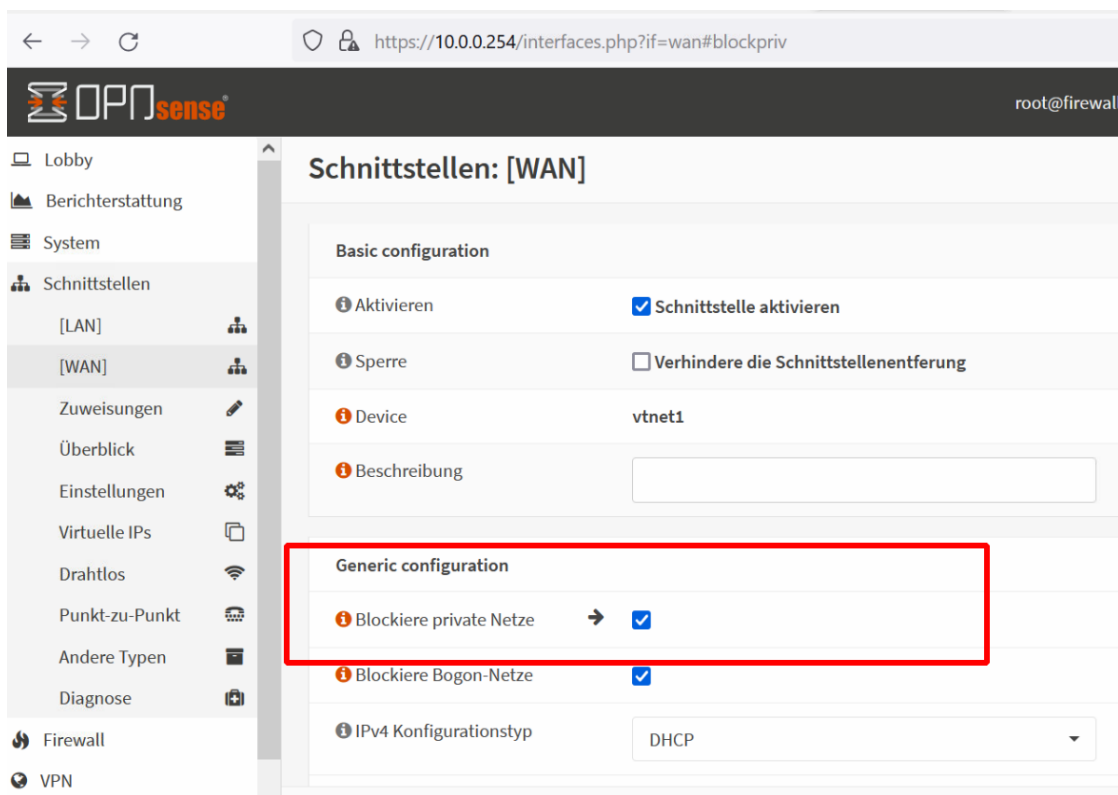
Aktualisiert
10/27/20 22:09:55 (root@192.168.10.6)

Speichern
Abbrechen

Bei *Ziel-IP umleiten* trägst Du natürlich die IP-Adresse Deines Servers ein. Im Allgemeinen wird das 10.0.0.1 sein. In der lmn6 war das 10.16.1.1.

Externer NC-Docker

Steht der NC-Docker extern so ist folgende Einstellung für die WAN-Schnittstelle zu setzen:

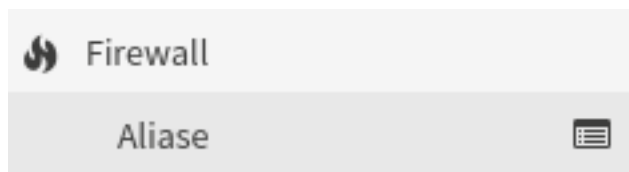


Firewallregel für den Zugriff über Samba

Hinweis: Sollte der Nextcloud-Service extern stehen, so sollten diese Ports nicht weitergeleitet werden.

Für den Zugriff über Samba müssen die Ports 139 und 445 an den Server weitergeleitet werden. Dazu legst Du erst mal einen Alias an.

Navigiere auf Firewall -> Aliase.



In der Zeile unter dem letzten Alias klickst Du auf + um einen neuen Alias anzulegen.



Und trage die folgenden Werte ein.

Edit Alias

vollständige Hilfe

Aktiviert

☒

Name

SMB_CIFS

Typ

Port(s)

Inhalt

139

445

Alles entfernen

Beschreibung

Ports für Samba

Abbrechen

Speichern

Klicke anschließend auf **Speichern**.

Jetzt kommt noch die eigentliche Firewall-Regel. Navigiere wieder zu **Firewall** -> **NAT** -> **Portweiterleitung**.



Klicke auf **Hinzufügen**, um eine neue Firewallregel hinzuzufügen und trage die folgenden Werte ein:

Weiterleitungseintrag bearbeiten vollständige Hilfe

☐ Deaktiviert Diese Regel deaktivieren

☐ Kein RDR (NICHT)

Schnittstelle: WAN

TCP/IP Version: IPv4

Protokoll: TCP

☐ Quelle / Umkehren

Quelle: Einzelner Host oder Netzwerk
10.20.30.40 29

Quellportbereich: von: jeglich an: jeglich

☐ Ziel / Umkehren

Ziel: Diese Firewall

Zielportbereich: von: SMB_CIFS an: SMB_CIFS

Ziel-IP umleiten: Einzelner Host oder Netzwerk
10.0.0.1

Zielport weiterleiten: SMB_CIFS

Pooloptionen: Standard

☐ Protokoll

Kategorie:

Beschreibung: Docker darf Samba

Setze lokal-Tag:

Prüfe auf die lokale Markierung:

☐ Keine XMLRPC Synchronisation

NAT reflection: Aktivieren

Filter Regel Zuordnung: Erlauben

Regelinformation

Erstellt	10/27/20 21:52:27 (root@192.168.10.6)
Aktualisiert	11/6/20 22:03:20 (root@192.168.10.6)

Speichern Abbrechen

Bei Quelle trägst Du die IP-Adresse und die Netzwerkmaske Deines Docker-Hosts ein. Und bei *Ziel-IP umleiten* trägst Du wieder die IP-Adresse Deines Servers ein. Im Allgemeinen wird das 10.0.0.1 sein. In der lmn6 war dies die IP 10.16.1.1.

4.42.4 Nextcloud installieren

Autor des Abschnitts: @rettich, Ergänzungen: @cweikl

Auf einem Docker-Host sind folgende Schritte zur Installation notwendig:

1. Erstellen eines Let's Encrypt - Zertifikats.
2. Erstellen einer Site für die Nextcloud in nginx.
3. Erstellen und Starten der Nextcloud Docker App.

Hinweis: Im Folgenden musst Du natürlich nextcloud.meine-schule.de durch Deine URL ersetzen.

Erstellung des Zertifikats

Zuerst musst Du Dir einen Dienstenamen ausdenken und SSL-Zertifikate besorgen. Also z.B. nextcloud.meine-schule.de.

Dazu legst Du einen DNS Eintrag für Deine Dockerapp, z.B. nextcloud.meine-schule.de, der auf die IP des Docker-Hosts zeigt an. Das darf auch ein CNAME sein.

Trage diesen Host in die Datei `/etc/dehydrated/domains.txt` ein.

Führe den Befehl `dehydrated -c` aus. Jetzt hast Du die Zertifikate im Verzeichnis `/var/lib/dehydrated/certs/` zur Verfügung, der Docker Host aktualisiert diese per Cronjob.

Erstellen einer Site für die Nextcloud in nginx

Wir benutzen nginx als Reverse-Proxy. So können auf Deinem Docker-Host viele Services wie beispielsweise `mrbs.meine-schule.de` und `nextcloud.meine-schule.de` unter der gleichen IP-Adresse laufen.

Wenn beispielsweise ein Benutzer die Seite `nextcloud.meine-schule.de` aufruft, schaut sich nginx die URL an, die aufgerufen wurde, und liefert dann die entsprechende Seite aus.

Melde Dich als root auf Deinem Docker-Host an.

Erstelle mit `mkdir -p /srv/docker/nextcloud` das Verzeichnis, in das alle Nextcloud-Dateien abgelegt werden.

Erzeuge die Datei `/srv/docker/nextcloud/nextcloud.nginx.conf` mit folgendem Inhalt:

```
server {
    listen 80;
    listen [::]:80;
    server_name nextcloud.meine-schule.de;

    location / {
        return 301 https://nextcloud.staufer-gymnasium.de$request_uri;
    }

    location ^~ /.well-known/acme-challenge {
        alias /var/www/dehydrated;
    }
}

server {
    listen 443 ssl http2;
    listen [::]:443 ssl http2;
    server_name nextcloud.meine-schule.de;
    ssl_certificate /var/lib/dehydrated/certs/nextcloud.meine-schule.de/fullchain.pem;
    ssl_certificate_key /var/lib/dehydrated/certs/nextcloud.meine-schule.de/privkey.pem;
    ssl_protocols TLSv1.2;
    ssl_prefer_server_ciphers on;
    location /.well-known/caldav {
        return 301 $scheme://$host/remote.php/dav;
    }
    location /.well-known/carddav {
        return 301 $scheme://$host/remote.php/dav;
    }
}
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```

location / {
    proxy_read_timeout 600s;
    client_max_body_size 0;
    proxy_set_header Connection "";
    proxy_set_header Host $host;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_set_header X-Forwarded-Proto $scheme;
    add_header Strict-Transport-Security "max-age=31536000; includeSubDomains; preload
↪";
    access_log /var/log/nginx/nextcloud.access.log;
    error_log /var/log/nginx/nextcloud.error.log;
    proxy_pass http://localhost:7771;
}
}

```

Diese conf-Datei geht davon aus, dass Deine Nextcloud auf localhost:7771 erreichbar sein wird. Den Port 7771 kannst Du frei wählen. Dies muss identisch sein mit dem später in docker-compose.yml anzugebenen Port für nextcloud.

Jetzt musst Du noch im Verzeichnis /etc/nginx/sites-enabled einen Link auf Deine nextcloud.nginx.conf anlegen und nginx neu starten.

Melde Dich wieder als root am Docker-Host an und lege mit `ln -s /srv/docker/nextcloud/nextcloud.nginx.conf /etc/nginx/sites-enabled/nextcloud.meine-schule.de` den Link an.

So, jetzt musst Du nur noch mit `systemctl restart nginx.service` nginx neu starten.

Prüfe noch, welche Ports nun genutzt werden. Gib dazu den Befehl `netstat -tulp` an.

Nextcloud mit docker-compose einrichten und starten

Jetzt musst Du nur noch drei Dateien anlegen, die docker-compose sagen, was es machen soll.

Alles was wir jetzt machen, spielt sich im Verzeichnis /srv/docker/nextcloud ab. Später werden auch dort sämtliche Daten liegen. Für eine Datensicherung musst Du nur dieses Verzeichnis sichern.

Melde Dich wieder als root auf dem Docker-Host an und gehe mit `cd /srv/docker/nextcloud` in das Verzeichnis /srv/docker/nextcloud.

Die Datei Dockerfile

```

FROM nextcloud:stable
RUN apt-get update && apt-get install -y smbclient libsmbclient-dev imagemagick && pecl_
↪install smbclient && docker-php-ext-enable smbclient && rm -rf /var/lib/apt/lists/*

```

Wenn Du experimentierfreudig bist, kannst Du statt stable auch latest schreiben.

Mit der zweiten Zeile werden die Vorbereitungen für die Einbindungen der Home-Verzeichnisse (Samba-Shares) durchgeführt.

Die Datei db.env

```
MYSQL_ROOT_PASSWORD=geheim
MYSQL_PASSWORD=geheim
MYSQL_DATABASE=nextcloud
MYSQL_USER=nextcloud
```

Hier sind die Zugangsdaten für die Datenbank hinterlegt.

Die Datei docker-compose.yml

```
version: '3'

services:
  db2:
    image: mariadb:10.5
    command: --transaction-isolation=READ-COMMITTED --binlog-format=ROW
    restart: always
    volumes:
      - ./db:/var/lib/mysql
    env_file:
      - db.env

  redis2:
    image: redis:alpine
    restart: always

  app2:
    build:
      context: .
      dockerfile: Dockerfile
    restart: always
    ports:
      - 7771:80
    volumes:
      - ./nextcloud:/var/www/html
    environment:
      - MYSQL_HOST=db2
      - REDIS_HOST=redis2
    env_file:
      - db.env
    depends_on:
      - db2
      - redis2

  cron2:
    build:
      context: .
      dockerfile: Dockerfile
    restart: always
    volumes:
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
- ./nextcloud:/var/www/html
entrypoint: /cron.sh
depends_on:
  - db2
  - redis2

volumes:
  db:
  nextcloud:
```

In der Datei `docker-compose.yml` werden die Services Deiner Nextcloud beschrieben.

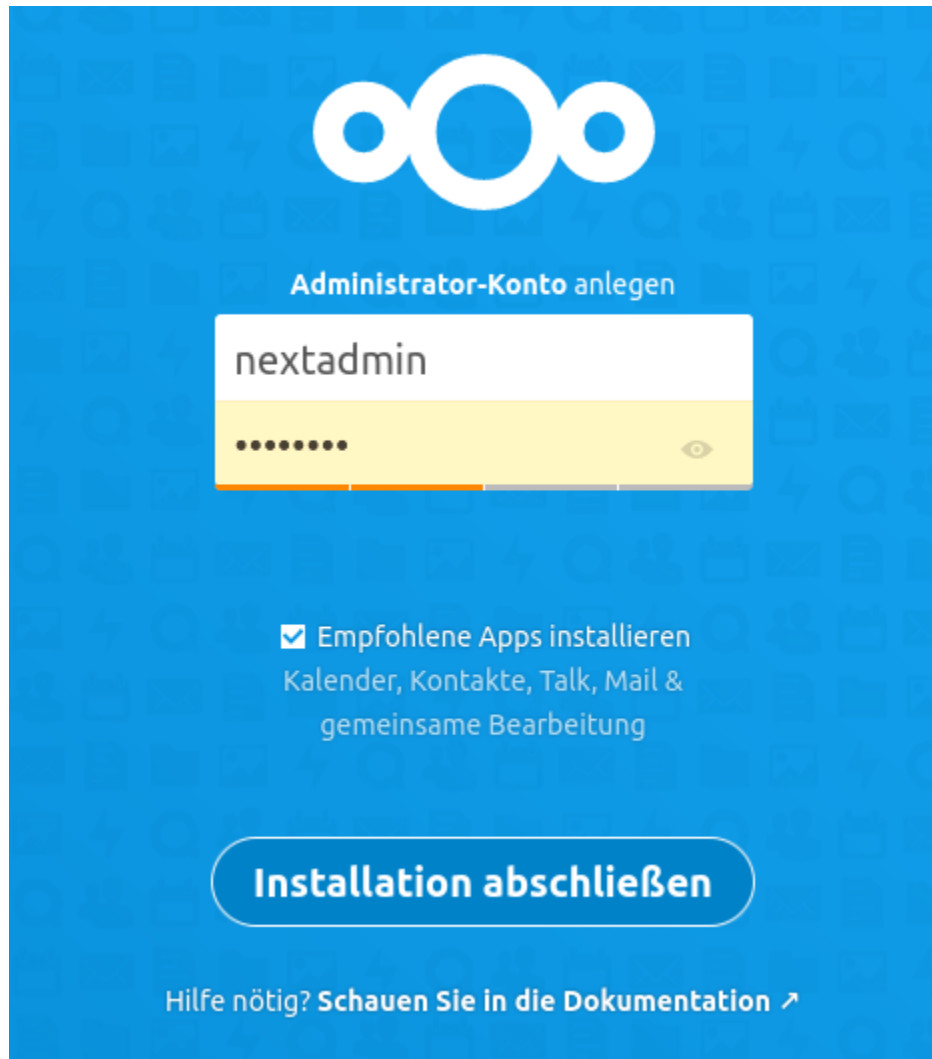
Das Verzeichnis `/var/www/html` des Webservers wird unter dem Verzeichnis `/srv/docker/nextcloud/nextcloud` auf dem Docker-Host abgelegt. Und das Datenverzeichnis `/var/lib/mysql` der Maria Datenbank wird unter dem Verzeichnis `/srv/docker/nextcloud/db` auf dem Docker-Host abgelegt.

Sollte für nginx noch eine `default.conf` aktiv sein, so findet sich diese im Verzeichnis `/srv/docker/nextcloud` als symbolischer Link. Diesen kannst Du löschen und nginx wie zuvor neu starten.

Damit sind alle Daten im Verzeichnis `/srv/docker/nextcloud`.

Wenn Du im Verzeichnis `/srv/docker/nextcloud` bist, startest Du die Nextcloud mit `docker-compose up -d --build`.

Jetzt must Du mit einem Browser die Startseite `https://nextcloud.meine-schule.de` Deiner neuen Nextcloud aufrufen und einen Benutzernamen und ein Passwort für den Nextcloud-admin angeben.



Nextcloud-App: Einstellungen

Da die Nextcloud hinter dem nginx-Proxy liegt und nicht weiß, ob die Benutzer die Nextcloud über http oder https aufrufen, wird eine Anmeldung über eine Nextcloud-Client-App scheitern. Mit einem Eintrag in `/srv/docker/nextcloud/nextcloud/config/config.php` kannst Du das Problem lösen:

```
...
'ldapProviderFactory' => 'OCA\User_LDAP\LDAPProviderFactory',
# Das ist der Eintrag #####
'overwriteprotocol' => 'https',
#####
);
```


Nextcloud: Hinweise config.php

Melde Dich an der Nextcloud als admin an und wähle links unter Verwaltung -> Übersicht aus. Es erscheinen ggf. Sicherheits- & Einrichtungswarnungen.

Solltest Du hier einen Hinweis auf eine fehlende default phone region sehen, so kannst Du in der config.hphp den Eintrag 'default_phone_region' => 'DE', ergänzen.

Nachstehendes Code-Beispiel der Datei /srv/docker/nextcloud/nextcloud/config/config.php zeigt, wo dieser Eintrag neben anderen Ergänzungen plaziert werden kann.

```
'htaccess.RewriteBase' => '/',
'memcache.local' => '\\OC\\Memcache\\APCu',
'auth.bruteforce.protection.enabled' => true,
'blacklisted_files' =>
array (
    0 => '.htaccess',
    1 => 'Thumbs.db',
    2 => 'thumbs.db',
),
'cron_log' => true,
'default_phone_region' => 'DE',
'enable_previews' => true,
'enabledPreviewProviders' =>
array (
    0 => 'OC\\Preview\\PNG',
    1 => 'OC\\Preview\\JPEG',
    2 => 'OC\\Preview\\GIF',
    3 => 'OC\\Preview\\BMP',
    4 => 'OC\\Preview\\XBitmap',
    5 => 'OC\\Preview\\Movie',
    6 => 'OC\\Preview\\PDF',
    7 => 'OC\\Preview\\MP3',
    8 => 'OC\\Preview\\TXT',
    9 => 'OC\\Preview\\MarkDown',
),
'filesystem_check_changes' => 0,
'filelocking.enabled' => 'true',
'filelocking.ttl' => 3600,
'integrity.check.disabled' => false,
'apps_paths' =>
...

```

Danach ist der Docker-Container erneut zu starten:

4.42.5 Externe Authentifizierung - Nextcloud

Autor des Abschnitts: @cweikl, @rettich

Eine Nextcloud-Instanz kann extern oder intern betrieben werden. Hierbei kann diese so konfiguriert werden, dass das Active Directory (AD) der linuxmuster.net 7 als zentrale Authentifizierungsinstanz genutzt wird.

Nachstehende Konfigurationsschritte sind auf der Nextcloud-Instanz auszuführen.

App installieren

Um via LDAP eine Authentifizierung vornehmen zu können, musst Du zuerst oben rechts als admin auf Dein Profil-Icon klicken, dann auf Apps. Es erscheinen links im Menü die Einträge Deine Apps, Aktive Apps, Deaktivierte Apps, App-Pakete. Klicke auf deaktivierte Apps und wähle dort die App LDAP user and group backend aus und aktiviere diese.

Danach klickst Du wieder oben rechts als admin auf Dein Profil-Icon und klickst danach auf Einstellungen. Danach klickst Du links im Menü Verwaltung den Eintrag LDAP/AD Integration.

Die nachstehenden Schritte führst Du dann dort entsprechend aus.

Einstellungen: Server

Hinweis: Die Einstellungen kannst Du schrittweise testen (z.B. Base-DN testen). Hier musst Du ggf. mehrfach den Test durchführen, bevor eine erfolgreiche Bestätigung erfolgt. Z.T. werden vier Versuche - trotz korrekter Einstellungen - benötigt.

Sollte der Nextcloud-Server extern betrieben werden, so muss die OPNsense®-Firewall so konfiguriert werden, dass Anfragen über den LDAPS-Port 636 an den Server weitergeleitet werden. Siehe [Firewallregeln](#).

In der Konfigurationsoberfläche ist unter Firewall -> NAT -> Portweiterleitung eine entsprechende Regel anzulegen.

Bind-User

Achtung: Grundsätzlich sollten alle externen Dienste, die via LDAP an das AD angebunden werden, mit einem eigens dafür angelegten Bind-User genutzt werden. Für Nextcloud sollte so z.B. ein Benutzer nextcloud-binduser angelegt werden, der für die Verbindung zum AD genutzt wird. Hinweise hierzu findest Du unter <https://github.com/linuxmuster/sophomorix4/wiki/bindusers>

Vorgehen zur Anlage eines neuen Bind-Users

1. Auf dem linuxmuster.net Server folgenden Befehl in der Konsole als Benutzer root absetzen, um einen neuen Benutzer (nextcloud-binduser) für den Bind-Zugriff zu definieren. Das zufällig erzeugte Kennwort wird in einer Datei auf dem Server hinterlegt.

```
# sophomorix-admin --create-school-binduser nextcloud-binduser --school default-school --  
↪ random-passwd-save
```

2. Gib für den neu angelegten Benutzer einen Kommentar an, um später einen Hinweis zu erhalten, für welchen Zweck der Benutzer genutzt wird.

```
# sophomorphix-user -u nextcloud-binduser --comment "AD access from nextcloud"
```

3. Lasse nun die Daten für den neu angelegten Benutzer anzeigen, die dann in den Nextcloud-Einstellungen als bind-user einzutragen sind.

```
# sophomorphix-admin -i -a nextcloud-binduser
```

4. Trage auf dem Nextcloud-Server im Konfigurationsmenü die Daten wie in nachstehender Abb. ein. Ändere dabei aber den Bind-User von global-binduser in den neu angelegten Bind-User z.B. nextcloud-binduser:

Trage auf dem Nextcloud-Server im Konfigurationsmenü folgende Werte ein:

Sollte der Nextcloud Server extern betrieben werden, so ist als URL für den LDAP-Server eine Adresse nach diesem Schema anzugeben: `ldaps://hostname.subdomain.domain.topleveldomain` - z.B. `ldaps://nextcloud.schule.meineschule.de`. Als Port ist dann 636 einzutragen, um eine gesicherte Verbindung aufzubauen.

Für den binduser ist die Domäne anzupassen, so dass mit o.g. Beispiel die Eintragungen dort wie folgt aussehen könnten:

```
CN=nextcloud-binduser,OU=Management,OU=GLOBAL,DC=schule,DC=meineschule,DC=de
```

In der Zeile darunter ist das Kennwort des binduser einzutragen. Dieses Passwort des neuen Bind-Users erhältst Du mit dem Befehl unter 3., den Du auf dem linuxmuster.net Server absetzen musst. Das Passwort trägst Du hier ein.

Als Base-DN trägst Du `OU=default-school,OU=SCHOOLS`, gefolgt von Deiner Domain (z.B. `DC=schule,DC=meineschule,DC=de`) ein.

