linuxmuster.net

Release 7.1

linuxmuster.net

20.03.2024

Über

Herzlich Willkommen zur Dokumentation von linuxmuster.net v7.1!

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 verschieden gelagert.

KAPITEL 1

Kennst Du linuxmuster.net noch nicht,

dann empfehlen wir Dir das Kapitel

Was ist linuxmuster.net?

KAPITEL 2

Hattest Du schon Kontakt mit einer Installation von

linuxmuster.net Version 7?

Dann ist das Kapitel *Was ist neu in 7.1?* für Dich von Interesse.

Mit der Version 7.1 gibt es einige Neuerungen. Das zuvor genannte Kapitel *Was ist linuxmuster.net?* geht auf diese Neuerungen detailliert ein. Ein Blick lohnt sich daher auf alle Fälle.

KAPITEL 3

Installation from Scratch

Diese Dokumentation führt Dich durch die Vorbereitung der Virtualisierungslösungen Proxmox, um linuxmuster.net 7.1 installieren zu können. Hierzu gehört die spezifische Einrichtung des Netzwerks sowie die Vorbereitung der Virtuellen Maschinen.

KAPITEL 4

Weitere Hilfe

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 6.2 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

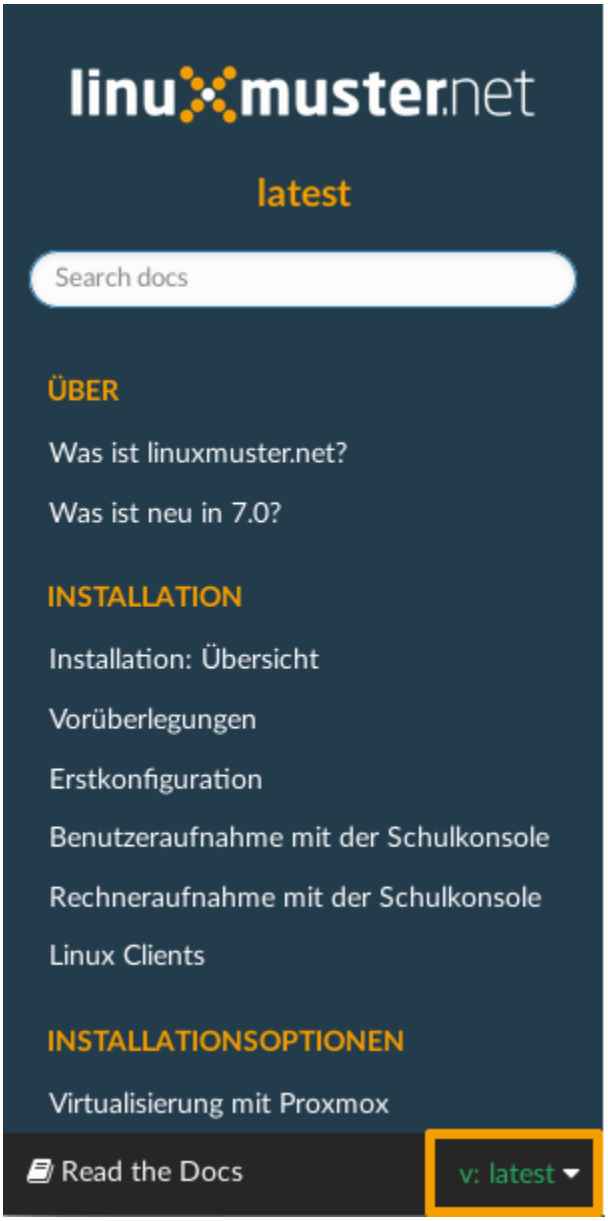
4.1.1 Anforderungen

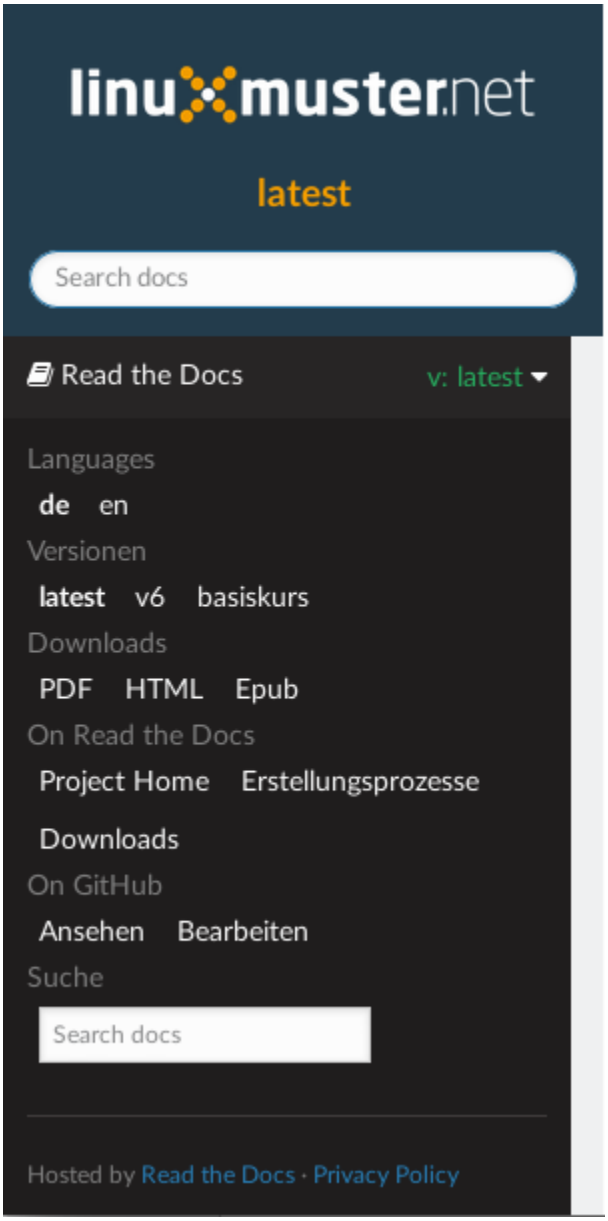
Schulnetzwerk vs. „normales“ Netzwerk

Warum unterscheiden wir eigentlich zwischen einer IT in einer Firma und einer Schule?

Im Prinzip gibt es vier große Merkmale, die auffallen:

1. Das Verhältnis der Anzahl von Usern zu den Arbeitsmitteln


linuxmusternet
latest
Search docs
ÜBER
Was ist linuxmuster.net?
Was ist neu in 7.0?
INSTALLATION
Installation: Übersicht
Vorüberlegungen
Erstkonfiguration
Benutzeraufnahme mit der Schulkonsole
Rechneraufnahme mit der Schulkonsole
Linux Clients
INSTALLATIONSOPTIONEN
Virtualisierung mit Proxmox
Read the Docs
v: latest


linuxmusternet
latest
Search docs
Read the Docs
v: latest
Languages
de en
Versionen
latest v6 basiskurs
Downloads
PDF HTML Epub
On Read the Docs
Project Home Erstellungsprozesse
Downloads
On GitHub
Ansehen Bearbeiten
Suche
Search docs
Hosted by Read the Docs · Privacy Policy

Schule	Firma		
User PC	PC		User
50	50		500
50			

2. Die Zusammensetzung von Usern in Abteilungen

Schule	Firma		
User Gruppe	Abteilung		User
A	1		A
Klasse			
Kurs 1			
Kurs 2			
AG 1			
B	1		B
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 unablässig, 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

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 Porfolio 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 7.1?

Autor des Abschnitts: Das Dokuteam

Linuxmuster.net 7.1 ist das Release-Update der linuxmuster.net v7.0. Es erfolgt auf Basis der bislang eingesetzten Ubuntu LTS Version ein Update der Kernpakete der linuxmuster.net Lösung, die neue Features bereitstellt.

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 Steuerung

- Webbasierte Steuerung der pädagogischen Funktionen mit einem sog. responsive design
- Aktuelle Betriebssysteme der Server und der vorkonfigurierten, kostenlos bereitgestellten Linux-Arbeitsplätze
- Mit LINBO 4: Neues User-Interface für die Steuerung an den Clients
- WebUI mit vielen administrativen Möglichkeiten, die zuvor nur an der Server-Konsole zu erreichen waren.

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 oder kann direkt auf zwei Hardware-Maschinen installiert werden.

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
- Zusätzlich Session-basierte Berechtigungen für die Unterrichtsteuerung
  - Gruppen können freiwählbar zusammengestellt werden
  - Benutzerbezogene statt rechnerbezogene Verwaltung

Netzwerkverwaltung

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

Selbstheilende Arbeitsstationen

- LINBO ist weiterhin das zentrale Softwareverteilungssystem.
- Es erfolgt ein Major Release Update auf LINBO 4.
  - Umstellung der Images-Abbilder auf das qcow2 Format
  - Neues User-Interface für die Steuerung an den Clients

4.2.3 Hinweise

Hinweis:

- Release-Informationen werden im Forum im Thread Neue Pakete für lmn7.1 veröffentlicht.

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

4. Vorbereitung der benötigten Server

* Bei der aktuellen linuxmuster.net Version dient die LTS Version 18.04 (Bionic Beaver) als Basis.

5. Installation from Scratch in die vorbereiteten VMs - oder alternativ direkt auf zwei Hardware-Maschinen

* Die Bezeichnung des Scriptes enthält immer einen Verweis auf die Version.

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`

4.4 Vorüberlegungen

Autor des Abschnitts: @cweikl, @Tobias

Linuxmuster.net wird als Zwei-Server-Lösung (Firewall und linuxmuster.net-Server) 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). linuxmuster.net kann virtualisiert oder ohne Virtualisierung betrieben werden.

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	• 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 sollte. 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® das Betriebssystem FreeBSD. Hinweise zu den Anforderungen von FreeBSD bzw. zur Kompatibilität mit eingesetzten Hardware-Komponenten finden sich unter der HCL - Hardware Compatibility List

Server linuxmuster v7.1

Für linuxmuster.net v7.1 wird als Basis ein Ubuntu Server 18.04 LTS eingesetzt. Es wird empfohlen folgende Hardware-Mindestanforderungen zu erfüllen:

Prozessor	>= 2 GHz Multi-Core CPU (64 Bit)
RAM	>= 4 GByte
Festplatte System + Daten	• 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.

		Festplatten		RAM	
Schule	Features	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 weiterhin mit Farben gekennzeichnet, um diese deutlich voneinander abzuheben:

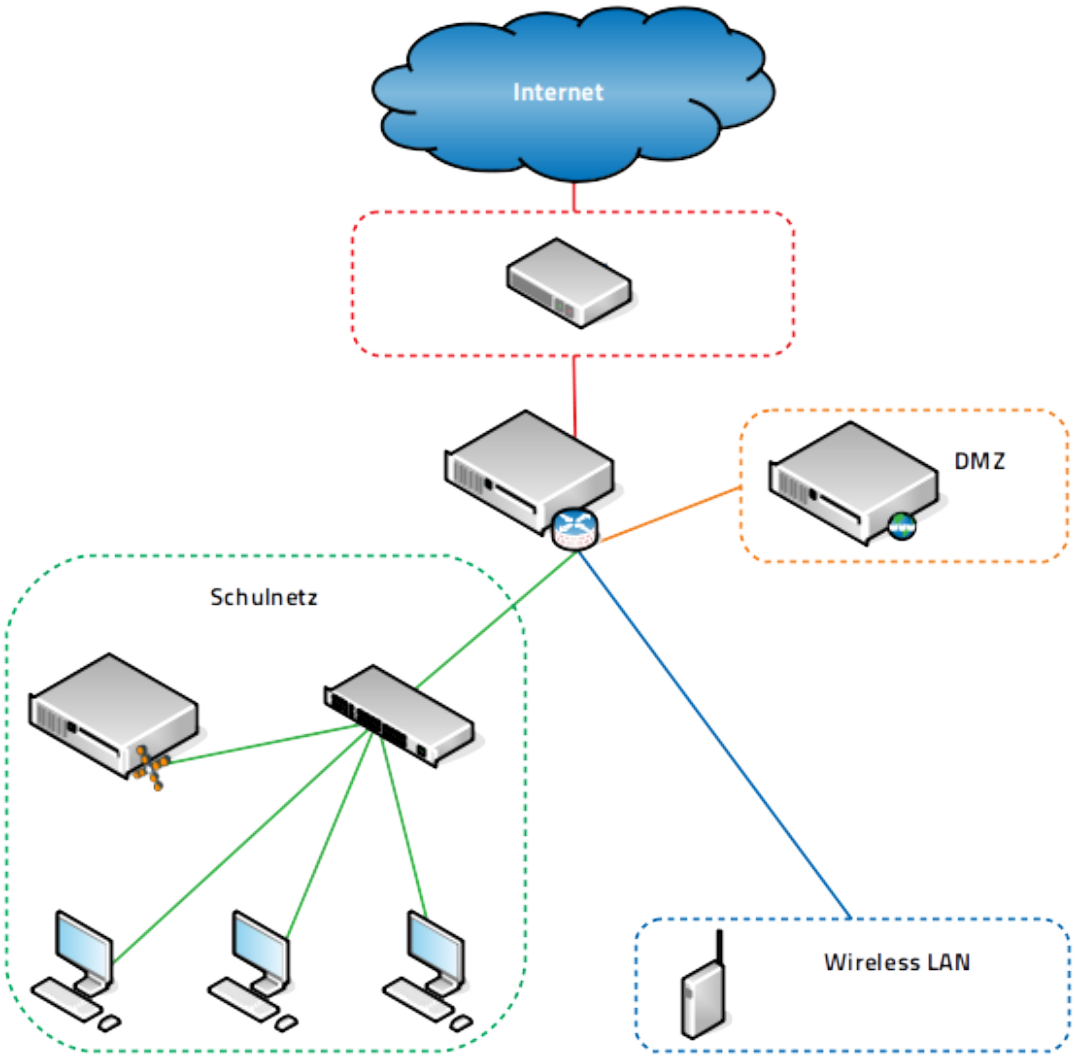


Abb. 1: Schematischer Aufbau eines Computernetzes mit linuxmuster.net.

- 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 auszulegen.

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 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 Switche („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 etwaige 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.

Alternativ installierst Du von Grund auf die Serverbetriebssysteme *Ubuntu Server* und *OPNsense®* direkt auf der Hardware oder innerhalb deiner Virtualisierungslösung. Hinweise auf andere Virtualisierungslösungen finden sich im Anwenderwiki von linuxmuster.net:

1. XCP-ng: https://wiki.linuxmuster.net/community/anwenderwiki:virtualisierung:xcpng:xcpng4lmn71
2. KVM: https://wiki.linuxmuster.net/community/anwenderwiki:virtualisierung:kvm:kvm4lmn71

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 die zentrale Managementkonsole.

Das web-basierte Verwaltungs-Interface 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 v7.1 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 7.1?*)
- *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 ermittel Du den korrekten Buchstaben für den USB-Stick unter Linux. X ist durch den korrekten Buchstaben zu ersetzen und dann ist nachstehender Befehl als Benutzer *root* oder mit einem *sudo* vorangestellt einzugeben:

```
dd if=proxmox-ve_7.2-1.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.

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

Um zu Beginn den Proxmox-Host zu administrieren, ist ein Laptop mit dem Switch zu verbinden, der an den lokalen (DSL-)Router angeschlossen ist. Der Laptop 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.

4.5.3 Installieren von Proxmox

Basis-Installation

Vom USB-Stick booten, danach erscheint folgender Bildschirm:

Wähle `Install Proxmox VE` und starte die Installation mit `ENTER`.

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

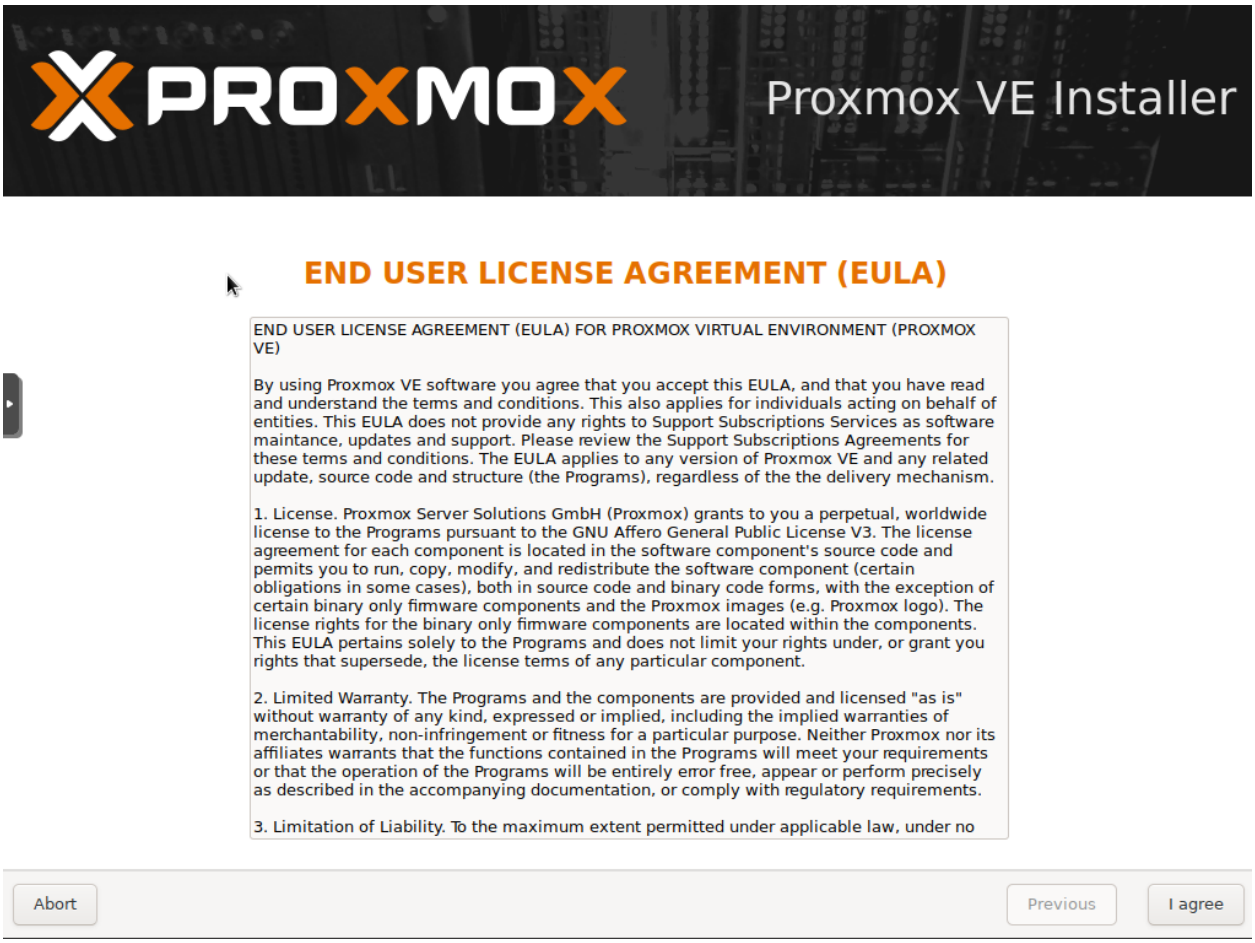
Wähle die gewünschte Festplatte auf dem Server zur Installation aus. Hast Du mehrere einzelne Festplatten im Server verbaut und kein RAID-Verbund definiert, so kannst Du hier mit der Schaltfläche *Optionen* weitere Einstellungen aufrufen. Hier kannst Du z. B. mehrere Festplatten angeben, die in einem 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)

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

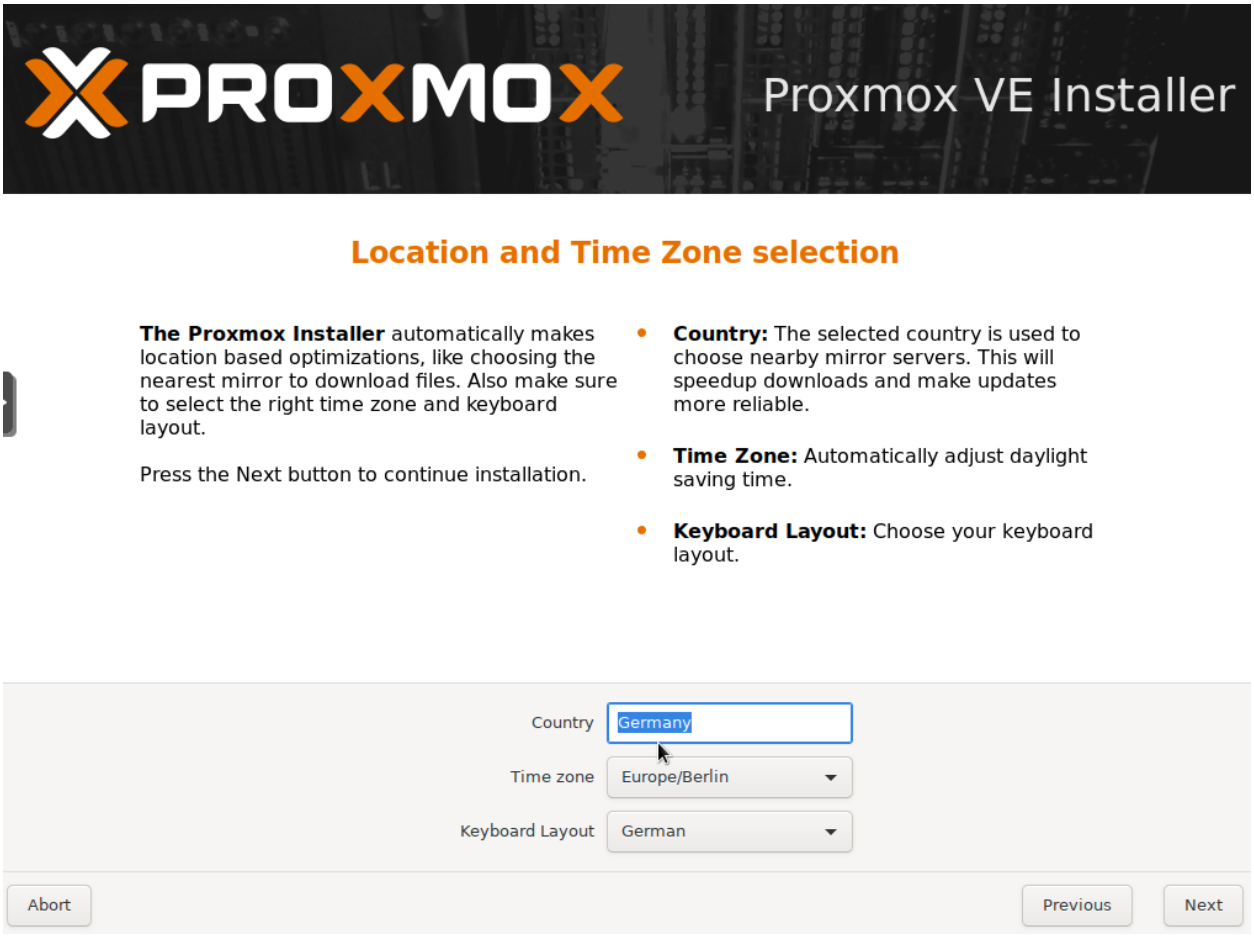
Lege ein Kennwort für den Administrator des Proxmox-Host fest und gib eine E-Mail-Adresse an. Klicke auf `Weiter`.

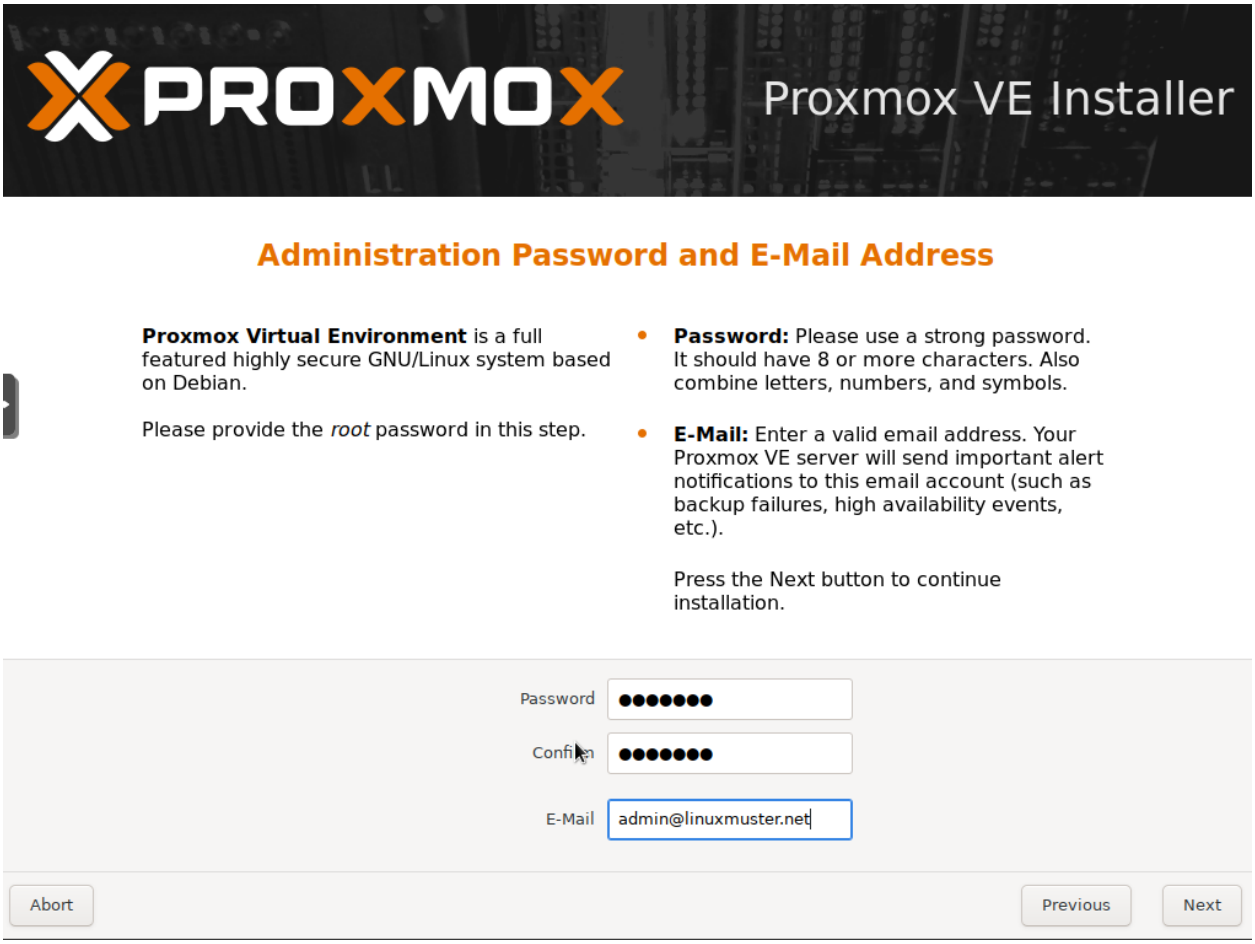
Lege die IP-Adresse des Proxmox-Host im internen Netz fest. Solltest Du intern z. B. auf dem (DSL-)Router einen DHCP-Server laufen haben, dann erhältst Du hier bereits eine vorausgefüllte Konfigurationsseite. Passe diese Werte nun den gewünschten Werten an. Der Hostname des Proxmox-Host ist hier in gewünschter Form – hier *hv01.linuxmuster.lan* – anzugeben.


Proxmox VE 7.2 (iso release 1) - https://www.proxmox.com/
PROXMOX
Welcome to Proxmox Virtual Environment
Install Proxmox VE
Advanced Options


PROXMOX
Proxmox VE Installer
END USER LICENSE AGREEMENT (EULA)
END USER LICENSE AGREEMENT (EULA) FOR PROXMOX VIRTUAL ENVIRONMENT (PROXMOX VE)
By using Proxmox VE software you agree that you accept this EULA, and that you have read and understand the terms and conditions. This also applies for individuals acting on behalf of entities. This EULA does not provide any rights to Support Subscriptions Services as software maintance, updates and support. Please review the Support Subscriptions Agreements for these terms and conditions. The EULA applies to any version of Proxmox VE and any related update, source code and structure (the Programs), regardless of the the delivery mechanism.
1. License. Proxmox Server Solutions GmbH (Proxmox) grants to you a perpetual, worldwide license to the Programs pursuant to the GNU Affero General Public License V3. The license agreement for each component is located in the software component's source code and permits you to run, copy, modify, and redistribute the software component (certain obligations in some cases), both in source code and binary code forms, with the exception of certain binary only fimware components and the Proxmox images (e.g. Proxmox logo). The license rights for the binary only fimware components are located within the components. This EULA pertains solely to the Programs and does not limit your rights under, or grant you rights that supersede, the license terms of any particular component.
2. Limited Warranty. The Programs and the components are provided and licensed "as is" without warranty of any kind, expressed or implied, including the implied warranties of merchantability, non-infringement or fitness for a particular purpose. Neither Proxmox nor its affiliates warrants that the functions contained in the Programs will meet your requirements or that the operation of the Programs will be entirely error free, appear or perform precisely as described in the accompanying documentation, or comply with regulatory requirements.
3. Limitation of Liability. To the maximum extent permitted under applicable law, under no
Abort
Previous
I agree

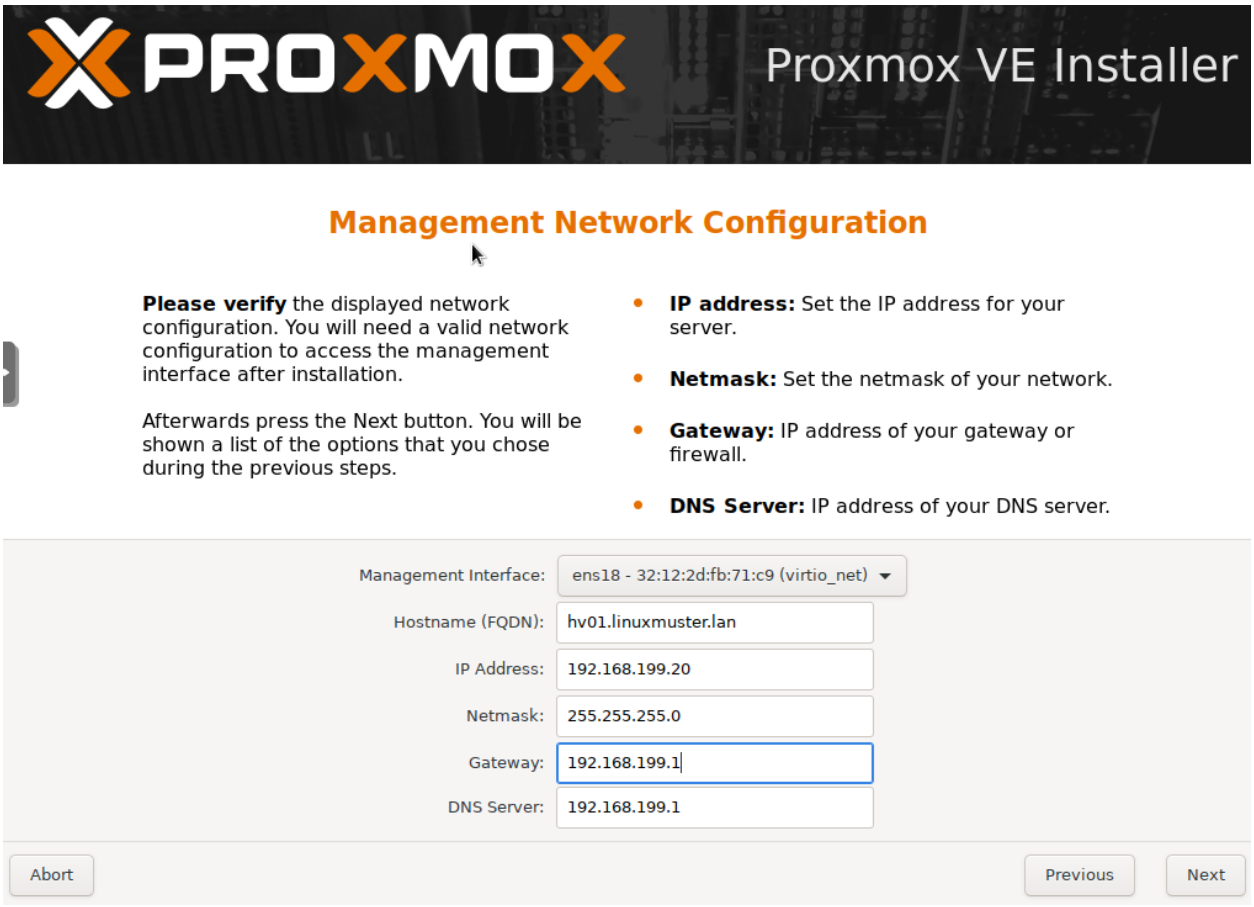

PROXMOX
Proxmox VE Installer
Proxmox Virtualization Environment (PVE)
The Proxmox Installer automatically partitions your hard disk. It installs all required packages and finally makes the system bootable from hard disk. All existing partitions and data will be lost.
Press the Next button to continue installation.
Please verify the installation target
The displayed hard disk is used for installation.
Warning: All existing partitions and data will be lost.
Automatic hardware detection
The installer automatically configures your hardware.
Graphical user interface
Final configuration will be done on the graphical user interface via a web browser.
Target Harddisk:
/dev/sda (120GB, QEMU HARDDISK)
/dev/sdb (1000GB, QEMU HARDDISK)
Options
Abort
Previous
Next


PROXMOX
Proxmox VE Installer
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.
Country
Germany
Time zone
Europe/Berlin
Keyboard Layout
German
Abort
Previous
Next


PROXMOX
Proxmox VE Installer
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.
Password
Confirm
E-Mail
admin@linuxmuster.net
Abort
Previous
Next

Hinweis: Diese muss zu diesem Zeitpunkt der Installation diejenige Adresse sein, die ebenfalls Zugriff auf das Internet hat. In einem lokalen Netz mit DSL-Router wäre dies eine IP-Adresse 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.

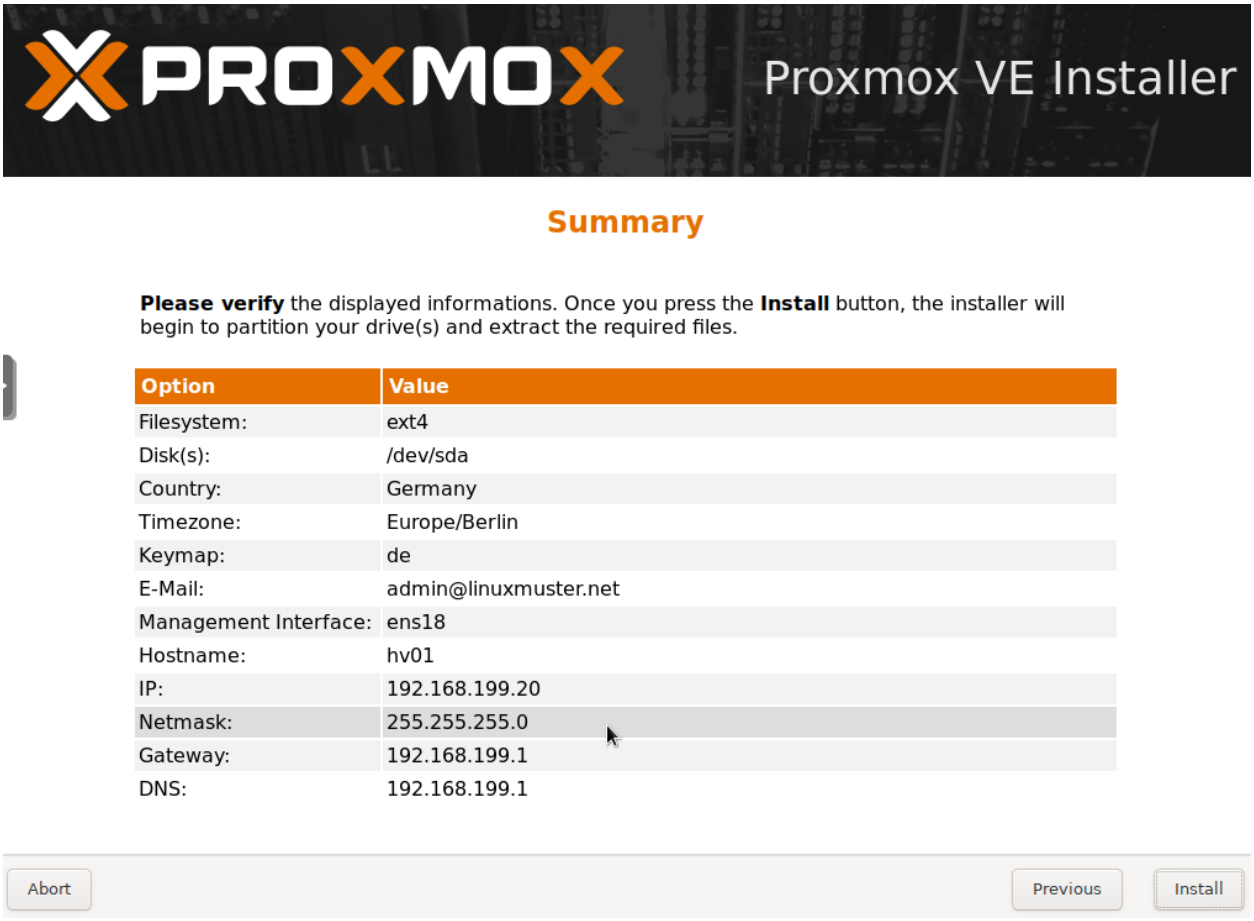
Nach erfolgreicher Installation lasse Proxmox über *Reboot* neu starten.

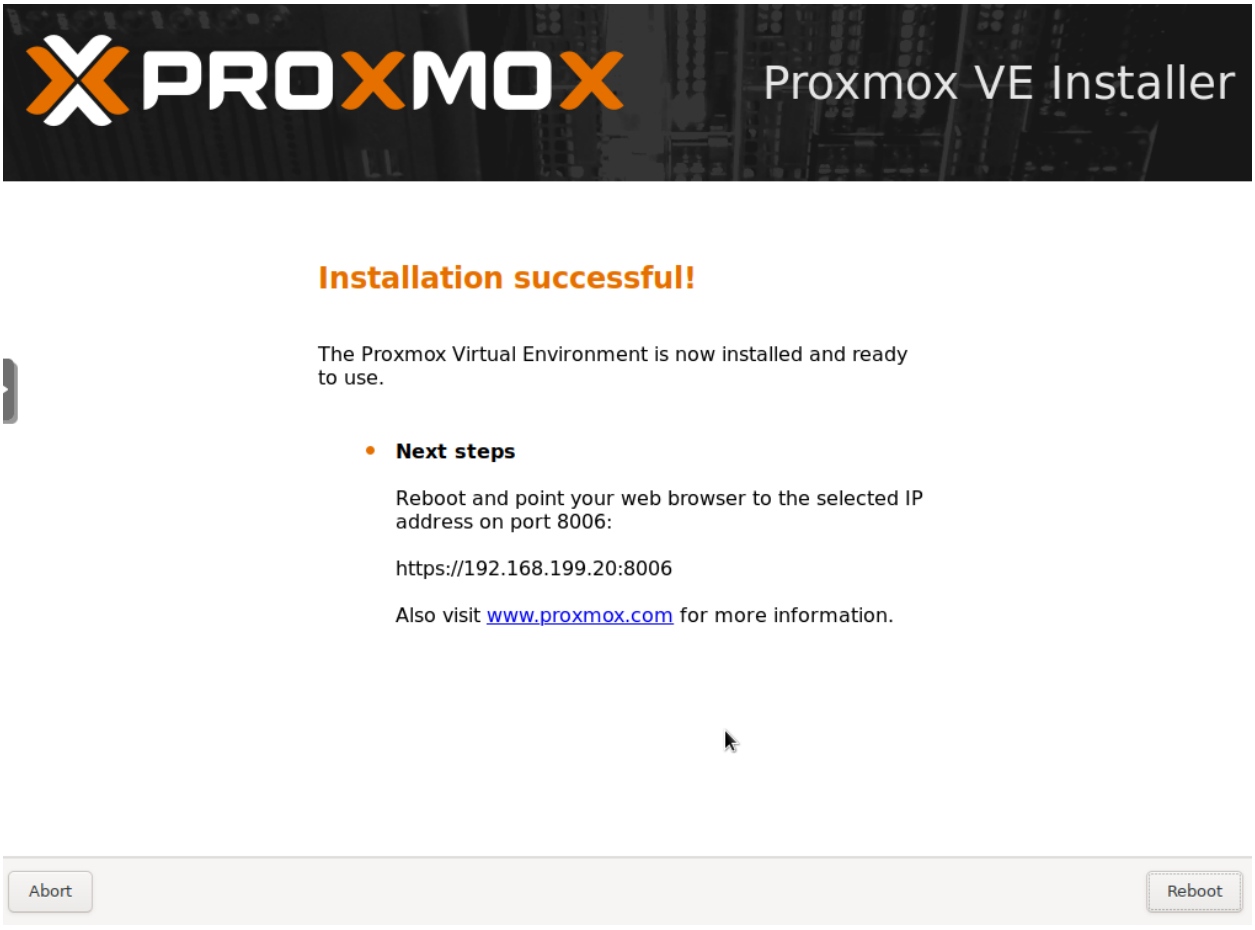
Proxmox Einrichtung

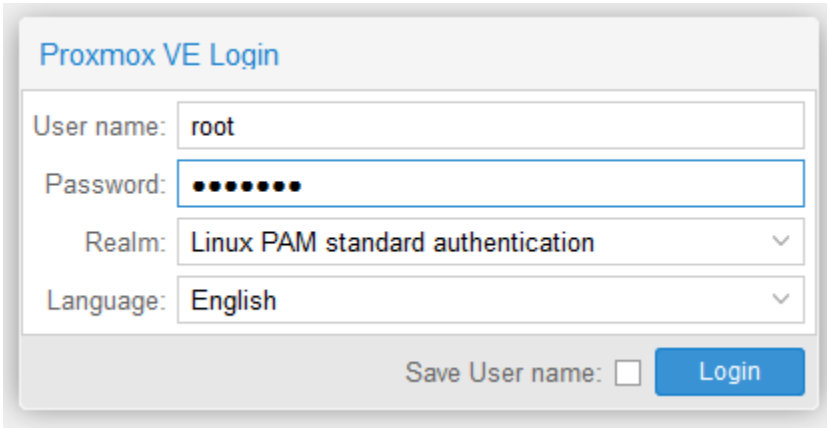
Nach dem Neustart von Proxmox kannst Du Dich über einen PC, der sich im selben Netz befindet, via Browser auf das grafische Webinterface zur Verwaltung des Proxmox-Hosts aufschalten. Hierzu gibst Du die URL https://192.168.199.20:8006 ein. Du erhältst ein „Warning“, da ein mögliches Sicherheitsrisiko 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.

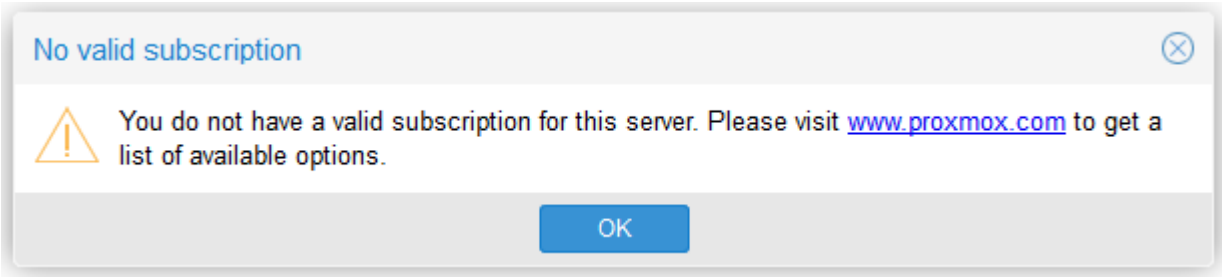
Es erscheint die Anmeldemaske des Proxmox-Webinterface. Melde Dich als User `root` und dem vorher gesetzten Passwort an:


PROXMOX
Proxmox VE Installer
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
Abort
Previous
Install


PROXMOX
Proxmox VE Installer
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.
Abort
Reboot

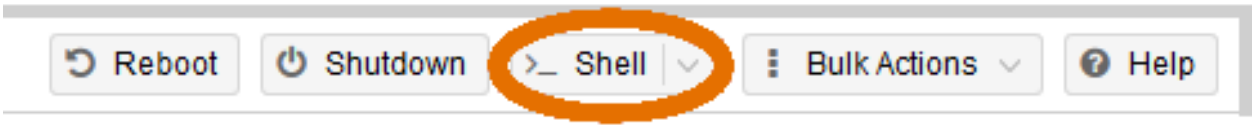

Proxmox VE Login
User name: root
Password: ●●●●●●●
Realm: Linux PAM standard authentication
Language: English
Save User name:
Login

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



Updates ermöglichen

Um Proxmox Updates installieren zu können, müssen in der Shell des Nodes hv01 folgende Änderungen an den Repositorien vorgenommen werden. Dafür den Node im Datacenter auswählen und eine Shell öffnen.



Folgende vier Befehle müssen der Reihe nach ausgeführt werden:

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

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

```
apt update
```

```
apt upgrade -y
```

Netzwerkbrücken einrichten

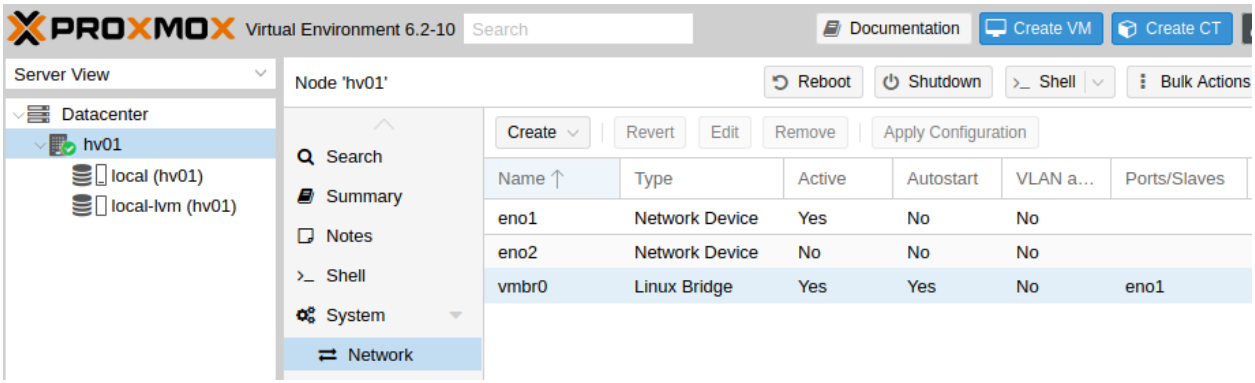
Für eine funktionierende Umgebung müssen `zwei Netzwerkbrücken/Bridge (vSwitch)` auf dem Hypervisor eingerichtet werden.

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 sogenannte Bridge (vmbr0) eingerichtet. Diese ist mit der ersten Netzwerkschnittstelle (NIC) des Proxmox-Hosts verbunden. Das Ethernet-Kabel der 1. NIC ist mit dem (DSL)-Router verbunden. Verlief 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: `Host hv01 –> Network`



Die bisherige Netzwerkkonfiguration stellt sich wie folgt dar:

Für die folgende Überprüfung öffnest Du nochmals die Konsole auf dem Hypervisor hv01, falls sie nicht geöffnet sein sollte, wie oben 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

iface eno1 inet manual

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

iface eno2 inet manual
```

Hinweis: Die Bezeichnungen für die Netzwerkkarten eno1, eno2 können je nach eingesetztem System von der dargestellten Bezeichnung abweichen.

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

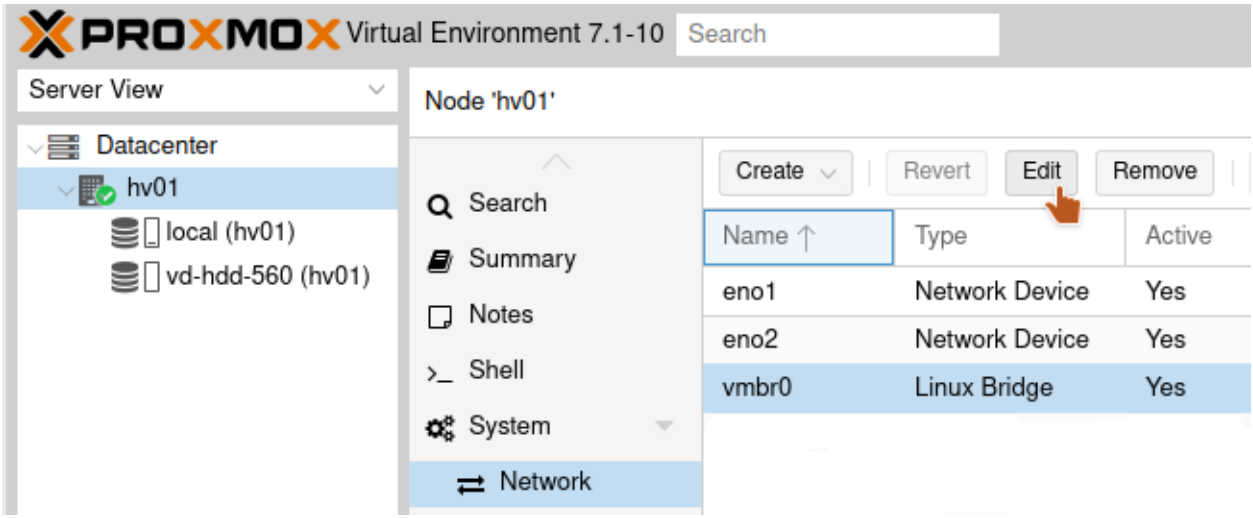
Markiere wie gezeigt `vmbr0` und betätige den `Edit`-Button, um das Konfigurationsfenster zu öffnen.

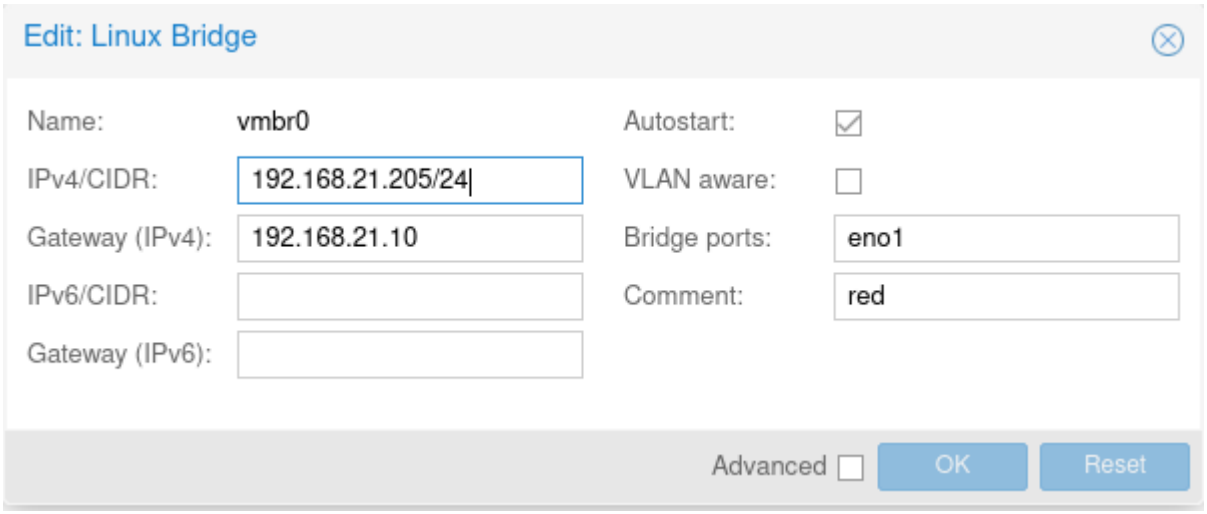
Trage unter `Comment` einen Kommentar ein, der veranschaulicht, dass diese Brücke die Verbindung zum Internet stellt. Zum Beispiel wie hier gezeigt `red`, den bei uns historisch gewachsenen Begriff für dieses Interface.

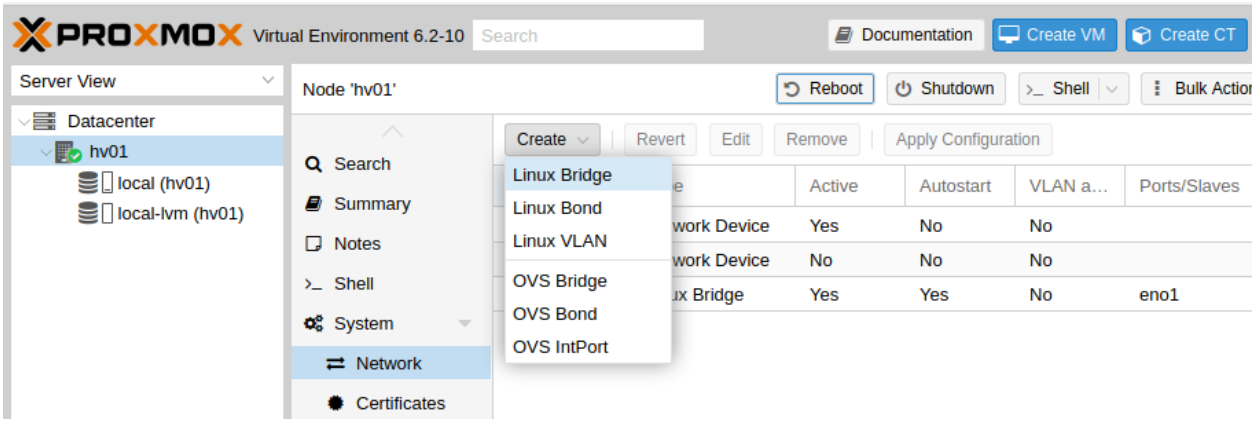
Mit *OK* wird der Kommentar übernommen.

Nun erstellst Du die zweite Bridge `vmbr1`:

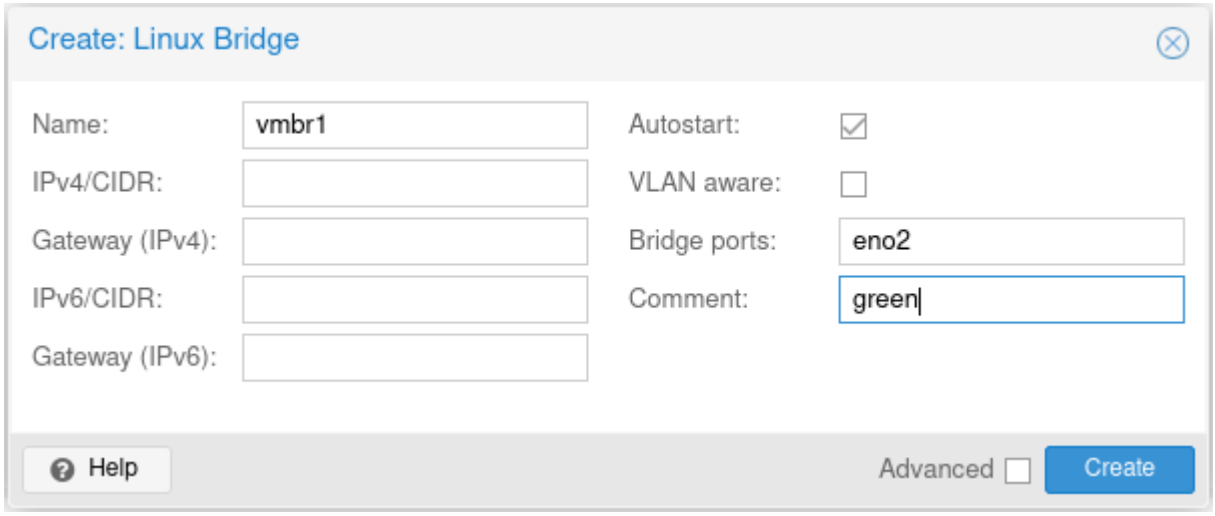
Dazu wähle das Menü `Datacenter` –> `hv01` –> `Network` –> `Create` –> `Linux Bridge`


PROXMOX Virtual Environment 7.1-10
Search
Server View
Node 'hv01'
Datacenter
hv01
local (hv01)
vd-hdd-560 (hv01)
Search
Summary
Notes
Shell
System
Network
Create
Revert
Edit
Remove
Name
Type
Active
eno1
Network Device
Yes
eno2
Network Device
Yes
vmbr0
Linux Bridge
Yes


Edit: Linux Bridge
Name:
vmbr0
IPv4/CIDR:
192.168.21.205/24
Gateway (IPv4):
192.168.21.10
IPv6/CIDR:
Gateway (IPv6):
Autostart:
VLAN aware:
Bridge ports:
eno1
Comment:
red
Advanced
OK
Reset

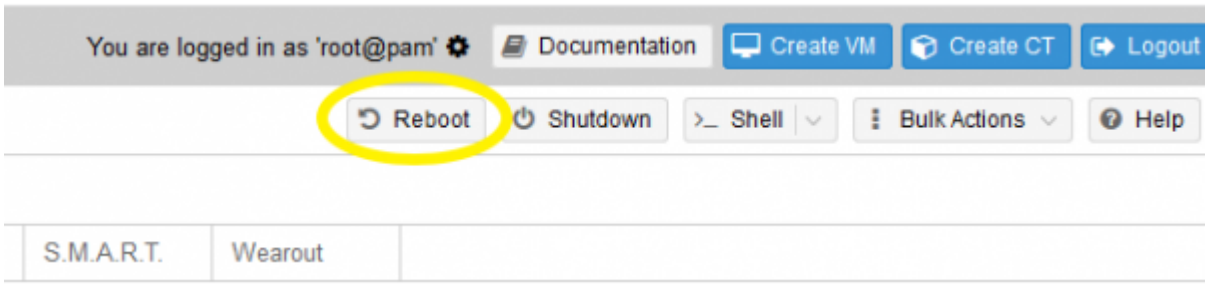

PROXMOX Virtual Environment 6.2-10
Search
Documentation
Create VM
Create CT
Server View
Node 'hv01'
Reboot
Shutdown
Shell
Datacenter
hv01
local (hv01)
local-lvm (hv01)
Search
Summary
Notes
Shell
System
Network
Certificates
Create
Revert
Edit
Remove
Apply Configuration
Linux Bridge
Linux Bond
Linux VLAN
OVS Bridge
OVS Bond
OVS IntPort
Active
Autostart
VLAN a...
Ports/Slaves
Yes
No
No
No
No
Yes
Yes
No
eno1

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



Mit *Create* wird die Brücke erstellen.

Anschließend Proxmox über den Button `Reboot` oben rechts neu starten, um die neue Netzwerkkonfiguration zu laden. Node hv01 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.

```
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
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
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.

(Optional) Festplatten anpassen

Zweiten Datenträger als Speicher einbinden

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

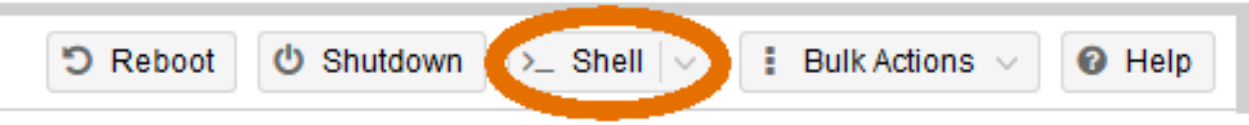
Bemerkung: Die folgenden Schritte bitte dann ausführen, wenn nicht auf einem einzigen Volume Proxmox eingerichtet werden soll! In diesem Fall geht es hier weiter: *Vorbereiten des ISO-Speichers*

---

local-lvm(hv01)-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 hv01 oben rechts Shell anklicken:



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

Es ist zu sehen, dass die Festplatten sda (931.5G) und sdb (111.8G) vorhanden sind. Die erste Festplatte sda ist eine HDD mit 1 TByte Kapazität und soll nun für die VMs genutzt werden. Die zweite Festplatte ist eine SSD, auf der Proxmox selbst installiert wurde. Von dieser zweiten Platte startet dieses System automatisch Proxmox. Zudem findet sich auf *sdb3* 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 *sdb* wird vollständig dem Proxmox-Host zugeordnet. Danach wird die Festplatte *sda* als LVM für die VM eingerichtet.

3. Vorhandene local-lvm entfernen:

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

Bestätige die Nachfrage mit `y`

4. Speicherbereich von local erweitern:

```
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                  8:0    0 931.5G  0 disk
sdb                  8:16   0 111.8G  0 disk
├─sdb1               8:17   0  1007K  0 part
├─sdb2               8:18   0   512M  0 part /boot/efi
└─sdb3               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
root@hv01:~#
```

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

```
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:~#
```

```
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:~#
```

5. Filesystem anpassen:

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

```
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:~#
```

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

```
root@hv01:~# lsblk
NAME         MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
sda            8:0    0 931.5G  0 disk
sdb            8:16   0 111.8G  0 disk
├─sdb1         8:17   0  1007K  0 part
├─sdb2         8:18   0   512M  0 part /boot/efi
└─sdb3         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  /
root@hv01:~#
```

Es ist zu erkennen, dass auf `/dev/sdb3` 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 (hv01)` mit dem `Remove`-Button grafisch zu entfernen:

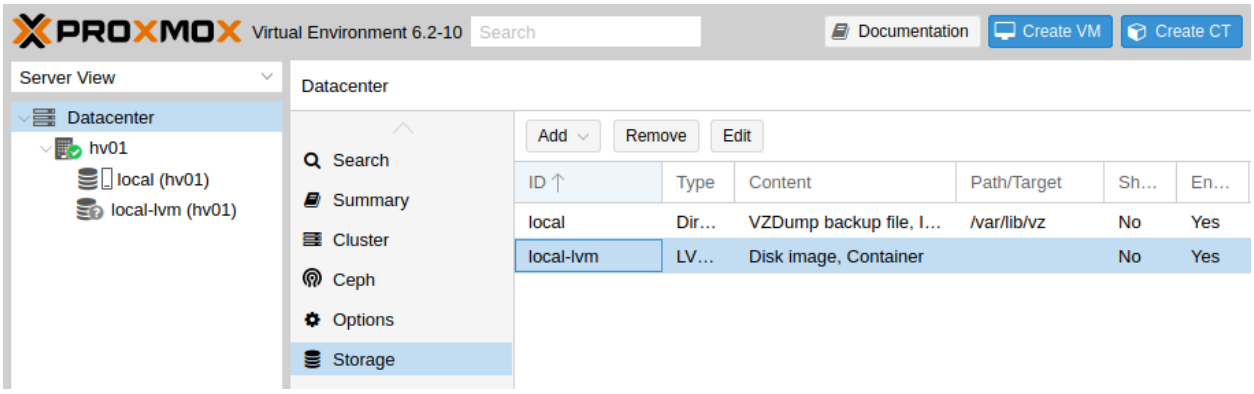
Danach findest Du noch folgenden Speicher:

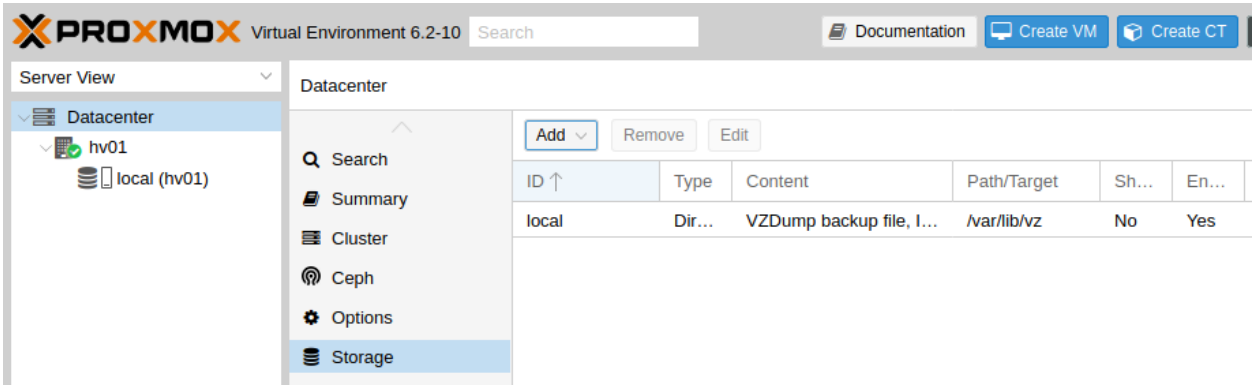
Die SSD `/dev/sdb` steht für den Proxmox-Host zur Verfügung.

Zweiten Datenträger vorbereiten

Die erste Festplatte heißt hier sda 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:

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 TByte Kapazität.





1. Datenträger vorher partitionieren, z. B. mit `fdisk /dev/sda` → `g` → `n` → `w` (über lsblk den richtigen Datenträgernamen herausfinden; in diesem Fall sda)
2. Jetzt eine neue Partition auf der Festplatte anlegen - `pvcreate /dev/sd<xy>1`

Beispiel:

```
pvcreate /dev/sda1
```

und anschließend mit `y` bestätigen:

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/sda1
```

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 TByte Speicher, weshalb die Namen im Befehl so angepasst werden:

Beispiel:

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

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

Beispiel:

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

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:~#
```

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

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

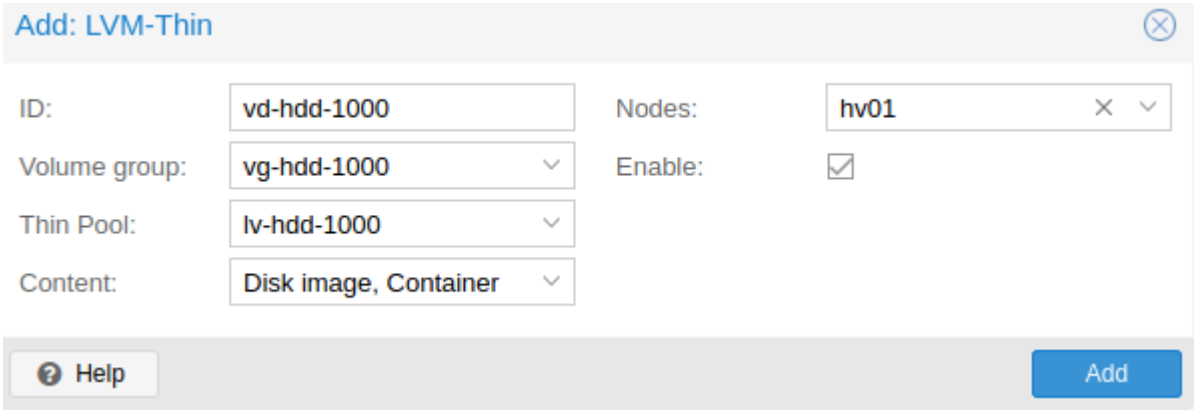
```
root@hv01:~# lvcreate -l 99%VG -n lv-hdd-1000 vg-hdd-1000
  Logical volume "lv-hdd-1000" created.
root@hv01:~#
```

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

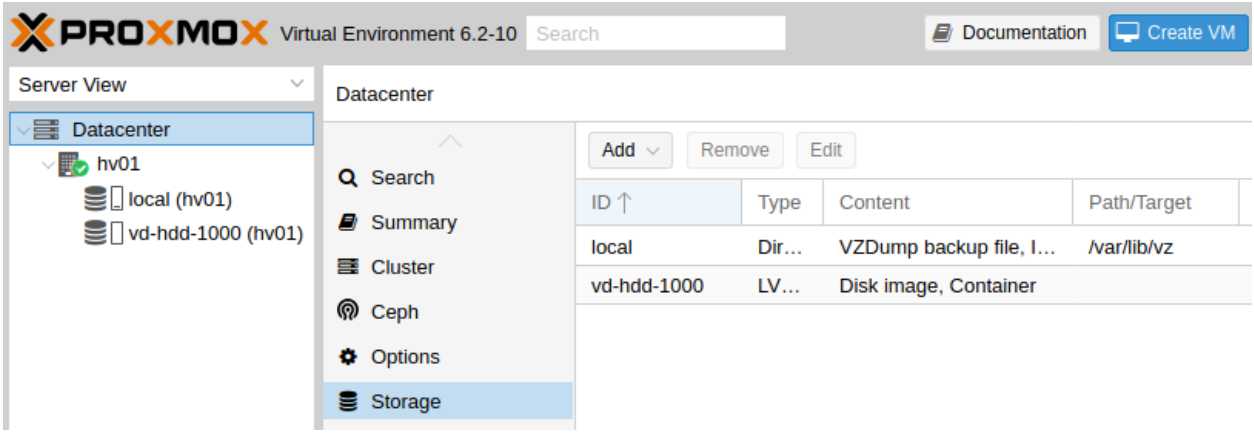
```
root@hv01:~# lvconvert --type thin-pool vg-hdd-1000/lv-hdd-1000
  Thin pool volume with chunk size 512.00 KiB can address at most 126.50 TiB of data.
  WARNING: Pool zeroing and 512.00 KiB large chunk size slows down thin provisioning.
  WARNING: Consider disabling zeroing (-Zn) or using smaller 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:~#
```

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 TByte Speicherkapazität, weshalb die Bezeichnung vd-hdd-1000 gewählt wird. Unter Volume Group die erstellte virtuelle Gruppe auswählen, welche hier vg-hdd-1000 ist:

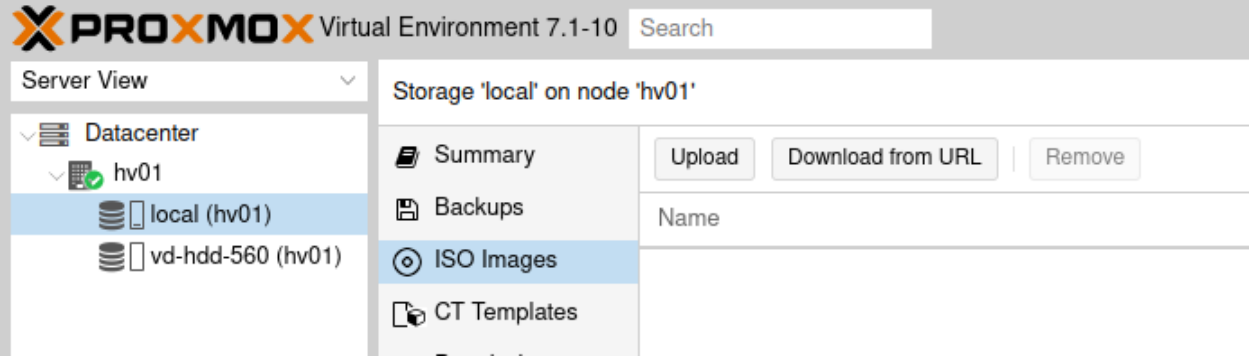


2. Nun sollte im linken Menü der zweite Storage zu sehen sein, auf welchem die Maschinen für Linuxmuster installiert werden können:



4.5.4 Vorbereiten des ISO-Speichers

Um die v7.1 zu installieren, müssen zwei virtuelle Maschinen angelegt werden. OPNsense und Ubuntu Server 18.04 LTS werden in die VMs installiert. Dazu ist es erforderlich, dass Du die ISO-Images für OPNsense und Ubuntu Server 18.04 LTS auf den Proxmox-Hypervisor in den Datenspeicher für ISO-Images lädst.



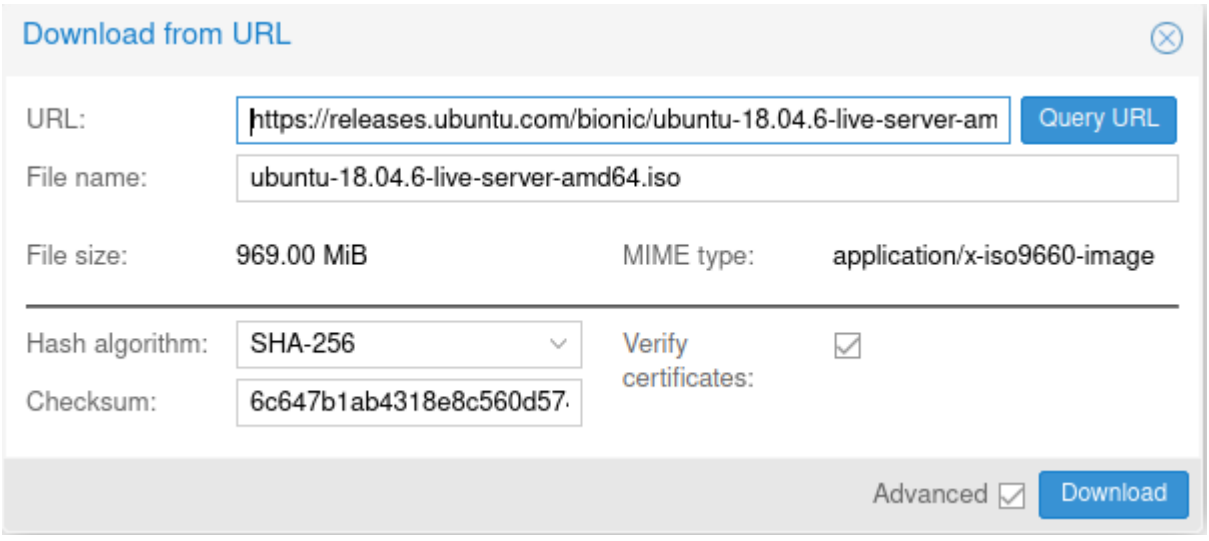
Gehe dazu auf `Datacenter –> <proxmox-host> –> Datenspeicher (auf local oder zfsfile) –> ISO Images –> Download from URL`

Ubuntu Server

In dem nun geöffneten Fenster trägst Du die URL

```
https://releases.ubuntu.com/bionic/ubuntu-18.04.6-live-server-amd64.iso
```

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



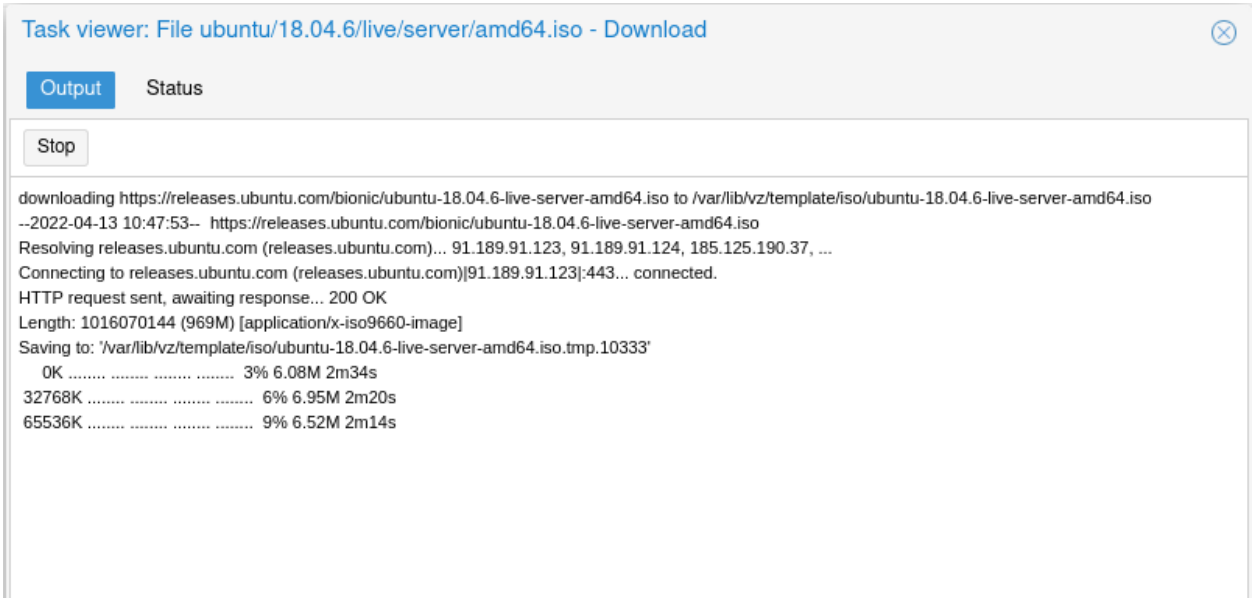
Wenn die Abfrage der URL positiv war, sollten sich die Felder ausgefüllt haben.

Zum Überprüfen der Datei-Integrität aktiviere `Verify certificates`, das sich unter den `Advanced` Optionen befindet.

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