Solltest Du auf Deinem Sever ein self-signed certificate verwenden, so sind die Einstellungen unter Fortgeschritten -> Verbindungseinstellungen wichtig, die später in dieser Dokumentation dargestellt werden.

Einstellungen: Benutzer

Wenn Du mit einem Tool wie Apache Directory Studio die Attribute eines Lehrer-Accounts anschaust, siehst Du, dass Du sie an zwei Attributen erkennst: `objectClass=person` und `sophomorphixRole=teacher`.

Bei Schüler-Accounts ist `sophomorphixRole=student`.

Daraus ergibt sich die Filterregel:

```
(&(objectClass=person)
(|(sophomorphixRole=teacher)
(sophomorphixRole=student)))
```

Trage also unter Benutzer in die LDAP-Abfrage folgendes ein:

```
(&(objectClass=person)(|(sophomorphixRole=teacher)(sophomorphixRole=student)))
```

Um den Zugriff auf die Nextcloud auf Lehrer zu begrenzen, ist unter Benutzer diese LDAP-Abfrage einzutragen.

```
(&(objectClass=person)(sophomoxRole=teacher))
```

Anmelde-Attribute

Bei der Anmeldung suchen wir den Eintrag, bei dem zusätzlich `samaccountname=%uid` gilt. In dem Fall ist `%uid` der Benutzername, den wir bei der Anmeldung eingeben.

Nehme folgende Einstellungen vor:

```
(&(objectClass=person)(sAMAccountName=%uid))
```

Einstellungen: Gruppe

Wir wollen nicht die Gruppen `attic` und `wificlass`. Aber wir wollen Schüler, Lehrer, Projekte und alle Untergruppen der Gruppe `students`.

```

(&(objectClass=group)
  (
    (
      (&(cn=attic)
        (&(cn=wificlass)
          )
        )
      )
    (
      (&(cn=teachers)
        (&(cn=role=student)
          (memberOf=CN=students,OU=Students,OU=default-school,OU=SCHOOLS,DC=linuxmuster,DC=lan)
          (&(sophomoxRole=project)
            )
          )
        )
      )
    )
  )
)

```

Nehme folgende Einstellungen vor:

```
(&(objectclass=group)(!(cn=attic)(cn=wificlass)))(cn=teachers)(cn=role-
↪ student)(memberof=CN=students,OU=Students,OU=default-school,OU=SCHOOLS,DC=linuxmuster,
↪ DC=lan)(sophomoriXType=project))
```

Die nachstehende Abfrage liefert nur die Gruppe der Lehrer:

```
(&(objectclass=group)(cn=teachers))
```

Einstellungen Experte

Klicke in dem Einstellungsmenü oben rechts auf den Eintrag **Experte** und trage nachstehende Werte ein:

LDAP / AD Integration

Trage dort folgenden Wert ein:

```
samaccountname
```

Einstellungen Fortgeschritten

Verbindungseinstellungen

Konfiguration aktiv ☒

Backup-Host (Kopie)

Port des Backup-Hosts (Kopie)

Hauptserver deaktivieren ☐

Schalten Sie die SSL-Zertifikatsprüfung aus. ☒

Speichere Time-To-Live zwischen

Setze eine Häkchen bei Konfiguration aktiv und, falls Dein Server mit einem selbstsigniertem Zertifikat arbeitet, auch bei Schalten Sie die SSL-Zertifikatsprüfung aus.

Ordnerseinstellungen

Feld für den Anzeigenamen des Benutzers

2. Benutzeranzeigename

Feld Basis-Benutzerbaum

Benutzersucheigenschaft

Feld für den Anzeigenamen der Gruppe

Feld Basis-Gruppenbaum

Gruppensucheigenschaft

Assoziation zwischen Gruppe und Benutzer

Dynamische Gruppenmitglied URL

Verschachtelte Gruppen ☐

Seitenstücke (Paging chunksize)

LDAP-Passwortänderungen pro Benutzer aktivieren ☐

(Das neue Passwort wurde als einfacher Text an LDAP gesendet)

Standard Passwort-Regeln DN

In Benutzersucheigenschaften gibst Du sn und givenName ein. So können Benutzer über ihren Vor- und Nachnamen gefunden werden.

Spezielle Eigenschaften

Kontingent-Feld

Standard-Kontingent

E-Mail-Feld

Benennungsregel für das Home-Verzeichnis des Benutzers

"\$home" Platzhalter-Feld

Im Feld Standard-Kontingent wird festgelegt, wie viel Speicher dem Benutzer auf der Nextcloud zur Verfügung steht. Da die Benutzer ihre Daten eigentlich auf dem Schulserver und nicht auf der Nextcloud speichern sollen, hältst Du diesen Wert eher klein.

Das "\$home"Platzhalter-Feld brauchst Du, wenn Du die Home-Verzeichnisse auch in der Nextcloud zur Verfügung stellen möchtest.

So, das war's. Sicherheitshalber gehst Du nochmal auf den Reiter Experte und klicks auf Lösche LDAP-Benutzernamenzuordnung und Lösche LDAP-Gruppenamenzuordnung.

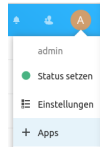
4.42.6 Zugriff auf die Home-Verzeichnisse

Autor des Abschnitts: @cweikl, @rettich

Die Benutzer können sich jetzt an der Nextcloud anmelden. Was noch fehlt ist, dass sie auf Ihre Daten auf dem Schulserver zugreifen können. Was Du nicht möchtest ist, dass die Benutzer Daten auf der Nextcloud ablegen, auf die sie von einem Rechner in der Schule keinen direkten Zugriff haben.

Aktivierung der App External storage support

Als erstes musst Du die App External storage support aktivieren.

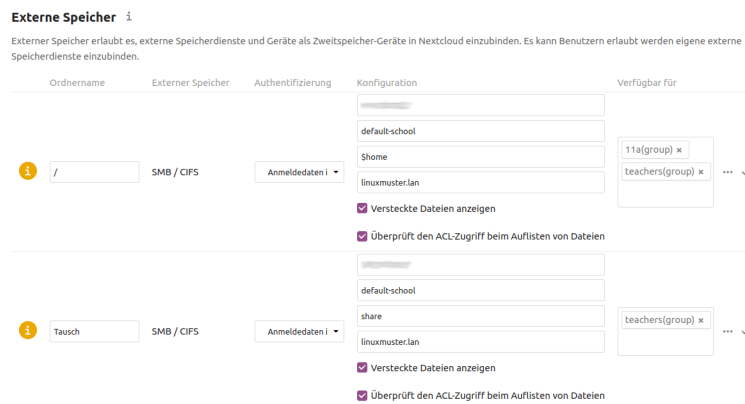


Gehe dazu auf A -> + Apps. Auf der Seite ganz unten findest Du die deaktivierten Apps. Aktiviere External storage support.

Einbindung der Home- und Tauschverzeichnisse

Sollte der Nextcloud-Server extern betrieben werden, so muss die OPNsense®-Firewall so konfiguriert werden, dass Anfragen über die SMB-Ports 139 und 445 an den Server weitergeleitet werden. Siehe [Firewallregeln](#).

In der Konfigurationsoberfläche ist unter Firewall -> NAT -> Portweiterleitung eine entsprechende Regel anzulegen.

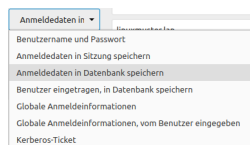


In den Einstellungen von Externer Speicher kannst Du jetzt, wie oben im Bild zu sehen ist, die Tauschverzeichnisse und das Home-Verzeichnis / der Benutzer einbinden.

Achtung: Das Share / ist das Wurzelverzeichnis der Benutzer. Wenn sich ein Benutzer nicht am Schulserver anmelden kann, kann er sich auch nicht an der Nextcloud anmelden. Und das trifft für den Admin der Nextcloud zu!!! Für den Share / müssen also die Gruppen angegeben werden, die Zugriff auf ein Home-Verzeichnis haben sollen. Sonst kann sich der Admin an der Nextcloud nicht mehr anmelden!!!

Wichtig: Du solltest das Share Tausch nicht für Schüler freigeben. Die Nextcloud registriert Änderungen nur dann, wenn ein Benutzer seine Dateien ändert, oder wenn die Nextcloud selbst teilt. Wenn Schüler oder Schülerinnen an

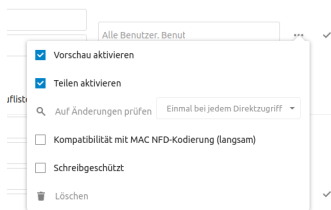
Dateien oder Verzeichnissen Änderungen vornehmen, wird die Desktop-App diese Änderungen bei anderen Benutzern nicht aktualisieren. Das passiert nicht, wenn Du als Lehrer über die Nextcloud diese Tauschverzeichnisse mit den Schülern/Gruppen teilst. Dann arbeitet die Desktop-App einwandfrei.



Achte darauf, dass Du **Anmeldedaten in Datenbank speichern** wählst.

Achtung: Bei Auswahl dieser Option ist zu beachten, dass die Anmeldedaten in der Datenbank symmetrisch verschlüsselt werden. Der Schlüssel dazu wird in der config.php hinterlegt. Dies kann ein Sicherheitsrisiko darstellen, wenn der Server kompromittiert worden sein sollte. Der bessere Weg wäre, die Option **Anmeldedaten in Sitzung speichern** dies hat aber andere Nebeneffekte, so dass die Einbindung nicht erfolgreich funktioniert.

Ob Du die Vorschau aktivierst oder nicht hängt vom Standort der Nextcloud ab. Ist die Nextcloud nicht in der Schule gehostet und ist Deine Internet-Verbindung eher langsam, so ist es besser, wenn Du den Haken bei **Vorschau aktivieren** nicht setzt.



Am Anfang scheint der Server noch langsam zu sein. Das liegt daran, dass die External Storage App einen Datei-Index aufbaut. Bei mir an der Schule hat das ca. 12 Stunden gedauert. Danach läuft die Nextcloud flott.

4.42.7 Das Online-Office Collabora

Autor des Abschnitts: @rettich

Collabora Online ist eine angepasste Version von LibreOffice Online, einem Online-Office, welches sich auf dem Docker-Host betreiben lässt.

Mit Collabora können beispielsweise in Moodle und Nextcloud gleichzeitig mehrer Benutzer an einem Dokument arbeiten. Mit Collabora hat man so auch auf Tablets oder Handys ein Office-Paket zur Verfügung.

Um Collabora auf dem Docker-Host zu installieren, sind die identischen Schritte wie bei der Nextcloud-Installation notwendig.

1. Erstellen eines Let's Encrypt - Zertifikats.
2. Erstellen einer Site für die Collabora in nginx.
3. Erstellen und Starten der Collabora App.

Hinweis: Im Folgenden musst Du natürlich `office.meine-schule.de` durch Deine URL ersetzen.

Erstellung des Zertifikats

Zuerst musst Du Dir einen Dienstenamen ausdenken, den DNS Eintrag dazu setzen und SSL-Zertifikat besorgen. Also z.B. office.meine-schule.de.

Dazu legst Du einen DNS Eintrag für Deine Dockerapp, z.B. office.meine-schule.de, der auf die IP des Docker-Hosts zeigt an. Das darf auch ein CNAME sein.

Trage diesen Host in die Datei `/etc/dehydrated/domains.txt` ein.

Führe den Befehl `dehydrated -c` aus. Jetzt hast Du die Zertifikate im Verzeichnis `/var/lib/dehydrated/certs/` zur Verfügung, der Docker-Host aktualisiert diese per Cronjob.

Erstellen einer Site für Collabora in nginx

Melde Dich als root auf Deinem Docker-Host an.

Erstelle mit `mkdir -p /srv/docker/collabora` das Verzeichnis, in das alle Collabora-Dateien abgelegt werden.

Erzeuge die Datei `office.nginx.conf` im Verzeichnis `srv/docker/collabora`.

```
server {
    listen 80;
    listen [::]:80;
    server_name office.meine-schule.de;

    location ^~ /.well-known/acme-challenge {
        alias /var/www/dehydrated;
    }
}

server {
    listen 443 ssl;
    server_name office.meine-schule.de;
    add_header X-XSS-Protection "1; mode=block"; #Wenn es nicht geht, notfalls
↳ deaktivieren

    ssl_certificate /var/lib/dehydrated/certs/office.meine-schule.de/fullchain.pem;
    ssl_certificate_key /var/lib/dehydrated/certs/office.meine-schule.de/privkey.pem;

# static files
    location ^~ /browser {
        proxy_pass https://127.0.0.1:9980;
        proxy_set_header Host $http_host;
    }

# WOPI discovery URL
    location ^~ /hosting/discovery {
        proxy_pass https://127.0.0.1:9980;
        proxy_set_header Host $http_host;
    }

# Capabilities
    location ^~ /hosting/capabilities {
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
    proxy_pass https://127.0.0.1:9980;
    proxy_set_header Host $http_host;
}

# main websocket
location ~ ^/cool/(.*)/ws$ {
    proxy_pass https://127.0.0.1:9980;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection "Upgrade";
    proxy_set_header Host $http_host;
    proxy_read_timeout 36000s;
}

# download, presentation and image upload
location ~ ^/(c|l)ool {
    proxy_pass https://127.0.0.1:9980;
    proxy_set_header Host $http_host;
}

# Admin Console websocket
location ^~ /cool/adminws {
    proxy_pass https://127.0.0.1:9980;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection "Upgrade";
    proxy_set_header Host $http_host;
    proxy_read_timeout 36000s;
}
}
```

Diese conf-Datei geht davon aus, dass Dein Collabora auf localhost:9980 erreichbar sein wird. Den Port 9980 kannst Du wieder frei wählen. Der Port muss mit dem Port übereinstimmen, der in der docker-compose.yml später für collabora angegeben wird.

Jetzt musst Du noch im Verzeichnis /etc/nginx/sites-enabled einen Link auf Deine office.nginx.conf anlegen und nginx neu starten.

Melde Dich wieder als root am Docker-Host an und lege mit `ln -s /srv/docker/collabora/office.nginx.conf /etc/nginx/sites-enabled/office.meine-schule.de` den Link an.

So, jetzt musst Du nur noch mit `systemctl restart nginx.service` nginx neu starten.

Collabora mit docker-compose einrichten und starten

Du legst jetzt noch eine Datei docker-compose.yml an.

Alle Schritte sind jetzt im Verzeichnis `/srv/docker/collabora` durchzuführen.

Melde Dich wieder als root auf dem Docker-Host an und gehe mit `cd /srv/docker/collabora` in das Verzeichnis `/srv/docker/collabora`.

Die Datei docker-compose.yml

```
version: '2.2'

services:
  collabora:
    image: collabora/code
    restart: always
    ports:
      - 127.0.0.1:9980:9980
    cap_add:
      - MKNOD
    environment:
      - domain=[a-z]*+.meine-schule.de
      - username=admin
      - password=Stgy3431
      - VIRTUAL_HOST=office.meine-schule.de
      - VIRTUAL_NETWORK=proxy-ssl
      - VIRTUAL_PORT=9980
      - VIRTUAL_PROTO=https
      - ssl.enable=false
      - ssl.termination=true
```

Der Eintrag `- domain=[a-z]*+.meine-schule.de` bewirkt, dass alle Rechner in der Domäne `meine-schule.de` Zugriff auf den Collabora-Service haben.

Möchtest Du, dass nur `nextcloud.meine-schule.de` Zugriff auf den Collabora-Service hat, muss der Eintrag `- domain=nextcloud.meine-schule.de` lauten.

Wenn Du im Verzeichnis `/srv/docker/collabora` bist, startest Du Collabora mit `docker-compose up -d`.

Collabora updaten

Fall Du feststellst, dass die Collabora-Version, die Du gerade benutzt, nicht mehr aktuell ist, meldest Du Dich wieder als root auf dem Docker-Host an und gehst mit `cd /srv/docker/collabora` in das Verzeichnis `/srv/docker/collabora`. Dann beendest Du mit `docker-compose down` Collabora. Mit `docker-compose pull` holst Du Dir das aktuelle Image und mit `docker-compose up -d` startest Du Dein aktualisiertes Collabora wieder.

Collabora in der Nextcloud nutzen

Als erstes musst Du die App Collabora Online aktivieren. Gehe dazu auf **A -> + Apps**. Auf der Seite ganz unten findest Du die deaktivierten Apps. Aktiviere Collabora Online.

Navigiere links zu **Verwaltung -> Einstellungen -> Collabora Online Development Edition** und trage dort unter **Verwende Deinen eigenen Server** die URL Deines Collabora-Services ein.

Collabora Online

Collabora Online ist eine leistungsstarke LibreOffice-basierte Online-Office-Suite mit kollaborativer Bearbeitung, die alle wichtigen Dokumenten-, Tabellen- und Präsentationsdateiformate unterstützt und mit allen modernen Browsern zusammenarbeitet.

☒ Collabora Online Server ist erreichbar.

☒ Verwenden Sie Ihren eigenen Server

Collabora Online benötigt einen separaten Server, der als WOPI-ähnlicher-Client fungiert, um Bearbeitungsfunktionen bereitzustellen.

URL (und Port) des Collabora Online-Servers

Save

☐ Zertifikatsüberprüfung deaktivieren (unsicher)

Hinweis: Achte darauf, dass Du Deine <https://<deineurl>> angibst, damit Collabora auch via https erreichbar ist.

Damit ist die Einrichtung abgeschlossen und Du kannst Nextcloud für Deine Schule weiter anpassen.

Unter <https://office.meine-schule.de/browser/dist/admin/admin.html> erreichst Du die Monitoring-Oberfläche von Collabora.

4.43 Externe Authentifizierung - Aleksis

Autor des Abschnitts: @supergamer

Aleksis ist eine Schulische Informationsplattform, die als Open-Source Software entwickelt wurde. alexis.org

Folgende Funktionen bietet Aleksis an:

- Stundenplan Verwaltung
- Vertretungsplan
- Digitales Klassenbuch
- Sitzpläne
- Info Dashboard (z.B. für Bildschirme)
- Bücherei Verwaltung

4.43.1 Voraussetzungen

Diese Dokumentation setzt voraus, dass eine Aleksis Instanz eingerichtet wurde mit der direkten Installationsmethode.

Die Dokumentaion für die LDAP Anbindung der Docker Variante erfolgt noch.

Eine Installationsanleitung für Aleksis ist hier zu finden: [Installation Aleksis](#)

Außerdem muss auf der Aleksis Instanz dieser Installationsbefehl ausgeführt werden um alle nötigen LDAP Pakete zu installieren.

```
# sudo apt install python3-ldap libldap2-dev libssl-dev libsasl2-dev python3-dev
```

4.43.2 LDAP-Anbindung

Verbindungseinstellungen

Sind die benötigten LDAP Pakete installiert muss die LDAP Konfiguration in der Aleksis Konfigurationsdatei angepasst / erstellt werden.

```
# nano /etc/aleksis/aleksis.toml
```

```
[ldap]
uri = "ldap://server.linuxmuster.lan:389"
bind = { dn = "cn=global-binduser,OU=Management,OU=GLOBAL,dc=linuxmuster,dc=lan", ↵
↵password = "GLOBAL-BINDUSER-PASSWORT" }

[ldap.users]
search = { base = "ou=default-school,ou=schools,dc=linuxmuster,dc=lan", filter = "(&
↵(|(memberof=CN=role-student,OU=Groups,OU=GLOBAL,DC=linuxmuster,DC=lan)(memberof=C>map↵
↵= { first_name = "givenName", last_name = "sn", email = "mail", username=
↵"samaccountname" }

[ldap.groups]
search = { base = "OU=default-school,OU=SCHOOLS,DC=linuxmuster,DC=lan", filter="(&
↵(|(memberOf=CN=students,OU=Students,OU=default-school,OU=SCHOOLS,DC=linuxmuster,DC=>
↵type = "groupOfNames"
# Users in group "admins" are superusers
#flags = { is_superuser = "cn=admins,ou=groups,dc=myschool,dc=edu" }
```

Die uri muss natürlich auf die jeweilige Schule mit dem entsprechenden Domain Namen angepasst werden ebenso bei search

Sollte die Aleksis Instanz extern betriebe werden. Ist es dringend empfohlen den Port 636 für LDAPs zu verwenden außerdem bei uri statt ldap: ebenfalls ldaps einzutragen.

Als nächstes wechselt man in die Aleksis Weboberfläche und wechselt auf der linken Seite auf Admin und dann auf LDAP

Dort ändert man folgende Werte:

LDAP-Synchronisation aktivieren	Haken setzen
Fehlende Personen für LDAP-Benutzer erstellen	Haken setzen
LDAP-Benutzer bei der Anmeldung synchronisieren	Haken setzen
LDAP-Synchronisation von Gruppen aktivieren	Haken setzen
Feld für den Kurznamen der Gruppe	cn
LDAP-Synchronisation für passende Felder durchführen	UID
Abgleich-Modus für die LDAP-Synchronisation	Alle Felder müssen passen
LDAP-Passwort bei ALEKSiS-Passwortänderung ändern	Haken entfernen
Admin-Konto nutzen, um Passwörter zu ändern	Haken entfernen
LDAP field for ‚First name‘ on core.Person	givenName
LDAP field for ‚Last name‘ on core.Person	sn
LDAP sync matching fields	nur first_name & last_name auswählen

Alle anderen Felder sollten leer bleiben

Am Ende die Einstellungen mit **EINSTELLUNGEN** **SPEICHERN** bestätigen.

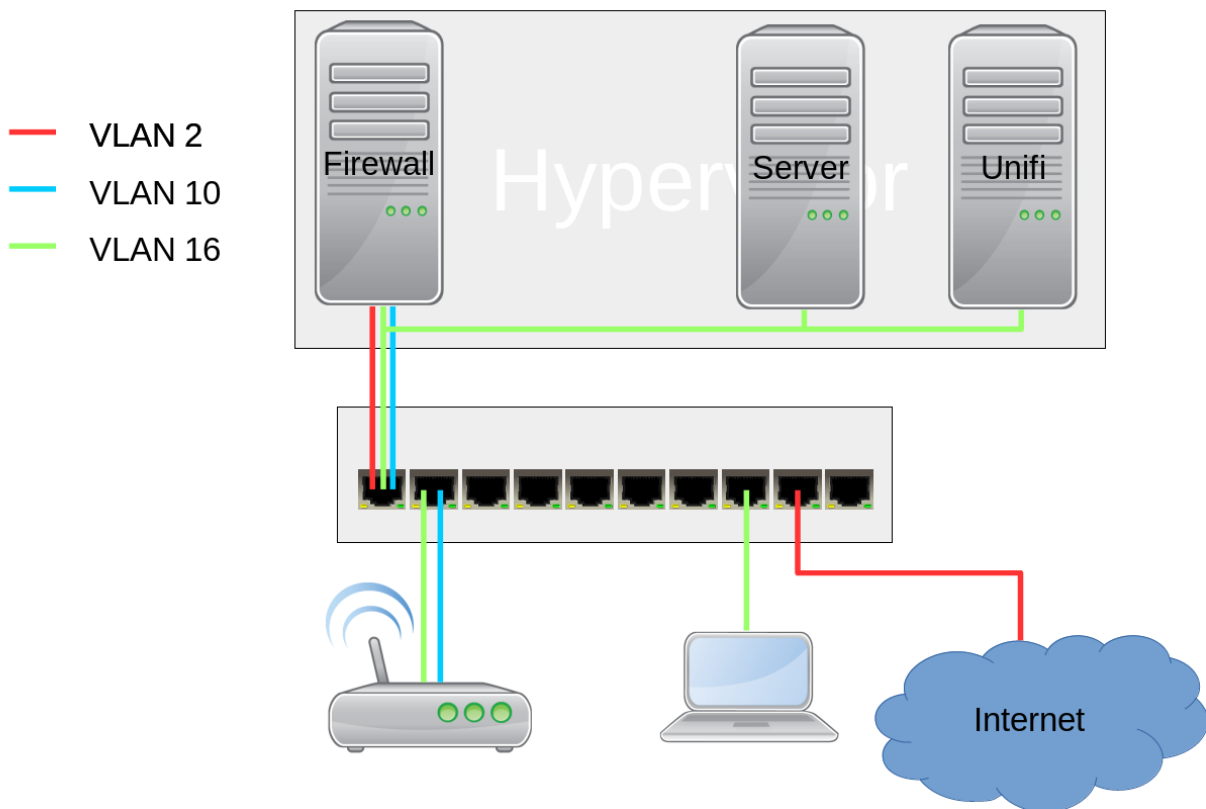
Jetzt sollte der Benutzer in der Lage sein sich anzumelden. Die LDAP Anbindung ist hiermit abgeschlossen.

4.44 Unifi-WLAN-Lösung für linuxmuster.net

Autor des Abschnitts: @rettich

Eine WLAN-Lösung für Schulen sollte mindestens zwei WLAN-Netze aufspannen.

- Das Lehrernetz für schuleigene Geräte, wie Beamer, Laptops oder Chromecasts, und für private Geräte der Lehrer, die auf Beamer und Chromecasts zugreifen wollen.
- Das Schülernetz für Schüler.



In der hier vorgestellten Lösung kommen Accesspoints von Unifi und der kostenlose Unifi-Controller zum Einsatz.

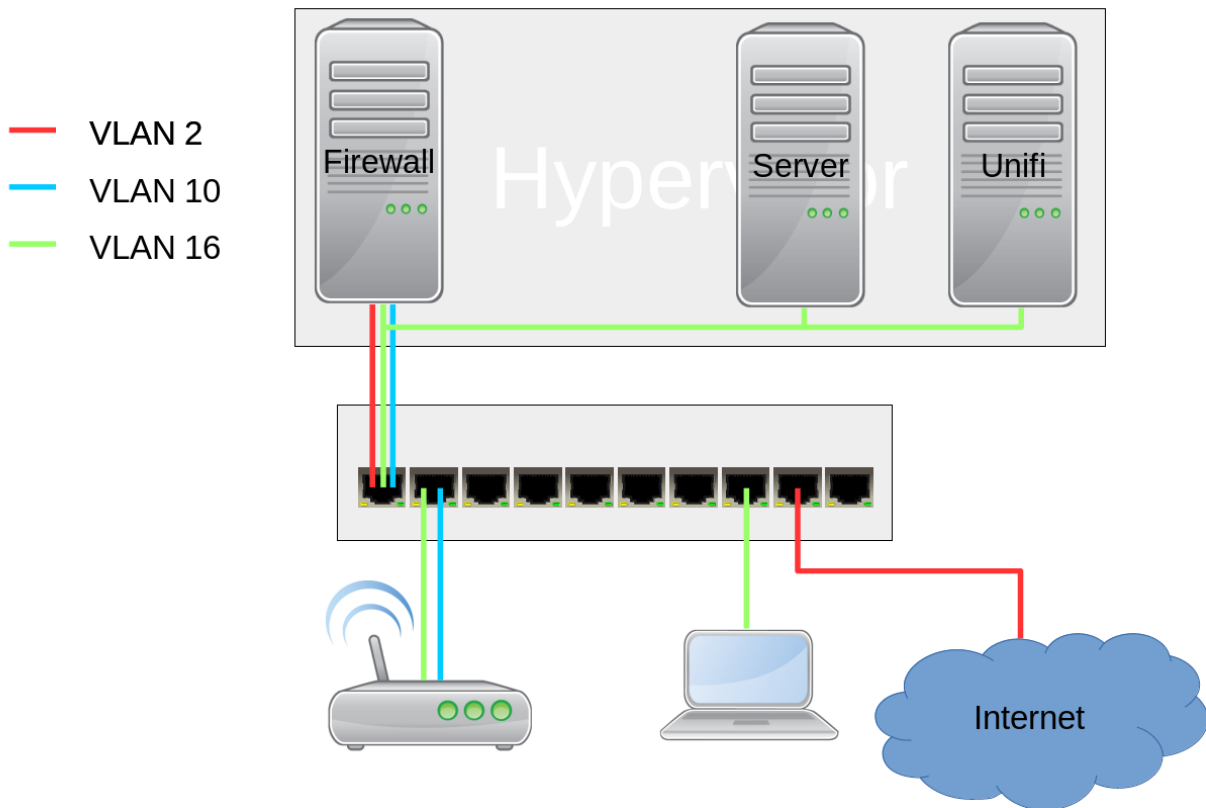
Die Geräte im Lehrernetz werden in die Datei `/etc/linuxmuster/sophomorix/default-school/devices.csv` aufgenommen. Das Lehrernetz ist ein Teil des Schulnetzes. Damit können sich beispielsweise Benutzer mit einem Schullaptop per WLAN wie gewohnt anmelden und auf ihre Daten zugreifen.

Im Schülernetz müssen sich die Benutzer für das WLAN mit ihrem Benutzernamen und Kennwort anmelden. Über die Schulkonsole kann einem Schüler oder einer Gruppe von Schülern das WLAN freigeschaltet oder gesperrt werden. Eine Verwaltung der Benutzergeräte durch den Netzwerkberater entfällt.

Inhalt:

4.44.1 Die Netztopologie

Sollen 2 WLANs über einen Accesspoint (AP) ausgestrahlt werden, muss mindestens ein Netzwerk ein getaggttes VLAN sein.



Im Beispiel ist der Hypervisor (z.B. Proxmox) mit einem Netzkabel mit dem Switch verbunden.

Die virtuellen Maschinen sollten somit nicht direkt mit der Netzwerkkarte des Hypervisors verbunden sein. Es muss noch zusätzlich die VLAN-ID angegeben werden.

Im Beispiel werden die Datenpakete des Unifi-Controllers mit der Nummer 16 gekennzeichnet. Man sagt getaggt.

Bearbeite: Netzwerkkarte

☒ Bridged mode

VLAN Tag:

Bridge:

Firewall: ☐

☐ NAT mode

Modell:

MAC-Adresse:

Rate limit (MB/s):

Multiqueues:

Trennen: ☐

[? Help](#) [OK](#) [Reset](#)

4.44.2 Der Switch

In der hier vorgestellten Lösung wird ein Cisco SG300-10 Switch verwandt. Die Überlegungen lassen sich aber leicht auf andere Switches übertragen.

Grundsätzliches

Bei vielen Switches ist es unmöglich, sich komplett auszusperren. Der SG300 hat die Konfigurationsspeicher *Ausgeführte Konfiguration* und *Startkonfiguration*.

In die *Ausgeführte Konfiguration* werden alle Einstellungen gespeichert, die Du vornimmst. Bei einem Neustart wird als erstes die *Startkonfiguration* in die *Ausgeführte Konfiguration* kopiert und dann die *Ausgeführte Konfiguration* ausgeführt.

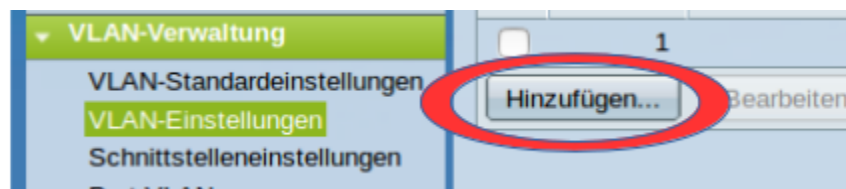
Wenn Du sich also mit einer Einstellung ausgeschlossen hast, starte den Switch einfach neu und Du hast den zuletzt in die *Startkonfiguration* gespeicherten Stand.

Sobald Du eine Einstellung vorgenommen hast, die Dich nicht aussperrt, siehst Du oben neben dem Benutzernamen einen Link zum Speichern der *Aktuellen Konfiguration* in die *Startkonfiguration*.



VLANs anlegen

Das VLAN für den Internetzugang hat die VLAN-ID 2, das Schüler-WLAN die VLAN-ID 10 und das Schulnetz die VLAN-ID 16.



Wähle VLAN-Verwaltung -> VLAN-Einstellungen und klicken auf *Hinzufügen*.

Es öffnet sich ein Dialogfenster, mit dem Du die VLANs hinzufügen kannst.

VLAN hinzufügen - Mozilla Firefox

https://192.168.0.130/cs3ca8f581/Vmember/bridg_vlan_properties_a.htm 110%

VLAN

VLAN-ID: (Bereich: 2 - 4094)

VLAN-Name: (8/32 verwendete Zeichen)

VLAN-Schnittstellenstatus: ☒ Aktivieren

Leitungsstatus SNMP-Traps: ☒ Aktivieren

☐ Bereich

VLAN-Bereich: - (Bereich: 2 - 4094)

Übernehmen **Schließen**

Füge die VLANs wie im Bild hinzu.

Administration

Portverwaltung

Smartport

VLAN-Verwaltung

VLAN-Standardeinstellungen

VLAN-Einstellungen

Schnittstelleneinstellungen

Port-VLAN

Port-VLAN-Mitgliedschaft

VLAN-Tabelle

<input type="checkbox"/>	VLAN-ID	VLAN-Name	Ersteller	VLAN-Schnittstellenstatus	Leitungsstatus SNMP-Traps
<input type="checkbox"/>	1		Standard	Aktiviert	Aktiviert
<input type="checkbox"/>	2	Internet	Statisch	Deaktiviert	Aktiviert
<input type="checkbox"/>	10	Schüler-WLAN	Statisch	Deaktiviert	Aktiviert
<input type="checkbox"/>	16	Schulnetz	Statisch	Deaktiviert	Aktiviert

Hinzufügen...

Bearbeiten...

Entfernen

Sobald alle VLANs hinzugefügt sind, schließe das Fenster. Die VLANs sollten jetzt aufgeführt sein.

Jetzt wäre ein guter Zeitpunkt, um die *Ausgeführte Konfiguration* zu speichern.

Ausgeschlossen, Getaggt, Ungetaggt und PVID

Für jeden Switchport und für jedes VLAN muss festgelegt werden, ob das VLAN mit der VLAN-ID x ausgeschlossen, getaggt akzeptiert oder Datenpakete, die mit der VLAN-ID x getaggt sind, ungetaggt weitergeleitet werden.

Ausgeschlossen:

Datenpakete, die mit der VLAN-ID x getaggt sind, werden verworfen.

Getaggt:

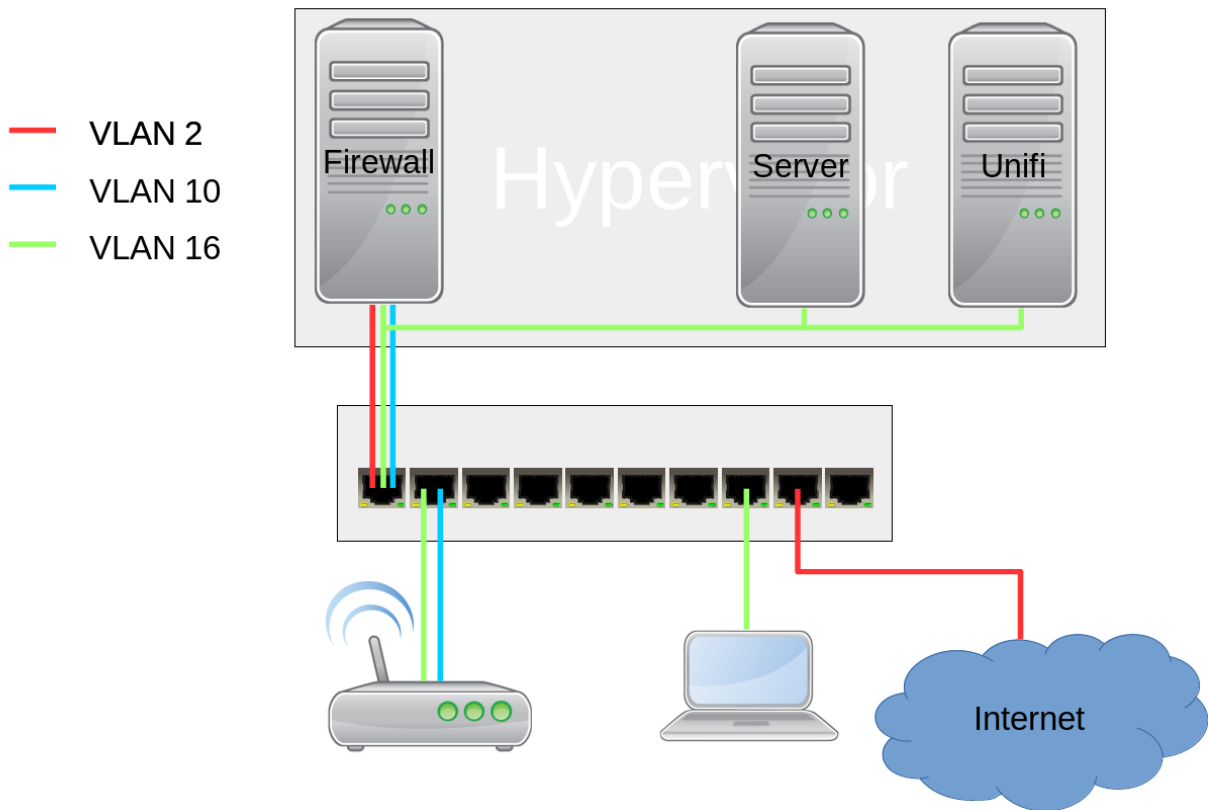
Datenpakete, die mit der VLAN-ID x getaggt sind, werden weitergeleitet.

Ungetaggt:

Von Datenpaketen, die mit der VLAN-ID x getaggt sind, wird die VLAN-ID entfernt und zum Client weitergeleitet. Die meisten Clients können mit getaggtten Datenpaketen nichts anfangen.

PVID:

Bei einem Port, der mit der PVID x markiert ist, werden alle ungetaggten Datenpakete des Clients mit der VLAN-ID x getaggt.

Den Ports die VLANs zuweisen**Port 1:**

Der Hypervisor ist über ein Netzkabel mit Port 1 des Switches verbunden. Der Port 1 ist getaggt Mitglied der VLANs 2, 10 und 16.

Port 2-5:

Die APs sind im Schulnetz und werden über ein ungetaggt VLAN verwaltet. VLAN 16 ist ungetaggt und PVID ist 16.

Zusätzlich soll das Schüler-WLAN vom AP ausgestrahlt werden. Um es vom Schulnetz zu trennen, muss es getaggt am AP ankommen. VLAN 10 ist getaggt.

Port 7-8:

Die Clients sind nur im Schulnetz und arbeiten mit ungetaggt Datenpaketen. VLAN 16 ist ungetaggt und PVID ist 16.

Port 9:

Auch der Router arbeitet mit ungetaggt Datenpaketen. VLAN 2 ist ungetaggt und PVID ist 2.

Port 10:

Über diesen Port wird der Switch gemanaged. Er ist das einzige Mitglied des Standard VLAN 1. Damit ist der Switch weder über das WLAN noch über das Schulnetz managebar.

Schritt für Schritt

Wähle VLAN-Verwaltung -> Port-VLAN.

VLAN-Mitgliedschaftstabelle

Filtern: VLAN-ID ist gleich

UNDSchnittstellentyp ist gleich

Schnittstellename	VLAN-Modus	Mitgliedschaftstyp	PVID
GE1	Trunk	<input type="text" value="Ungetaggt"/>	<input checked="" type="checkbox"/>
GE2	Trunk	<input type="text" value="Ungetaggt"/>	<input checked="" type="checkbox"/>
GE3	Trunk	<input type="text" value="Ungetaggt"/>	<input checked="" type="checkbox"/>
GE4	Trunk	<input type="text" value="Ungetaggt"/>	<input checked="" type="checkbox"/>
GE5	Trunk	<input type="text" value="Ungetaggt"/>	<input checked="" type="checkbox"/>
GE6	Trunk	<input type="text" value="Ungetaggt"/>	<input checked="" type="checkbox"/>
GE7	Trunk	<input type="text" value="Ungetaggt"/>	<input checked="" type="checkbox"/>
GE8	Trunk	<input type="text" value="Ungetaggt"/>	<input checked="" type="checkbox"/>
GE9	Trunk	<input type="text" value="Ungetaggt"/>	<input checked="" type="checkbox"/>
GE10	Trunk	<input type="text" value="Ungetaggt"/>	<input checked="" type="checkbox"/>

In der Grundeinstellung ist für jeden Port VLAN 1 ungetaggt und PVID 1 eingestellt.

Da der Switch nur über den Port 1 verwaltet wird, verbiete den Ports 1 bis 9 die Mitgliedschaft zu VLAN 1 und bestätige anschließend mit *Übernehmen*. Man beachte, dass dabei PVID 1 automatisch gelöscht wird.

Nun wähle die VLAN-ID 2 und klicken auf *Los*.

Für Port 1 wähle getaggt und für Port 9 Ungetaggt. Dabei wird PVID automatisch selektiert.

Jetzt ist VLAN 10 an der Reihe.

Für die Ports 1 bis 5 wählst Du getaggt.

Und schließlich noch VLAN 16.

Da die APs und die Clients im Schulnetz sind, sind die Ports 2 bis 8 ungetaggt und PVID ist gesetzt.

Über *VLAN-Verwaltung -> Port-VLAN-Mitgliedschaft* erhält man eine Zusammenfassung.

Jetzt wäre ein guter Zeitpunkt zum Speichern der Konfiguration.

Administration

Portverwaltung

Smartport

VLAN-Verwaltung

VLAN-Standardeinstellungen

VLAN-Einstellungen

Schnittstelleneinstellungen

Port-VLAN

Port-VLAN-Mitgliedschaft

Private VLAN-Einstellungen

GVRP-Einstellungen

VLAN-Gruppen

Voice-VLAN

Zugriffsport-Multicast-TV-VLAN

Kundenport-Multicast-TV-VLAN

Spanning Tree

MAC-Adresstabellen

Multicast

VLAN-Mitgliedschaftstabelle

Filtern: VLAN-ID ist gleich

UNDSchnittstellentyp ist gleich

Schnittstellenname	VLAN-Modus	Mitgliedschaftstyp	PVID
GE1	Trunk	<input type="text" value="Getaggt"/>	<input type="checkbox"/>
GE2	Trunk	<input type="text" value="Ausgeschlosse"/>	<input type="checkbox"/>
GE3	Trunk	<input type="text" value="Ausgeschlosse"/>	<input type="checkbox"/>
GE4	Trunk	<input type="text" value="Ausgeschlosse"/>	<input type="checkbox"/>
GE5	Trunk	<input type="text" value="Ausgeschlosse"/>	<input type="checkbox"/>
GE6	Trunk	<input type="text" value="Ausgeschlosse"/>	<input type="checkbox"/>
GE7	Trunk	<input type="text" value="Ausgeschlosse"/>	<input type="checkbox"/>
GE8	Trunk	<input type="text" value="Ausgeschlosse"/>	<input type="checkbox"/>
GE9	Trunk	<input type="text" value="Ungetaggt"/>	<input checked="" type="checkbox"/>
GE10	Trunk	<input type="text" value="Ausgeschlosse"/>	<input type="checkbox"/>

Smartport

VLAN-Verwaltung

VLAN-Standardeinstellungen

VLAN-Einstellungen

Schnittstelleneinstellungen

Port-VLAN

Port-VLAN-Mitgliedschaft

Private VLAN-Einstellungen

GVRP-Einstellungen

VLAN-Gruppen

Voice-VLAN

Zugriffsport-Multicast-TV-VLAN

Kundenport-Multicast-TV-VLAN

Spanning Tree

MAC-Adresstabellen

Multicast

IP-Konfiguration

Sicherheit

Zugriffssteuerung

VLAN-Mitgliedschaftstabelle

Filtern: VLAN-ID ist gleich

UNDSchnittstellentyp ist gleich

Schnittstellenname	VLAN-Modus	Mitgliedschaftstyp	PVID
GE1	Trunk	<input type="text" value="Getaggt"/>	<input type="checkbox"/>
GE2	Trunk	<input type="text" value="Getaggt"/>	<input type="checkbox"/>
GE3	Trunk	<input type="text" value="Getaggt"/>	<input type="checkbox"/>
GE4	Trunk	<input type="text" value="Getaggt"/>	<input type="checkbox"/>
GE5	Trunk	<input type="text" value="Getaggt"/>	<input type="checkbox"/>
GE6	Trunk	<input type="text" value="Ausgeschlosse"/>	<input type="checkbox"/>
GE7	Trunk	<input type="text" value="Ausgeschlosse"/>	<input type="checkbox"/>
GE8	Trunk	<input type="text" value="Ausgeschlosse"/>	<input type="checkbox"/>
GE9	Trunk	<input type="text" value="Ausgeschlosse"/>	<input type="checkbox"/>
GE10	Trunk	<input type="text" value="Ausgeschlosse"/>	<input type="checkbox"/>

Smartport

VLAN-Verwaltung

- VLAN-Standardeinstellungen
- VLAN-Einstellungen
- Schnittstelleneinstellungen
- Port-VLAN**
- Port-VLAN-Mitgliedschaft
- Private VLAN-Einstellungen
- GVRP-Einstellungen
- VLAN-Gruppen
- Voice-VLAN
- Zugriffsport-Multicast-TV-VLAN
- Kundenport-Multicast-TV-VLAN

Spanning Tree

MAC-Adresstabellen

Multicast

IP-Konfiguration

Sicherheit

Zugriffssteuerung

VLAN-Mitgliedschaftstabelle

Filtern: VLAN-ID ist gleich

UND Schnittstellentyp ist gleich

Schnittstellename	VLAN-Modus	Mitgliedschaftstyp	PVID
GE1	Trunk	Getaggt	<input type="checkbox"/>
GE2	Trunk	Ungetaggt	<input checked="" type="checkbox"/>
GE3	Trunk	Ungetaggt	<input checked="" type="checkbox"/>
GE4	Trunk	Ungetaggt	<input checked="" type="checkbox"/>
GE5	Trunk	Ungetaggt	<input checked="" type="checkbox"/>
GE6	Trunk	Ungetaggt	<input checked="" type="checkbox"/>
GE7	Trunk	Ungetaggt	<input checked="" type="checkbox"/>
GE8	Trunk	Ungetaggt	<input checked="" type="checkbox"/>
GE9	Trunk	Ausgeschlosse	<input type="checkbox"/>
GE10	Trunk	Ausgeschlosse	<input type="checkbox"/>

Portverwaltung

Smartport

VLAN-Verwaltung

- VLAN-Standardeinstellungen
- VLAN-Einstellungen
- Schnittstelleneinstellungen
- Port-VLAN
- Port-VLAN-Mitgliedschaft**
- Private VLAN-Einstellungen
- GVRP-Einstellungen
- VLAN-Gruppen
- Voice-VLAN
- Zugriffsport-Multicast-TV-VLAN
- Kundenport-Multicast-TV-VLAN

Spanning Tree

MAC-Adresstabellen

Multicast

IP-Konfiguration

Sicherheit

Tabelle für Port-VLAN-Mitgliedschaft

Filtern: Schnittstellentyp ist gleich

	Schnittstelle	Modus	Administrative VLANs	Betriebs-VLANs	LAG
<input type="radio"/>	GE1	Trunk	1V, 2M, 10M, 16M, 4095P	2M, 10M, 16M, 4095P	
<input type="radio"/>	GE2	Trunk	1V, 10M, 16OP	10M, 16OP	
<input type="radio"/>	GE3	Trunk	1V, 10M, 16OP	10M, 16OP	
<input type="radio"/>	GE4	Trunk	1V, 10M, 16OP	10M, 16OP	
<input type="radio"/>	GE5	Trunk	1V, 10M, 16OP	10M, 16OP	
<input type="radio"/>	GE6	Trunk	1V, 16OP	16OP	
<input type="radio"/>	GE7	Trunk	1V, 16OP	16OP	
<input type="radio"/>	GE8	Trunk	1V, 16OP	16OP	
<input type="radio"/>	GE9	Trunk	1V, 2OP	2OP	
<input type="radio"/>	GE10	Trunk	1OP	1OP	

V - Verbotenes Mitglied M: getaggtes Mitglied O: ungetaggtes Mitglied I: Intern verwendetes VLAN P - PVID

4.44.3 Der Unifi-Kontroller

Inhalt:

Die Installation

Hardwareanforderungen

- 3 GB RAM
- Eine Netzwerkkarte im Schulnetz (VLAN 16)
- 10 GB Festplatte (bei mir im Schulbetrieb sind 3,3 GB vom 40 GB belegt).