```
6c647b1ab4318e8c560d5748f908e108be654bad1e165f7cf4f3c1fc43995934
```

Das Herunterladen des ISOs beginnt mit `Download`.



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 Importes mittels 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.

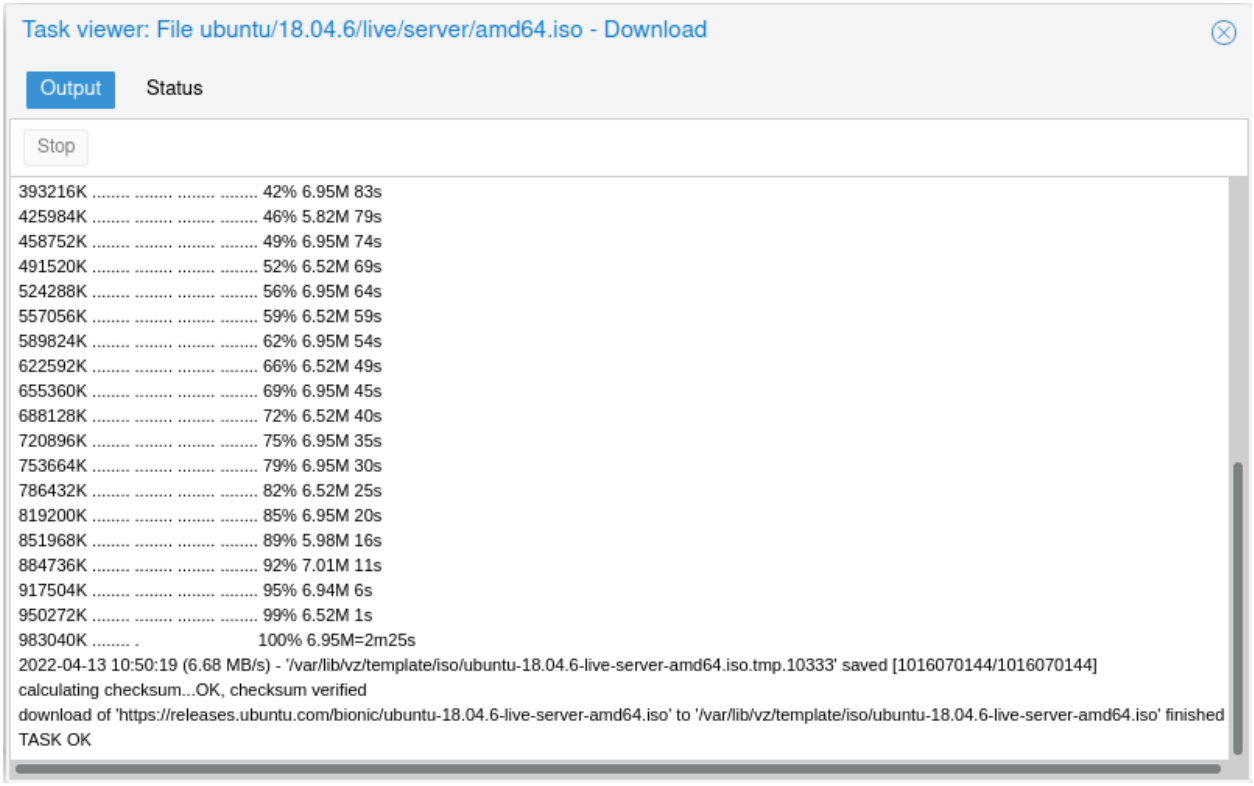
Als Nächstes musst Du in das Verzeichnis wechseln, wo Proxmox die ISO-Dateien sucht. Dazu kopierst Du diese Zeile in das gezeigte Fenster.

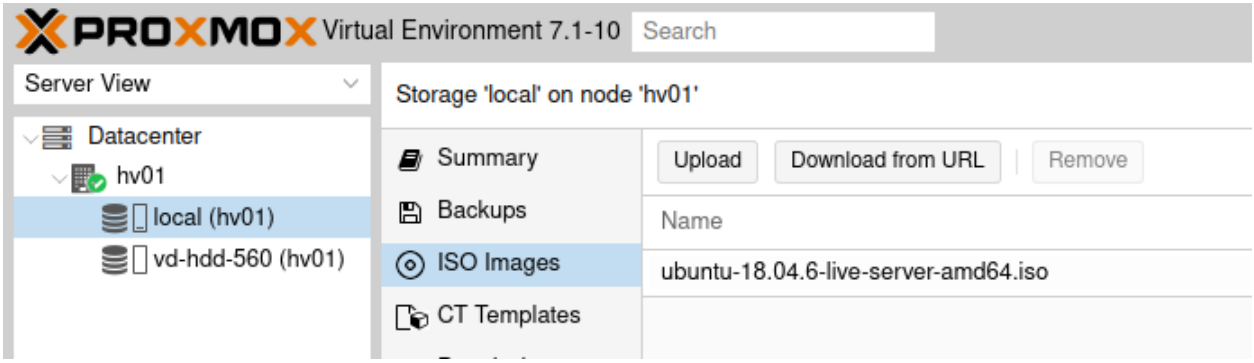
```
cd /var/lib/vz/template/iso
```

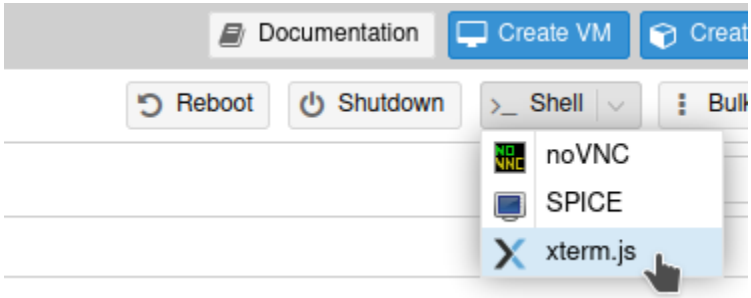
Mit `[Enter]` wechselt Du dann in das Verzeichnis.

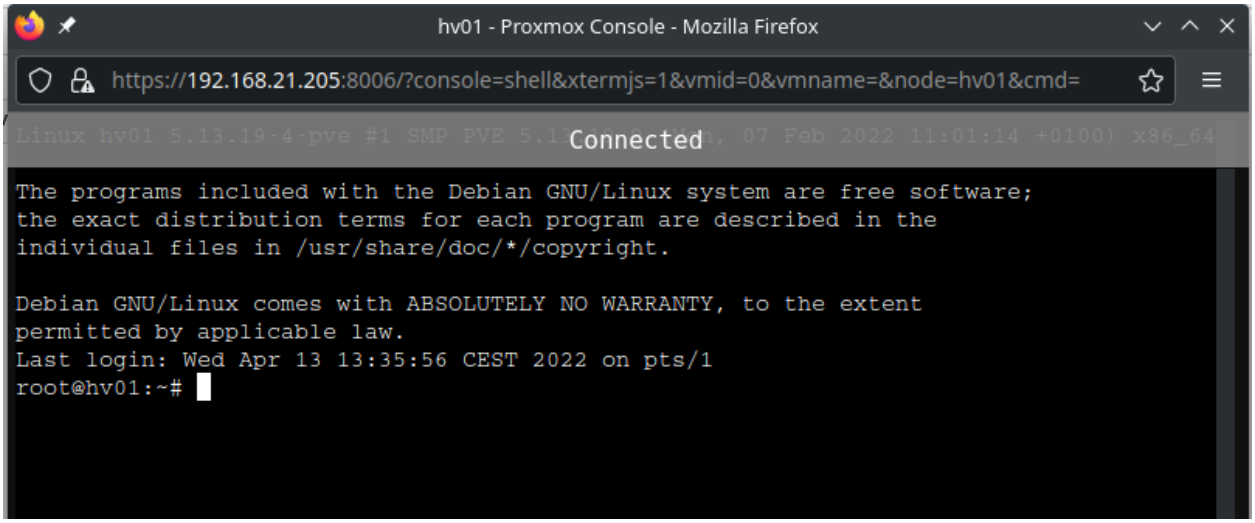
Dann musst Du die folgenden vier Dateien herunterladen:

Prüfsummendatei (<filename>.sha256)


Task viewer: File ubuntu/18.04.6/live/server/amd64.iso - Download
Output
Status
Stop
393216K 42% 6.95M 83s
425984K 46% 5.82M 79s
458752K 49% 6.95M 74s
491520K 52% 6.52M 69s
524288K 56% 6.95M 64s
557056K 59% 6.52M 59s
589824K 62% 6.95M 54s
622592K 66% 6.52M 49s
655360K 69% 6.95M 45s
688128K 72% 6.52M 40s
720896K 75% 6.95M 35s
753664K 79% 6.95M 30s
786432K 82% 6.52M 25s
819200K 85% 6.95M 20s
851968K 89% 5.98M 16s
884736K 92% 7.01M 11s
917504K 95% 6.94M 6s
950272K 99% 6.52M 1s
983040K ..... . 100% 6.95M=2m25s
2022-04-13 10:50:19 (6.68 MB/s) - '/var/lib/vz/template/iso/ubuntu-18.04.6-live-server-amd64.iso.tmp.10333' saved [1016070144/1016070144]
calculating checksum...OK, checksum verified
download of 'https://releases.ubuntu.com/bionic/ubuntu-18.04.6-live-server-amd64.iso' to '/var/lib/vz/template/iso/ubuntu-18.04.6-live-server-amd64.iso' finished
TASK OK


PROXMOX Virtual Environment 7.1-10
Search
Server View
Datacenter
hv01
local (hv01)
vd-hdd-560 (hv01)
Storage 'local' on node 'hv01'
Summary
Backups
ISO Images
CT Templates
Upload
Download from URL
Remove
Name
ubuntu-18.04.6-live-server-amd64.iso


Documentation
Create VM
Reboot
Shutdown
Shell
noVNC
SPICE
xterm.js




```
wget https://mirror.informatik.hs-fulda.de/opnsense/releases/22.7/OPNsense-22.7-OpenSSL-
↪checksums-amd64.sha256
```

Signatur Datei (<filename>.sig)

```
wget https://mirror.informatik.hs-fulda.de/opnsense/releases/22.7/OPNsense-22.7-OpenSSL-
↪dvd-amd64.iso.bz2.sig
```

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

```
wget https://mirror.informatik.hs-fulda.de/opnsense/releases/22.7/OPNsense-22.7.pub
```

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

```
wget https://mirror.informatik.hs-fulda.de/opnsense/releases/22.7/OPNsense-22.7-OpenSSL-
↪dvd-amd64.iso.bz2
```

Überprüfen der heruntergeladenen Dateien auf deren Integrität:

```
openssl base64 -d -in OPNsense-22.7-OpenSSL-dvd-amd64.iso.bz2.sig -out /tmp/image.sig
```

```
openssl dgst -sha256 -verify OPNsense-22.7.pub -signature /tmp/image.sig OPNsense-22.7-
↪OpenSSL-dvd-amd64.iso.bz2
```

Der letzte Befehl sollte Dir ein `Verified OK` liefern.

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

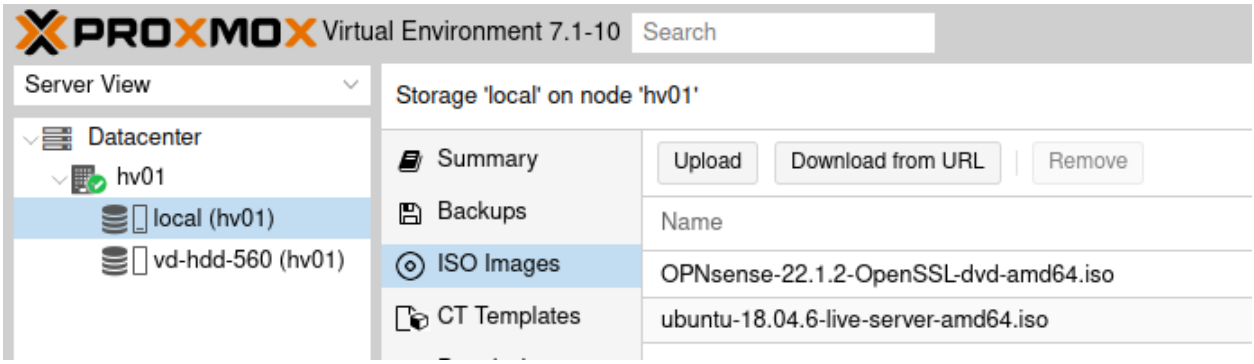
```
bunzip2 OPNsense-22.7-OpenSSL-dvd-amd64.iso.bz2
```

Das Entpacken kann einige Zeit in Anspruch nehmen. Anschließend sollte sich in dem Verzeichnis die OPNsense-ISO-Datei befinden. Die daneben befindlichen anderen OPNsense-Datei kannst Du nun wieder löschen.

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

Somit hast Du nun alle nötigen ISO-Dateien für die weitere Installation zusammen.

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

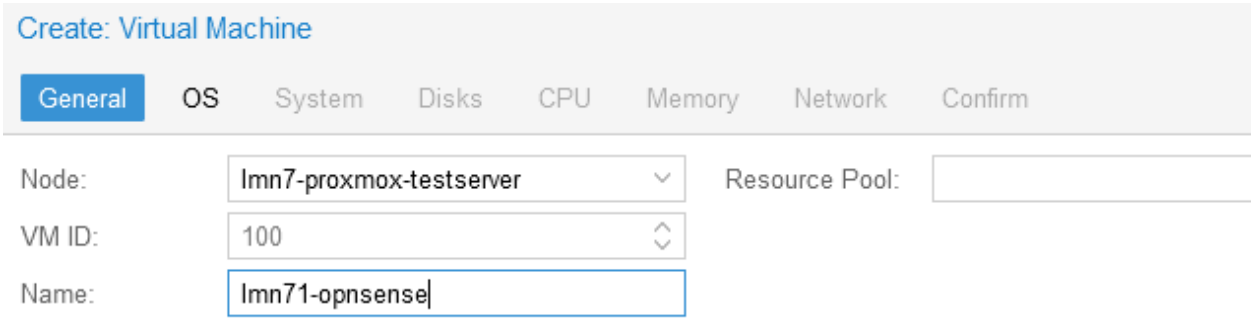


4.5.5 Vorbereiten der virtuellen Maschinen

Anlegen der VM für OPNsense

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

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.

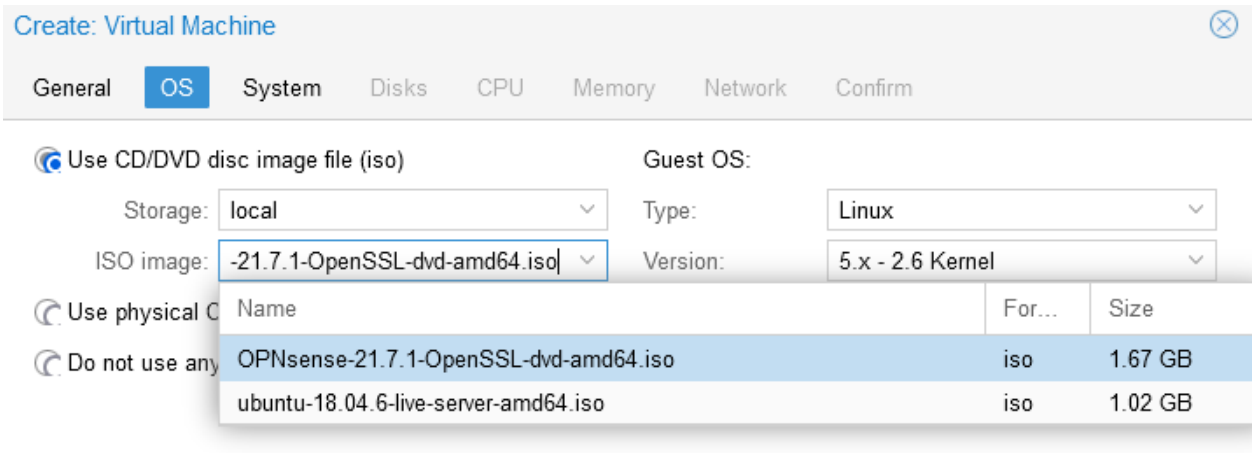
Klicke dann auf `Next`.

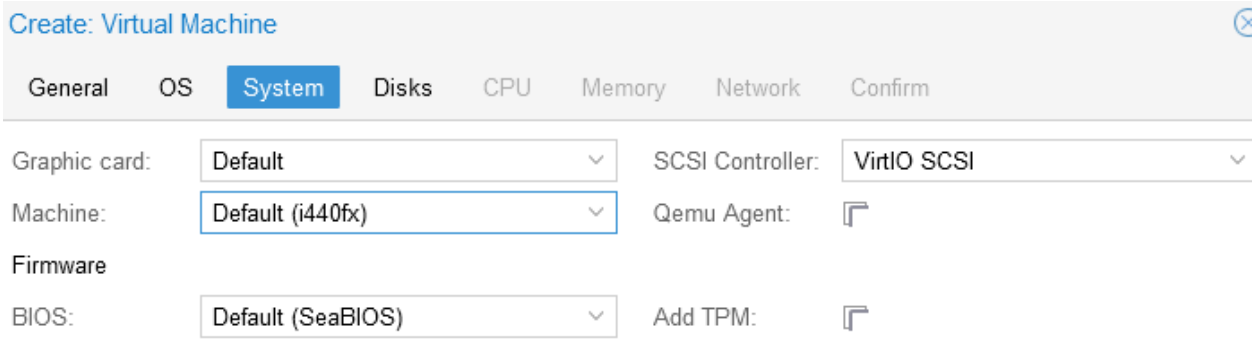
Belasse hier zunächst alle Voreinstellungen für Grafikkarte und Festplatten-Controller wie angezeigt.

Klicke dann auf `Next`.

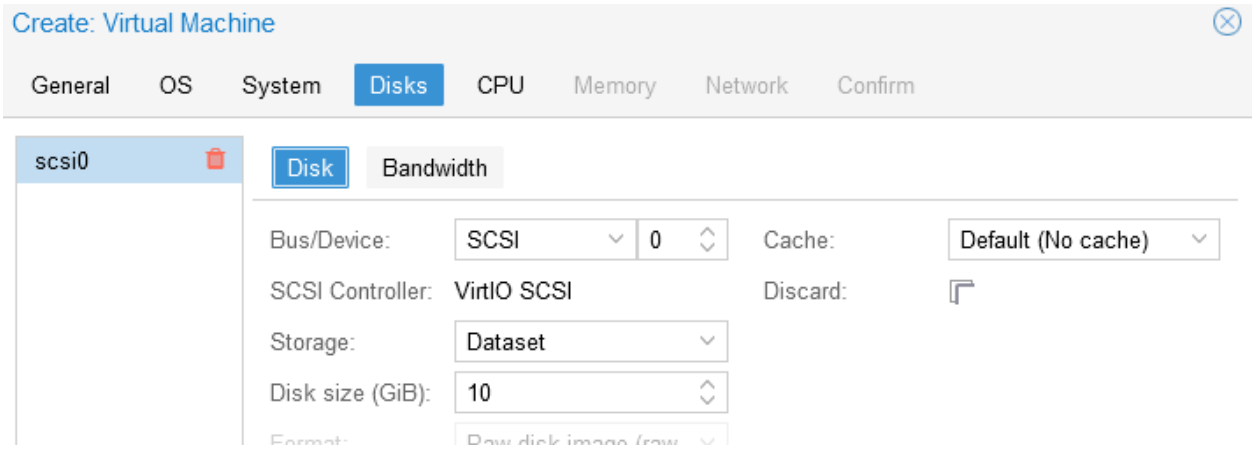
Wähle nun hier unter `Storage` den geeigneten Datenspeicher auf, um die Festplatte der VM dort abzulegen. In der Abb. wird der Datenspeicher `Dataset` verwendet. In dem Drop-down Menü siehst Du alle in Deinem System verfügbaren Datenspeicher.

Hinweis: Folgende Größenangaben beziehen sich, wie schon geschrieben, auf eine Testumgebung. Für andere Einsatzszenarien solltest Du Dich unbedingt mit den Hardware-Anforderungen gemäß der OPNsense® -Dokumentation


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:
-21.7.1-OpenSSL-dvd-amd64.iso
Version:
5.x - 2.6 Kernel
Use physical C
Do not use any
Name
For...
Size
OPNsense-21.7.1-OpenSSL-dvd-amd64.iso
iso
1.67 GB
ubuntu-18.04.6-live-server-amd64.iso
iso
1.02 GB

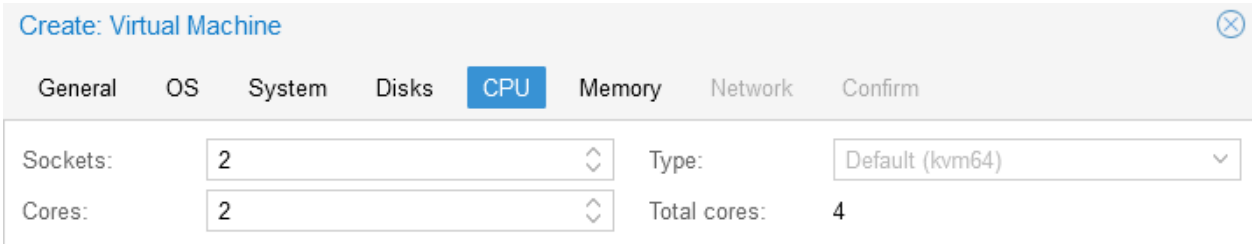

Create: Virtual Machine
General
OS
System
Disks
CPU
Memory
Network
Confirm
Graphic card:
Default
SCSI Controller:
VirtIO SCSI
Machine:
Default (i440fx)
Qemu Agent:
Firmware
BIOS:
Default (SeaBIOS)
Add TPM:

auseinandersetzen. Wie in der Dokumentation schon ausgeführt, solltest Du hier besser mindestens 8 GiB RAM und 50 GiB HDD wählen.



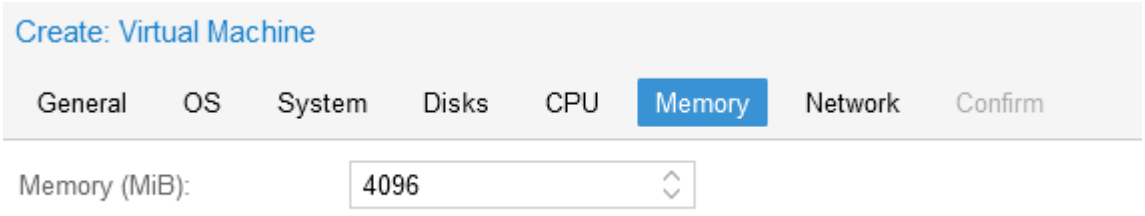
Klicke dann auf `Next`.

Gib nun für die CPU Sockel und Kerne an.



Klicke dann auf `Next`.

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



Klicke dann auf `Next`.

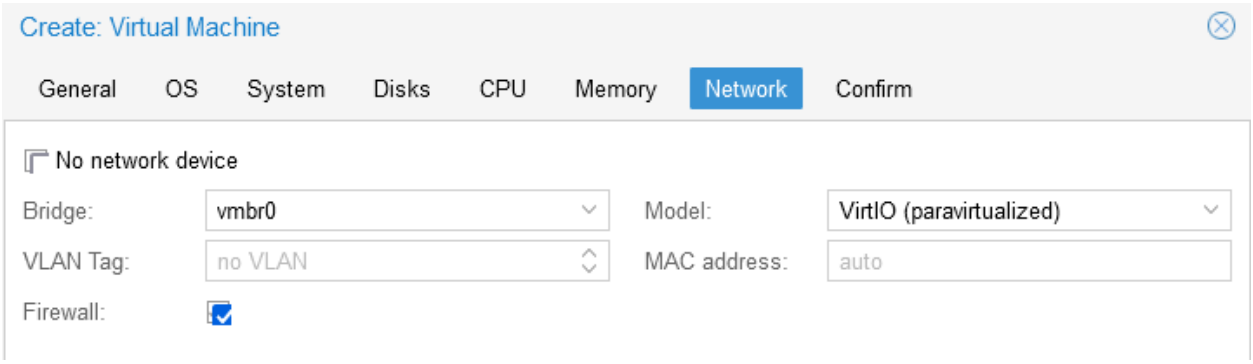
Gib danach die `Bridge vmbr0` für die einzurichtende Netzwerkkarte an. Die zweite Netzwerkkarte fügst Du nach Anlage der VM hinzu. Dies muss noch vor der eigentlichen Installation erfolgen.

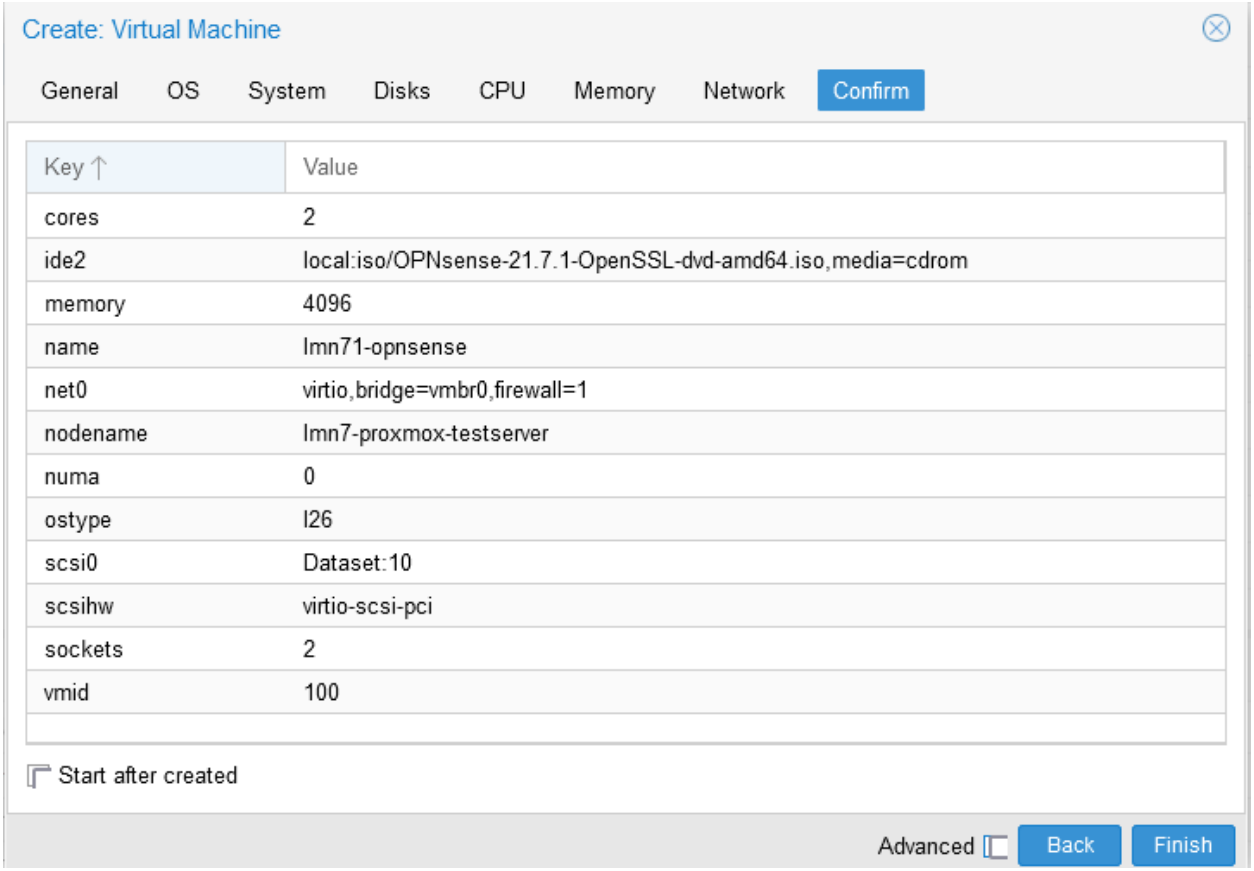
Klicke dann auf `Next`.

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.

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

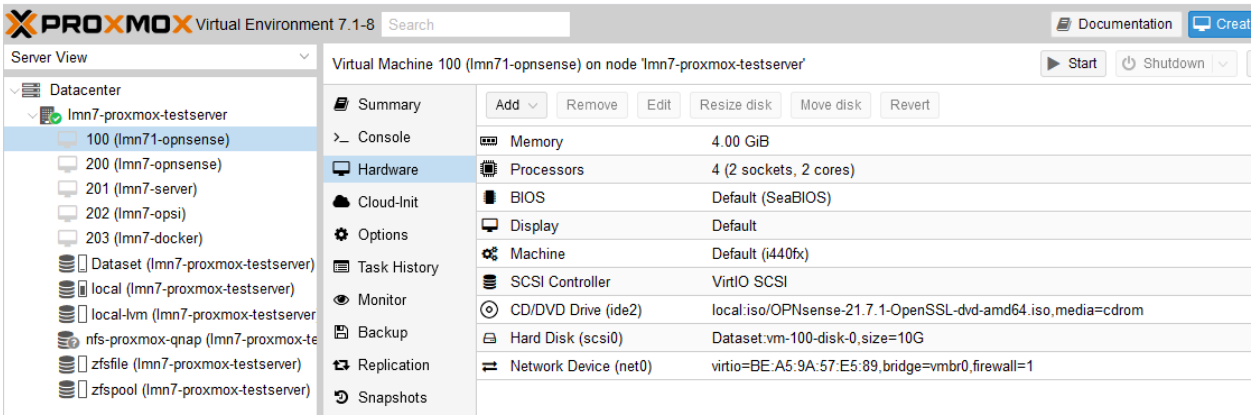
Klicke dann auf `Finish`.


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:

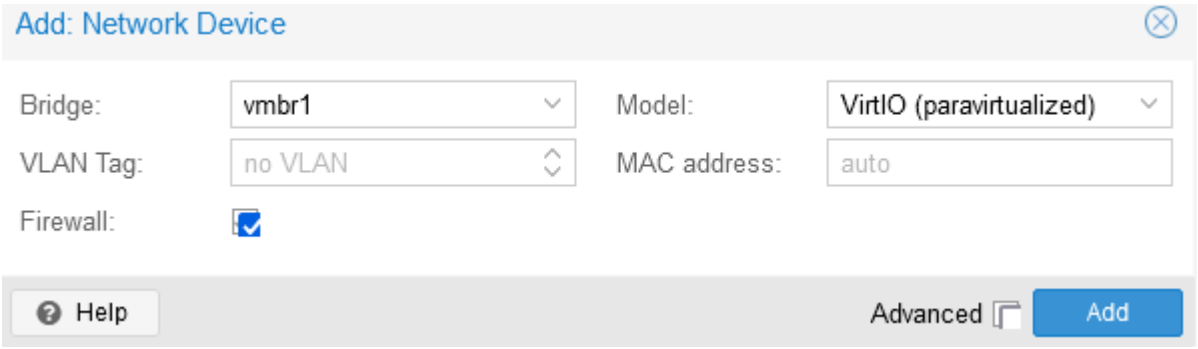

Create: Virtual Machine
General
OS
System
Disks
CPU
Memory
Network
Confirm
Key
Value
cores
2
ide2
local:iso/OPNsense-21.7.1-OpenSSL-dvd-amd64.iso,media=cdrom
memory
4096
name
lmn71-opnsense
net0
virtio,bridge=vmbr0,firewall=1
nodename
lmn7-proxmox-testserver
numa
0
ostype
l26
scsi0
Dataset:10
scsihw
virtio-scsi-pci
sockets
2
vmid
100
Start after created
Advanced
Back
Finish

Hinzufügen einer weiteren Netzwerkbrücke

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



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

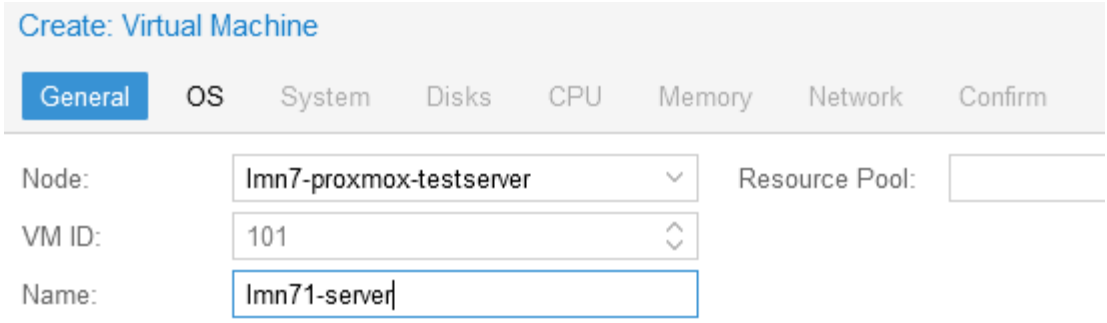
Klicke auf `Add`.

Anlegen der VM für linuxmuster server

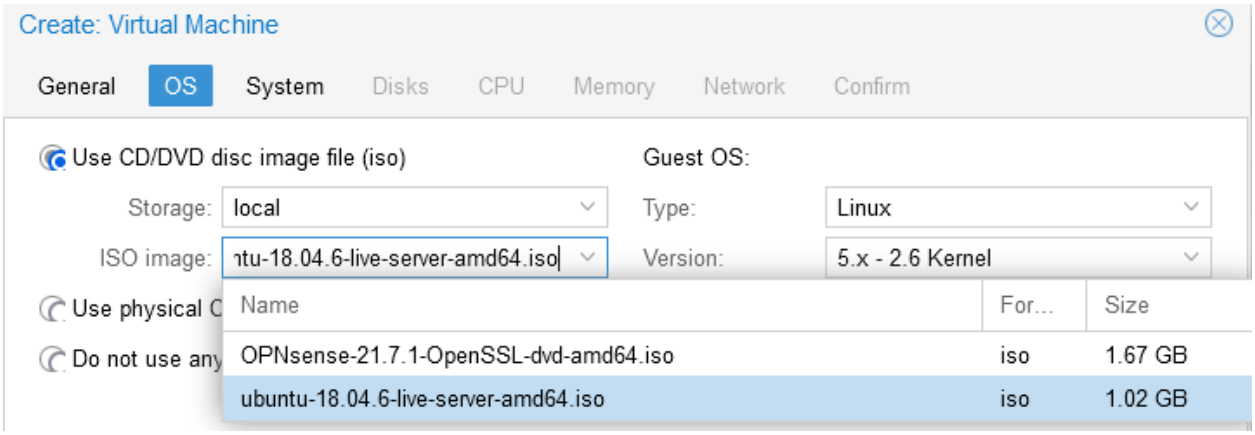
Um für den linuxmuster.net Server v7.1 die VM anzulegen, wählst Du erneut in der Proxmox - Verwaltungsoberfläche den Button `Create VM`.

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`.

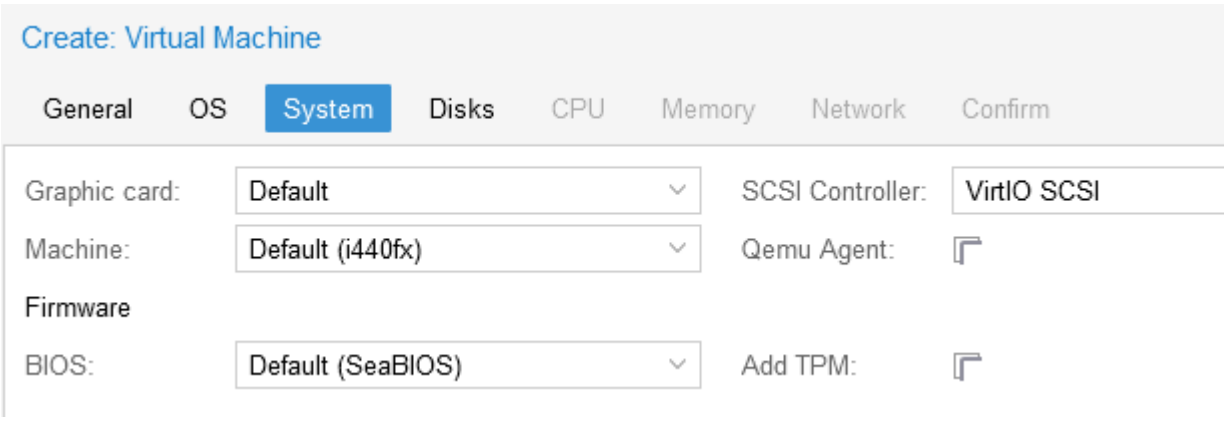


Wähle nun den ISO-Datenspeicher unter Storage aus. Das ist der Speicher, auf den Du vorher die ISO-Images abgelegt hast. Wähle dann das ISO image der OPNsense aus.



Klicke dann auf `Next`.

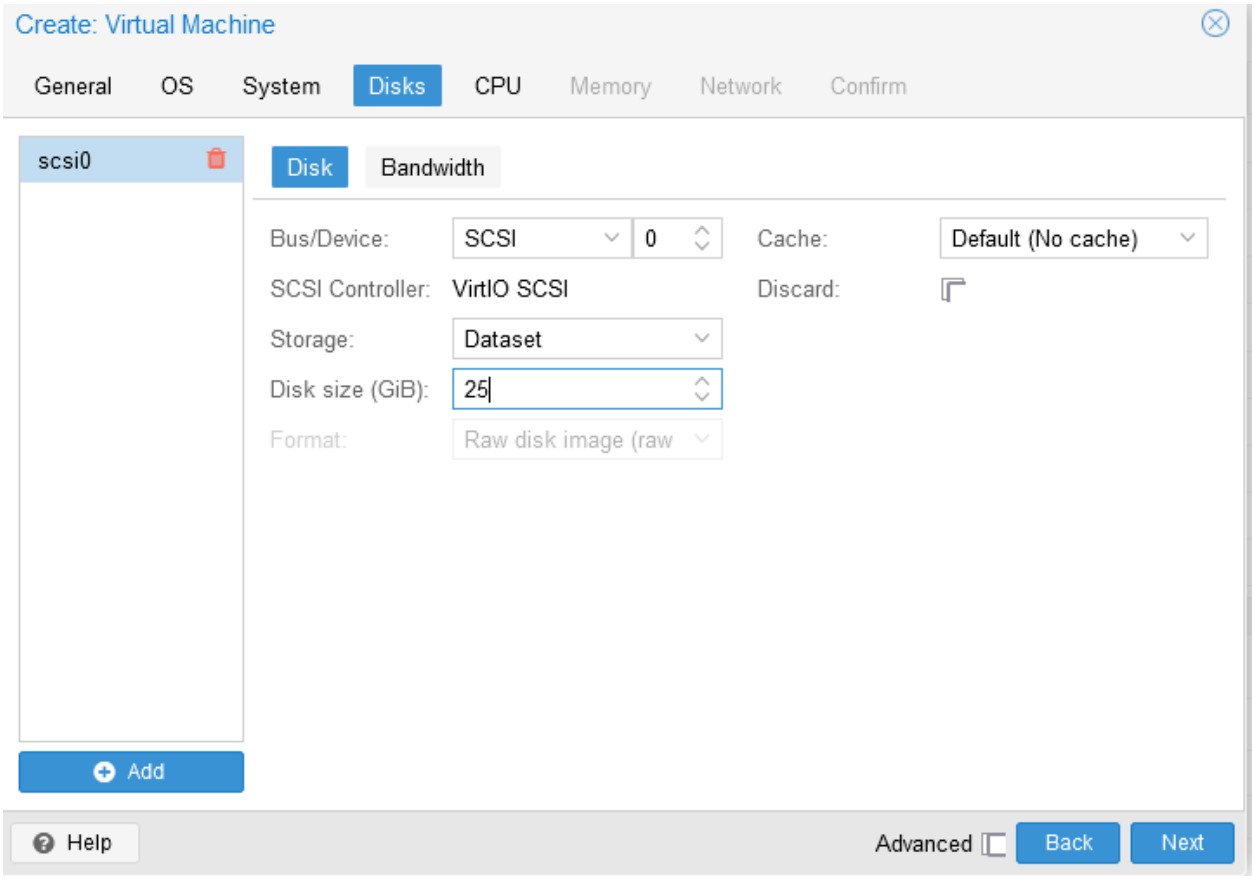
Belasse hier zunächst alle Voreinstellungen für Grafikkarte und Festplatten-Controller wie angezeigt.



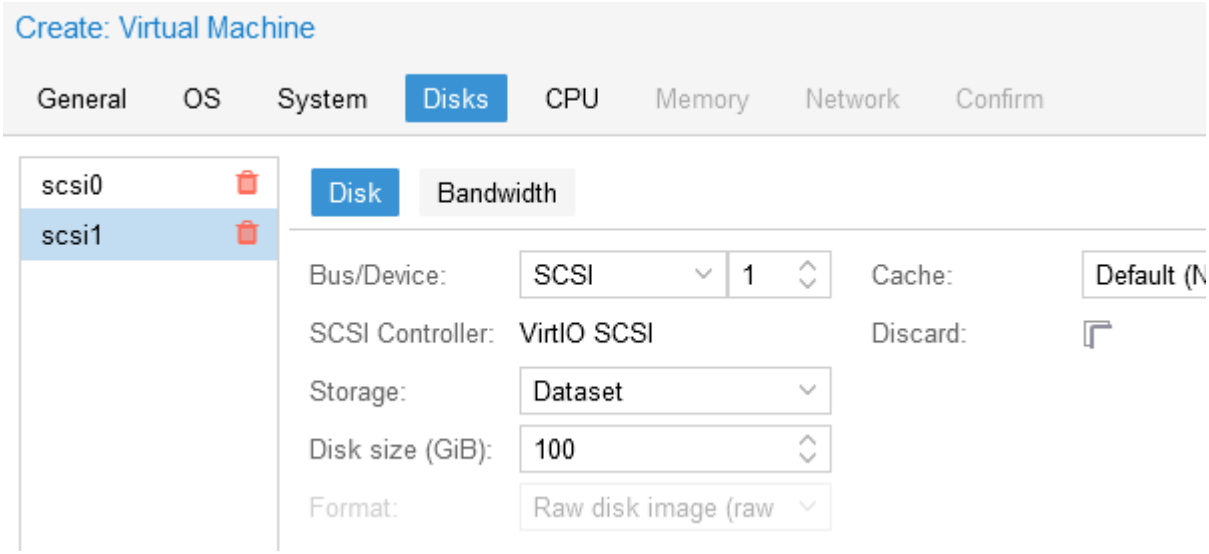
Klicke dann auf `Next`.

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.

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

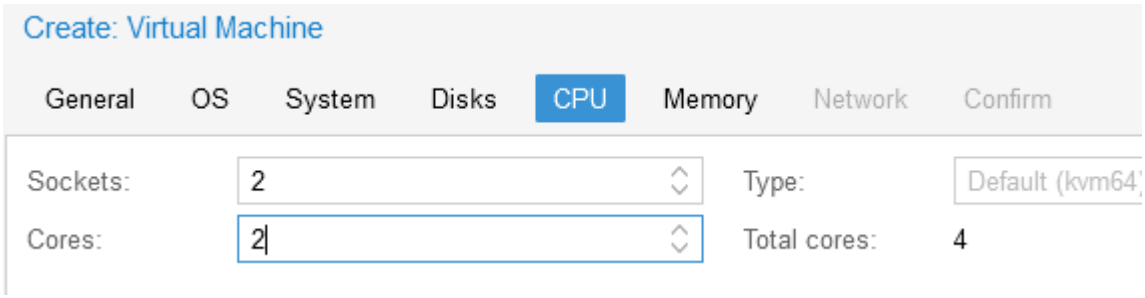

Create: Virtual Machine
General
OS
System
Disks
CPU
Memory
Network
Confirm
scsi0
Disk
Bandwidth
Bus/Device:
SCSI
0
Cache:
Default (No cache)
SCSI Controller:
VirtIO SCSI
Discard:
Storage:
Dataset
Disk size (GiB):
25
Format:
Raw disk image (raw
Add
Help
Advanced
Back
Next

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



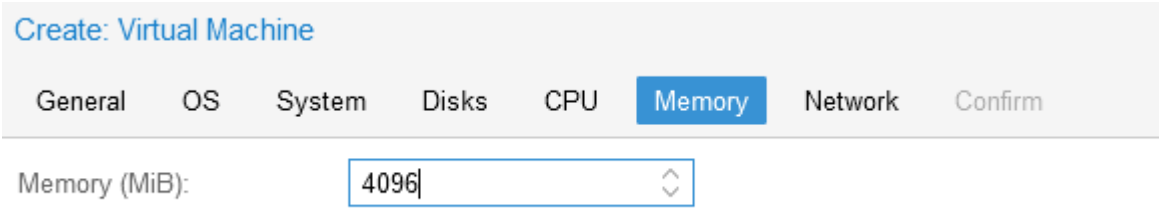
Klicke dann auf `Next`.

Gib nun für die CPU Sockel und Kerne an.



Klicke dann auf `Next`.

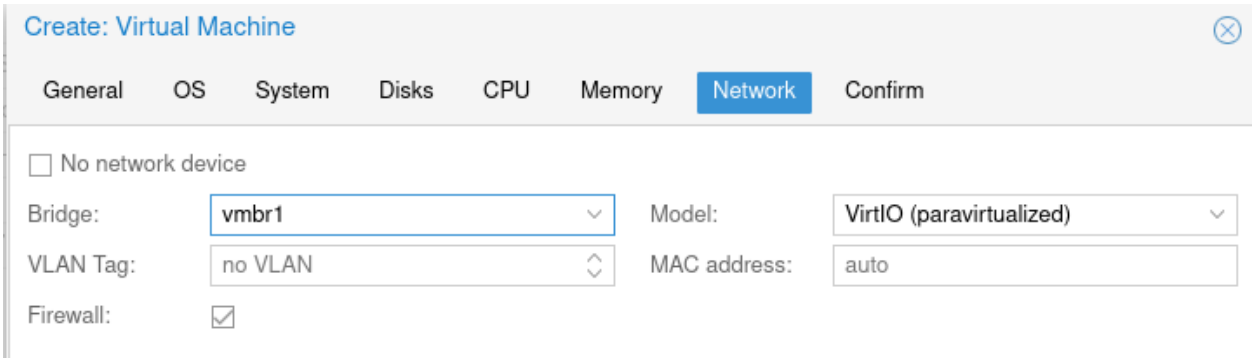
Gib nun für den Server die gewünschte Größe des Arbeitsspeichers an.



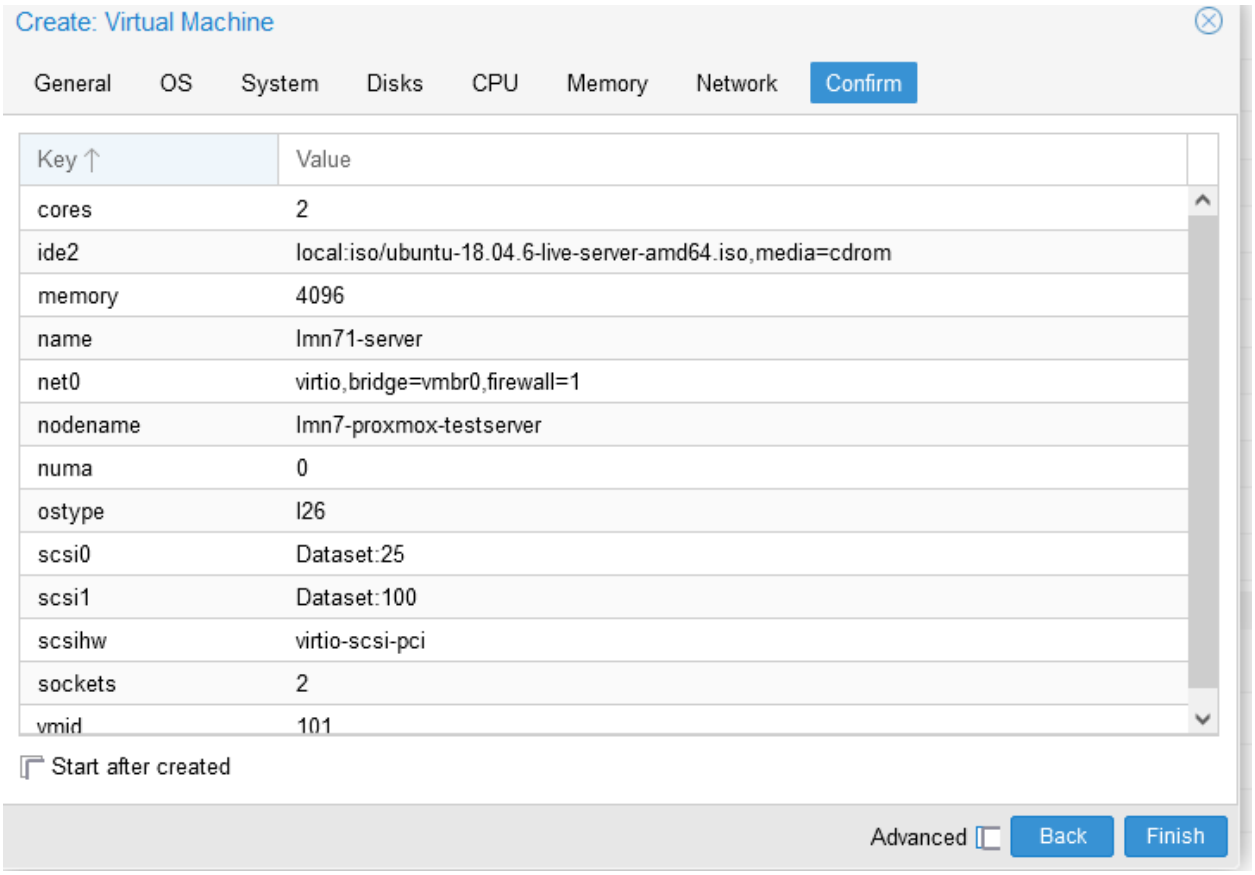
Klicke dann auf `Next`.

Gib danach die Bridge vmbr1 für die einzurichtende Netzwerkkarte an. Dies muss die Bridge für das interne Netz (green) sein.

Klicke dann auf `Next`.



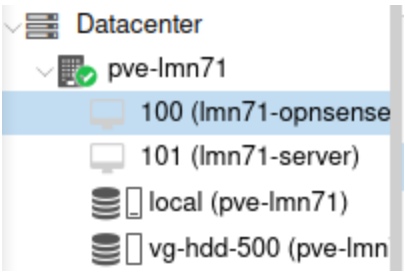
Zum Abschluss siehst Du nochmals alle getroffenen Einstellungen. Überprüfe diese. Solltest Du Änderungen vornehmen wollen, kannst Du auf die entsprechende Reiterkarte klicken, Änderungen durchführen und wieder zur Reiterkarte `Confirm` wechseln.



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.

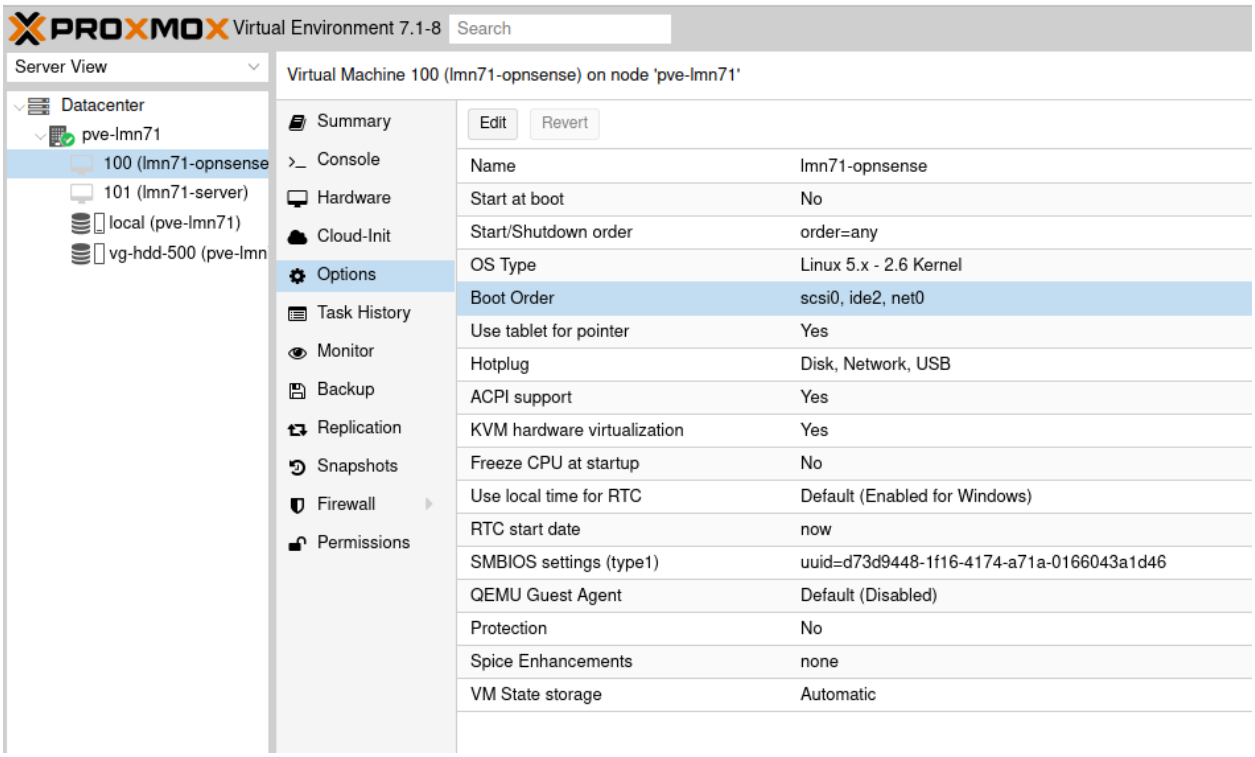


Abschließende Konfiguration der virtuellen Maschinen

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

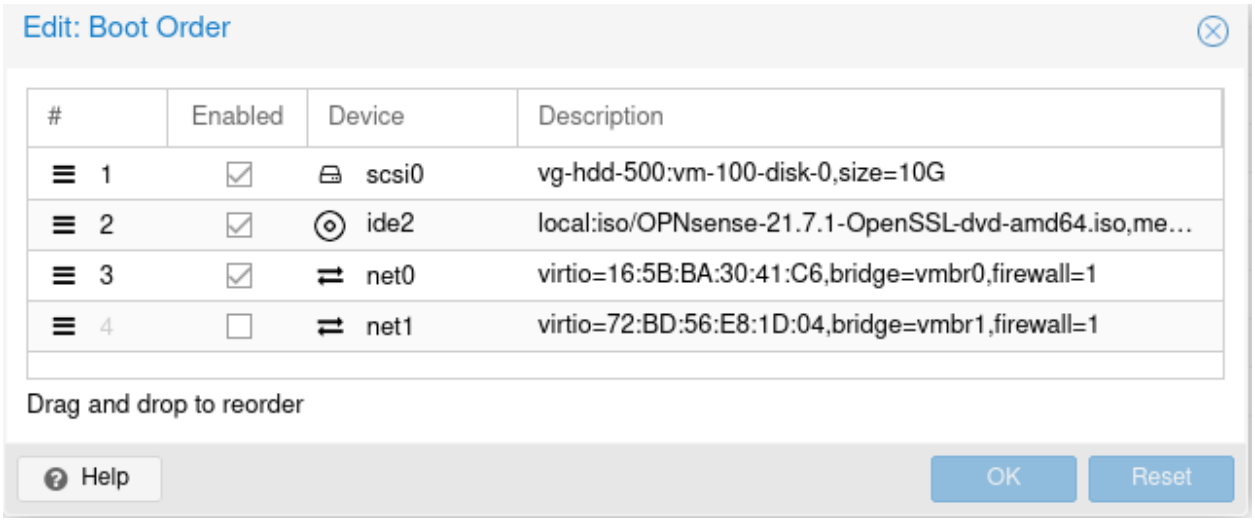
Um bei der from Scratch Installation von CD zu starten, wählst Du die VM aus, klickst auf `Options` und klickst oben auf den Menüeintrag `Edit`.

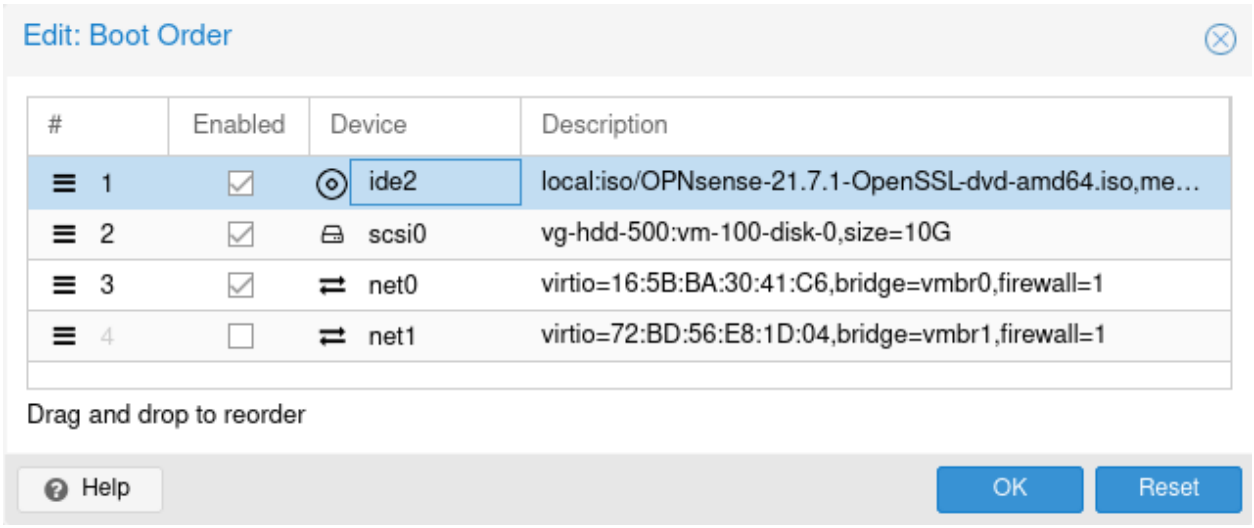


Markiere mit der Maus den Eintrag ide2 (CD) und ziehe diesen an Position 1.

Vorher:

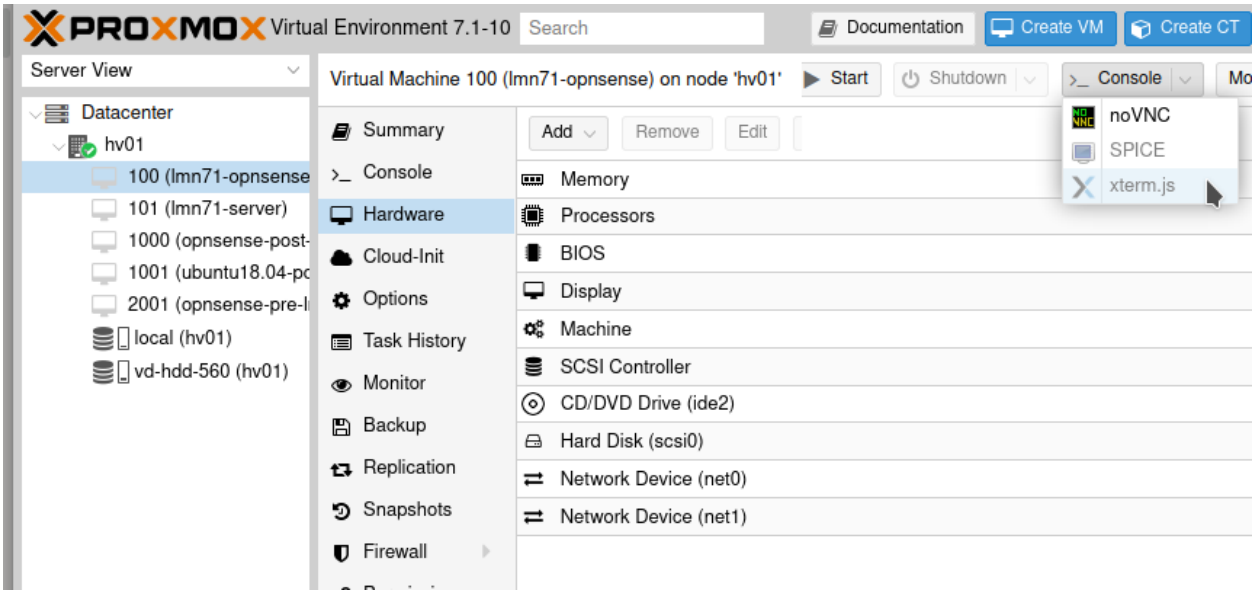
Nachher:


Edit: Boot Order
Enabled Device Description
1 scsi0 vg-hdd-500:vm-100-disk-0,size=10G
2 ide2 local:iso/OPNsense-21.7.1-OpenSSL-dvd-amd64.iso,me…
3 net0 virtio=16:5B:BA:30:41:C6,bridge=vmbr0,firewall=1
4 net1 virtio=72:BD:56:E8:1D:04,bridge=vmbr1,firewall=1
Drag and drop to reorder
Help
OK
Reset

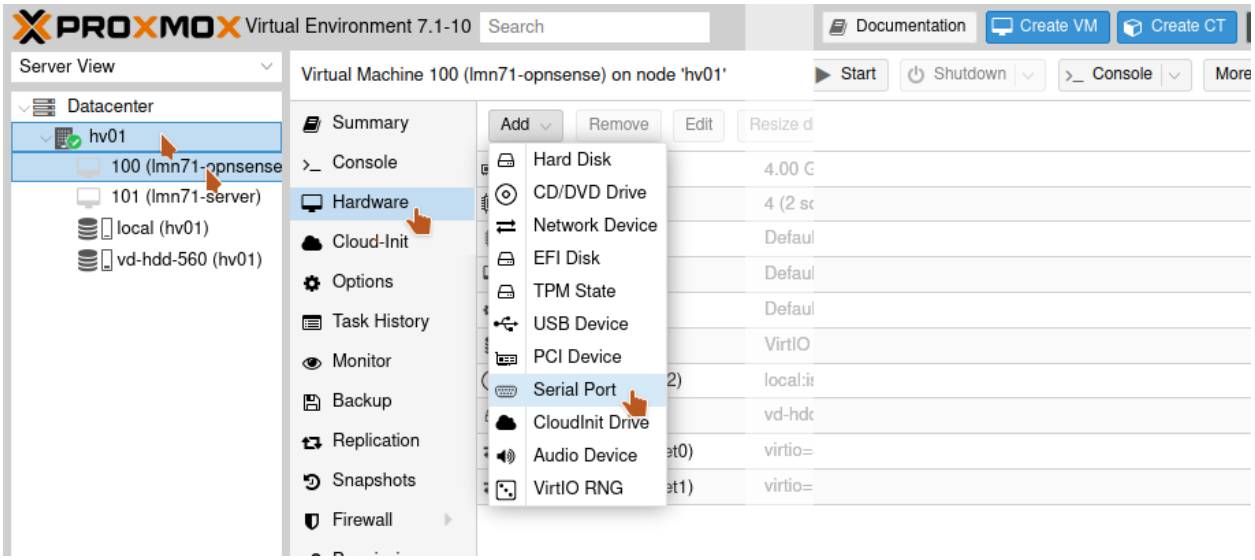

Edit: Boot Order
Enabled Device Description
1 ide2 local:iso/OPNsense-21.7.1-OpenSSL-dvd-amd64.iso,me…
2 scsi0 vg-hdd-500:vm-100-disk-0,size=10G
3 net0 virtio=16:5B:BA:30:41:C6,bridge=vmbr0,firewall=1
4 net1 virtio=72:BD:56:E8:1D:04,bridge=vmbr1,firewall=1
Drag and drop to reorder
Help
OK
Reset

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 Maßnahmen musst Du eine serielle Schnittstelle für die jeweilige VM aktivieren.



Das obige Bildschirmfoto zeigt den Zustand vor der Aktivierung.



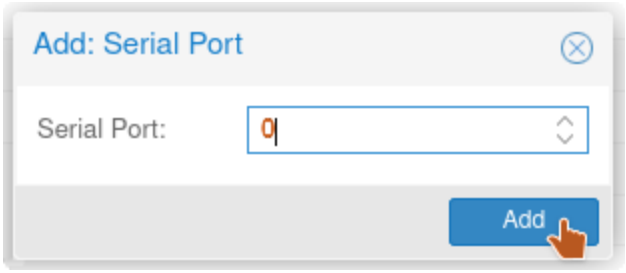
Gehe auf `hv01` –> `lmn71-opnsense` –> `Hardware` –> `Serial Port`

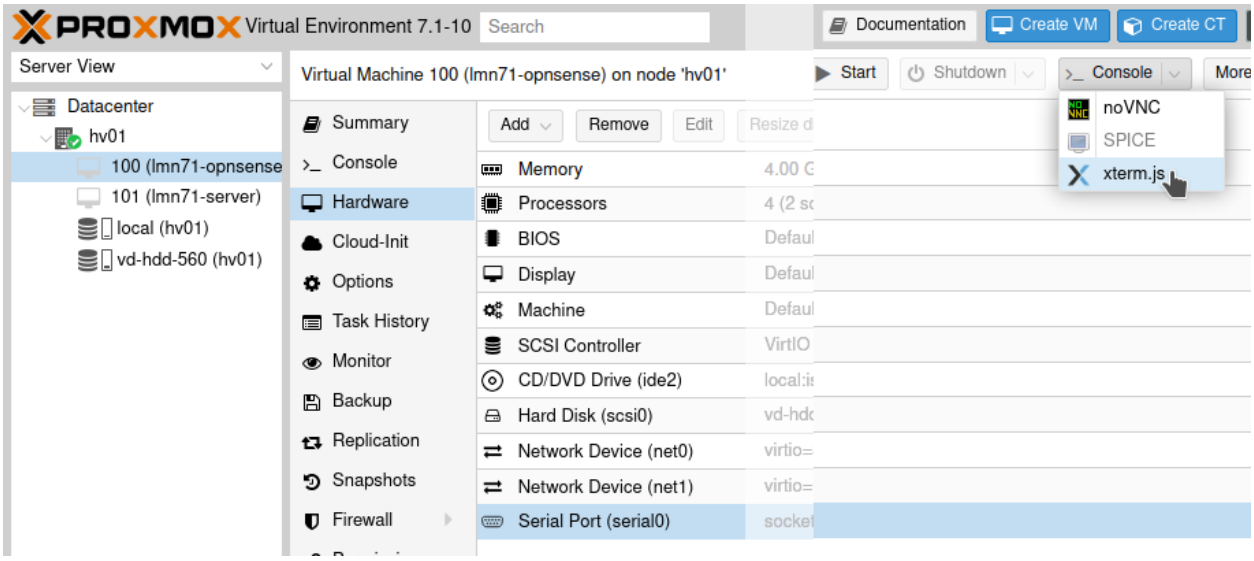
Lege einen Seriellen Port mit der Bezeichnung `0` an.

Klicke auf `Add`, anschließend sollte der gezeigte Menüpunkt nicht mehr ausgegraut sein.

Kontrolliere nochmals alle Einstellungen der neu angelegten VM.

Die beiden letzten Einstellungen musst Du **nochmals für den Server** 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.

Nun sind Deine virtuellen Maschinen für die weitere Installation bereit und Du kannst gemäß der Anleitung: *Install-from-Scratch* weiterarbeiten.

4.6 Install-from-Scratch

Autor des Abschnitts: @rettich, @cweikl @MachtDochNiX

In diesem Dokument findest Du eine „Schritt-für-Schritt“ Anleitung zur Installation der linuxmuster.net Musterlösung direkt auf der Hardware. Zugleich nutzt Du diese Anleitung zur Installation in vorbereitete VMs.

Lies zuerst die Abschnitte „*Was ist neu in 7.1?*“ 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®.
- Gefolgt von der Installation des Ubuntu-Servers.
- Schließlich richtest Du linuxmuster.net ein.

4.6.1 Anlegen und Installieren der Firewall

Autor des Abschnitts: @rettich, @cweikl @MachtDochNiX

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

Installation der OPNsense®

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 v7.1 ist die Version 22.7. https://mirror.informatik.hs-fulda.de/opnsense/releases/22.7/OPNsense-22.7-OpenSSL-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.

Gib unter Linux folgenden Befehl an:

```
bunzip2 OPNsense-22.7-OpenSSL-dvd-amd64.iso.bz2
```

Brenne die entpackte ISO-Datei auf eine DVD oder fertige davon einen bootbaren USB-Stick an. In einer 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 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.

Achtung, unter XCP-ng bricht die Installation mit o.g. Einstellungen beim Punkt `guided installation` ab, wenn UEFI als Boot-Mode angegeben wurde. Es ist als Boot-Mode in der VM Boot/MBR auszuwählen. Bei der weiteren Installation kann dann hingegen GPT/UEFI mode angegeben werden.

Vgl. hierzu auch: https://xcp-ng.org/docs/guides.html#pfsense-opnsense-vm

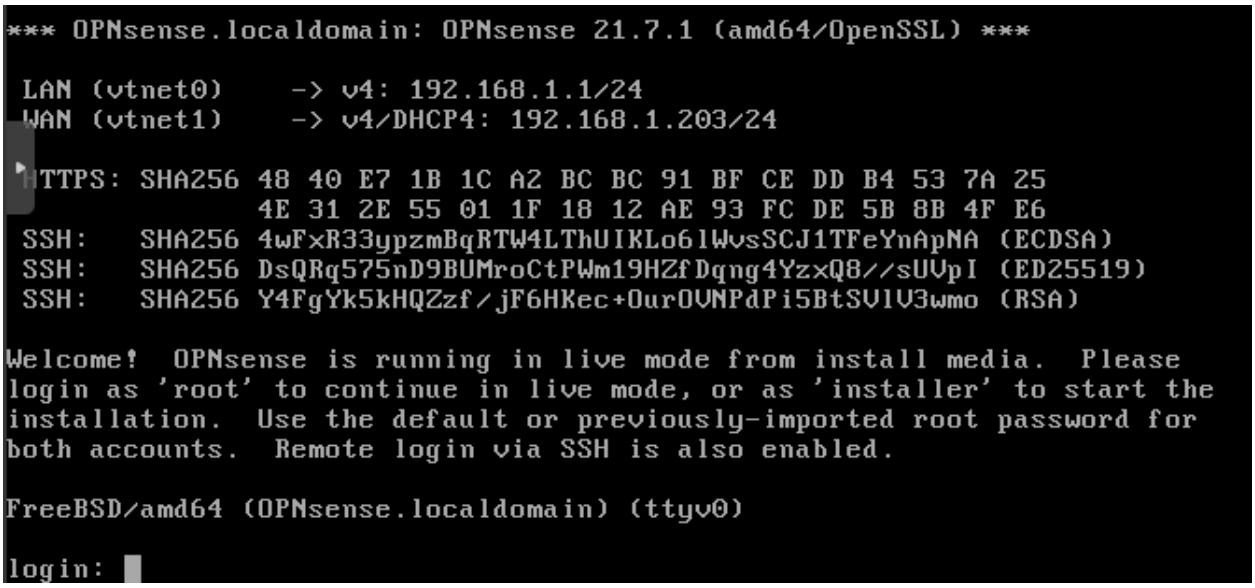
---

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 den ISO-Datenspeicher des Hypervisors abgelegt. Boote dann die VM hierüber.

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

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



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 die Umlaute im Test noch nicht korrekt wiedergegeben.

Wähle trotzdem die eingestellte deutsche Tastatur aus:

Wähle <Select>.

Installiere nun OPNsense® via `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.

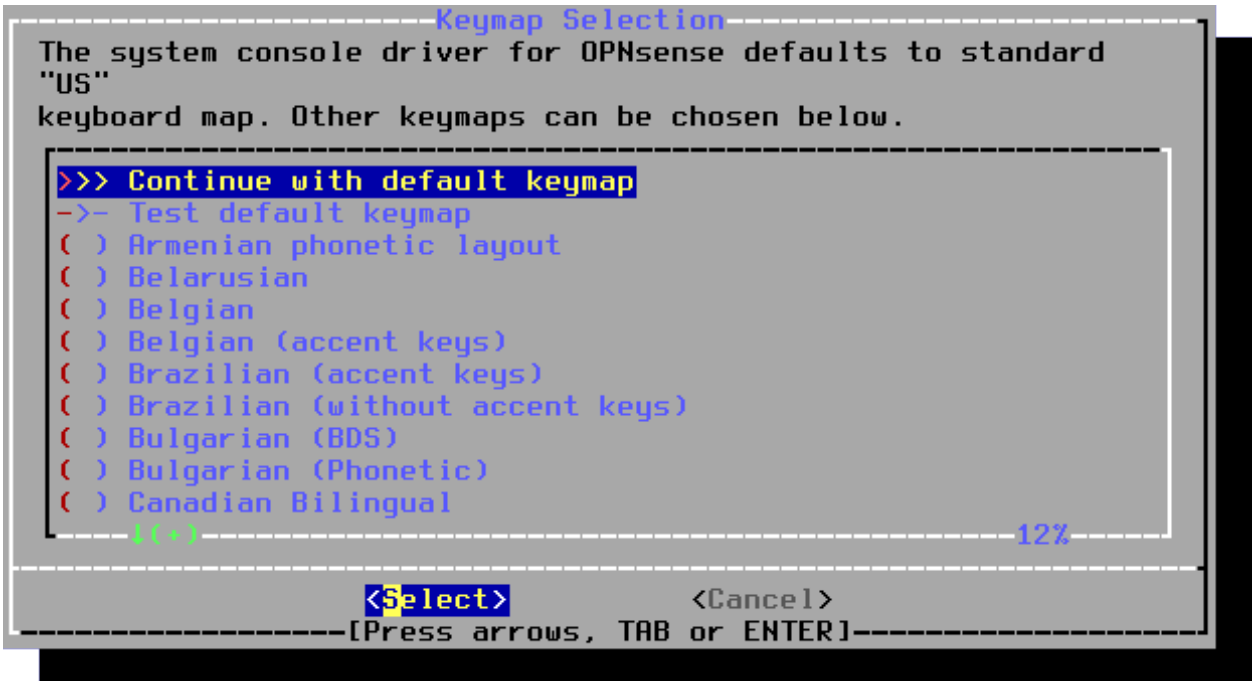
Mit `OK` übernimmst Du Deine Auswahl.

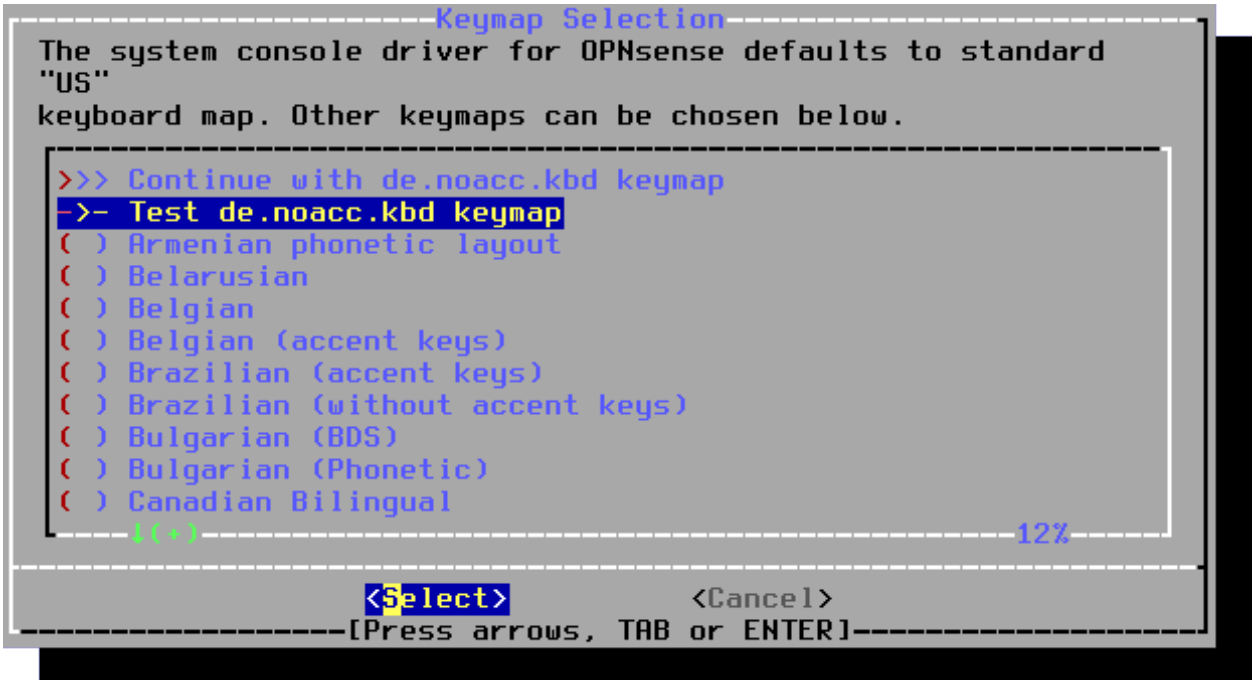
Sollte Dir dieses Fenster angezeigt werden, dann akzeptiere die Frage nach der empfohlenen Auslagerungsdatei.

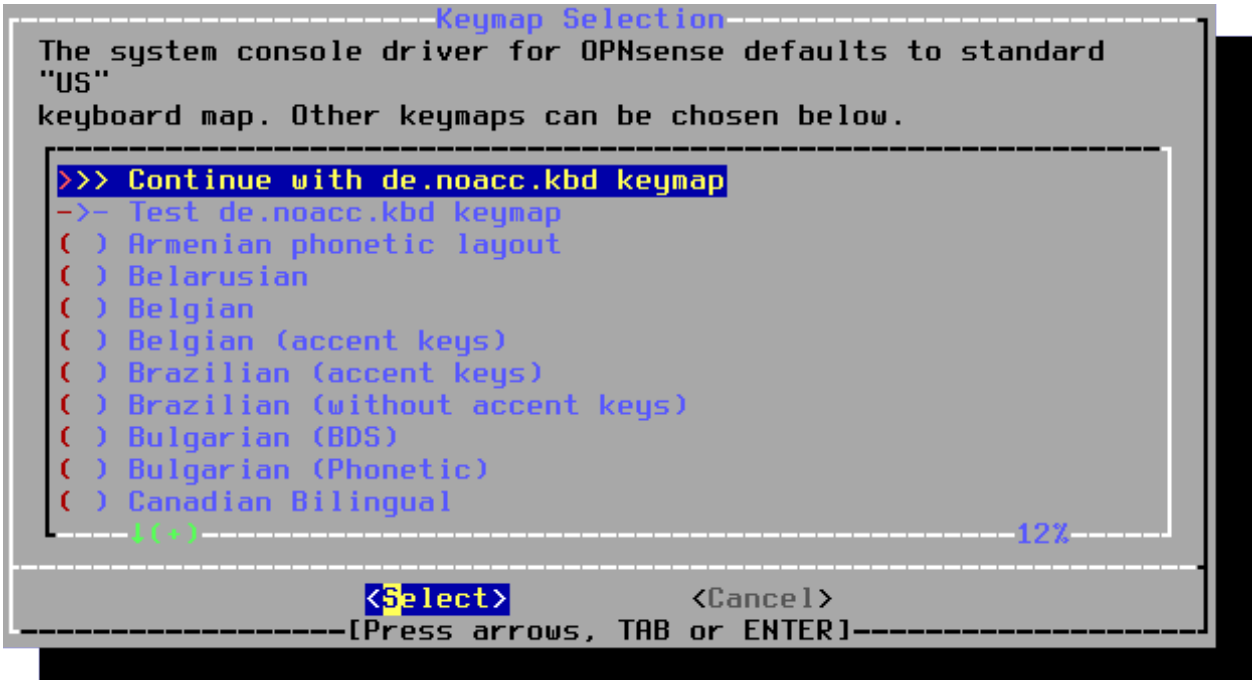
Danach erfolgt die Rückfrage, ob die Festplatte wirklich überschrieben werden soll.

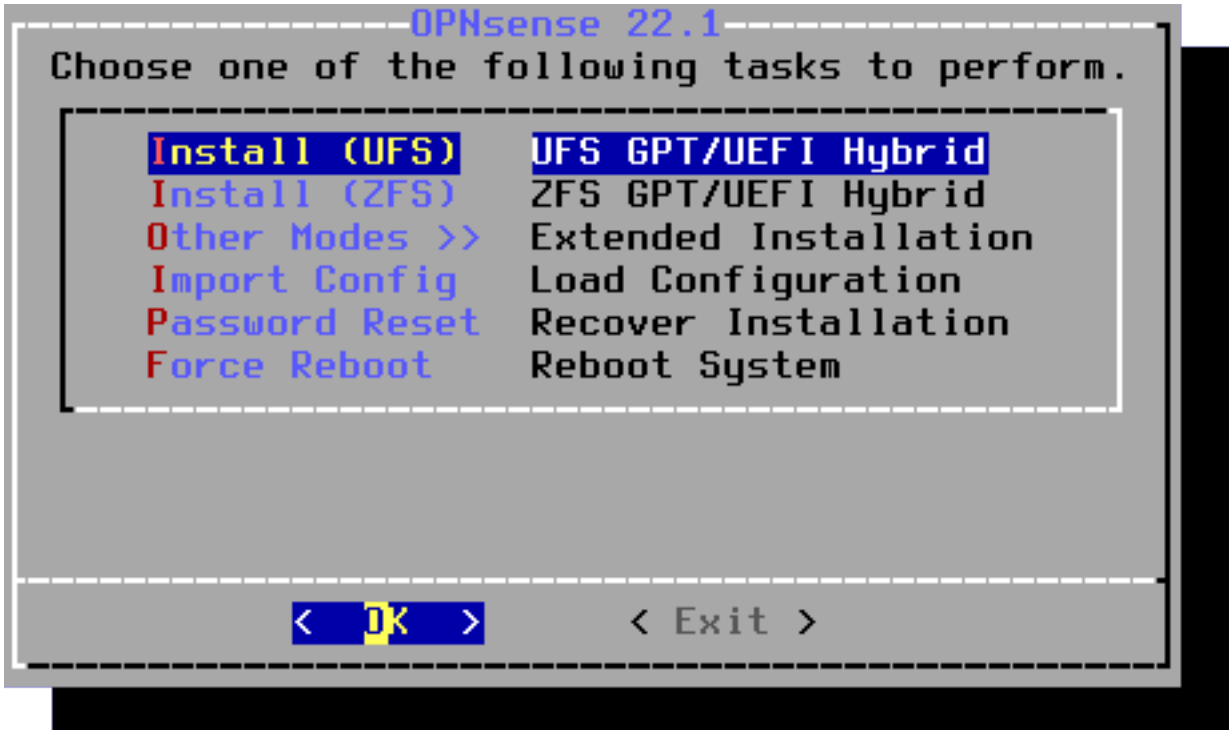
Bestätige diesen Vorgang, um die Installation zu starten.

Warte jetzt, bis die Installation abgeschlossen ist.

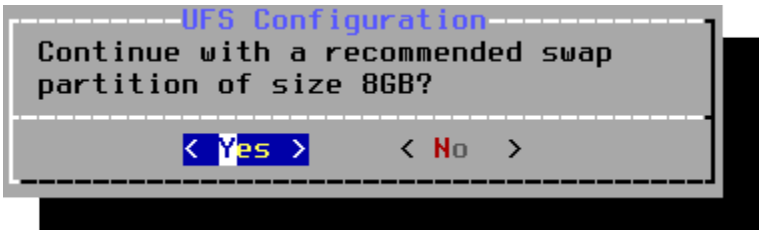

Keymap Selection
The system console driver for OPNsense defaults to standard
"US"
keyboard map. Other keymaps can be chosen below.
>>> Continue with default keymap
->- Test default keymap
( ) Armenian phonetic layout
( ) Belarusian
( ) Belgian
( ) Belgian (accent keys)
( ) Brazilian (accent keys)
( ) Brazilian (without accent keys)
( ) Bulgarian (BDS)
( ) Bulgarian (Phonetic)
( ) Canadian Bilingual
12%
<Select>
<Cancel>
[Press arrows, TAB or ENTER]

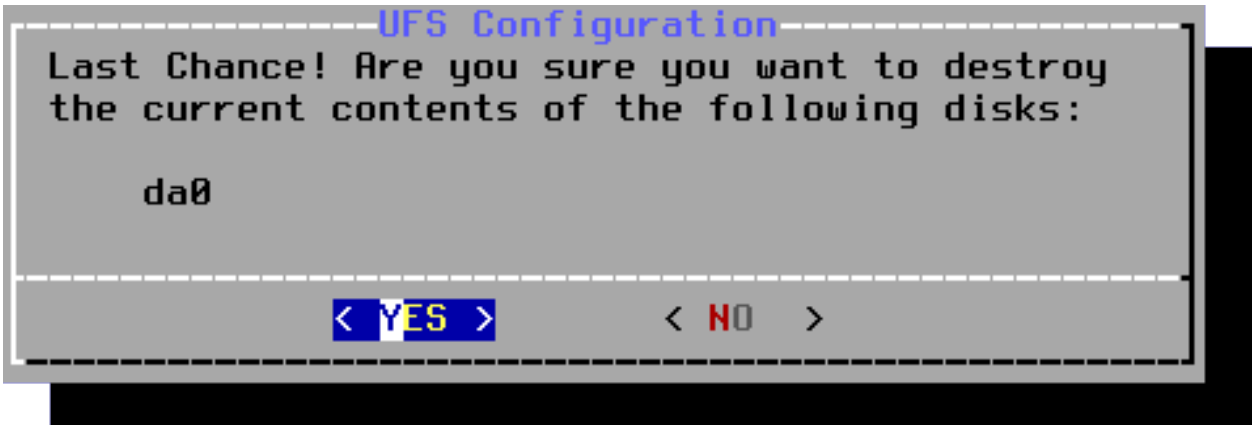

Keymap Selection
The system console driver for OPNsense defaults to standard
"US"
keyboard map. Other keymaps can be chosen below.
>>> Continue with de.noacc.kbd keymap
->- Test de.noacc.kbd keymap
( ) Armenian phonetic layout
( ) Belarusian
( ) Belgian
( ) Belgian (accent keys)
( ) Brazilian (accent keys)
( ) Brazilian (without accent keys)
( ) Bulgarian (BDS)
( ) Bulgarian (Phonetic)
( ) Canadian Bilingual
12%
<Select>
<Cancel>
[Press arrows, TAB or ENTER]

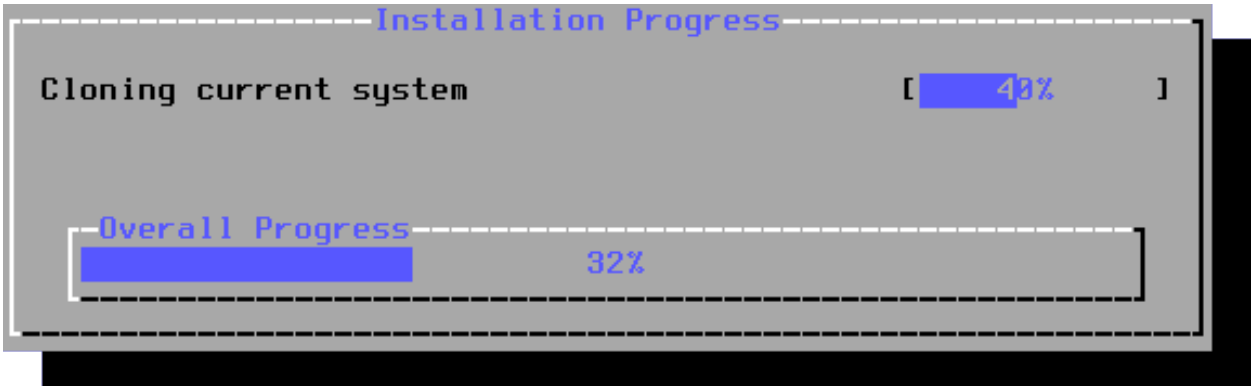

Keymap Selection
The system console driver for OPNsense defaults to standard
"US"
keyboard map. Other keymaps can be chosen below.
>>> Continue with de.noacc.kbd keymap
->- Test de.noacc.kbd keymap
( ) Armenian phonetic layout
( ) Belarusian
( ) Belgian
( ) Belgian (accent keys)
( ) Brazilian (accent keys)
( ) Brazilian (without accent keys)
( ) Bulgarian (BDS)
( ) Bulgarian (Phonetic)
( ) Canadian Bilingual
12%
<Select>
<Cancel>
[Press arrows, TAB or ENTER]


OPNsense 22.1
Choose one of the following tasks to perform.
Install (UFS) UFS GPT/UEFI Hybrid
Install (ZFS) ZFS GPT/UEFI Hybrid
Other Modes >> Extended Installation
Import Config Load Configuration
Password Reset Recover Installation
Force Reboot Reboot System
< OK >
< Exit >

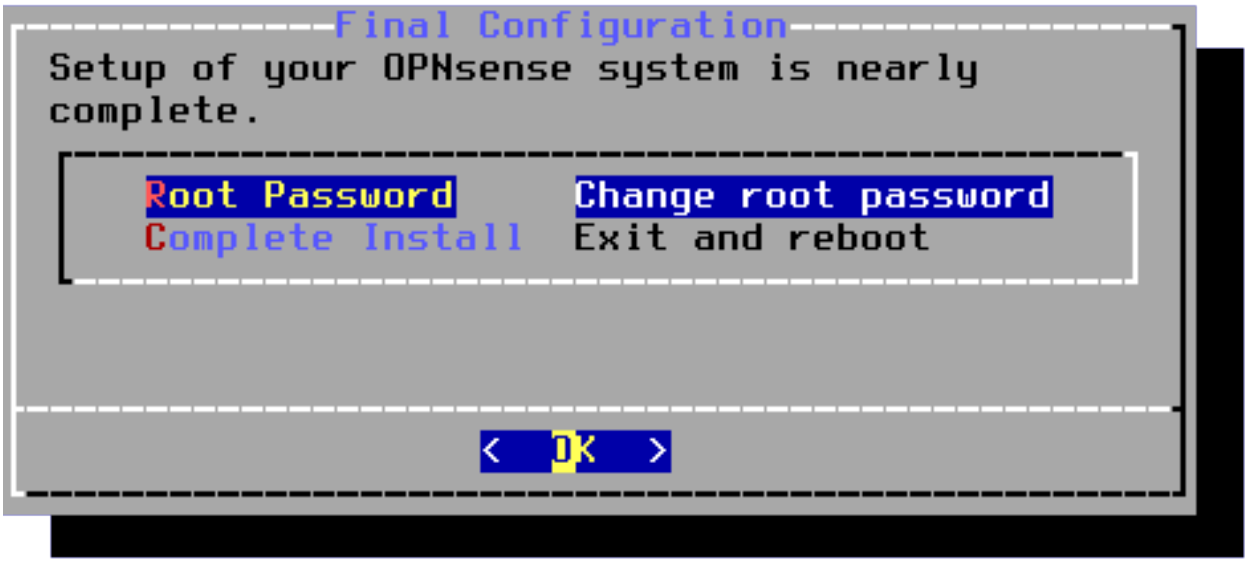

UFS Configuration
Please select a disk to continue.
cd0 <QEMU QEMU DVDROM 25> (1GB)
da0 <QEMU QEMU HARDDISK 25> (10GB)
< OK >
<Cancel>


UFS Configuration
Continue with a recommended swap
partition of size 8GB?
< Yes >
< No >


UFS Configuration
Last Chance! Are you sure you want to destroy
the current contents of the following disks:
da0
< YES >
< NO >

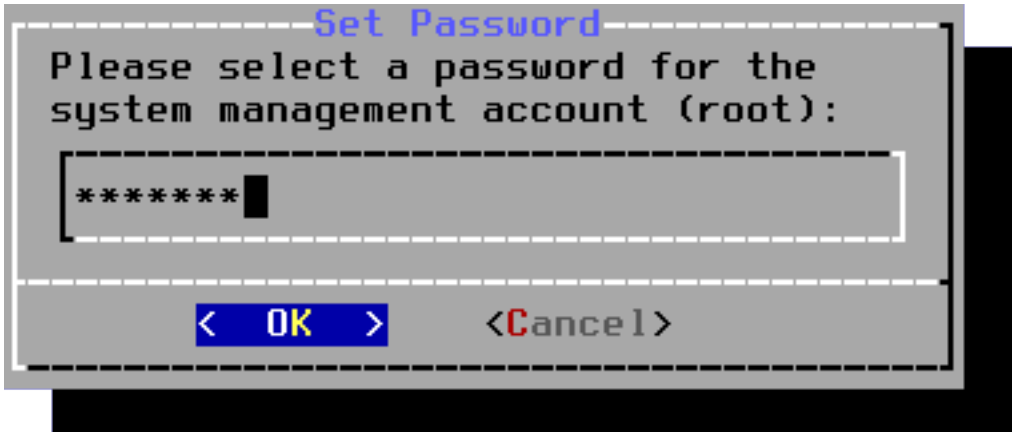

Installation Progress
Cloning current system
[40%]
Overall Progress
32%

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 für root ein.



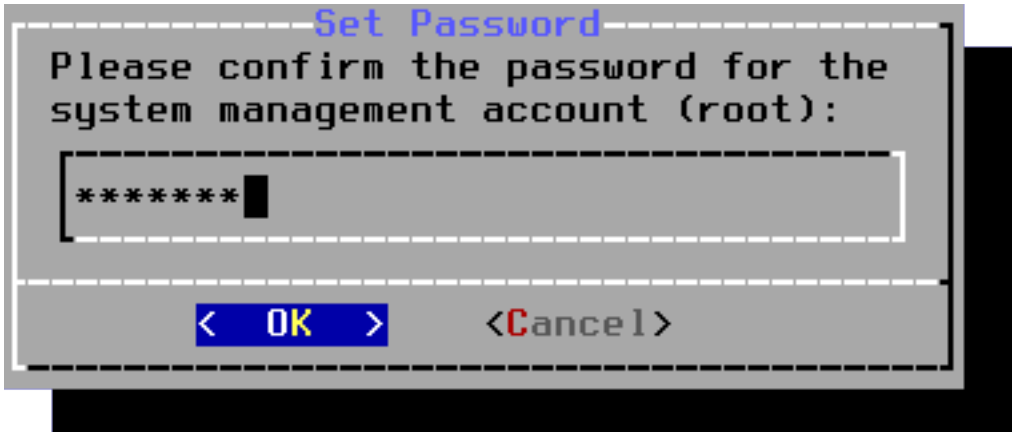
Gib dieses Kennwort erneut ein.

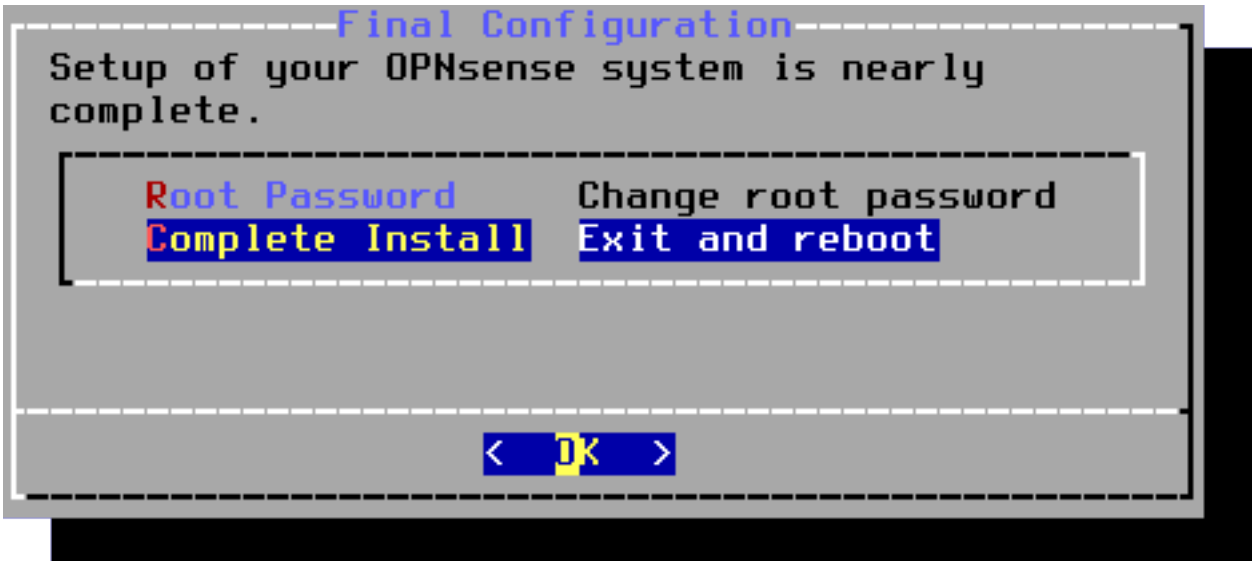
Setze es mit `OK`

Wähle danach die Option `Exit and reboot` aus.

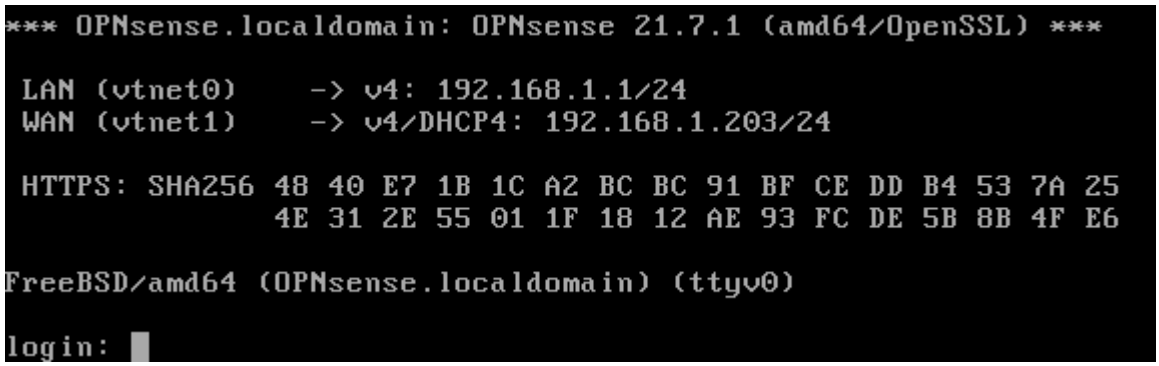
Hinweis: Solltest Du nicht zum Entfernen, das Installationsmedium aufgefordert werden, fahre Deine neue Firewall herunter (schalte sie aus). Ansonsten gerätst Du eventuell in eine erneute Installation. Starte sie neu, nachdem Du das Installationsmedium ausgeworfen hast und fahre mit der Installation fort.

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


Set Password
Please confirm the password for the system management account (root):
****
< OK >
<Cancel>


Final Configuration
Setup of your OPNsense system is nearly complete.
Root Password
Change root password
Complete Install
Exit and reboot
< OK >

Wenn alles geklappt hat, ist Folgendes zu sehen:

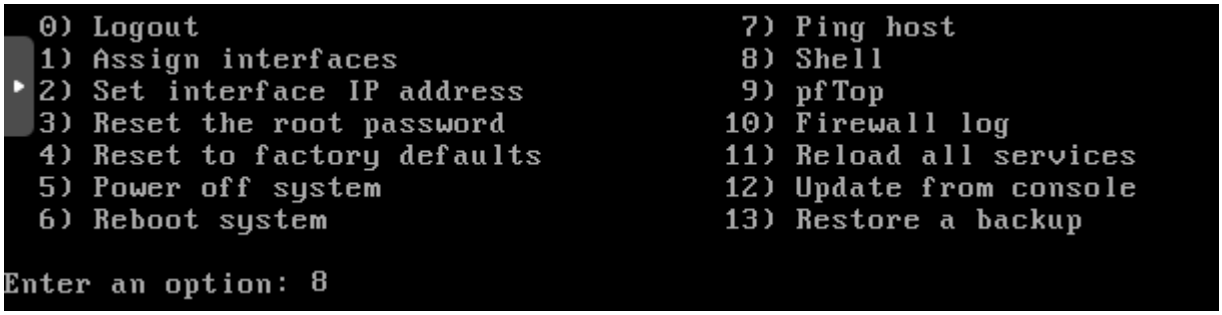


Hinweis: Die dargestellte IPs und Netze können bei Deiner OPNsense® andere sein.

Basis-Konfiguration der OPNsense®

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

Tastaturbelegung



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:

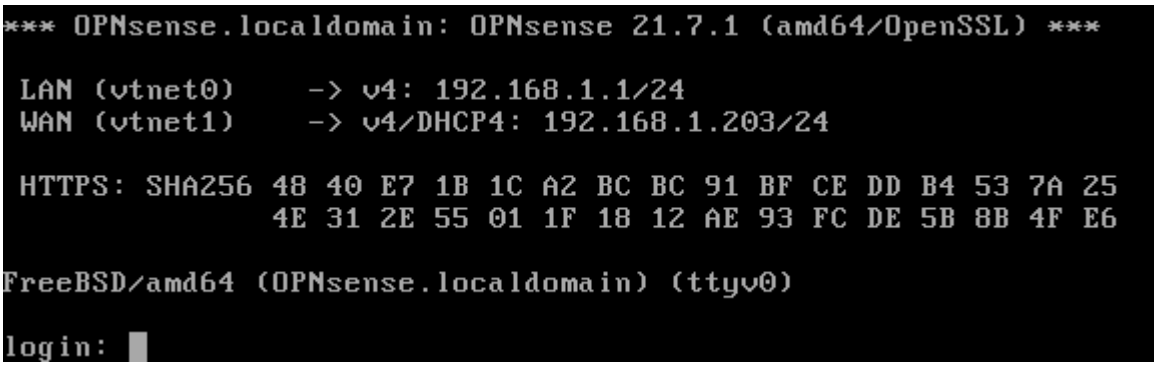
```
cd /usr/share/syscons/keymaps     # Für den Buchstaben "z" musst Du die Taste "y" drücken␣
↪;-)