Die Grundinstallation

Für die Installation brauchen wir einen Dockerhost ohne nginx und dehydrated (siehe [Installation eines Dockerhosts](#)).

Hinweis: Es kann hierzu jeder bereits bestehende Docker-Host verwendet werden, sofern die u.g. Ports nicht bereits belegt sind.

Unifi-Controller mit docker-compose einrichten und starten

Melde Dich auf dem Docker-Host an, werde mit `sudo -i root` und lege mit `mkdir -p /srv/docker/unifi` das Verzeichnis `/srv/docker/unifi` an.

Gehe mit `cd /srv/docker/unifi` in das neue Verzeichnis und lege die Datei `docker-compose.yml` an mit folgendem Inhalt an:

```
version: "2.1"
services:
  unifi-controller:
    image: ghcr.io/linuxserver/unifi-controller
    container_name: unifi-controller
    environment:
      - PUID=1000
      - PGID=1000
    volumes:
      - ./data:/config
    ports:
      - 3478:3478/udp
      - 10001:10001/udp
      - 8080:8080
      - 8443:8443
      - 1900:1900/udp #optional
      - 8843:8843 #optional
      - 8880:8880 #optional
      - 6789:6789 #optional
      - 5514:5514 #optional
    restart: unless-stopped
```

Starte den Unifi-Controller mit `docker-compose up -d`.

Hinweis: Zur Zeit wird die Unifi-Controller-Version 7.3.76 installiert. Möchtest Du eine frühere Version installieren, musst Du das in Zeile 4 angeben. Beispiel: `image: ghcr.io/linuxserver/unifi-controller:LTS-version-5.6.42`. Welche Versionen es gibt, siehst Du [hier](#).

Die Grundkonfiguration

Hier werden die Standardsprache sowie der Adminaccount gewählt und es können die APs aufgenommen werden.

Schritt für Schritt

Öffne von einem Rechner im Schulnetz mit einem Browser <https://unifi:8443> (falls der Unificontroller in der Datei *workstations* unifi heißt).

Da der Unifi-Kontroller mit einem selbstzertifizierten Zertifikat arbeitet, wirst Du eine Zertifikatswarnung erhalten.

UniFi Setup-Assistent

Vielen Dank dass Sie sich für UniFi, Ubiquiti's Enterprise WLAN Lösung entschieden haben. Sie werden die Möglichkeit haben Ihren Controller in wenigen Minuten einzurichten.

Land auswählen

Germany

Zeitzone auswählen

(UTC+01:00) Brussels, Copenhagen, Madrid, Paris

Automatisches Backup
aktivieren

AUS

Alternativ können Sie [Aus vorherigem Backup wiederherstellen](#).

WEITER

Wähle Germany als Land und klicke auf *weiter*.

Wähle die Geräte aus, die Du mit dem Unifi-Kontroller managen möchtest (also alle) und klicke auf *WEITER*.

An dieser Stelle überspringst Du die Einrichtung eines WLANs. Das wird später ausführlich beschrieben.

An dieser Stelle wird ein Administrator-Zugang angelegt.

Überspringe auch diesen Schritt.

Bestätige schließlich Deine Einstellungen.

Geräte konfigurieren

Bitte wählen Sie die Geräte aus, die Sie konfigurieren möchten.

<input type="checkbox"/>	GERÄTENAME	MODELL	IP ADRESSE	LAUFZEIT ↓
<input checked="" type="checkbox"/>	80:2a:a8:d9:cf:0a	UniFi AP-AC-Pro	10.20.50.1	30m 25s

Zeige 1-1 von 1 Datensätzen. Einträge pro Seite:

[ZURÜCK](#)[WEITER](#)

WLAN konfigurieren

Sie können diesen Schritt überspringen, wenn Sie keine UniFi Access Points (AP) einrichten möchten.

Optional können Sie ein offenes WLAN für Ihre Gäste erstellen:

☐ Gastzugang aktivieren

[ZURÜCK](#)[ÜBERSPRINGEN](#)[WEITER](#)

Controller-Zugriff

Bitte geben Sie den Namen und das Passwort für den Administrator des UniFi Controllers an.

Passwortstärke: Sehr gut

[ZURÜCK](#)[WEITER](#)

Cloud-Zugriff

Bitte geben Sie die Zugangsdaten Ihres Ubiquiti-Kontos ein, um den Cloud-Zugriff zu aktivieren.

Falls Sie noch kein Ubiquiti-Konto haben [registrieren Sie sich jetzt](#).

[ZURÜCK](#)[ÜBERSPRINGEN](#)[WEITER](#)

Bestätigen

Bitte die Einstellungen unten nochmals prüfen. Sobald Sie fertig sind, werden Sie zum Management-Interface weitergeleitet.

Land	Germany
Zeitzone	Europe/Brussels
Sichere SSID	-
Gast SSID	-
Name des Administrators	admin

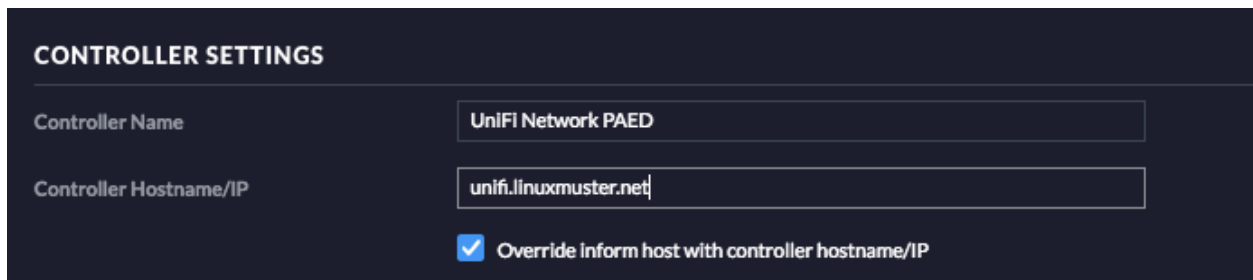
[ZURÜCK](#)[ÜBERNEHMEN](#)

Einstellungen zur Aufnahme der APs

Damit der Unificontroller die angeschlossenen Access Points (APs) aufnehmen kann und mit diesen kommuniziert, sind noch folgende Einstellungen zu treffen:

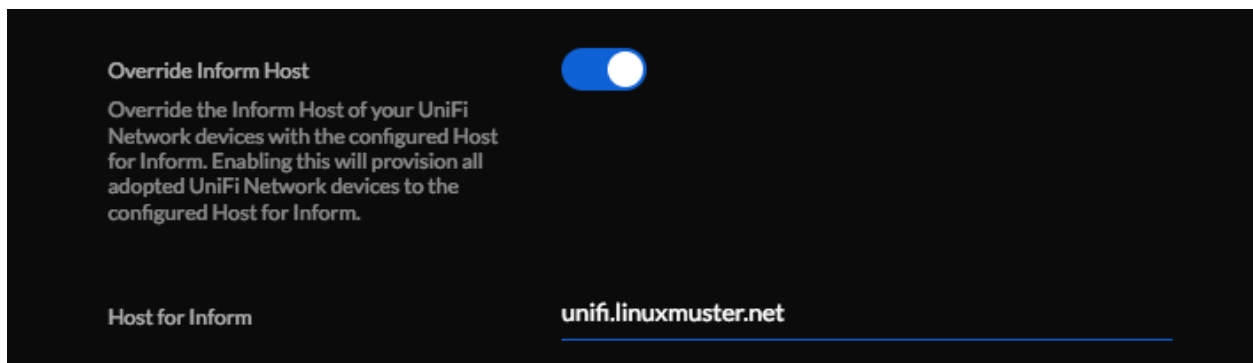
1. Wähle Settings → System Settings → Controller/Application Configuration
2. Gib dort bei der Option Host to inform die IP-Adresse des Dockerhosts, den FQDN oder ein CNAME als FQDN ein.
3. Teste die Aufnahme, indem Du einen AP anschließt. Nachdem dieser gestartet ist, siehst Du im Controller den AP in der Phase Adopting. Diese muss erfolgreich beendet worden sein. Sollte dies nicht der Fall sein, so solltest Du in den log files des Unifi Controllers nach Fehlern suchen.

Die Einstellungen sehen in der alten UI des Unifi Controllers wie folgt aus:



The screenshot shows the 'CONTROLLER SETTINGS' page in the old Unifi Controller UI. It has a dark theme. There are two input fields: 'Controller Name' with the value 'UniFi Network PAED' and 'Controller Hostname/IP' with the value 'unifi.linuxmuster.net'. Below these fields is a checked checkbox labeled 'Override Inform host with controller hostname/IP'.

In der neuen UI des Unifi Controllers entspricht dies folgender Einstellung:



The screenshot shows the 'Override Inform Host' toggle in the new Unifi Controller UI. The toggle is turned on (blue). Below the toggle is a description: 'Override the Inform Host of your UniFi Network devices with the configured Host for Inform. Enabling this will provision all adopted UniFi Network devices to the configured Host for Inform.' At the bottom, there is a label 'Host for Inform' and the value 'unifi.linuxmuster.net'.

Einrichtung des Lehrer-WLANs

Im Lehrer-WLAN sind alle schuleigenen Geräte und die Geräte der Lehrer.

So könnte beispielsweise ein Lehrer mit seinem Smartphone eine Aufgabe abfotografieren und zum Beamer schicken. Oder er könnte einen Film per Smartphone direkt über einen Beamer abspielen.

Achtung: All diese Geräte müssen in die Datei *devices.csv* aufgenommen sein.

Hinweis: Schülergeräte haben in diesem Netzwerk nichts zu suchen. Denn Schüler sollen nicht in der Lage sein, Filmchen per Handy zu starten.

Schritt für Schritt

Öffne von einem Rechner im Schulnetz den Unifi-Kontroller <https://unifi:8443> und melde Dich an.

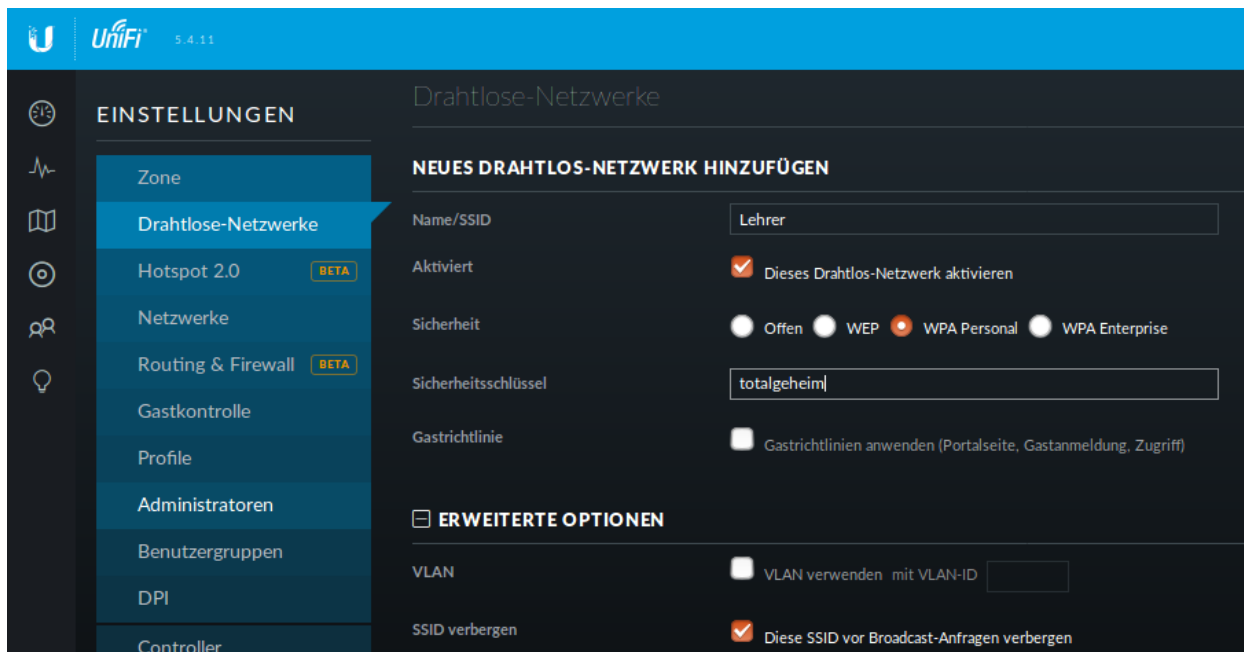


Klicke unten links auf *Einstellungen*. Gehe auf *drahtlose Netzwerke*.



Es ist bereits eine WLAN-Gruppe *Default* eingerichtet. Die wird Dir für den Betrieb in einer Schule ausreichen.

Wie erwartet sind noch keine drahtlosen Netzwerke eingerichtet. Für Dein erstes WLAN klickst Du auf *NEUES DRAHTLOS-NETZWERK HINZUFÜGEN*.



Gib dem Lehrernetz einen Namen (z.B. Lehrer).

Wähle die Verschlüsselung *WPA Personal* und ein Passwort.

Wähle **nicht** Gastrichtlinie. Im Schulnetz möchtest Du keine Gäste!

Wenn Du möchtest, verbirg die SSID. Was Schüler nicht sehen, macht sie nicht neugierig.

Speichere die Einstellungen.

Das Lehrernetz ist nun eingerichtet und wird auf alle APs ausgerollt.

Einrichtung des Schüler-WLANs

Im Schüler-WLAN sind die Geräte der Schüler. Es liegt im blauen Netz der OPNsense®. Der Netzwerk-Schlüssel des Schüler-WLANs basiert auf ihrem Benutzernamen und ihrem Kennwort.

Schritt für Schritt

Installiere auf dem linuxmuster.net-Server das Paket `freeradius`. Siehe [Netzwerkzugriff über Radius](#)

Melde Dich am Unifi-Kontroller an <https://unifi:8443>.

Gehe zu *Einstellungen* -> *Profile* -> *NEUES RADIUS-PROFIL ERSTELLEN*.

DAS RADIUS-PROFIL RADIUS IM SCHULNETZ BEARBEITEN. ✕

Profil Name

VLAN Support ☐ RADIUS-verknüpftes VLAN für das Ethernet aktivieren.

☐ RADIUS verknüpftes VLAN für das WLAN aktivieren **BETA**

RADIUS-Authentifizierungsserver IP Adresse Port Passwort ✕

+ AUTHENTIFIZIERUNGSSERVER HINZUFÜGEN

Abrechnung ☐ Abrechnungsserver aktivieren

ABBRECHEN **SPEICHERN**

Gib dem neuen Radius-Profil einen Namen.

Trage bei *Radius-Authentifikationsserver* die IP-Adresse des linuxmuster.net-Servers und das Passwort für die APs ein.

Speichere die Einstellungen.

Gehe zu *Einstellungen* -> *Drahtlose-Netzwerke* -> *NEUES DRAHTLOSES NETZWERK HINZUFÜGEN*.

Gib dem Schüler-WLAN einen Namen.

Sicherheit ist *WPA Enterprise*.

Wähle das vorher definierte Radius-Profil.

Da das blaue Netz der OPNsense® als getaggttes VLAN mit der VLAN-ID 10 zu den APs kommt, setze ein Häkchen bei VLAN und gib als VLAN-ID 10 ein.

Speichere die Einstellungen.

Das Schüler-WLAN wird jetzt an die APs ausgerollt.

EINSTELLUNGEN

Zone

Drahtlose-Netzwerke

Hotspot 2.0 BETA

Netzwerke

Routing & Firewall BETA

Gastkontrolle

Profile

Administratoren

Benutzergruppen

DPI

Controller

Cloud-Zugriff

Wartung

Automatisches Backup

DRAHTLOS-NETZWERK - SCHUELER-WLAN - BEARBEITEN.

Name/SSID

Schueler-WLAN

Aktiviert

☒ Dieses Drahtlos-Netzwerk aktivieren

Sicherheit

☐ Offen
☐ WEP
☐ WPA Personal
☒ WPA Enterprise

RADIUS-Profil

Radius im Schulnetz

NEUES RADIUS-PROFIL ERSTELLEN

Hotspot 2.0

☐ Hotspot 2.0 aktivieren GEN2

Gastrichtlinie

☐ Gastrichtlinien anwenden (Portalseite, Gastanmeldung, Zugriff)

ERWEITERTE OPTIONEN

VLAN

☒ VLAN verwenden mit VLAN-ID

10

☐ RADIUS-verknüpftes VLAN aktivieren BETA

☐ Diese SSID vor Broadcast-Anfragen verbergen

SSID verbergen

☐

WPA Modus


Nur WPA2

Verschlüsselung

Nur AES/CCMP

Benutzergruppe

Default

 Note that the configuration and rate limits of this user group will be ignored by any client that has a user group already selected.

UAPSD

☐ "Unscheduled Automatic Power Save Delivery" aktivieren

geplant

☐ Geplantes WLAN aktivieren

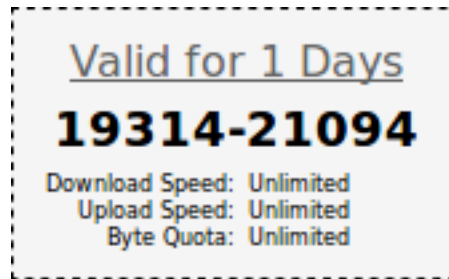
802.11 GESCHWINDIGKEIT- UND BEACON-KONTROLLEN

SPEICHERN

ABBRECHEN

Gast-WLAN mit Gutschein / Voucher

Unifi unterstützt auch WLAN-Gutscheine (WLAN-Voucher).



Bei einem WLAN-Gutschein meldet man sich, wie in einigen Hotels, an einem unverschlüsselten Gästenetz an und wird auf eine Anmeldeseite umgeleitet. Dort gibt man einen Gutschein-Code ein.

Der Unifi-Controller unterstützt zwei Arten von Gutscheinen:

Einmaliger Gebrauch:

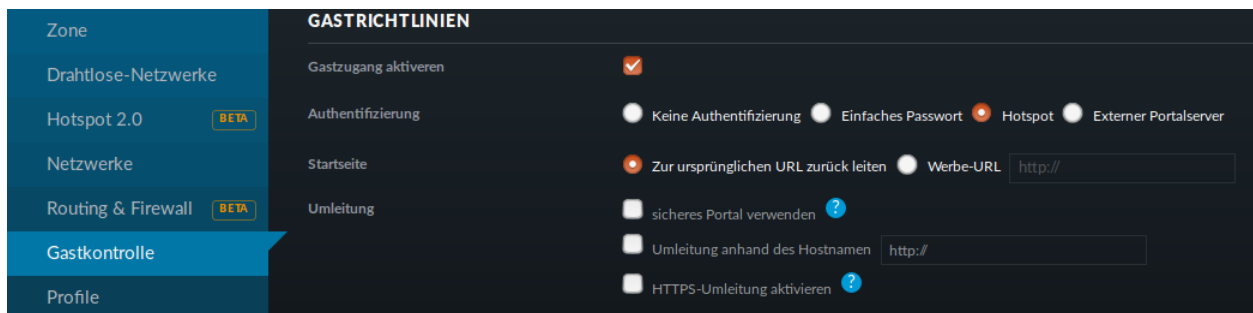
Der Gutschein-Code ist nur für ein Gerät gültig. Nach der Anmeldung kann man mit seinem Gerät so lange ins Internet, bis der Gutschein abgelaufen ist. Das Gerät kann sich in dieser Zeit unbegrenzt mit dem Gäste-WLAN neu verbinden.

Mehrmaliger Gebrauch:

Der Gutschein-Code ist für beliebig viele Geräte gültig. Sobald sich das erste Gerät mit dem Gutschein-Code angemeldet hat, beginnt die Gültigkeit des Gutscheins abzulaufen. Solche Gutscheine eignen sich beispielsweise für VHS-Kurse, die keine Accounts im Schulnetz haben.

Schritt für Schritt

Melde Dich an und gehe auf *Einstellungen* -> *Gastkontrolle*.



Im Bereich Gastrichtlinien setzt Du einen Haken bei *Gastzugang aktivieren*.

Bei *Authentifizierung* wählst Du *Hotspot*.

Hat *HTTPS-Umleitung aktivieren* ein Häkchen, so werden Clients auch dann umgeleitet, wenn Sie auf HTTPS-Seiten surfen. Leider erhält man dann eine Zertifikatswarnung, da der Unifi-Kontroller mit einem selbstsignierten Zertifikat arbeitet. Allerdings leiten viele Betriebssysteme von selbst auf das Gastportal um.

In der Portal-Anpassung wählst Du die Template-Engine AngularJS und fügst die Sprache Deutsch hinzu.

Den Rest der Einstellungen kannst Du so lassen.

Unter *HOTSPOT* setzt Du ein Häkchen bei Gutschein.

PORTAL-ANPASSUNG

Template-Engine ☒ AngularJS NEU ☐ Veralter JSP

Standard-Vorlagen überschreiben BETA ☐ Vorlagen mit eigenen Anpassungen überschreiben. ?

Titel

Begrüßungstext ☐ Begrüßungstext aktivieren

Nutzungsbedingungen ☐ Nutzungsbedingungen aktivieren

Sprachen BETA

CODE	SPRACHE	AKTIONEN
de_DE	Deutsch (Deutschland)	LÖSCHEN
en	Englisch	LÖSCHEN

[+ SPRACHE HINZUFÜGEN](#)

Portal-Anpassung

☐ Benutzerdefiniertes Logo

☒ Hintergrundbild [Bild hochladen](#)

☐ Hintergrundbild teilen

☐ Hintergrundfarbe

☐ Textfarbe

☒ Schaltflächenfarbe

☐ Farbe von Schaltflächenbeschriftung

☒ Farbe von Links

☐ Farbe von Rahmen

☐ Textfarbe in Rahmen

☒ Textfarbe von Links in Rahmen

☒ Transparenz von Rahmen %

[ANGEPASSTES STYLE ZURÜCKSETZEN](#)

DESKTOP-VORSCHAU MOBILE VORSCHAU

HOTSPOT

API



API-basierte Berechtigung aktivieren



Gutscheine



Gutschein-basierte Anmeldung aktivieren

Zahlungen



Zahlungsbasierte Anmeldung aktivieren

Facebook BETA



Facebook-Anmeldung aktivieren

Google+ BETA



Google-Anmeldung aktivieren

GUTSCHEIN-ANPASSUNG

Template-Engine



Veralter JSP

Standard-Vorlagen überschreiben



Vorlagen mit eigenen Anpassungen überschreiben.



ZUGRIFFSKONTROLLE

Zugriff vor der Anmeldung

unifi



HOSTNAME ODER SUBNETZ HINZUFÜGEN

Beschränkungen nach der Anmeldung



HOSTNAME ODER SUBNETZ HINZUFÜGEN

ÄNDERUNGEN ANWENDEN

ZURÜCKSETZEN

In der *Zugriffskontrolle* musst Du den Zugriff auf den Unifi-Kontroller noch vor der Anmeldung erlauben, da man sonst nicht auf die Anmeldeseite kommt.

Gehe auf *ÄNDERUNGEN ANWENDEN*. Damit werden die Änderungen gespeichert und auf die APs ausgerollt.

Firewall-Regeln für die OPNsense®

Damit die Clients überhaupt auf den Unifi-Kontroller zugreifen können, muss eine neue Firewallregel für die OpnSense angelegt werden:

Schritt für Schritt

Öffne die OPNsense® <https://firewall.linuxmuster.lan> und melde Dich an.

Gehe auf *Firewall->`Regeln`->`WLAN`* und wähle *Hinzufügen*.

The screenshot shows the 'Firewall: Regeln: WLAN' configuration page in OPNsense. The rule is named 'WLAN' and is set to 'Erlauben' (Allow). It is active and set to 'Schnell' (Quick). The rule is applied to the 'WLAN' interface, with 'in' direction, 'IPv4' protocol, and 'TCP' protocol. The source is 'jeder' (any) and the destination is '10.16.1.100' on port '16'. The rule is described as 'WLAN darf auf Unifi Port 8880'. The 'Erweiterte Funktionen' (Advanced Functions) section is expanded, showing 'Quellbetriebssystem' (Source Operating System) set to 'Jedes' (Every), 'Keine XMLRPC Synchronisation' (No XMLRPC Synchronization) checked, 'Zeitplan' (Schedule) set to 'keiner' (none), and 'Gateway' set to 'standard'. The 'Erweiterte Optionen' (Advanced Options) section is also expanded, showing 'Zeigen/Verstecken' (Show/Hide) checked. The 'Speichern' (Save) button is highlighted in orange.

Mache die folgenden Eingaben:

Schnittstelle: WLAN

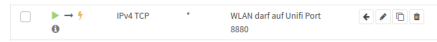
Protokoll: TCP

Ziel: *Einzelner Host oder Netzwerk* und gib in der Eingabezeile die IP-Adresse des Unifi-Controllers ein.

Zielportbereich: Wähle (*andere(r/s)*) und gib von 8880 an 8880 ein.

Beschreibung: *WLAN hat Zugriff auf Unifi-Controller Port 8880*

Speichere Deine Eingaben.



Kopiere die eben erstellte Regel und ändere:

Zielportbereich: Wähle (*andere(r/s)*) und gib von 8443 an 8443 ein.

Beschreibung: *WLAN hat Zugriff auf Unifi-Controller Port 8443*

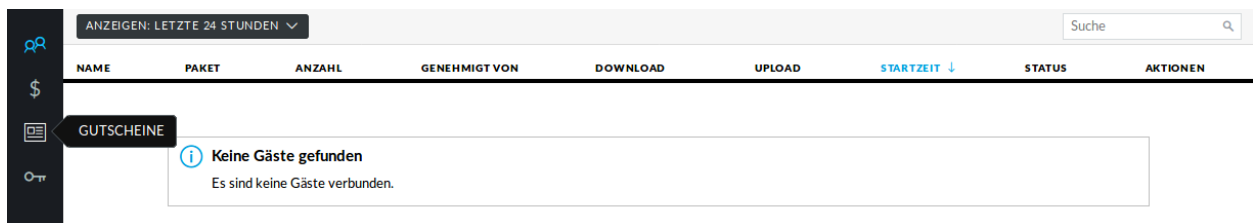
Speichere Deine Eingabe und übernehme die Änderungen.

WLAN-Gutscheine / Voucher erstellen

Jetzt müssen die Gutscheine noch erzeugt und ausgedruckt werden.

Schritt für Schritt

Gehe auf <https://unifi:8443/manage/hotspot> und melde Dich an.



Gehe auf *GUTSCHEINE*->`GUTSCHEIN ERSTELLEN`.

Fülle die Felder des Dialogfensters aus und speichere Deine Eingabe.

In dieser Ansicht siehst Du alle gültigen Gutscheine.

Du hast die Möglichkeit, einzelne Gutscheine, alle nicht benutzten Gutscheine oder alle Gutscheine, die an einem bestimmten Zeitpunkt erstellt wurden, zu drucken.

Hier kannst auch Gutscheine löschen.

4.45 Mitarbeit linuxmuster.net

Autor des Abschnitts: @cweikl

Es gibt verschiedene Möglichkeiten, wie Sie helfen können, linuxmuster.net zu verbessern.

- Über linuxmuster.net berichten (z.B. in Blogs, Sozialen Netzwerken, etc.)
- Fragen stellen und Fehler melden: <https://ask.linuxmuster.net>
- selbst Fragen beantworten: <https://ask.linuxmuster.net>
- Eigene Tipps und Tricks dokumentieren: <https://linuxmuster.net/wiki>
- dem Verein beitreten

GUTSCHEINE ERSTELLEN

Erstellen

10

Mehrmaliger Gebrauch

Ablaufdatum

24 Stunden

Bandbreitenlimit (Download)

☐

Begrenzt auf

Kbps

Bandbreitenlimit (Upload)

☐

Begrenzt auf

Kbps

MByte-Limit

☐

Begrenzt auf

MBytes

Notiz

Gutscheine für mehrmaligen Gebrauch

ABBRECHEN

SPEICHERN

U
Unifi 5.4.11

AKTUALISIERUNGSINTERVALL
15 Sekunden

+ GUTSCHEIN ERSTELLEN

ALLE NICHT BENUTZTEN GUTSCHEINE DRUCKEN

STAPELDRUCK

Suche

CODE	ZEITPUNKT DER ERSTELLUNG	EMPFANGEN	GESENDET	04/13/2017 9:57 am	ERKUNGEN	DAUER	STATUS	AKTIONEN
26513-24349	04/13/2017 9:57 am				Gutscheine für mehrmaligen Gebrauch	1d	Gültig für Mehrfachnutzung	DRUCKEN ZURÜCKZIEHEN
51327-16829	04/13/2017 9:57 am				Gutscheine für mehrmaligen Gebrauch	1d	Gültig für Mehrfachnutzung	DRUCKEN ZURÜCKZIEHEN
45183-52646	04/13/2017 9:57 am				Gutscheine für mehrmaligen Gebrauch	1d	Gültig für Mehrfachnutzung	DRUCKEN ZURÜCKZIEHEN
78629-32176	04/13/2017 9:57 am				Gutscheine für mehrmaligen Gebrauch	1d	Gültig für Mehrfachnutzung	DRUCKEN ZURÜCKZIEHEN
83035-46102	04/13/2017 9:57 am				Gutscheine für mehrmaligen Gebrauch	1d	Gültig für Mehrfachnutzung	DRUCKEN ZURÜCKZIEHEN
06046-68420	04/13/2017 9:57 am				Gutscheine für mehrmaligen Gebrauch	1d	Gültig für Mehrfachnutzung	DRUCKEN ZURÜCKZIEHEN
06652-06915	04/13/2017 9:57 am				Gutscheine für mehrmaligen Gebrauch	1d	Gültig für Mehrfachnutzung	DRUCKEN ZURÜCKZIEHEN
74940-30376	04/13/2017 9:57 am				Gutscheine für mehrmaligen Gebrauch	1d	Gültig für Mehrfachnutzung	DRUCKEN ZURÜCKZIEHEN
65887-20520	04/13/2017 9:57 am				Gutscheine für mehrmaligen Gebrauch	1d	Gültig für Mehrfachnutzung	DRUCKEN ZURÜCKZIEHEN
32876-13049	04/13/2017 9:57 am				Gutscheine für mehrmaligen Gebrauch	1d	Gültig für Mehrfachnutzung	DRUCKEN ZURÜCKZIEHEN

Zeige 1-10 von 10 Datensätzen.

Einträge pro Seite: 50

Wir freuen uns, wenn Du darüber hinaus an der Dokumentation mitarbeiten würdest. Dies können

- einfache Änderungen auf Github sein,
- die Übersetzung von Abschnitten,
- die Erstellung neuer Dokumentationskapitel

Für alle drei Möglichkeiten findest Du links im Menü weitere Hinweise. Zudem haben wir Dokumentationsleitlinien erstellt. Diese sollten von allen Mitarbeitenden an der Dokumentation berücksichtigt werden.

4.45.1 Dokumentation übersetzen

Die Dokumentation kann auf der [Projektseite bei Transifex](#) übersetzt werden. Klicke einfach auf den blauen Button `Help Translate official documentation` und melde Dich mit Deinem Transifex-Konto an bzw. erstelle ein neues Konto.

4.45.2 Dokumentation in GitHub ändern

Wenn Du einen Fehler (Rechtschreibfehler, kleine inhaltliche Fehler, etc.) in der Dokumentation gefunden hast, klicke einfach auf den `Edit on Github` Link am rechten oberen Rand jeder Dokumentationsseite.

[Docs](#) » [Handbuch für Netzwerkbetreuer](#) » [Linux Client's in linuxmuster.net](#)

[Edit on GitHub](#)

Linux Client's in linuxmuster.net

Zielgruppe: Ambitionierte Netzwerkberater oder Dienstleister

In dieser Anleitung wird beschrieben, wie man Linux auf einer Musterarbeitsstation installiert. Ein

Damit wirst Du auf [github.com](#) geleitet. Mit einem Klick auf den Stift (siehe Bild) kannst Du das aktuelle Kapitel bearbeiten. Dafür müsst du Dich bei GitHub anmelden. Wenn Du noch kein Konto bei GitHub hast, kannst Du [hier eines anlegen](#) oder oben rechts auf „Sign up“ klicken.

Die Dokumentation ist in der Auszeichnungssprache „rST“ geschrieben. [Hier](#) findest Du einen guten Überblick über die am häufigsten verwendeten Elemente.


Im Beispiel wurde der Rechtschreibfehler und die Länge der zur Überschrift gehörenden Unterschreibung geändert.

Nachdem Du alle Änderungen vorgenommen hast, gib unten einen Titel und einen Kommentar ein. Die Änderungen können nun mit einem Klick auf „Propose file changes“ eingereicht werden.

Dein Änderungsvorschlag wird dann vom Dokumentationsteam geprüft und gegebenenfalls übernommen. Sekunden später erscheint die Änderung dann auch hier in der offiziellen Dokumentation.

Hinweis: Bitte beachte auch unbedingt die [Leitlinien zur Dokumentation](#), damit Deine Änderungen schnell eingepflegt werden können!


Solltest Du bereits Schreibrechte am Repositorium haben und bist Dir sicher, dass die Dokumentation durch Deine Änderung nicht beeinträchtigt wird, kannst Du die Änderungen direkt einbauen („Commit“) oder im Zweifel einen Zweig und einen so genannten Pull-Request erstellen.


 [Features](#) [Business](#) [Explore](#) [Marketplace](#) [Pricing](#) [This repository](#) [Sign in](#) or [Sign up](#)

[linuxmuster-docs](#) / [main](#) Watch 19 Star 3 Fork 10

[Code](#) [Issues 33](#) [Pull requests 1](#) [Projects 1](#) [Insights](#)

Branch: **master** [main](#) / [source](#) / [howtos](#) / [linuxclients](#) / **index.rst** Find file Copy path

 **Jolly-Jump** Update index.rst 60d9656 17 minutes ago
1 contributor

26 lines (17 sloc) | 873 Bytes Raw Blame History 

Linux Client's in linuxmuster.net

Zielgruppe: Ambitionierte Netzwerkberater oder Dienstleister

In dieser Anleitung wird beschrieben, wie man Linux auf einer Musterarbeitsstation installiert. Ein fertig vorkonfiguriertes

[Edit file](#) [Preview changes](#)

Spaces 3 Soft wrap

```
1 .. install-linux-clients-label:  
2  
3 Linux Clients in linuxmuster.net  
4 =====  
5  
6 Zielgruppe: Ambitionierte Netzwerkberater oder Dienstleister  
7  
8 In dieser Anleitung wird beschrieben, wie man Linux auf einer Musterarbeitsstation installiert.
```

Propose file change

Update index.rst

Add an optional extended description...

[Propose file change](#) [Cancel](#)



Commit changes

Update index.rst

fixed small typo: no apostrophe, just plural

- ☒ Commit directly to the `master` branch.
☐ Create a **new branch** for this commit and start a pull request. [Learn more about pull requests.](#)

Commit changes

Cancel

Größere Änderungen an der Dokumentation sind immer über Pull-Requests zu erstellen. Dafür ist es nützlich, lokal eine Kopie (fork) vorzuhalten und Änderungen lokal zu testen, das im [entsprechenden Kapitel](#) erklärt wird.

4.45.3 Dokumentation lokal bearbeiten und veröffentlichen

Wenn Du die Dokumentation erweitern willst, z.B. mit einem eigenen HowTo, ein fehlendes Kapitel ergänzen möchtest, oder größere Änderungen machen und testen willst, benötigst Du folgende Dinge:

- ein Konto bei [Github](#)
- Die Software [git](#) (wird zur Verwaltung und Versionierung der Dokumentation verwendet)
- Die Software [sphinx](#) (zum Übersetzen und Testen der Quelldateien), die wiederum python voraussetzt
- optional: SSH-Schlüssel bei Github [hochladen](#) (erleichtert die Arbeit mit git)

Lokale Installation (Ubuntu)

Mit folgenden Befehlen kannst Du unter einer aktuellen (ab 22.04 LTS) Ubuntu-Distributionen git ($\geq 2.39.2$), python (≥ 3.10) und sphinx ($\geq 7.2.6$) nachinstallieren:

```
$ sudo apt install git
$ sudo apt install python3-pip
$ pip3 install sphinx
$ pip3 install sphinx_rtd_theme
```

Offizielle Dokumentation kompilieren

Hast Du bereits eine heruntergeladene Dokumentation aus dem offiziellen Repository, dann könntest Du nun eine lokale Version der Dokumentation bauen und betrachten. Ansonsten mach mit dem nächsten Punkt weiter: [GitHub Konto erstellen](#)

Öffne dazu ein Terminal, navigiere zum Ordner `linuxmuster-docs/main`, führe `make clean && make html` aus und rufe die Datei `linuxmuster-docs/main/build/html/index.html` z.B. mit dem Browser Firefox auf, um das Ergebnis zu betrachten.

```
linuxadmin@lmn-docs:~$ cd linuxmuster-docs/
linuxadmin@lmn-docs:~/linuxmuster-docs$ cd main/
linuxadmin@lmn-docs:~/linuxmuster-docs/main$ make celan && make html
sphinx-build -b html -d build/doctrees source build/html
Running Sphinx v7.2.6
loading translations [de_DE]... done
loading pickled environment... done
...
linuxadmin@lmn-docs:~/linuxmuster-docs/main$ firefox build/html/index.html
```

GitHub Konto erstellen

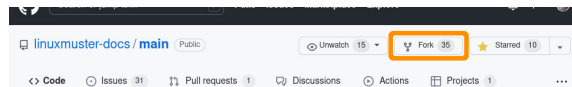
Spätestens jetzt solltest Du ein Konto bei GitHub erstellen: <https://github.com/join>.

Verifiziere Deine E-Mail-Adresse. Natürlich kannst Du die Dokumentation zu GitHub durchlesen. Weiter geht es dann unter <https://github.com/linuxmuster-docs/main>

Hinweis: Im folgenden wird das Konto „lmn-docs-bot“ verwendet. Überall wo dieser auftaucht, ersetze ihn durch Dein Kontonamen bei GitHub.

Linuxmuster Dokumentation forken

Öffne die [linuxmuster.net Dokumentation auf Github](https://github.com/linuxmuster-docs/main) und klicke auf „Fork“.



Öffne nun einen Terminal / Eingabeaufforderung (Strg+Alt+t in Ubuntu) und gib folgenden Befehl ein:

Bemerkung: Nutze die URL `git@github.com:lmn-docs-bot/main.git` falls Du bereits einen SSH-Schlüssel bei Github hochgeladen hast!

```
linuxadmin@lmn-docs:~$ git clone https://github.com/lmn-docs-bot/main.git my-docs
Klone nach 'my-docs' ...
...
linuxadmin@lmn-docs:~$ cd my-docs
```

Du kannst nun mit

```
linuxadmin@lmn-docs:~/my-docs$ make clean && make html
linuxadmin@lmn-docs:~/my-docs$ firefox build/html/index.html
```

die Dokumentation in HTML übersetzen und diese lokal in Deinem Browser öffnen.

Dokumentation ändern oder neu erstellen

Die Dokumentation ist in der Markupsprache „rST“ geschrieben. [Hier](#) findest Du einen guten Überblick über die häufig verwendeten Elemente.

Hinweis: Bitte beachte auch unbedingt die [Leitlinien zur Dokumentation](#), damit die Änderungen schnell eingepflegt werden können!

Im Verzeichnis `source` und den entsprechenden Unterordnern befinden sich alle Dokumentationsdateien. Öffne einfach eine dieser Dateien und führe die gewünschten Änderungen durch. Du kannst auch eine neue Dokumentation in einem der Unterordner anlegen. Erstelle dazu einfach einen Ordner mit einem passenden Namen und die notwendige `index.rst` Datei.

```
$ mkdir source/howto/foobar
$ touch source/howto/foobar/index.rst
```

Schau Dir auch die anderen Dokumentationsdateien an, um mehr über den Aufbau und Syntax zu lernen.

Commit und push

Hast Du alle Änderungen vorgenommen, kannst Du diese nun zur Überprüfung einreichen. Dazu sind folgende Schritte notwendig:

Wichtig: Überprüfe bitte zuerst, ob `make clean && make html` ohne Fehler durchläuft! Falls nicht, behebe bitte alle Fehler und Warnungen, bevor Du Deine Änderungen hochlädst!

```
$ make html
```

Falls Du neue Dateien oder Ordner erstellt hast, müssen diese noch hinzugefügt werden:

```
$ git add source/howto/foobar
```

Gib nun noch einen Kommentar zu Deinen Änderungen ein und lade alles in Deinen Fork hoch:

```
$ git commit -a -m"My great documentation"
$ git push
```

Pull-Request

Erstelle nun einen „Pull-Request“ unter <https://github.com/lmn-docs-bot/main>, indem Du auf New Pull Request klickst.

Wenn Du weitere Änderungen vornehmen möchtest und diese mit `git commit -a -m"My comment"` und `git push` bei Github hochlädst, werden diese Änderungen automatisch dem Pull Request hinzugefügt.

The full documentation with all individual docs pulled in as sub-repos — Edit

144 commits 2 branches 0 releases 1 contributor GPL-2.0

Branch: master **New pull request** Create new file Upload files Find file Clone or download

This branch is 36 commits behind linuxmuster-docs:master. Pull request Compare

zefanja * minor changes (typos, code blocks) Latest commit 1ecd951 on 23 Jul

File	Commit Message	Time
source	* minor changes (typos, code blocks)	2 months ago
.gitignore	Revert "file mode changes"	2 months ago
LICENSE	Revert "file mode changes"	2 months ago
Makefile	Revert "file mode changes"	2 months ago
README.rst	update README.rst: make a low entrance level, link to linuxmuster.net	2 months ago
make.bat	Revert "file mode changes"	2 months ago

Eigenen Fork aktualisieren

Um später weiter Änderungen vornehmen zu können, kann der eigene Fork bei GitHub komplett gelöscht und ein neuer erzeugt werden. Alternativ kann der eigene Fork auf den Stand des offiziellen Repository gebracht werden:

- Verschiebe alle lokalen Änderungen mit `git stash` in den Hintergrund

```
~/my-docs$ git stash
```

- Füge (einmalig) einen remote-tracking branch hinzu:

```
~/my-docs$ git remote add upstream https://github.com/linuxmuster-docs/main.git
```

- Hole und merge den aktuellen offiziellen branch:

```
~/my-docs$ git fetch upstream
~/my-docs$ git merge upstream/master
Aktualisiere 76e2e32..be2f941
Fast-forward
```

- Wenn der merge nicht in einem Fast-forward endet, solltest Du besser den Fork löschen und neu erzeugen. Andernfalls kannst Du jetzt die offiziellen Änderungen hochladen.

```
~/my-docs$ git push
```

- Jetzt kannst Du Deine lokalen Änderungen wieder hervorholen:

```
~/my-docs$ git stash pop
```

Für Fortgeschrittene: andere Zweige bearbeiten

Unterschiedliche Versionen von linuxmuster.net werden in unterschiedlichen Zweigen des github-Repository dokumentiert. Die aktuelle Version ist im Zweig `master` untergebracht und obige Abschnitte beziehen sich darauf.

Will man einen anderen Zweig bearbeiten, beispielsweise den Zweig `v7.2`, dann gibt es nur Folgendes zu beachten:

1. Man muss einmalig den Zweig mit `git checkout v7.2` lokal initialisieren. Mit `git branch` sieht man, welche Zweige aktuell sind.

```
linuxadmin@lmn-docs:~/my-docs$ git branch -l
* master
linuxadmin@lmn-docs:~/my-docs$ git checkout v7.2
Zu Branch 'v7.2' gewechselt
Ihr Branch ist auf demselben Stand wie 'origin/v7.2'.
linuxadmin@lmn-docs:~/my-docs$ git branch
master
* v7.2
```

Man sollte also immer nachschauen, in welchem Zweig man gerade arbeitet.

2. Die Abschnitte zu `commit` und `push` stimmen in jedem Zweig.
3. Wird ein Pull-Request in Github erstellt, dann ist zu beachten, dass auch die gleichen Zweige verglichen werden.

Open a pull request

Create a new pull request by comparing changes across two branches. If you need to, you can also [compare across forks](#).

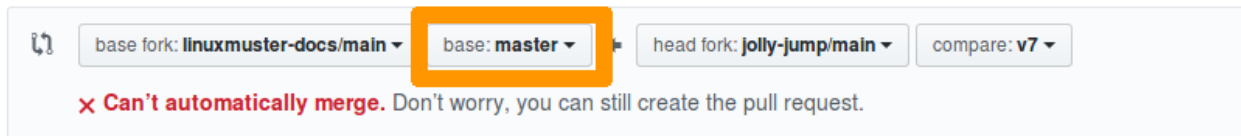


Abb. 502: Ein Pull-Request mit falsch gewähltem Zweig, die sich nicht automatisch zusammenführen lassen.

4. Aktualisiert man den eigenen Fork über das upstream-Repository, dann muss man den Befehl zum Zusammenführen anpassen. Ein Ablauf kann dann so aussehen:

```
linuxadmin@lmn-docs:~/my-docs$ git fetch upstream
remote: Enumerating objects: 15, done.
remote: Counting objects: 100% (15/15), done.
remote: Compressing objects: 100% (12/12), done.
remote: Total 19 (delta 4), reused 3 (delta 3), pack-reused 4
Entpacke Objekte: 100% (19/19), Fertig.
Von https://github.com/linuxmuster-docs/main
7d25598..2c31c06 master    -> upstream/master
4a27d6b..d4edde9 v7.2     -> upstream/v7.2
linuxadmin@lmn-docs:~/my-docs$ git branch
master
* v7.2
linuxadmin@lmn-docs:~/my-docs$ git merge upstream/v7.2
Aktualisiere d3ada10..d4edde9
Fast-forward
source/appendix/install-on-kvm/index.rst | 2 ++
1 file changed, 2 insertions(+)
```

Ein „merge“ des falschen Zweiges, z.B. `upstream/master` hätte hier zu Folge, dass alle Änderungen zwischen den Zweigen zusammengeführt werden würden. Dies führt bei stark unterscheidenden Zweigen zu Fehlern.

Der `master`-Zweig ist kein besonderer Zweig. Man kann also dorthin zurückkehren, wie man zu jedem Zweig wechselt, mit `git checkout master`.

4.45.4 Leitlinien zur Dokumentation

Strukturguide

Auf Ebene der Dateien:

rst-Dateien

- Dateinamen klein schreiben, englisch Begriffe, Leerzeichen vermeiden, Bindestrich (-) statt Unterstrich (_)
- Eine rst-Datei pro Kapitel, möglichst ein englischer Begriff, bsp: `configuration.rst`

Medien, wie Bilder, etc.