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
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
                                # - teste, ob es dem gewünschten Layout entspricht

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

cat /etc/rc.conf                # kontrolliere, ob der Eintrag vorhanden ist

exit                            # Konsole verlassen
```

Überprüfung der Zuordnung der Netzwerkkarten



Die erste Netzwerkkarte (LAN) ist mit dem pädagogischen Netz verbunden. Allerdings noch mit den falschen Netzwerkeinstellungen, da die Installationsroutine der OPNsense® immer die IP 192.168.1.1/24 zuweist. Diese gilt es noch zu ändern.

Die zweite Netzwerkkarte (WAN) ist mit dem Router verbunden. Die IP hängt davon ab, welche IPs via DHCP von Deinem DSL_Router verteilt werden.

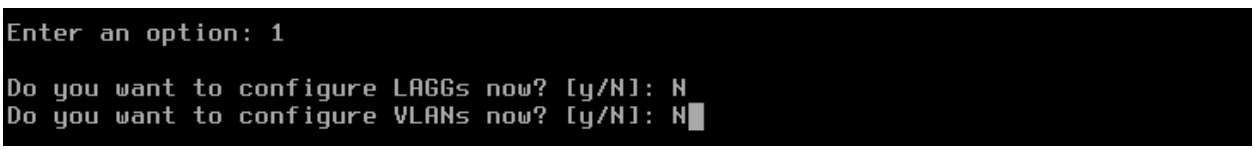
In einer Schulumgebung kann es sein, dass der Router keinen DHCP-Service anbieten. In diesem Fall musst Du dafür sorgen, dass sich sowohl das Interface (WAN) der OPNsense® als auch der Router im gleichen Netzwerk befinden.

Hier in unserem Beispiel hat die Zuordnung der Netzwerkkarten nicht geklappt, der Router sollte 192.168.21.212 der OPNsense® zuweisen.

Sollte bei dem WAN Interface keine, eine IP-Adresse nach dem Muster 0.0.0.0/8 oder eine andere als die von Dir erwartete erscheinen, dann muss die Zuordnung der Netzwerkkarte überprüft werden. Hier beispielhaft anhand unserer Proxmox-Umgebung.

Anpassung der Zuordnung der Netzwerkkarten

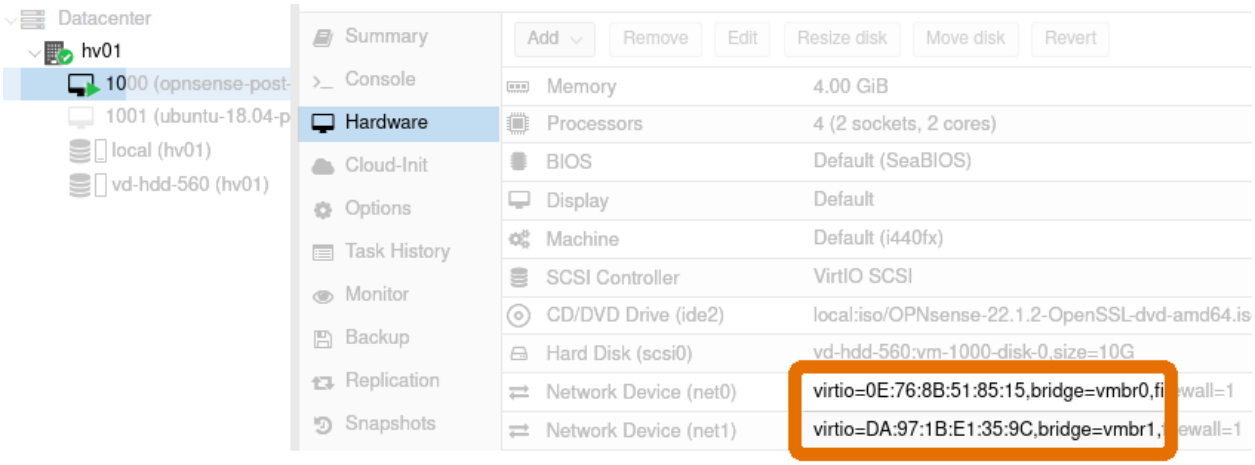
Rufe dazu den Menüeintrag `1) Assign interfaces` auf. Die Nachfragen bezüglich LAGGs und VLAN verneinst du.



Dann gilt es die MAC-Adressen zwischen denen der virtuellen Maschine, hier vtnet0 und vtnet1

```
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:
```

und denen der Netzwerkbrücken vmbr0 und vmbr1 zu überprüfen:



`hv01` –> `VM100` –> `Hardware` –> `Network Device (net.)`

Unter `hv01` unter `Network` kannst Du Dir jetzt mittels des Kommentarfeldes wieder die Zuordnung ins Gedächtnis rufen.

Bridge des Visualisierers			<->	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

Aus diesem Wissen und dem Vergleich erkennst Du …

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

… das WAN zum Interface vtnet0 zugeordnet gehört.

… das LAN zum Interface vtnet1 gehört.

Hast Du kein weiteres Interface, dann `Enter`

Diese Zuordnung ist nun richtig, also weiter mit `y` …

… welches dann die Konfiguration startet.

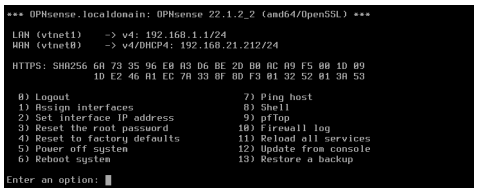
Die Zuordnung des WAN-Interfaces ist nun richtig. Das erkennst Du daran, das dessen IP-Adresse dem Adress-Pool des Routers entnommen ist.

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

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

```
The interfaces will be assigned as follows:

WAN  -> vtnet0
LAN  -> vtnet1

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

```
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.
```



WAN Zugang testen

Um zwei erste Tests durchzuführen, wechsel mit `8) Shell` auf die 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
```

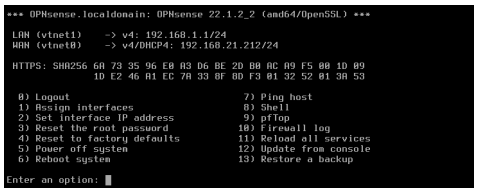
Die Ausgabe sollte wie folgt aussehen:

```
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:~ #
```

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

```
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:~ #
```

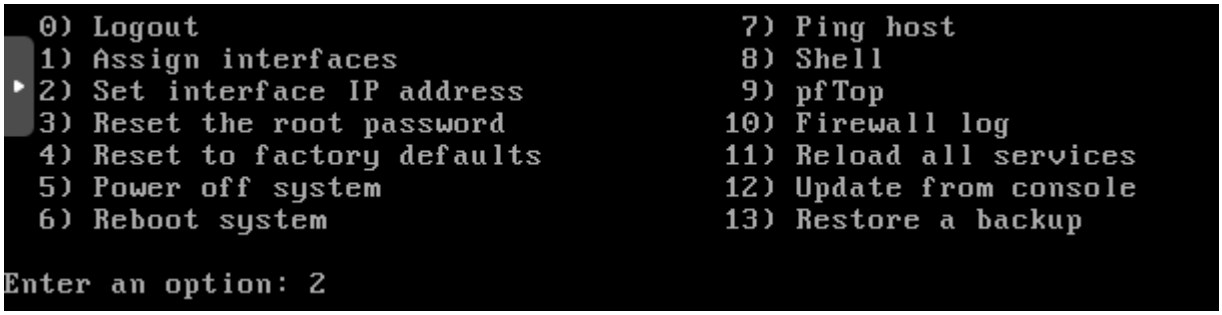
`exit` um wieder zum Dashboard zurückzukommen.



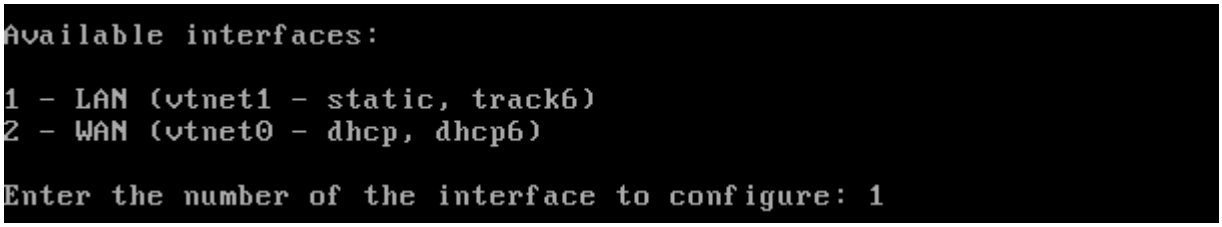
Hinweis: Sollte einer der Test auch nach `11) Reload all services` nicht erfolgreich verlaufen, dann stimmt etwas mit der Netzwerkkartenzuordnung nicht. Überprüfe Deine vorherige Netzwerk-Konfiguration auf Fehler.

IP-Adressen zuweisen

Solltest Du in Deiner Netzwerkkonfiguration von unserem Muster abweichen, musst Du bei nachfolgenden Schritten Deiner Festlegung folgen.



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



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

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 `16` für die Netzwerkmaske ein

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.

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

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

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

```
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):
> 16
```

```
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] N
```

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

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

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

```
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...
```

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

    https://10.0.0.254
```

Aktualisierung der OPNsense®

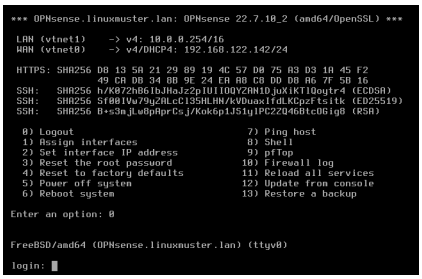
Aktualisiere die OPNsense® in der Konsole, indem Du den Punkt `12) Update from console` aufrufst und die Rückfrage mit `y` bestätigst.

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.

Klappt das Update, startet die OPNsense® neu.



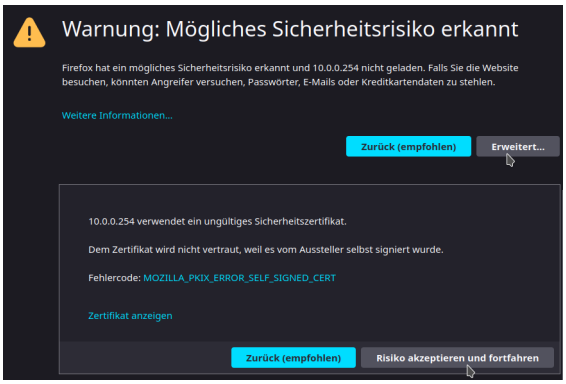
Konfiguration der OPNsense®

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 dem LAN-Adapter der OPNsense® verbunden ist und sich im gleichen Netzwerk wie die OPNsense® befindet. In unserer Beschreibung gehen wir davon aus, dass seine manuell zugewiesene IP-Adresse 10.0.0.10 ist.

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

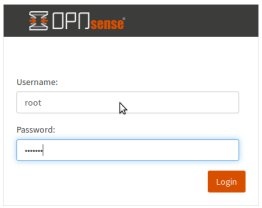
`https://10.0.0.254`

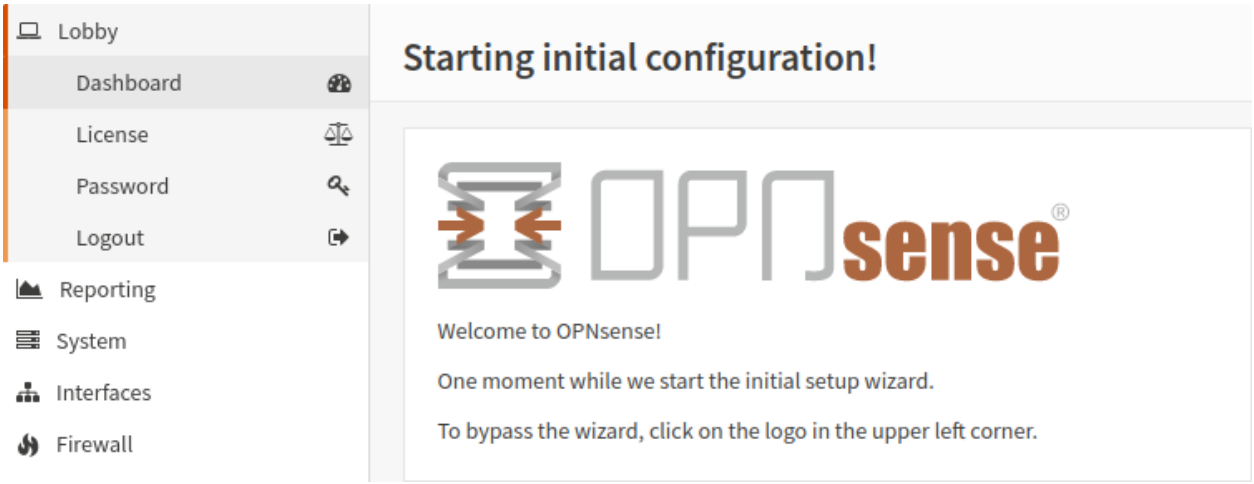
Du erhältst zunächst eine Zertifikatswarnung, da OPNsense® ja ganz frisch installiert ist und ein selbst erstelltes Zertifikat nutzt.



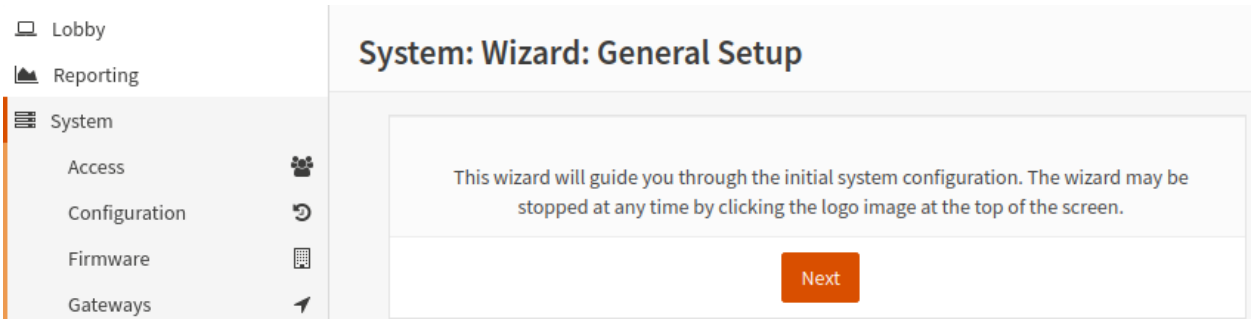
`Erweitert` und anschließend `Risiko akzeptieren und fortfahren` bringt Dich auf die Log-in-Seite.

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





Gefolgt von folgender Aufforderung:



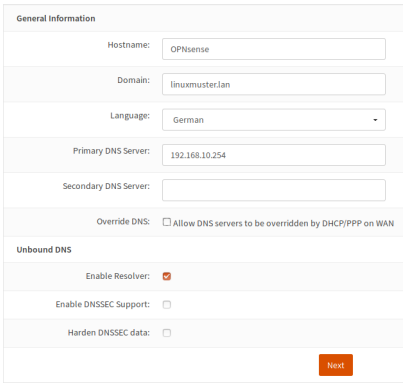
Starte den General Setup Wizard mit dem `Next`-Knopf. „Er“ wird Dich durch die Konfiguration führen, wobei schon einiges richtig durch die zuvor erfolgte Basis-Konfiguration eingerichtet wurde.

System: Assistent: Allgemeine Information

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.

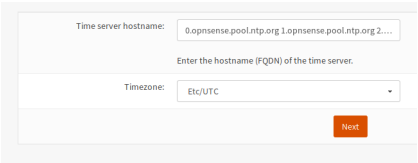
Eine gute Wahl ist beispielsweise `linuxmuster.lan`. Beim späteren Setup von linuxmuster.net wird diese ggf. für alle Server-Dienste angepasst.

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

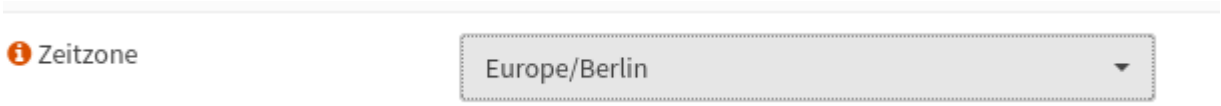


Weiter geht es mit `Next`

System: Assistent: Zeitserverinformation



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



Die Angaben übernimmst Du mit `Next`.

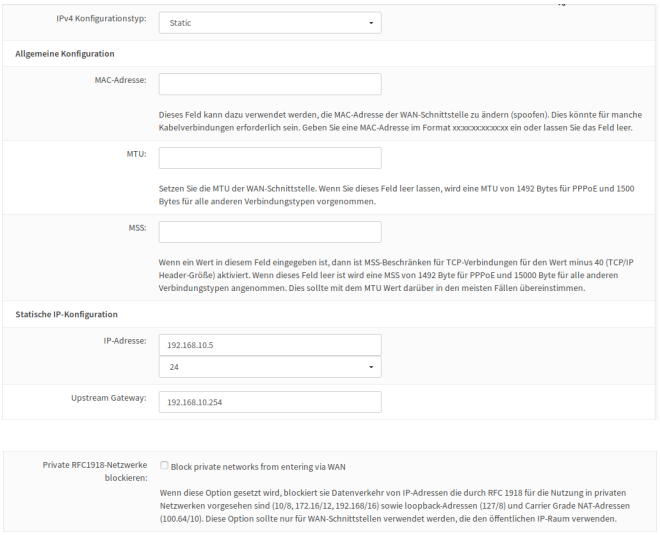
System: Assistent: Konfiguriere WAN-Schnittstelle

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`.

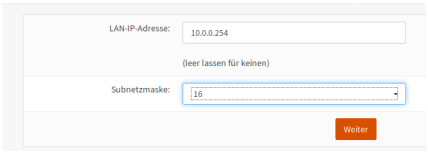
Falls Deine Firewall eine statische IP-Adresse hat, die nicht über DHCP erteilt wird, trägst Du sie hier ein.

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 runtergescrollt hast.

Mit `Weiter` übernimmst Du die von Dir gemachten Einstellungen



System: Assistent: Konfiguriere LAN-Schnittstelle



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

System: Assistent: Setze Root-Passwort

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!

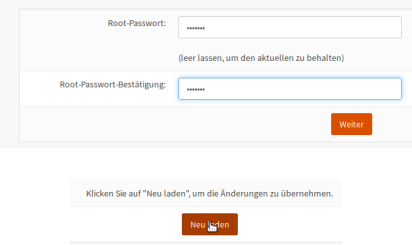
System: Assistent: Konfiguration neu laden

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.

Sollte das bei Dir der Fall sein, musst Du Deinem Admin PC die passende IP-Adresse 10.0.0.10/16, DNS: 10.0.0.254und 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.

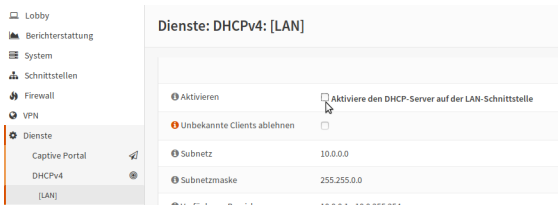
Gehe auf `Dienste -> DHCPv4 -> [LAN]` und lösche den Haken bei `Aktivieren`, wenn gesetzt. `Speichern` lässt Dich Deine Einstellungen unten auf der Seite.

Zusätzliche Netzwerkkarte hinzufügen (Optional)

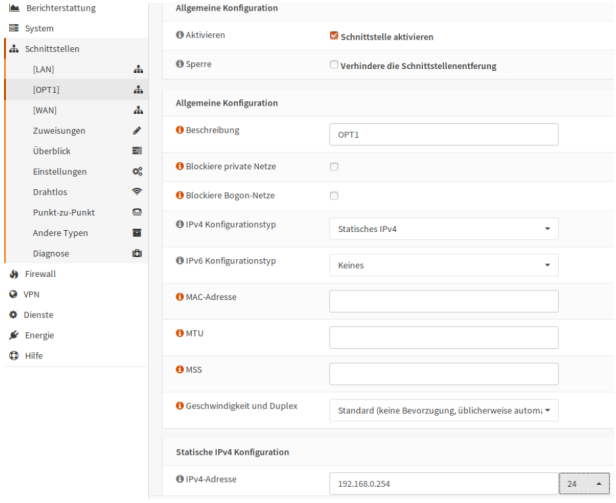
Die linuxmuster.net v7 läuft bereits mit zwei Netzwerkkarten. Möchtest Du allerdings ein WLAN oder in einer DMZ einen Webserver betreiben, brauchst Du noch weitere Netzwerkkarten.

Wie das geht, siehst Du im Folgenden:

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.


Lobby
Berichterstattung
System
Schnittstellen
Firewall
VPN
Dienste
Captive Portal
DHCPv4
[LAN]
Dienste: DHCPv4: [LAN]
Aktivieren
Aktiviere den DHCP-Server auf der LAN-Schnittstelle
Unbekannte Clients ablehnen
Subnetz
10.0.0.0
Subnetzmaske
255.255.0.0


Lobby
Berichterstattung
System
Schnittstellen
[LAN]
[WAN]
Zuweisungen
Überblick
Einstellungen
Drahtlos
Punkt-zu-Punkt
Schnittstellen: Zuweisungen
Schnittstelle
Netzwerkport
LAN
vtnet0 (12:fc:10:55:de:f6)
WAN
vtnet1 (f2:94:3a:06:fc:fd)
Neue Schnittstelle:
vtnet2 (c2:6b:ef:49:71:dd)
Hinzufügen
Speichern

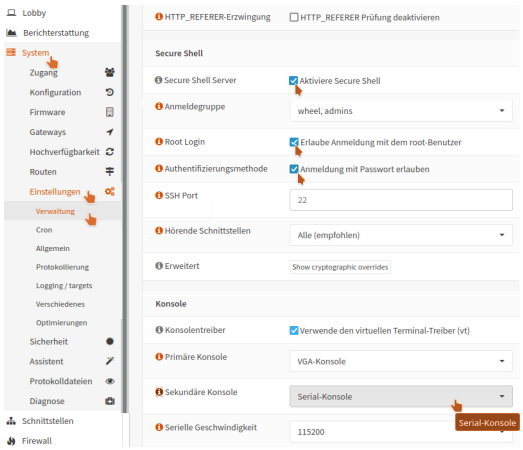

Berichterstattung
System
Schnittstellen
[LAN]
[OPT1]
[WAN]
Zuweisungen
Überblick
Einstellungen
Drahtlos
Punkt-zu-Punkt
Andere Typen
Diagnose
Firewall
VPN
Dienste
Energie
Hilfe
Allgemeine Konfiguration
Aktivieren
Schnittstelle aktivieren
Sperre
Verhindere die Schnittstellenentferung
Allgemeine Konfiguration
Beschreibung
OPT1
Blockiere private Netze
Blockiere Bogon-Netze
IPv4 Konfigurationstyp
Statisches IPv4
IPv6 Konfigurationstyp
Keines
MAC-Adresse
MTU
MSS
Geschwindigkeit und Duplex
Statische IPv4 Konfiguration
IPv4-Adresse
192.168.0.254
24

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

---

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`.



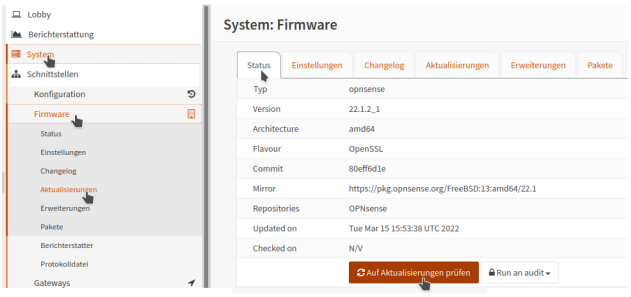
Setze jeweils den Haken bei `Aktiviere Secure Shell`, `Erlaube Anmeldung mit dem root-Benutzer` und `Anmeldung mit Passwort erlauben`.

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

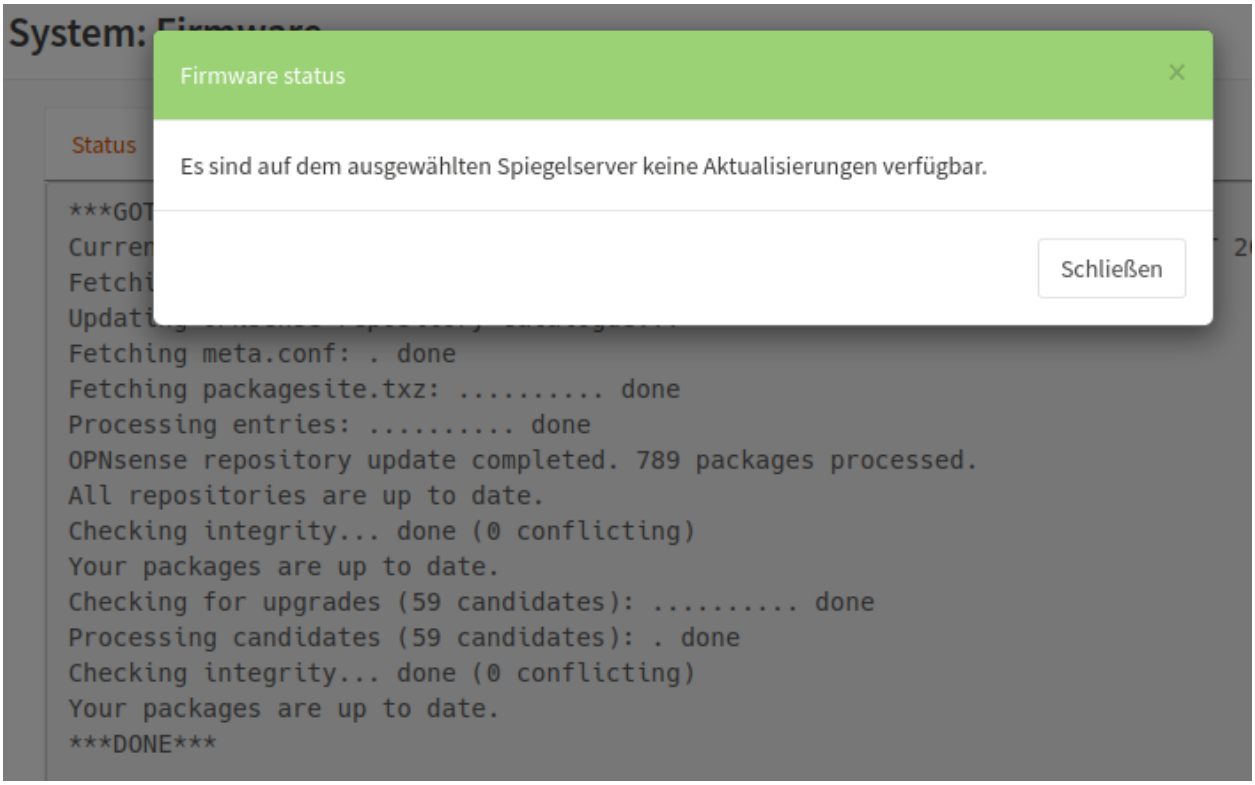
Diese Einstellungen wieder `Speichern`.

Update der OPNsense®

Aktualisiere nun die OPNsense®, indem Du unter



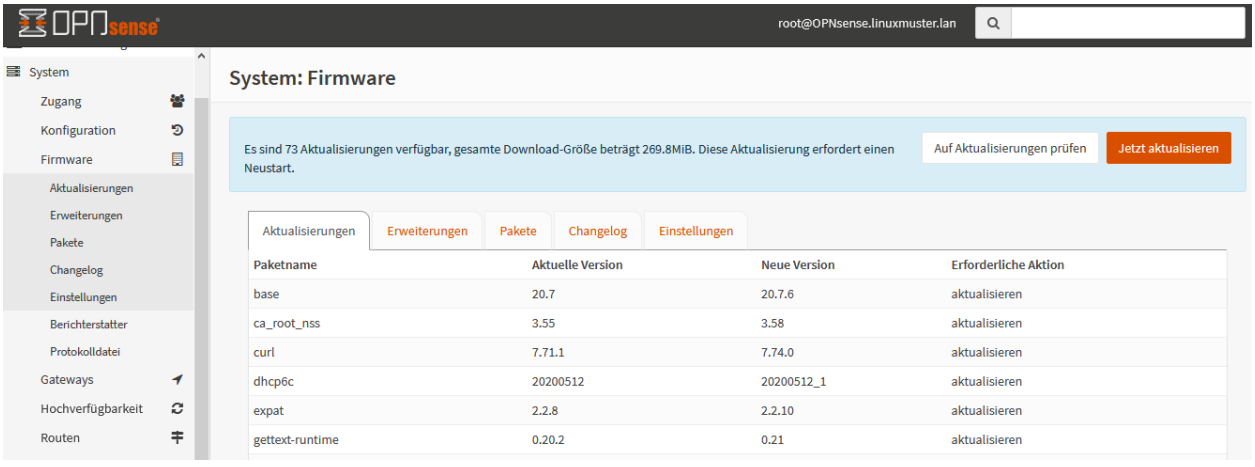
`System -> Firmware --> Aktualisierungen ---> Status ----> `` ``Auf Aktualisierungen prüfen` klickst.



Wenn keine Aktualisierungen verfügbar sind, erhältst Du folgende Meldung …

… und kannst zum abschließenden Schritt *Logout* gehen.

Sollten Dir wie in nachstehender Abbildung unter dem Reiter `Aktualisierungen` zu aktualisierenden Pakete angezeigt werden …



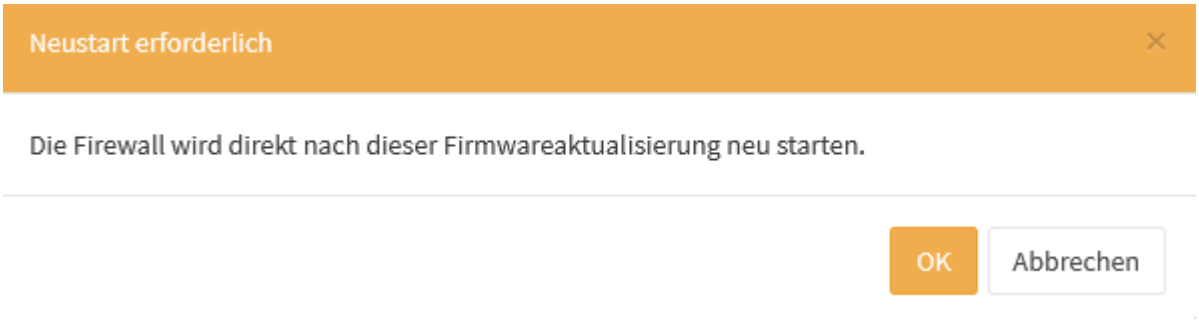
Hinweis: Falls Du nicht ins Internet kommst, kann es an der Gateway-Einstellung liegen. Gehe auf `System` –> `Gateways` –> `Einzeln` und editiere Dein Gateway (WANGW).

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.

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

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



Danach werden die Aktualisierungen heruntergeladen und angewendet.

Zum Abschluss erfolgt der Neustart automatisch.

Nach dem Neustart ist die OPNsense® soweit vorbereitet.

Logout

4.6.2 Anlegen und Installieren des Servers

Autor des Abschnitts: @rettich, @cweikl @MachtDochNiX

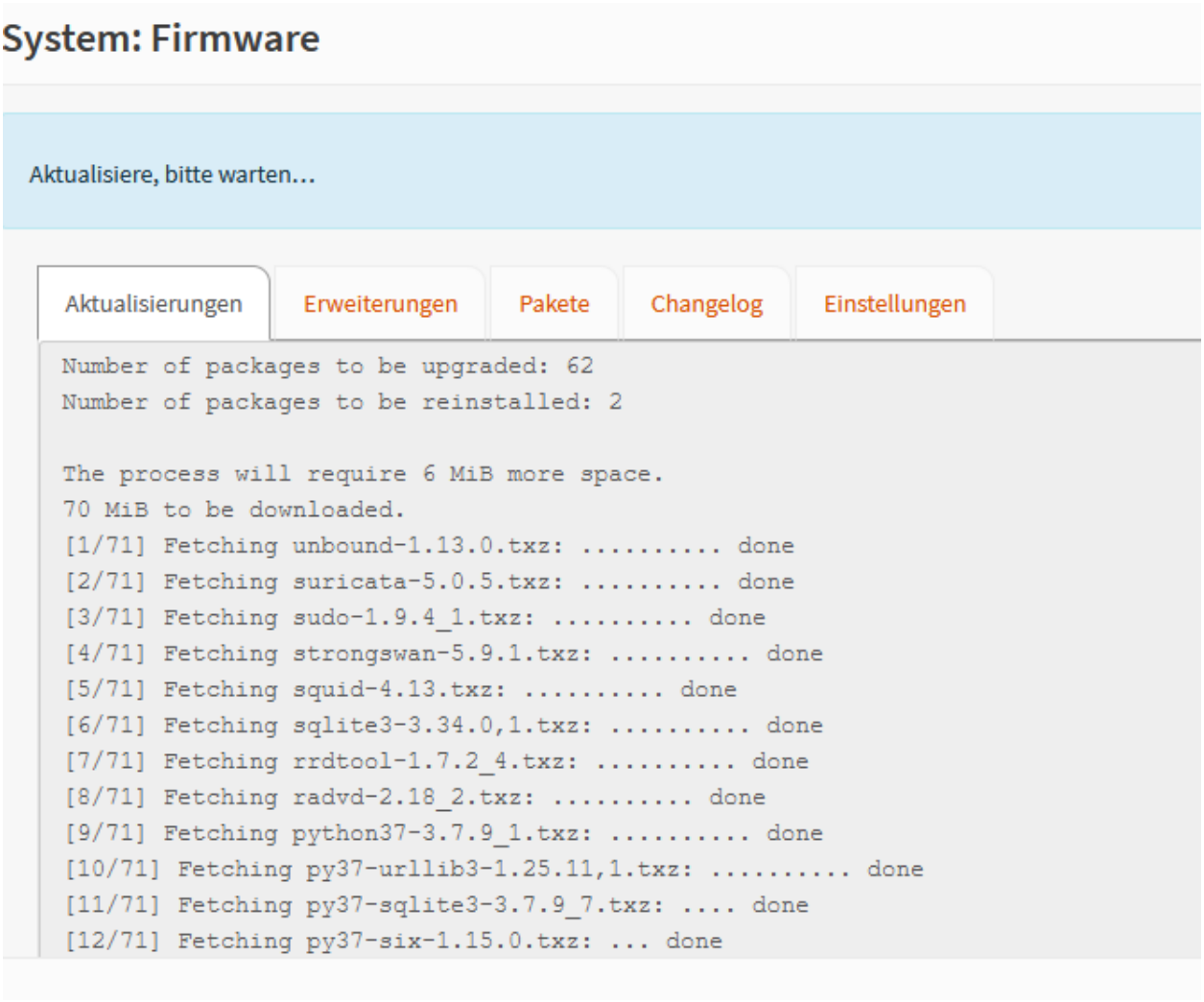
Bemerkung: Bist Du zuvor der Anleitung „Proxmox vorbereiten“ gefolgt, dann kannst Du fortfahren mit *Erster Start des Servers vom Installationsmedium*.

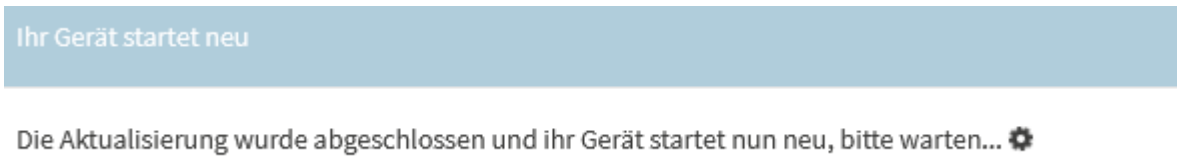
Hinweis: Willst Du in einer VM installieren, so must Du für die neue VM folgende Mindesteinstellungen angeben:

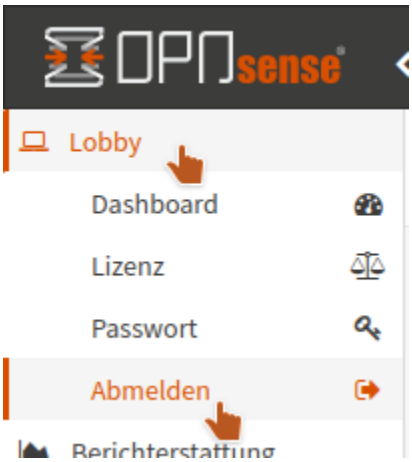
- Template - Ubuntu Bionic Beaver 18.04, installation from ISO library,
- Boot-Mode - BIOS Boot / MBR,
- 2 vCPU,
- 3 GiB RAM,
- storage -> hdd1: 25 GiB -> hdd2: 100 GiB,
- 1 NIC mit Zuordnung zu vSwitch green.

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 18.04 auf der ersten HDD installieren. Die zweite HDD bleibt frei. Auf dieser 2. HDD richtest Du - wie nachstehend beschrieben - ein LVM ein.


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

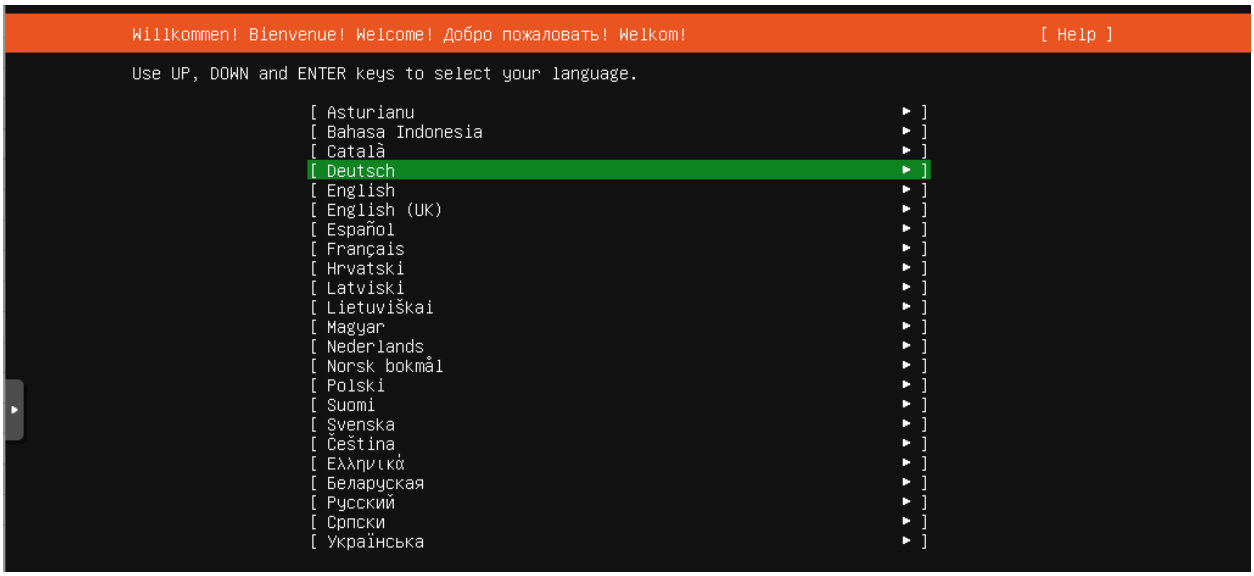

Ihr Gerät startet neu
Die Aktualisierung wurde abgeschlossen und ihr Gerät startet nun neu, bitte warten...


OPNsense
Lobby
Dashboard
Lizenz
Passwort
Abmelden

Erster Start des Servers vom Installationsmedium

Sprachauswahl

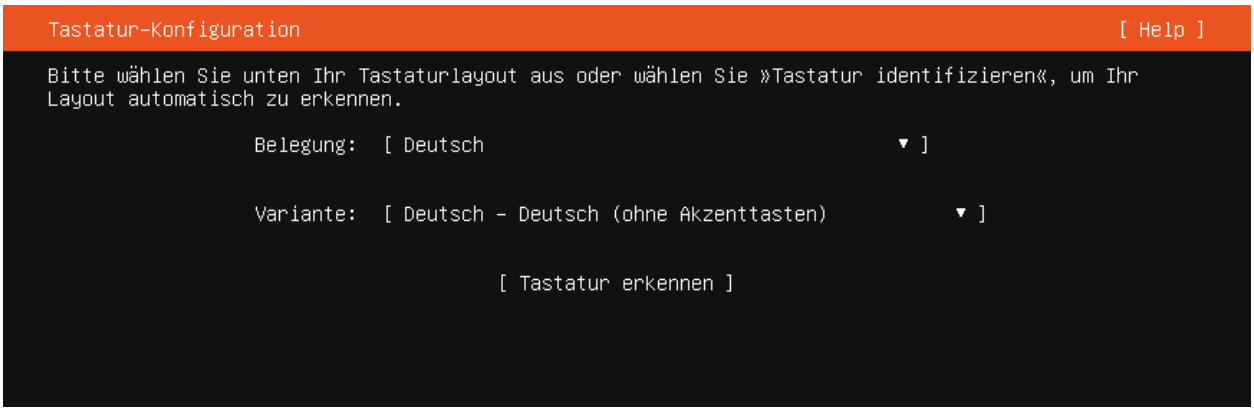
Starte den Server via Ubuntu 18.04 Server ISO-Image (USB-Stick oder CD-ROM). Es erscheint das erste Installationsfenster mit der Abfrage zur gewünschten Sprache.



Wähle Deine bevorzugte Sprache.

Tastaturlayout

Danach 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:

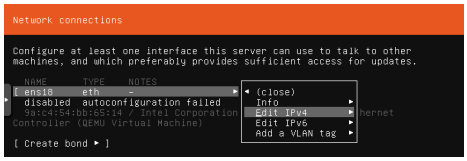
Wähle nacheinander

`Tastatur erkennen` –> `OK` –> `y` –> `Ja` –> `ö` –> `Nein` –> `OK`

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

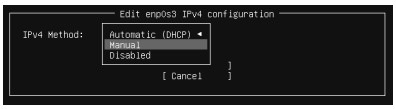
Netzwerk

Konfiguriere danach 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 von Hand einstellen.

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



Wähle `Manual` aus.

Gib die Netzwerkkonfiguration, wie im oberen Bild ein beziehungsweise …

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

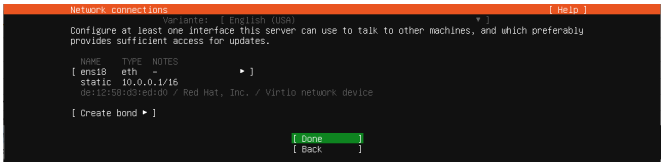
Achtung: Die Länge des ersten Teils der Domäne darf maximal 15 Zeichen betragen. Die Domäne „muster-gymnasium.de“ überschreitet diese Grenze um ein Zeichen, da „muster-gymnasium“ 16 Zeichen lang ist.

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

Mit `Èrledigt` geht es weiter.

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 `Ohne Akualisierung fortfahren`.

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

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

Speicher des Systems

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

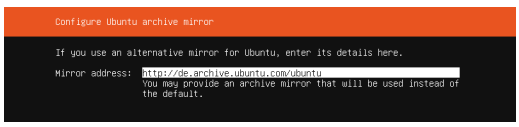
Es werden Dir dann die verfügbaren Geräte angezeigt.

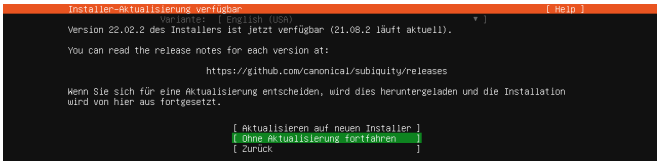
Wähle die erste Festplatte bzw. die erste Partition aus, auf der Du das System des Servers unterbringen möchtest. Es wird ein Kontextmenü angezeigt, bei dem Du mit `Add GPT Partition` diese erstellen musst.

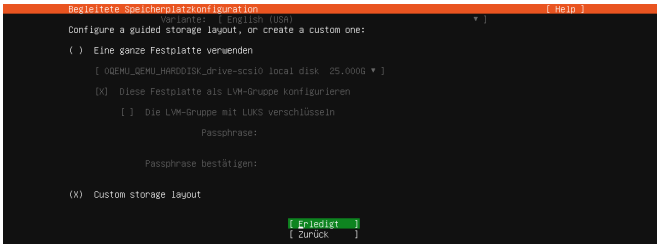
Wähle den gesamten Festplattenplatz (einfach das Eingabefeld leer lassen) und formatiere diesen mit dem ext4-Dateiformat und weise diese dem Mount Point `/` zu.

Gehe auf `Erstellen`.

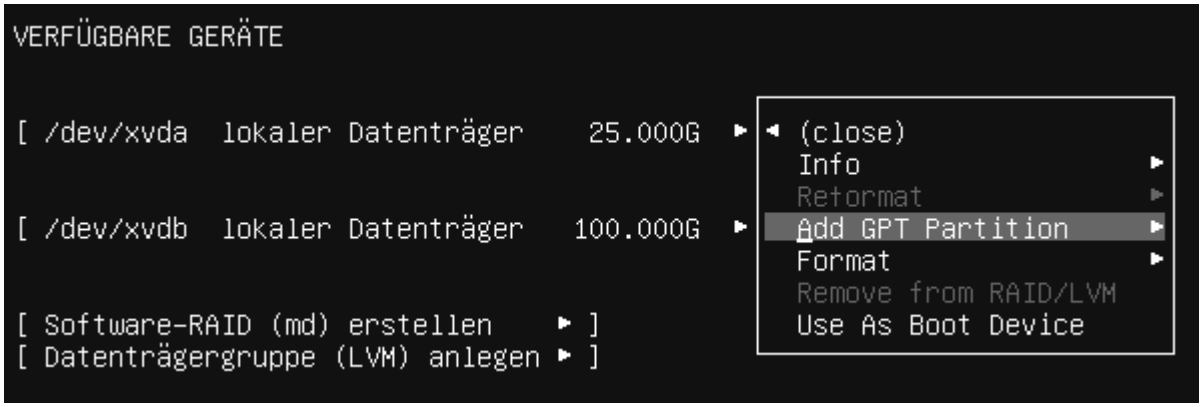
Danach gelangst Du zu nachstehendem Bildschirm.



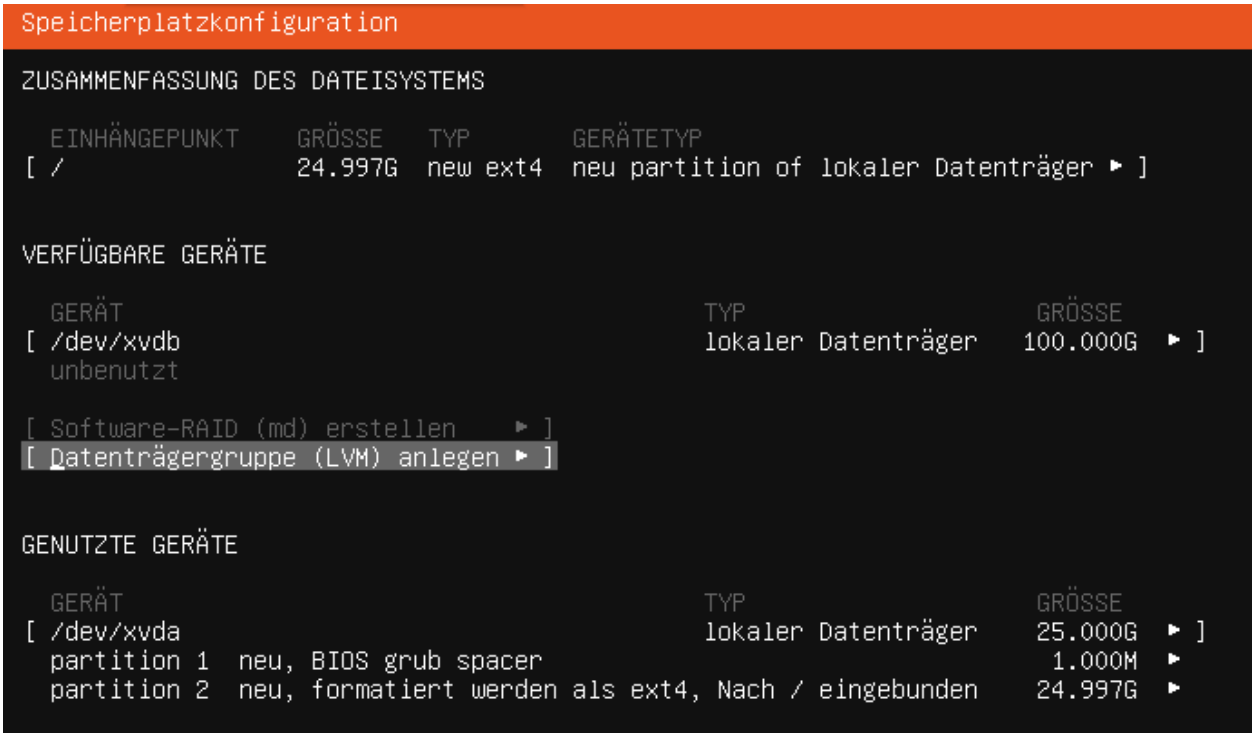

Installer-Aktualisierung verfügbar
[Help]
Variante: [English (USA)]
Version 22.02.2 des Installers ist jetzt verfügbar (21.08.2 läuft aktuell).
You can read the release notes for each version at:
https://github.com/canonical/subiquity/releases
Wenn Sie sich für eine Aktualisierung entscheiden, wird dies heruntergeladen und die Installation wird von hier aus fortgesetzt.
[Aktualisieren auf neuen Installer]
[Ohne Aktualisierung fortfahren]
[Zurück]


Begleitete Speicherplatzkonfiguration
[Help]
Variante: [English (USA)]
Configure a guided storage layout, or create a custom one:
( ) Eine ganze Festplatte verwenden
[QEMU_QEMU_HARDDISK_drive-scsi0 local disk 25.000G]
[X] Diese Festplatte als LVM-Gruppe konfigurieren
[ ] Die LVM-Gruppe mit LUKS verschlüsseln
Passphrase:
Passphrase bestätigen:
(X) Custom storage layout
[Erledigt]
[Zurück]


VERFÜGBARE GERÄTE
GERÄT TYP GRÖSSE
[/dev/xvda lokaler Datenträger 25.000G ▸]
unbenutzt
[/dev/xvdb lokaler Datenträger 100.000G ▸]
unbenutzt
[Software-RAID (md) erstellen ▸]
[Datenträgergruppe (LVM) anlegen ▸]
GENUTZTE GERÄTE
Keine genutzten Geräte


VERFÜGBARE GERÄTE
[/dev/xvda lokaler Datenträger 25.000G ▸
[/dev/xvdb lokaler Datenträger 100.000G ▸
[Software-RAID (md) erstellen ▸]
[Datenträgergruppe (LVM) anlegen ▸]
◂ (close)
Info ▸
Reformat ▸
Add GPT Partition ▸
Format ▸
Remove from RAID/LVM
Use As Boot Device


Adding GPT partition to /dev/xvda
Size (max 24.998G): 24.998G
Format: [ext4 ▾]
Mount: [/ ▾]
[Erstellen]
[Abbrechen]


Speicherplatzkonfiguration
ZUSAMMENFASSUNG DES DATEISYSTEMS
EINHÄNGEPUNKT GRÖSSE TYP GERÄTETYP
[/ 24.997G new ext4 neu partition of lokaler Datenträger ▸]
VERFÜGBARE GERÄTE
GERÄT TYP GRÖSSE
[/dev/xvdb lokaler Datenträger 100.000G ▸]
unbenutzt
[Software-RAID (md) erstellen ▸]
[Datenträgergruppe (LVM) anlegen ▸]
GENUTZTE GERÄTE
GERÄT TYP GRÖSSE
[/dev/xvda lokaler Datenträger 25.000G ▸]
partition 1 neu, BIOS grub spacer 1.000M ▸
partition 2 neu, formatiert werden als ext4, Nach / eingebunden 24.997G ▸

Speicherplatz für das Testsystem

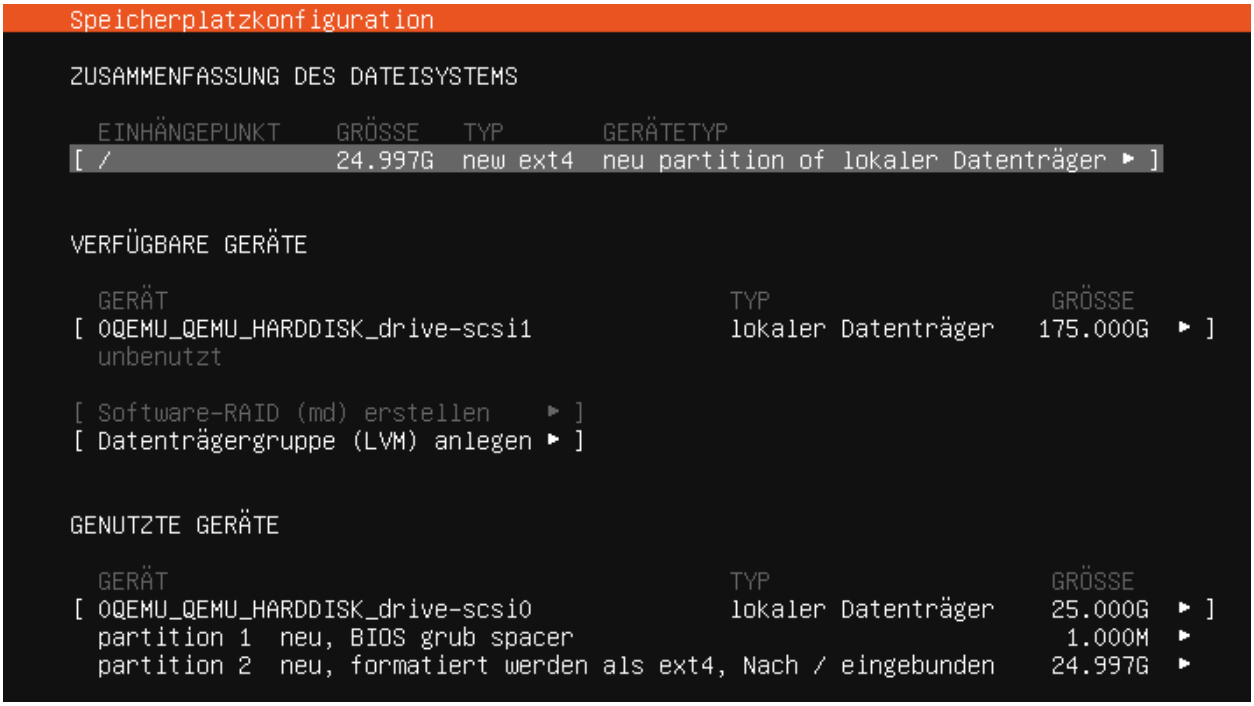
Für das Setup werden noch weitere Partitionen benötigt. Dafür haben wir uns für folgende Größenvorgabe entschieden.

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 linuxmuster-setup nimmt Dir die nötigen vorbereitenden Aktionen ab. Du läßt also das *zweite Speichermedium unkonfiguriert*.

Zum Abschluss werden Dir die Partitionsierungseinstellungen gemäß Deiner Eingaben angezeigt.



Wenn Du es für Deine Installation nutzen willst, dann kannst Du die nächsten Punkte überspringen und mit *Speicherplatzkonfiguration übernehmen* weitermachen.

[1] Sollte Deine Festplatte größer sein als die vorgeschlagene Mindestgröße so wird für diese Partition der maximal übrige freie Platz mit verwendet.

Speicherplatz nach Deinen Vorgaben (optional)

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.

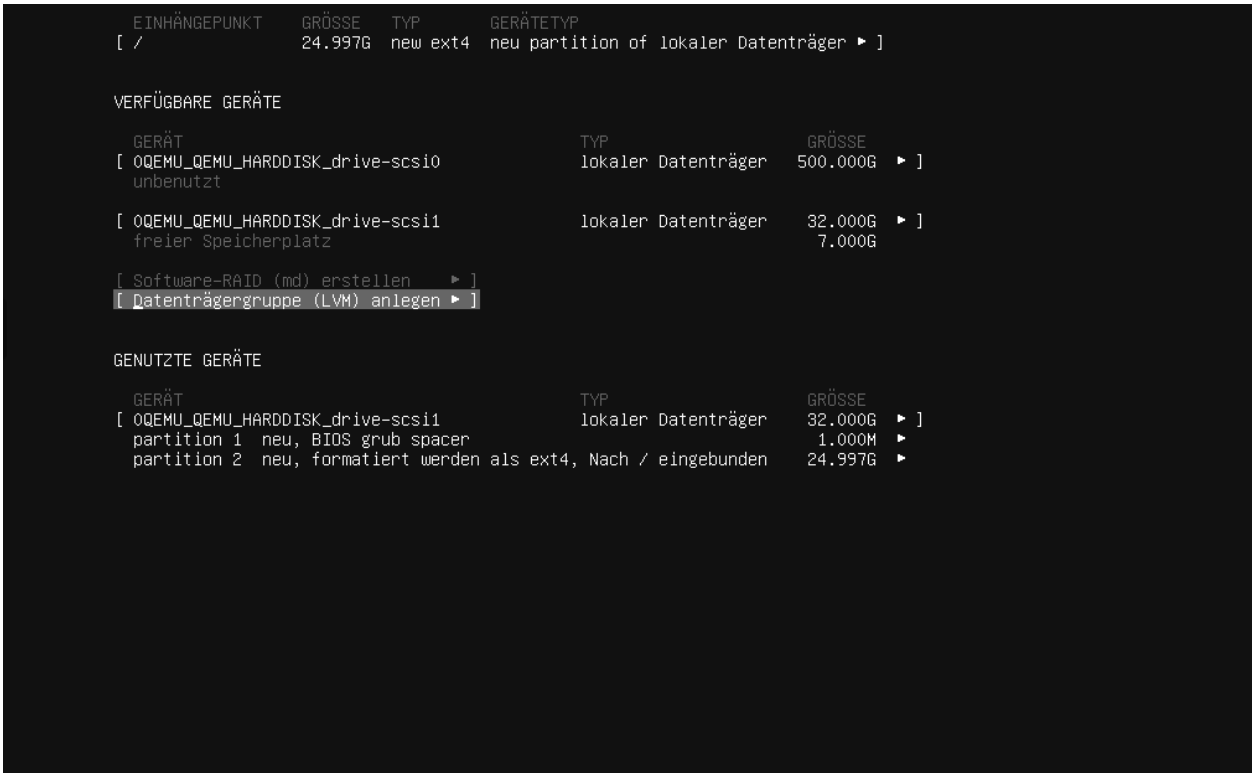
LV Name	LV Pfad	Mountpoint	Größe
var	/dev/sg_srv/var	/var	20G
linbo	/dev/sg_srv/linbo	/srv/linbo	80G
global	/dev/sg_srv/global	/srv/samba/global	20G
default-school	/dev/sg_srv/default-school	/srv/samba/schools/default-school	80G

Wir beschreiben hier exemplarisch das Vorgehen für die Größen aus der obigen Tabelle für die …

… *Einrichtung eines LVM auf der 2. HDD nach Deinen Vorgaben (optional)*

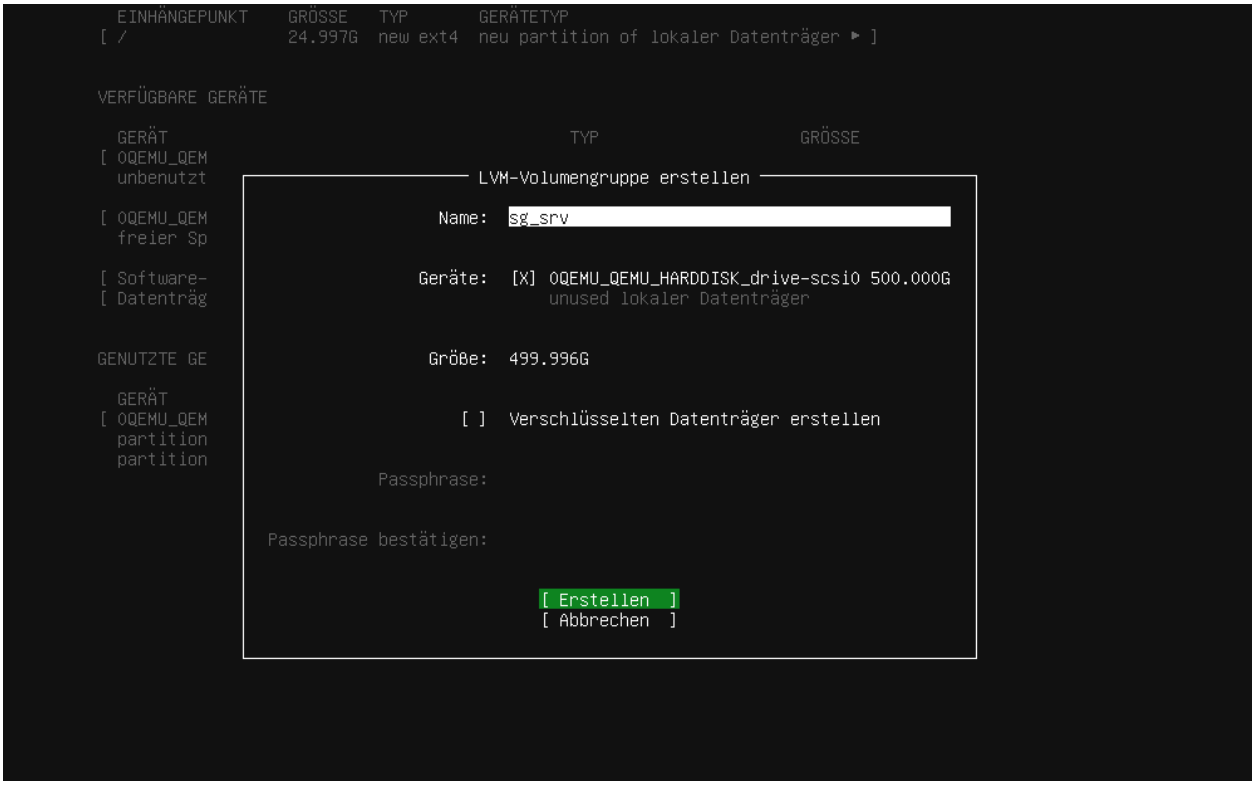
… *Einrichtung ohne LVM auf HDD nach Deinen Vorgaben (optional)*

Einrichtung eines LVM auf der 2. HDD nach Deinen Vorgaben (optional)



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.



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“.

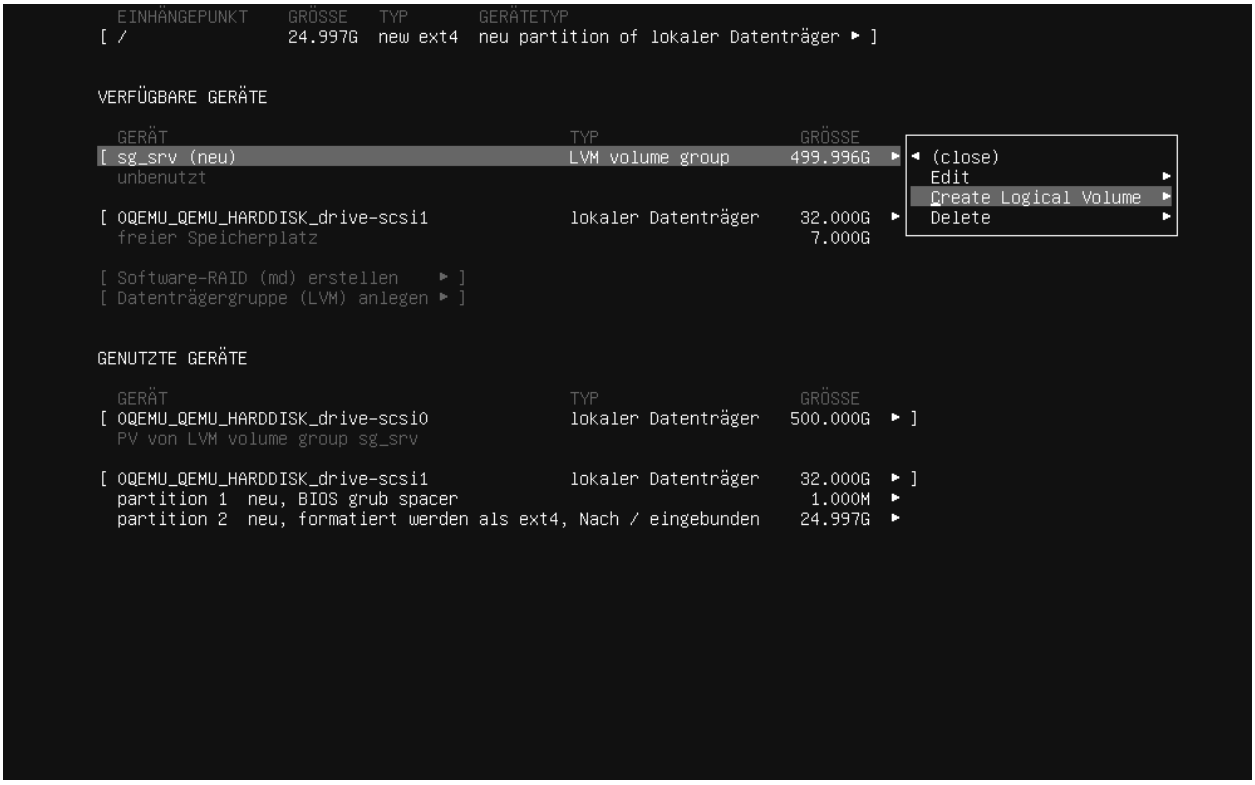
Wieder schließt Du diese Aktion mit `[Èrstellen]` ab.

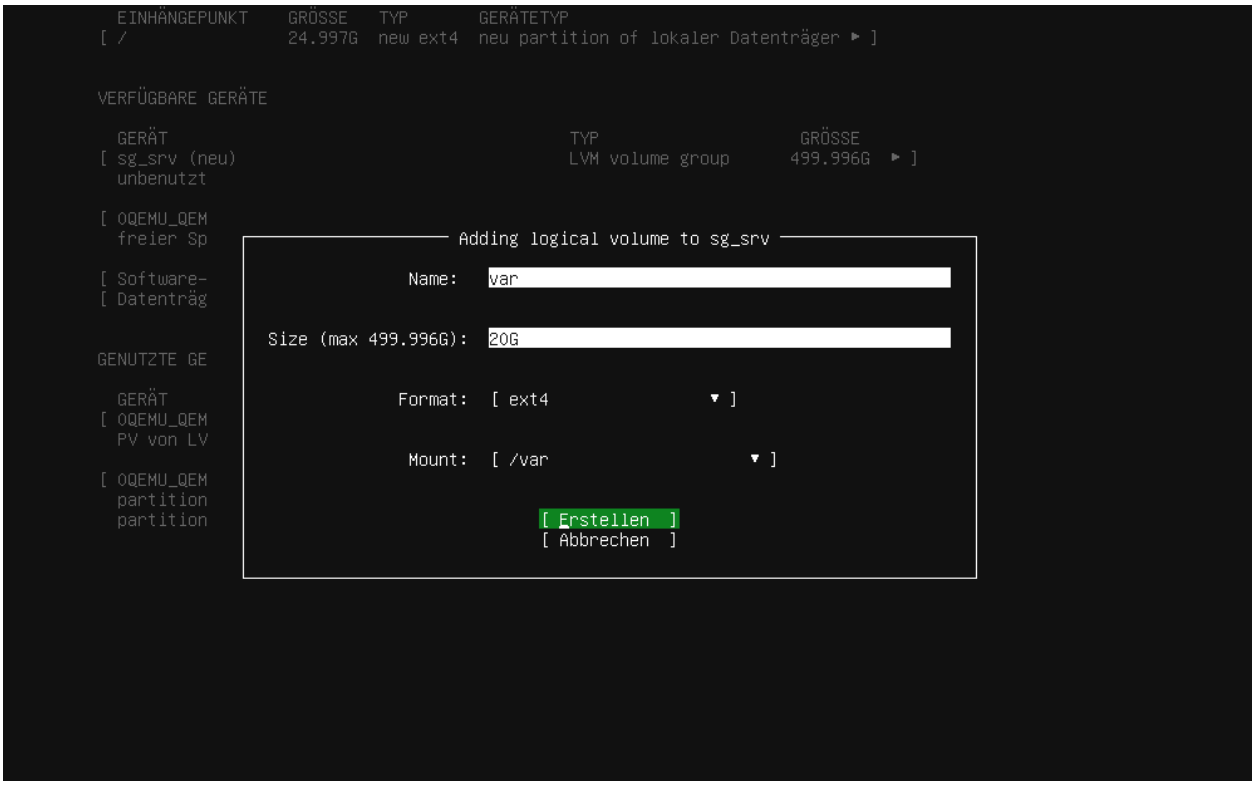
Die letzten zwei Schritte wiederholst Du für die anderen Positionen der Tabelle …

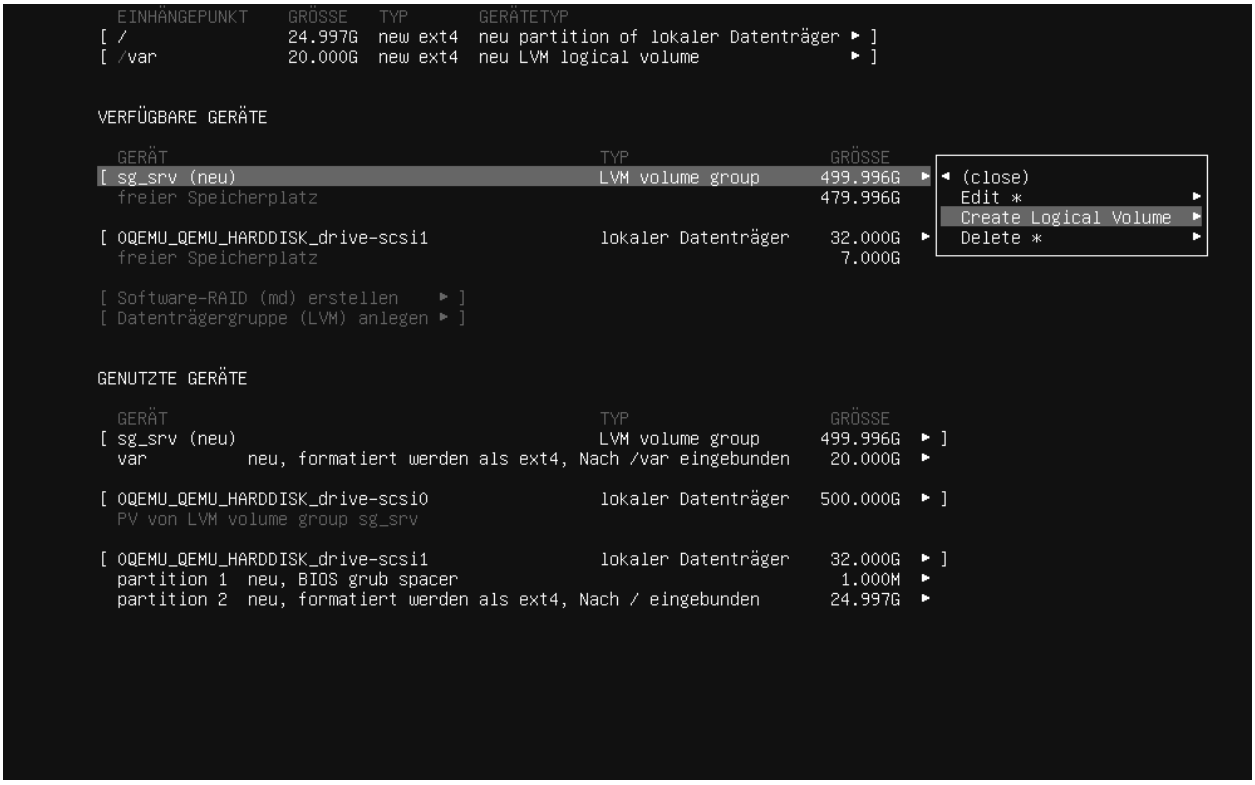
… linbo:

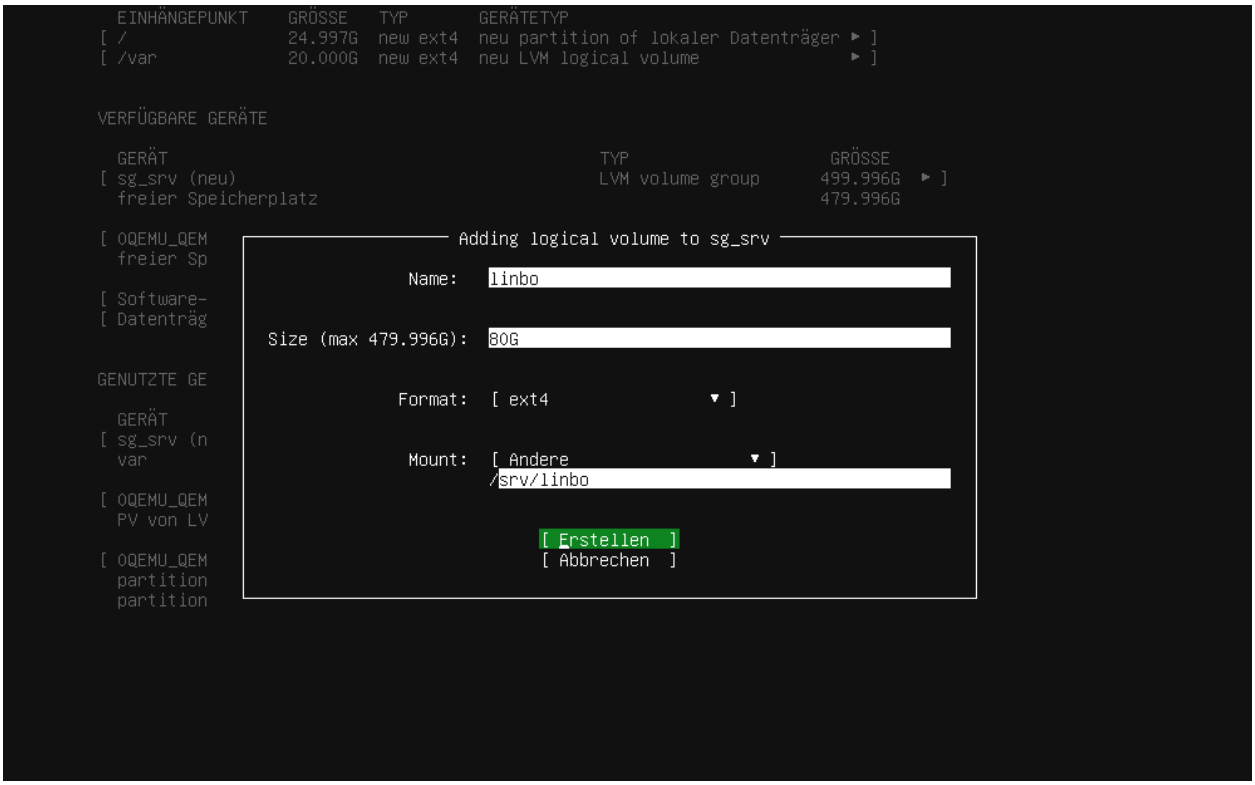
… global:

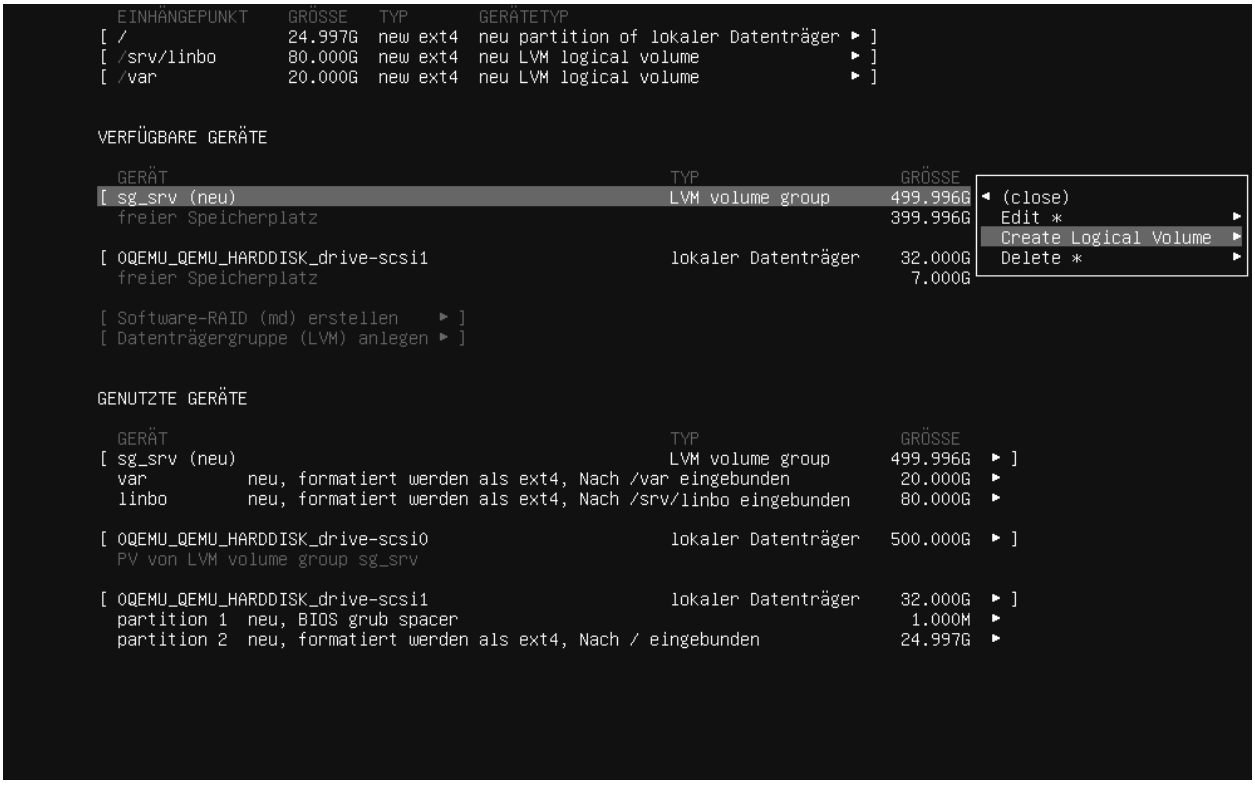
… default-school:

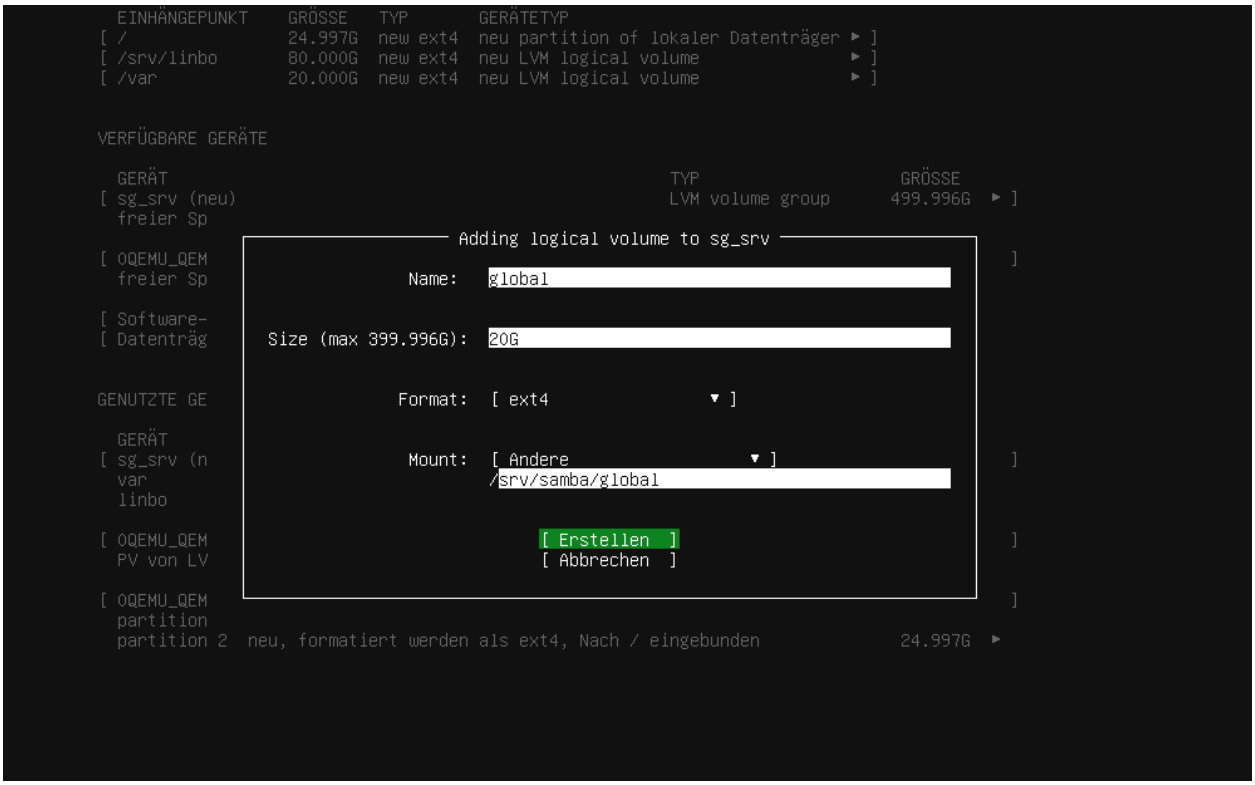

EINHÄNGEPUNKT GRÖSSE TYP GERÄTETYP
[/ 24.997G new ext4 neu partition of lokaler Datenträger ▸]
VERFÜGBARE GERÄTE
GERÄT TYP GRÖSSE
[sg_srv (neu) LVM volume group 499.996G ▸
unbenutzt
[OQEMU_QEMU_HARDDISK_drive-scsi1 lokaler Datenträger 32.000G ▸
freier Speicherplatz 7.000G
[Software-RAID (md) erstellen ▸]
[Datenträgergruppe (LVM) anlegen ▸]
GENUTZTE GERÄTE
GERÄT TYP GRÖSSE
[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 ▸
◂ (close)
Edit ▸
Create Logical Volume ▸
Delete ▸

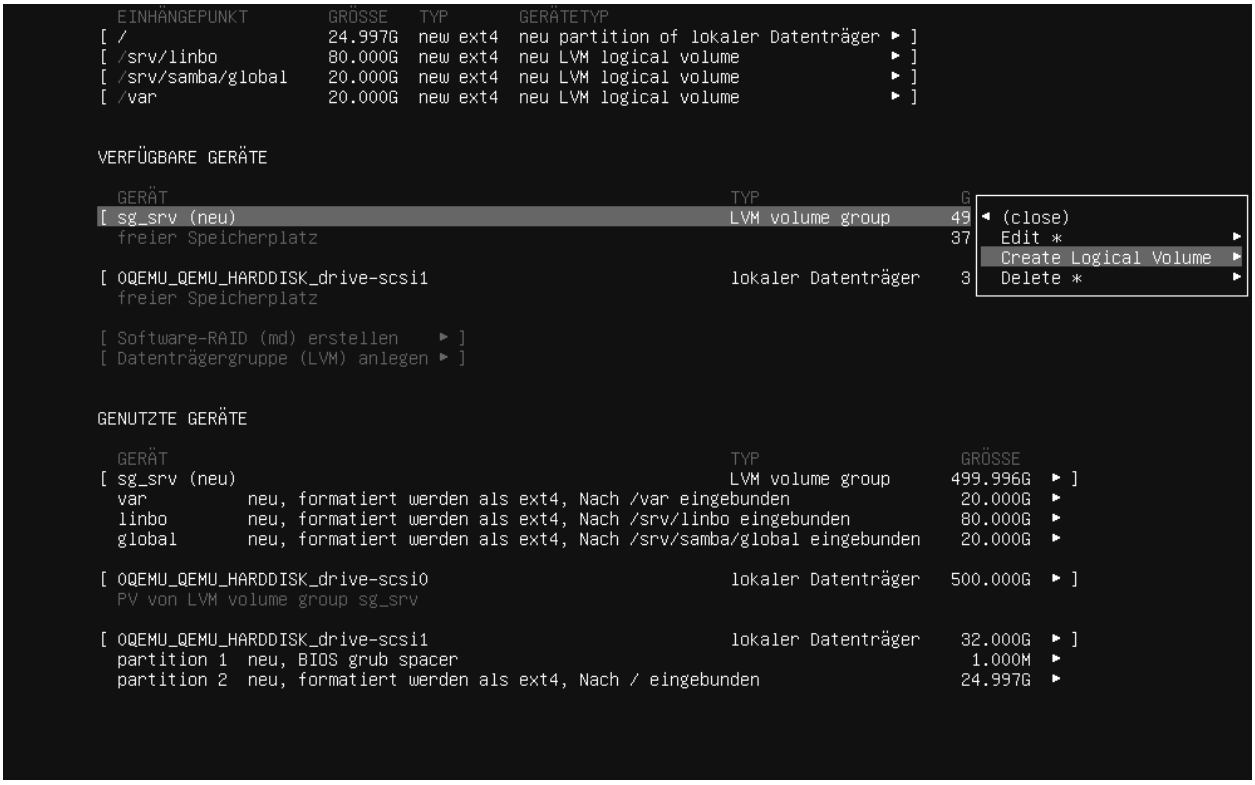

EINHÄNGEPUNKT GRÖSSE TYP GERÄTETYP
[/ 24.997G new ext4 neu partition of lokaler Datenträger ▸]
VERFÜGBARE GERÄTE
GERÄT TYP GRÖSSE
[sg_srv (neu) LVM volume group 499.996G ▸]
unbenutzt
Adding logical volume to sg_srv
Name: var
Size (max 499.996G): 20G
Format: [ext4 ▾]
Mount: [/var ▾]
[Erstellen]
[Abbrechen]

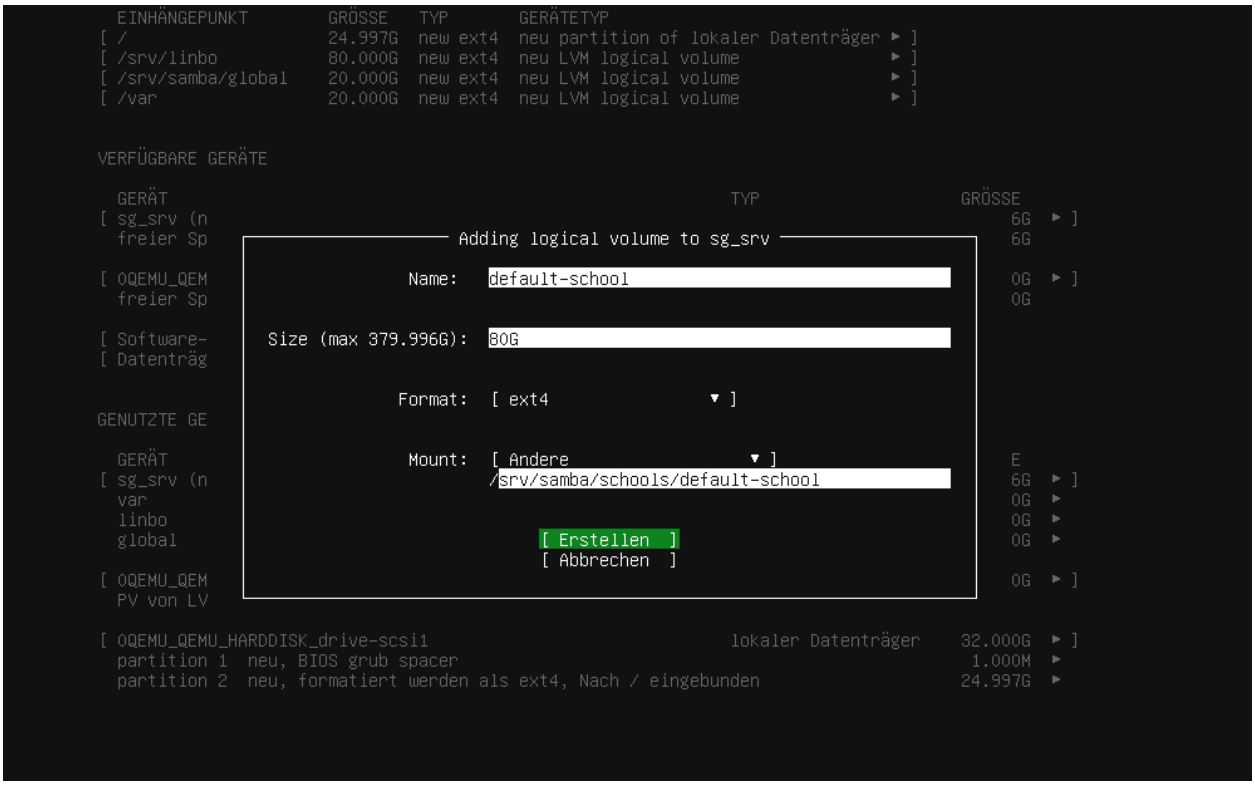

EINHÄNGEPUNKT GRÖSSE TYP GERÄTETYP
[/ 24.997G new ext4 neu partition of lokaler Datenträger ▸]
[/var 20.000G new ext4 neu LVM logical volume ▸]
VERFÜGBARE GERÄTE
GERÄT TYP GRÖSSE
[sg_srv (neu) LVM volume group 499.996G ▸
freier Speicherplatz 479.996G
[OQEMU_QEMU_HARDDISK_drive-scsi1 lokaler Datenträger 32.000G ▸
freier Speicherplatz 7.000G
[Software-RAID (md) erstellen ▸]
[Datenträgergruppe (LVM) anlegen ▸]
◂ (close)
Edit ∗ ▸
Create Logical Volume ▸
Delete ∗ ▸
GENUTZTE GERÄTE
GERÄT TYP GRÖSSE
[sg_srv (neu) LVM volume group 499.996G ▸]
var neu, formatiert werden als ext4, Nach /var eingebunden 20.000G ▸
[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 ▸

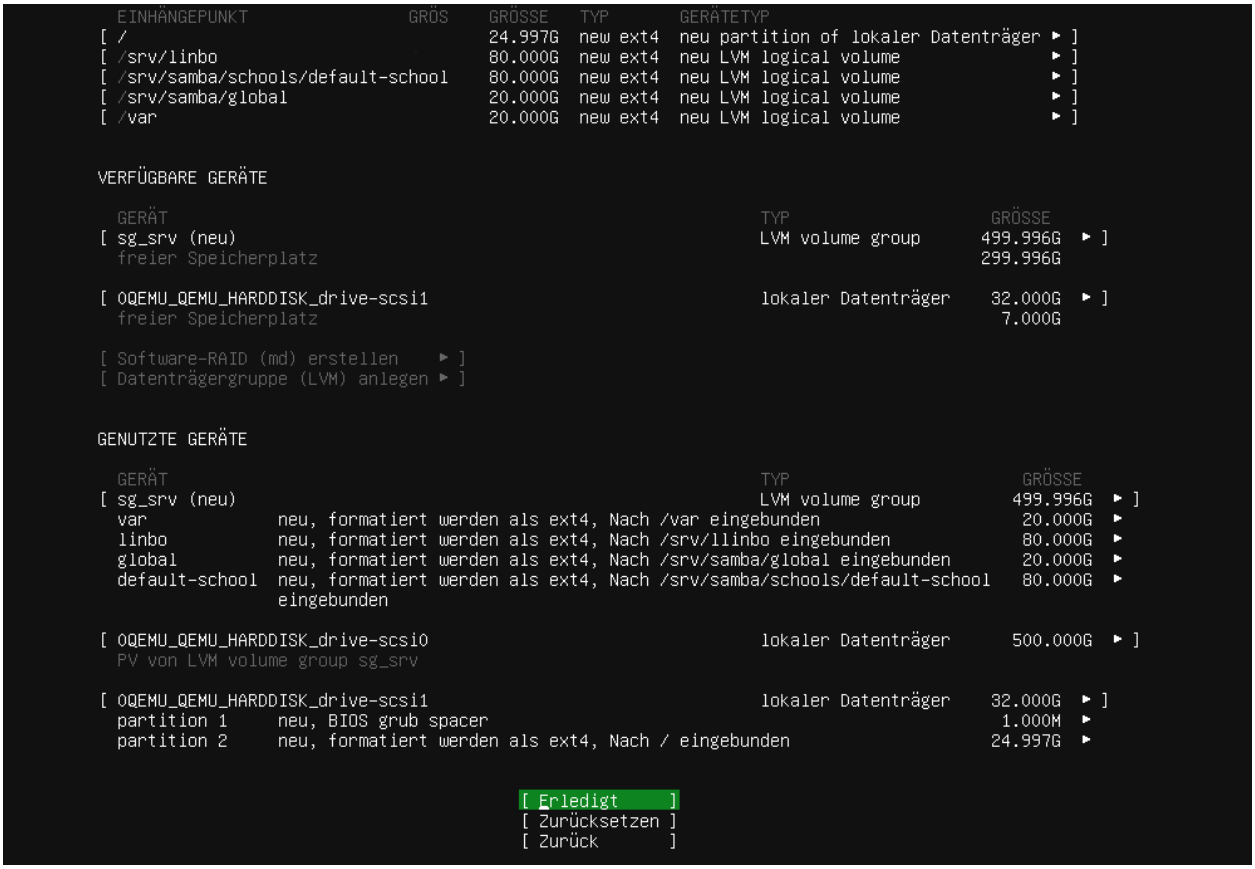

Adding logical volume to sg_srv
Name: linbo
Size (max 479.996G): 80G
Format: [ext4 ▾]
Mount: [Andere ▾]
/srv/linbo
[Erstellen]
[Abbrechen]


EINHÄNGEPUNKT GRÖSSE TYP GERÄTETYP
[/ 24.997G new ext4 neu partition of lokaler Datenträger ▸]
[/srv/linbo 80.000G 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 399.996G
[OQEMU_QEMU_HARDDISK_drive-scsi1 lokaler Datenträger 32.000G
freier Speicherplatz 7.000G
[Software-RAID (md) erstellen ▸]
[Datenträgergruppe (LVM) anlegen ▸]
◂ (close)
Edit ∗ ▸
Create Logical Volume ▸
Delete ∗ ▸
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 ▸
[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 ▸


EINHÄNGEPUNKT GRÖSSE TYP GERÄTETYP
[/ 24.997G new ext4 neu partition of lokaler Datenträger ▸]
[/srv/linbo 80.000G 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 ▸]
Adding logical volume to sg_srv
Name: global
Size (max 399.996G): 20G
Format: [ext4 ▾]
Mount: [Andere ▾]
/srv/samba/global
[Erstellen]
[Abbrechen]
partition 2 neu, formatiert werden als ext4, Nach / eingebunden 24.997G ▸


EINHÄNGEPUNKT GRÖSSE TYP GERÄTETYP
/ 24.997G new ext4 neu partition of lokaler Datenträger
/srv/linbo 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 G
sg_srv (neu) LVM volume group 49
freier Speicherplatz 37
OQEMU_QEMU_HARDDISK_drive-scsi1 lokaler Datenträger 3
freier Speicherplatz
Software-RAID (md) erstellen
Datenträgergruppe (LVM) anlegen
(close)
Edit *
Create Logical Volume
Delete *
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
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


EINHÄNGEPUNKT GRÖSSE TYP GERÄTETYP
/ 24.997G new ext4 neu partition of lokaler Datenträger
/srv/linbo 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
Adding logical volume to sg_srv
Name: default-school
Size (max 379.996G): 80G
Format: ext4
Mount: Andere
/srv/samba/schools/default-school
[Erstellen]
[Abbrechen]
GENUTZTE GERÄTE
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



Zum Abschluss werden Dir die Partitionsierungseinstellungen gemäß Deiner Eingaben angezeigt.

Wenn Du es für Deine Installation nutzen willst, dann kanst Du mit *Speicherplatzkonfiguration übernehmen* weitermachen.

Einrichtung ohne LVM auf HDD nach Deinen Vorgaben (optional)

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.

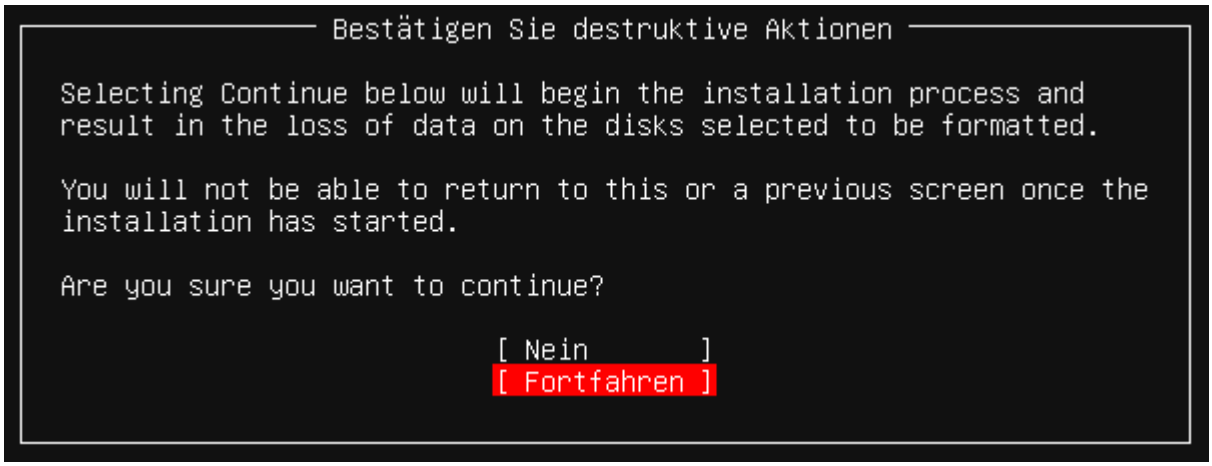
Auf eine detaillierte Beschreibung verzichten wir hier. Wir gehen davon aus, dass Du weißt, wie Du es umsetzen musst, wenn Du es so einrichten willst.

Die vorhergehende Beschreibung bietet Dir sicherlich genügende Hinweise, daher verlinken wir sie hier noch einmal für Dich. *Einrichtung eines LVM auf der 2. HDD nach Deinen Vorgaben (optional)*

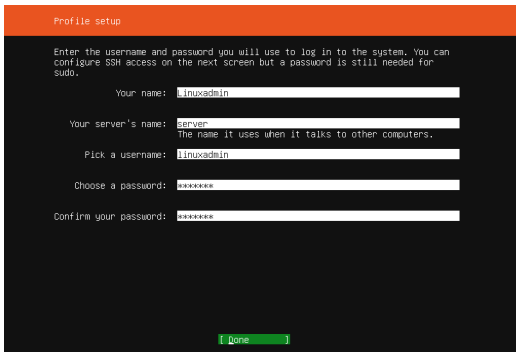
Speicherplatzkonfiguration übernehmen

Stimmen diese mit den gewünschten überein, so wähle `Erledigt` wie in dem zuletzt gesehen Bild aus.

Danach erhälst Du die Rückfrage, ob die Installation fortgesetzt werden soll und das die Daten auf der Festplatte dabei gelöscht werden.



Bestätige dies mit `Fortfahren`.



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

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

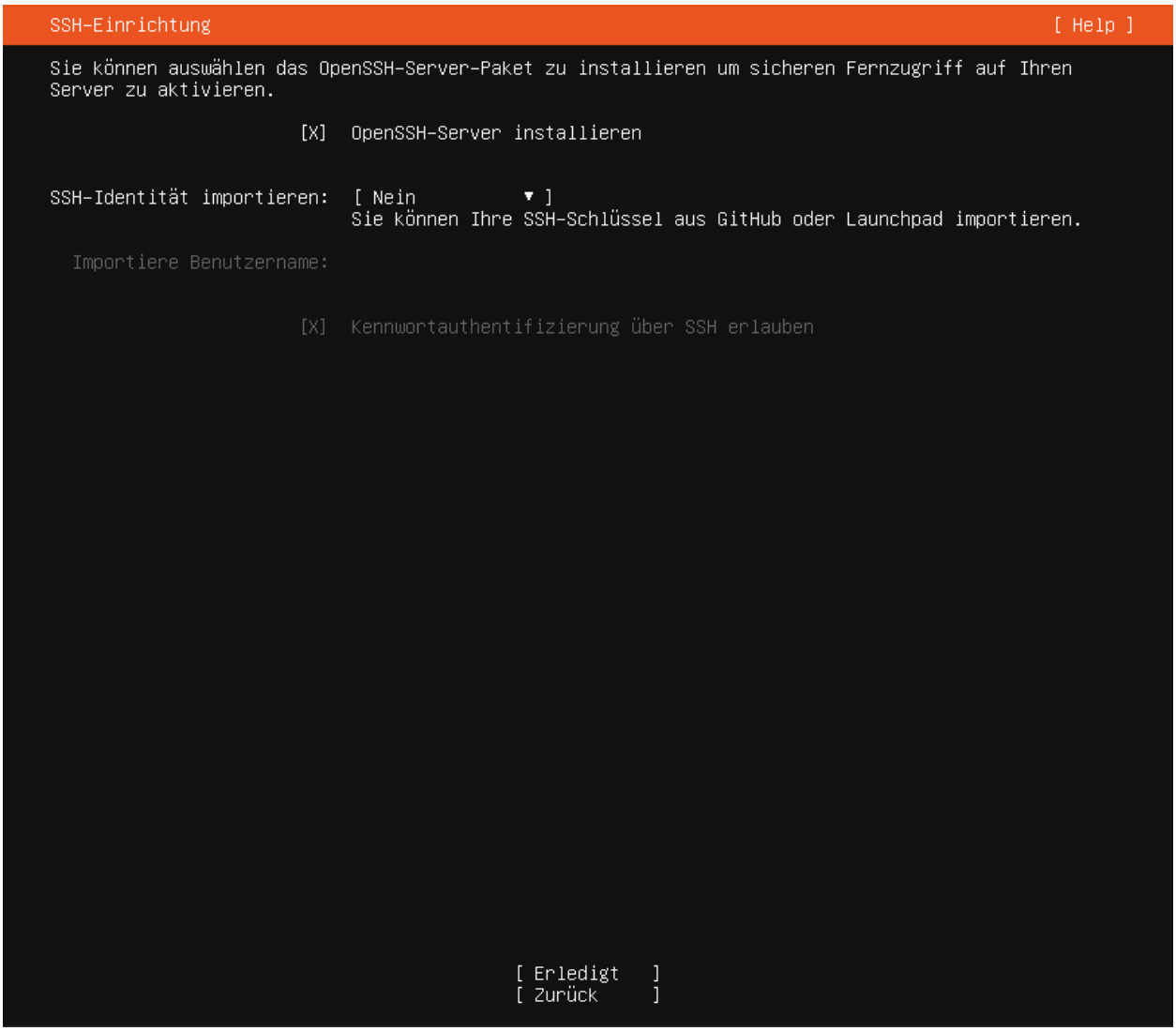
> **Achtung:** Wenn Du dies machst, mache Dir auch Gedanken wie Du diesen Zugang absichern kannst.
>
> Wir empfehlen das PublicKey-Verfahren. https://wiki.ubuntuusers.de/SSH/#Publickey-Authentifizierung (externer Link)

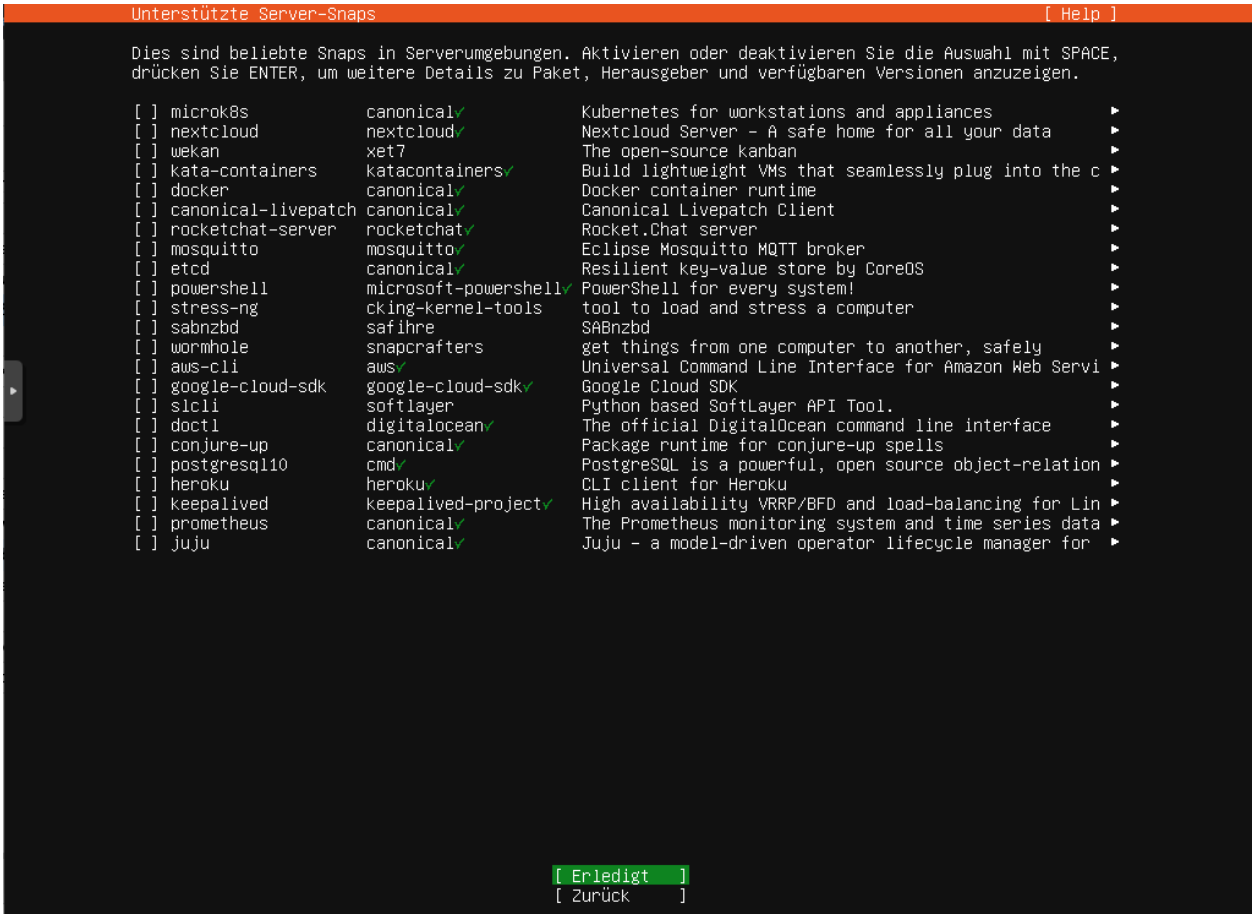
Installiere keine weiteren optionalen Pakete.

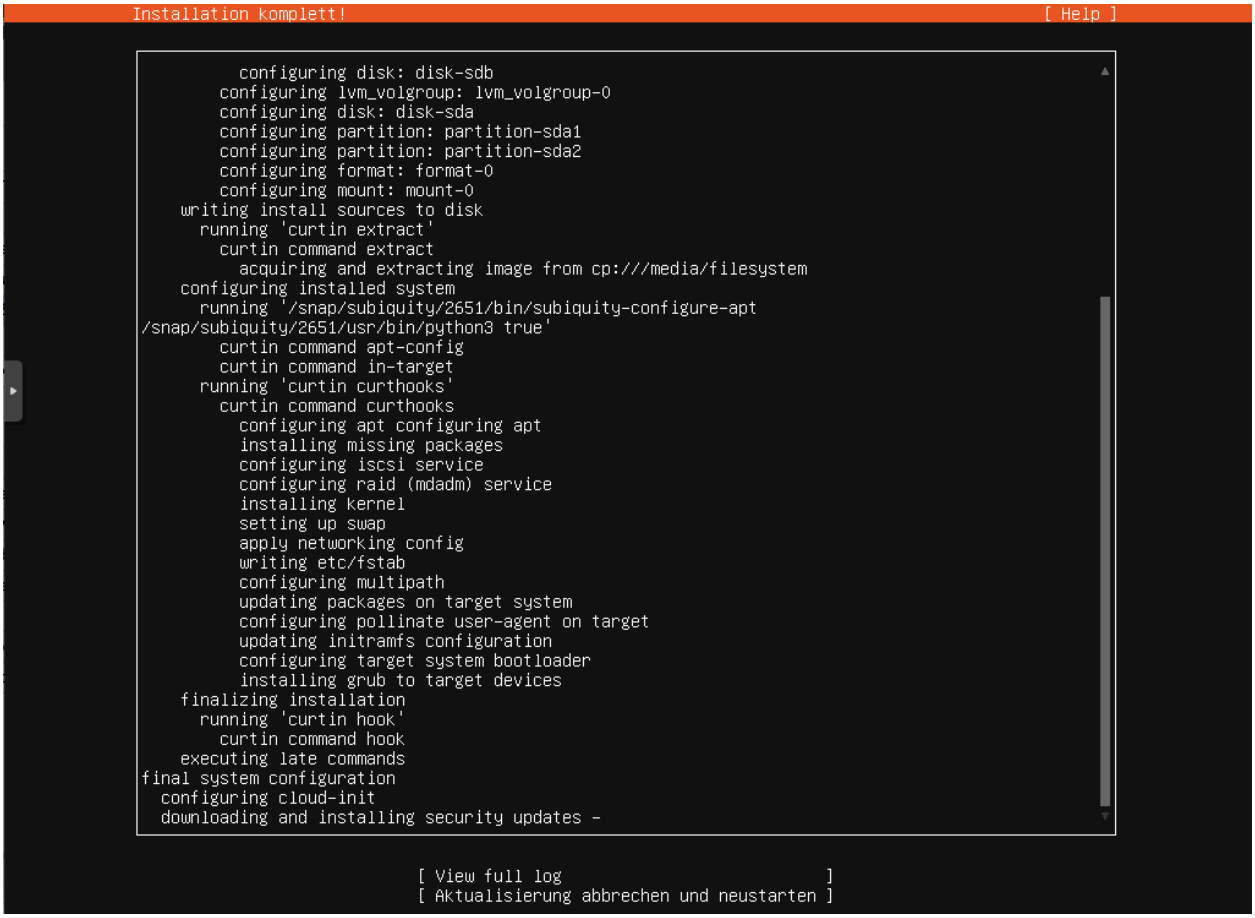
Bestätige den Start des Installationsvorganges mit `Erledigt`.

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

… und danach gilt es den Server neu zu starten.


SSH-Einrichtung
[Help]
Sie können auswählen das OpenSSH-Server-Paket zu installieren um sicheren Fernzugriff auf Ihren Server zu aktivieren.
[X] OpenSSH-Server installieren
SSH-Identität importieren: [Nein ▾]
Sie können Ihre SSH-Schlüssel aus GitHub oder Launchpad importieren.
Importiere Benutzername:
[X] Kennwortauthentifizierung über SSH erlauben
[Erledigt]
[Zurück]

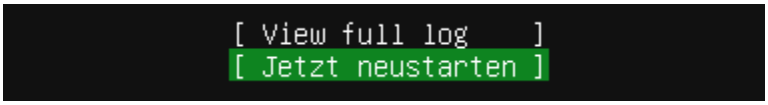

Unterstützte Server-Snaps
[Help]
Dies sind beliebte Snaps in Serverumgebungen. Aktivieren oder deaktivieren Sie die Auswahl mit SPACE,
drücken Sie ENTER, um weitere Details zu Paket, Herausgeber und verfügbaren Versionen anzuzeigen.
[ ] microk8s canonical✓ Kubernetes for workstations and appliances ▸
[ ] nextcloud nextcloud✓ Nextcloud Server - A safe home for all your data ▸
[ ] wekan xet7 The open-source kanban ▸
[ ] kata-containers katacontainers✓ Build lightweight VMs that seamlessly plug into the c ▸
[ ] docker canonical✓ Docker container runtime ▸
[ ] canonical-livepatch canonical✓ Canonical Livepatch Client ▸
[ ] rocketchat-server rocketchat✓ Rocket.Chat server ▸
[ ] mosquitto mosquitto✓ Eclipse Mosquitto MQTT broker ▸
[ ] etcd canonical✓ Resilient key-value store by CoreOS ▸
[ ] powershell microsoft-powershell✓ PowerShell for every system! ▸
[ ] stress-ng cking-kernel-tools tool to load and stress a computer ▸
[ ] sabnzbd safihre SABnzbd ▸
[ ] wormhole snapcrafters get things from one computer to another, safely ▸
[ ] aws-cli aws✓ Universal Command Line Interface for Amazon Web Servi ▸
[ ] google-cloud-sdk google-cloud-sdk✓ Google Cloud SDK ▸
[ ] slcli softlayer Python based SoftLayer API Tool. ▸
[ ] doctl digitalocean✓ The official DigitalOcean command line interface ▸
[ ] conjure-up canonical✓ Package runtime for conjure-up spells ▸
[ ] postgresql10 cmd✓ PostgreSQL is a powerful, open source object-relation ▸
[ ] heroku heroku✓ CLI client for Heroku ▸
[ ] keepalived keepalived-project✓ High availability VRRP/BFD and load-balancing for Lin ▸
[ ] prometheus canonical✓ The Prometheus monitoring system and time series data ▸
[ ] juju canonical✓ Juju - a model-driven operator lifecycle manager for ▸
[Erledigt]
[Zurück]


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]

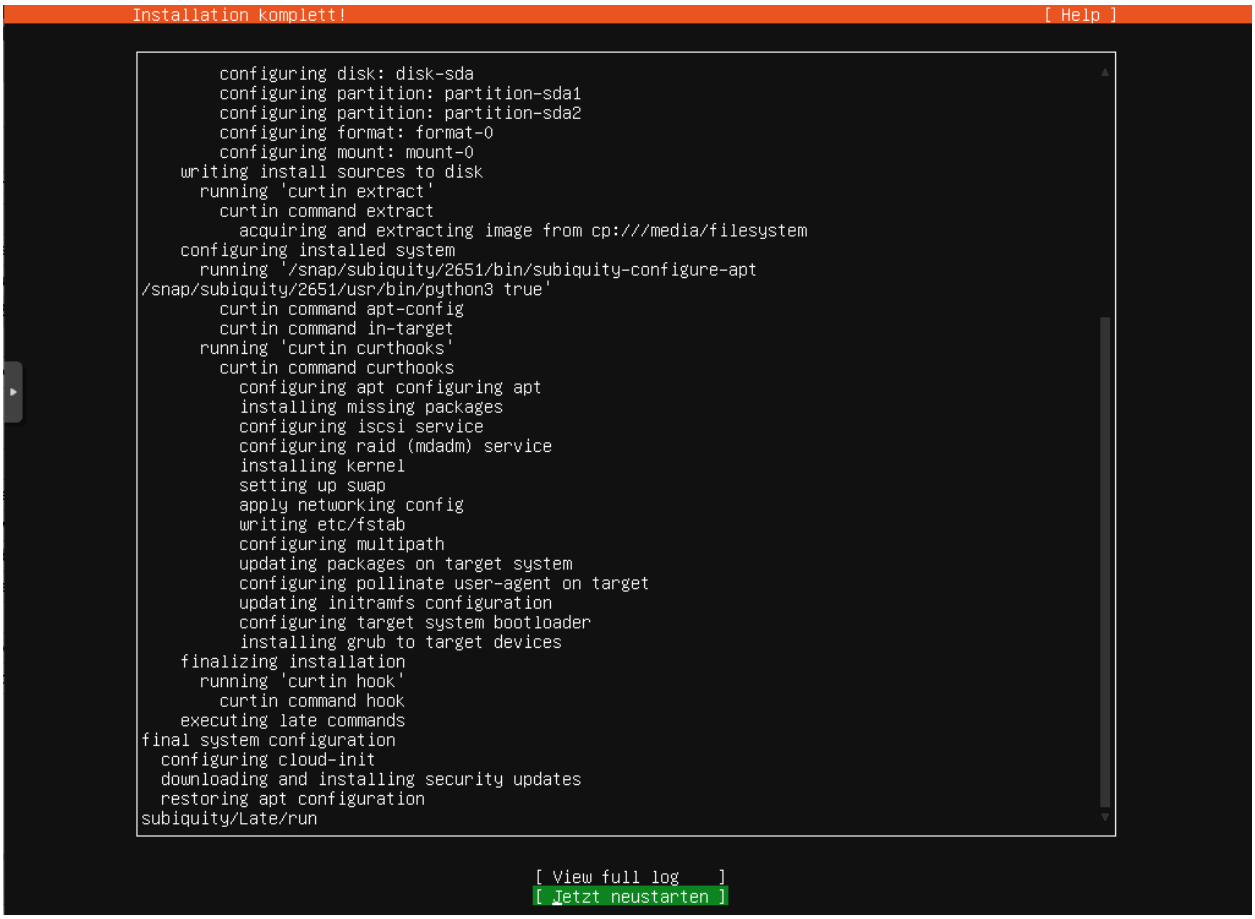
Hinweis: Bei einer VM achte vor dem Neustart darauf, dass Du die ISO-Datei / DVD ausgeworfen hast und die Boot-Reihenfolge so umgestellt hast, dass die VM direkt von HDD bootet.

Wann die Installation abgeschlossen ist, erkennst Du daran das die Anzeige am unteren Bildschirmrand von

auf



gewechselt ist.



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

Tipp: Folgendes Vorgehen bieten 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.

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

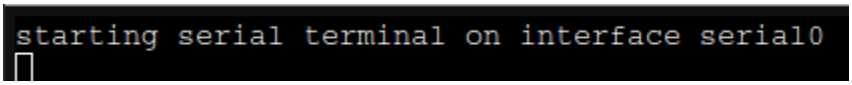
Nachdem Du Dich erneut als `linuxadmin` beziehungsweise mit dem von Dir angelegten Nutzer an der `noVNC` Konsole angemeldet hast, gib diese zwei Zeilen Code nacheinander ein:

```
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:



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.

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*

```
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
```

Bemerkung: Notiere Dir HDD- und Partition-Bezeichnungen für die spätere Verwendung.

Automatische Updates abschalten

Der frisch installierte Ubuntu-Server hat automatische Updates aktiviert. Das solltest Du abschalten, denn nur so kannst Du sichern 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 …

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

Ersetze bei `APT::Periodic::Unattended-Upgrade` die `"1";` durch `"0";`. Mit `<Strg>+o` und anschließendem `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`.

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 rufst 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
```

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 Vrtualisierungslösung empfehlen wir an dieser Stelle einen Snapshot zu erstellen!

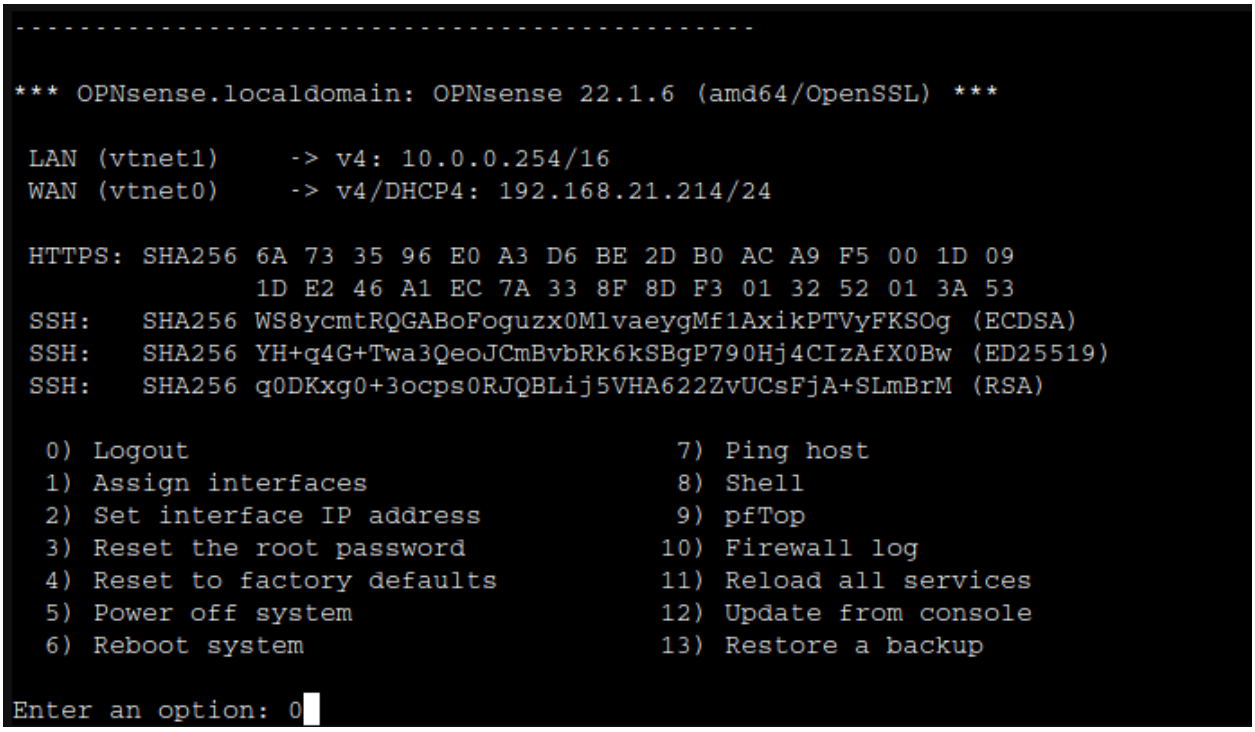
Weiter geht es jetzt mit *Server auf lmn7.1 vorbereiten*

4.6.3 Server auf lmn7.1 vorbereiten

Autor des Abschnitts: @rettich, @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.



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 korrkte 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
```

Das Skript lmn-prepare

Installation des Pakets `linuxmuster-prepare`

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

Führe danach folgende Befehle in der Eingabekonsole aus:

```
sudo wget -qO- "https://deb.linuxmuster.net/pub.gpg" | gpg --dearmour -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.

Die nächste Zeile fügt 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'
```

Aktualisiere die Softwareliste des Servers mittels

```
sudo apt update
```

Damit ist die Vorbereitung abgeschlossen und Du installierst das Paket „linuxmuster-prepare“.

```
sudo apt install linuxmuster-prepare
```

Nachdem Du den Befehl mit `J` bestätigt hast, wird das Skript lmn-prepare auf den Server geladen, welches …

- die benötigten Linuxmuster-Pakete und die benötigten anderen Pakete installiert,
- das Betriebssystem des Servers nochmals auf den aktuellen Stand bringt,
- das root-Passwort auf Muster! setzt,
- das Netzwerk konfiguriert und
- im Falle des Serverprofils das LVM eingerichtet.

Default-Locale setzen

Passe noch vor der Ausführung von lmn-prepare auf dem Server die `Default-Locale` an.

Erzeuge zuerst die Locales mit:

```
$sudo locale-gen
Generating locales (this might take a while)...
de_DE.UTF-8... done
en_GB.UTF-8... done
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
en_US.UTF-8... done
fr_FR.UTF-8... done
Generation complete.
```

Setze nun die Default-Locale. Diese muss unbedingt in o.g. Ausgabe enthalten sein!

```
$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, müssen Deine Einstellungen unbedingt vor dem Aufruf des Skriptes lmn-prepare eingearbeitet sein!

Anlegen und Installieren der Firewall

Anlegen und Installieren des Servers

Letzter Test vor Anwendung des Skriptes „lmn-prepare“

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:

Aufruf lmn-prepare

Wechsele Deinen Log-in und werde `root`:

```
sudo -i
```

Für die weitere Konfiguration nutzt Du unser lmn-prepare Script. Hilfe erhältst Du mittels

```
lmn-prepare -h
```

Hier ein Auszug mit den benötigten Optionen, die Du gleich anwenden wirst.

```
Usage: lmn-prepare [options]

[options] are:

-x, --force                : Force run on an already configured system.
-i, --initial              : Prepare the appliance initially for rollout.
-s, --setup                : Further appliance setup (network, swapsize).
                             on the profile).
|...|
-p, --profile=<profile>    : Host profile to apply, mandatory. Expected
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
                              values are "server" or "ubuntu".
-l, --pvdevice=<device>     : Initially sets up lvm on the given device (server
                              profile only). <device> can be a partition or an
                              entire disk.
-v, --volumes=<volumelist>  : List of lvm volumes to create (to be used together
                              with -l/--pvdevice). Syntax (size in GiB):
                              <name>:<size>,<name>:<size>,...
|...|
```

Installation mit Standard-Vorgaben

Hast Du eine zweite HDD mit 100GiB kannst Du lmn-prepare mit den Standard-Werten ausführen.

```
lmn-prepare -i -p server -l /dev/sdb -u
```

Mit dem Parameter `-u` 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-prepare -i -p server -l /dev/sdb -v var:50,linbo:500,global:50,default-school:100
↪%FREE
```

Für zusätzliche Informationen bitte https://github.com/linuxmuster/linuxmuster-prepare beachten.

Es wird hier also eine Erstinstallation (-i) mit dem Profil `server` auf der zweiten Festplatte (/dev/sdb) durchgeführt. Auf der zweiten Platte werden vier Volumes mit

- 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-prepare ohne Fehler durchgelaufen, führe nun noch folgenden Befehl aus:

```
pip3 install jinja2
```

Es erscheint ggf. der Hinweis, dass die Abhängigkeiten bereits erfüllt sind.

Starte danach den Server neu mit dem Befehl: `reboot`.

Danach steht dem *Setup v7.1* nichts mehr im Wege.

4.7 Setup v7.1

Autor des Abschnitts: @cweikl, @MachtDochNix

Achtung: Alle linuxmuster 6.x Systeme können statt einer Neuinstallation über eine *Migration auf linuxmuster 7.1* umgezogen werden, dennoch ist die Erstkonfiguration hier eine notwendige Voraussetzung.

Alle linuxmuster 7.0 Systeme werden lediglich über ein *Upgrade v7.0 auf v7.1* auf linuxmuster v7.1 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 authoritativ 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 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‘
  - hostname -> server01ad, subdomain -> linuxmuster, meineschule -> domain, tld -> de
- 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 Domane. 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 7.1 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 7.1 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

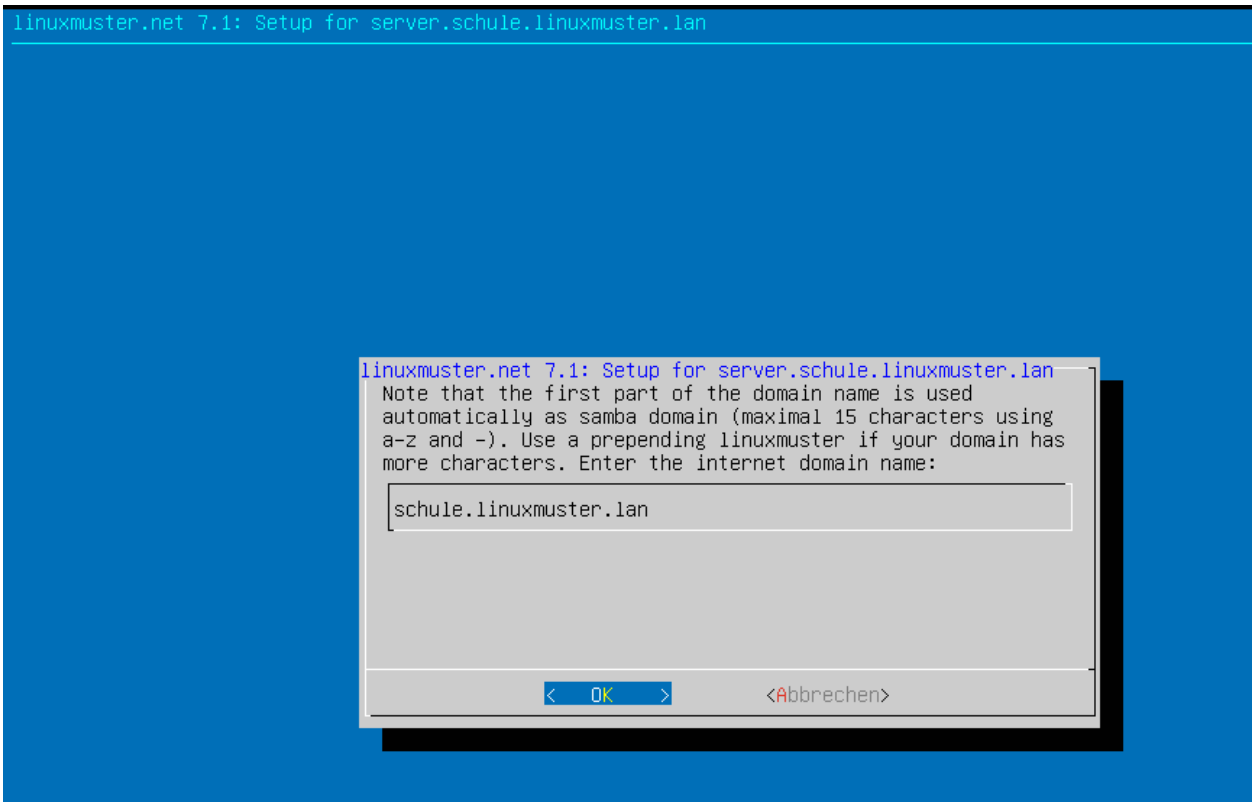


Abb. 2: Hier geht es zum *Setup im Terminal*

WEB UI

(formerly known as Schulkonsole)

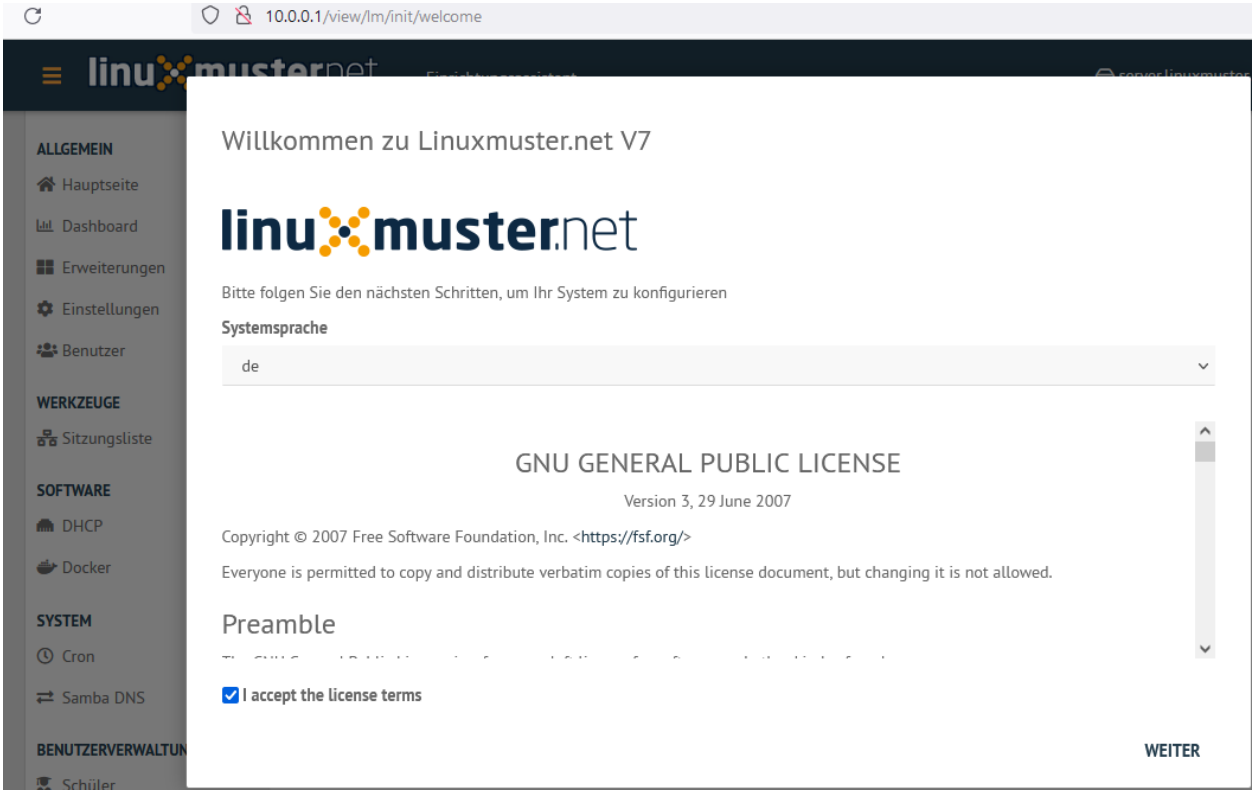


Abb. 3: Hier geht es zum *Setup via Schulkonsole*

4.8 Setup via Schulkonsole

Autor des Abschnitts: @cweikl, @MachtDochNix

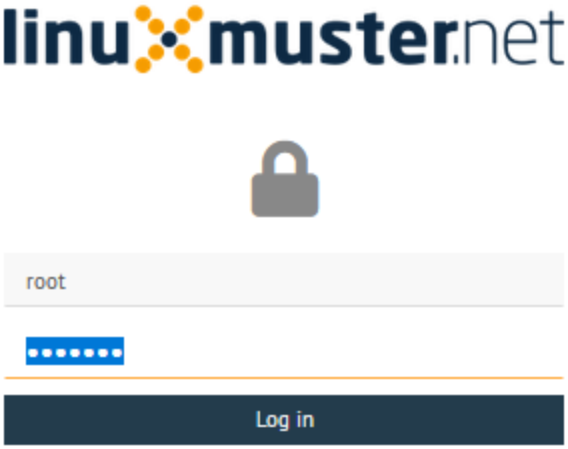
4.8.1 Setup über die Schulkonsole

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.

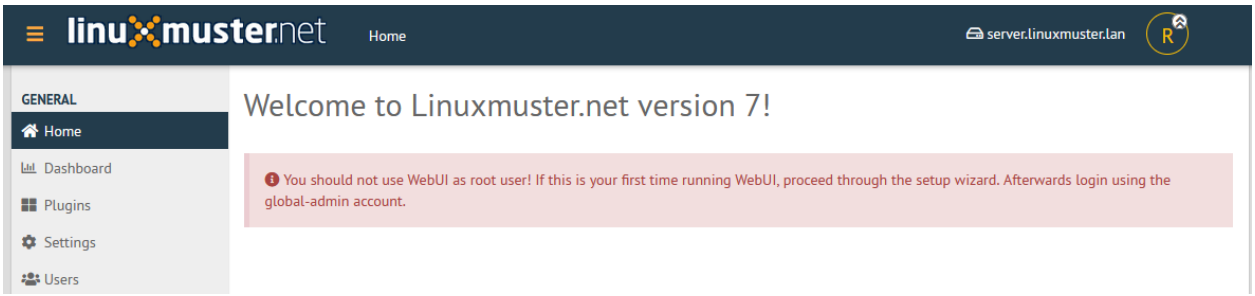
Hinweis: Achte darauf, dass vor dem Setup die Verbindung zur Schulkonsole via URL noch unverschlüsselt mit HTTP erfolgt.

Sollte das nicht möglich sein: Führe auf dem Server folgende Befehle aus:




```
sudo pip3 install Jinja2
sudo service linuxmuster-webui start
```

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.

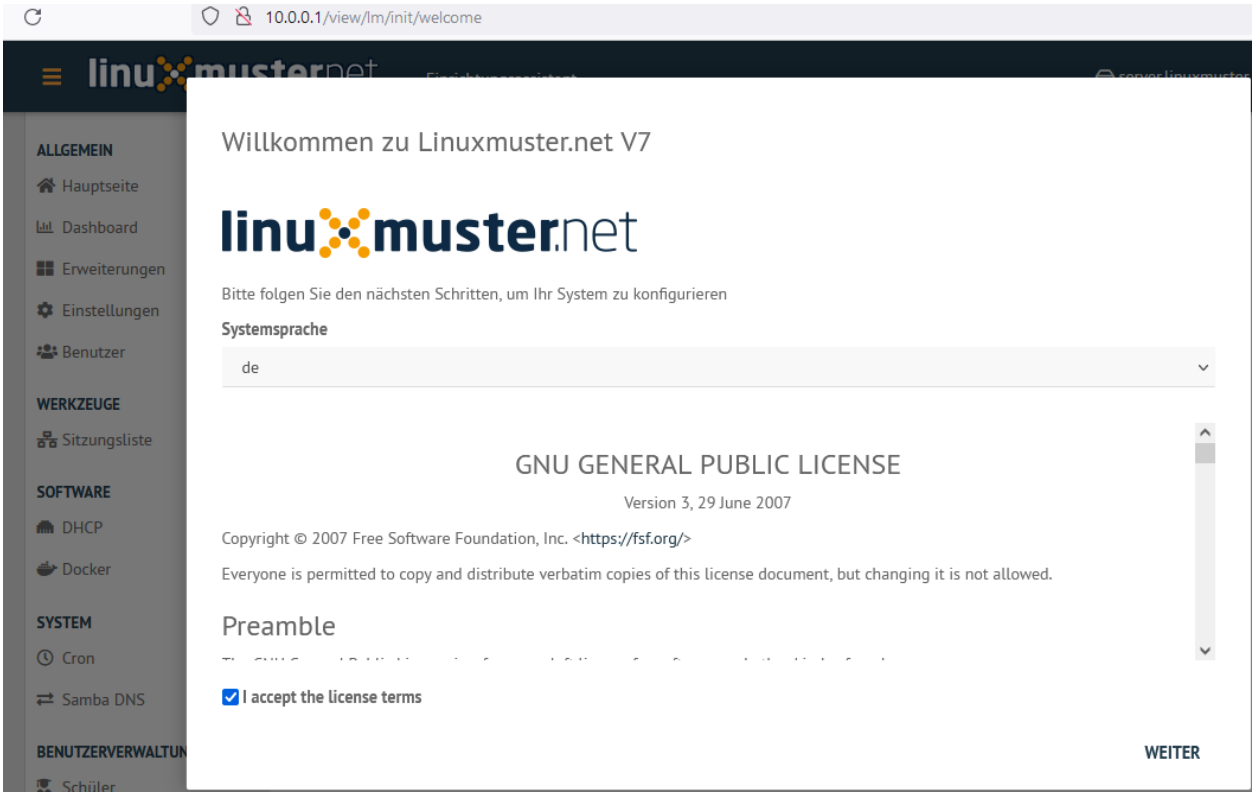
Es erscheint der Einrichtungsassistent. Hier musst Du zunächst die gewünschte Sprache auswählen. Zudem musst Du die GNU Lizenzbedingungen akzeptieren, indem Du bei `I accept the licence terms` einen Haken setzt.

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 `Domain name` spielt eine besondere Rolle, insbesondere, 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)

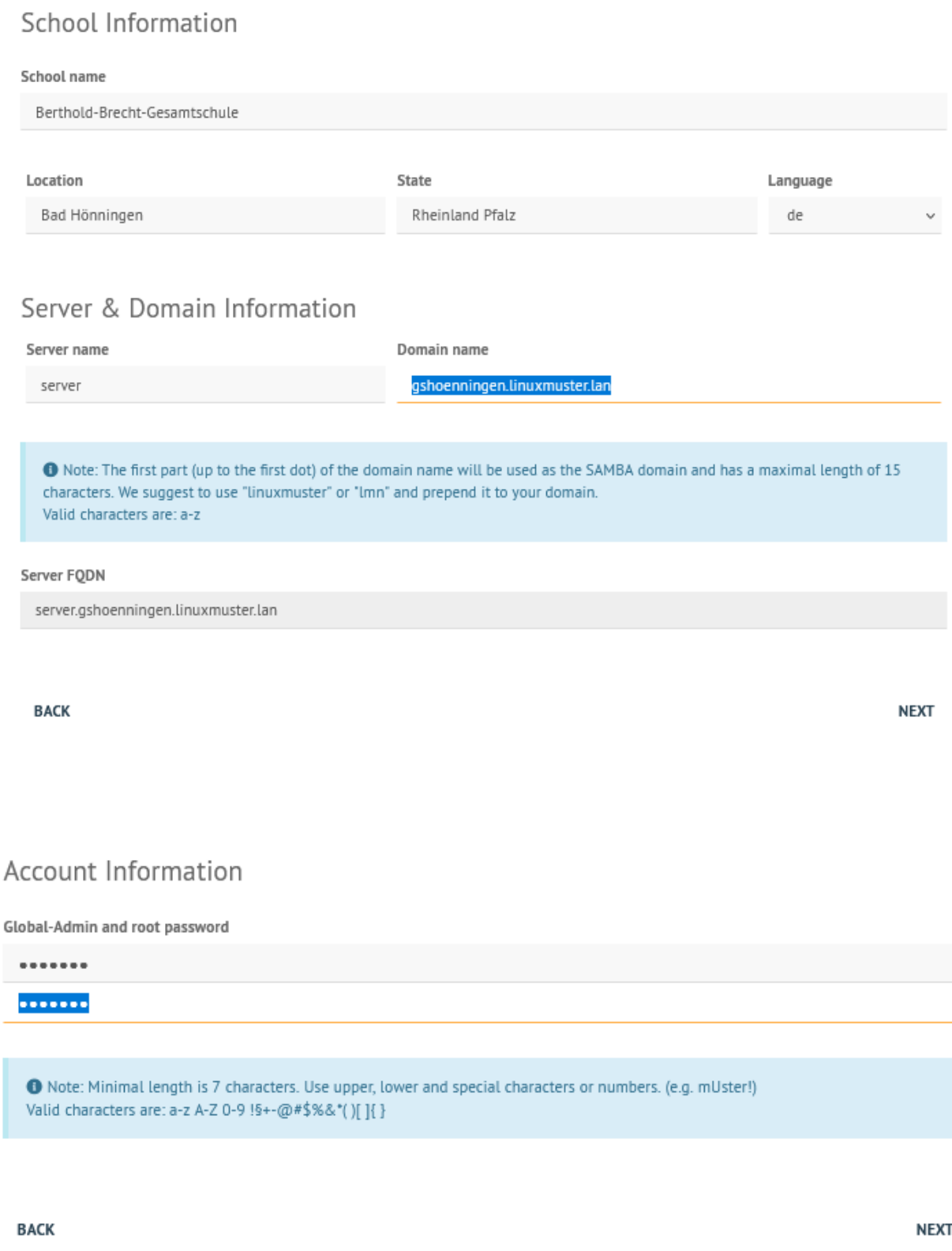
Danach klickst Du auf `Weiter/Next`.

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:**
  - 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 ?!§+-@#%&*( )[ ]{ }

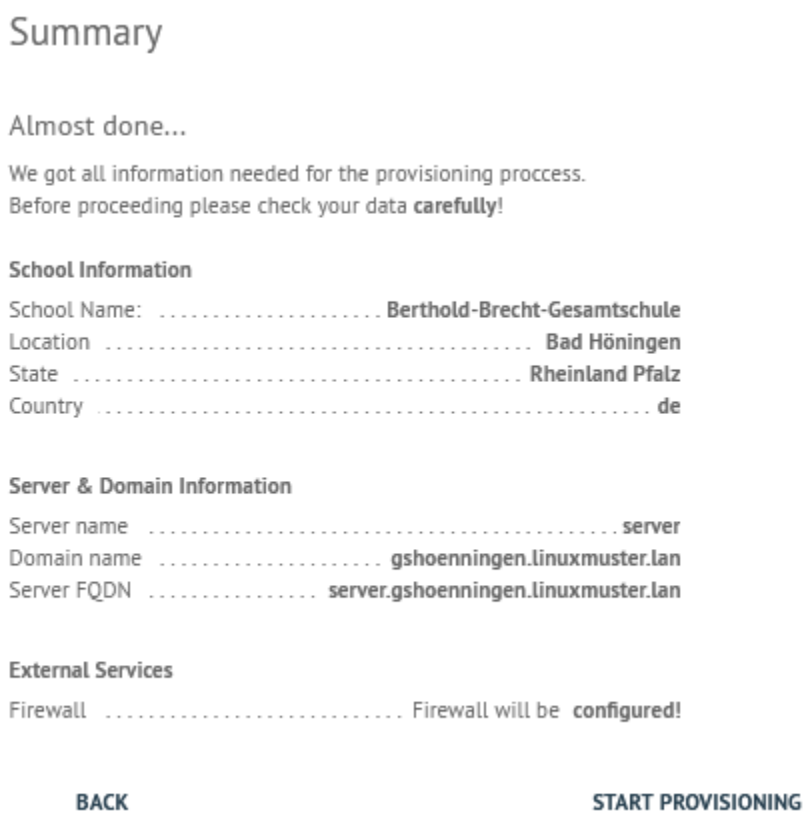

School Information
School name
Berthold-Brecht-Gesamtschule
Location
Bad Hönningen
State
Rheinland Pfalz
Language
de
Server & Domain Information
Server name
server
Domain name
gshoenningen.linuxmuster.lan
Note: The first part (up to the first dot) of the domain name will be used as the SAMBA domain and 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.linuxmuster.lan
BACK
NEXT
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

- 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 erhälst 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`.

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



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:

Zum Abschluss siehst Du den Eintrag

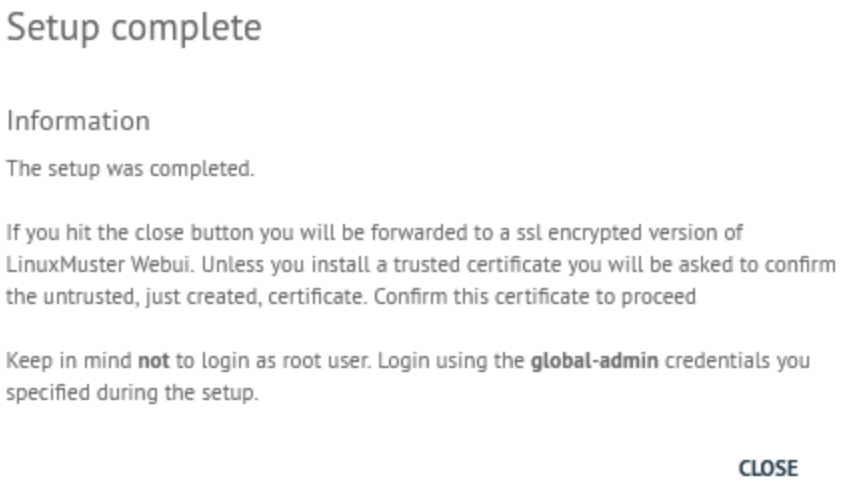
```
### linuxmuster-setup finished at ... ###
```

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`.

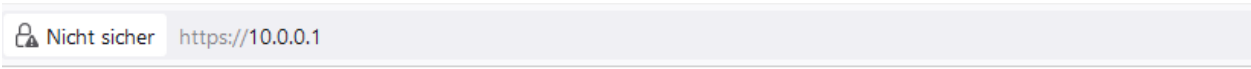
Rufe auf dem Server das Terminal auf und starte den Server neu:

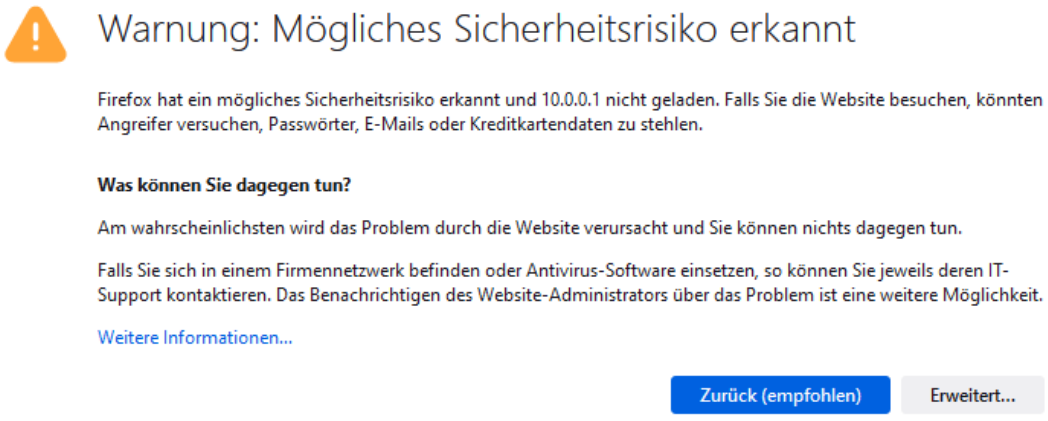
```
sudo reboot
```



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 akzetieren musst.

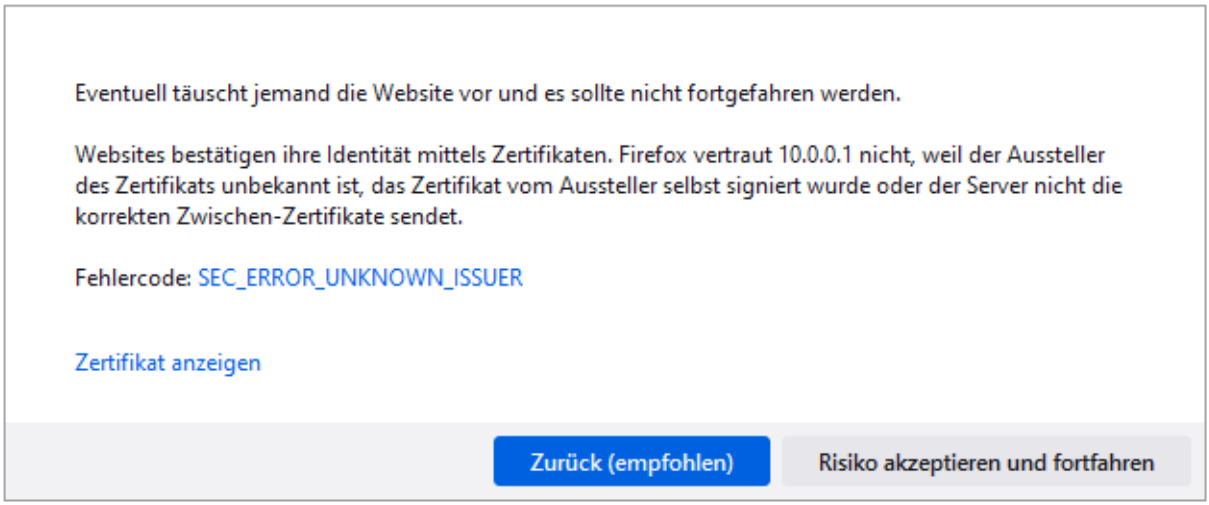




Der Browser zeigt Dir den Warnhinweis an. Klicke auf `Erweitert...`.

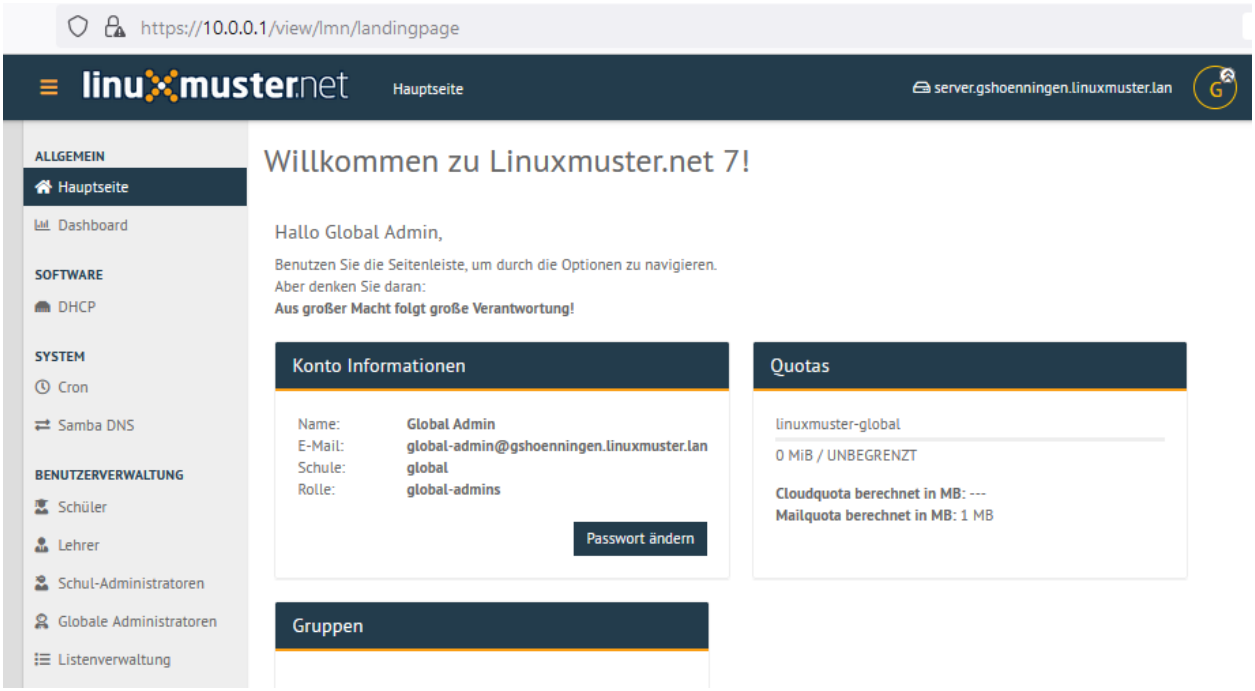
Es erscheint auf der gleichen Seite unten ein weiterer Eintrag. Bestätige diesen, indem Du den Button `Risiko akzeptieren und fortfahren` auswählst.

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


Eventuell täuscht jemand die Website vor und es sollte nicht fortgefahren werden.
Websites bestätigen ihre Identität mittels Zertifikaten. Firefox vertraut 10.0.0.1 nicht, weil der Aussteller des Zertifikats unbekannt ist, das Zertifikat vom Aussteller selbst signiert wurde oder der Server nicht die korrekten Zwischen-Zertifikate sendet.
Fehlercode: SEC_ERROR_UNKNOWN_ISSUER
Zertifikat anzeigen
Zurück (empfohlen)
Risiko akzeptieren und fortfahren


linuxmuster.net
global-admin
Anmelden

Nach erfolgreicher Anmeldung gelangst Du zur 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:

Setze die Ersteinrichtung fort, indem Du

Benutzeraufnahme mit der Schulkonsole und *Rechneraufnahme* aufrufst.

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

Migration auf linuxmuster 7.1

```
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:~#
```

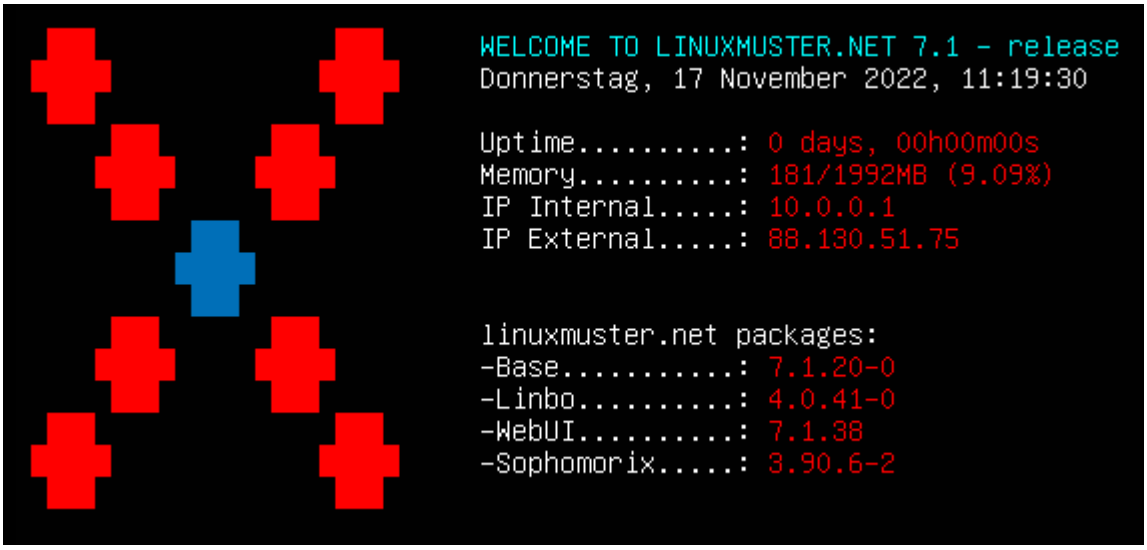
4.9 Setup im Terminal

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 v7.1 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 dazugehörende Ausgabe:

```
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 = \ndhcprange = \nschoolname = \nlocation =␣
↪\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.