- In einen Unterordner *media/* des Kapitles ablegen
- Benennung der Medien-Dateien:

(unter)kapitelbezeichnung_laufende-nummer_beschreibung-des-dargestellten

- (unter)kapitelbezeichnung <– Titel des Kapitels bzw. des Unterkapitels in dem die Medien-Datei verwendet wird
- laufende-nummer <– Bilder ihrer Verwendung von oben nach unten fortlaufend durchnummeriert; eine führende Null
- beschreibung-des-dargestellten <– Bei Fenstern zum Beispiel der Namen des Fensters
- Unterstrich (_) um die drei Felder voneinander abzugrenzen

Beispiel:

`../install-on-xcp-ng/media/install-on-xcp-ng_01_network-sketch.png`

Hinzugefügte Dateien erben von der vorhergehenden Datei die Laufende-Nummer und diese wird um eine neu aufsteigende Nummerierung ergänzt.

Medien und Bilder, die in der Dokumentation mehrfach genutzt werden.

Du solltest von diesem Schema abweichen, da diese nur in dem `root`-Verzeichnis vorhanden sein müssen. Indem auf die laufenden Nummern und Kapitelbezeichnungen verzichtet wird, werden sie als solche kenntlich gemacht. Beispiel wäre die SVG-Grafik `follow_arrow.svg` die dann mit `/media/follow_arrow.svg` in der Datei `/guided_inst.subst` eingebunden wird.

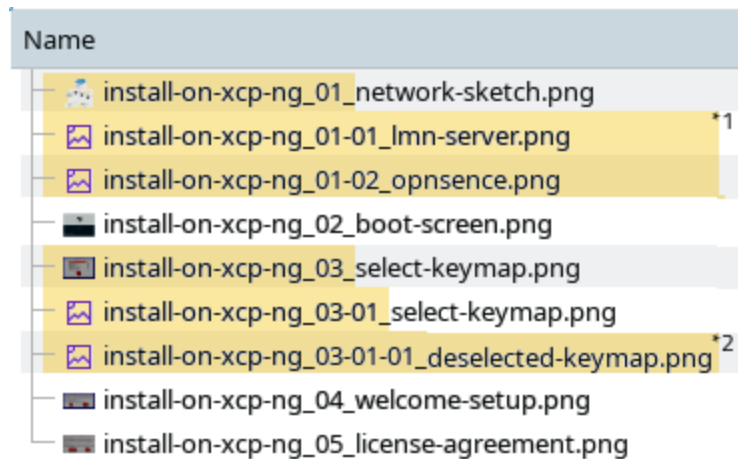


Abb. 503: Beispiel: *1 erste Ergänzung; *2 zweite Ergänzung

Styleguide

- Verwende „Du“
- Benutze zwei ``backticks`` für URLs, URIs, Dateipfade und Dateinamen und Code im Fließtext (inline)
- Benutze einen `backtick` für das Hervorheben für Benutzernamen, Schaltflächen, besondere Aktionen
- für Konsolenbefehle nutze

```
.. code-block:: console

# mein kommando --force
output
```

- Für Bilder kann man image oder figure verwenden. Bei figure kann man Bildunterschriften hinzufügen.

```
.. figure:: media/04_edit-on-github_propose-changes.png
:align: center
:alt: propose changes

Bildunterschriften
```

- Ein Kapitel sollte einen toctree enthalten, wenn es mehrere Dateien gibt.
- Ein Kapitel kann ein Label erhalten bzw. muss eines erhalten wenn es als Sprungziel dienen könnte.

```
.. _knownbugs-label:
```

Bekannte Fehler

=====

Die Benennung dieser Sprungpunkte sollen immer mit -label enden.

- Mit diesem Sprungpunkt kann man an anderer Stelle auf ihn verweisen

Bitte lies :ref:`hier <knownbugs-label>` nach, welche Fehler bekannt sind.

- Um eine Tabelle

Spalte A	Spalte B	Spalte C
Bla	Balbla	Blablabla
Blub	Blubblub	Blubblubblub
Rababa	Rababarababa	Rababarabarabara

einzustellen, nutze folgende einfache Syntax:

```
=====
Überschrift Überschrift Überschrift
Spalte A   Spalte B   Spalte C
=====
Bla        Balbla    Blablabla
Blub       Blubblub  Blubblubblub
Rababa     Rababarababa Rababarabarabara
=====
```

4.46 Active Directory-Domäne

Autor des Abschnitts: @MachtDochNiX

Die Seite ist dem Wiki von samba.org entnommen

https://wiki.samba.org/index.php/Active_Directory_Naming_FAQ

und übersetzt mittels Deepl:

<https://www.deepl.com/translate>

4.46.1 Einführung

Das Auswählen eines Active-Directory-Domänennamens ist einer der wichtigsten Schritte beim Einrichten einer Domäne. Wichtig ist, dass er beim ersten Mal richtig gewählt wird, da eine spätere Änderung eine nicht triviale Aufgabe ist. Es gab religiöse Debatten zu diesem Thema, und die Empfehlungen von MS haben sich im Laufe der Zeit geändert.

4.46.2 Was ist eine Active Directory-Domäne?

Eine Active-Directory-Domäne ist im Grunde dasselbe wie eine Internet-Domäne. Diese »definiert einen Bereich der administrativen Autonomie, Autorität und Kontrolle« für eine Gruppe von Computern. Active Directory-Domänennamen unterliegen denselben Regeln und Grundsätzen, die auch für herkömmliche Domain-Name-Systems (DNS) gelten. Um die Benennung von Active Directory-Domänen zu verstehen, ist es daher wichtig, DNS zu kennen.

4.46.3 Wie funktioniert DNS?

DNS ist das System, mit dem Namen in andere Datentypen für den Computergebrauch übersetzt werden, wie eine IP-Adresse (ein A-Datensatz) oder eine Reihe anderer Datensatztypen.

Eine häufig verwendete Analogie ist die eines Telefonbuchs. Ein DNS-Server dient als eine Art Computer-Telefonbuch, mit dem Computernamen schnell in IPs (oder andere Arten von Daten) übersetzt werden können. Dieses Telefonbuch ist jedoch gigantisch groß (es gibt allein ~4 Milliarden IPv4-Adressen) und diese ändert sich ständig, sodass DNS ein hierarchisches System verwendet, um zu bestimmen, welches Telefonbuch oder genauer gesagt welcher Namensserver für welche Adressensätze zuständig ist.

Praktisch jedes Mal, wenn ein Domänenname aufgelöst wird, sei es durch einen Webbrowser oder eine andere Quelle, wird eine DNS-Anfrage gestellt. Die eigentliche Namensauflösung in Windows ist ein etwas komplexes Thema, aber im Allgemeinen prüft ein Windows-PC seinen lokalen Namen, dann seine Hosts-Datei und stellt dann eine DNS-Anfrage (es sei denn, der Name befindet sich im Cache). Die DNS-Namensserver suchen dann nach der Adresse und geben eine Antwort zurück oder leiten die Anfrage an einen anderen Server zur Auflösung weiter, wenn es sich um einen rekursiven DNS-Server handelt.

Active Directory DNS-Server sind in der Regel rekursiv und bedienen alle DNS-Anfragen für PCs innerhalb der Domäne. DNS-Namen müssen nicht unbedingt auf eine einzige Adresse aufgelöst werden, diese können auch mehreren anderen Einträgen entsprechen und sogar rekursiv auf andere Einträge verweisen, indem Einträge wie CNAME verwendet werden.

DNS-Anfragen werden hauptsächlich über UDP gesendet. Bei UDP gibt es keine Garantie für die Zustellung von Nachrichten oder Antworten, und da die Benutzer erwarten, dass die Namensauflösung schnell und nahtlos erfolgt, ist die Zeitspanne für eine DNS-Antwort kurz (3 Sekunden ist der Windows-Standard, 5 Sekunden der Linux-Standard). Im Großen und Ganzen ist DNS schnell und zuverlässig, aber es ist wichtig, daran zu denken, dass es sporadisch zu einem Fehler bei der Namensauflösung kommen kann.

DNS-Hierarchie

Ein DNS-Name wird durch Punkte in verschiedene Teile unterteilt. Jedes Segment steht für einen anderen Teil der Hierarchie, eine sogenannte Domäne.

Das erste Segment von rechts (.de, .com, .net usw.) wird als Top-Level-Domain (TLD) bezeichnet, jede darunter liegende Domain wird als Subdomain bezeichnet.

Diese Subdomains können ihrerseits Subdomains enthalten, die bis zu 127 Ebenen tief sind.

So ist »example.com« eine Subdomäne der Domäne .com und kann selbst mehrere Subdomänen wie »sandom.example.com« enthalten.

Ein DNS-Name, der auf ein bestimmtes Gerät oder eine bestimmte Datei verweist, wird als »Fully qualified Domain Name« (FQDN) bezeichnet. Technisch gesehen sollte ein FQDN auch die Root-Zone angeben, bei der es sich um einen leeren Domännennamen handelt, der durch einen Punkt am Ende des Domännennamens angegeben wird, z. B. »www.sandom.example.com.«, aber in der Praxis wird die Root-Zone oft weggelassen.

Jeder DNS-Namensserver ist für verschiedene Teile dieser Hierarchie zuständig, die als Zone bezeichnet werden. Eine Zone besteht aus einem DNS-Namen, z. B. »sandom.example.com«, und allen Namen unterhalb dieser Ebene, z. B. »www.sandom.example.com«, »ftp.sandom.example.com« oder »server.sandom.example.com«.

DNS-Server geben autoritative oder endgültige Antworten auf Anfragen mit den Zonen, für die sie konfiguriert sind.

Weitere Einzelheiten zu diesem Verfahren findest Du auf der [http://en.wikipedia.org/wiki/DNS#Address_resolution_mechanism Wikipedia DNS-Seite].

Warum das wichtig ist?

Der Domänenname, den Du für Deine Active Directory-Domäne auswählst, wird auch die primäre Domäne sein, für die der AD DNS-Server autorisierend ist.

Alle Ihre PCs in Active Directory haben einen Namen innerhalb dieser Domäne. Damit Active Directory ordnungsgemäß funktioniert, müssen alle Computer, die Teil davon sind, diese Namen korrekt auflösen können. Das bedeutet, dass er als DNS-Server für alle PCs innerhalb Ihrer Domäne fungieren muss.

Probleme können entstehen, wenn ein DNS-Konflikt auftritt, d. h. wenn zwei DNS-Server denselben Namen für zwei verschiedene Adressen auflösen. Ein DNS-Konflikt ist nicht dasselbe wie ein IP-Adressenkonflikt, er verhindert nicht den Netzwerkverkehr, aber wenn er auftritt, kann man oft das Problem haben, dass der Verkehr zu Adressen fließt, die man nicht beabsichtigt, oder dass Namen, die man aufgelöst haben möchte, überhaupt nicht aufgelöst werden.

Wenn Du unter anderem Deine AD-Domäne »samdom.example.com« nennen, wäre Ihr AD-DNS-Server natürlich für alle Anfragen auf oder unterhalb der Hierarchieebene »samdom.example.com« maßgebend. Er würde direkt auf alle Anfragen für Namen innerhalb dieser Domäne wie »workstation.samdom.example.com« oder »server.samdom.example.com« oder jeden anderen im DNS-Server konfigurierten Namen antworten.

Wenn Du www.samba.org anfragen würdest, wäre das auch kein Problem. Der Server würde erkennen, dass er für die Domäne [samba.org](http://www.samba.org) nicht maßgeblich ist, und die Anfrage an den Server weiterleiten, der für den Namen zuständig ist, und Dir dann die Antwort zurückschicken.

Was aber, wenn Du auch eine externe Website wie »www.samdom.example.com« hast, die wahrscheinlich von einem anderen externen DNS-Server verwaltet wird? Wenn Du diesen Namen anfordern, wird der DNS-Server feststellen, dass er für die Domäne »samdom.example.com« zuständig ist, und eine Antwort für suchen. Wenn dieser keine Antwort hat, wird die Anfrage nicht an einen anderen Server weitergeleitet, da davon auszugehen ist, dass dieser DNS-Server letzte Autorität für diese Domäne ist. Daher wird dieser Dir die Antwort »kein solcher Name existiert« oder NXDOMAIN zurückgeben.

Auswirkungen auf die Sicherheit

Obwohl es sich technisch gesehen nicht um einen Aspekt der Benennung von Domänen an sich handelt, sind die Sicherheitsaspekte von DNS essenziell zu beachten. Ihr AD DNS-Server enthält eine Liste aller PCs innerhalb Ihres Netzwerks. Die meisten DNS-Server lassen es nicht zu, dass jemand eine vollständige Liste von Domännennamen anfordert (auch als Zonentransfer bekannt). Aber es stellt eine die Möglichkeit dar, dass Geräte außerhalb Ihrer Domäne Namen aus dieser Liste auflösen. Dieses ist eine unnötige Preisgabe interner Informationen und stellt ein mögliches Sicherheitsrisiko dar. Ebenso sind die meisten AD-DNS-Server rekursiv, und der Betrieb eines rekursiven DNS-Servers im Internet hat erhebliche Sicherheitsauswirkungen, die über den Rahmen dieser Dokumentation hinausgehen.

Ebenso solltest Du keine DNS-Anfragen für interne Namen außerhalb des internen Netzwerks senden. Selbst wenn Du dem DNS-Server, an den Du diese sendest, vertraust, ist DNS nicht verschlüsselt, sodass jeder Router, der den Datenverkehr weiterleitet, ein ernsthaftes Sicherheitsrisiko darstellt. Ein Angreifer, der diesen Datenverkehr kontrolliert, könnte den Datenverkehr Ihres PCs an jeden beliebigen Ort leiten.

Aus diesen Gründen sollte ein sicherer AD DNS-Server nur auf Anfragen reagieren, die von innerhalb Ihres Netzwerks kommen, und ein anderer DNS-Server sollte DNS-Anfragen von außerhalb Ihres Netzwerks bearbeiten. Außerdem sollten alle Ihre Arbeitsstationen so konfiguriert werden, dass diese nur den eigenen AD DNS-Server für DNS-Anfragen heranziehen und keine externen DNS-Server. Dies ist bekannt als [https://en.wikipedia.org/wiki/Split-horizon_DNS split-horizon DNS].

4.46.4 NetBIOS-Namen

Bevor Windows DNS nutzte, stützte es sich auf ein anderes Benennungssystem NetBIOS (technisch NetBIOS-NS), und den Windows Internet Name Service (WINS).

NetBIOS ähnelt DNS insofern, als es als Verzeichnisdienst dienen kann, ist aber eingeschränkter, da es keine Bestimmungen für eine Namenshierarchie hat und die Namen auf 15 Zeichen begrenzt waren. NetBIOS bietet jedoch ein Mittel zur Peer-to-Peer-Namensauflösung über die Layer-2-Rundfunkdomäne (alle PCs innerhalb desselben Subnetzes).

Microsoft hat dies mit WINS erweitert, um die Namensauflösung über Layer 3 (geroutete) Netzwerke zu ermöglichen. Wenn die Namensauflösung in einem Netzwerk ohne DNS-Dienst funktioniert, wird diese wahrscheinlich von NetBIOS durchgeführt.

Die Tage dieser Systeme liegen zwar größtenteils hinter uns, aber Spuren dieses Altsystems sind noch überall in Windows zu finden.

Beispielsweise sind einige Aspekte des Windows-Netzwerks, wie Networking Neighbourhood und seine Nachkommen, immer noch auf diesen Dienst angewiesen. Insbesondere hat jede AD-Domäne neben ihrem traditionellen DNS-Namen auch einen NetBIOS-Namen. Und jeder Computer in Ihrer Domäne hat auch einen NetBIOS-Namen (selbst wenn Du den NetBIOS-Namensdienst ausschalten). In den meisten Fällen sind dies die ersten 15 Zeichen des PC-Namens.

Warum das wichtig ist?

So wie DNS-Namen in Konflikt geraten können, können auch NetBIOS-Namen in Konflikt geraten.

In den meisten Fällen stellt dies kein Problem dar. Windows fragt NetBIOS als letzte Möglichkeit zur Namensauflösung ab, und ohne einen WINS-Server in Ihrem Netzwerk können NetBIOS-Namen die Schicht 2 (das Subnetz) nicht überqueren. Active Directory verhindert zwar bereits, dass Du PCs mit doppelten Namen hast, aber nicht, dass Du doppelte NetBIOS-Namen haben, was im Allgemeinen nur dann der Fall wäre, wenn die ersten 15 Ziffern Ihres Computernamens identisch wären. Solche Namenskonflikte sollten vermieden werden.

NetBIOS-Domänenbenennung

Da NetBIOS [<https://support.microsoft.com/en-us/kb/188997>] sehr wenige Möglichkeiten hat, welche Domännennamen akzeptabel sind, kannst Du nur wenig tun, um mögliche Namenskonflikte zu vermeiden.

Typischerweise wird empfohlen, den ersten Teil des Domännennamens für die NetBIOS-Domäne zu verwenden (Anmerkung: dies ist ein anderer Name für „Arbeitsgruppe“). Wenn Ihr Domänenname zum Beispiel „samdom.example.com“ lautet, kannst Du den NetBIOS-Namen „SAMDOM“ wählen.

Was auch immer Du für Deinen NetBIOS-Namen verwendest, achte darauf, dass dieser nur aus einem Wort besteht, nicht länger als 15 Zeichen ist und keine Satzzeichen enthält, auch keine Punkte , . ' . Dies scheint besonders bei Windows 10-Clients wichtig zu sein, da es Berichte gibt, dass diese der Domäne nicht beitreten können, wenn der NetBIOS-Domänenname einen Punkt enthält.

4.46.5 Wie soll ich meine Domäne benennen?

Bevor wir uns Ihre Optionen ansehen, lass uns einige wünschenswerte Eigenschaften betrachten, die unser Domänenname haben sollte:

- Der Domänenname sollte weltweit eindeutig sein. Dadurch wird sichergestellt, dass der Name unabhängig von der Konfiguration des Computers für die DNS-Auflösung entweder richtig aufgelöst wird oder keine Domäne (NXDOMAIN) ergibt. Es sollte nie einen Konflikt mit dem Domännennamen geben!
- Die Domäne sollte mit Ihrer Organisation assoziiert sein. Der Domänenname sollte idealerweise einen Bezug zu Ihrer Organisation haben, damit er leicht zu merken ist.

- Die Domäne sollte unter Ihrer Kontrolle stehen. Ein Domänenname, den Du kontrollierst (weil Du der eingetragene Eigentümer sind), hilft, böswillige Nutzung zu verhindern. Die Registrierung eines Domännennamens ist billig und für jedes Unternehmen ohnehin wünschenswert.
- Der Domänenname sollte immer noch ein gültiger Domänenname sein, sodass Du auf Wunsch SSL-Zertifikate von Drittanbietern dafür erhalten können.
- Der FQDN für einen Active-Directory-Domännennamen ist auf 64 Byte begrenzt, einschließlich der Punkte, ein Active-Directory-Servername zum Beispiel: »s4ad01.office.example.tld«
- Welchen Domännennamen Du auch immer verwendest, dieser sollte nicht über das Internet auflösbar sein. Es ist keine gute Idee, einen AD-Domänen-Computer direkt mit dem Internet zu verbinden.

Mit diesen Kriterien im Hinterkopf können wir uns nun einige Ihrer Optionen ansehen:

4.46.6 Subdomain einer eigenen Domäne

In diesem Szenario würdest Du Deine Domäne nach dem Muster »subdomain.domainyouown.tld« benennen, z. B. »samdom.example.com«. Dies ist in der Regel die beste Option, die Du wählen kannst! Dies steht auch im Einklang mit den aktuellen [<https://technet.microsoft.com/en-us/library/cc738121%28WS.10%29.aspx> best practices] von Microsoft.

Der Name der Subdomain kann zwar beliebig gewählt werden, aber es ist wahrscheinlich eine gute Idee, ihn kurz und einfach zu halten (z. B. »ad.«). Diese Art von Name erfüllt alle oben genannten Kriterien, die wir für einen wünschenswerten Domännennamen aufgestellt haben, vor allem aber:

- Er ist weltweit einzigartig. Da Du die Registrierung der Domäne im Netz (und vermutlich auch deren DNS-Einträge) kontrollieren, kannst Du sicherstellen, dass die von Ihnen intern verwendete Domäne nicht nach außen hin aufgelöst wird.
- Es handelt sich um einen gültigen Domännennamen für den Abruf von SSL-Zertifikaten von Drittanbietern.

Wichtiger Hinweis

Bei der Benennung Ihrer Domäne erzeugen Windows und samba-tool auch einen [<https://technet.microsoft.com/en-us/library/cc961556.aspx> suggestion] Legacy-NetBIOS-Domännennamen.

Standardmäßig sind dies die ersten 15 Zeichen des Domännennamens ganz links.

Wenn Ihre Domäne also „ad.example.com“ heißt, dann wäre der Standardvorschlag einfach „AD“.

Die Auswahl eines solchen NetBIOS-Domännennamens wäre keine gute Idee, da es sehr wahrscheinlich zu Konflikten mit anderen Domänen kommen würde, die denselben NetBIOS-Namen haben. Dies würde ein Problem darstellen, wenn Du jemals eine Vertrauensbeziehung zwischen diesen beiden Domänen einrichten müsstest. Wähle stattdessen einen benutzerdefinierten Namen, der auf Ihrem Domännennamen basiert, z. B. »BEISPIEL« für eine Domäne namens „ad.example.com“.

Häufige Einwände

Meine Benutzer-Logins stimmen nicht mit meiner E-Mail überein

Es ist richtig, dass der Teil des Benutzernamens, der auf das @-Zeichen folgt, der User Principle Name Suffix (UPN-Suffix), standardmäßig dem Domänennamen entspricht und daher bei diesem Schema standardmäßig „subdomain.domain.tld“ lautet. Der UPN Suffix ist jedoch beliebig und konfigurierbar. Du kannst [<https://technet.microsoft.com/en-us/library/cc772007.aspx> konfigurieren], was immer Du willst, einschließlich der E-Mail Ihrer Benutzer. Er muss für alle Sicherheitsprinzipalobjekte innerhalb einer Verzeichnisstruktur eindeutig sein. Das bedeutet, dass der Präfix eines UPNs wiederverwendet werden kann, nur nicht mit demselben Suffix.

Er unterliegt den folgenden Beschränkungen:

Er muss der DNS-Name einer Domäne sein, muss aber nicht der Name der Domäne sein, die den Benutzer enthält. Es muss der Name einer Domäne in der aktuellen Domänenstruktur sein (was in Samba AD dasselbe bedeutet), oder ein alternativer Name, der im upnSuffixes-Attribut des Containers Partitionen im Container Konfiguration aufgeführt ist.

Der Stil des Domänennamens ist zu lang

Der Zusatz des Suffixes kann so kurz sein, wie Du es Dir wünscht (die Verwendung von nur „ad“ oder „ds“ ist sehr üblich). Das Eintippen des Domänennamens kann jedoch ganz vermieden werden, indem die Variablen DNS-Suffix und DNS-Suffix-Suchliste gesetzt werden. Wenn diese Variablen gesetzt sind, versuchen die Clients, Single-Label-Domainnamen wie „server“ als „server.dnssuffix.tld“ aufzulösen. Dies gilt sogar für Zertifikate, sodass Du ein Zertifikat für einen internen Server ausstellen können, das für »<https://server/>« anstelle von »<https://server.samdom.example.com>« gilt, wenn Du möchtest. Und wenn Du irgendwann einmal die Verwendung des DNS-Such-Suffixes bei einer DNS-Anfrage vermeiden müssen, kannst Du dies tun, indem Du den FQDN angibst und dabei daran denkst, den abschließenden ».« für die Root-Zone einzuschließen.

Dies funktioniert nicht mit meiner externen Domäne

Diese Annahme ist falsch. Der AD DNS-Server ist nur für diese eine Subdomain und die darunter liegenden Namen autoritativ. Er ist nicht für andere Domänennamen zuständig. Wenn Ihr AD-Domänenname also „samdom.example.com“ lautet und Du möchtest den Namen „www.example.com“ auflösen, wird erkannt, dass der DNS-Server für „www.example.com“ nicht autoritativ ist, und die Anfrage an den externen Server weiterleiten, der für diese Domäne autoritativ ist.