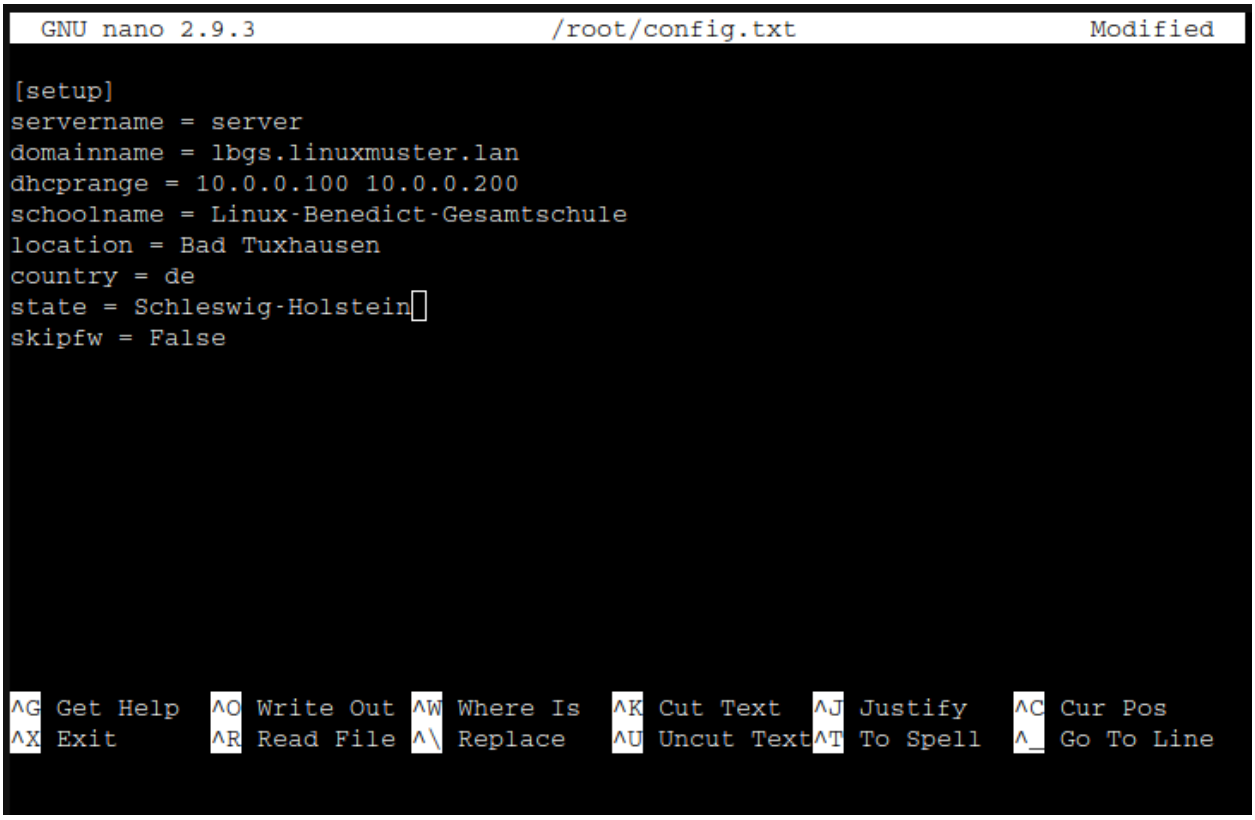
Klicke jeweils auf `< OK >`, um zum nächsten Schritt zu gelangen.

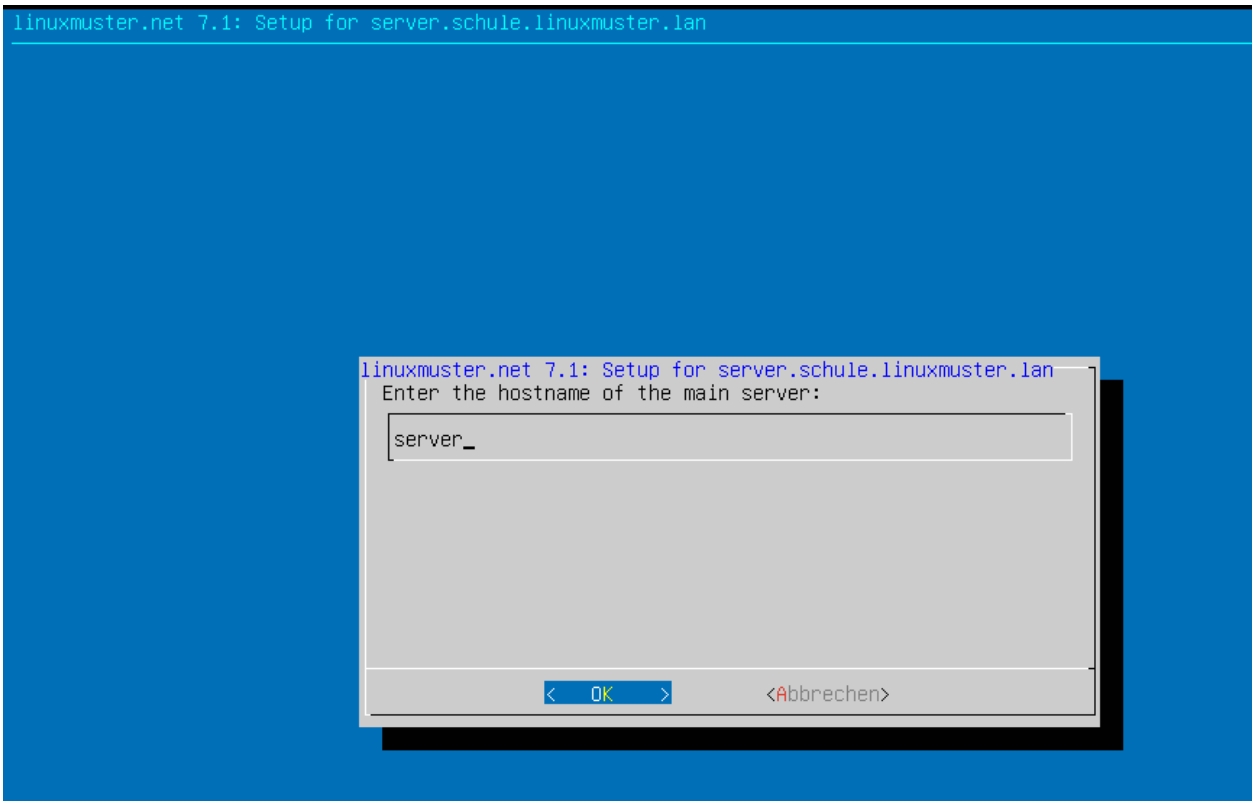
Danach gelangst Du zur Angabe der sogenannten Domain. Beachte bei dessen Festlegung u.g. Hinweise zum FQDN.

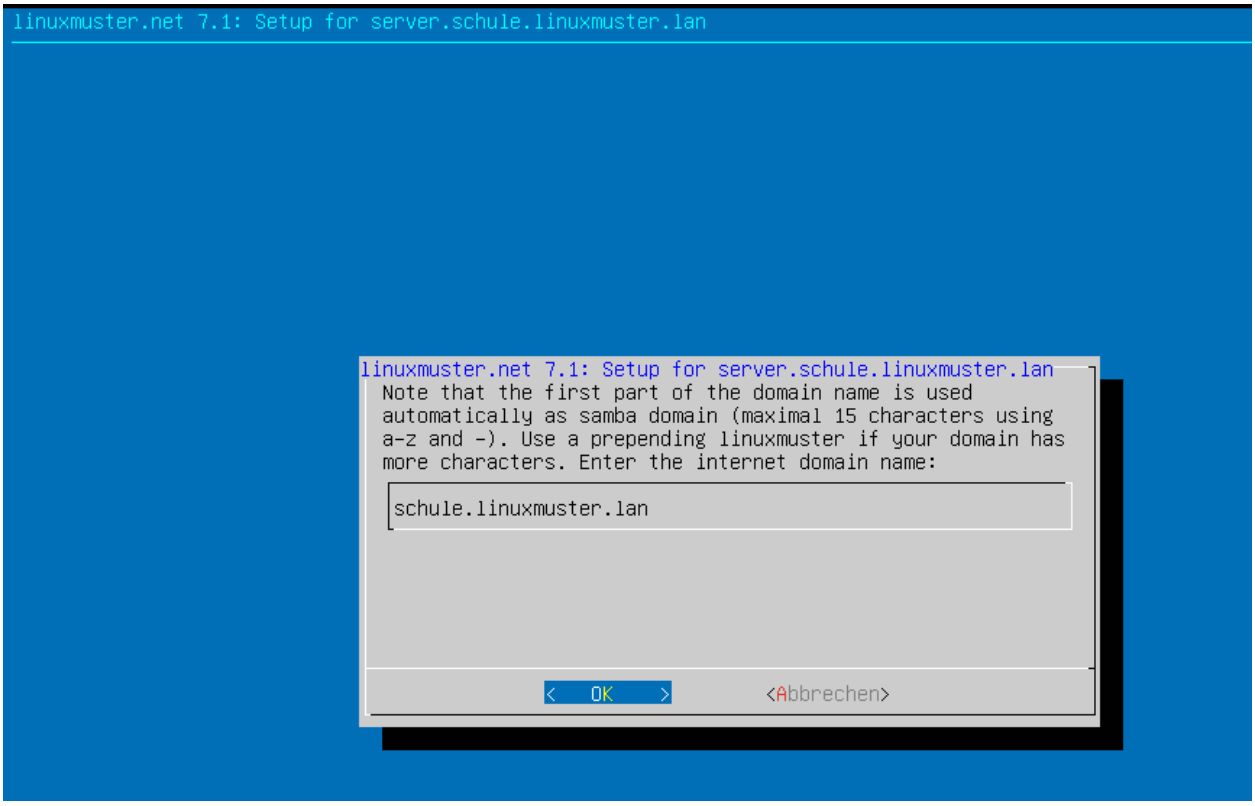
Hinweis: Der `Domain name` spielt eine besondere Rolle für das Setup.

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**


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


linuxmuster.net 7.1: Setup for server.schule.linuxmuster.lan
linuxmuster.net 7.1: Setup for server.schule.linuxmuster.lan
Enter the hostname of the main server:
server
< OK >
<Abbrechen>



- **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 defininationsmäßig 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.)

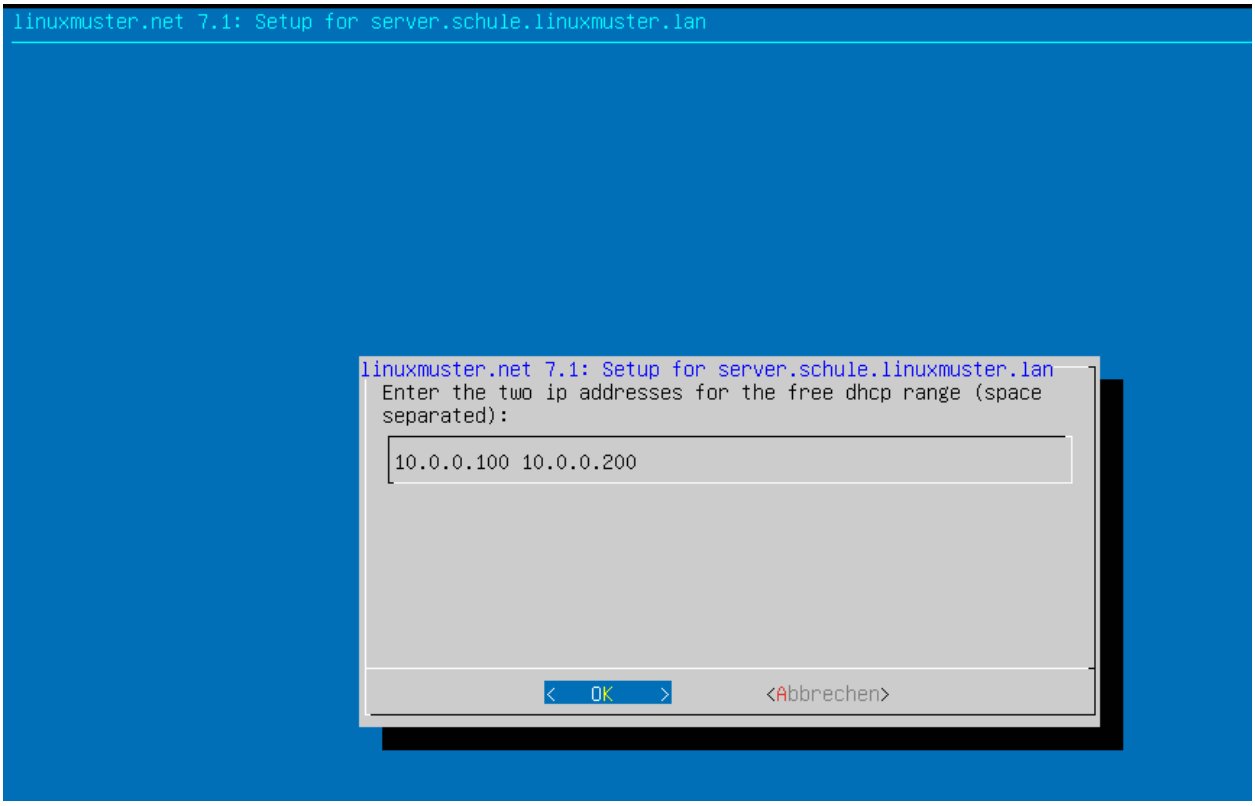
Falsch: GSO-Heinrich-Böll-Hönningen (26 Zeichen, Großbuchstaben, Umlaute, Bindestriche)

Weitergehende Informationen findest du hier: https://wiki.samba.org/index.php/Active_Directory_Naming_FAQ

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`.

Wechsele mit < `OK` > zur nächsten EIngabemaske.

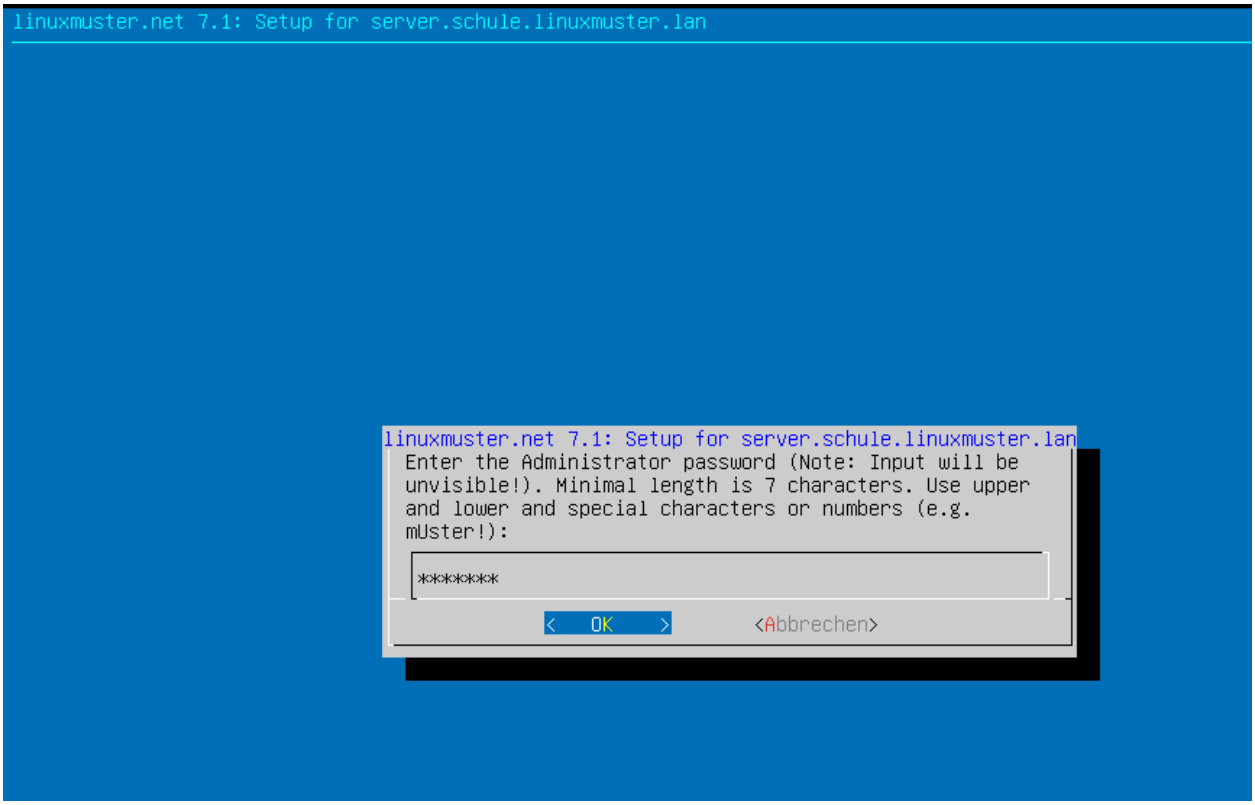


Hier setzt Du ein neues Administrations-Kennwort. Dieses wird zugleich das neue Kennwort aller administrativens Benutzer, so auch vom `gobal-admin` in der Schulkonsole.

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 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 wie oben genannt)
- 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
```

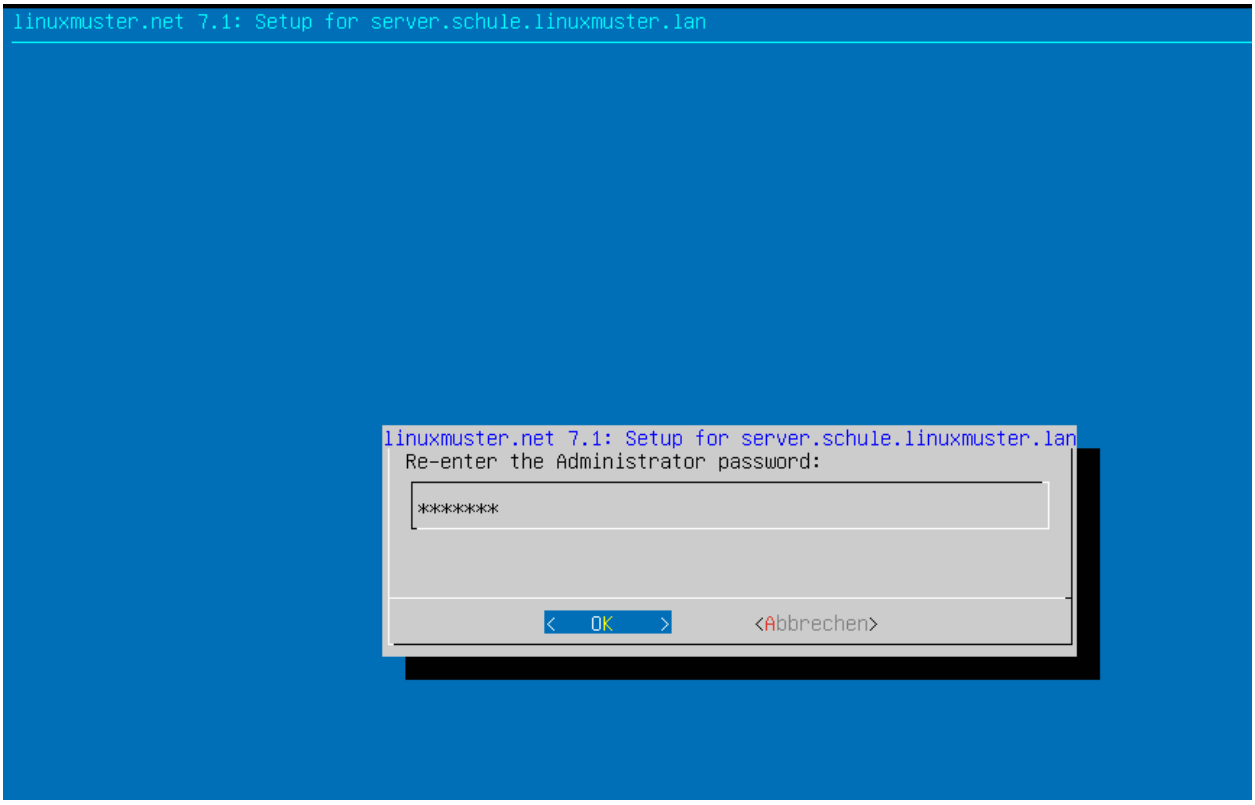
alternativ

```
# reboot
```

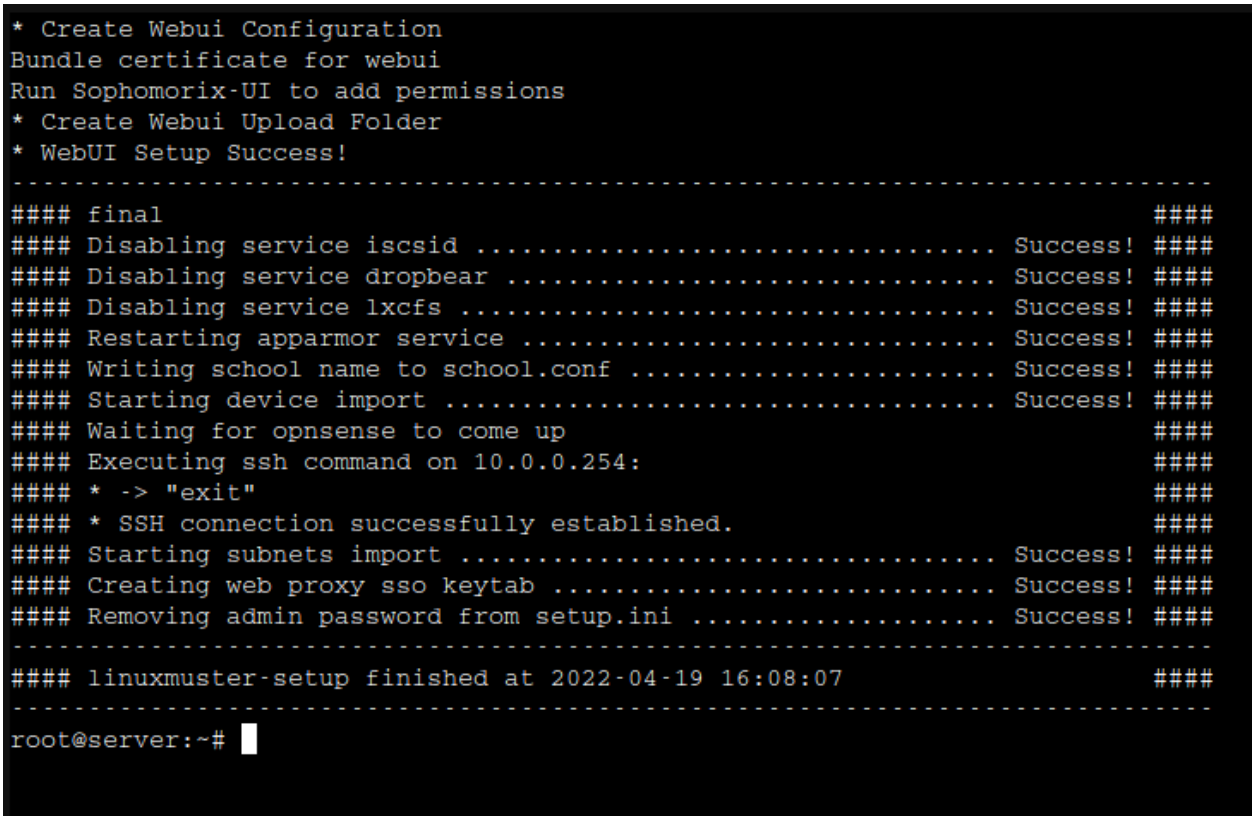
Das erste Verfahren hat den Vorteil, dass Du nicht die Zeit des Neustarts abwarten, Dich erneut verbinden und anmelden musst.

Nach abgeschlossenem Set-up und dem Neustart des Dienstes `linuxmuster-webui` bzw. eventuellen Neustart des Servers, könntest Du Dich mit einem PC via Browser an der Schulkonsole von linuxmuster.net v7.1 anmelden.

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.




```
#### Writing input to setup ini file ........................... Success! ####
#### Setting root password ..................................... Success! ####
--------------------------------------------------------------------------------
#### templates                                                             ####
#### Reading setup data ........................................ Success! ####
#### Processing config templates:                                          ####
#### * cupsd.conf .............................................. Success! ####
#### * subnets.csv ............................................. Success! ####
#### * nsswitch.conf ........................................... Success! ####
#### * smb.conf ................................................ Success! ####
#### * webui-sudoers ........................................... Success! ####
#### * dhcpd.events.conf ....................................... Success! ####
#### * devices.csv ............................................. Success! ####
#### * dhcpd.custom.conf ....................................... Success! ####
#### * dhcpd.subnets.conf ...................................... Success! ####
#### * rsyncd.conf ............................................. Success! ####
#### * dhcpd.apparmor.d ........................................ Success! ####
#### * dhcpd.devices.conf ...................................... Success! ####
#### * smb.conf.admin .......................................... Success! ####
#### * ntp.conf ................................................ Success! ####
#### * dhcpd.conf .............................................. Success! ####
#### Server prepare update ..................................... Success! ####
#### Adjusting server time
```



Daher muss sich der Rechner in einem besonderen LAN-Bereich befinden, etwa die 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

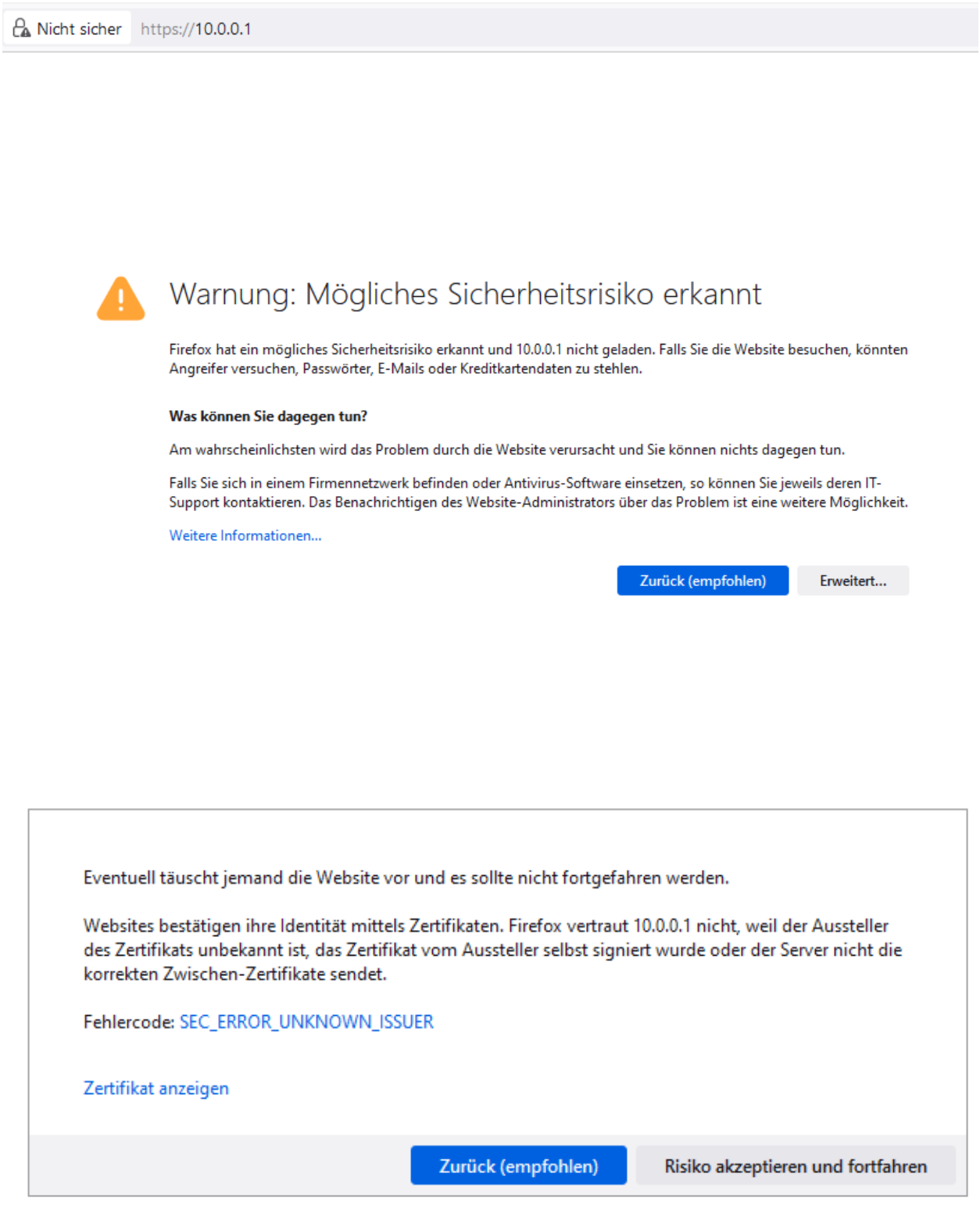
Öffne die URL `https://10.0.0.1` mit dem Admin-PC. Es wurde beim Setup ein self-signed certificate erstellt, sodass Du dieses beim erstmaligen Aufruf mit dem Browser akzeptieren musst.

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

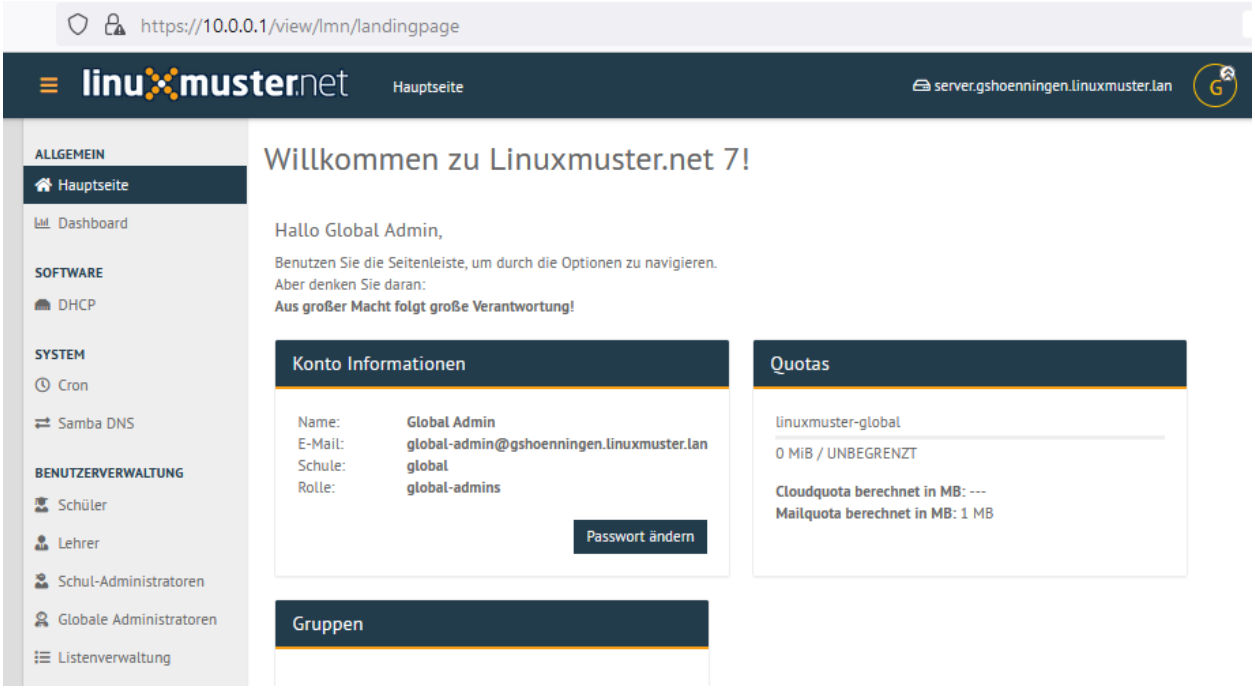
Es erscheint auf der gleichen Seite unten ein weiterer Eintrag. Bestätige diesen, indem Du den Button `Risiko akzeptieren und fortfahren` auswählst.

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.


Nicht sicher
https://10.0.0.1
Warnung: Mögliches Sicherheitsrisiko erkannt
Firefox hat ein mögliches Sicherheitsrisiko erkannt und 10.0.0.1 nicht geladen. Falls Sie die Website besuchen, könnten Angreifer versuchen, Passwörter, E-Mails oder Kreditkartendaten zu stehlen.
Was können Sie dagegen tun?
Am wahrscheinlichsten wird das Problem durch die Website verursacht und Sie können nichts dagegen tun.
Falls Sie sich in einem Firmennetzwerk befinden oder Antivirus-Software einsetzen, so können Sie jeweils deren IT-Support kontaktieren. Das Benachrichtigen des Website-Administrators über das Problem ist eine weitere Möglichkeit.
Weitere Informationen...
Zurück (empfohlen)
Erweitert...
Eventuell täuscht jemand die Website vor und es sollte nicht fortgefahren werden.
Websites bestätigen ihre Identität mittels Zertifikaten. Firefox vertraut 10.0.0.1 nicht, weil der Aussteller des Zertifikats unbekannt ist, das Zertifikat vom Aussteller selbst signiert wurde oder der Server nicht die korrekten Zwischen-Zertifikate sendet.
Fehlercode: SEC_ERROR_UNKNOWN_ISSUER
Zertifikat anzeigen
Zurück (empfohlen)
Risiko akzeptieren und fortfahren


linuxmuster.net
global-admin
Anmelden


https://10.0.0.1/view/lmn/landingpage
linuxmuster.net
Hauptseite
server.gshoenningen.linuxmuster.lan
ALLGEMEIN
Hauptseite
Dashboard
SOFTWARE
DHCP
SYSTEM
Cron
Samba DNS
BENUTZERVERWALTUNG
Schüler
Lehrer
Schul-Administratoren
Globale Administratoren
Listenverwaltung
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@gshoenningen.linuxmuster.lan
Schule: global
Rolle: global-admins
Passwort ändern
Quotas
linuxmuster-global
0 MiB / UNBEGRENZT
Cloudquota berechnet in MB: ---
Mailquota berechnet in MB: 1 MB
Gruppen

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:~#
```

Setze die Ersteinrichtung fort, indem Du

Benutzeraufnahme mit der Schulkonsole und *Rechneraufnahme* aufrufst.

Alternativ wenn du eine Migration durchführen willst, geht es weiter mit

Migration auf linuxmuster 7.1

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.

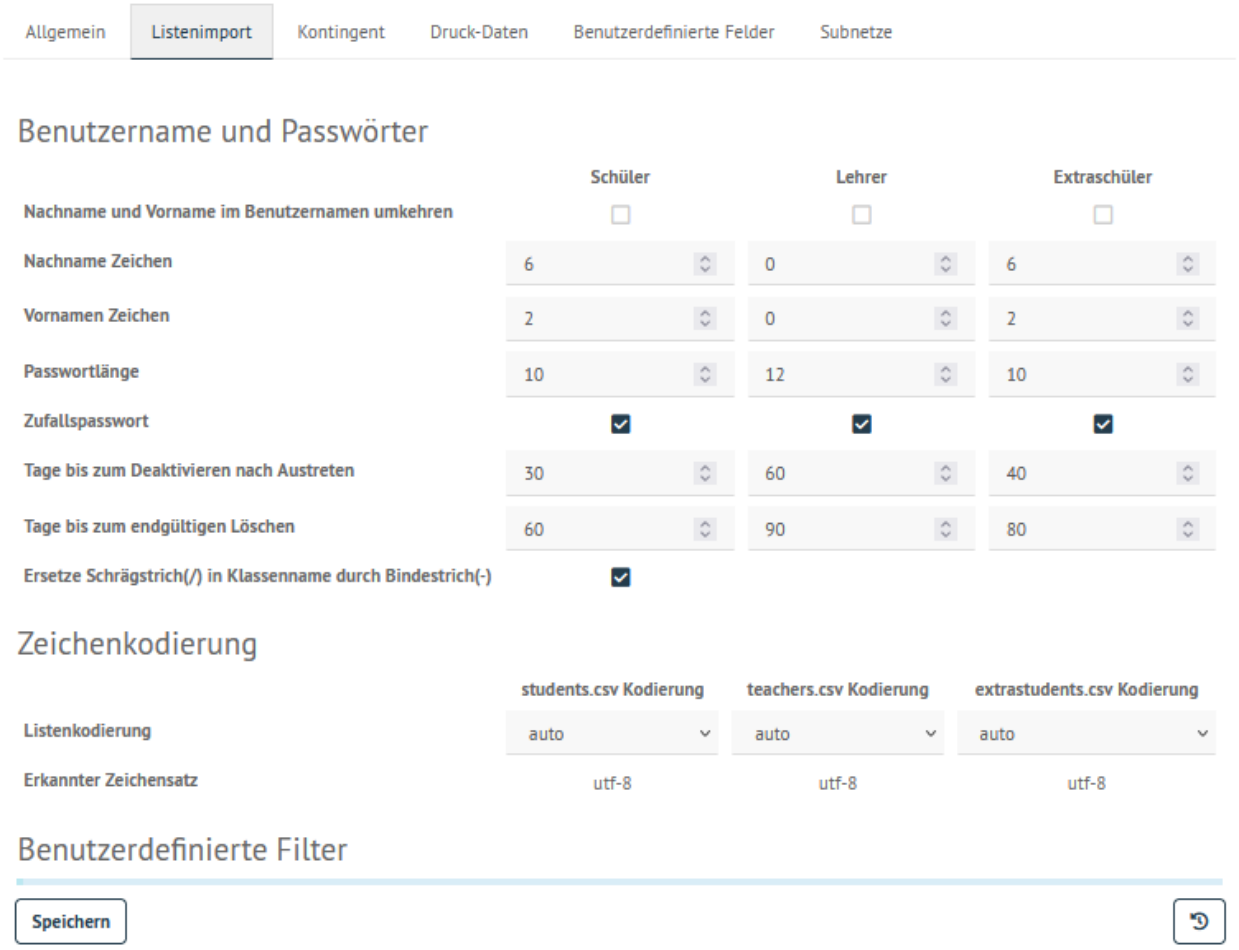
In diesen Abschnitten wird beispielhaft `ein Lehrer händisch` angelegt und per Datei-Import einige Schüler aufgenommen. Melde Dich dafür an der Schulkonsole als `global-admin` an.

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`.

Klicke rechts auf die Reiterkarte `Listenimport` unterhalb von `Zeichenkodierung` 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:

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`.

Einzelnen Lehrer hinzufügen

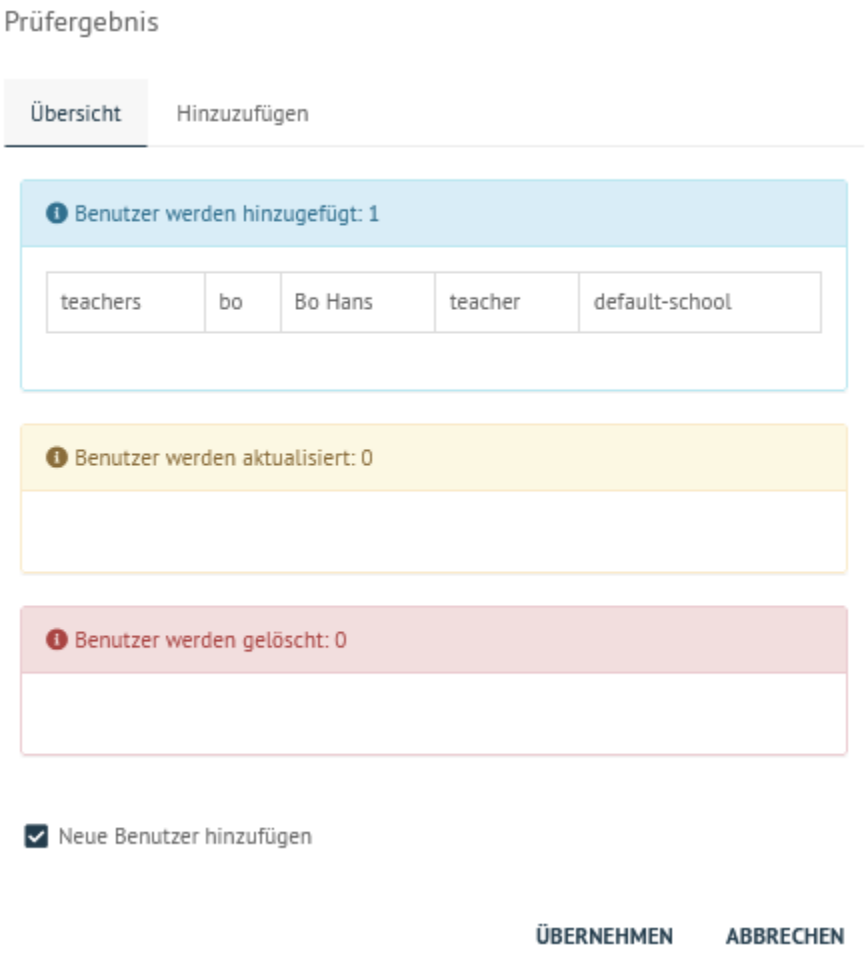
Klicke auf den Button `+ Lehrer hinzufügen`. Es wird eine leere Zeile hinzugefügt, die nun mit den angezeigten Daten zu füllen ist.

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.

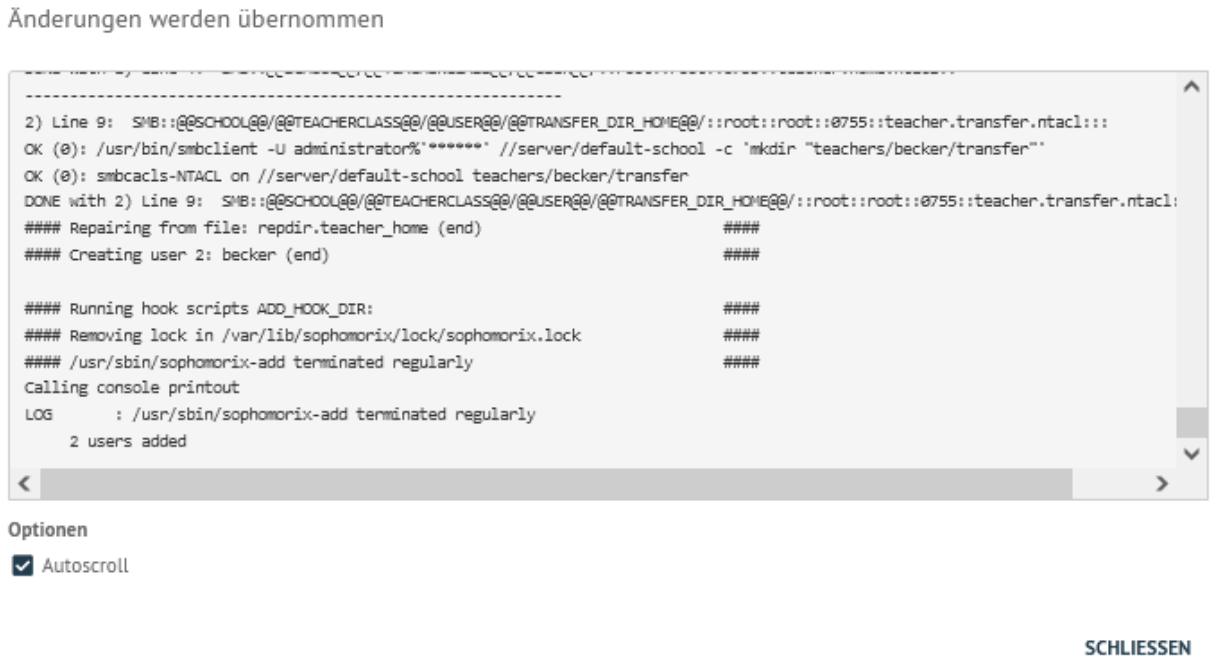


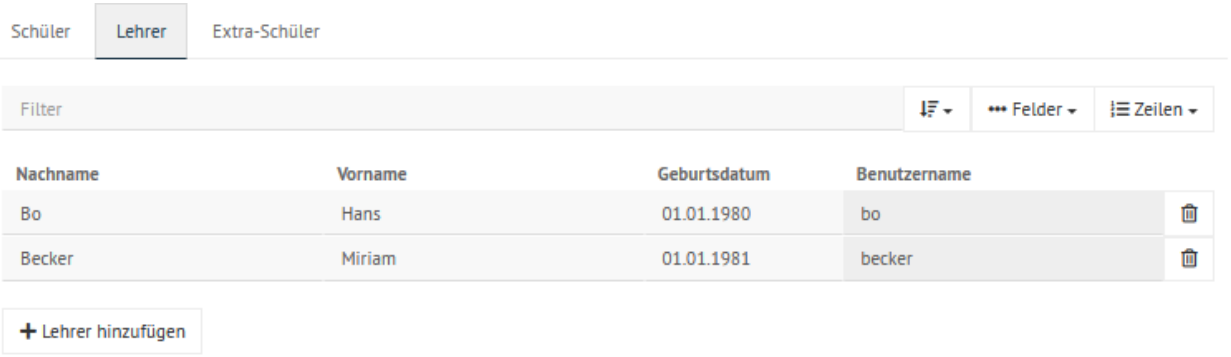
In o.g. Fenster ist zu sehen, dass ein neuer Lehrer hinzugefügt wird. Mit dem Button `Übernehmen` werden die dargestellten Aktionen ausgeführt (hinzufügen, aktualisieren, löschen).

Der Importdialog zeigt den Fortschritt an und meldet zurück, wenn die Aufnahme abgeschlossen wurde.

Bestätige dies mit dem Button `Schliessen`.

Die neune oder geänderten Benutzer findest Du nun im Menü `Benutzerverwaltung --> Lehrer`. Hier können deren Kontoinformationen abgerufen und z.B. Erstpasswörter (zurück-)gesetzt werden.


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/sophomorix/lock/sophomorix.lock
/usr/sbin/sophomorix-add terminated regularly
Calling console printout
LOG : /usr/sbin/sophomorix-add terminated regularly
2 users added
Optionen
Autoscroll
SCHLIESSEN

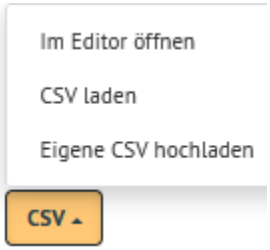

Schüler
Lehrer
Extra-Schüler
Filter
Felder
Zeilen
Nachname
Vorname
Geburtsdatum
Benutzername
Bo
Hans
01.01.1980
bo
Becker
Miriam
01.01.1981
becker
Lehrer hinzufügen

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.



Eine zu importierende Datei sollte folgende Daten aufweisen:

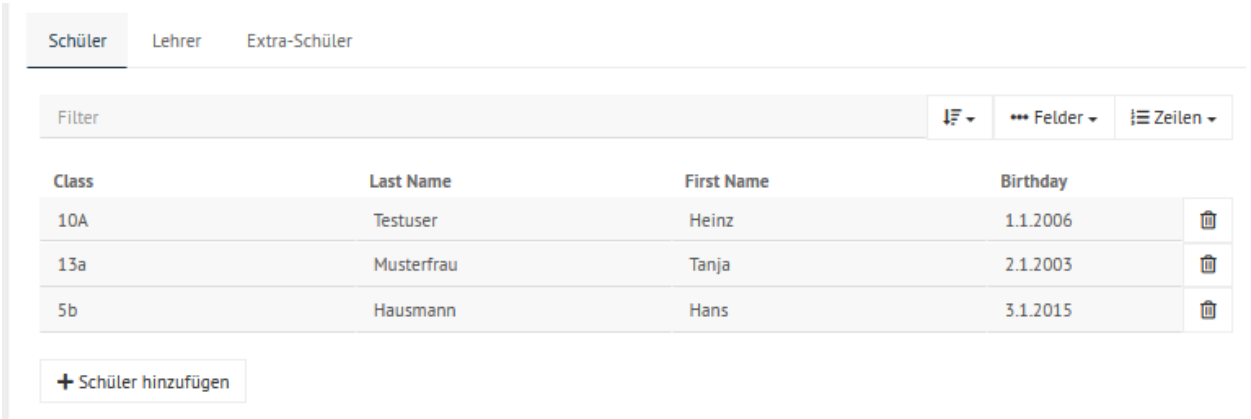
```
Klassenbezeichnung;Nachname;Vorname;Geburtsdatum;ID (optional aus einem␣
↪Schulverwaltungsprogramm)
```

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.

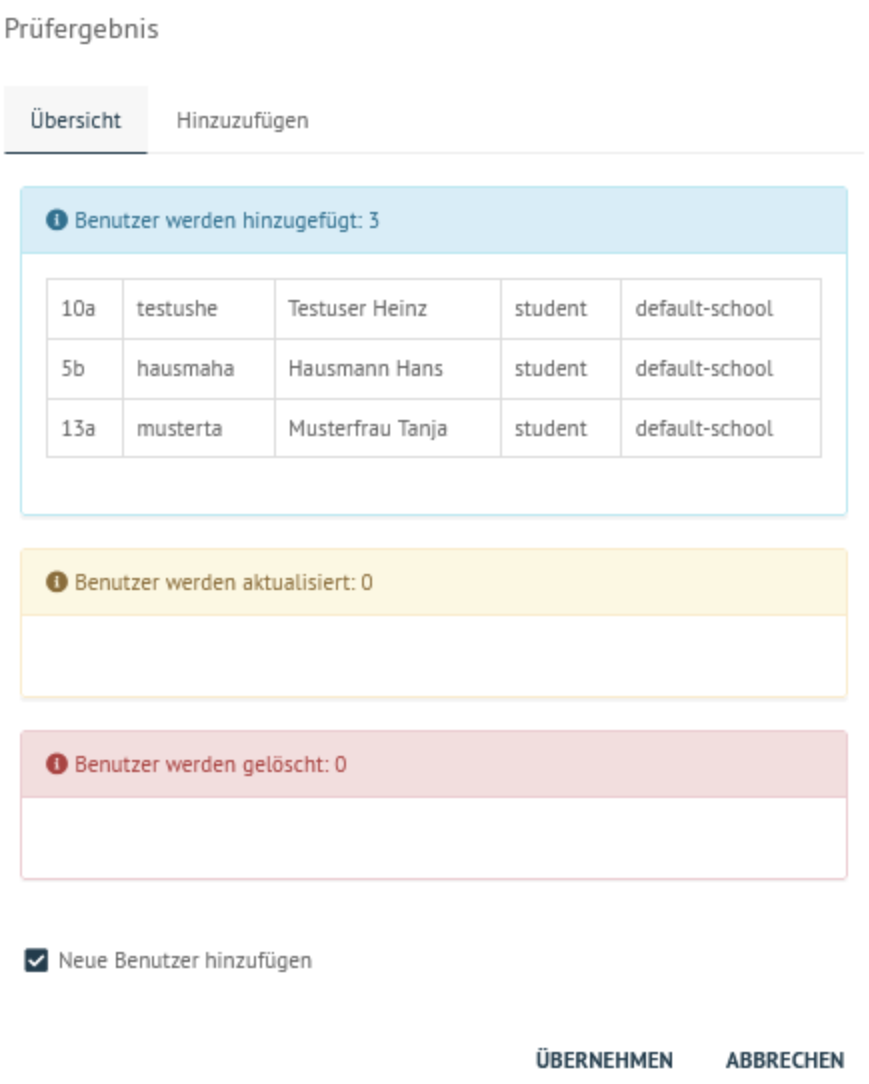
```
10A;Testuser;Heinz;1.1.2006;1234
13a;Musterfrau;Tanja;2.1.2003;1235
5b;Hausmann;Hans;3.1.2016;1236
```

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.

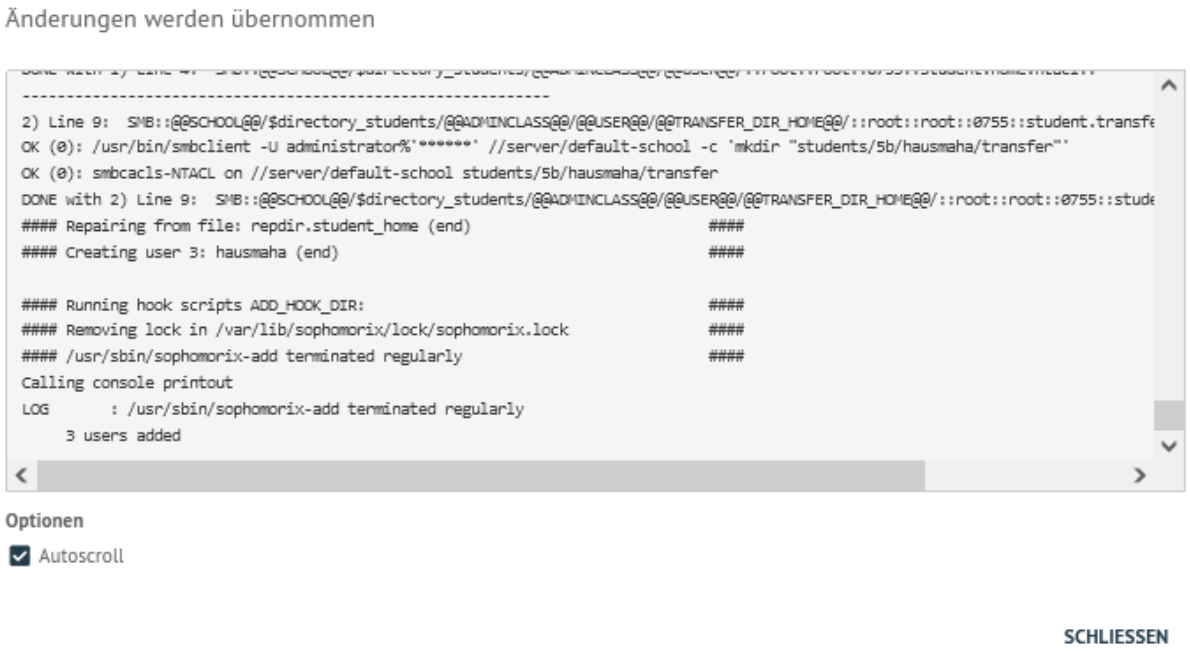
Mit der Option `Eigene CSV hochladen` kann eine so formatierte Datei nun hochgeladen werden. Die Schüler der zu importierenden Datei sind dann in der Listenverwaltung unter den Schülern zu sehen.



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
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
Benutzer werden aktualisiert: 0
Benutzer werden gelöscht: 0
Neue Benutzer hinzufügen
ÜBERNEHMEN
ABBRECHEN

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.

4.10.4 Fehlerkorrektur

Hat man fehlerhafte Daten in das System eingepflegt und hat sie noch nicht imporiert, lassen sich Schüler und Lehrerlisten aus einer Sicherung zurückholen. Der Knopf für die Sicherung ist rechts unten in der Listenverwaltung.

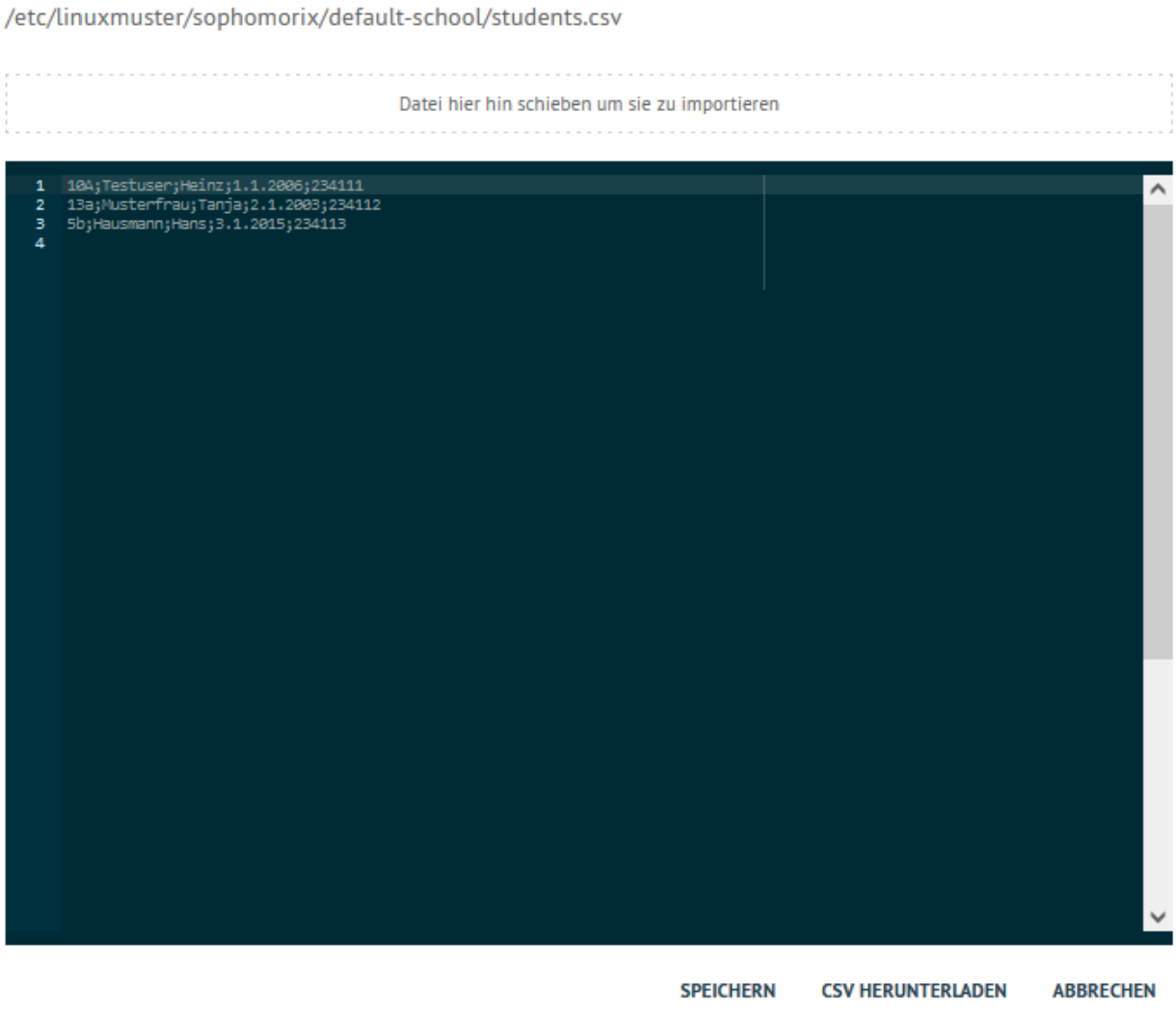
Hast Du z.B. bei der zuvor importierten CSV-Datei die IDs vergessen, kannst Du diese in der CSV-Datei ergänzen, diese erneut importieren. Es werden Dir dann die Änderungen angezeigt. In diesem Fall wird die `uid` auf die neu eingetragenen ID geändert.

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.


Prüfergebnis
Übersicht
Zu versetzen
Benutzer werden hinzugefügt: 0
Benutzer werden aktualisiert: 3
musterta
Unid : --- --> 234112
hausmaha
Unid : --- --> 234113
testushe
Unid : --- --> 234111
Benutzer werden gelöscht: 0
Benutzer versetzen
ÜBERNEHMEN
ABBRECHEN
Im Editor öffnen
CSV laden
Eigene CSV hochladen
CSV


/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

4.11 Muster-Client aufsetzen

Autor des Abschnitts: @cweikl, @MachtDochNix

Clients sollen mithilfe von LINBO automatisiert verwaltet werden. Hierbei kann ein Betriebssystem oder es können auch mehrere Multi-Boot Betriebssysteme auf dem Client installiert werden. Mithilfe von LINBO erfolgt so ein automatischens Ausrollen der Clients im Netzwerk oder das Verteilen zusätzlich installierter Software.

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
- 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` vom linuxmuster.net-Server aufgenommen wird und somit dem System bekannt ist.

Es gibt drei Möglichkeiten die Rechneraufnahme durchzuführen, welche das sind, wird Dir im Kapitel *Rechneraufnahme* gezeigt.

OS-Installation

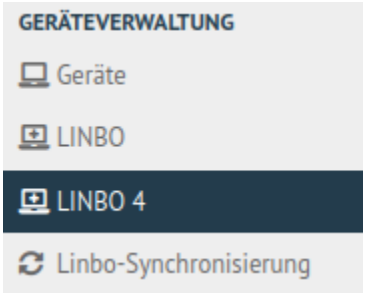
Im letzten Schritt wird nun das eigentliche Betriebssystem auf dem Muster-Client erstellt, in die Domäne eingebunden und das endgültige Image auf den linuxmuster.net-Server geschrieben. Da sich das Vorgehen je nach verwendetem System unterscheidet, gehen die Unterkapitel von *Betriebssysteme installieren* 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. Dafür klickst Du links im Menü 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.

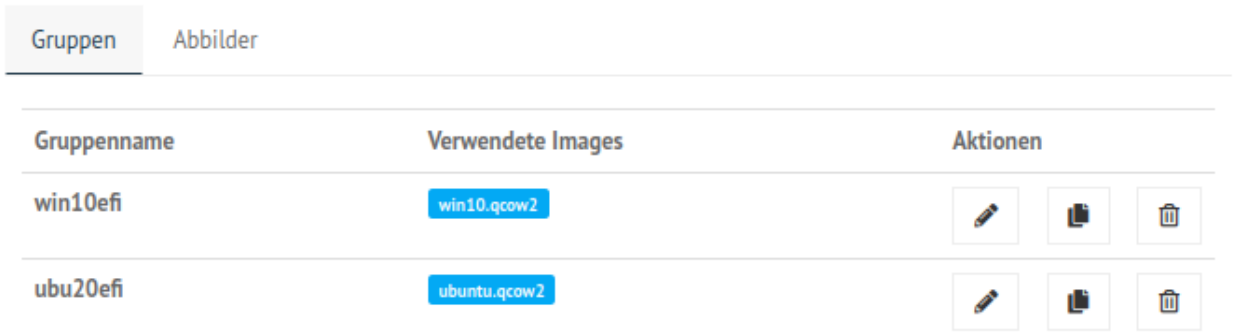
Es öffnet sich ein Fenster, in dem Du die Namen der neuen Hardwareklasse angibst. Diesen wirst Du später benötigen, um Geräte dieser Hardwareklasse zuzuweisen.

Hinweis: Die neu angelegte Hardwareklasse wird nicht direkt in der Übersicht mit allen eingerichteten Klassen angezeigt. Hierzu musst Du zunächst mit `F5` die Webseite neu laden.

Die Liste der angelegten Hardwareklassen kann dann - z.B. wie nachstehend dargestellt - aussehen (andere Namen für die HWK verwendet):


Leer
start.conf.win10-ubuntu-efi
start.conf.win7-efi
start.conf.ubuntu-efi
start.conf.remote_cache
start.conf.win7-ubuntu2004
start.conf.win10-win10-efi
start.conf.win7-ubuntu2004-efi
start.conf.ubuntu2004-efi
+ ERSTELLEN

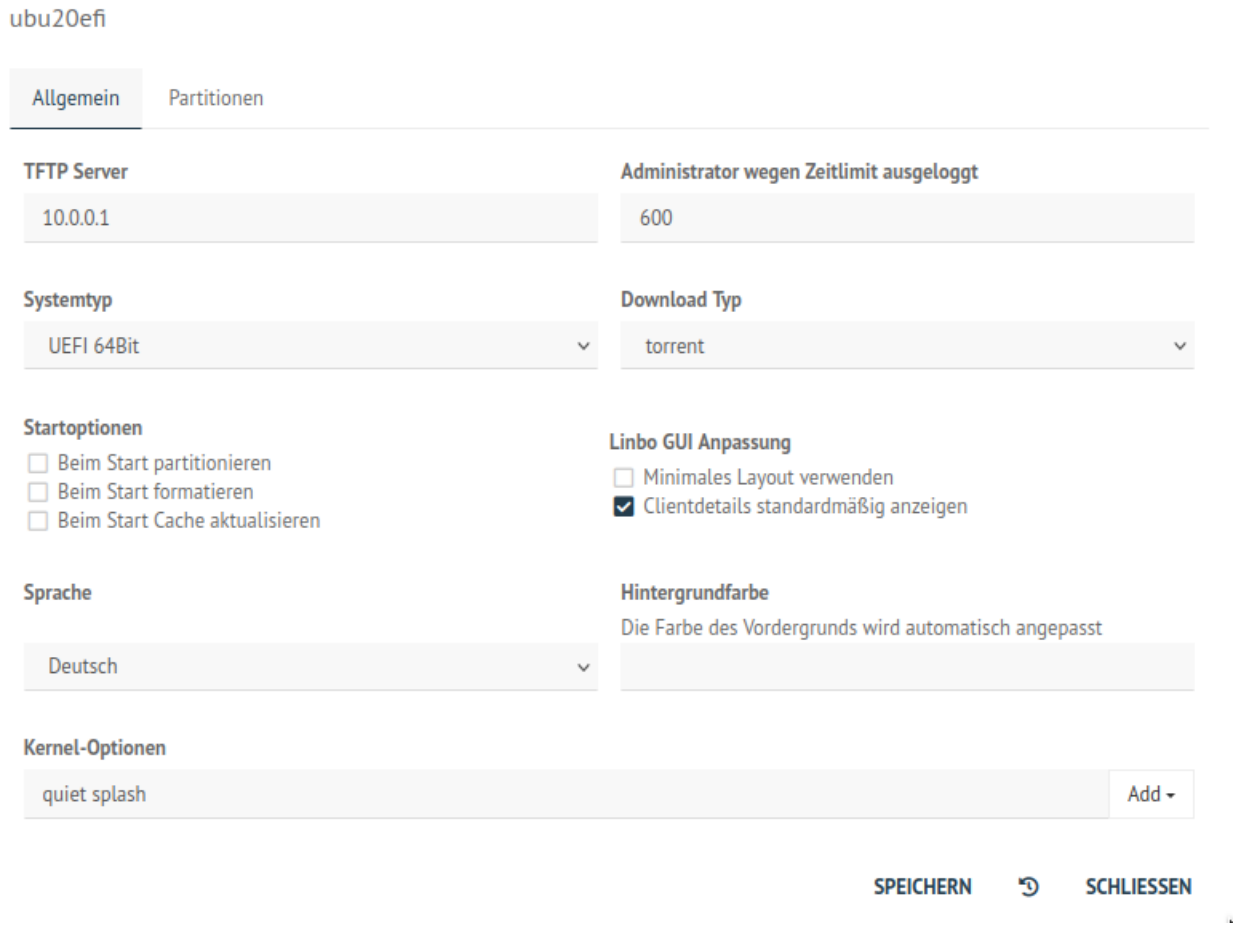

New name
my-ubuntu-20-04-muster-client
OK
ABBRECHEN


Gruppen
Abbilder
Gruppenname
Verwendete Images
Aktionen
win10efi
win10.qcow2
ubu20efi
ubuntu.qcow2

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 für den Boot bei besonderer Hardware an.



Unter `Partitionen` legst Du fest, welche Partitionen auf der Festplatte vorgesehen werden sollen.

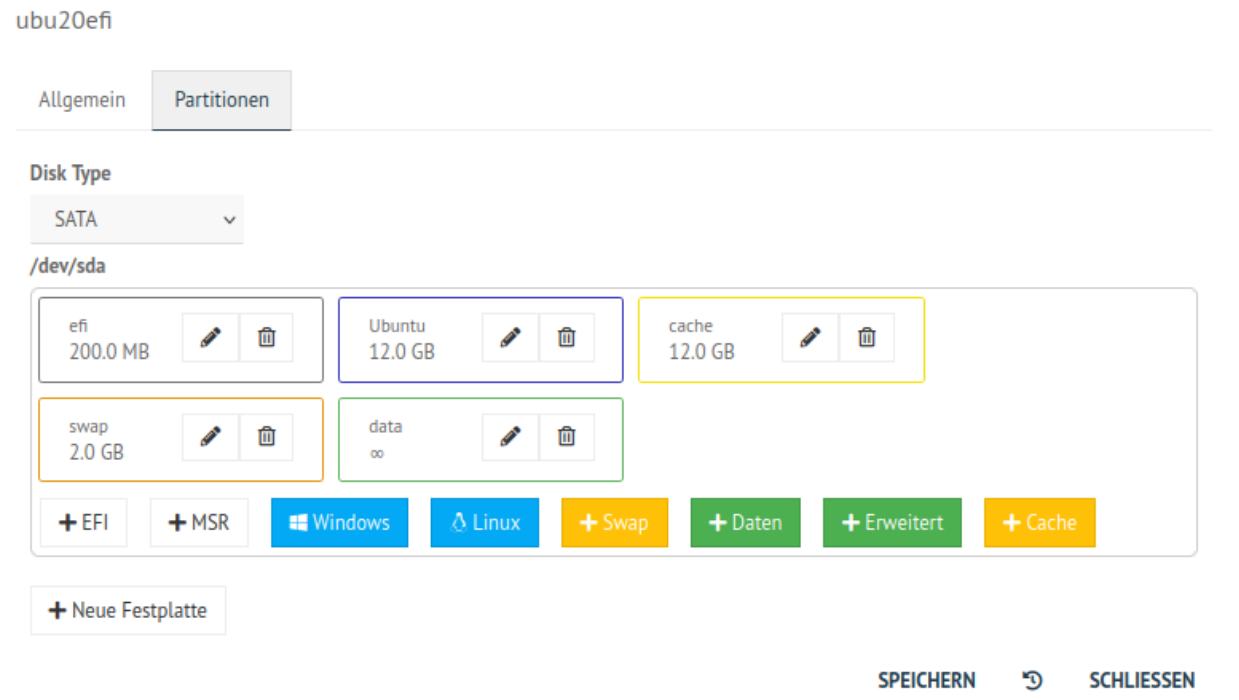
Löschst Du dort z.B. die Partitionen `swap` und `data` so sieht Deine Partitionierung wie folgt aus:

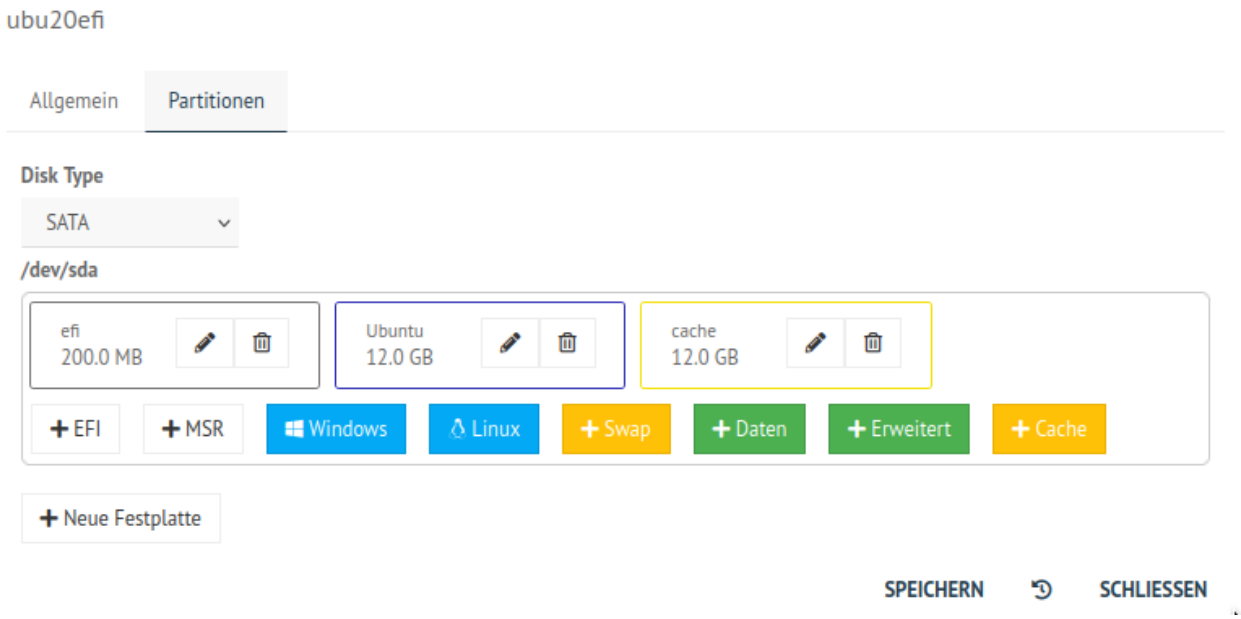
Um Einstellungen für das Betriebssystem vorzunehmen, klickst Du auf das Stift-Icon. Es öffnet sich ein weiteres Fenster, um Einstellungen für das Betriebssystem vorzunehmen.

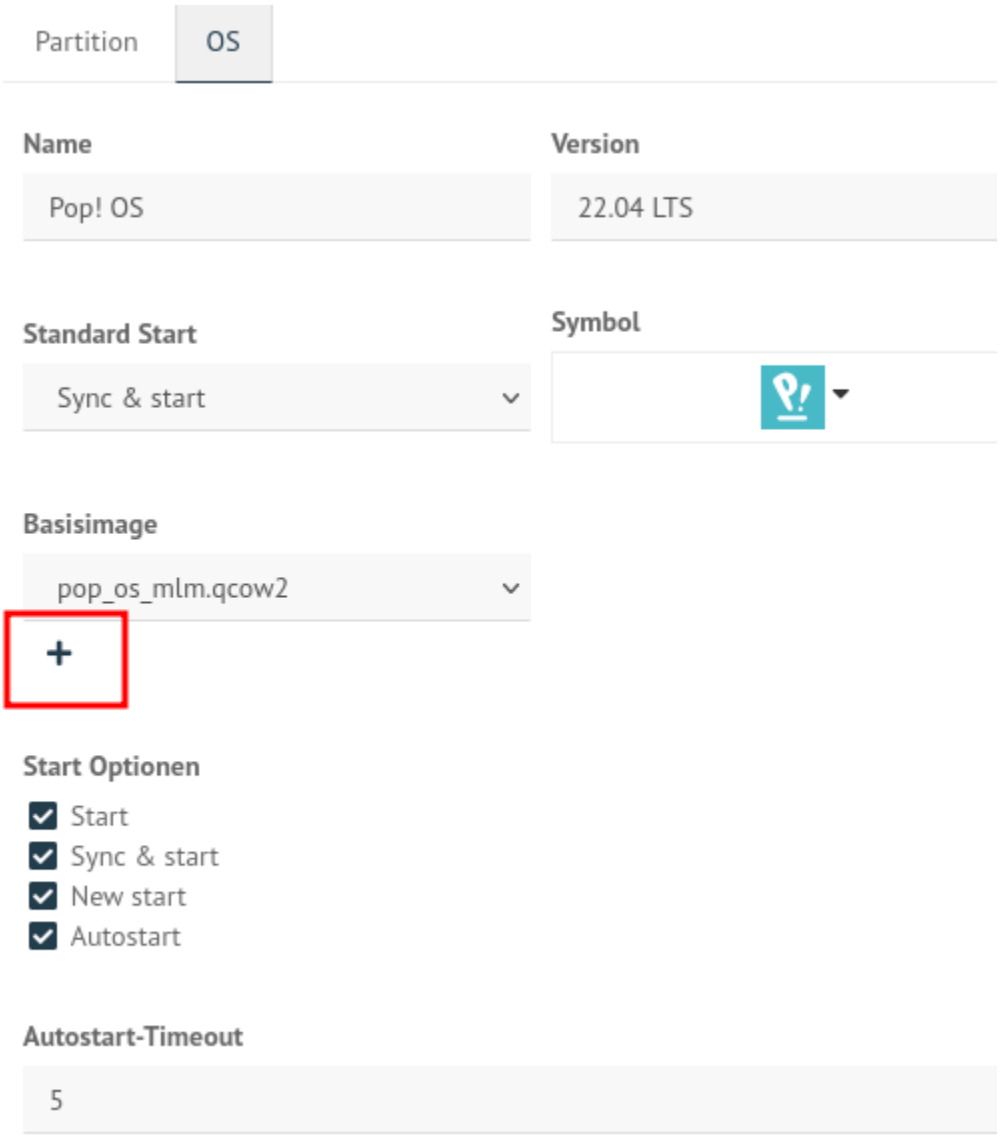
Unter der Reiterkarte `OS` legst Du für das Betriebssystem (OS) die gewünschten Icons, die Start-Optionen und u.a. auch den Namen für das Basisimage fest. Um ein neues Image festzulegen, klickst Du auf das + - Zeichen und trägst einen neuen Namen für das Image ein. Achte darauf, dass die Dateiendung `.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.qwco2 -, 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 vor-


ubu20efi
Allgemein
Partitionen
Disk Type
SATA
/dev/sda
efi
200.0 MB
Ubuntu
12.0 GB
cache
12.0 GB
swap
2.0 GB
data
∞
+ EFI
+ MSR
Windows
Linux
+ Swap
+ Daten
+ Erweitert
+ Cache
+ Neue Festplatte
SPEICHERN
SCHLIESSEN


ubu20efi
Allgemein
Partitionen
Disk Type
SATA
/dev/sda
efi
200.0 MB
Ubuntu
12.0 GB
cache
12.0 GB
+ EFI
+ MSR
Windows
Linux
+ Swap
+ Daten
+ Erweitert
+ Cache
+ Neue Festplatte
SPEICHERN
SCHLIESSEN


Partition
OS
Name
Pop! OS
Version
22.04 LTS
Standard Start
Sync & start
Symbol
Basisimage
pop_os_mlm.qcow2
+
Start Optionen
Start
Sync & start
New start
Autostart
Autostart-Timeout
5

nehmen lassen. Das folgende Beispiel dient nur dazu, zu zeigen, was „unter der Decke“ passiert.

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
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
[Partition]
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 Gerätename darf nicht mit einem Bindestrich beginnen oder enden.

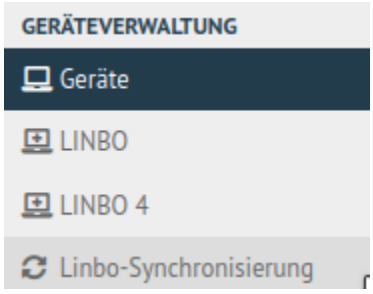
Für den Gerätenamen dürfen maximal 15-Zeichen verwendet werden.

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`.



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 Ende der Geräteliste eingefügt.

In der neuen Zeile gibst Du nun folgenes an:

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 UP 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:

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.

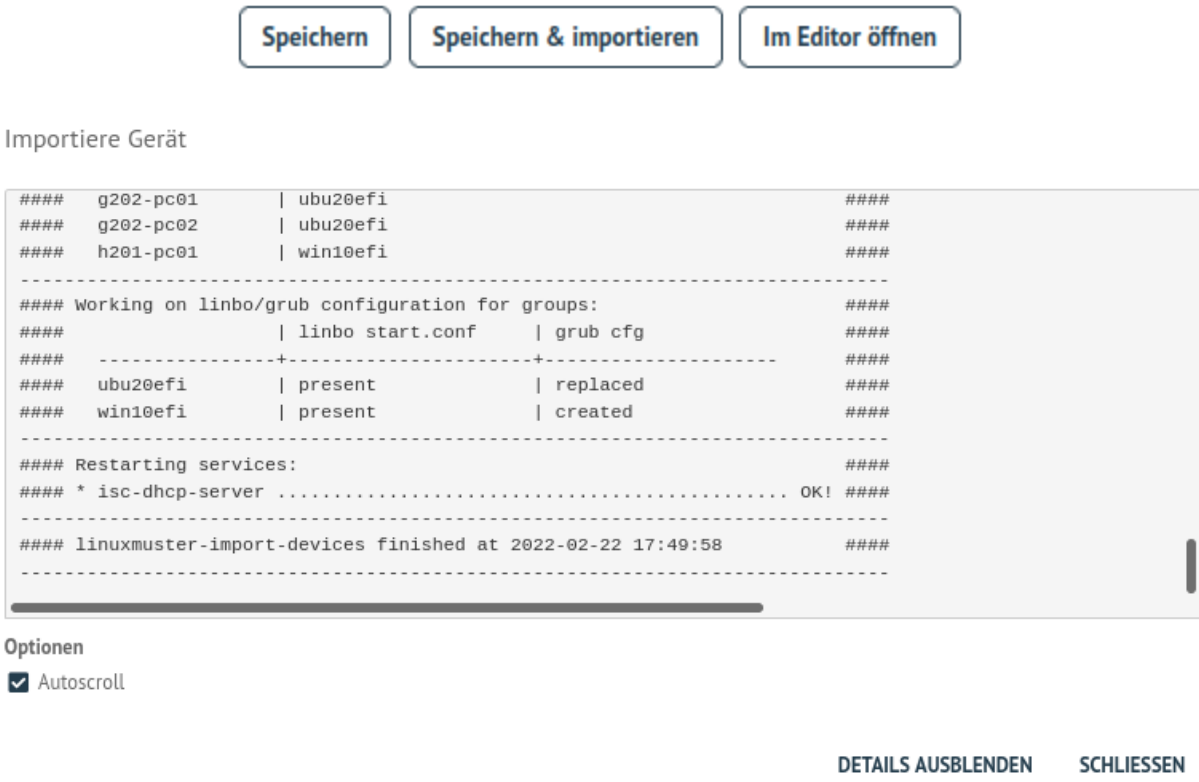
Im folgenden erscheinen einige Log-Meldungen und - wenn der Import erfolgreich war - „Import abgeschlossen“

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*

… 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:

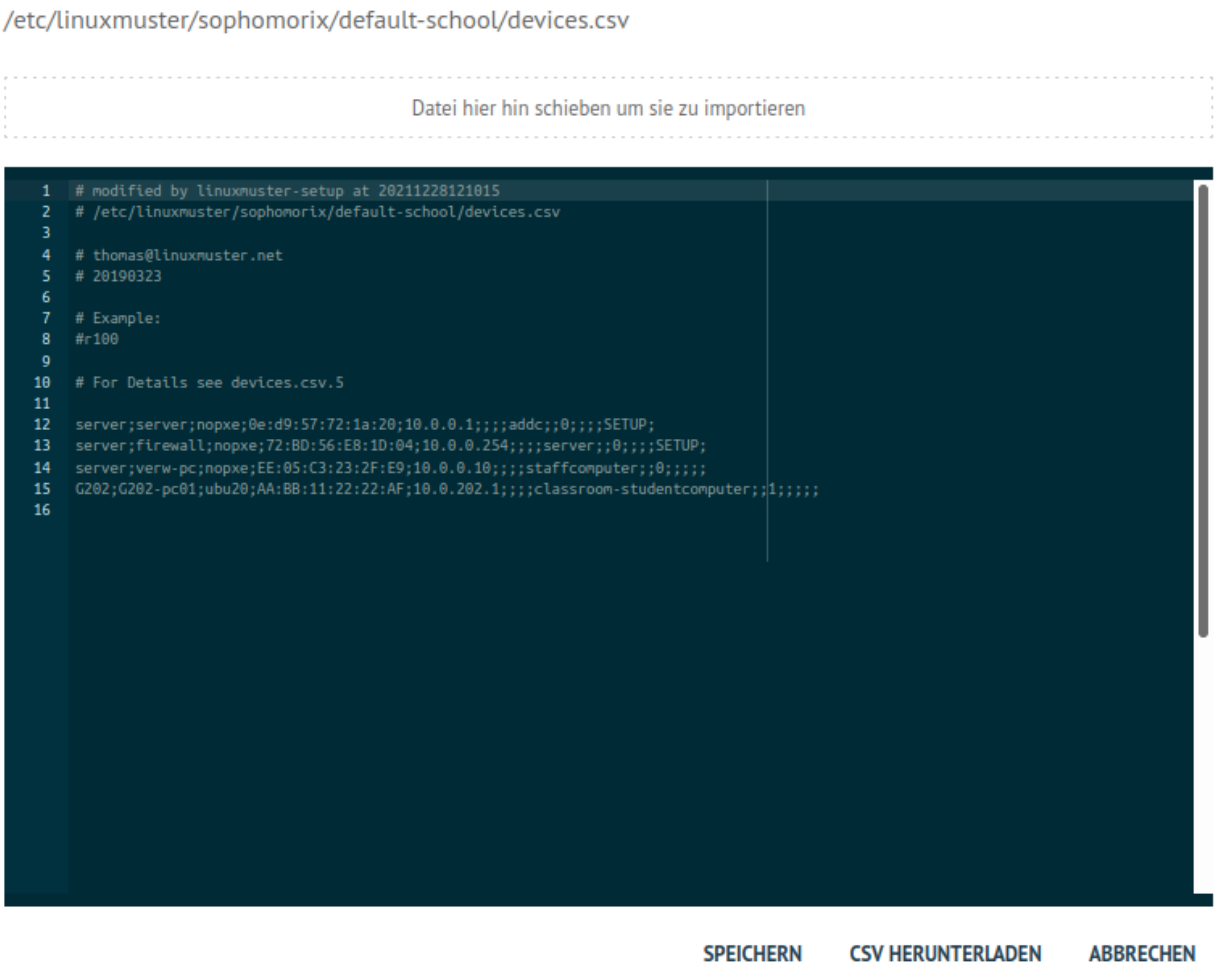
https://github.com/linuxmuster/sophomorix4/wiki/objectClasses

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
modified by linuxmuster-setup at 20211228121015
/etc/linuxmuster/sophomorix/default-school/devices.csv
thomas@linuxmuster.net
20190323
Example:
#r100
For Details see devices.csv.5
server;server;nopxe;0e:d9:57:72:1a:20;10.0.0.1;;;;addc;;0;;;;SETUP;
server;firewall;nopxe;72:BD:56:E8:1D:04;10.0.0.254;;;;server;;0;;;;SETUP;
server;verw-pc;nopxe;EE:05:C3:23:2F:E9;10.0.0.10;;;;staffcomputer;;0;;;;;
G202;G202-pc01;ubu20;AA:BB:11:22:22:AF;10.0.202.1;;;;classroom-studentcomputer;;1;;;;;
SPEICHERN
CSV HERUNTERLADEN
ABBRECHEN

... mittles LINBO

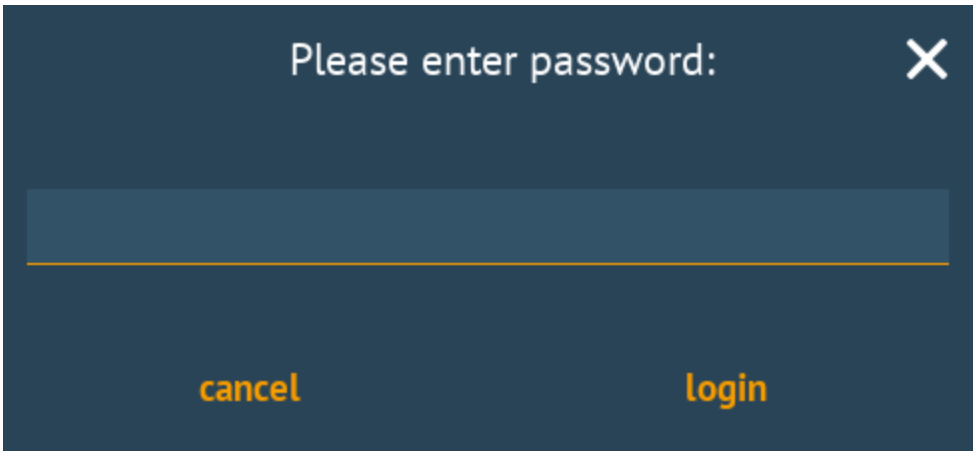
Wurde z.B. ein neuer Schulungsraum mit 20 PCs ausgestattet, deren MAC-Adressen Du nicht kennst, dann bietet sich diese Möglichkeit an.

Dazu hat sich folgendes Vorgehen bewährt:

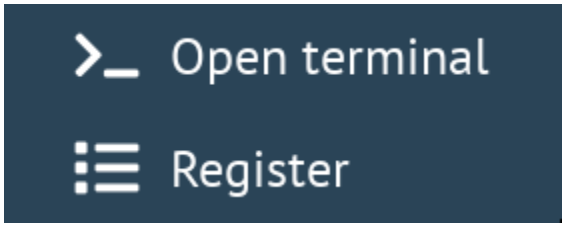
1. Der Clientrechner muss mit dem Schulnetzwerk verbunden sein und den Server erreichen können.
2. Um LINBO zu starten, den PC über das Netzwerk booten (PXE). Dazu entweder im BIOS-Setup in der Bootreihenfolge PXE-Boot als erstes Bootmedium einstellen oder über das Bootmenü PXE-Boot auswählen. Dies gelingt 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-Symvol 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:

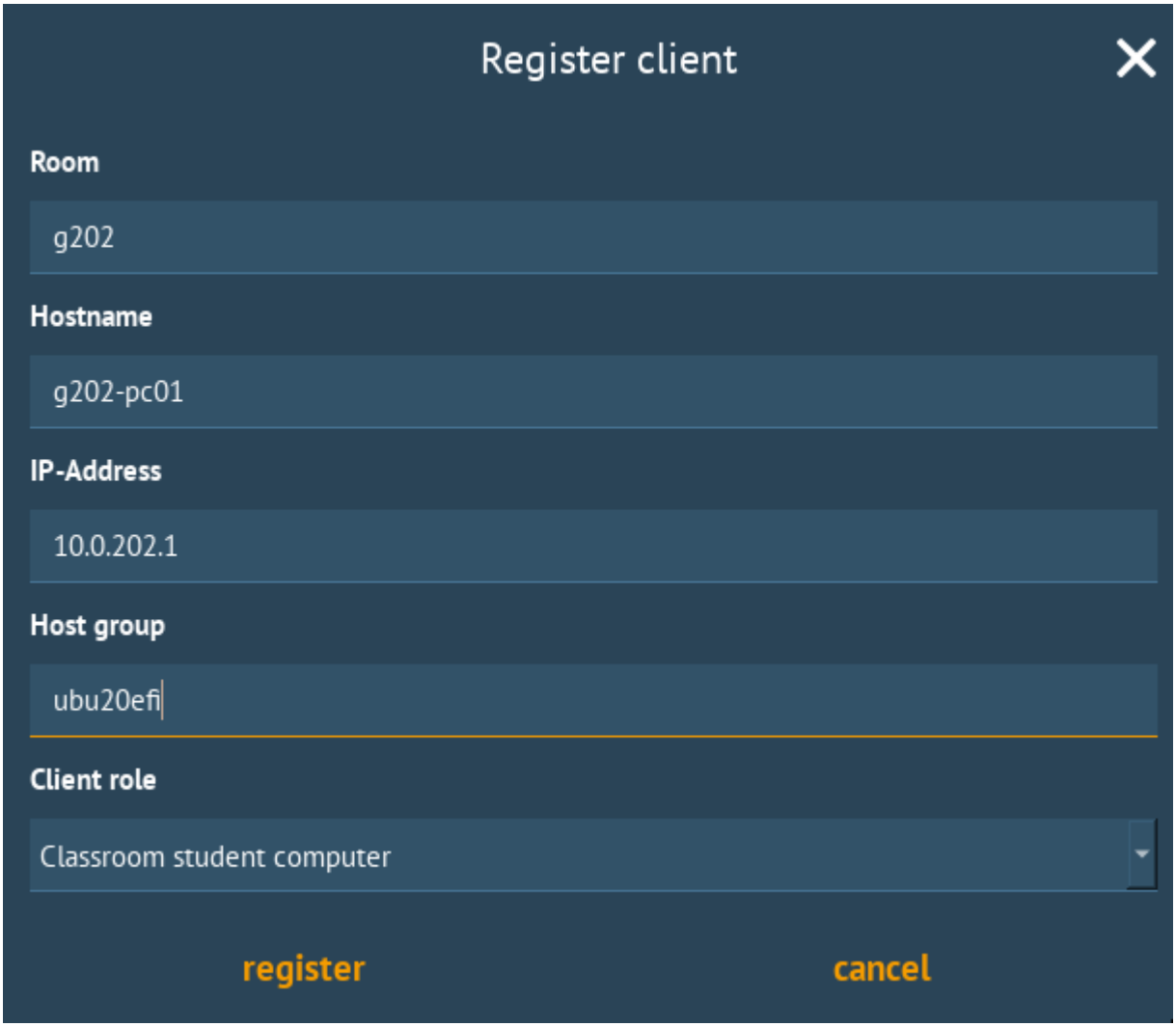


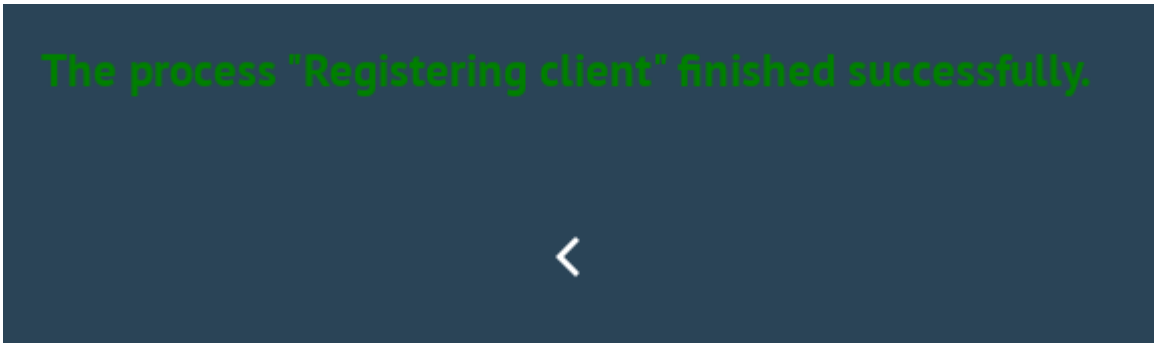
6. Wähle den Eintrag `Register` aus.
7. Es öffnet sich ein Fenster, um den Client zu registrieren. Fülle alle Felder aus. Achte darauf, dass Du als Host group die zuvor neu angelegte einträgst.
8. Klicke dann auf den Eintrag `register`. Nach Abschluss der Neuaufnahme siehst Du nachstehende Meldung:
9. 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 `Geräteverwwaltung --> Geräte` aus. Du siehst nun neben den schon vorhandenen Geräten ebenfalls die neu aufgenommen Geräte (in der Abb. sind dies die PCs für den Raum g202):
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*


Register client
Room
g202
Hostname
g202-pc01
IP-Address
10.0.202.1
Host group
ubu20efi
Client role
Classroom student computer
register
cancel


The process "Registering client" finished successfully.

Raum	Rechnername	Gruppe	MAC	IP	Sophomorix-Rolle	PXE
g202	g202-pc01	ubu20efi	F6:E8:B0	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

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

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 Sus) abbilden. linuxmuster.net ist darauf ausgelegt, als durchgängige Linux-Lösung genutzt zu werden. Hierzu wurden f?r 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 Schulkonsole oder der devices.csv aufgenommen/importiert.

Festplatte mit LINBO vorbereiten

Bevor Du mit der eigentlichen Installation des Client-Betriebssystem beginnen kannst, musst Du die Festplatte mittels LINBO vorbereiten. Dieses wird detailiert 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

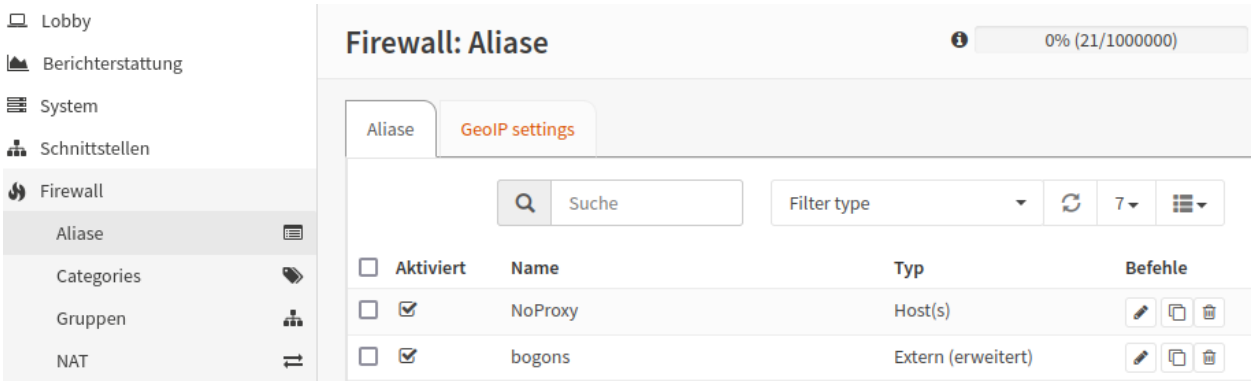
Für den Zeitraum der Installation und Aktualisierung des Muster-Clients ist es wichtig, dass dieser Internet-Zugriff hat, um Aktualisierungen laden zu können. Dazu ist es erforderlich, dass nachdem der Client als Gerät importiert wurde, Du die IP-Adresse des Gerätes in der sog. `NoProxy` Gruppe in der Firewall der OPNsense aufnimmst.

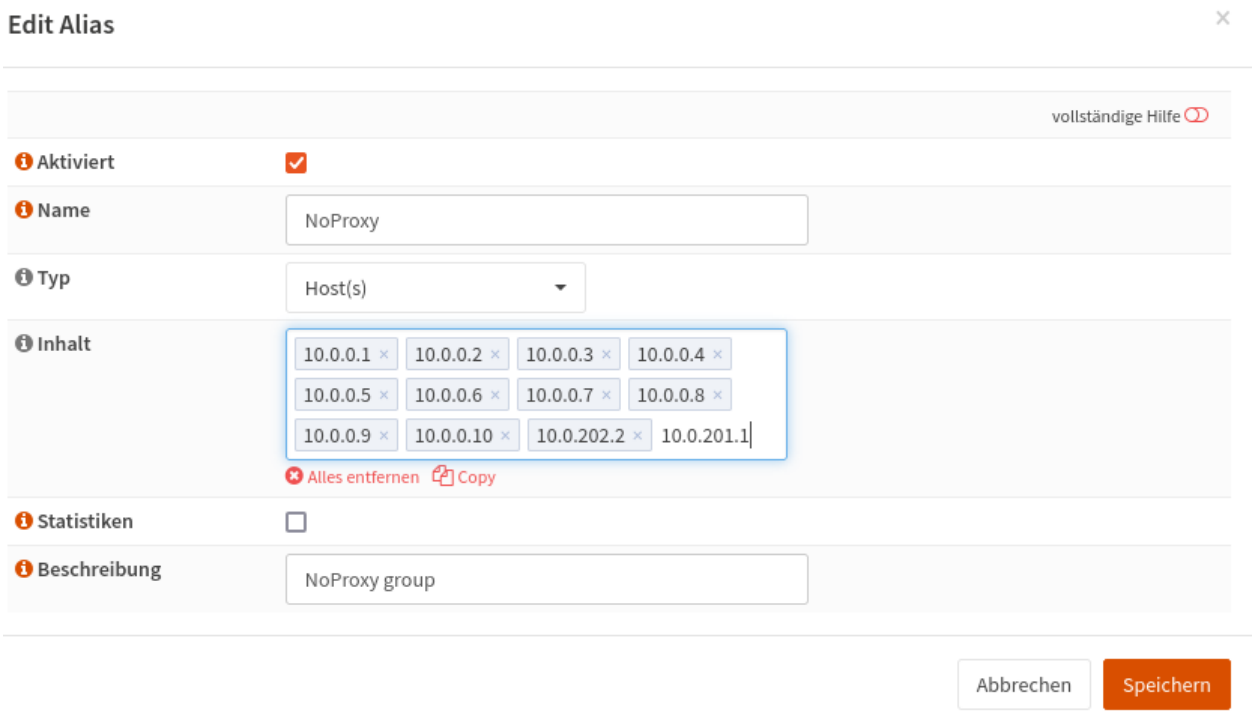
Dazu meldet Du Dich an der OPNsense als Benutzer `root` an und wählst links im Menü unter `Firewall -> Aliase` aus.

Du siehst dann anchstehende Firewall: Aliase.

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.

Bestätige die IP mit ENTER, so dass der Eintrag grau hinterlegt wird. Klicke zum Abschluss auf `Speichern`, um die Einstellungen zu übernehmen.


Lobby
Berichterstattung
System
Schnittstellen
Firewall
Aliase
Categories
Gruppen
NAT
Firewall: Aliase
0% (21/1000000)
Aliase
GeoIP settings
Suche
Filter type
7
Aktiviert
Name
Typ
Befehle
NoProxy
Host(s)
bogons
Extern (erweitert)


Edit Alias
vollständige Hilfe
Aktiviert
Name
NoProxy
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
10.0.202.2
10.0.201.1
Alles entfernen
Copy
Statistiken
Beschreibung
NoProxy group
Abbrechen
Speichern

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

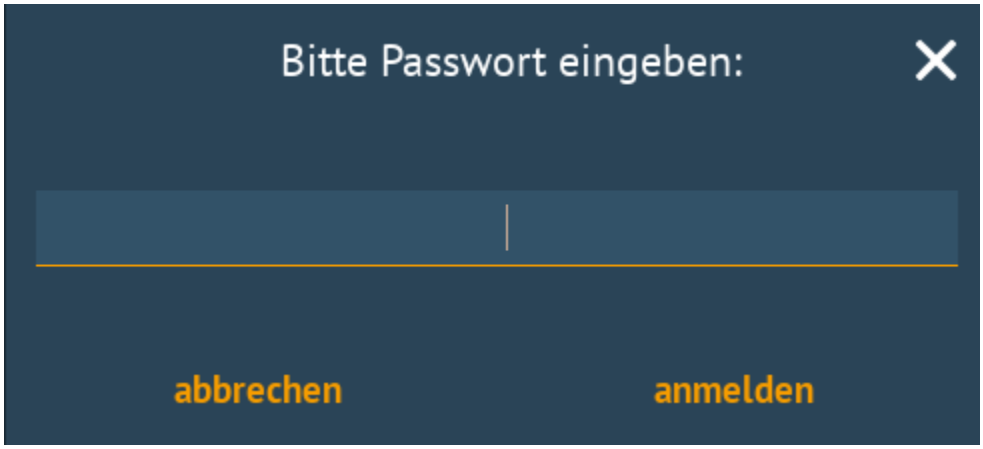
Autor des Abschnitts: @cweikl, @MachtDochNix (pics)

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 Windows 10):

Wähle nun das `Werkzeug-Symbol` rechts aus.

Es erscheint die Aufforderung, dass Du das LINBO-Passwort eingeben must. 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.

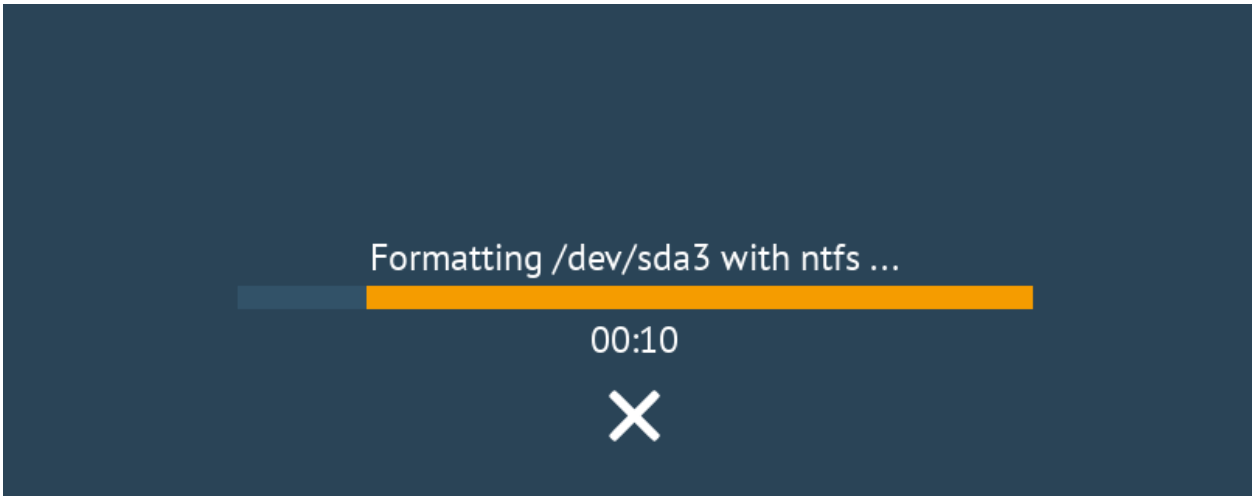

Bitte Passwort eingeben:
abbrechen
anmelden


LINBO
Windows 10
Terminal öffnen
Cache aktualisieren
Festplatte partitionieren
Registrieren

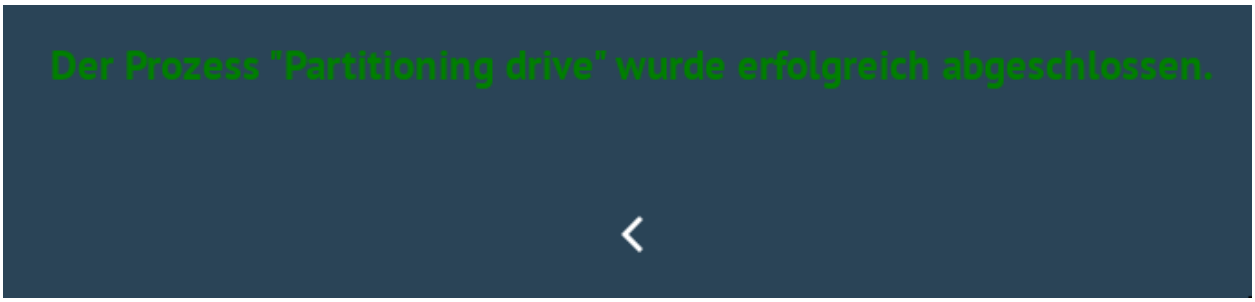
Wähle hier nun den Eintrag `Festplatte partitionieren` aus, damit die Festplatte Deines Clients wie zuvor in der Hardwareklasse angegeben, partitioniert und formatiert wird. Bevor der Vorgang angewendet wird, erhälst Du die Rückfrage, ob damit wirklich alle Daten auf dem Laufwerk gelöscht werden sollen.

Bestätige dies mit `Ja`.

Während der Partitionierung und Formatierung der Festplatte des Clients siehst Du eine Status-Anzeige.



Wurde der Vorgang abgeschlossen, so findest Du nachstehende Status-Meldung:



Klicke dann auf das Kleiner-Zeichen <.

Fahre nun den Client herunter, indem Du folgenden Button klickst:

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 automatisiert 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 augfgenommen
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.

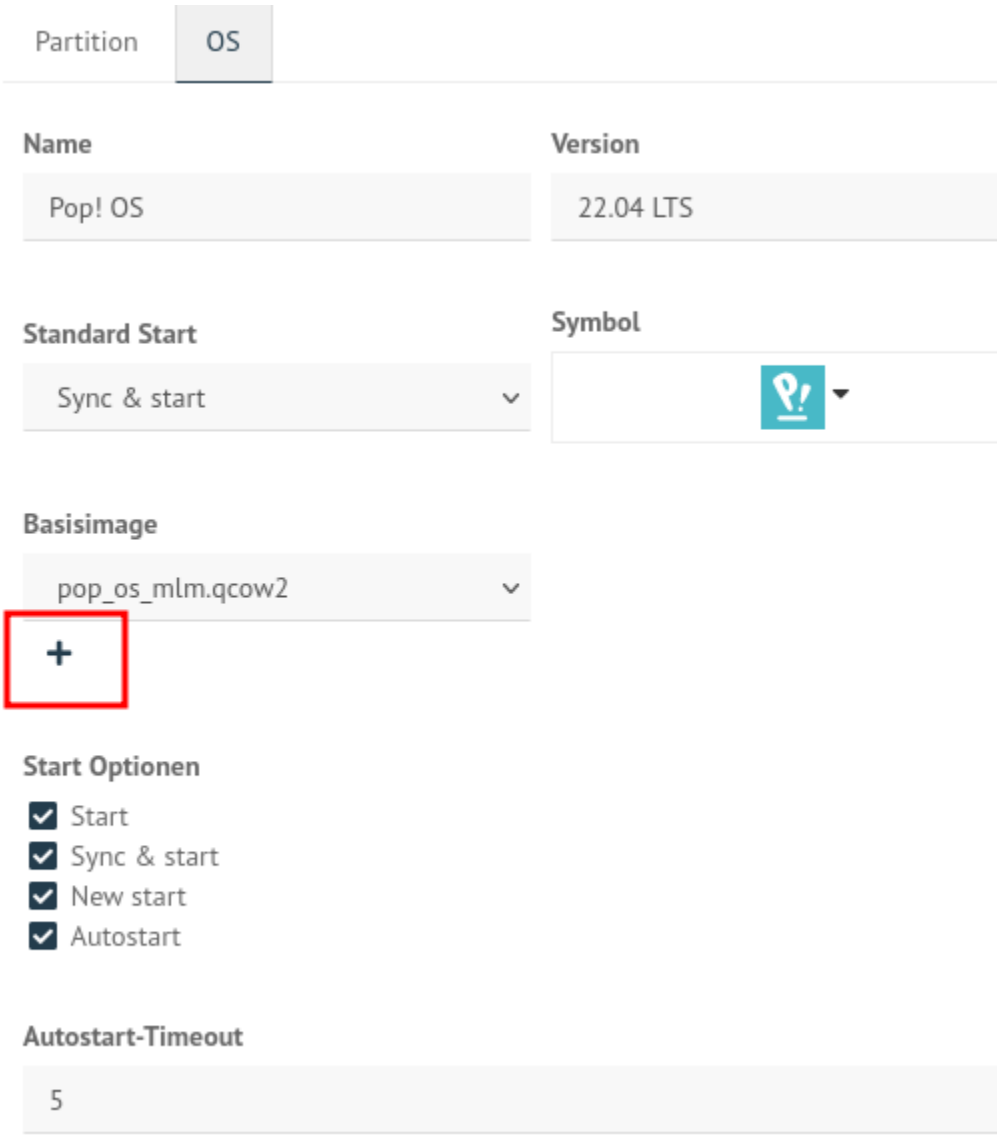
Einrichten eines Linux-Clients

Imagenamen eintragen (HWK)

Vor der Installation bzw. Imageerstellung musst Du eine Hardwareklasse 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 `Basisisimage` festzulegen. Alternativ kannst Du auch einen Nmane 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
Pop! OS
Version
22.04 LTS
Standard Start
Sync & start
Symbol
Basisimage
pop_os_mlm.qcow2
+
Start Optionen
Start
Sync & start
New start
Autostart
Autostart-Timeout
5

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.

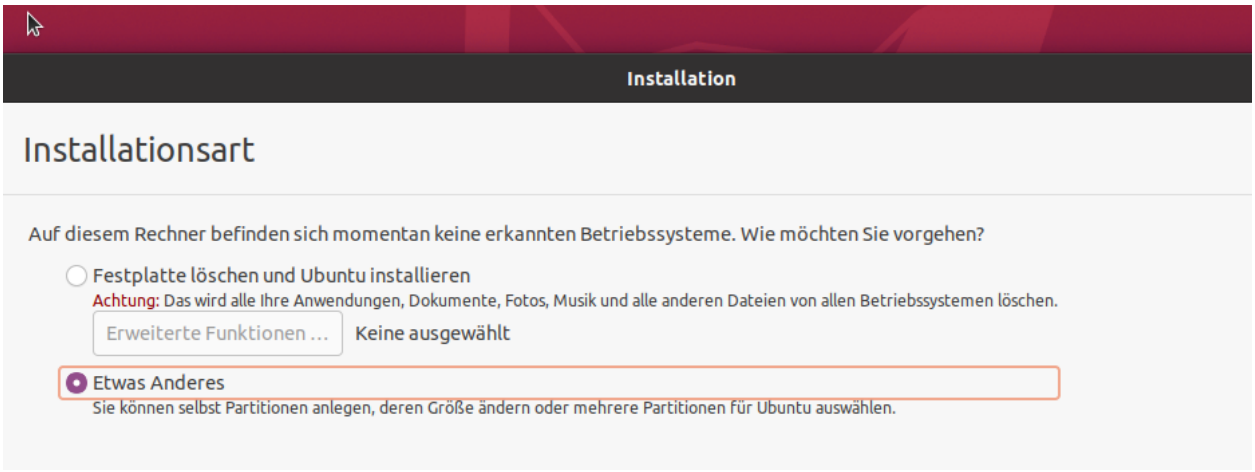
Möchtest Du pop!os installieren, so folge dieser Beschreibung *Linux-Client: Pop!_OS*

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!

Gib in den ersten Schritten der Installation die gewünschte Sprache und Tastaturbelegung an.

Bei der `Installationsart` wählst Du `Etwas Anderes` aus.



Du hattest mit Linbo ja 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/sda` und die Partionen als `/dev/sda1` etc. angezeigt werden.

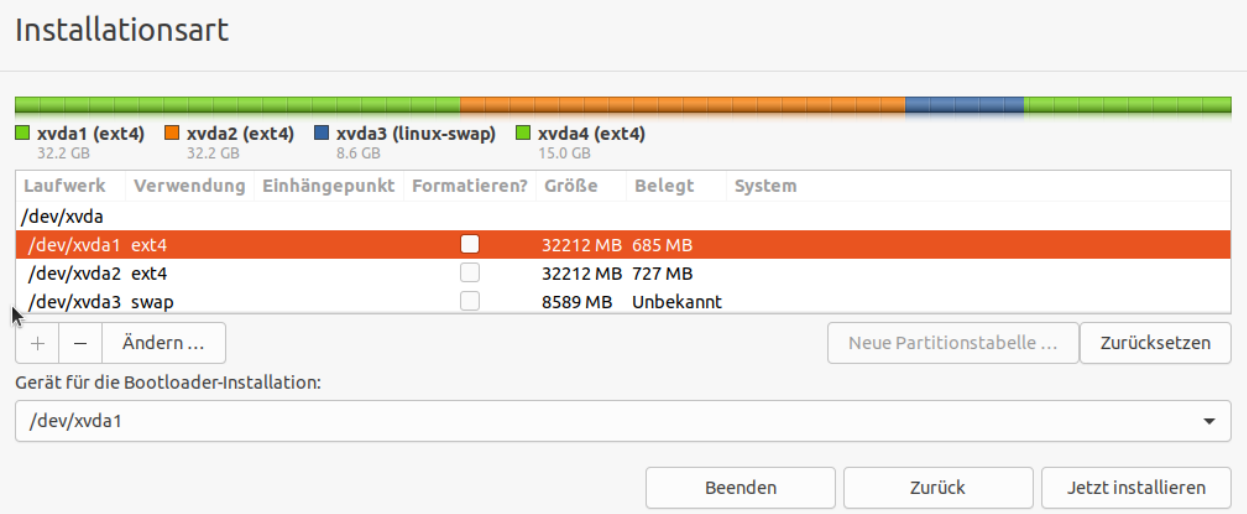
Wähle, wie in der nachstehenden Abb. zu sehen, die Partition aus, auf der Ubuntu installiert werden soll.

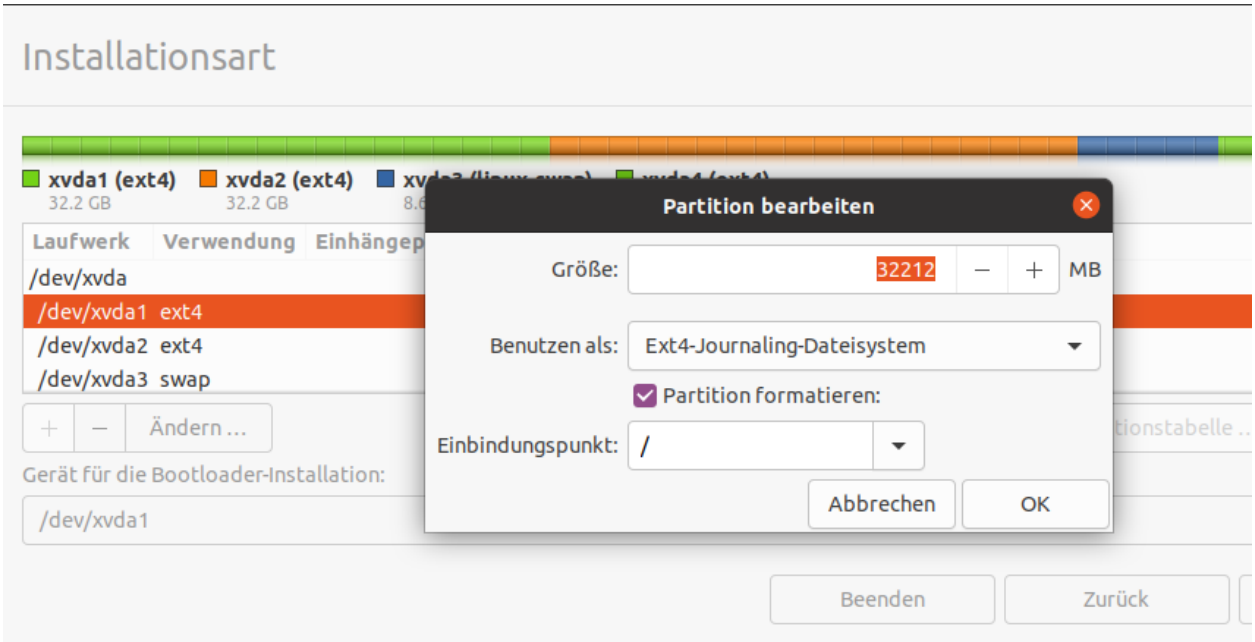
Klicke nun auf `Ändern` und es erscheint das nächste Fenster:

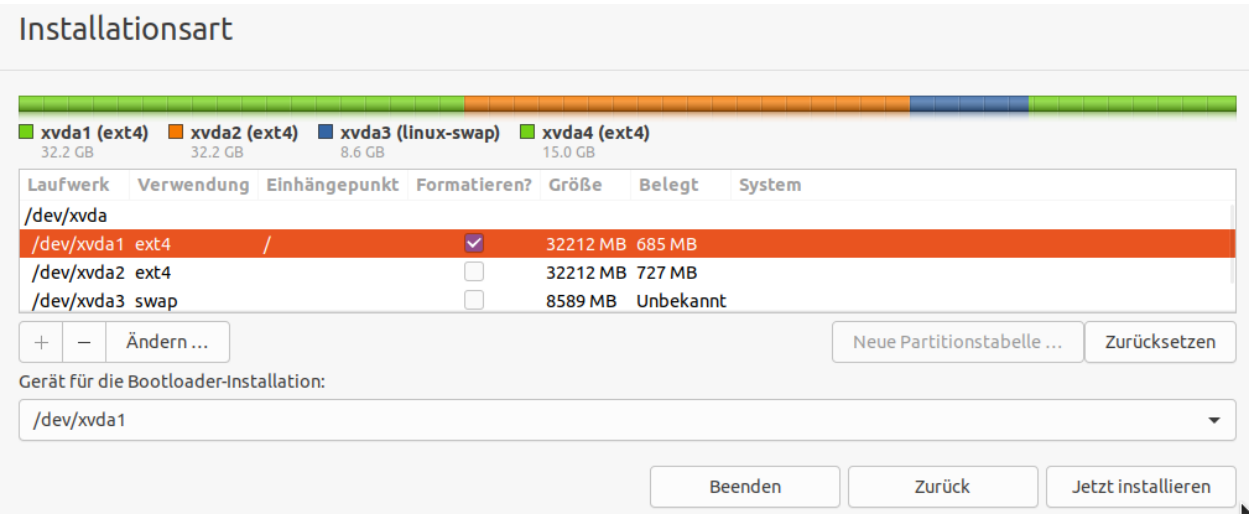
Belasse die angezeigte Größe und das Dateisystem. Setze den Haken bei `Partition formatieren` und wähle als `Einbindungspunkt` das Root-Verzeichnis `/` aus.

Klicke auf `ok` und es werden nochmals alle Einstellungen angezeigt:

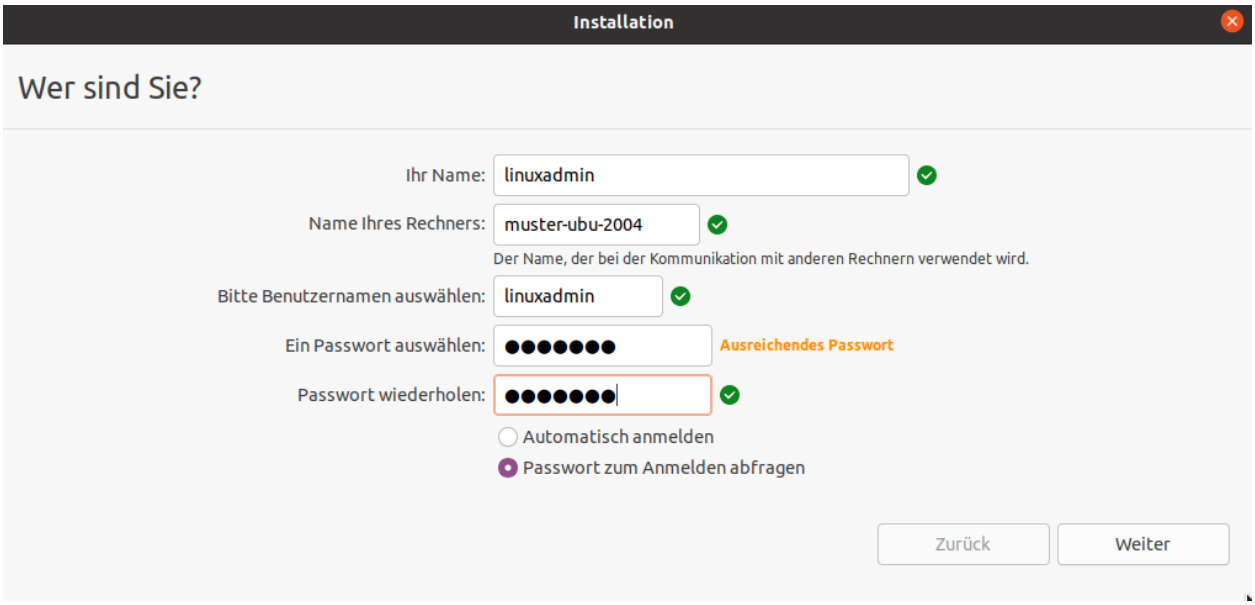
Sind diese Einstellungen korrekt, so setze die Installation mit dem Button `Jetzt installieren` fort.


Installationsart
xvda1 (ext4) 32.2 GB
xvda2 (ext4) 32.2 GB
xvda3 (linux-swap) 8.6 GB
xvda4 (ext4) 15.0 GB
Laufwerk Verwendung Einhängepunkt Formatieren? Größe Belegt System
/dev/xvda
/dev/xvda1 ext4 32212 MB 685 MB
/dev/xvda2 ext4 32212 MB 727 MB
/dev/xvda3 swap 8589 MB Unbekannt
Ändern ...
Neue Partitionstabelle ...
Zurücksetzen
Gerät für die Bootloader-Installation:
/dev/xvda1
Beenden
Zurück
Jetzt installieren


Installationsart
xvda1 (ext4) 32.2 GB
xvda2 (ext4) 32.2 GB
Partition bearbeiten
Größe: 32212 MB
Benutzen als: Ext4-Journaling-Dateisystem
Partition formatieren:
Einbindungspunkt: /
Abbrechen
OK
Laufwerk Verwendung
/dev/xvda
/dev/xvda1 ext4
/dev/xvda2 ext4
/dev/xvda3 swap
Ändern ...
Gerät für die Bootloader-Installation:
/dev/xvda1
Beenden
Zurück


Installationsart
xvda1 (ext4) 32.2 GB
xvda2 (ext4) 32.2 GB
xvda3 (linux-swap) 8.6 GB
xvda4 (ext4) 15.0 GB
Laufwerk Verwendung Einhängepunkt Formatieren? Größe Belegt System
/dev/xvda
/dev/xvda1 ext4 / 32212 MB 685 MB
/dev/xvda2 ext4 32212 MB 727 MB
/dev/xvda3 swap 8589 MB Unbekannt
Ändern ...
Neue Partitionstabelle ...
Zurücksetzen
Gerät für die Bootloader-Installation:
/dev/xvda1
Beenden
Zurück
Jetzt installieren

Im Verlauf der Installation wirst Du nach dem Namen für den Computer und dem Benutzername 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

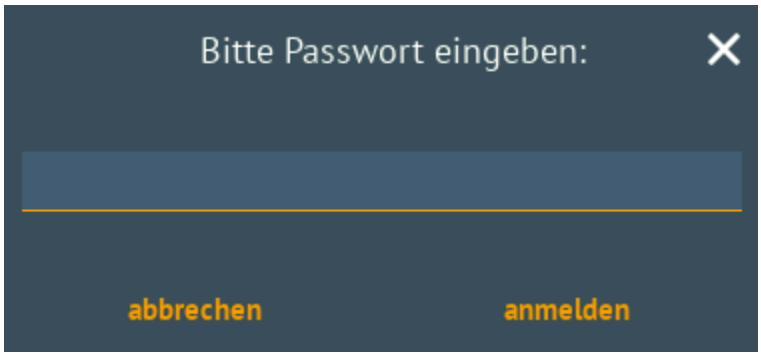
Passe die Boot-Reihenfolge für den PC / die VM jetzt so an, dass diese wieder via PXE bootet. Du siehst dann die Startoptionen in Linbo für das installierte Ubuntu 20.04.

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:


Bitte Passwort eingeben:
abbrechen
anmelden


Ubuntu
Terminal öffnen
Cache aktualisieren
Festplatte partitionieren
Registrieren

Klicke auf das große Festplatten-Icon, das in der Ecke rechts unten farblich markiert ist, um nun ein Image zu erstellen. Anstatt des Festplatten-Icons wird bei Dir eventuell das Icon des Betriebssystems angezeigt, dass Du in der WebUI festgelegt hast.

Es wird ein neues Fenster geöffnet:

Wähle aus, dass Du das aktuelle Image ersetzen möchtest. Gibt es das Image noch nicht, so wird ein neues Image mit dem zuvor in der WebUI festgelegten Namen erstellt.

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 Icon von den drei Icsons ganz rechts, um sich abzumelden.

Du siehst nun drei Start-Icons. Der grosse Icons started das Image sychronisiert, während das grüne Icon das locale Image started.

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 7.1 Repository ein.
3. Installiere 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 7.1 Repository:

```
sudo wget -qO- "https://deb.linuxmuster.net/pub.gpg" | gpg --dearmour -o /usr/share/
↪keyrings/linuxmuster.net.gpg
```

2. Schritt

Trage das linuxmuster.net 7.1 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`.

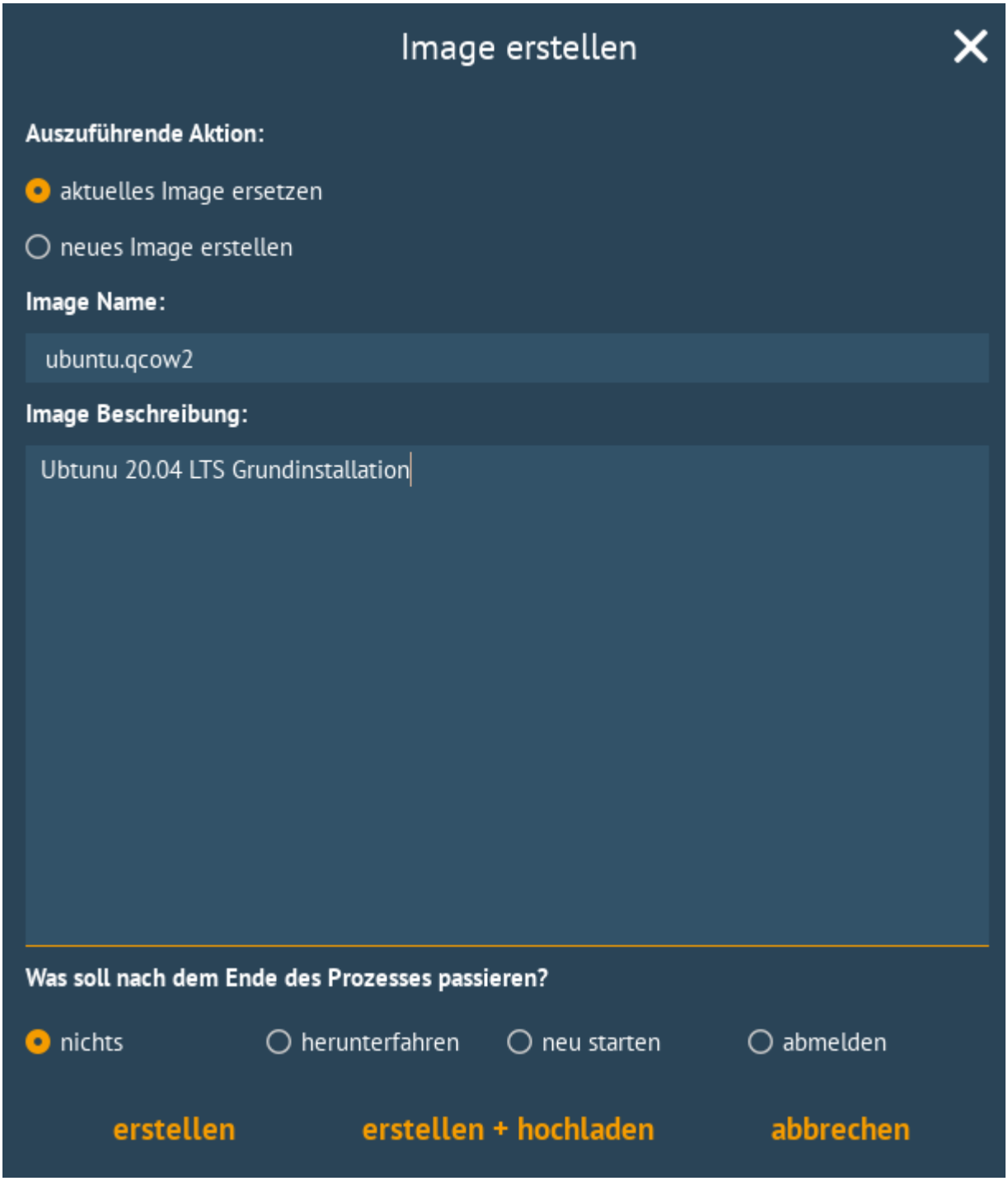
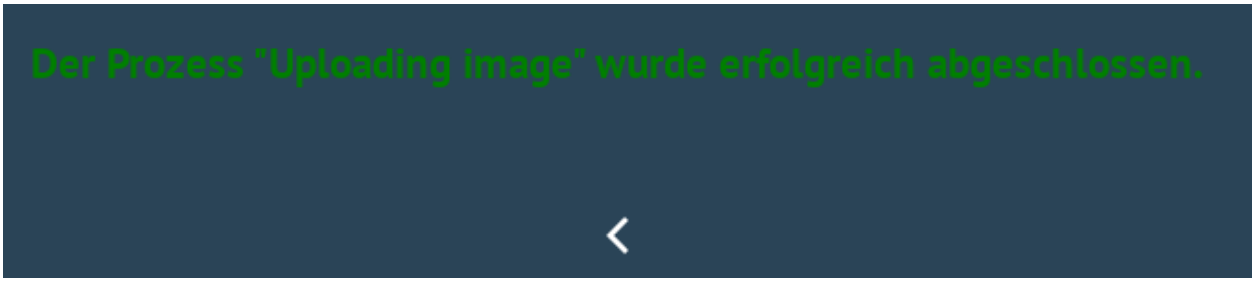
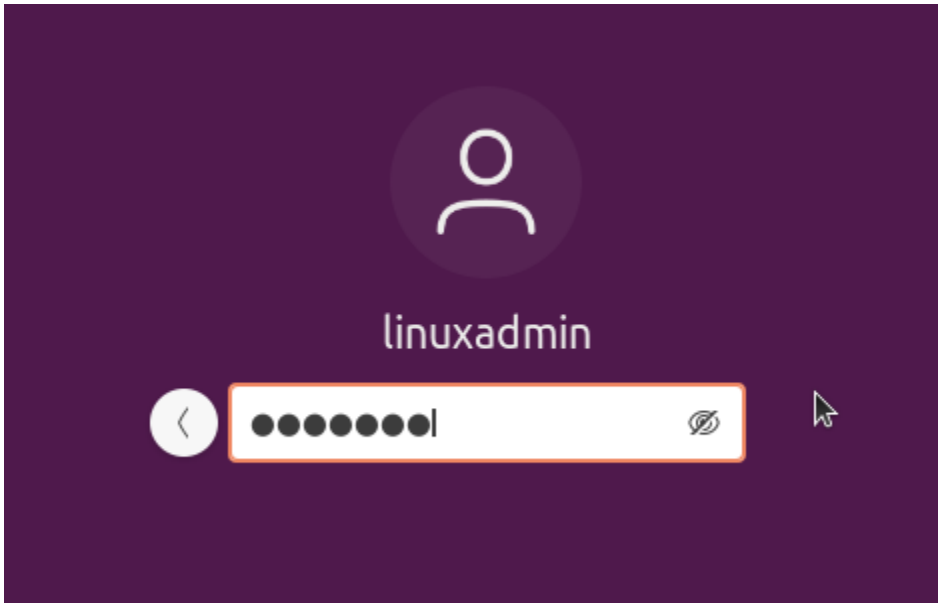


Image erstellen
Auszuführende Aktion:
aktuelles Image ersetzen
neues Image erstellen
Image Name:
ubuntu.qcow2
Image Beschreibung:
Ubtunu 20.04 LTS Grundinstallation
Was soll nach dem Ende des Prozesses passieren?
nichts
herunterfahren
neu starten
abmelden
erstellen
erstellen + hochladen
abbrechen


LINBO
(24.01/100%)
04:03
LINBO 4.0.4-0: Subterranean Homesick Blues- GUI 7.0.4 - 10.0.202.2 - F1
by linuxmuster.net


Der Prozess "Uploading image" wurde erfolgreich abgeschlossen.


Ubuntu


linuxadmin

3. Schritt

Führe 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 daruch 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. Achte hierbei darauf, dass Du dieses Mal `aktuelles Image ersetzen` auswählst.

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. Auch hier: `aktuelles Image ersetzen` auswählen.

Serverseitige Anpassungen

Damit der Linux-Client die Drucker automatisch ermittelt und der Proxy korrekt eingerichtet wird, ist es erforderlich, dass auf dem linuxmuster Server einige Anpassungen vorgenommen werden.

Proxy-Einstellungen

Bei der Anmeldung vom Linux-Client werden sog. Hook-Skripte ausgeführt.

Diese finden sich auf dem linuxmuster 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 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/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:$PROXY_PORT
lmn-export ftp_proxy=$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. Tut man dies nicht, werden auf jedem Rechner ALLE Drucker angezeigt, nicht nur die ihm zugeteilten.

Weiterführende Dokumentation

- Entwicklerdokumentation
- *LINBO4 nutzen*

Linux-Client: Pop!_OS

Autor des Abschnitts: @cweikl,

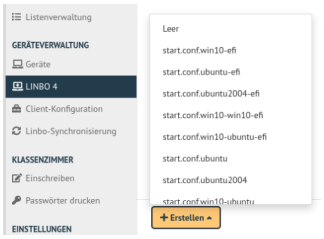
Hast Du alle Vorarbeiten wie im Kapitel *Linux-Client* ausgeführt, startetst Du nun den PC/die VM von CD/DVD/USB-Stick mit Pop!_OS.

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/20/pop-os_22.04_amd64_intel_20.iso

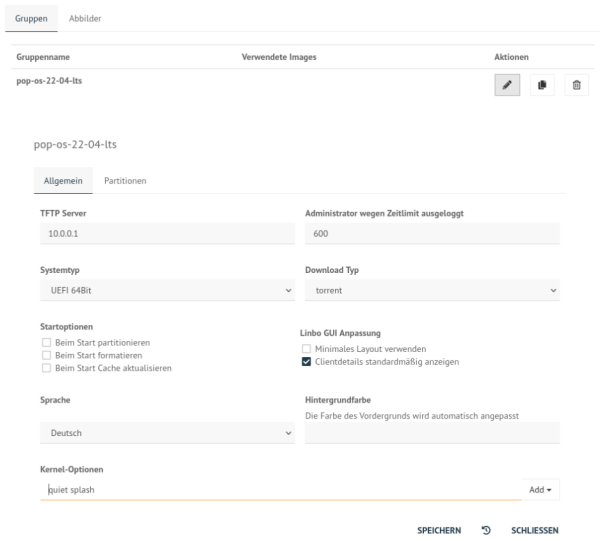
Zur Erinnerung - folgende Vorarbeiten sollten bereits erledigt sein:

1. Lege in der WebUI unter LINBO4 eine neue Hardbareklasse (HWK) an.

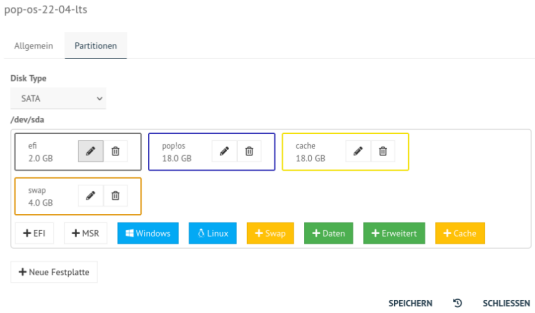


2. Vergebe für die HWK einen eindeutigen Namen.

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 Abbldung.

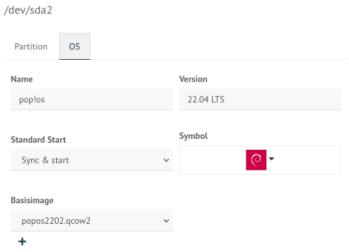


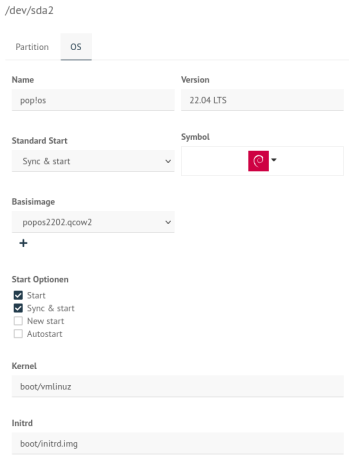
Hinweis: Bei pop!os sollte darauf geachtet werden, dass bei UEFI-System die EFI-Partition eine Größe von mind. 1 GiB aufweist!

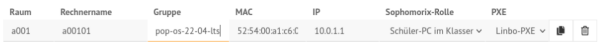
6. Bearbeite die Partition pop!os mit dem Stift und gebe auf der Reiterkarte `OS` einen eindeutigen Namen an. Lege den Namen für der Basisimage fest. Dies erreichst Du über das +-Symbol und der Angabe eines neuen Namens, der auf .qcow2 enden muss. Danach kannst Du diesen aus der Dropdwon-Liste auswählen.

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.

7. Gebe in der WebUI für diesen PC als Gruppe die neu angelegte HWK - hier pop-os-22-04-lts - an und klicke auf `Spechern & importieren`.
8. Starte danach den Client via PXE und LINBO.
9. Klicke auf das Werkzeugsymbol, authentifiziere Dich mit dem Kennwort das 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.


/dev/sda2
Partition
OS
Name
pop!os
Version
22.04 LTS
Standard Start
Sync & start
Symbol
Basisimage
popos2202.qcow2


/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

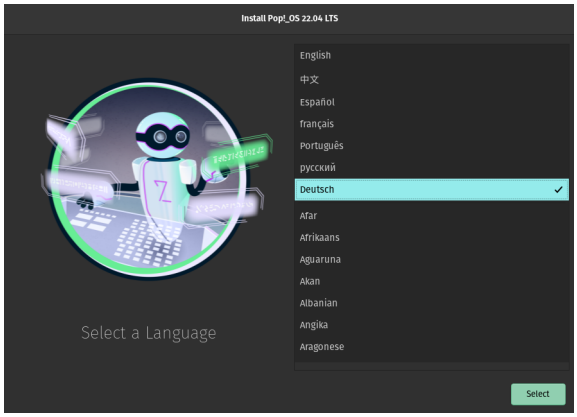

Raum
Rechnername
Gruppe
MAC
IP
Sophomorix-Rolle
PXE
a001
a00101
pop-os-22-04-lts
10.0.1.1
Schüler-PC im Klasser
Linbo-PXE


LINBO
pop!os
LINBO 4.0.42-0: Subterranean Homesick Blues- GUI 7.0.6 - 10.0.1.1 - F1
by linuxmusternet
Hostname: a00101
Host-Gruppe:
IP-Adresse: 10.0.1.1
Mac: 52:54:00:A1:C6:06


pop!os
Terminal öffnen
Cache aktualisieren
Festplatte partitionieren
Registrieren

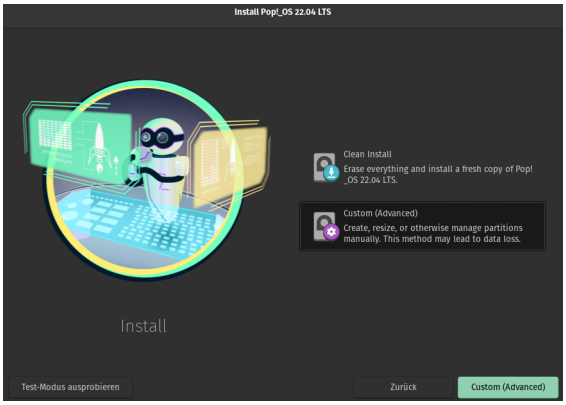
Installation Pop!_OS

Nach dem Start von dem Installationsmedium erhälst Du den Hinweis, dass Pop!_OS gestartet wird. Es kann einige Zeit dauern, bis Du den grafischen Installations-Bildschirm siehst.



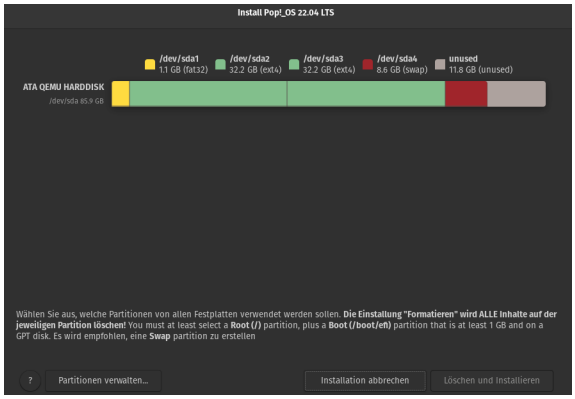
Wähle die gewünschte Sprache und bestätige dies mit `Select`.

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.

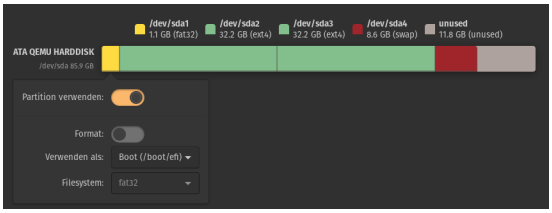
Du gelangst zu nachstehendem Bildschirm, in dem Dur Deine bisherigen Partitionen angezeigt werden.



Du hattest mit Linbo ja bereits die Festplatte partitioniert und formatiert.

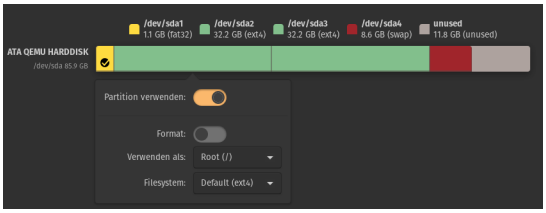
Es werden Dir also die bereits vorhandenen Partitionen und Dateisysteme angezeigt. Je nach genutzter Virtualisierungsumgebung / Hardware können die Festplattenbezeichnungen hier auch als `/dev/vda` und die Partionen als `/dev/vda1` etc. angezeigt werden.

Markiere zunächst Die EFI-Partition (gelb) und geben an, dass diese Partition verwendet werden soll.



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.



Klicke abschliessend auf die SWAP-Partition (rot) und binde diese als Swap ein.

Danach siehst Du Deine einegbundenden Partitionen, die jeweils mit einem Häkchen gekennzeichnet sind.

Starte die Installation mit dem Button `Löschen und installieren`.

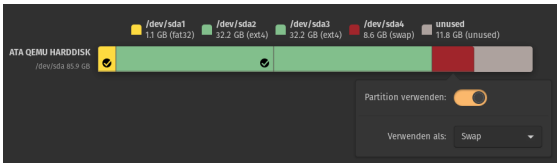
Danach musst Du noch einen neuen Benutzer `linuxadmin` festlegen.

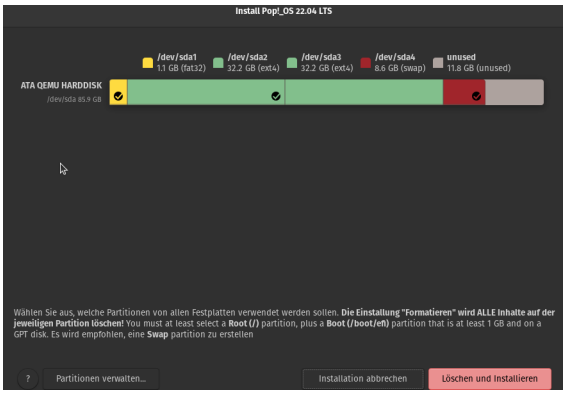
Lege für den neuen Benutzer ein Kennwort fest, das mind. 8 Zeichen aufweist.

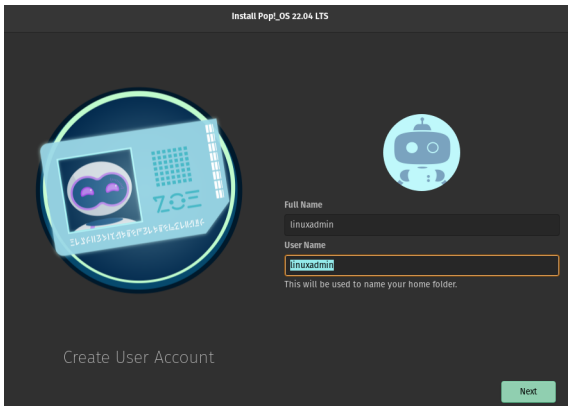
Bestätige dies mit `Next`. Danach startet die Installation.

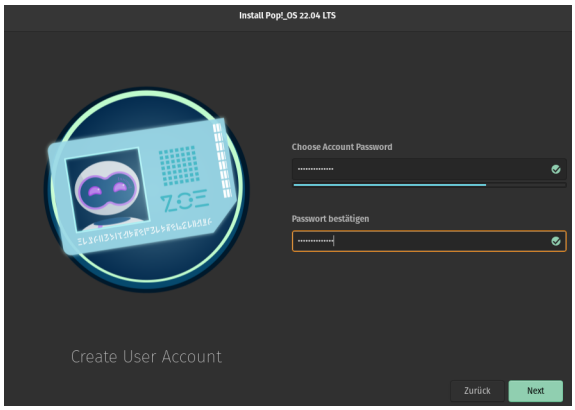
Gelangst Du nach erfolgreicher Installation zunm Abschluss-Bildschirm, so wähle hier `Herunterfahren` aus.

Werfe das Installationsmedium aus.


/dev/sda1
1.1 GB (fat32)
/dev/sda2
32.2 GB (ext4)
/dev/sda3
32.2 GB (ext4)
/dev/sda4
8.6 GB (swap)
unused
11.8 GB (unused)
ATA QEMU HARDDISK
/dev/sda 85.9 GB
Partition verwenden:
Verwenden als:
Swap


Install Pop!_OS 22.04 LTS
/dev/sda1
1.1 GB (fat32)
/dev/sda2
32.2 GB (ext4)
/dev/sda3
32.2 GB (ext4)
/dev/sda4
8.6 GB (swap)
unused
11.8 GB (unused)
ATA QEMU HARDDISK
/dev/sda 85.9 GB
Wählen Sie aus, welche Partitionen von allen Festplatten verwendet werden sollen. Die Einstallung "Formatieren" wird ALLE Inhalte auf der jeweiligen Partition löschen! You must at least select a Root (/) partition, plus a Boot (/boot/efi) partition that is at least 1 GB and on a GPT disk. Es wird empfohlen, eine Swap partition zu erstellen
Partitionen verwalten...
Installation abbrechen
Löschen und Installieren


Install Pop!_OS 22.04 LTS
Full Name
linuxadmin
User Name
linuxadmin
This will be used to name your home folder.
Create User Account
Next


Install Pop!_OS 22.04 LTS
Choose Account Password
Passwort bestätigen
Create User Account
Zurück
Next

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-Icon, das in der Ecke rechts unten farblich markiert ist, um nun ein Image zu erstellen. Anstatt des Festplatten-Icons wird bei Dir eventuell das Icon des Betriebssystems angezeigt, dass Du in der WebUI festgelegt hast.