Mein NetBIOS-Name kann in Konflikt geraten

Eine berechtigte Sorge. Der von samba-tool und im Windows DC Promo-Assistenten vorgeschlagene Name ist jedoch nur ein Vorschlag. Du kannst jeden beliebigen NetBIOS-Namen wählen. Die Wahl eines Namens, der auf Ihrem Domänennamen basiert, könnte eine gute Alternative sein, oder wähle einen anderen assoziativen, aber eindeutigen Namen für den NetBIOS-Domänennamen.

Unterschiedliche Namen verwenden, um Hostnamen intern und extern aufzulösen.

Ja, da bei diesem Schema kein DNS-Dienst außerhalb Ihres Netzes Namen innerhalb des Netzes auflösen kann, ist ein anderer DNS-Name erforderlich, um denselben Computer innerhalb Deines Netzes aufzulösen. In den meisten Fällen ist dies eine gute Sache, denn die interne und die externe Adresse von Computern sind im Allgemeinen grundverschieden und haben unterschiedliche IP-Adressen.

In manchen Situationen ist es jedoch nicht ratsam, diese zusätzliche Komplikation in Ihre Konfigurationen aufzunehmen. Wenn Du z. B. E-Mail-Einstellungen verteilen, die von den Benutzern konfiguriert werden müssen, könnte die zusätzliche Komplexität, die sich aus der Verwendung eines unterschiedlichen E-Mail-Schemas extern und intern ergibt, für die Benutzer zu kompliziert sein. Auf mobilen Geräten ist dieses Schema möglicherweise nicht einmal praktikabel. Zum Glück gibt es einige Lösungen für dieses Problem:

- Erlaubst Du, dass der Datenverkehr für den externen Namen nach außen und zurück in Ihr Netzwerk geleitet wird.

Für diese Einrichtung ist oft keine zusätzliche Konfiguration erforderlich. Der an externe IP-Adressen gebundene Datenverkehr kann im Allgemeinen wie jeder andere an das Internet gebundene Datenverkehr behandelt werden, auch wenn sein Ziel letztendlich wieder innerhalb Ihres Netzes liegt.

- Erstelle eine DNS-Zone, die nur den gewünschten Namen auflöst.:

Es gibt einen Trick, mit dem Du in AD DNS nur einen einzigen Host innerhalb einer Zone auflösen können, während der Rest der Hosts normal vom externen Server aufgelöst wird. Erstelle eine DNS-Zone mit dem Namen „host.domain.tld“, zum Beispiel „mail.example.com“. Erstelle innerhalb der Zone einen einzelnen A- oder CNAME-Eintrag (CNAME ist wahrscheinlich vorzuziehen), wobei Du den Namen des Eintrags leer läßt. Wie Du im Dialogfeld sehen, wird dieser Name zur Auflösung der übergeordneten Domäne verwendet, in diesem Fall „host.domain.tld“.

„host.domain.tld“ wird wie von Dir angegeben von Ihrem DNS-Server aufgelöst, während Anfragen an andere Hosts unter „domain.tld“ extern aufgelöst werden, da „host.domain.tld“ und „domain.tld“ verschiedenen Zonen entsprechen. Wenn Du einen CNAME als übergeordneten Eintrag verwendest, kannst Du diesen auf den Eintrag in Ihrem internen Domänennamen zurückverweisen.

4.46.7 Verwendung einer ungültigen TLD

In diesem Szenario würdest Du Deine Domäne im Format „domain.invalid.tld“ benennen, z. B. »SAMDOM.loc«. Die Verwendung einer ungültigen Top-Level-Domain (TLD) wie .local oder .internal war früher eine sehr gängige Praxis. Tatsächlich waren alle Versionen von Microsofts Small Business Servern so konfiguriert, dass diese eine Domäne in Form von „domain.local“ verwendeten. Da die TLD .local offiziell von der ICANN reserviert ist, kannst Du auch sicher sein, dass kein externer DNS-Server diese Domäne auflösen wird. Diese Art von Namen hat jedoch einige wesentliche Probleme:

- Die TLD .local wird von einigen Zeroconf-Systemen verwendet, vor allem von Apples Bonjour-Dienst. Die gleichzeitige Verwendung dieser beiden TLDs wird nicht korrekt funktionieren.
- Ungültige TLDs wie .local oder .internal werden bald nicht mehr in der Lage sein, SSL-Zertifikate von einem der großen Zertifikatsanbieter zu erhalten. Das CA/Browser Forum hat [<https://www.digicert.com/internal-names.htm?SSAID=314743> beschlossen], dass für diese ungültigen Domains ab dem 1. November 2015 keine Zertifikate mehr ausgestellt werden sollen. Tatsächlich kannst Du jetzt kein Zertifikat für diese Namen erwerben, wenn diese nach diesem Datum ablaufen. Dies gilt auch für Subject Alternative Names (SAN), die in ansonsten gültigen Zertifikaten verwendet werden (dies ist eine sehr häufige Konfiguration für Microsoft Exchange). Interne Zertifizierungsstellen haben zwar keine solche Einschränkung, aber es ist immer gut, diese Möglichkeit zu haben.
- Es ist möglich, dass die ungültige TLD, die Du jetzt verwendest, in Zukunft zu einer gültigen TLD wird. Während .local von der ICANN reserviert ist, ist für das TLD-System derzeit eine enorme [<http://www.gtld.com/>

Erweiterung] der von ihm unterstützten generischen TLD (gTLD) geplant, von 22 auf über tausend neue Namen. Dieser Trend wird sich wahrscheinlich fortsetzen.

Aus demselben Grund sollten Namen mit anderen ungültigen TLDs vermieden werden, einschließlich .internal und .lan.

4.46.8 Verwendung Ihres externen Domänennamens

In diesem Szenario verwendest Du einfach intern Ihren externen Domänennamen im Format „domain.tld“, zum Beispiel „example.com“. Dies ist zwar eine gute Option, kann aber auch Ihr DNS-System unnötig kompliziert machen. Wie bereits erläutert, besteht bei einem solchen System die Möglichkeit eines Domänennamenkonflikts, in der Regel zwischen einem Namen, der entweder intern nicht vorhanden ist, oder einem Namen, der extern anders aufgelöst wird als intern. Dies kann dadurch gelöst werden, dass Du die Einträge auf dem externen Server auf Ihrem internen Server duplizierst. Dies kann jedoch unpraktisch sein, wenn Du viele externe DNS-Einträge hast oder diese häufig wechselst. Du kannst und solltest ein internes Benennungsschema wählen, das niemals mit Ihrem externen Benennungsschema kollidiert.

4.46.9 Verwendung eines generischen Domänennamens

Es wurde vorgeschlagen, dass für Organisationen, die viele Fusionen und Übernahmen durchführen, die Verwendung eines generischen Domänennamens wie „corp.local“ eine gute Option sein könnte. Da die Umbenennung und Migration von Domänen oft ein schwieriges und kostspieliges Unterfangen ist, mag dies eine gewisse Berechtigung haben. Aber es gibt keine Garantie dafür, dass der gewählte Domänenname nicht von einem anderen Verwalter gewählt wird, der in dieselbe Richtung denkt wie man selbst. Dies würde eine Domänenfusion erheblich erschweren. Außerdem kann der generische Name zwar vor den Nutzern durch benutzerdefinierte UPN-Suffixe und DNS-Such-Suffixe verborgen werden, aber ein alter Domänenname mit garantierter Einzigartigkeit könnte auf die gleiche Weise verborgen werden.

4.46.10 Verwendung eines anderen Domänennamens

In diesem Szenario verwendest Du einen anderen, nicht verwendeten Domänennamen als Ihren primären Internet-Domänennamen. Du kannst zum Beispiel eine andere TLD („example.net“ im Gegensatz zu „example.com“) oder einen völlig anderen Domänennamen verwenden, der jedoch ganz normal bei der ICANN registriert ist. Der angebliche Vorteil dieses Systems ist die Möglichkeit, einige Domänennamen (z. B. „mail.domain.tld“) intern und extern über denselben Namen aufzulösen.

Dies ist zwar im Großen und Ganzen richtig, doch kann derselbe Effekt auch bei anderen Systemen durch einige DNS-Tricks (siehe oben) erzielt werden. Außerdem besteht jedes Mal, wenn Du Namen extern anders auflöst als intern, die Möglichkeit eines unerwünschten DNS-Namenskonflikts, sodass es fraglich ist, ob es überhaupt wünschenswert ist, dies für die gesamte Domäne zu tun.

This scheme also leaks a minor amount of sensitive information (the domain name) onto the net, and represents a minor additional cost (the cost of the domain registration), while offering only marginal advantages. It may however be a valid option for some organizations, such a scheme is often used by ISPs and other internet focused organizations.

4.47 LVM des Servers anpassen

Autor des Abschnitts: @cweikl @MachtDochNiX

Die nachstehenden Hinweise sind dafür gedacht,

Tipp: Alternativ kannst Du die zweite Platte mit anderen Größenangaben auch mit linuxmuster-prepare im Zuge des Setup ausführen. Möchtest Du dies so durchführen, kannst Du nachstehende Punkte überspringen.

Solltest Du Dich für eine andere Größeneinteilung oder für eine Einrichtung auf realen Festplatten entschieden haben, dann geht es hier für Dich weiter.

LV Name	LV Pfad	Mountpoint	Größe
var	/dev/sg_srv/var	/var	20G
linbo	/dev/sg_srv/linbo	/srv/linbo	80G
global	/dev/sg_srv/global	/srv/samba/global	20G
default-school	/dev/sg_srv/default-school	/srv/samba/schools/default-school	80G

4.47.1 Einrichtung eines LVM auf der 2. HDD

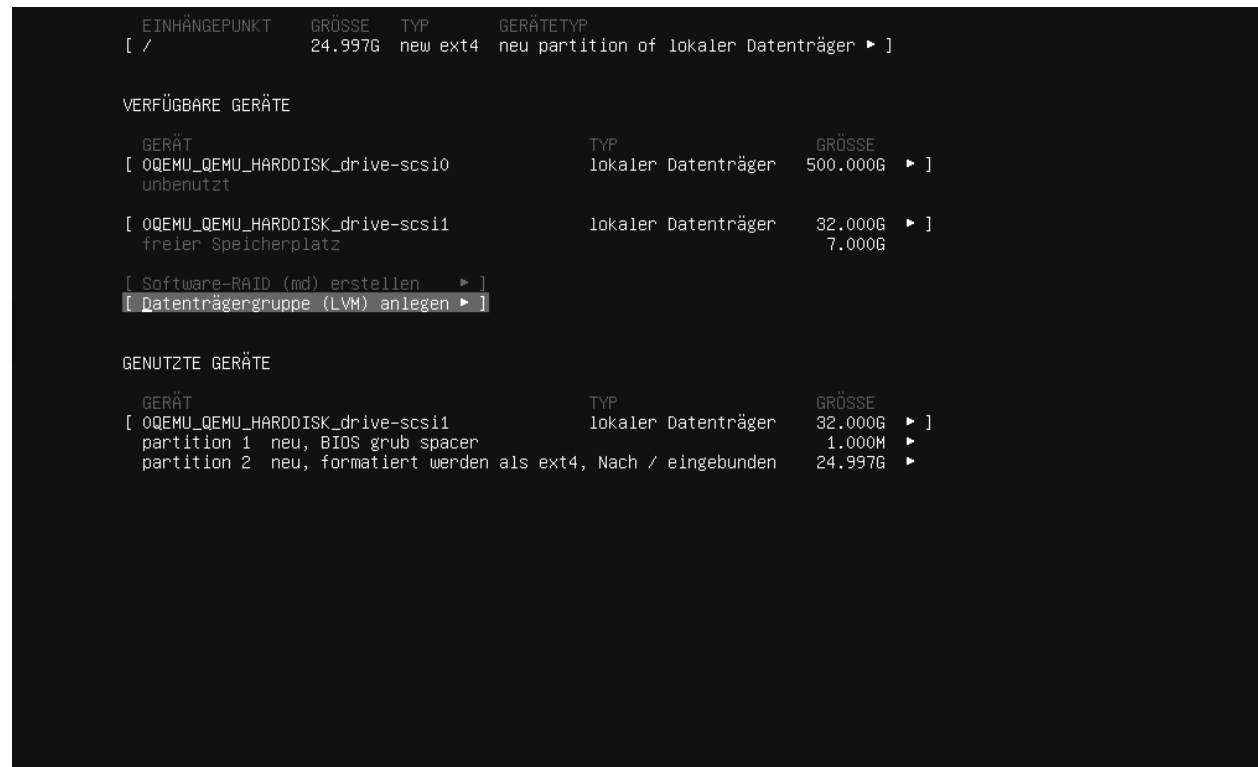


Abb. 504: Lege ein LVM an

Wähle den Eintrag Datenträgergruppe (LVM) anlegen aus.

Hier gibst Du einen Namen für die LVM Volume Group an (z.B. sg_srv) und wählst das Gerät aus wo es erstellt werden soll. Erstellen schließt dieses Fenster.

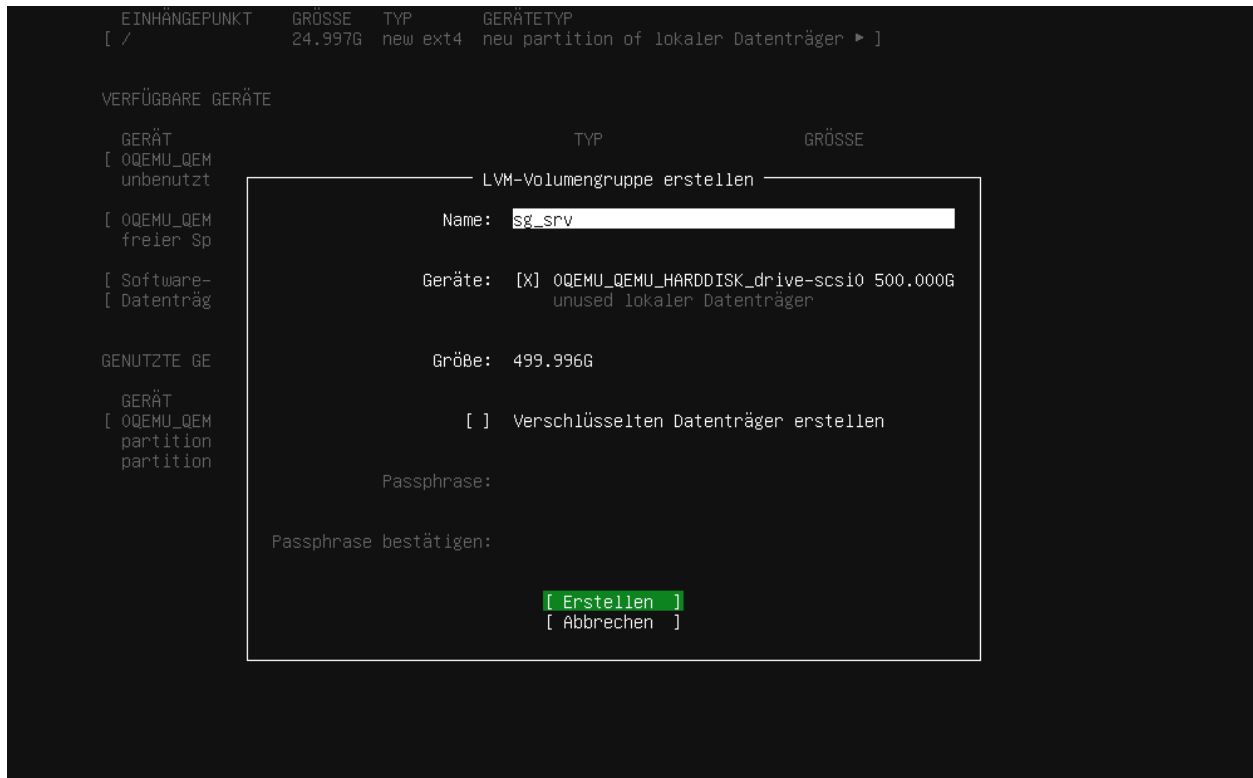


Abb. 505: LVM-Volume erstellen

Bei **VERFÜGBARE GERÄTE** gilt es nun in die angelegte LVM `volume group` die benötigten Logical Volume anzulegen.

Bei **VERFÜGBARE GERÄTE** findest Du die von Dir zuvor angelegte „LVM volume group“. Diese markierst Du , um dann **Create Logical Volume** auszuwählen.

Die benötigten Daten entnimmst Du aus der obigen Tabelle. Die Zuordnung ist folgende:

Name	→	LV Name
Size	→	Größe
Mount	→	Mountpoint

Bei **Format** wählst Du, wie in der Grafik gezeigt „ext4“.

Wieder schließt Du diese Aktion mit **[Erstellen]** ab.

Die letzten zwei Schritte wiederholst Du für die anderen Positionen der Tabelle ...

... linbo:

... global:

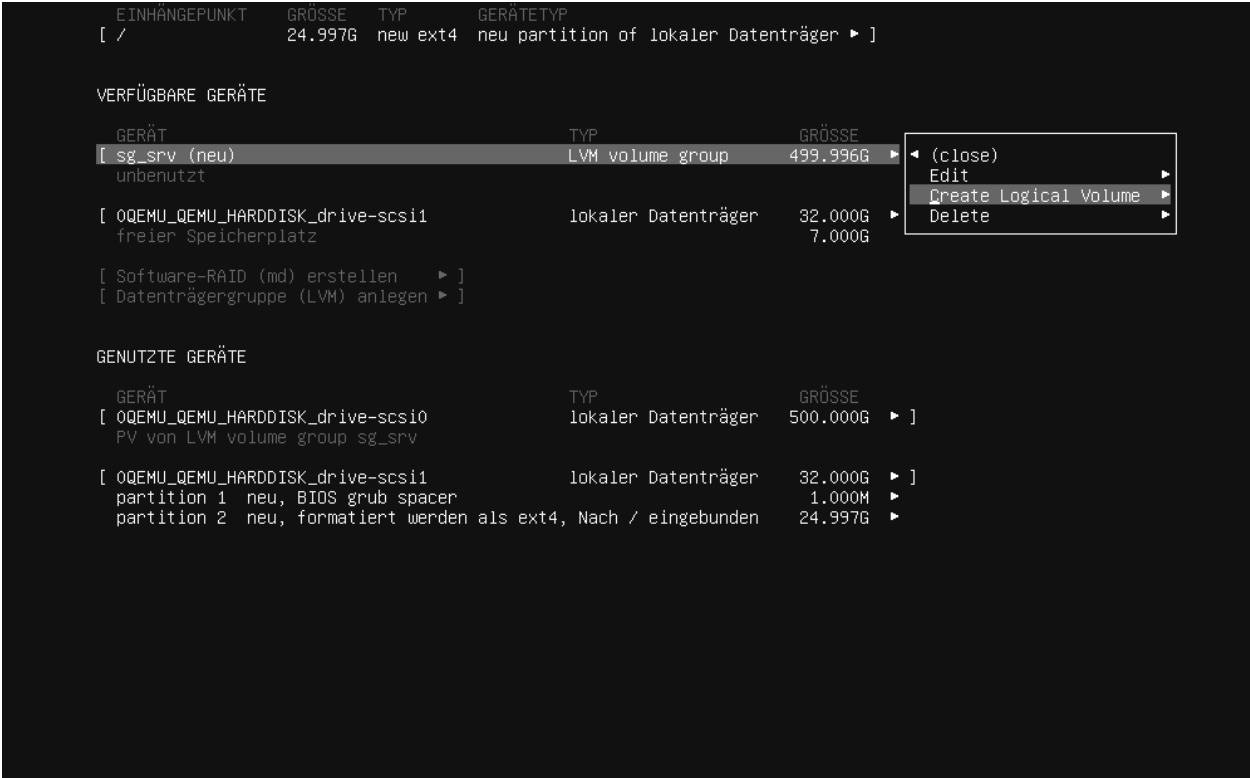


Abb. 506: Lege ein Logical Volume an

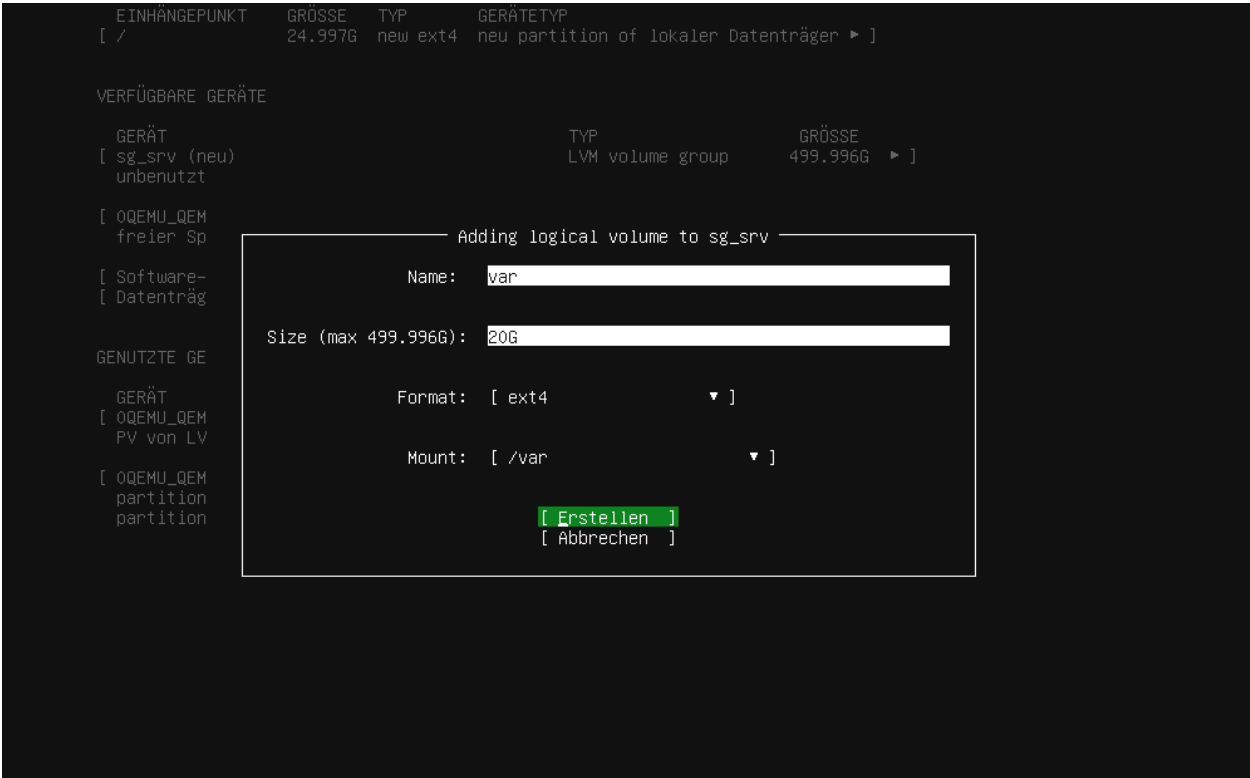


Abb. 507: Lege die Größe des Logical Volume fest

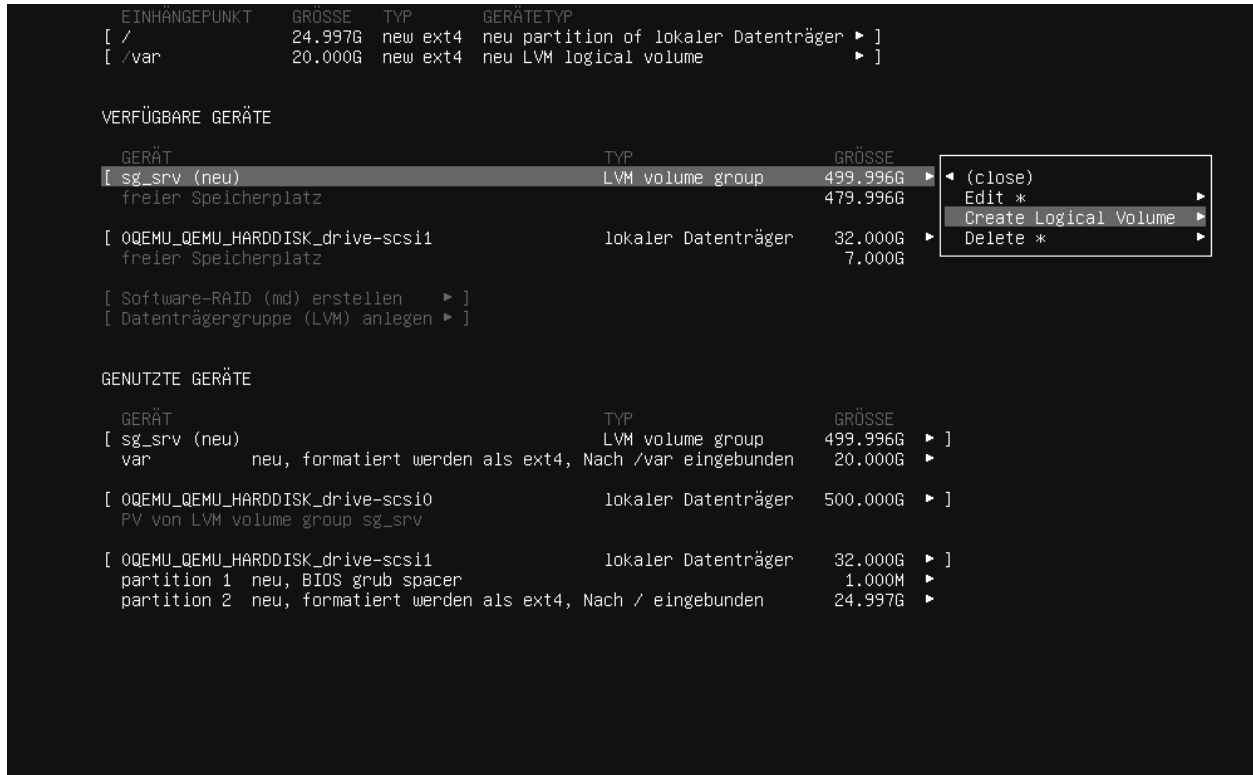


Abb. 508: Volume für LINBO festlegen

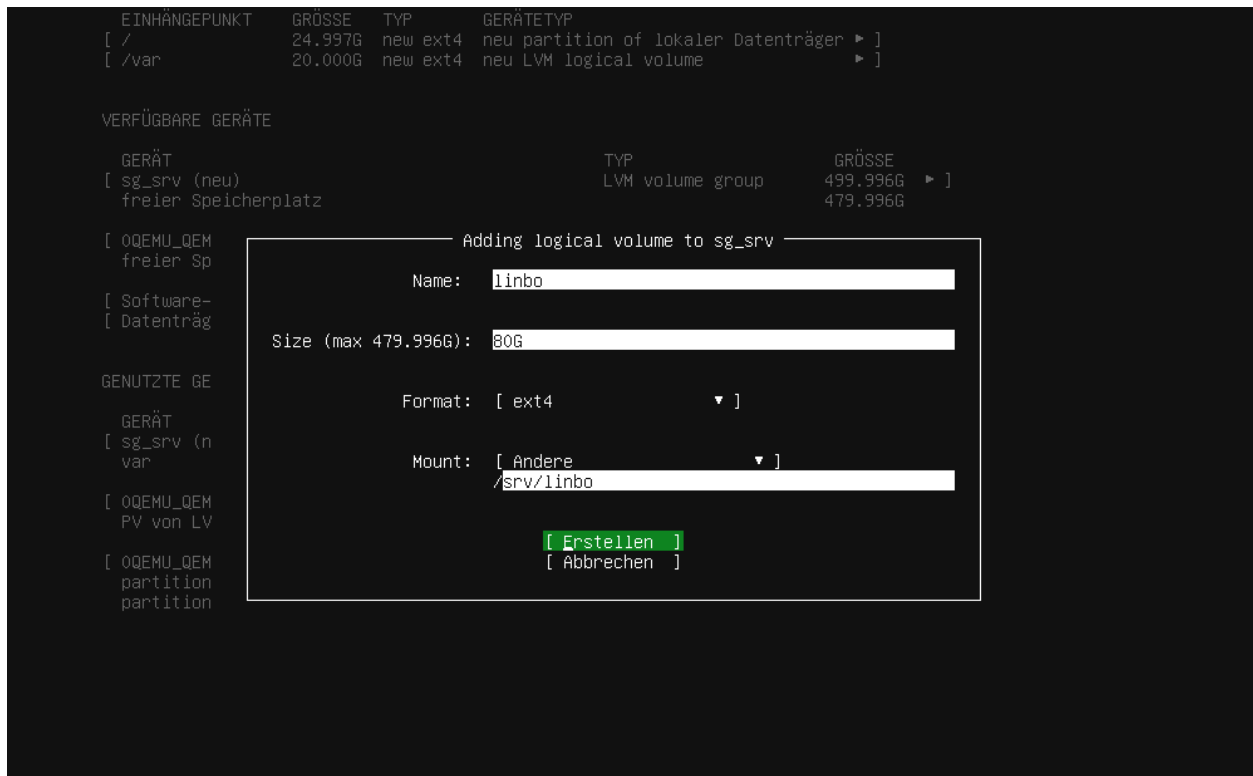


Abb. 509: Größe für LINBO festlegen

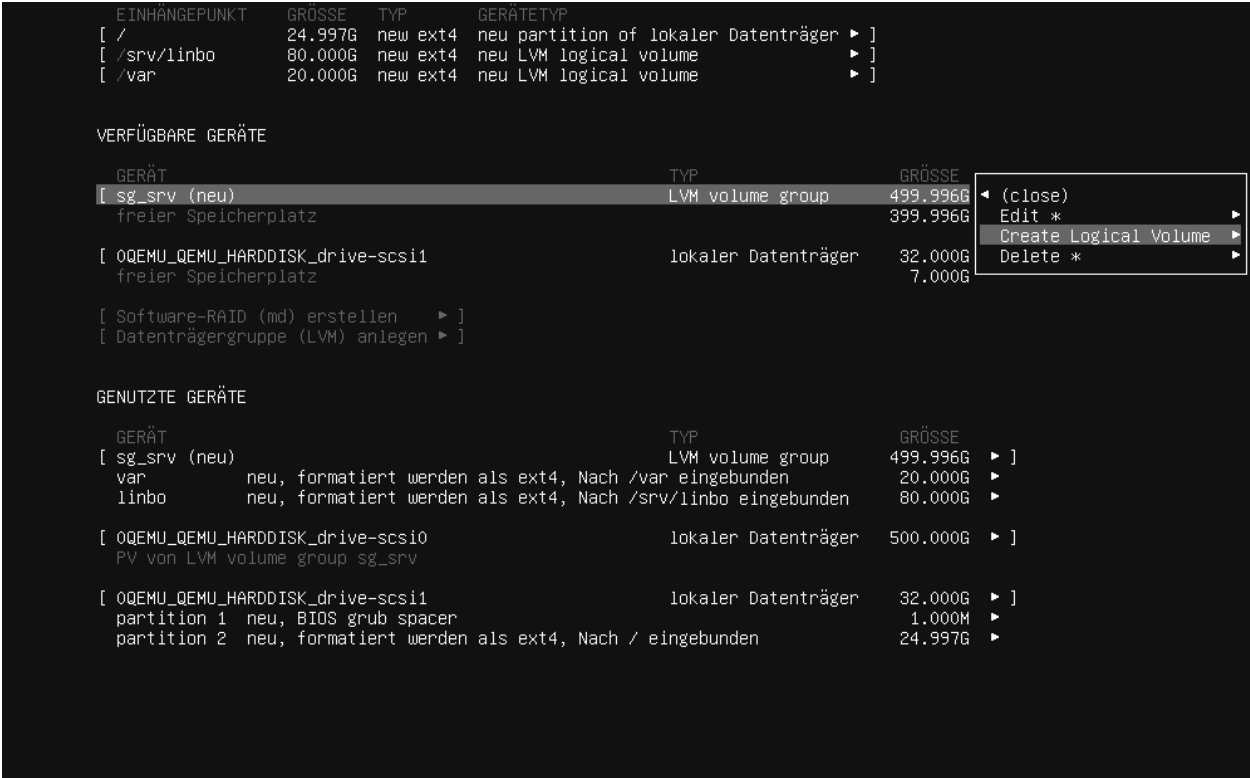


Abb. 510: Volume für global festlegen

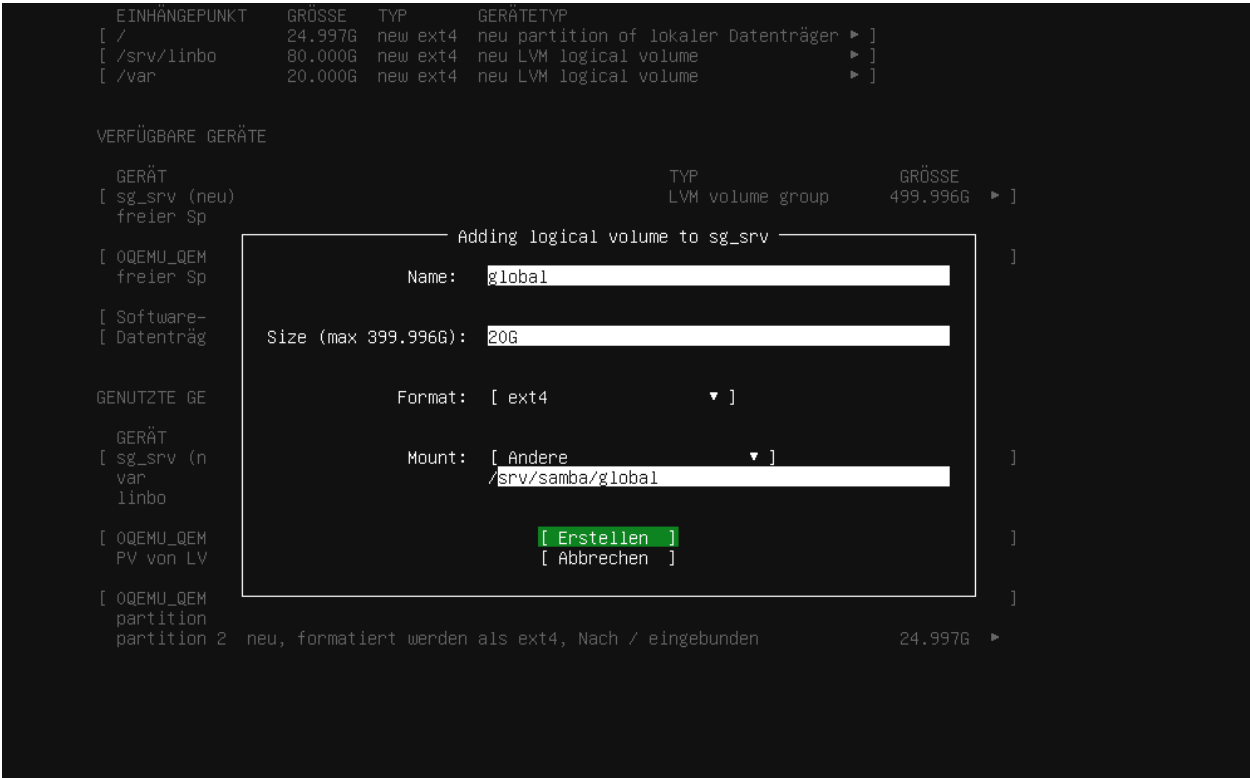


Abb. 511: Größe für global festlegen

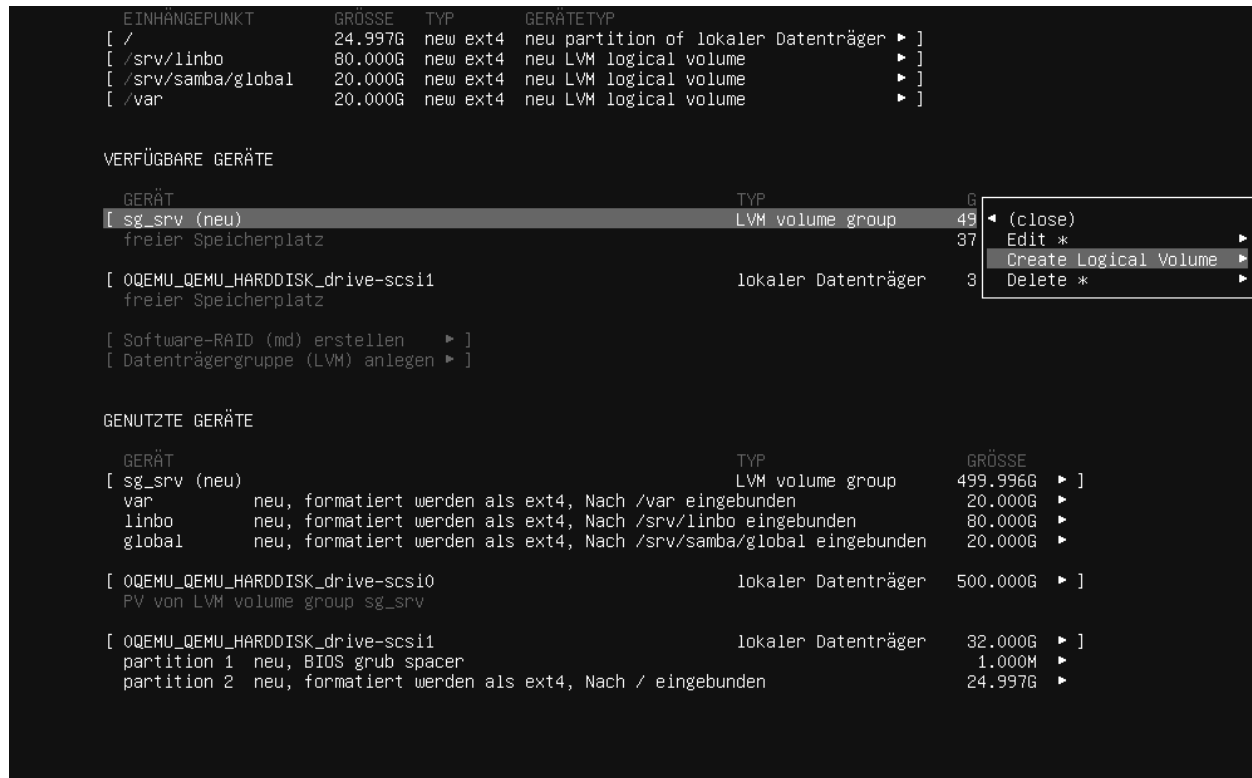


Abb. 512: Volume für default-school definieren

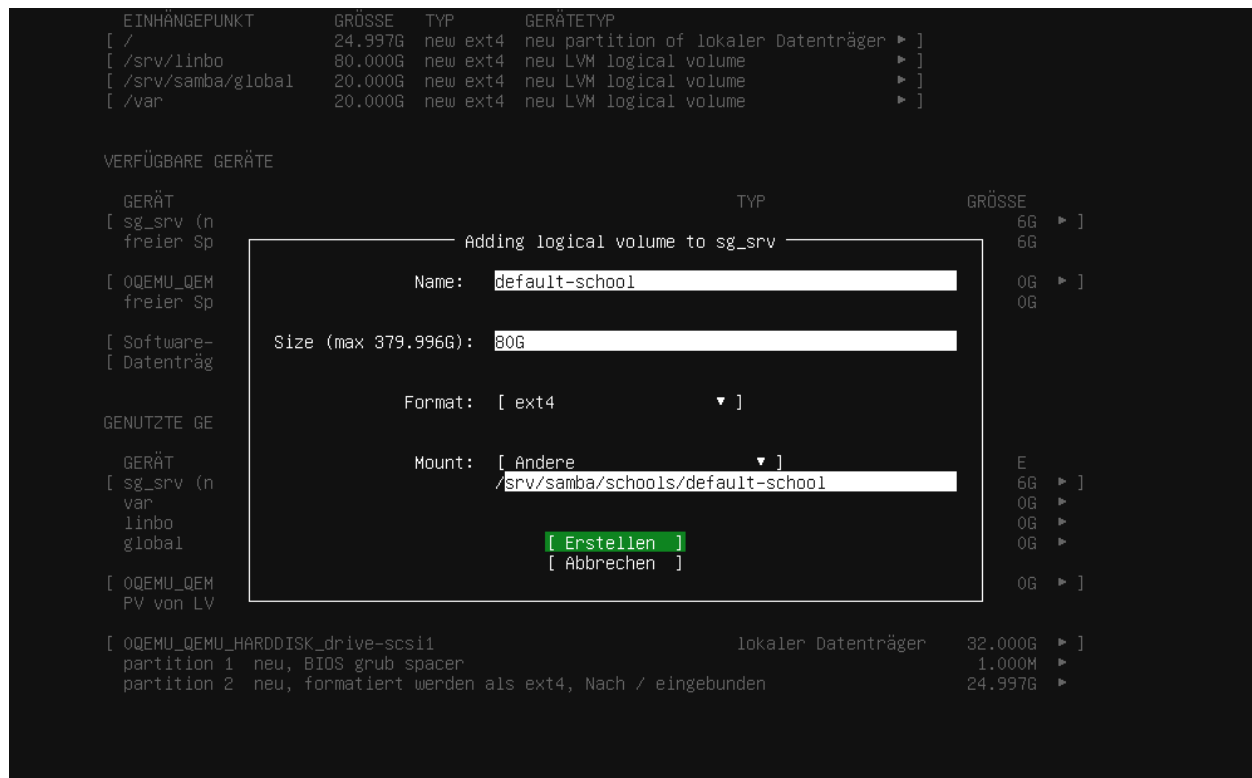


Abb. 513: Größe für das Volume default-school festlegen

... default-school:

Zum Abschluss werden Dir die Partitionsierungseinstellungen gemäß Deiner Eingaben angezeigt.

```

EINHÄNGEPUNKT      GRÖS  GRÖSSE  TYP      GERÄTETYP
[ /                24.997G  new ext4  neu partition of lokaler Datenträger ▶ ]
[ /srv/linbo       80.000G  new ext4  neu LVM logical volume                ▶ ]
[ /srv/samba/schools/default-school 80.000G  new ext4  neu LVM logical volume                ▶ ]
[ /srv/samba/global 20.000G  new ext4  neu LVM logical volume                ▶ ]
[ /var             20.000G  new ext4  neu LVM logical volume                ▶ ]

VERFÜGBARE GERÄTE

GERÄT              TYP              GRÖSSE
[ sg_srv (neu)      LVM volume group 499.996G ▶ ]
freier Speicherplatz                299.996G

[ OQEMU_QEMU_HARDDISK_drive-scsi1    lokaler Datenträger 32.000G ▶ ]
freier Speicherplatz                7.000G

[ Software-RAID (md) erstellen ▶ ]
[ Datenträgergruppe (LVM) anlegen ▶ ]

GENUTZTE GERÄTE

GERÄT              TYP              GRÖSSE
[ sg_srv (neu)      LVM volume group 499.996G ▶ ]
var                neu, formatiert werden als ext4, Nach /var eingebunden 20.000G ▶ ]
linbo              neu, formatiert werden als ext4, Nach /srv/linbo eingebunden 80.000G ▶ ]
global             neu, formatiert werden als ext4, Nach /srv/samba/global eingebunden 20.000G ▶ ]
default-school     neu, formatiert werden als ext4, Nach /srv/samba/schools/default-school eingebunden 80.000G ▶ ]

[ OQEMU_QEMU_HARDDISK_drive-scsi0      lokaler Datenträger 500.000G ▶ ]
PV von LVM volume group sg_srv

[ OQEMU_QEMU_HARDDISK_drive-scsi1      lokaler Datenträger 32.000G ▶ ]
partition 1    neu, BIOS grub spacer 1.000M ▶ ]
partition 2    neu, formatiert werden als ext4, Nach / eingebunden 24.997G ▶ ]

[ Erledigt ]
[ Zurücksetzen ]
[ Zurück ]

```

Abb. 514: Überblick über die Partitionseinstellungen

4.47.2 Einrichtung ohne LVM auf HDD

Ohne LVM sind die Mount Points `/var`, `/srv/linbo`, `/srv/samba/global` und `/srv/samba/schools/default-school` auf die HDD(s) beziehungsweise auf einzelne Partitionen zu legen.

Auf eine detaillierte Beschreibung verzichten wir hier. Wir gehen davon aus, dass Du weißt, wie Du es umsetzen musst, wenn Du es so einrichten willst.

Die vorhergehende Beschreibung bietet Dir sicherlich genügende Hinweise, daher verlinken wir sie hier noch einmal für Dich.

Quota-Einstellungen überprüfen

Hinweis: Nachstehende Schritte musst Du nur durchführen, wenn Du **nicht** mit den default-Einstellungen installierst.

Überspringe diesen Punkt und gehe zu: *Bezeichnung des Speichermediums für das LVM ermitteln*

Hast Du bei der Installation des Servers als Speichermedium **kein LVM manuell** angelegt, dann führst Du nachstehende Schritte aus. In allen anderen Fällen überspringst Du diesen Schritt.

```
nano /etc/fstab
```

Mit diesem Aufruf öffnest Du die Datei `/etc/fstab` mit dem Editor nano auf, damit Du die Ersetzung von `defaults` durchführen kannst. Das ist der Ersetzungstext:

```
user_xattr,acl,usrjquota=aquota.user,grpjquota=aquota.group,jqfmt=vfsv0,barrier=1
```

Vor Deiner Ersetzung:

```
/dev/vg0/var          /var ext4 defaults 0 1
/dev/vg0/linbo        /srv/linbo ext4 defaults 0 1
/dev/vg0/global       /srv/samba/global ext4 defaults 0 1
/dev/vg0/default-school /srv/samba/schools/default-school ext4 defaults 0 1
```

Nach der Änderung:

```
/dev/vg0/var          /var ext4 defaults 0 1
/dev/vg0/linbo        /srv/linbo ext4 defaults 0 1
/dev/vg0/global       /srv/samba/global ext4 user_xattr,acl,usrjquota=aquota.user,
↪grpjquota=aquota.group,jqfmt=vfsv0,barrier=1 0 1
/dev/vg0/default-school /srv/samba/schools/default-school ext4 user_xattr,acl,
↪usrjquota=aquota.user,grpjquota=aquota.group,jqfmt=vfsv0,barrier=1 0 1
```

Speichere die Einstellung mit `Strg+w` und verlasse den Editor mit `Strg+x`.

Lade die Eintragungen aus der Datei `/etc/fstab` neu mit `mount -a`. Ggf. erkennst Du auch noch Fehler, die sich aufgrund von Tippfehlern in der Datei `/etc/fstab` ergeben. Behebe diese zuerst, bevor Du fortfährst.

Bezeichnung des Speichermediums für das LVM ermitteln

Betrifft Dich nur, wenn Du die default-Einstellungen verwendest.

```
lsblk
```

Aus dessen Ausgabe kannst Du Namen für die weitere Verwendung ermitteln. Hier wäre er beispielhaft `/dev/sdb/`

```
linuxadmin@server:~$ lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda          8:0    0   25G  0 disk
├─sda1       8:1    0    1M  0 part
└─sda2       8:2    0   25G  0 part /
sdb          8:16   0  100G  0 disk
sr0         11:0    1 1024M  0 rom
```

Abb. 515: Ausgabe des `lsblk` - Befehls

Bemerkung: Notiere Dir HDD- und Partition-Bezeichnungen für die spätere Verwendung.