Es wird ein neues Fenster geöffnet:

Wähle aus, dass Du das aktuelle Image ersetzen möchtest. Gibt es das Image noch nicht, so wird ein neues Image mit dem zuvor in der WebUI festgelegten Namen erstellt. Starte den Vorgang mit `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 melde Dich ab.


pop!os
Terminal öffnen
Cache aktualisieren
Festplatte partitionieren
Registrieren

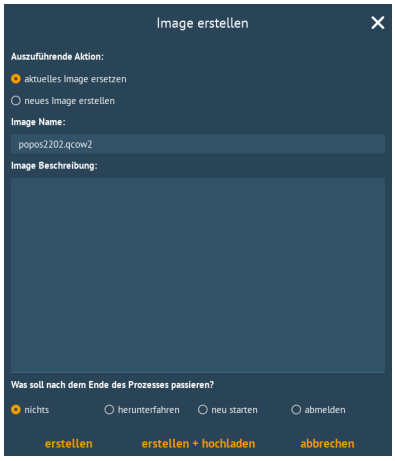


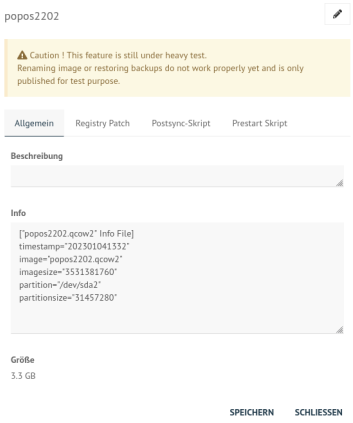
Image erstellen
Auszuführende Aktion:
aktuelles Image ersetzen
neues Image erstellen
Image Name:
popos2202.qcow2
Image Beschreibung:
Was soll nach dem Ende des Prozesses passieren?
nichts
herunterfahren
neu starten
abmelden
erstellen
erstellen + hochladen
abbrechen


LINBO
(6.00/100%)
01:49
LINBO 4.0.42-0: Subterranean Homesick Blues- GUI 7.0.6 - 10.0.1.1 - F1
by linuxmuster.net


Der Prozess "Uploading image" wurde erfolgreich abgeschlossen.
LINBO 4.0.42-0: Subterranean Homesick Blues- GUI 7.0.6 - 10.0.1.1 - F1
by linuxmuster.net

Rufst Du mit der WebUI denMenüpunkt `Geräteverwaltung --> LINBO4` auf, siehst Du Deine HWK. Klickst Du hier auf die Reiterkarte `Abbiler`, 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 mithile 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
# 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
```

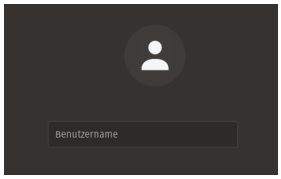
Hier musst Du ebenfalls UUID-Einträge durch die Angabe der SWAP-Partition ersetzen.

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.



Installiere das Paket `linuxmuster-linuxclient7` wie folgt:

1. Importiere den GPG-Schlüssel des linuxmuster.net Respository.
2. Trage das linuxmuster.net 7.1 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 7.1 Repository:

```
sudo wget -qO- "https://deb.linuxmuster.net/pub.gpg" | gpg --dearmour -o /usr/share/
↪keyrings/linuxmuster.net.gpg
```

2. Schritt

Trage das linuxmuster.net 7.1 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 daruch 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. Achte hierbei darauf, dass Du dieses Mal `aktuelles Image ersetzen` auswählst.

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. Auch hier: `aktuelles Image ersetzen` auswählen.

Serverseitige Anpassungen

Damit der Linux-Client die Drucker automatisch ermittelt und der Proxy korrekt eingerichtet wird, ist es erforderlich, dass auf dem linuxmuster Server einige Anpassungen vorgenommen werden.

Proxy-Einstellungen

Bei der Anmeldung vom Linux-Client werden sog. Hook-Skripte ausgeführt.

Diese finden sich auf dem linuxmuster 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)
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:$PROXY_PORT
lmn-export ftp_proxy=$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. Tut man dies nicht, werden auf jedem Rechner ALLE Drucker angezeigt, nicht nur die ihm zugeteilten.

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:

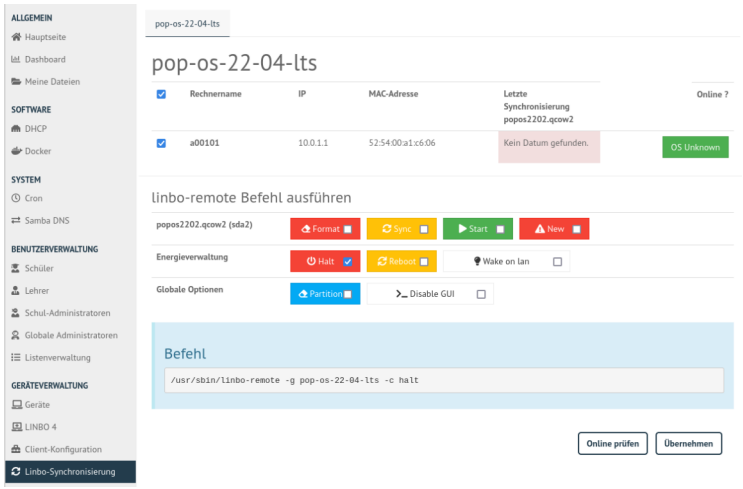
```
[LINBO]
Server = 10.0.0.1
Group = pop-os-22-04-lts
Cache = /dev/sda3
RootTimeout = 600
AutoPartition = no
AutoFormat = no
AutoInitCache = no
GuiDisabled = no
UseMinimalLayout = no
Locale = de-DE
DownloadType = torrent
SystemType = efi64
KernelOptions = quiet splash
clientDetailsVisibleByDefault = yes

[Partition]
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
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
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.



Windows 10 Clients

Autor des Abschnitts: @cweikl, @MachtDochNix (pics)

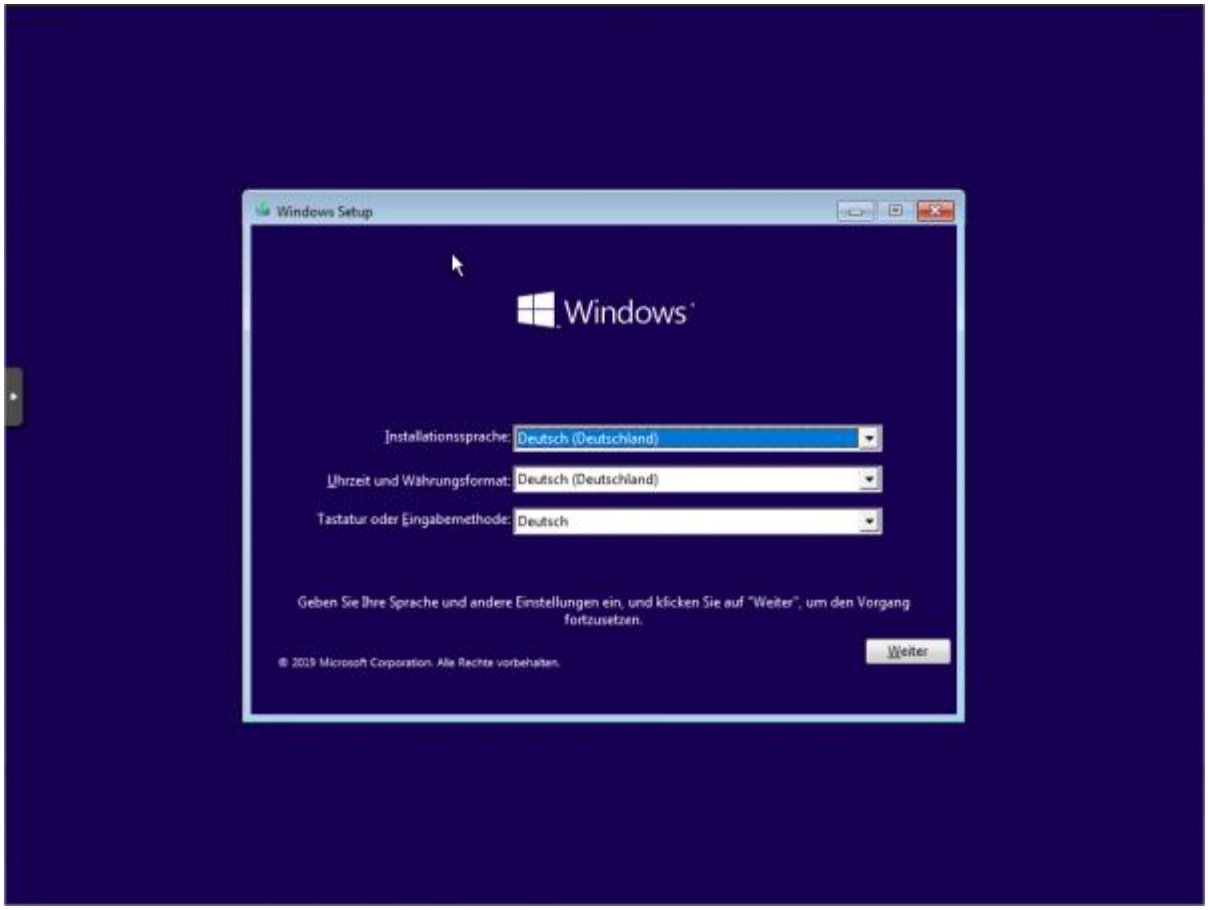
Betriebssystem Windows 10 installieren

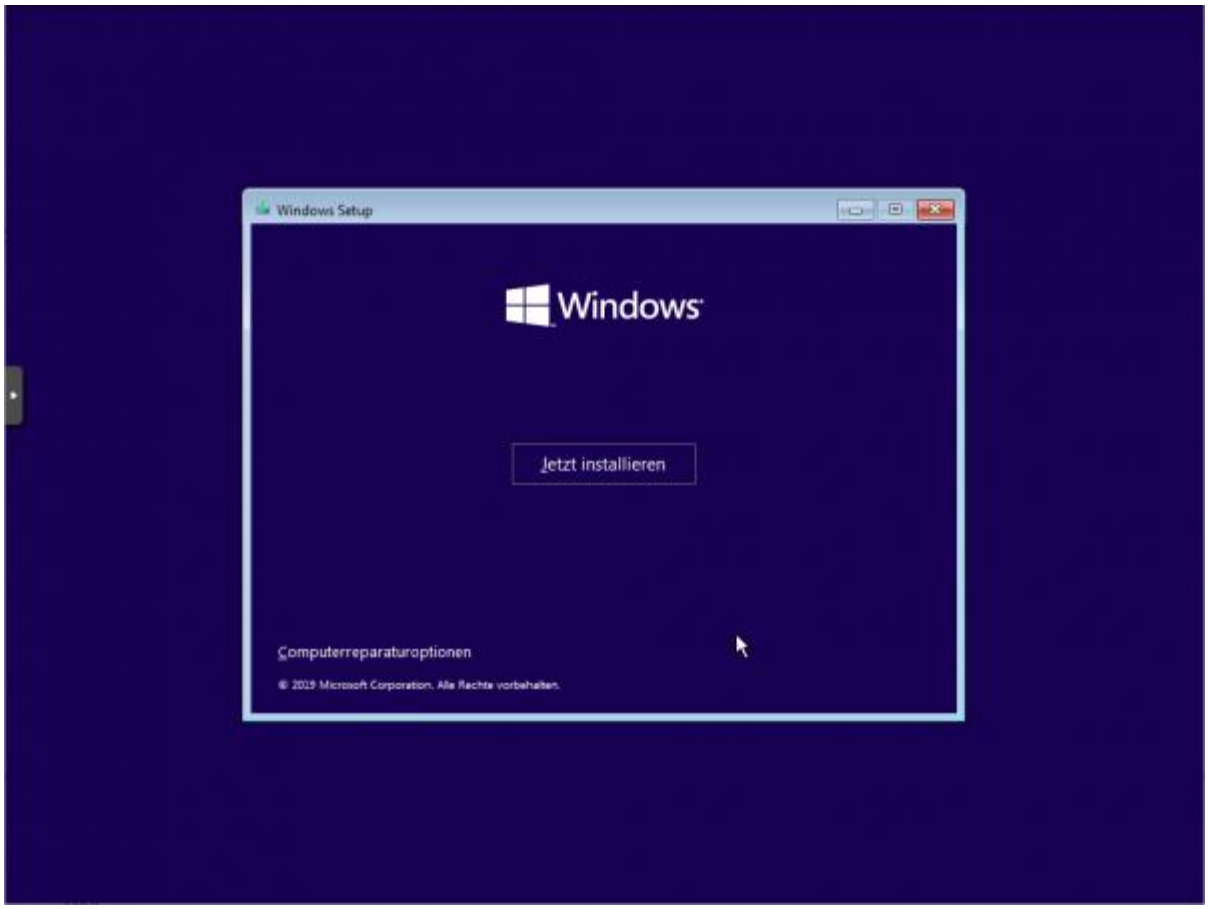
1. Du hast den PC wie zuvor beschrieben über CD/USB-Stick gebootet. Dieser wurde zudem zuvor mit LINBO partioniert und formatiert.
2. Drücke während des Boot-Vorgangs nach Aufforderung eine Taste, damit von dem Windows-Installationsmedium tatsächlich gebootet wird.
3. Danach siehst Du zu Beginn der Installation 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. `Benutzderfinierte 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.

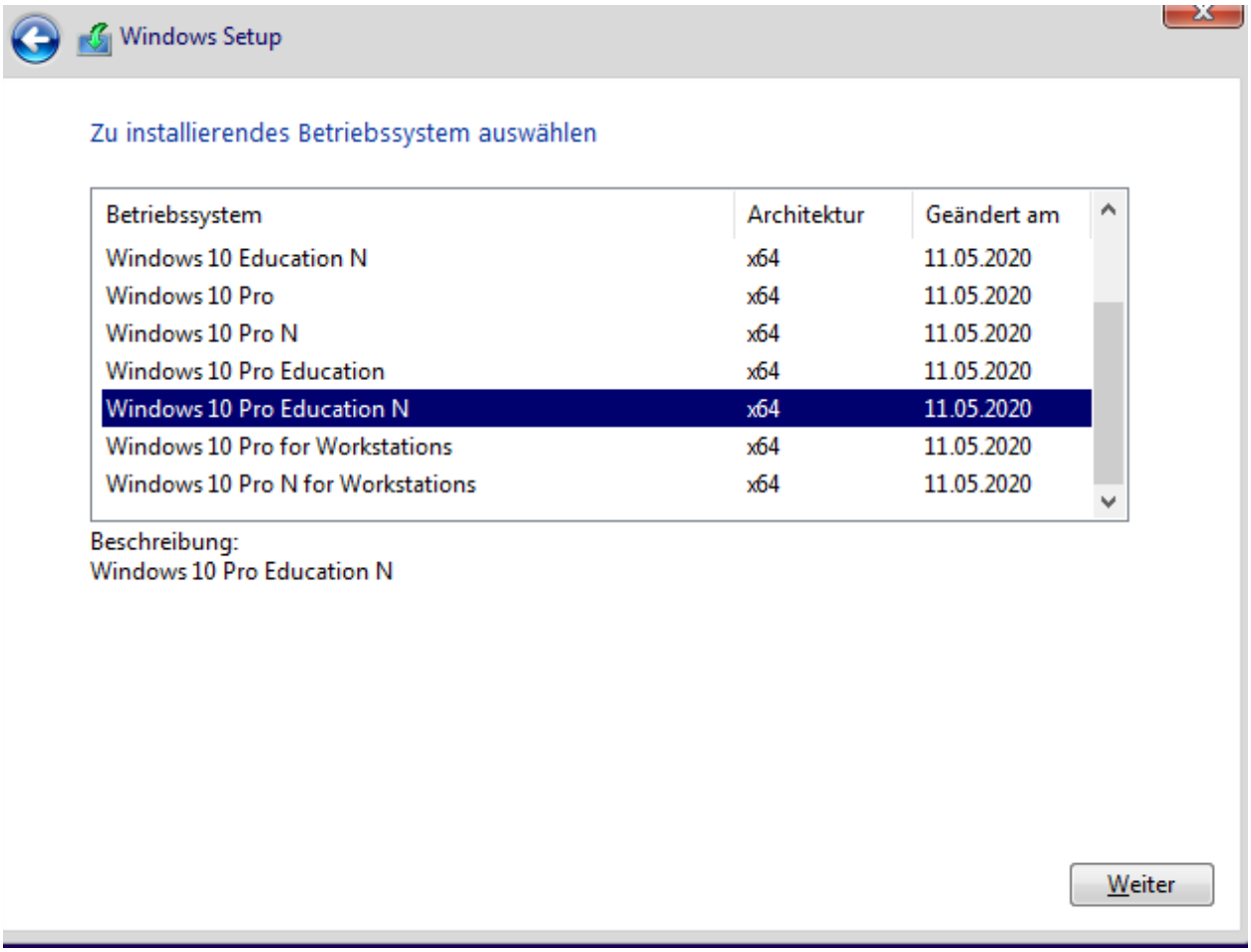
In der Abb. wurde ein UEFI-System vorbereitet. Partition 3 wurde für Windows 10 vorbereitet und Partition 4 ist die Cache-Parition. Wähle nun die richtige Parition (hier: Parition 3: windows) aus und klicke auf `Weiter`.

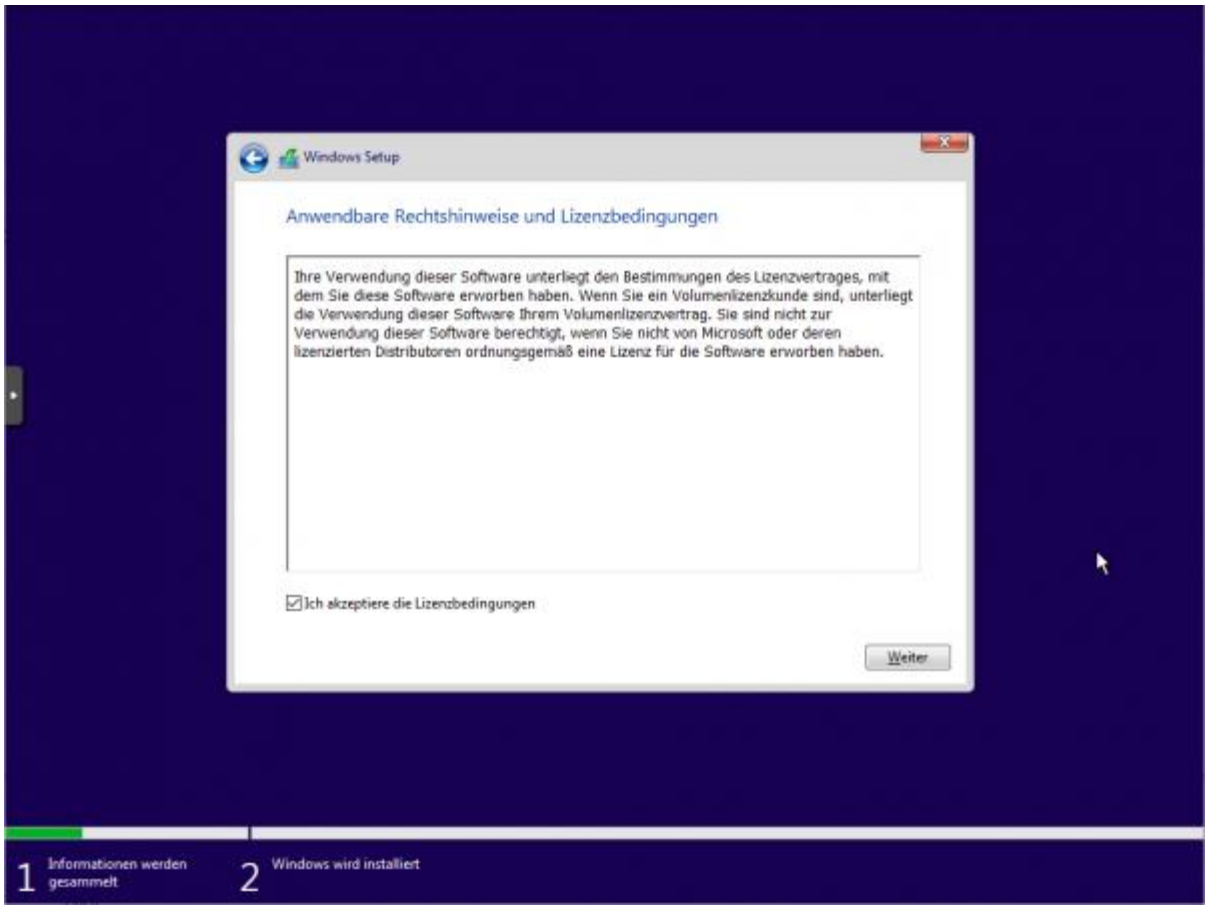
9. Warte bis die Installation von Windows abgeschlossen wurde.
10. Starte Windows neu.

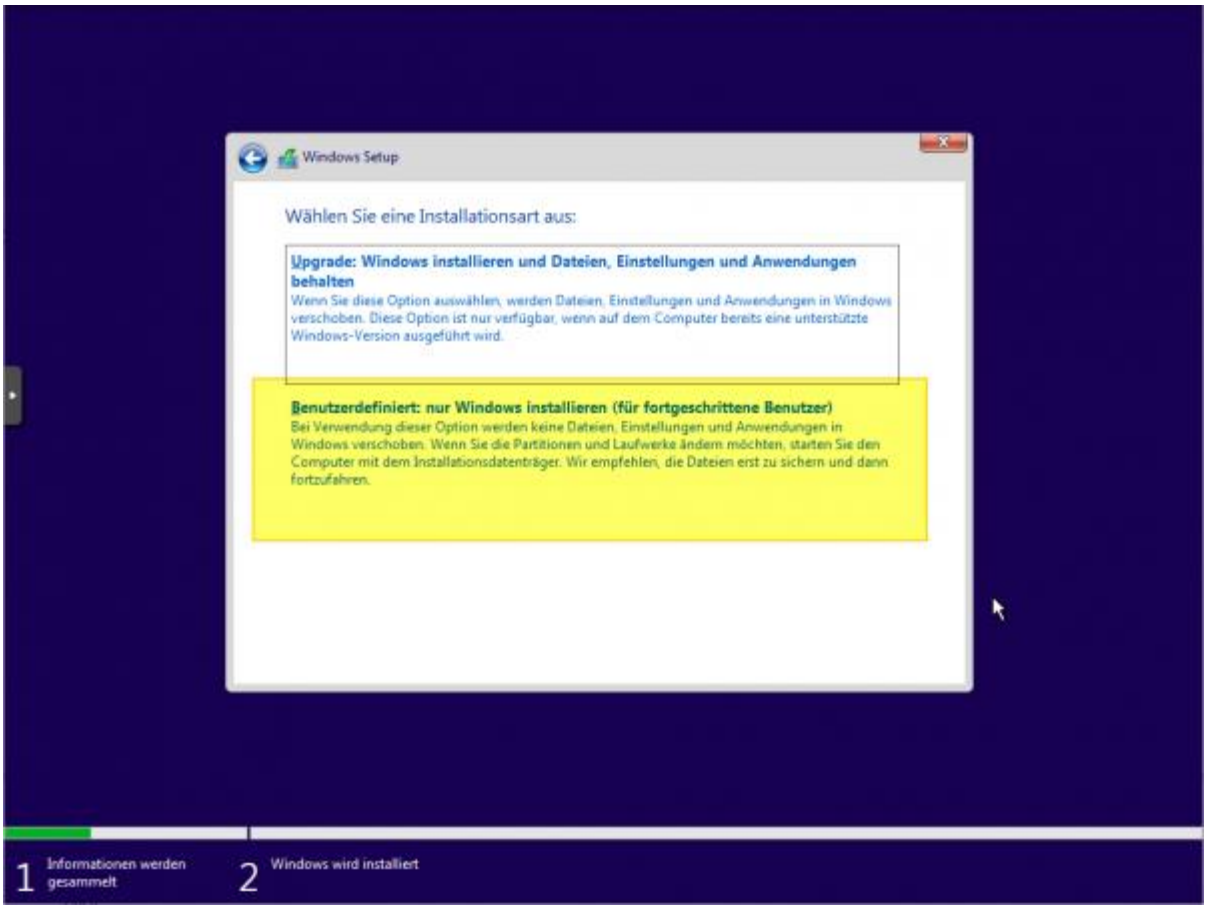
Hinweis: Es ist jetzt wichtig, dass der PC in LINBO gebootet wird. Stelle daher die Boot-Reihenfolge wieder so um, dass via PXE LINBO gebootet wird. Du gelangst dann wieder wie zuvor in den Linbo Startbildschirm.

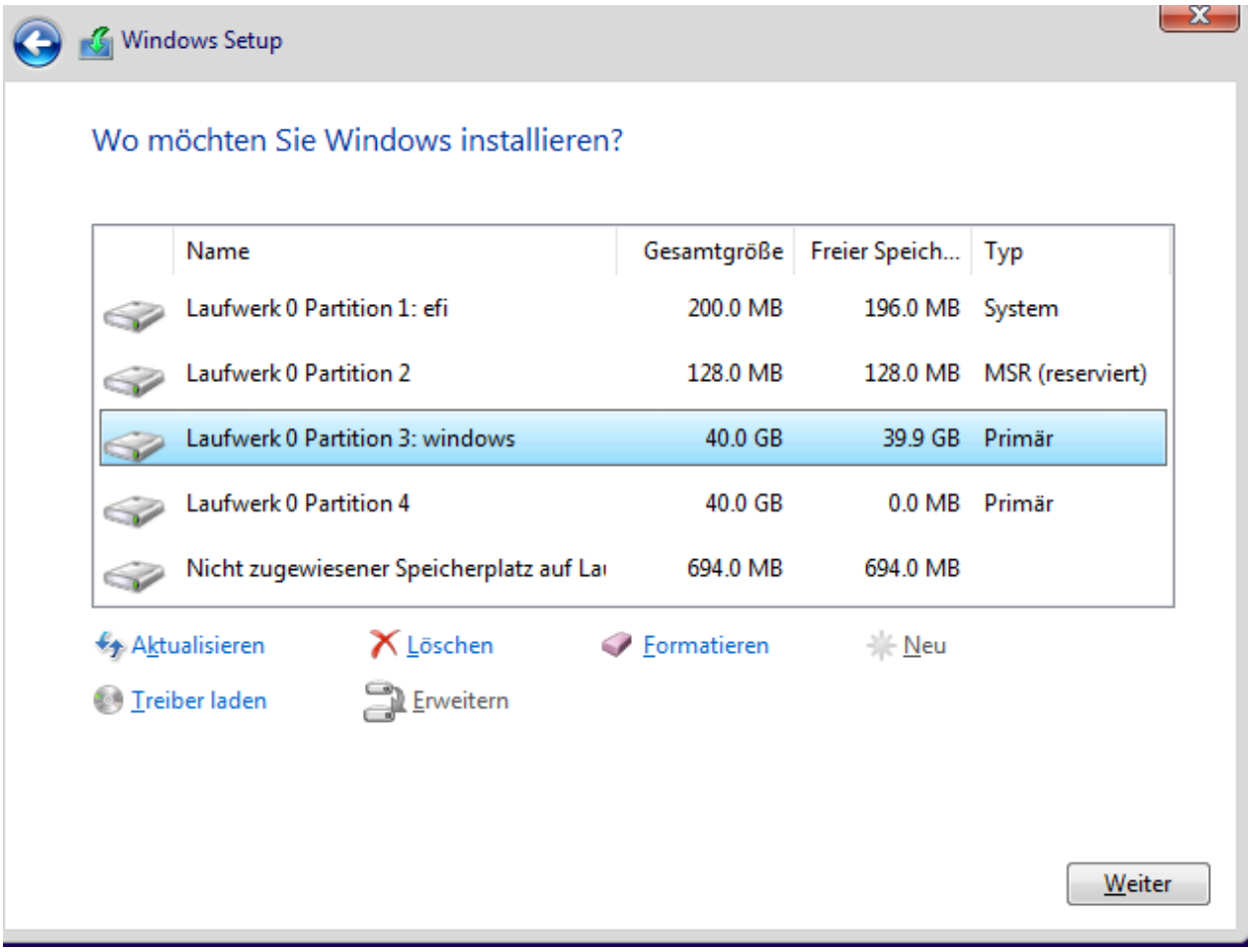

Windows Setup
Windows
Installationssprache:
Deutsch (Deutschland)
Uhrzeit und Währungsformat:
Deutsch (Deutschland)
Tastatur oder Eingabemethode:
Deutsch
Geben Sie Ihre Sprache und andere Einstellungen ein, und klicken Sie auf "Weiter", um den Vorgang fortzusetzen.
© 2019 Microsoft Corporation. Alle Rechte vorbehalten.
Weiter

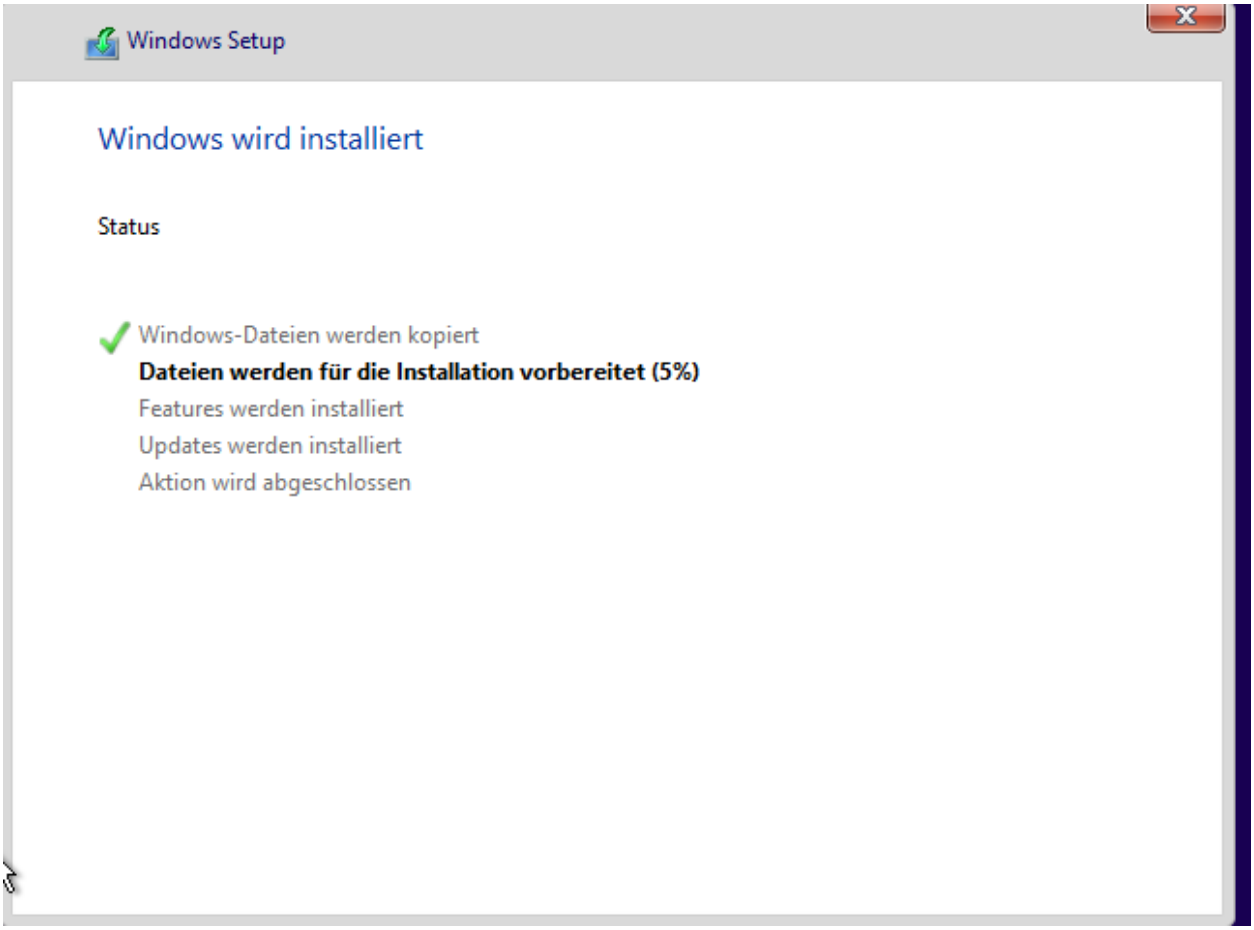

Windows Setup
Windows
Jetzt installieren
Computerreparaturoptionen
© 2019 Microsoft Corporation. Alle Rechte vorbehalten.


Windows Setup
Zu installierendes Betriebssystem auswählen
Betriebssystem
Architektur
Geändert am
Windows 10 Education N
x64
11.05.2020
Windows 10 Pro
x64
11.05.2020
Windows 10 Pro N
x64
11.05.2020
Windows 10 Pro Education
x64
11.05.2020
Windows 10 Pro Education N
x64
11.05.2020
Windows 10 Pro for Workstations
x64
11.05.2020
Windows 10 Pro N for Workstations
x64
11.05.2020
Beschreibung:
Windows 10 Pro Education N
Weiter


Windows Setup
Anwendbare Rechtshinweise und Lizenzbedingungen
Ihre Verwendung dieser Software unterliegt den Bestimmungen des Lizenzvertrages, mit dem Sie diese Software erworben haben. Wenn Sie ein Volumenlizenzkunde sind, unterliegt die Verwendung dieser Software Ihrem Volumenlizenzvertrag. Sie sind nicht zur Verwendung dieser Software berechtigt, wenn Sie nicht von Microsoft oder deren lizenzierten Distributoren ordnungsgemäß eine Lizenz für die Software erworben haben.
Ich akzeptiere die Lizenzbedingungen
Weiter
1 Informationen werden gesammelt
2 Windows wird installiert


Windows Setup
Wählen Sie eine Installationsart aus:
Upgrade: Windows installieren und Dateien, Einstellungen und Anwendungen behalten
Wenn Sie diese Option auswählen, werden Dateien, Einstellungen und Anwendungen in Windows verschoben. Diese Option ist nur verfügbar, wenn auf dem Computer bereits eine unterstützte Windows-Version ausgeführt wird.
Benutzerdefiniert: nur Windows installieren (für fortgeschrittene Benutzer)
Bei Verwendung dieser Option werden keine Dateien, Einstellungen und Anwendungen in Windows verschoben. Wenn Sie die Partitionen und Laufwerke ändern möchten, starten Sie den Computer mit dem Installationsdatenträger. Wir empfehlen, die Dateien erst zu sichern und dann fortzufahren.
1 Informationen werden gesammelt
2 Windows wird installiert


Windows Setup
Wo möchten Sie Windows installieren?
Name
Gesamtgröße
Freier Speich...
Typ
Laufwerk 0 Partition 1: efi
200.0 MB
196.0 MB
System
Laufwerk 0 Partition 2
128.0 MB
128.0 MB
MSR (reserviert)
Laufwerk 0 Partition 3: windows
40.0 GB
39.9 GB
Primär
Laufwerk 0 Partition 4
40.0 GB
0.0 MB
Primär
Nicht zugewiesener Speicherplatz auf La
694.0 MB
694.0 MB
Aktualisieren
Löschen
Formatieren
Neu
Treiber laden
Erweitern
Weiter


Windows Setup
Windows wird installiert
Status
Windows-Dateien werden kopiert
Dateien werden für die Installation vorbereitet (5%)
Features werden installiert
Updates werden installiert
Aktion wird abgeschlossen

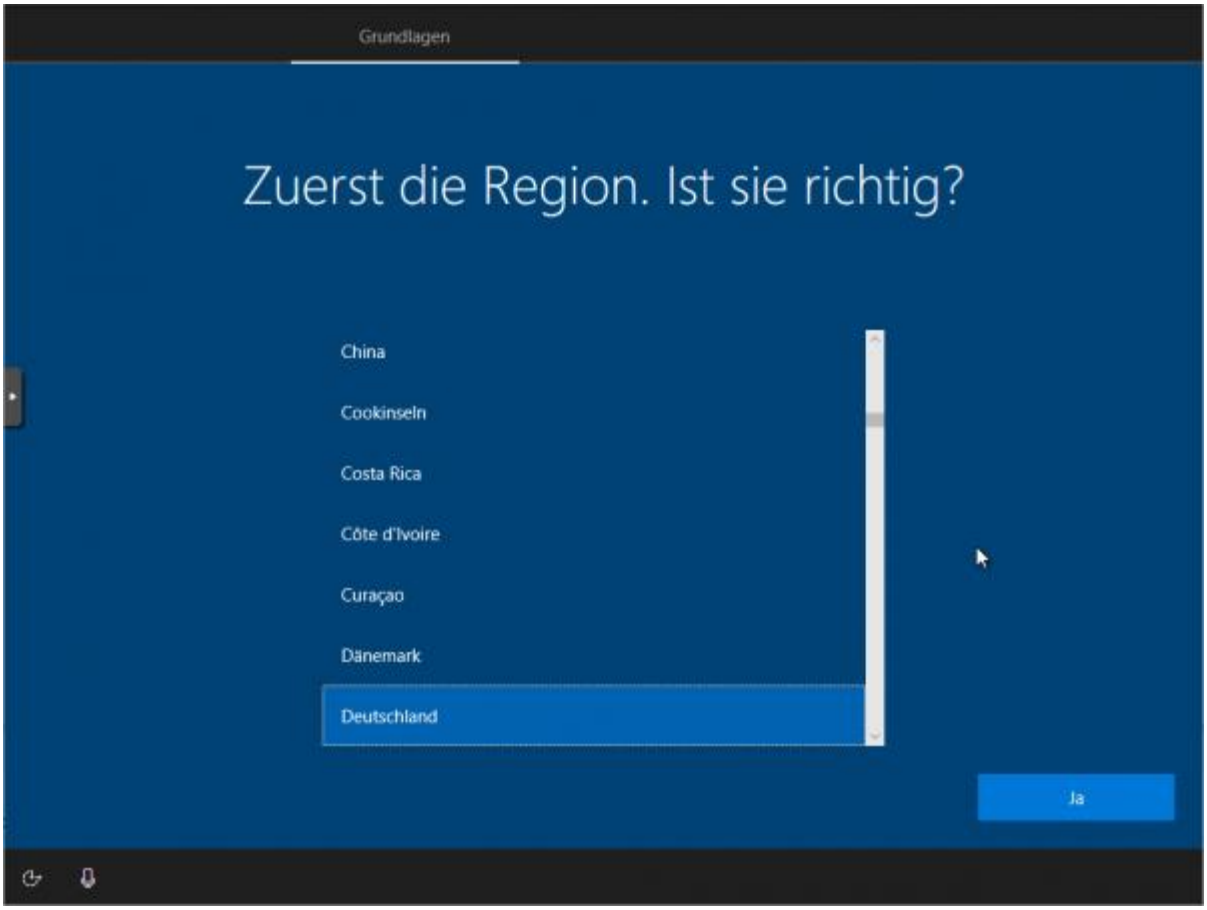
11. Starte im LINBO-Menü nun Windows unsynchronisiert über den kleinen GRÜNEN Startknopf neu (!!!nicht rot oder orange!!!):

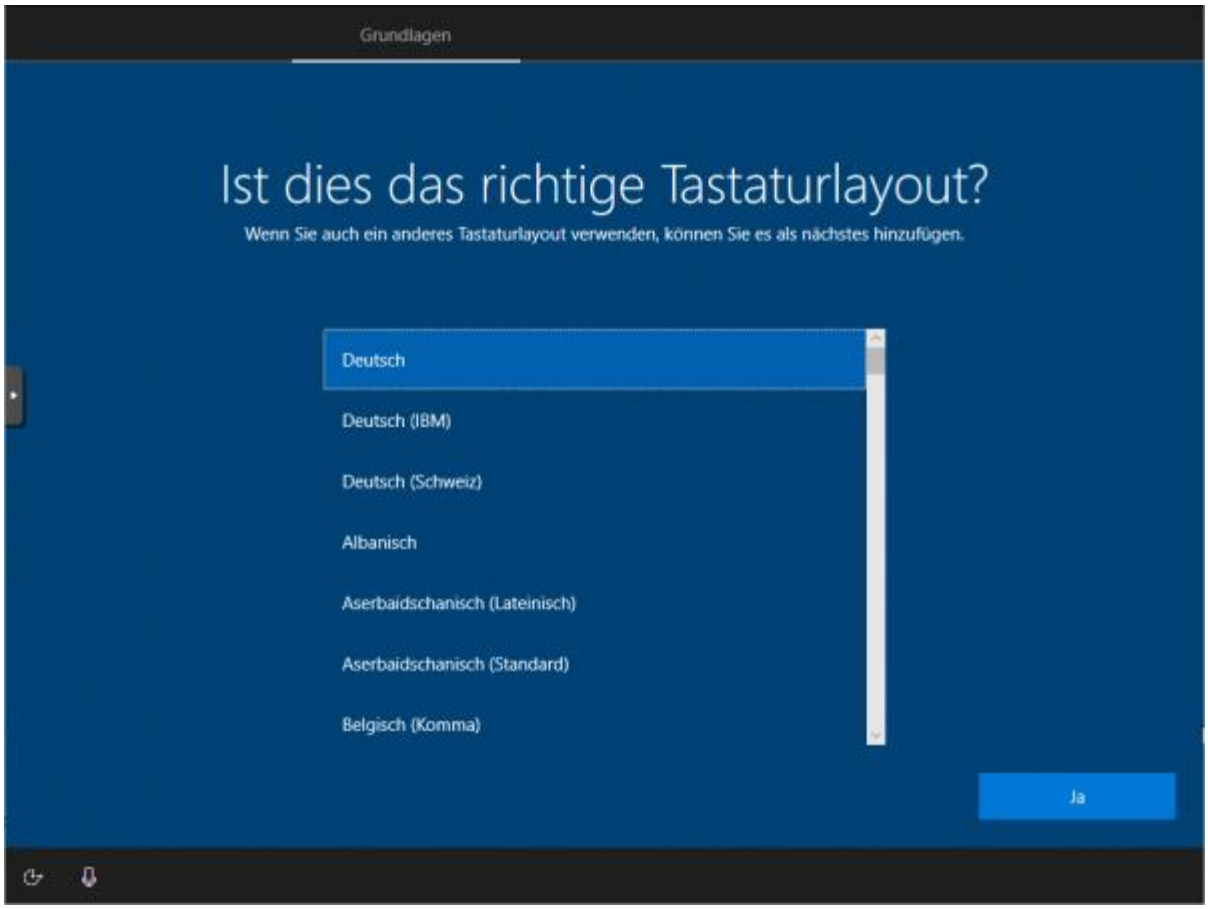
Hinweis: Solltest Du hier Probleme haben und ein UEFI-System als Client eingerichtet haben, so versuche, den Client auf den Legacy-Modus umzustellen und die Hardwareklasse in der Schulkonsole ebenfalls so anzupassen, dass BIOS64 genutzt wird. Importiere die Geräte neu, formatiere den Client mit LINBO neu, installiere Windows erneut und boote das installierte Windows aus dem lokalen Cache - wie zuvor beschrieben.

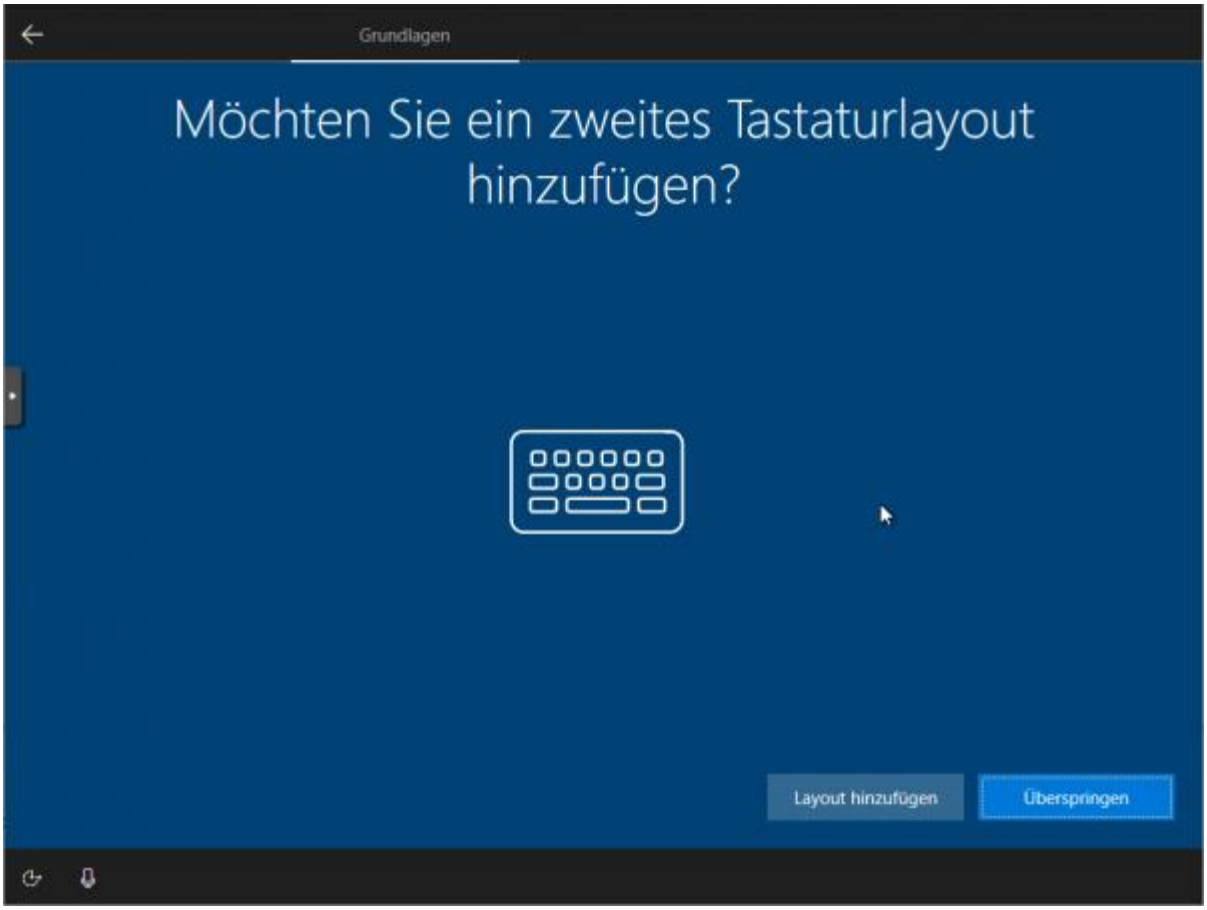
12. Nachdem Windows nun aus dem lokalen LINBO-Cache bootet, wird die Installation fortgeführt. Windows richtet Dienste ein und startet dann erneut. Du gelangst wieder in LINBO und startest Windows wieder unsynchronisiert mit der grünen Pfeiltaste.

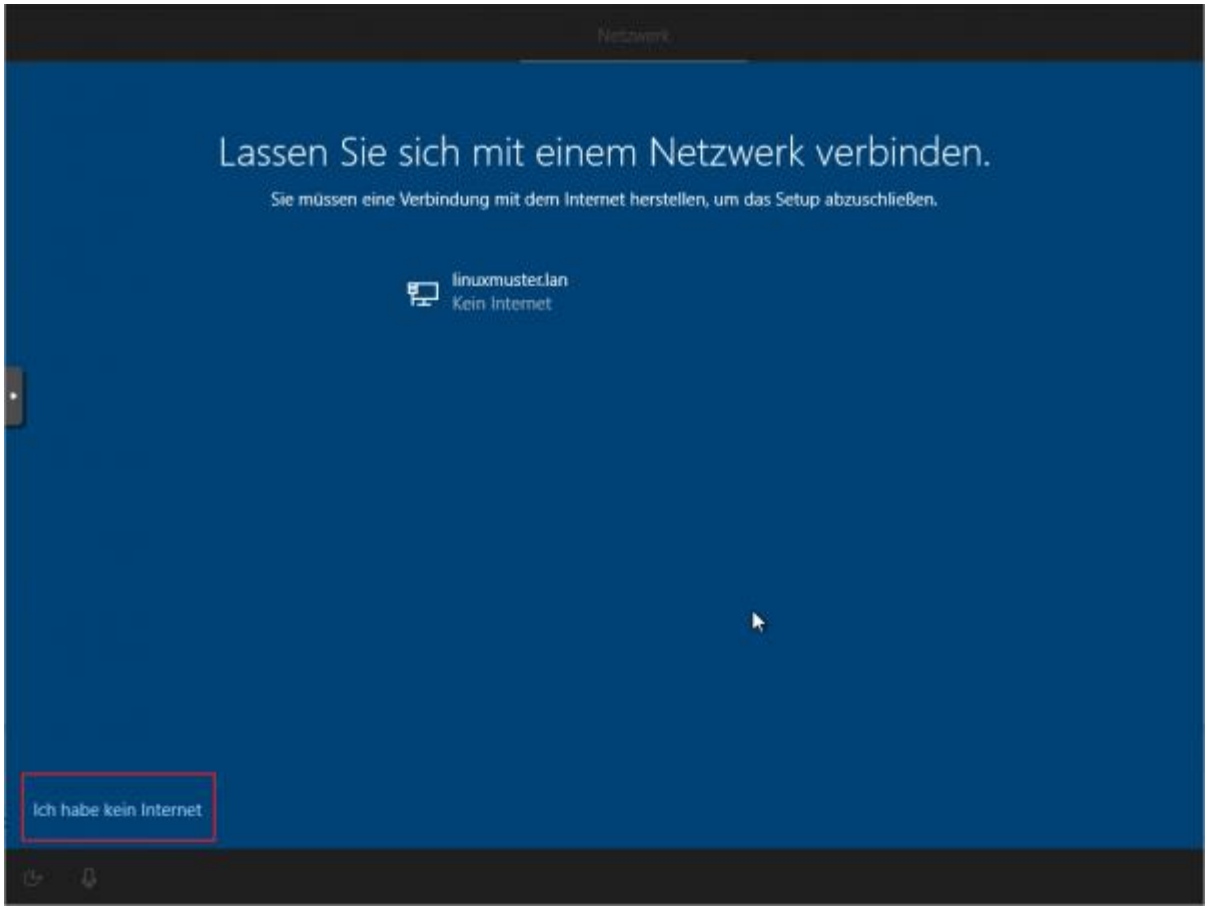
Nach dem erneuten Start von Windows wählst Du Deine Region aus.

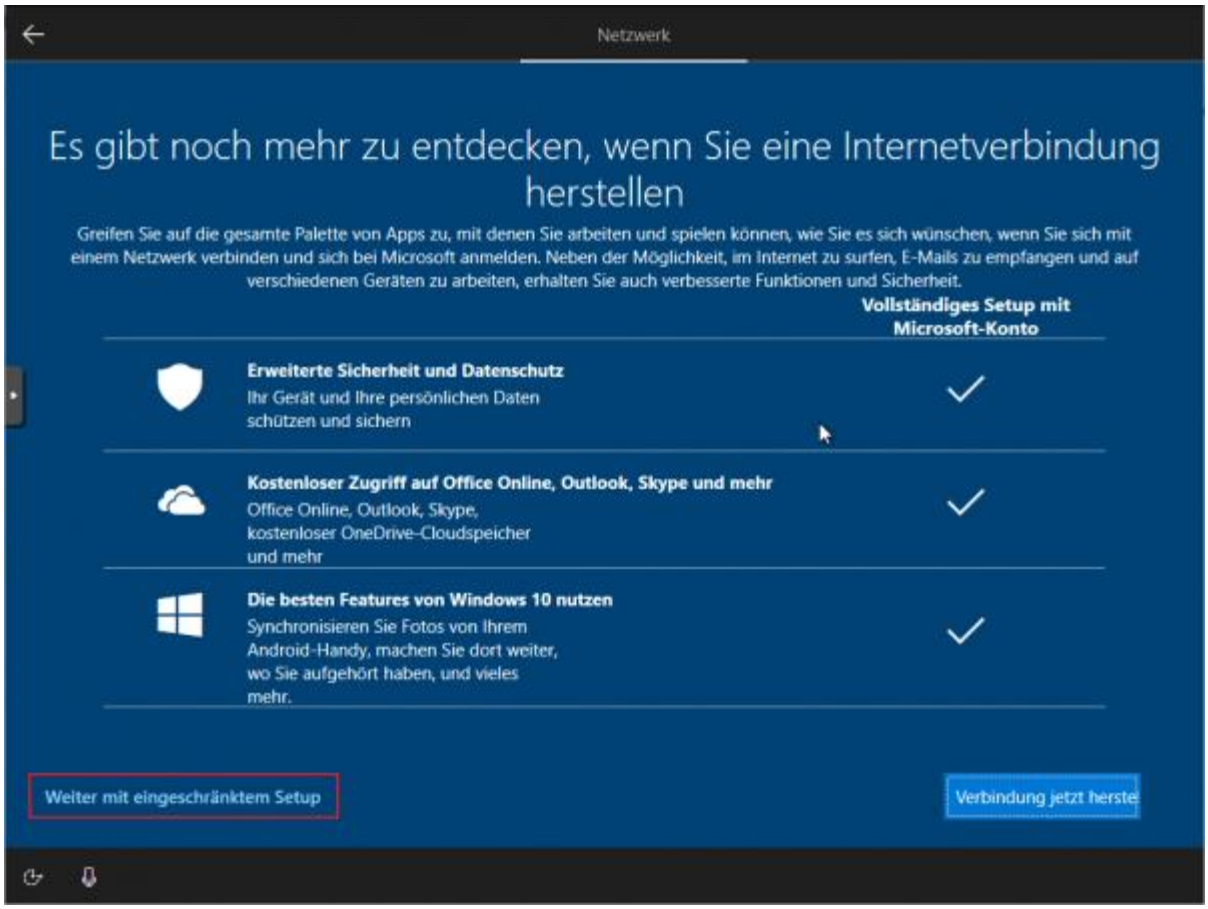
13. Tastaturlayout wählen.
14. Zweites Tastaturlayout ggf. wählen.
15. Mit Netzwerk verbinden.
16. Internet-Verbindung herstellen.
17. Admin-Benutzer festlegen.
18. Kennwort festlegen und die Sicherheitsfragen beantworten:
19. Aktivitätenverlauf deaktivieren.
20. Assistenten deaktivieren:
21. Spracherkennung deaktivieren:

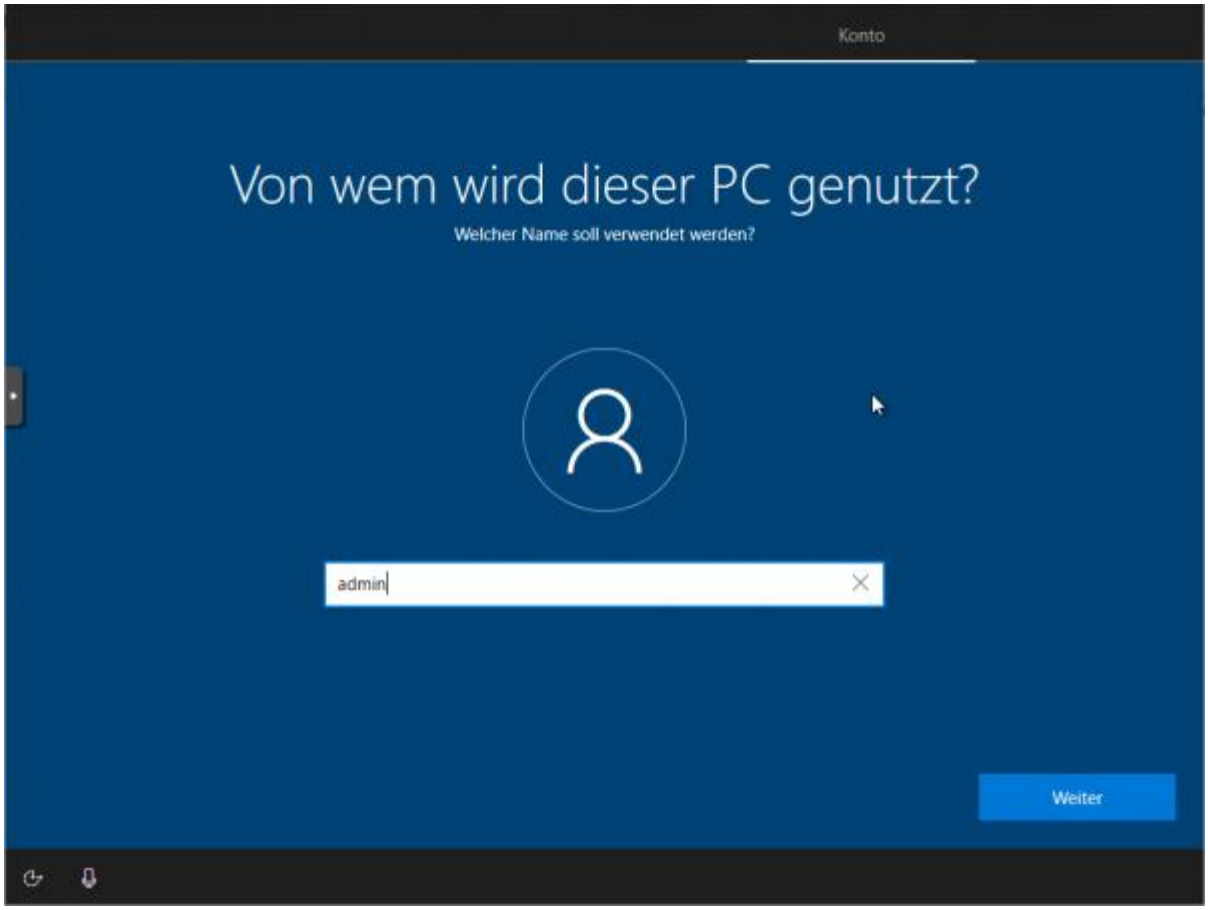

Grundlagen
Zuerst die Region. Ist sie richtig?
China
Cookinseln
Costa Rica
Côte d'Ivoire
Curaçao
Dänemark
Deutschland
Ja

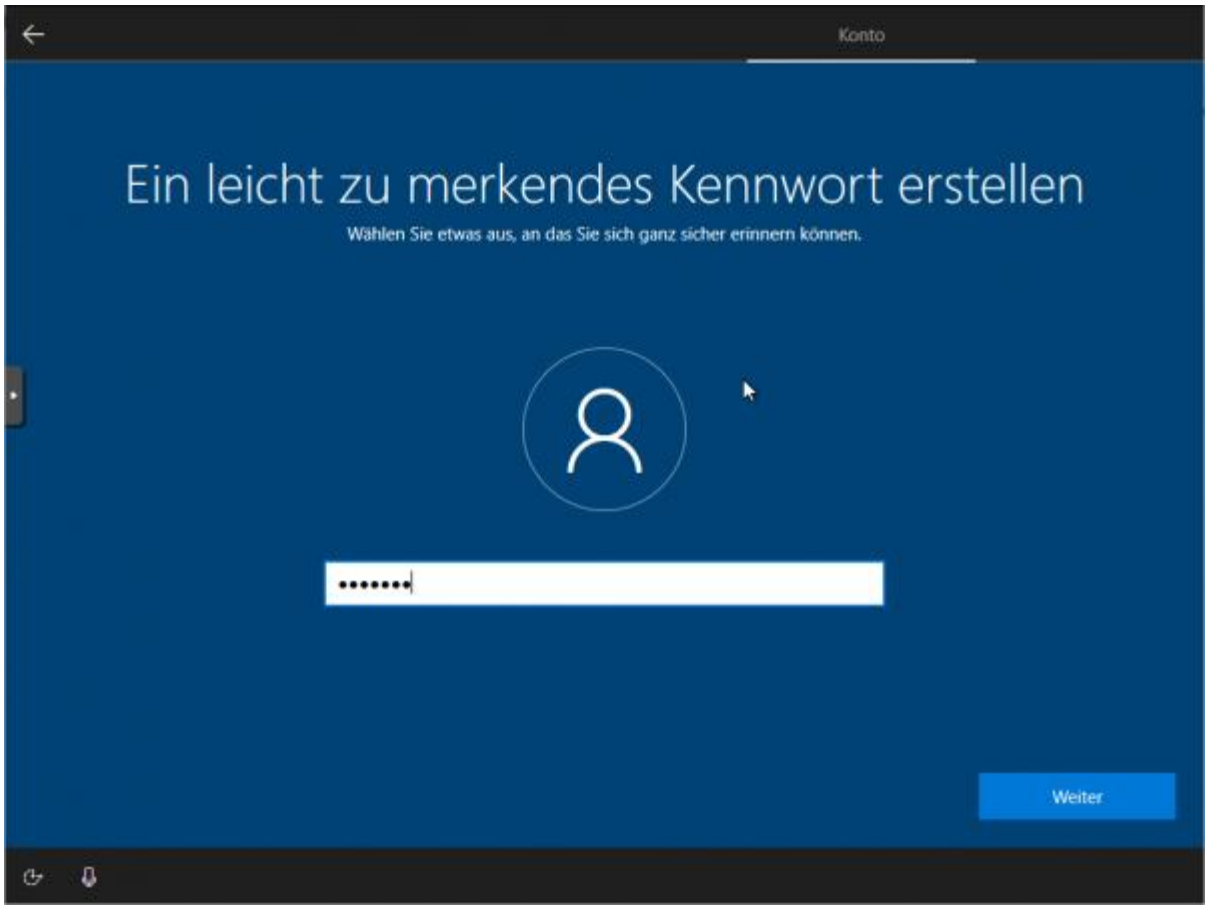

Grundlagen
Ist dies das richtige Tastaturlayout?
Wenn Sie auch ein anderes Tastaturlayout verwenden, können Sie es als nächstes hinzufügen.
Deutsch
Deutsch (IBM)
Deutsch (Schweiz)
Albanisch
Aserbaidschanisch (Lateinisch)
Aserbaidschanisch (Standard)
Belgisch (Komma)
Ja

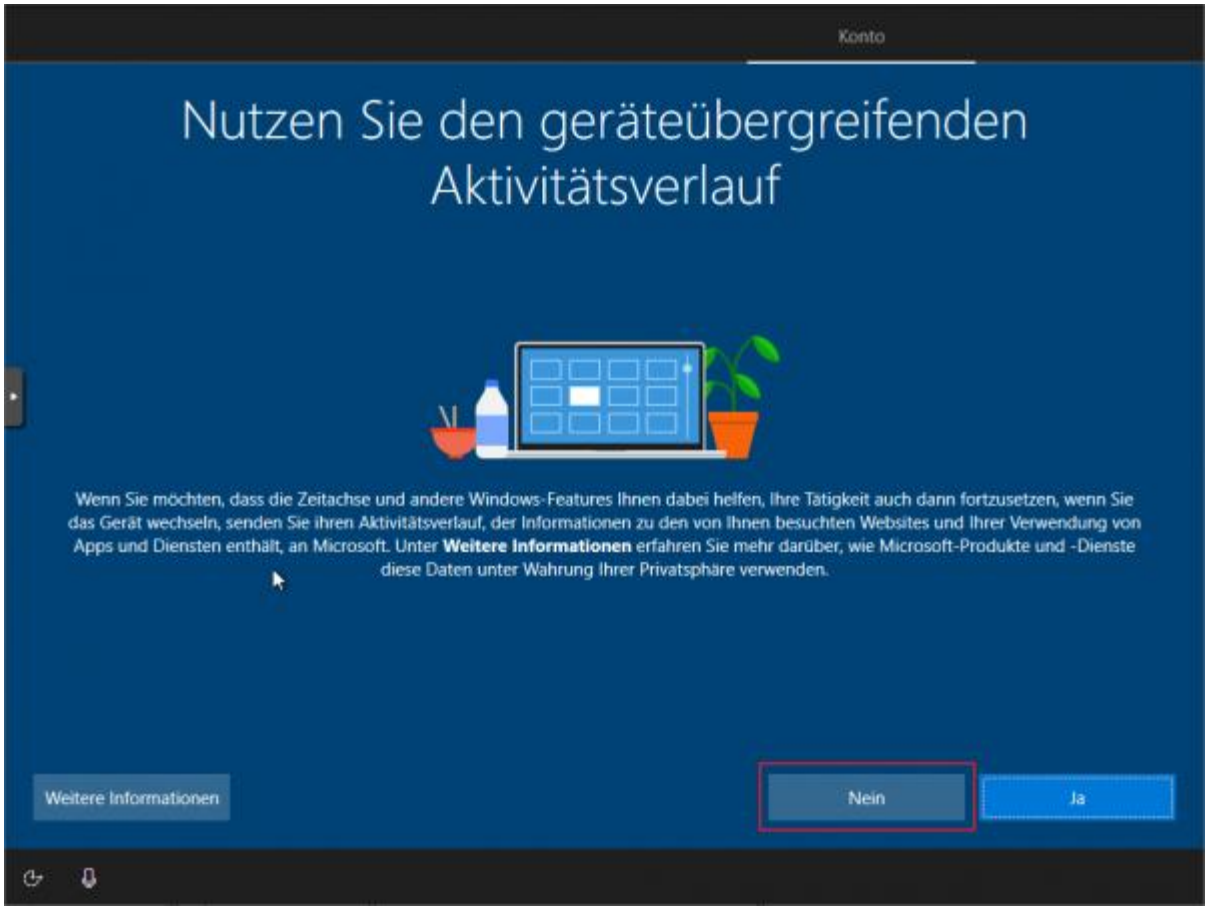

Grundlagen
Möchten Sie ein zweites Tastaturlayout hinzufügen?
Layout hinzufügen
Überspringen


Netzwerk
Lassen Sie sich mit einem Netzwerk verbinden.
Sie müssen eine Verbindung mit dem Internet herstellen, um das Setup abzuschließen.
linuxmuster.lan
Kein Internet
Ich habe kein Internet

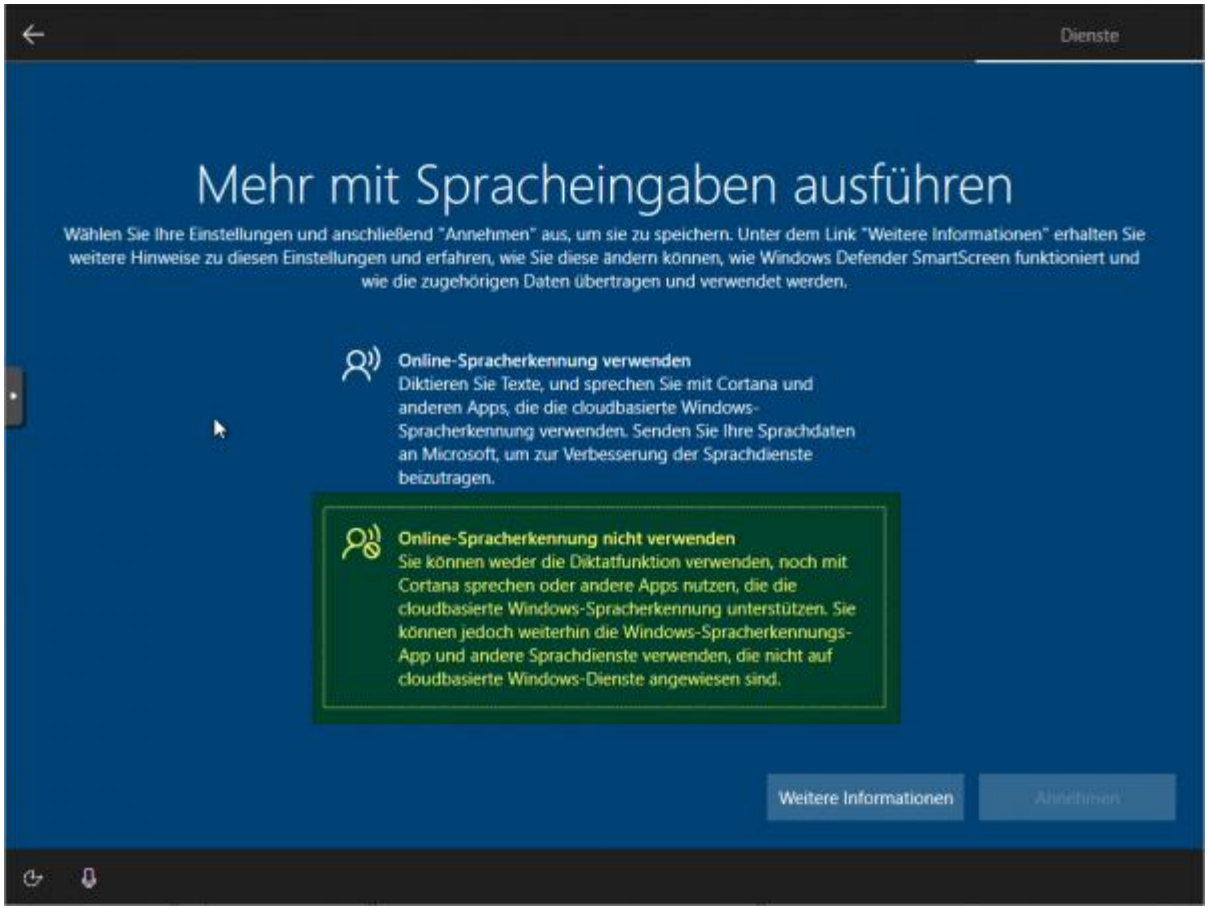

Netzwerk
Es gibt noch mehr zu entdecken, wenn Sie eine Internetverbindung herstellen
Greifen Sie auf die gesamte Palette von Apps zu, mit denen Sie arbeiten und spielen können, wie Sie es sich wünschen, wenn Sie sich mit einem Netzwerk verbinden und sich bei Microsoft anmelden. Neben der Möglichkeit, im Internet zu surfen, E-Mails zu empfangen und auf verschiedenen Geräten zu arbeiten, erhalten Sie auch verbesserte Funktionen und Sicherheit.
Vollständiges Setup mit Microsoft-Konto
Erweiterte Sicherheit und Datenschutz
Ihr Gerät und Ihre persönlichen Daten schützen und sichern
Kostenloser Zugriff auf Office Online, Outlook, Skype und mehr
Office Online, Outlook, Skype, kostenloser OneDrive-Cloudspeicher und mehr
Die besten Features von Windows 10 nutzen
Synchronisieren Sie Fotos von Ihrem Android-Handy, machen Sie dort weiter, wo Sie aufgehört haben, und vieles mehr.
Weiter mit eingeschränktem Setup
Verbindung jetzt herste


Konto
Von wem wird dieser PC genutzt?
Welcher Name soll verwendet werden?
admin
Weiter


Konto
Ein leicht zu merkendes Kennwort erstellen
Wählen Sie etwas aus, an das Sie sich ganz sicher erinnern können.
Weiter

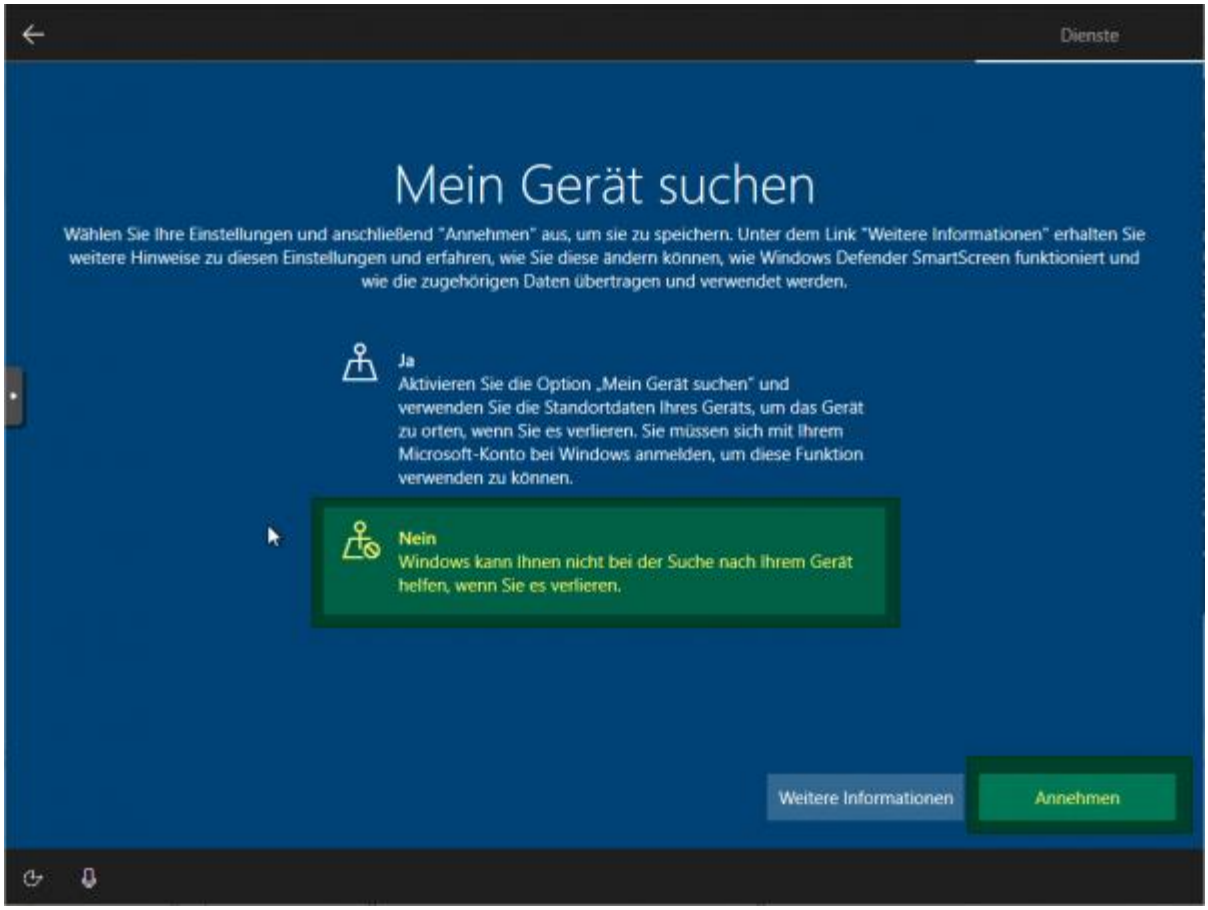

Konto
Nutzen Sie den geräteübergreifenden Aktivitätsverlauf
Wenn Sie möchten, dass die Zeitachse und andere Windows-Features Ihnen dabei helfen, Ihre Tätigkeit auch dann fortzusetzen, wenn Sie das Gerät wechseln, senden Sie ihren Aktivitätsverlauf, der Informationen zu den von Ihnen besuchten Websites und Ihrer Verwendung von Apps und Diensten enthält, an Microsoft. Unter **Weitere Informationen** erfahren Sie mehr darüber, wie Microsoft-Produkte und -Dienste diese Daten unter Wahrung Ihrer Privatsphäre verwenden.
Weitere Informationen
Nein
Ja


Dienste
Hilfe von Ihrem digitalen Assistenten erhalten
Cortana hilft Ihnen, Ihre Zeit einzuteilen, Dinge zu erledigen und in Verbindung zu bleiben.
Damit Cortana personalisiert werden kann und die passenden Vorschläge anbietet, sammelt und nutzt Microsoft Informationen wie Ihre Position und den Positionsverlauf, Kontakte, Spracheingaben, Sprach- und Handschriftmuster, den Eingabeverlauf, den Suchverlauf, Kalenderdetails, Inhalte und den Kommunikationsverlauf aus Microsoft-Diensten, -Nachrichten und -Apps. In Microsoft Edge verwendet Cortana Daten aus dem Browserverlauf. Sie können diese Optionen im Notizbuch jederzeit ändern und Cortana in Microsoft Edge deaktivieren.
Weitere Informationen
Ablehnen
Annehmen

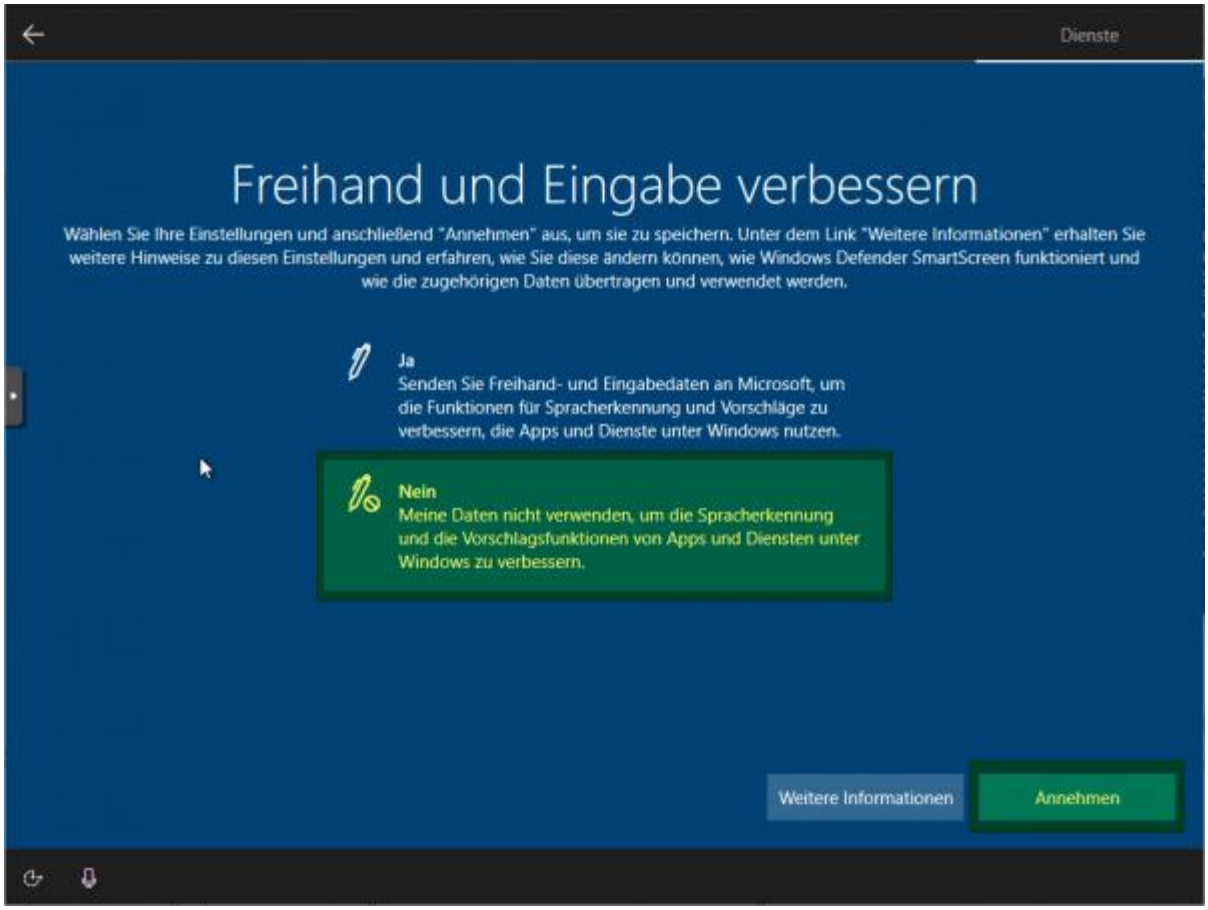

Dienste
Mehr mit Spracheingaben ausführen
Wählen Sie Ihre Einstellungen und anschließend "Annehmen" aus, um sie zu speichern. Unter dem Link "Weitere Informationen" erhalten Sie weitere Hinweise zu diesen Einstellungen und erfahren, wie Sie diese ändern können, wie Windows Defender SmartScreen funktioniert und wie die zugehörigen Daten übertragen und verwendet werden.
Online-Spracherkennung verwenden
Diktieren Sie Texte, und sprechen Sie mit Cortana und anderen Apps, die die cloudbasierte Windows-Spracherkennung verwenden. Senden Sie Ihre Sprachdaten an Microsoft, um zur Verbesserung der Sprachdienste beizutragen.
Online-Spracherkennung nicht verwenden
Sie können weder die Diktatfunktion verwenden, noch mit Cortana sprechen oder andere Apps nutzen, die die cloudbasierte Windows-Spracherkennung unterstützen. Sie können jedoch weiterhin die Windows-Spracherkennungs-App und andere Sprachdienste verwenden, die nicht auf cloudbasierte Windows-Dienste angewiesen sind.
Weitere Informationen
Annehmen

22. Standortdienste deaktivieren:

23. Gerätesuche deaktivieren
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. Installation abschließen.
30. Rechner **nicht herunterfahren**, sondern unbedingt den nächsten Schritt Global Registry-Patch einspielen ausführen, ansonsten funktioniert Windows **nicht** mehr und muss neu installiert werden!!


Dienste
Mein Gerät suchen
Wählen Sie Ihre Einstellungen und anschließend "Annehmen" aus, um sie zu speichern. Unter dem Link "Weitere Informationen" erhalten Sie weitere Hinweise zu diesen Einstellungen und erfahren, wie Sie diese ändern können, wie Windows Defender SmartScreen funktioniert und wie die zugehörigen Daten übertragen und verwendet werden.
Ja
Aktivieren Sie die Option „Mein Gerät suchen" und verwenden Sie die Standortdaten Ihres Geräts, um das Gerät zu orten, wenn Sie es verlieren. Sie müssen sich mit Ihrem Microsoft-Konto bei Windows anmelden, um diese Funktion verwenden zu können.
Nein
Windows kann Ihnen nicht bei der Suche nach Ihrem Gerät helfen, wenn Sie es verlieren.
Weitere Informationen
Annehmen


Dienste
Diagnosedaten an Microsoft senden
Wählen Sie Ihre Einstellungen und anschließend "Annehmen" aus, um sie zu speichern. Unter dem Link "Weitere Informationen" erhalten Sie weitere Hinweise zu diesen Einstellungen und erfahren, wie Sie diese ändern können, wie Windows Defender SmartScreen funktioniert und wie die zugehörigen Daten übertragen und verwendet werden.
Vollständig
Sendet neben allen Diagnosedaten der Stufe "Einfach" zusätzliche Informationen zu den besuchten Websites, zur Verwendung von Apps und Features, zur Geräteintegrität und -aktivität sowie erweiterte Fehlerberichte. Die Diagnosedaten werden genutzt, um Windows sicher und auf dem neuesten Stand zu halten, um Probleme zu beheben und Produktverbesserungen vorzunehmen. Ihr Gerät ist sicher und funktioniert normal, unabhängig davon, ob Sie "Einfach" oder "Vollständig" auswählen.
Einfach
Sendet nur Informationen zum Gerät, zu den Einstellungen und Funktionen und dazu, ob es ordnungsgemäß funktioniert. Die Diagnosedaten werden genutzt, um Windows sicher und auf dem neuesten Stand zu halten, um Probleme zu beheben und
Weitere Informationen
Annehmen


Dienste
Freihand und Eingabe verbessern
Wählen Sie Ihre Einstellungen und anschließend "Annehmen" aus, um sie zu speichern. Unter dem Link "Weitere Informationen" erhalten Sie weitere Hinweise zu diesen Einstellungen und erfahren, wie Sie diese ändern können, wie Windows Defender SmartScreen funktioniert und wie die zugehörigen Daten übertragen und verwendet werden.
Ja
Senden Sie Freihand- und Eingabedaten an Microsoft, um die Funktionen für Spracherkennung und Vorschläge zu verbessern, die Apps und Dienste unter Windows nutzen.
Nein
Meine Daten nicht verwenden, um die Spracherkennung und die Vorschlagsfunktionen von Apps und Diensten unter Windows zu verbessern.
Weitere Informationen
Annehmen

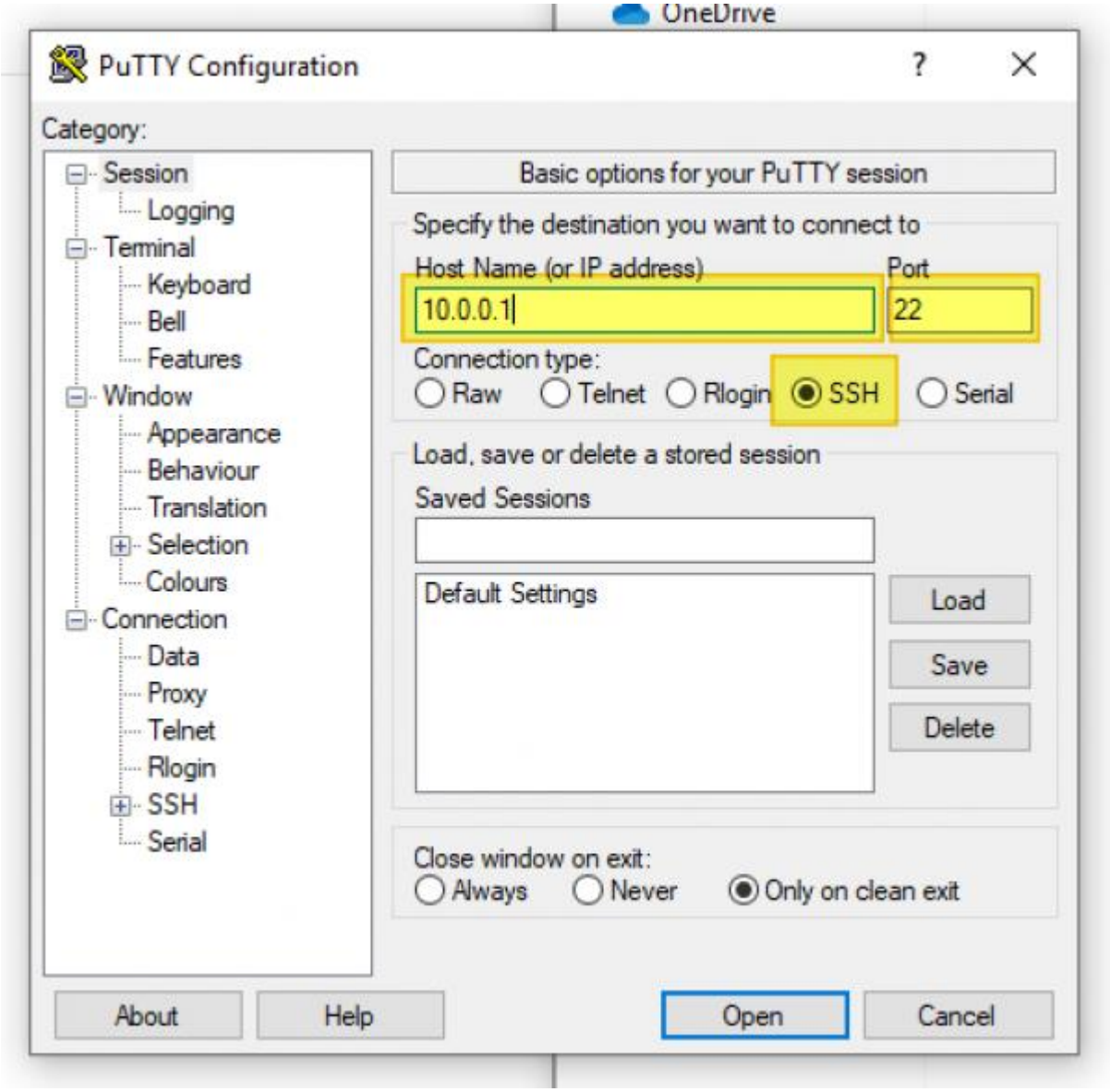
Global-Registry für Windows 10

Achtung: Die Global-Registry-Patch-Datei ist wichtig für Windows-Maschinen und **muss** einmal ausgeführt worden sein.

1. die Global Registry liegt als Vorlage auf der Server-VM in `\\server\srv\linbo\examples` und heißt `win10.global.reg` und muss nach `\\srv\samba\global\management\global-admin` kopiert werden, um Sie dann auf dem PC anwenden zu können. Das geht z.B. über die Console der Server-VM selbst:

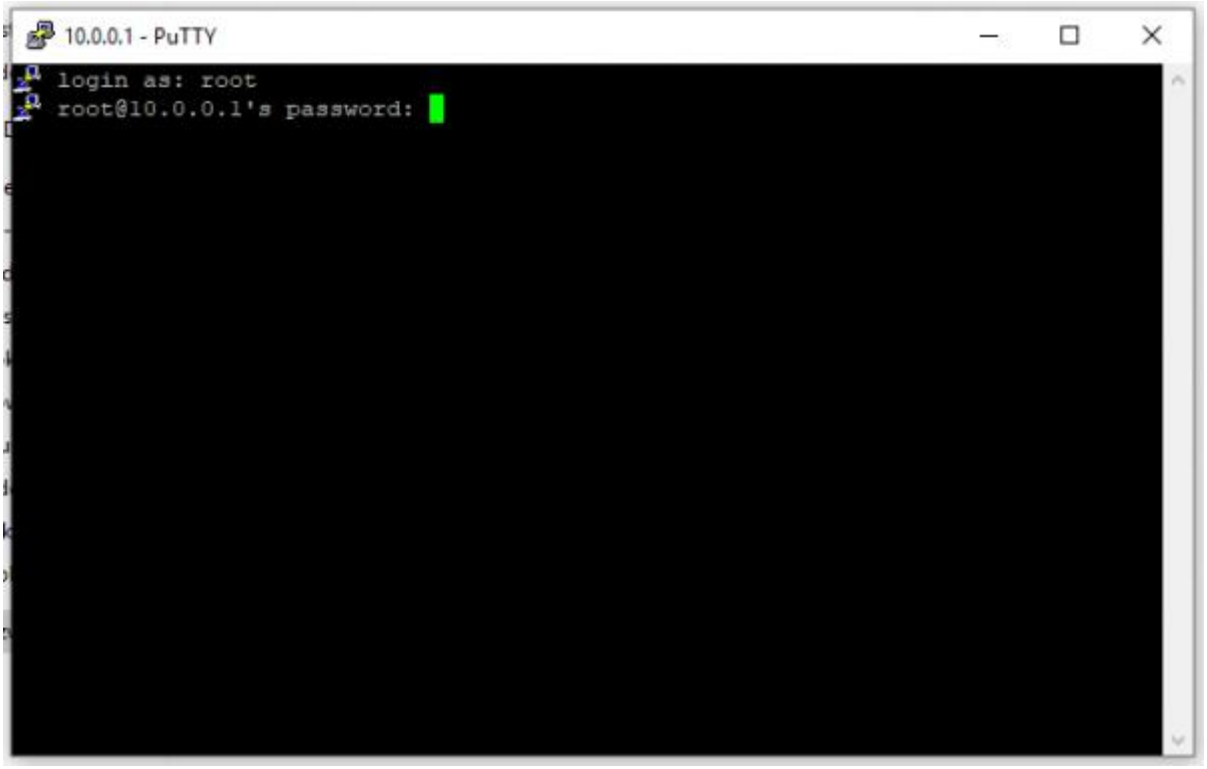
```
cp /srv/linbo/examples/win10.global.reg /srv/samba/global/management/global-admin/
```

oder auf dem Admin-PC über Putty. Dazu musst du a) Putty installieren und öffnen b) die richtigen Verbindungsdaten eingeben:



c) und mit Open unten links verbinden

d) für login as: root eingeben und als password das beim Setup vergeben Passwort eingeben (beim Tippen wird es nicht angezeigt)



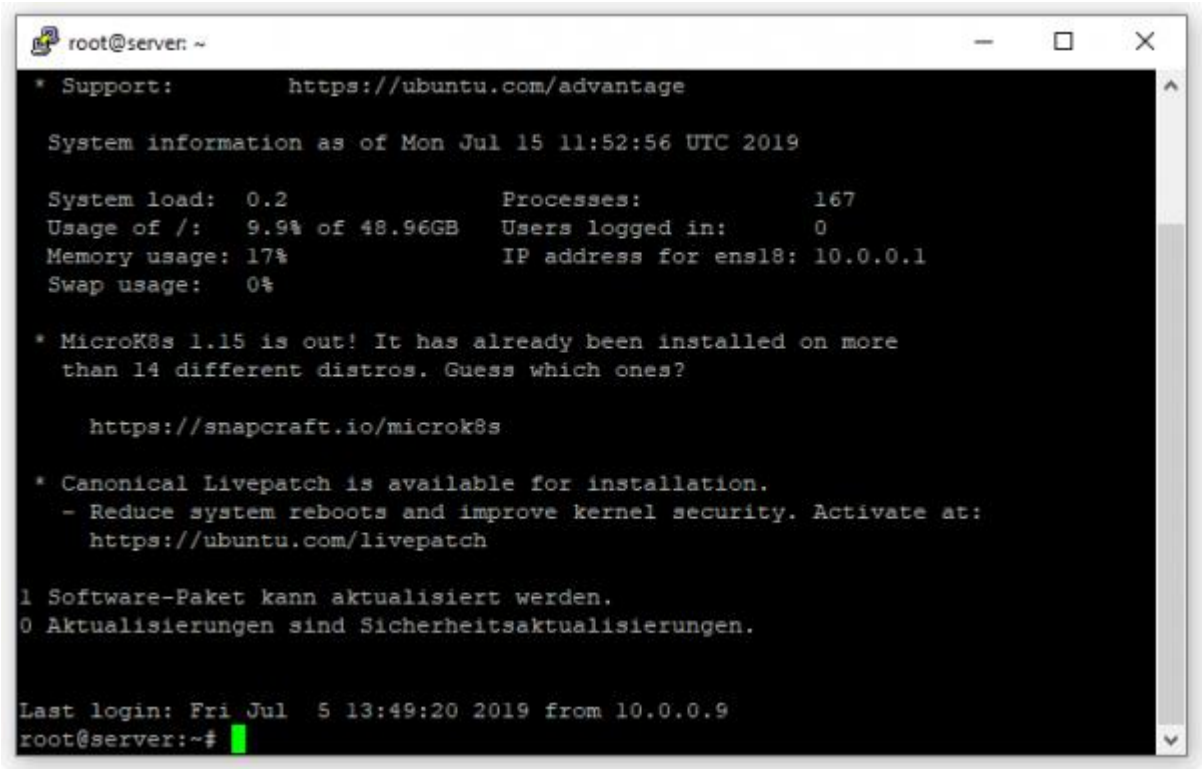
e) und mit Enter bestätigen, dann sollte sich ähnliche Darstellung zeigen:

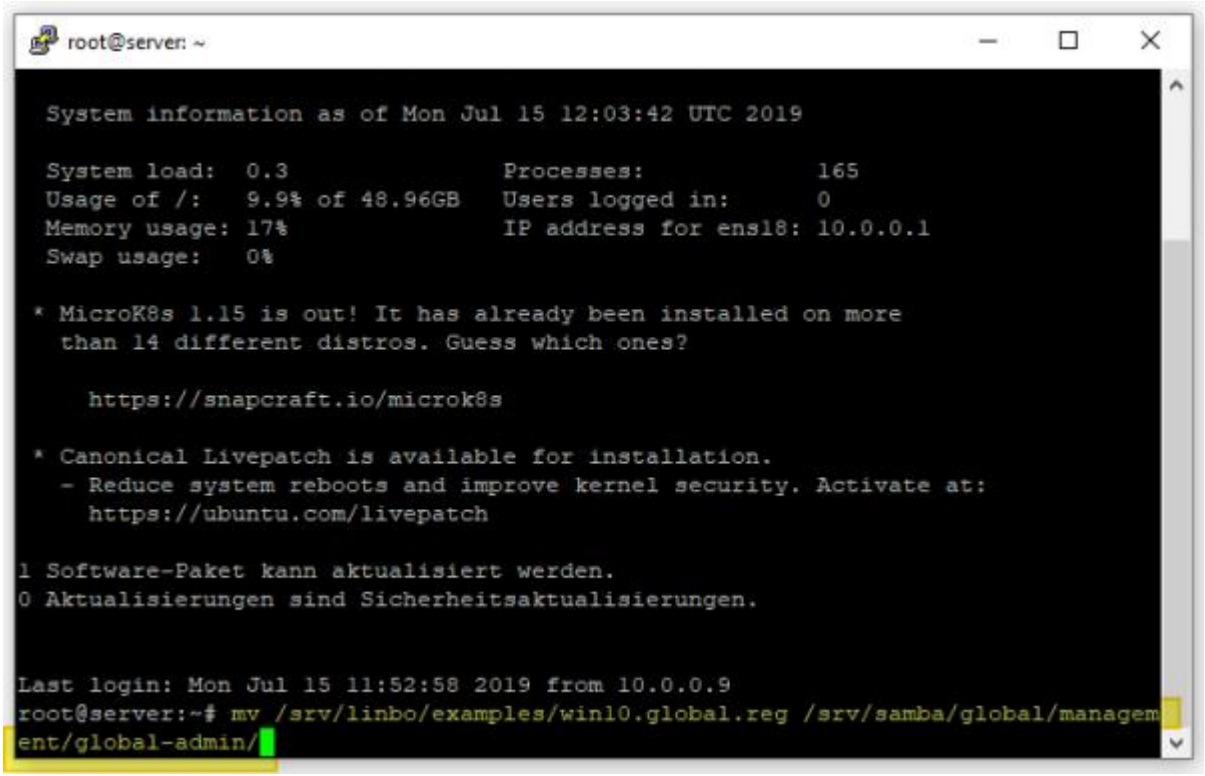
f) um die Datei nun in den richtigen Ordner zu kopieren, den Befehl `cp /srv/linbo/examples/win10.global.reg /srv/samba/global/management/global-admin/` eingeben.

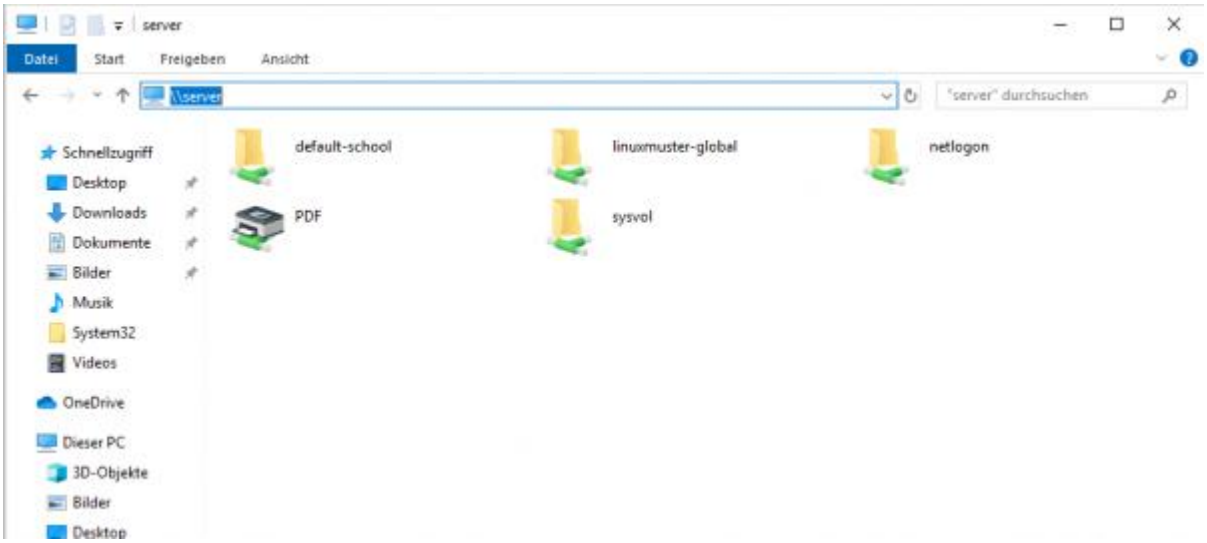
g) mit Enter bestätigen. Nun wurde die Datei übertragen.

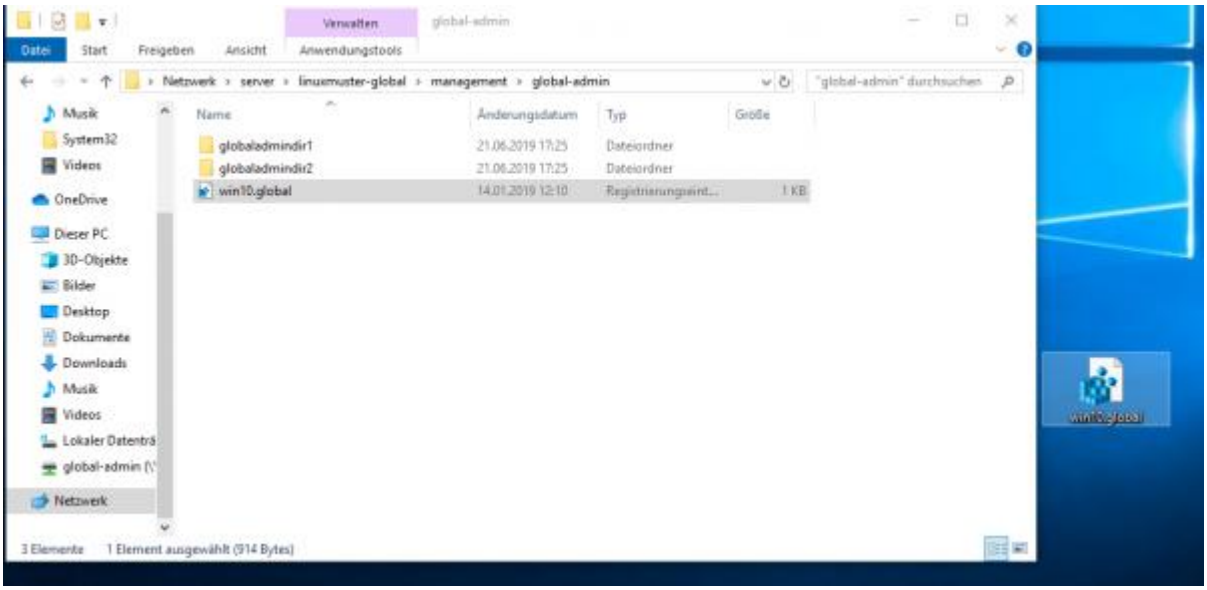
h) Putty schließen

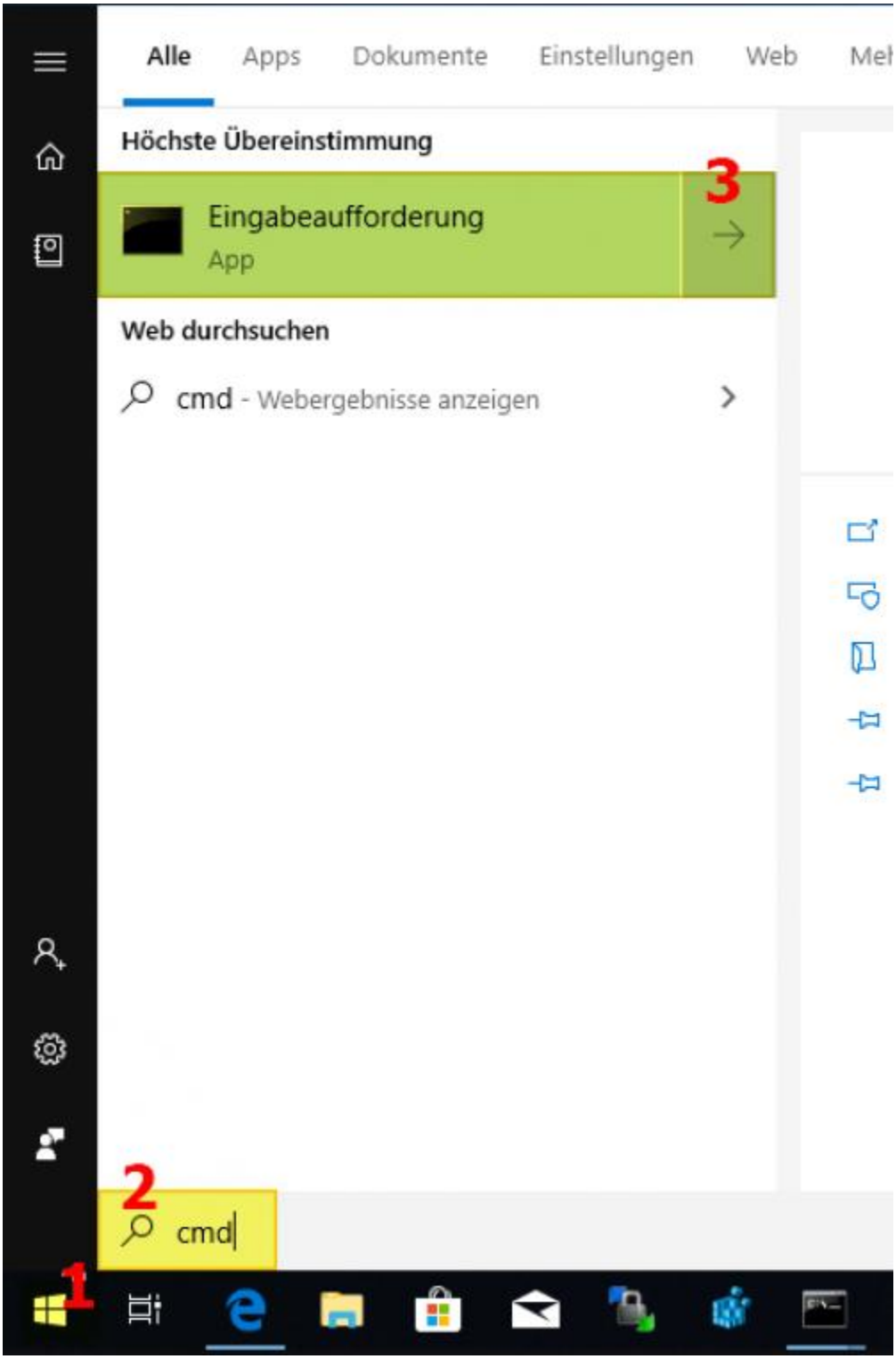
2. auf dem PC im Programm `Explorer` nun das Netzlaufwerk des Servers öffnen, indem Du in der Leiste oben `\\server` eingibst:
3. Du gibst ggf. die Anmeldedaten des `global-admin` ein. Danach öffnest Du nacheinander die Ordner `linuxmuster-global` → `managament` → `global-admin`
4. Hier liegt die Registry-Datei `win10.global`. Ziehe diese via Drag & Drop auf den Desktop.
5. Führen nun einen Doppelklick auf die Datei win10.global.reg aus. Lasse Änderungen durch diese App zu.
6. Evtl. weitere gewünschte System-Einrichtungen für die Vorlage vornehmen.
7. Zum Herunterfahren vorsichtshalber über das Windows-Startmenü in der Suche `cmd` eingeben und die Eingabeaufforderung öffnen.
8. In der Console `shutdown -s -t 1` eingeben und mit `Enter` bestätigen:

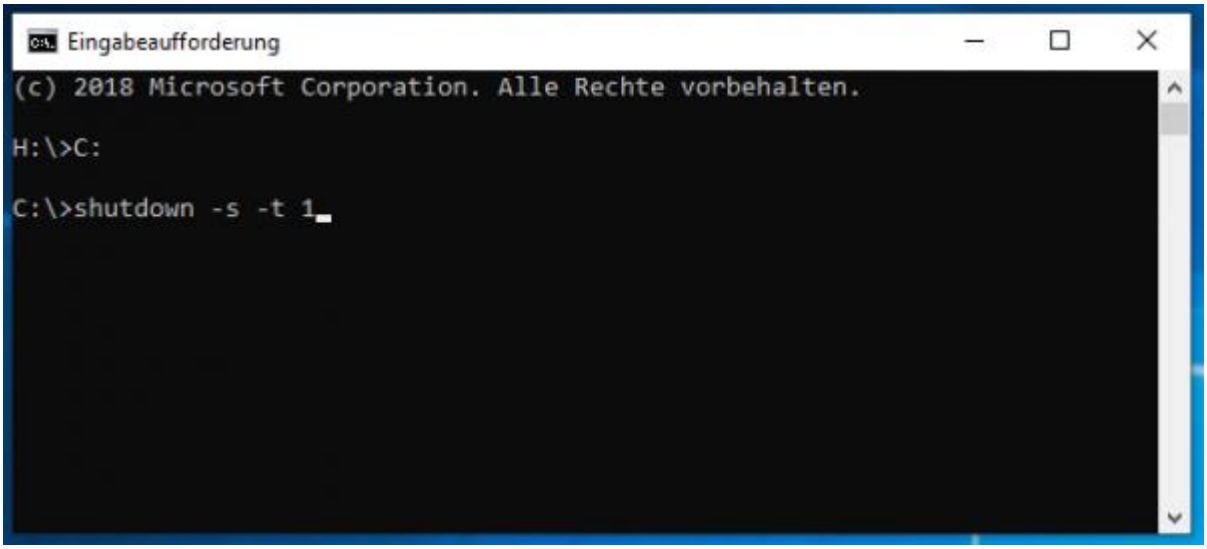

root@server: ~
* Support: https://ubuntu.com/advantage
System information as of Mon Jul 15 11:52:56 UTC 2019
System load: 0.2 Processes: 167
Usage of /: 9.9% of 48.96GB Users logged in: 0
Memory usage: 17% IP address for ens18: 10.0.0.1
Swap usage: 0%
* MicroK8s 1.15 is out! It has already been installed on more
than 14 different distros. Guess which ones?
https://snapcraft.io/microk8s
* Canonical Livepatch is available for installation.
- Reduce system reboots and improve kernel security. Activate at:
https://ubuntu.com/livepatch
1 Software-Paket kann aktualisiert werden.
0 Aktualisierungen sind Sicherheitsaktualisierungen.
Last login: Fri Jul 5 13:49:20 2019 from 10.0.0.9
root@server:~#


root@server: ~
System information as of Mon Jul 15 12:03:42 UTC 2019
System load: 0.3 Processes: 165
Usage of /: 9.9% of 48.96GB Users logged in: 0
Memory usage: 17% IP address for ens18: 10.0.0.1
Swap usage: 0%
* MicroK8s 1.15 is out! It has already been installed on more
than 14 different distros. Guess which ones?
https://snapcraft.io/microk8s
* Canonical Livepatch is available for installation.
- Reduce system reboots and improve kernel security. Activate at:
https://ubuntu.com/livepatch
1 Software-Paket kann aktualisiert werden.
0 Aktualisierungen sind Sicherheitsaktualisierungen.
Last login: Mon Jul 15 11:52:58 2019 from 10.0.0.9
root@server:~# mv /srv/linbo/examples/win10.global.reg /srv/samba/global/managem
ent/global-admin/


server
Datei
Start
Freigeben
Ansicht
\\server
"server" durchsuchen
Schnellzugriff
Desktop
Downloads
Dokumente
Bilder
Musik
System32
Videos
OneDrive
Dieser PC
3D-Objekte
Bilder
Desktop
default-school
linuxmuster-global
netlogon
PDF
sysvol


Verwalten
global-admin
Datei
Start
Freigeben
Ansicht
Anwendungstools
Netzwerk › server › linuxmuster-global › management › global-admin
"global-admin" durchsuchen
Name
Änderungsdatum
Typ
Größe
globaladmindir1
21.06.2019 17:25
Dateiordner
globaladmindir2
21.06.2019 17:25
Dateiordner
win10.global
14.01.2019 12:10
Registrierungseint...
1 KB
Musik
System32
Videos
OneDrive
Dieser PC
3D-Objekte
Bilder
Desktop
Dokumente
Downloads
Musik
Videos
Lokaler Datenträ
global-admin (\
Netzwerk
3 Elemente
1 Element ausgewählt (914 Bytes)


Alle
Apps
Dokumente
Einstellungen
Web
Mel
Höchste Übereinstimmung
Eingabeaufforderung
App
3
Web durchsuchen
cmd - Webergebnisse anzeigen
2
cmd
1



Domänenanbindung

Geräte die dauerhaft mit den Ressourcen der linuxmuster.net-Umgebung arbeiten sollen, sind nun in der Domäne aufzunehmen. Um Geräte richtig in das AD einzuordnen, sollten diese, wie weiter oben erklärt, zuerst in linuxmuster.net über die MAC mit richtigen Einstellungen aufgenommen worden sein.

Starte den Muster-Client wieder via LINBO, indem Du Win10 mit dem GÜNEN Start-Button aus dem lokalen Cache startest.

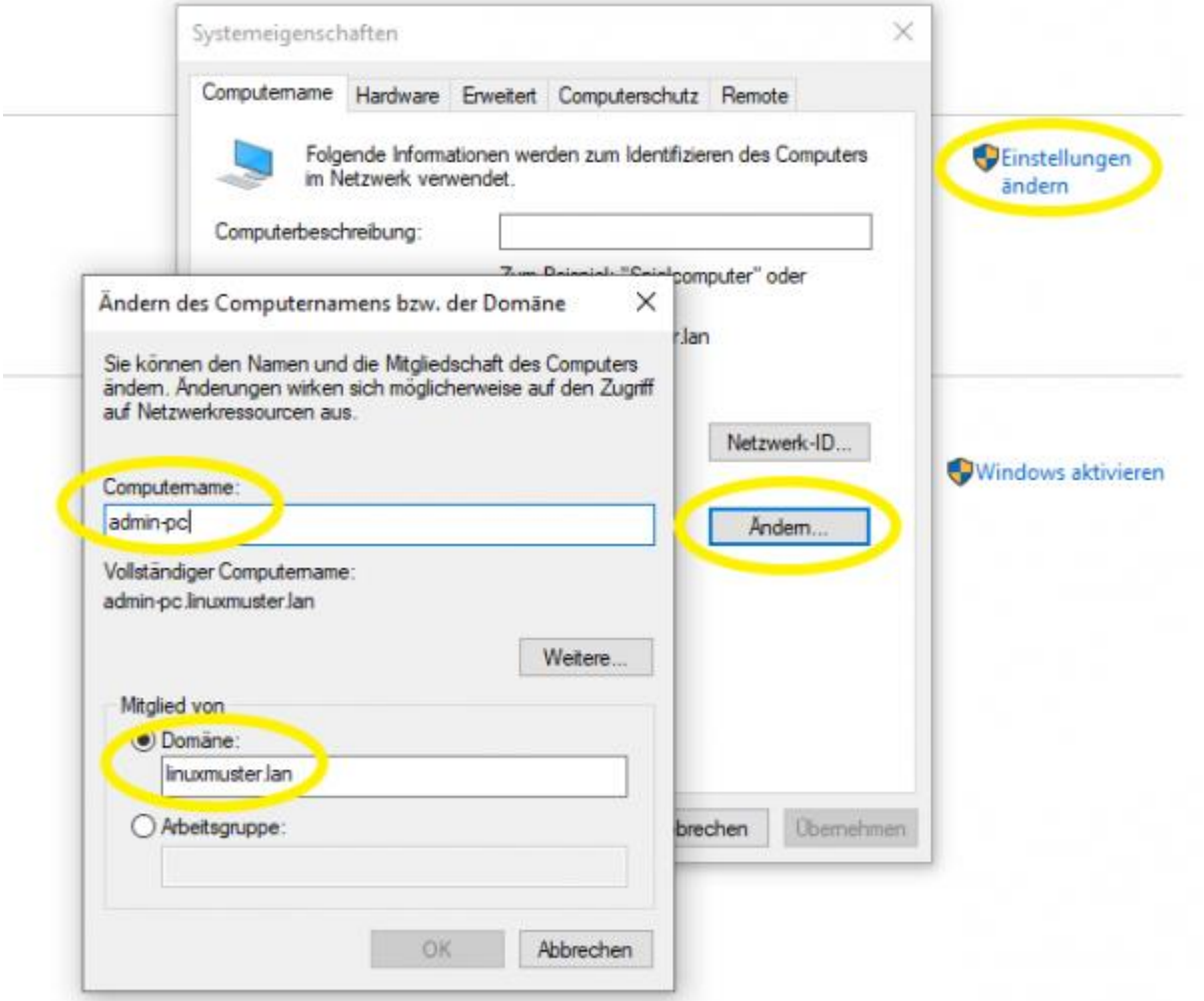
Manueller Domänen Join für Windows

1. Über `Systemsteuerung` → `System und Sicherheit` → `System` → `Einstellungen Ändern` → `Ändern` → `Computernamen` vergeben (übereinstimmend mit Namen in dern Geräteliste!) und unter Mitglied von als Domäne die im Schritt Setup mit der Schulkonsole oder Setup im Terminal gewählten Domain namen, z.B. linuxmuster.lan angeben. Mit `global-admin` und Ihrem beim Setup vergebenen Passwort bestätigen:
2. OK → Windows-Sicherheitsfrage: Hier musst Du Dich als Domänen-Benutzer `global-admin` anmelden. Zum Abschluss solltest Du die Meldung erhalten: „Willkommen in der Domäne ....“.
3. Danach musst Du das Fenster zum Neustart des PCs bestätigen. Schließe das Fenster der Domänenaufnahme. Es erscheint der Hinweis, dass der PC neu gestartet werden muss. Bestätige den Neustart.

Der PC bootet nun wieder in LINBO.

Achtung: Starte Windows 10 nun **NICHT** neu !

Es muss nach diesem Domänenbeitritt ein Muster-Image erstellt werden.


Systemeigenschaften
Computername
Hardware
Erweitert
Computerschutz
Remote
Folgende Informationen werden zum Identifizieren des Computers im Netzwerk verwendet.
Computerbeschreibung:
Einstellungen ändern
Ändern des Computernamens bzw. der Domäne
Sie können den Namen und die Mitgliedschaft des Computers ändern. Änderungen wirken sich möglicherweise auf den Zugriff auf Netzwerkressourcen aus.
Computername:
admin-pc
Vollständiger Computername:
admin-pc.linuxmuster.lan
Weitere...
Mitglied von
Domäne:
linuxmuster.lan
Arbeitsgruppe:
OK
Abbrechen
Netzwerk-ID...
Ändern...
Windows aktivieren
Übernehmen

LINBO Muster-Image mit Domänenbeitritt

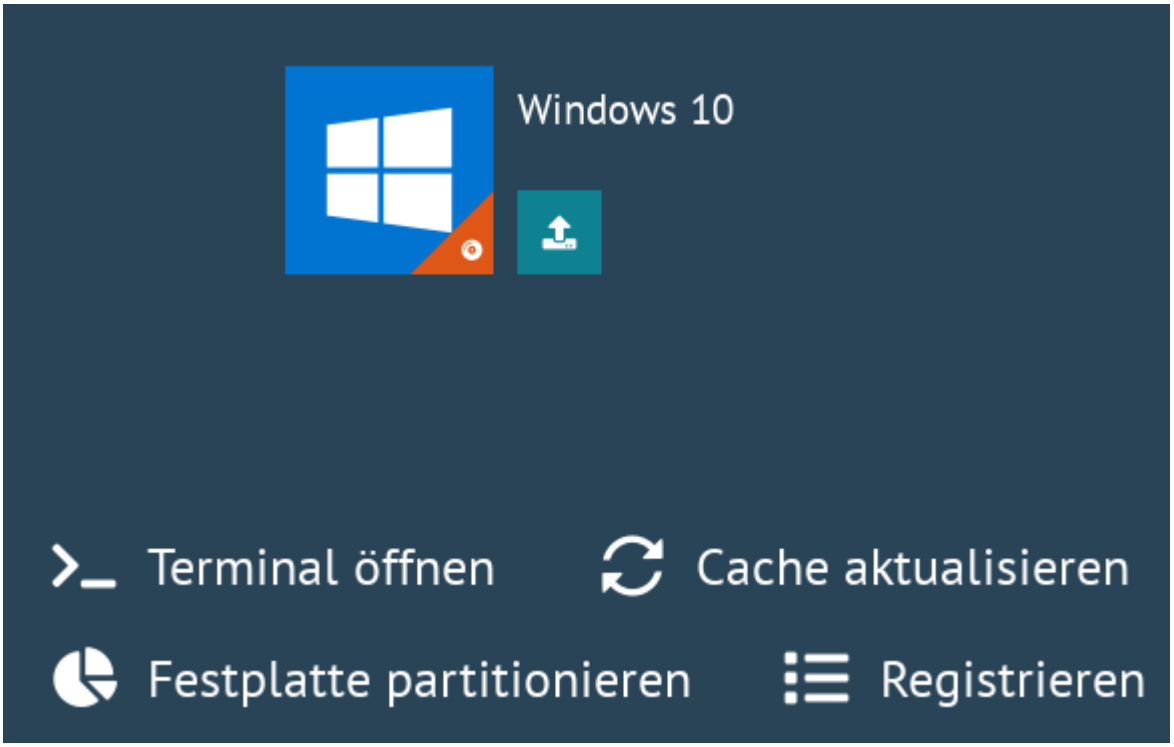
Nachdem der Muster-client mit Windows 10 - wie zuvor beschrieben - der Domäne hinzugefügt wurde, erstellst Du jetzt ein Image für den Muster-Client. Wird dieses Image auf andere Maschinen übertragen, so sind diese bereits in der Domäne aufgenommen.

Hierbei ist es notwenig, das für das Image in der Registry, den Namen der PCs jeweils automatisch anzupassen, da sonst jeder PC, der das Image kopiert, den selben Rechnernamen hätte.

Hinweis: Achtung: Nachdem eine Template-Maschine frisch der Domain gejoined ist, darf diese vor dem Upload nicht neugestartet 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.

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:



2. Klicke nun das grosse Windows-Symbol, um das Image zu erstellen. Es öffnet sich folgender Dialog:

Gib an, ob ein aktuelles Image ersetzt werden soll, den gewünschten Image-Namen (die Dateiendung ist immer .qcow2). Zudem kannst Du eine Beschreibung angeben, die Dir Hinweise zum Konfigurationsstand des Images gibt. Da Du das erste Image erstellst, klicke 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`

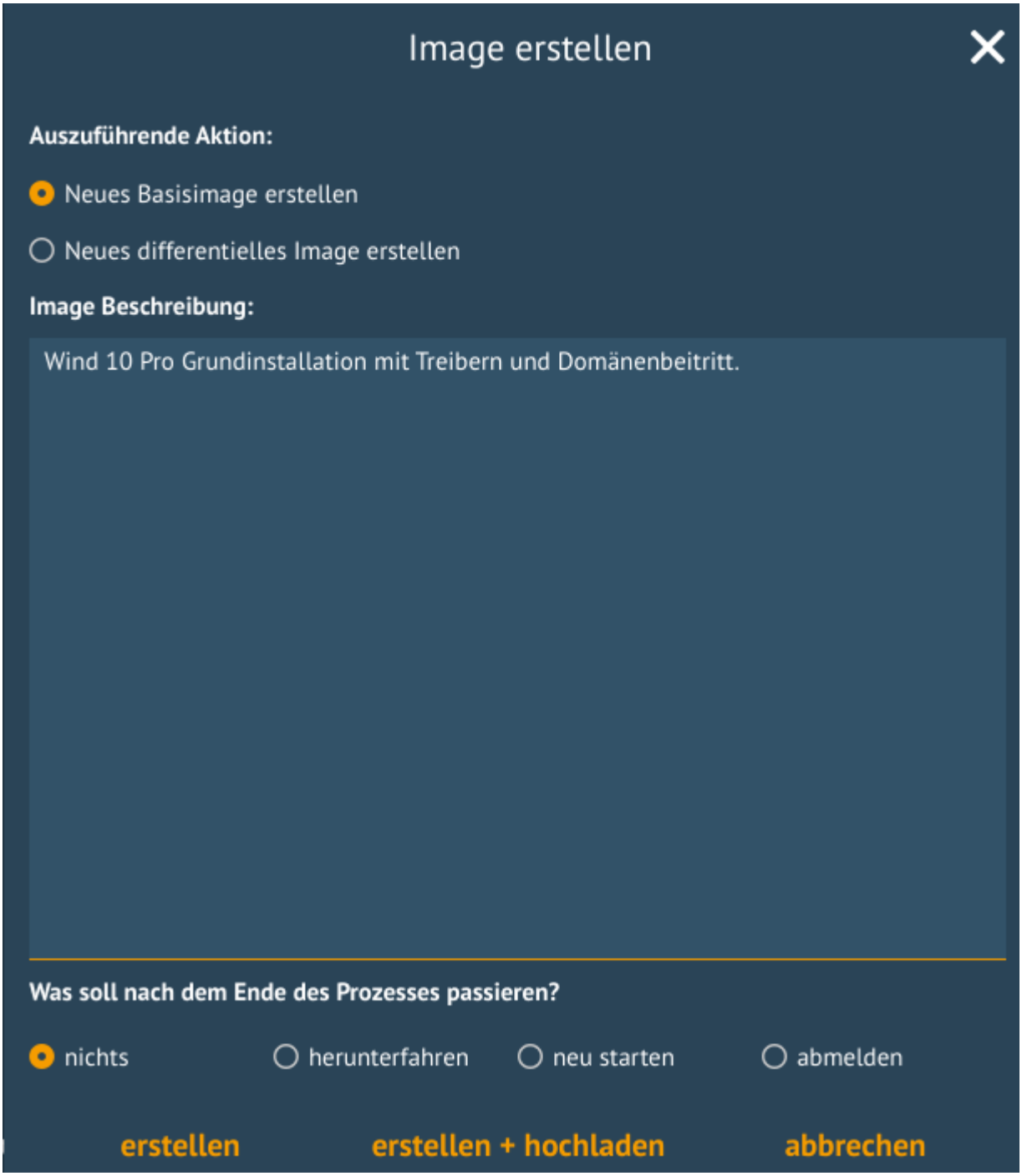
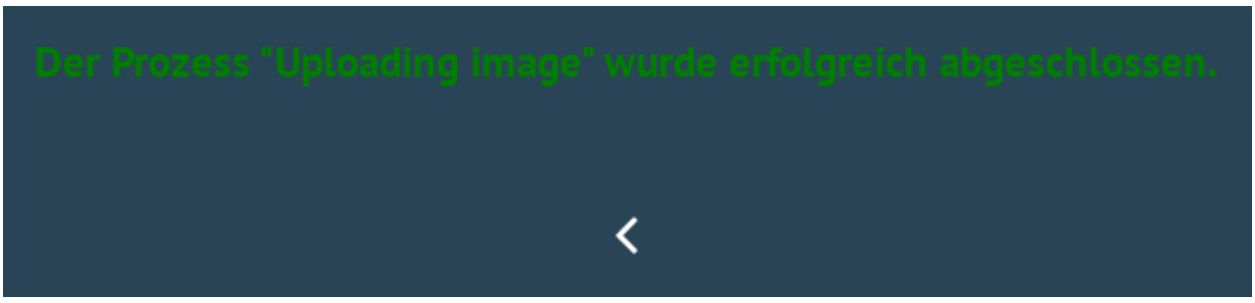
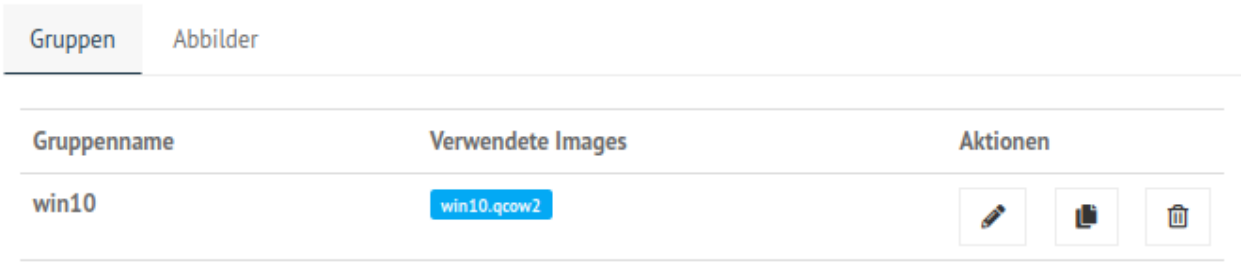


Image erstellen
Auszuführende Aktion:
Neues Basisimage erstellen
Neues differentielles Image erstellen
Image Beschreibung:
Wind 10 Pro Grundinstallation mit Treibern und Domänenbeitritt.
Was soll nach dem Ende des Prozesses passieren?
nichts
herunterfahren
neu starten
abmelden
erstellen
erstellen + hochladen
abbrechen


Der Prozess "Uploading image" wurde erfolgreich abgeschlossen.



Zudem finden sich die Abbilder selbst unter `` LINBO4 → Gruppen → Abbilder`` aufgelistet.

Falls der Gruppe anfangs kein Basisimage zugeordnet war, sollte das unter `Groups` → <gruppenname> → `Partitionen` → `Windows 10 edit` → `OS` → `Basisimage` nachgeholt werden. Speichern nicht vergessen.

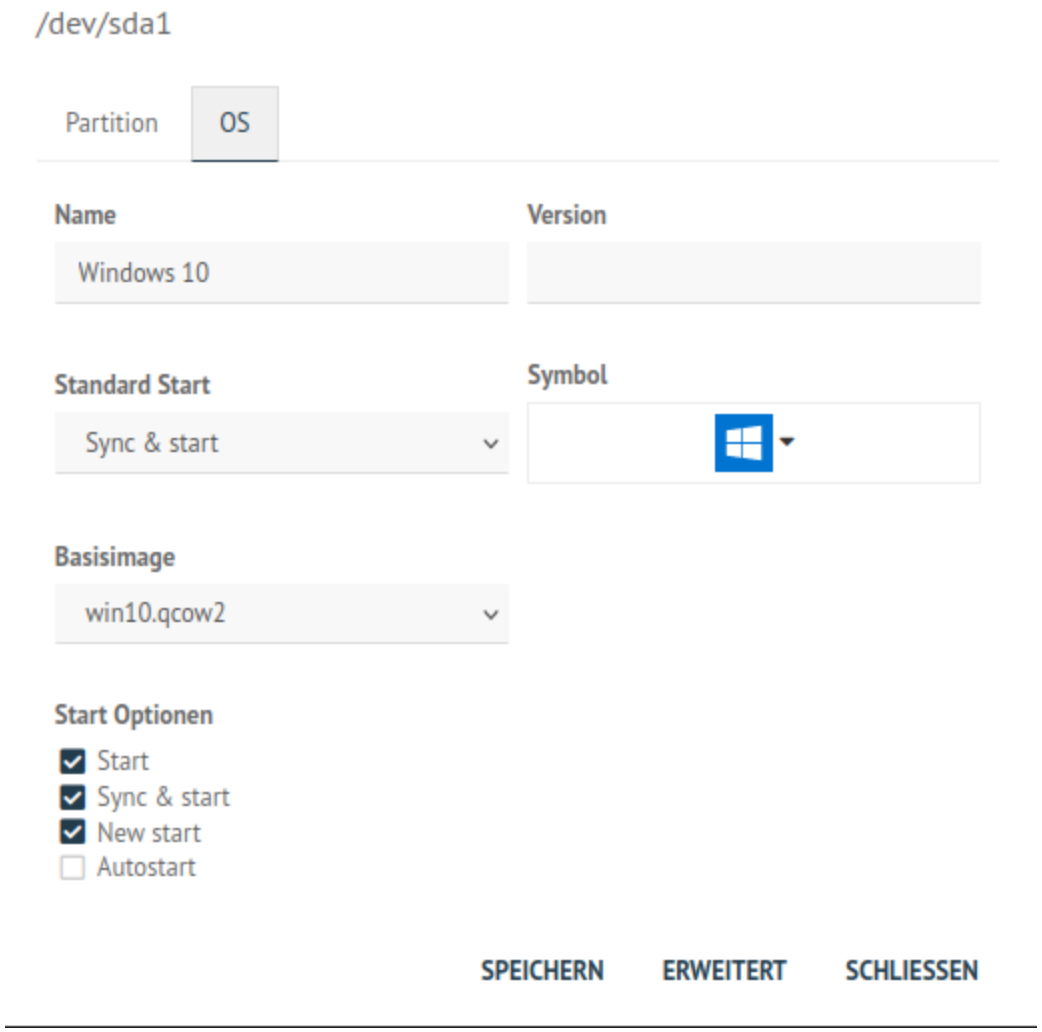
4. Einem Image muss ein Registry Patch angeben werden: Wähle dazu das gewünschte Image aus, klicke auf das Zahnrad-Symbol, gehe zur Reiterkarte `Registry-Patch`. Klicke nun unten auf die Drop-down Liste `Copy from` -> `win10.image.reg`. Es wird die Reg-Datei in dem Fenster angezeigt.

5. Alternativ in der Server-Shell aus `/srv/linbo/exmaples` die richtige Vorlage in `/srv/linbo` kopieren. Die Datei trägt dann den Namen <`imagename`>`.reg` - also in o.g. Beispiel win10.reg.

6. In Zeile 22 musst Du noch Folgendes ergänzen:

```
;setzt den Domänennamen richtig
[HKEY_LOCAL_MACHINE\System\ControlSet001\Services\Tcpip\Parameters]
"Domain"="<SAMBADOMAIN>"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]
"DefaultLogonDomain"="<SAMBADOMAIN>"
```

Hier <SAMBADOMAIN> durch den zuvor festgelegten Namen der Samba_Domäne ersetzen. Hattest Du z.B. während der Installation gshoenningen.linuxmuster.lan gewählt, so gibst Du hier nur gshoeningen an. Übernehme die Eintragungen mit `Speichern`.


/dev/sda1
Partition
OS
Name
Windows 10
Version
Standard Start
Sync & start
Symbol
Basisimage
win10.qcow2
Start Optionen
Start
Sync & start
New start
Autostart
SPEICHERN
ERWEITERT
SCHLIESSEN


win10
Caution ! This feature is still under heavy test.
Renaming image or restoring backups do not work properly yet and is only published for test purpose.
Allgemein
Registry Patch
Postsync-Skript
Prestart Skript
1 Windows Registry Editor Version 5.00
2
3 ; linuxmuster.net 7
4
5 ; patches hostname, to be applied after every image sync
6
7 [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\ComputerName\ActiveComputerName\]
8 "ComputerName"="{$HostName$}"
9
10 [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\ComputerName\ComputerName\]
11 "ComputerName"="{$HostName$}"
12
13 [HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\Tcpip\Parameters\]
14 "Hostname"="{$HostName$}"
15 "NV Hostname"="{$HostName$}"
16
17 [HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters]
18 "NV Hostname"="{$HostName$}"
19 "Hostname"="{$HostName$}"
20
21 ; add your custom registry patches below
22 [HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters]
23 "Domain" = "gshoenningen"
Copy from
SPEICHERN
SCHLIESSEN

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 aufnehmenn

→ `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, um Windows neu zu installieren.

4. Wenn das Image vollständig heruntergeladen ist, startet Windows automatisch.

Default Profil kopieren

Linuxmuster.net sieht vor, dass **Programminstallationen von „global-admin“** durchgeführt werden. Damit alle User die bei der Installation vorgenommenen Änderungen bekommen, muss das Profil des „global-admin“ nach „Default“ kopiert werden. Um das Profil zu kopieren, ist wie folgt vorzugehen:

1. Starte den Rechner nach der Installation von Programmen neu ohne Synchronisation

Achtung: Der Neustart ist notwenig, da das Profil des „global-admin“ ansonsten nicht kopiert werden kann bzw. um die Registry-Zweige für den global-admin freizugeben.

2. Melden Dich als `lokaler User mit Admin-Rechten` an dem Rechner an
3. Lade die Datei `https://www.forensit.com/Downloads/Support/DefProf.msi` herunter. Führe diese aus. Das Programm DefProf.exe befindet sich dann in entpackter Form in Ihrem Download-Verzeichnis. Kopiere dieses Programm in das Verzeichnis: `C:\Windows\system32\`.
4. Führe unter Win10 die PowerShell als Admin aus. Wechsel auf Laufwerk C:und führe den Befehl `C:\> defprof global-admin` aus. Die Nachfrage bei der Ausführung ist zu bejahen.
5. Melde Dich als lokaler User ab und als global-admin an
6. Fahre den Rechner herunter
7. Starte den Rechner neu und erstellen ein neues Image mit LINBO.

Zeitprobleme lösen

Auch wenn bereits beim Start über linbo die Systemzeit synchonisiert wird, sollte auch Windows statt der standardmäßigen Microsoft-Server im Internet den linuxmuster.net Server als NTP-Zeitserver benutzen. Dies kann z.B. per GPO (Computerkonfiguration - Administrative Vorlagen, System, Windows-Zeitdienst und Zeitanbieter) konfiguriert werden.

Bei der Synchronisation zwischen Client und Server kann es zu Beginn zu Zeitabweichungen kommen.

Diese sind dadurch zu beheben, indem Du auf dem linuxmuster.net Server ein Skript aufrufst, welches die NTP-Konfiguration anpasst.

Öffne auf dem Server eine Konsole als Benutzer `root` und gebe folgenden Befehl ein:

```
/usr/share/linuxmuster/fix-ntp_signd-dir.sh
```

Es wird hierdurch das Verzeichnis für NTP Sockets auf dem Server repariert, so dass Windows Clients erfolgreich hierauf zugreifen können. Danach sollte der Zeitabgleich via NTP erfolgreich durchlaufen.

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 großen Differenzen Probleme.

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:

```
# sophomorix-school --gpo-create default-school
```

Anschließend den Samba-Dienst noch neu starten:

```
# systemctl restart samba-ad-dc.service
```

4.12 Upgrade v7.0 auf v7.1

Autor des Abschnitts: @cweikl

4.12.1 Bestehendes System

Du hat linuxmuster.net bereits in der Version 7.0 installiert und Du verfügst über ein lauffähiges System bestehend aus OPNsense® und linuxmuster.net Server basierend auf Ubuntu 18.04 LTS.

Vom Server aus hast Du Internet-Zugriff.

4.12.2 Aktualisierung der Apt-Sources

Es müssen in den Paketquellen die `linuxmuster.net sources` für die neue lmn 7.1 eingetragen und der Schlüssel des Paketservers importiert werden.

Füge das neue repository auf dem Server in der Konsole wie folgt hinzu:

```
sudo -i
wget -qO - "https://deb.linuxmuster.net/pub.gpg" | sudo apt-key add -
sudo sh -c 'echo "deb https://deb.linuxmuster.net/ lmn71 main" > /etc/apt/sources.list.d/
↪lmn71.list'
sudo apt update
```

Danach löscht Du die bisherigen Paketquellen für die Version lmn 7.0. Gebe hierzu im Terminal auf dem Server folgendes an:

```
sudo rm /etc/apt/sources.list.d/lmn7.list
```

Alternativ kannst Du die Einträge in der Datei `/etc/apt/sources.list.d/lmn7.list` wie folgt auskommentieren:

```
# deb https://archive.linuxmuster.net lmn7/
# deb-src https://archive.linuxmuster.net lmn7/
```

Aktualisiere die Paketquellen auf dem Server und migriere / aktualisiere Deinen Server nun auf die Version lmn 7.1 mit:

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

Bestätige die Rückfragen zur Installation mit y / j.

Hinweis: Sollte die Rückfrage kommen, ob die `smb.conf` ersetzt werden soll, antworte unbedingt mit `nein`!

Nach Abschluss der Aktualisierung starte das System einmal neu mit `sudo reboot`.

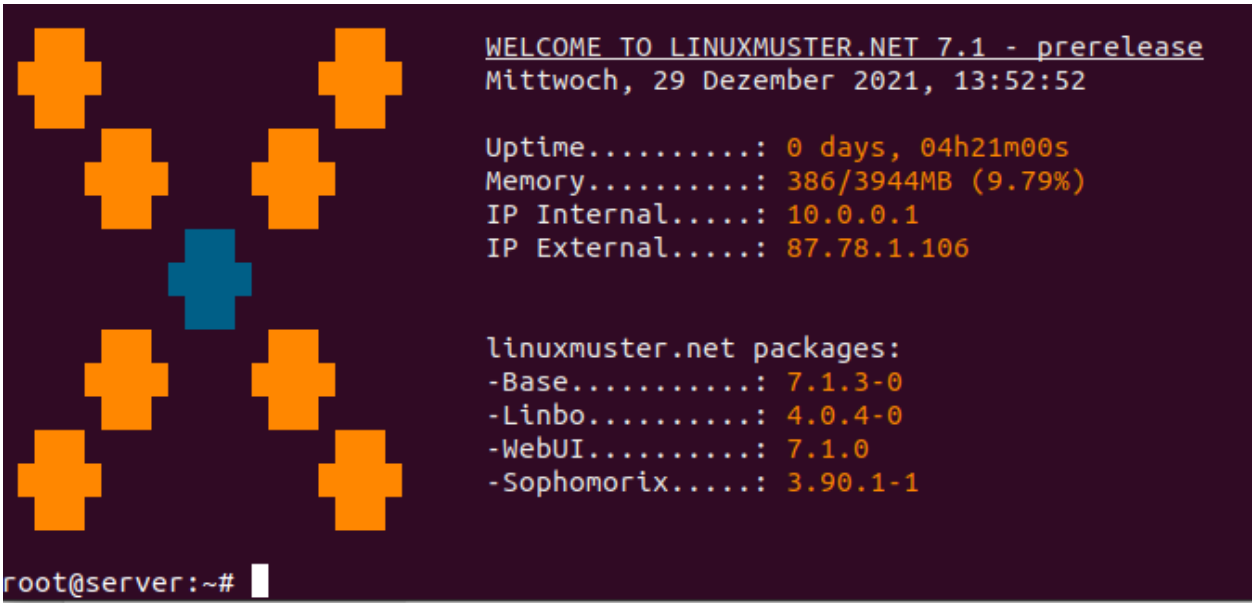
Hat alles erfolgreich funktioniert wirst Du nach der Anmeldung auf der Konsole des Servers mit folgendem Bildschirm begrüßt:

Solltest Du in den Log-Dateien oder bei der Installation folgenden Hinweis finden, kannst Du wie beschrieben das Update entsprechend ausführen:

```
Checking for python3-reconfigure ... WARNING: You are using pip version 20.0.2; however,␣
↪version 21.3.1 is available.
You should consider upgrading via the '/usr/bin/python3 -m pip install --upgrade pip'␣
↪command.
```

Danach musst Du noch Deine Linbo 2.4 Images auf Linbo 4 migrieren. Führe dies wie hier *Migration LINBO 2.4 zu 4.0* beschrieben durch.

Danach ist Dein Update auf linuxmuster v7.1 abgeschlossen und Du kannst wie bisher auch weiterarbeiten.



4.13 Migration LINBO 2.4 zu 4.0

Autor des Abschnitts: @cweikl

4.13.1 Hinweise zu LINBO 4

In der linuxmuster v7.1 löst LINBO 4 das bisherige LINBO 2.4 ab. 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 v7.1 umgestellt, ist es sinnvoll, die bisherigen LINBO 2.4 Cloop-Images zu konvertieren.

LINBO 4 weist einige Besonderheiten auf:

- neues Image-Format mit Abwärtskompatibilität zum alten Format für eine einfach Migration
- Änderungen an der Namensgebung und des Speicherortes der zum Image zugehörigen Dateien
- Es wird nur noch 64-Bit Client-Hardware unterstützt.
- LINBO 4 kann nicht mit linuxmuster v6.2 und kleiner verwendet werden.
- Es gibt derzeit *keine* differentiellen Images. Differentielle Images werden voraussichtlich erst wieder ab LINBO v4.1 unterstützt.

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.

4.14 Migration auf linuxmuster 7.1

Autor des Abschnitts: @cweikl

Um auf die linuxmuster 7.1 zu migrieren, können zwei Wege genutzt werden:

1. Sollte noch eine linuxmuster 6.2 genutzt werden, so ist eine vollständige die Migration durchzuführen. Diese ist deutlich aufwändiger.
2. Wird bereits linuxmuster 7.0 eingesetzt, besteht die Migration auf linuxmuster 7.1 in einem einfachen Upgrade des Servers und einer anschliessenden Migration der bisherigen Linbo 2.4 Images auf Linbo 4.

Folge je nach gegebenen Voraussetzungen Deinem Migrationspfad.

4.14.1 Migration lmn6.2.. –> lmn 7.1

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 v7.1 System

Es wird davon ausgegangen, dass …

- der Server der Version 7.1 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 Dokumenation 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 v7.1 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 druchführen
8. Erstsetup durchführen (*Setup v7.1*)

IPs OPNsense® anpassen .. ————————-

Die IP der externen Schnittstelle (WAN) der OPNsense® ist ggf. anzupassen. Diese ist in der Erstauslieferung so konfiguriert, das 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. Solle 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. Besipiel 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
```

Erhälst Du erfolgreich Pakete zurück, so kanst 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 Eingabekonsole 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 zukunftige 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:

```
./lmn71-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 rufst das Setup mit folgendem Befehl auf:

```
linuxmuster-setup
```

Nach erfolgreichem Setup *Setup v7.1* durchläuft 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 ~ # sophomorix-vampire.. --datadir /path/to/dir/sophomorix-dump --analyze
```

ERROR:
z.B. fehlende Dateien (`/etc/sophomorix/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 ~ # sophomorix-vampire.. --datadir /path/to/dir/sophomorix-dump --create-class-
↪script
server ~ # /root/sophomorix-vampire/sophomorix-vampire-classes.sh
```

Jetzt können die neu erstellten Klassen überprüft werden, beispielsweise

```
server ~ # sophomorix-class -i
server ~ # sophomorix-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 `sophomorix.add` erzeugt, die an die richtige Stelle im System kopiert werden muss, um danach die Benutzer regulär aufzunehmen.

```
server ~ # sophomorix-vampire.. --datadir /path/to/dir/sophomorix-dump --create-add-file
server ~ # cp /root/sophomorix-vampire/sophomorix.add /var/lib/sophomorix/check-result/
↪sophomorix.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/sophomorix/check-result/sophomorix.add korrigiert werden.

```
server ~ # sophomorix-add -i
...
WARNING:
ERROR:
...
```

Die Aufnahme der Benutzer wird ca. 1 Sekunde Zeit pro Benutzer in Anspruch nehmen, Zeit einen Tee zu trinken.

```
server ~ # sophomorix-add
...
```

Die Aufnahme

- nimmt die Benutzer mit ihren Erstpasswörtern auf, dies kann mit

  ```
  server ~ # sophomorix-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 werde mit folgendem Befehl importiert und sollte keine Fehler erzeugen

```
server ~ # sophomorix-vampire.. --datadir /path/to/dir/sophomorix-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 ~ # sophomorix-passwd.. --test-firstpassword
```

Zeige einen oder mehrere Benutzer an

```
server ~ # sophomorix-user -i
server ~ # sophomorix-user -i.. --user name
server ~ # sophomorix-user -i.. --user na*
```

5. Klassenadministratoren importieren .. ———————————————-

Wie bisher

```
server ~ # sophomorix-vampire.. --datadir /path/to/dir/sophomorix-dump --create-class-
↪adminadd-script
server ~ # /root/sophomorix-vampire/sophomorix-vampire-classes-adminadd.sh
```

6. Projekte importieren .. ——————————

Im nachfolgenden Schritt werden alle Projekte importiert.

```
server ~ # sophomorix-vampire.. --datadir /path/to/dir/sophomorix-dump --create-project-
↪script
server ~ # /root/sophomorix-vampire/sophomorix-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 ~ # sophomorix-device -d firewall -i
server ~ # sophomorix-device -r no-pxe -i
```

Überprüfe ob die Namensauflösung funktioniert:

```
server ~ # sophomorix-device.. --dns-test
```

10. Überprüfung von Benutzern und Gruppen .. ————————————————————

Benutzer und Gruppen können mit folgendem Skript getestet werden:

```
server ~ # sophomorix-vampire.. --datadir /path/to/dir/sophomorix-dump --verify-uidi
```

Fehler: Kommando liefert

Unknown option: verify-uid Command line:

You have made a mistake, when specifying options. See error message above.

... sophomorix-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 ~ # sophomorix-vampire.. --rsync-student-home <studentname> --path-oldserver /mnt
server ~ # sophomorix-vampire.. --rsync-teacher-home <teachername> --path-oldserver /mnt
server ~ # sophomorix-vampire.. --rsync-class-share <classname> --path-oldserver /mnt
server ~ # sophomorix-vampire.. --rsync-project-share <projectname> --path-oldserver /mnt
```

Jetzt können alle Schüler, Lehrer, Klassen und Projekte in einem Schritt importiert werden

```
server ~ # sophomorix-vampire.. --rsync-all-student-homes --path-oldserver /mnt
server ~ # sophomorix-vampire.. --rsync-all-teacher-homes --path-oldserver /mnt
server ~ # sophomorix-vampire.. --rsync-all-class-shares --path-oldserver /mnt
server ~ # sophomorix-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 ale Proxy-Skript auf dem Client
8. Entferne lightdm als Anmeldemanager
9. Installiere gdm3 als Anmeldemanager
10. Führe das Setup des neuen Pakets linuxmuster-linuxlient7 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 deinstallierenn ist. Ggf. must 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 detailiert unter *Muster-Client aufsetzen* beschrieben.

4.17 LINBO4 nutzen

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-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 Bennenung 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.

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.

Abb. 4: Linbo Startbildschirm

Sobald der Client registriert wurde, zeigt der Startbildschirm weitere Optionen an.

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

Abb. 5: Linbo Startbildschirm eines aufgenommenen Clients

Abb. 6: Client Informationen - F1

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.

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. 7: 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.

Abb. 8: Start Icon

Abb. 9: 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“.

Tools-Icon

Um Images zu verwalten, klickst Du zunächst auf das Werkzeug-Icon.

Abb. 10: 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.

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
```

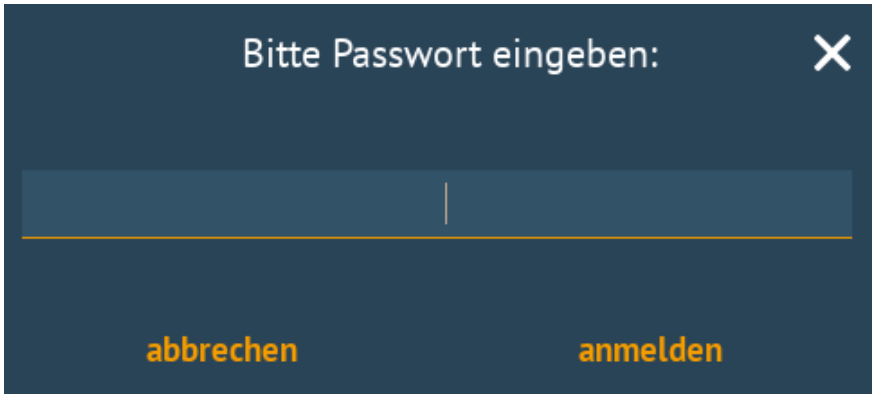


Abb. 11: LINBO Passwort

4.17.2 LINBO Imageverwaltung am Client

Über den Tab `Tools` erhält der Administrator neue Funktionen.

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.

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:

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 Registrierungdialog 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 wir 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.

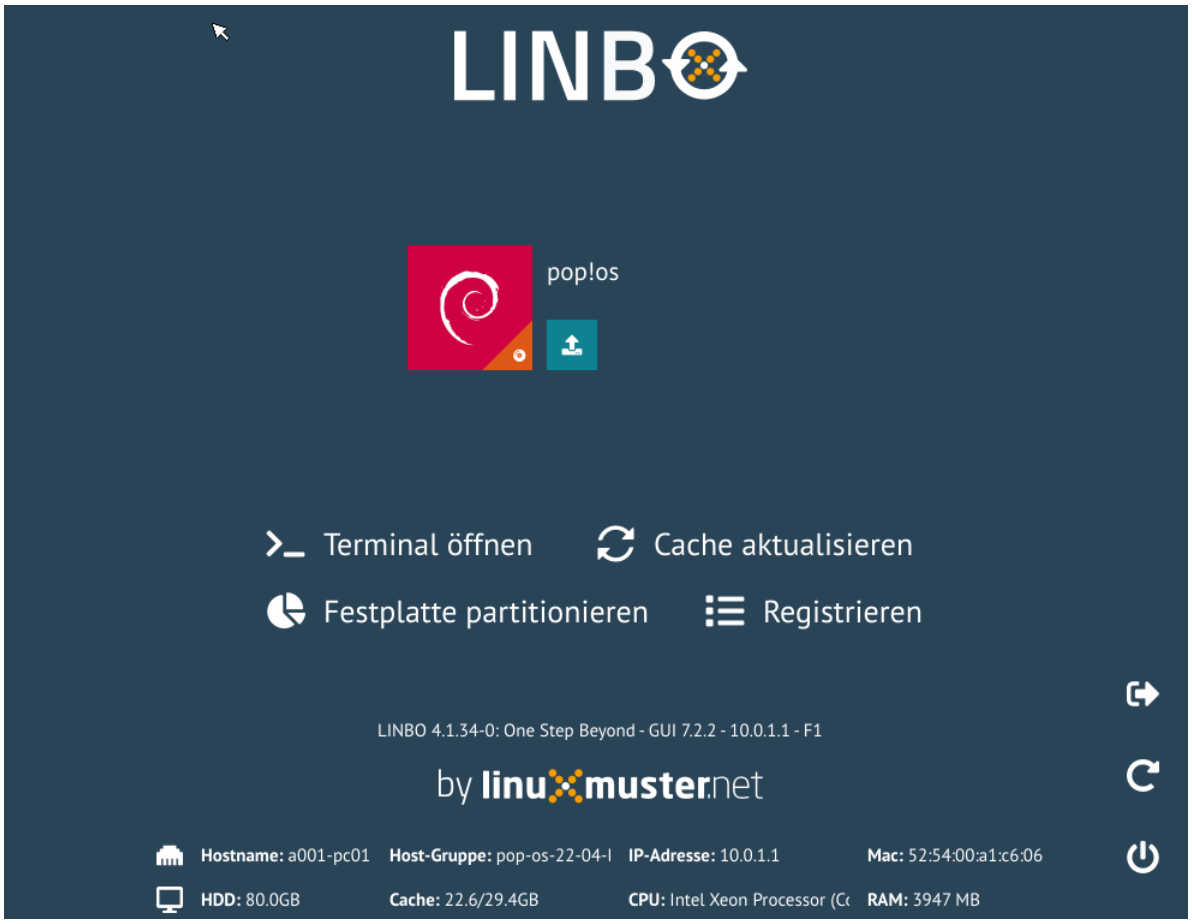


Abb. 12: LINBO Tools

Abb. 13: Image erstellen

Abb. 14: Image hochladen

Abb. 15: Console

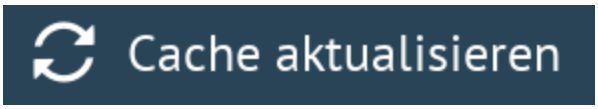


Abb. 16: Cache aktualisieren

Abb. 17: 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. 18: Registrieren

Abb. 19: Image erstellen

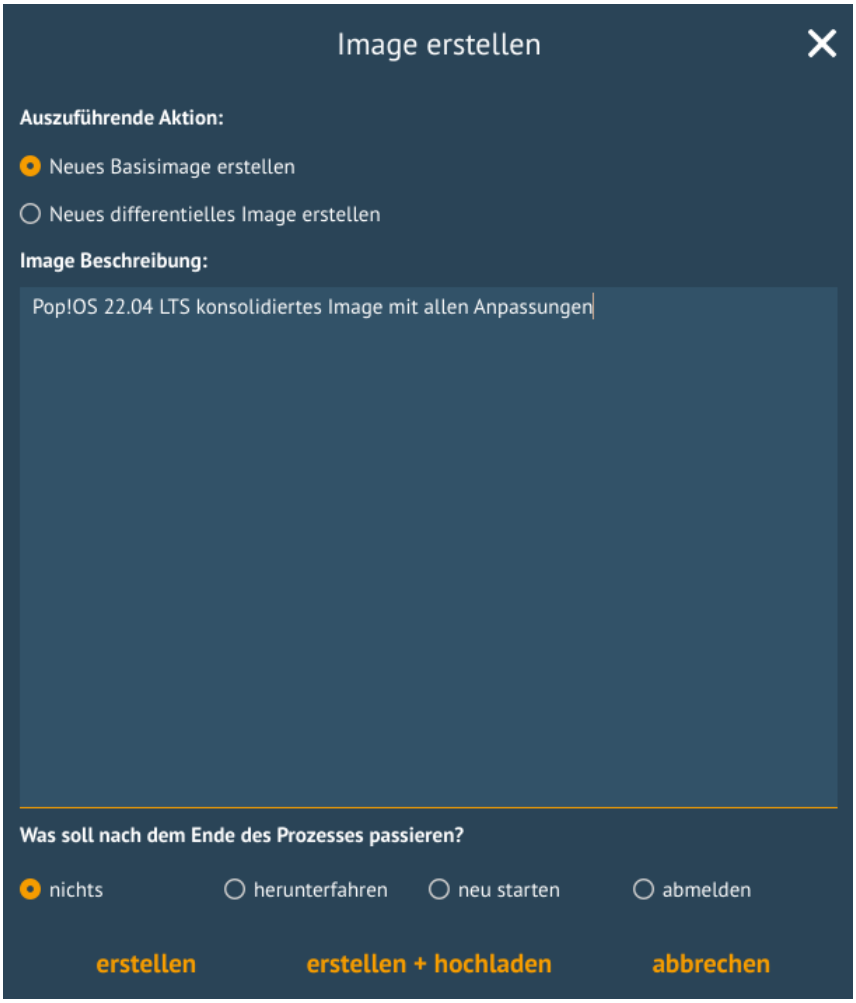


Abb. 20: LINBO - Image erstellen

Abb. 21: LINBO Image hochladen

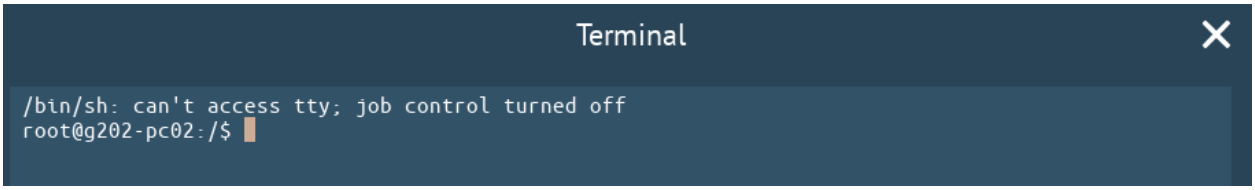


Abb. 22: LINBO Konsole

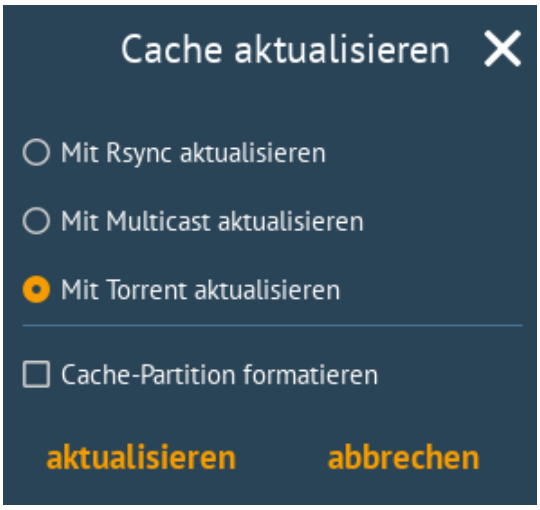


Abb. 23: LINBO Update Cache

Dialog: Registrieren

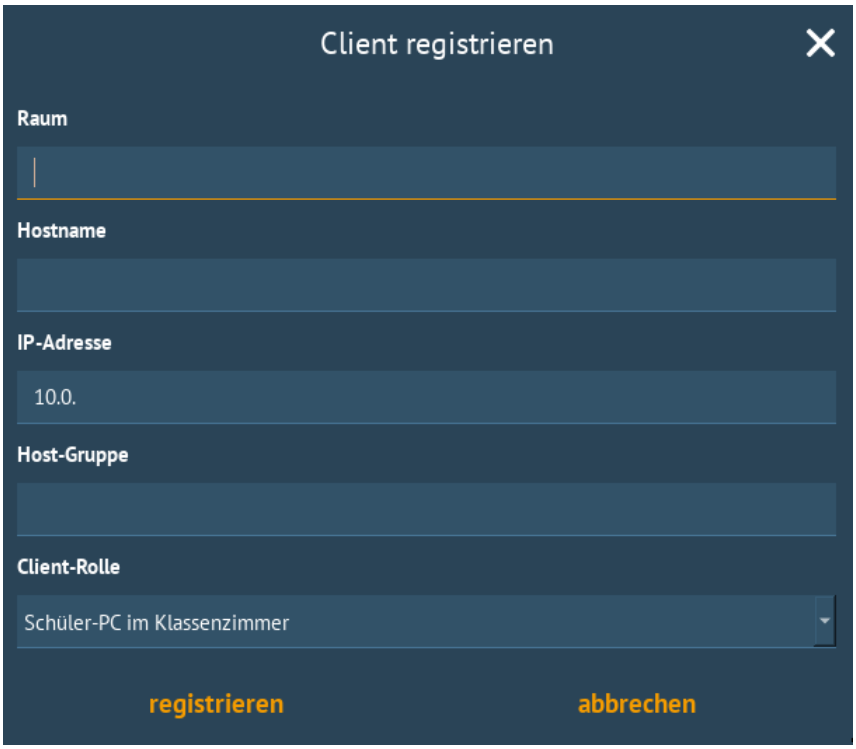


Abb. 24: LINBO Client registrieren

Mit diesem Dialog kann ein erstmalig genutzer 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 duch 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:

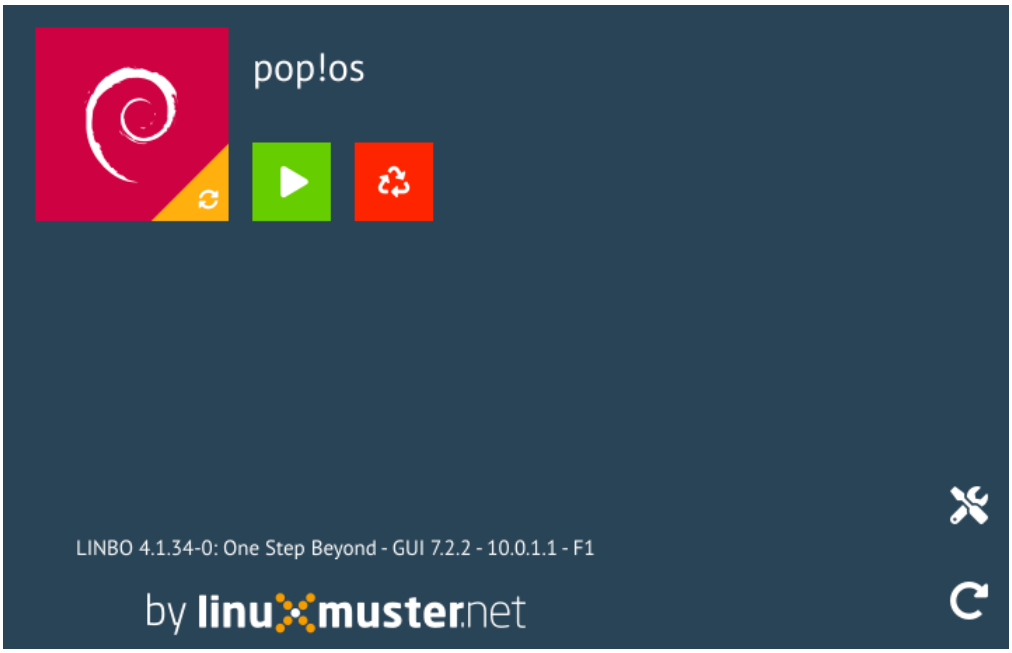


Abb. 25: LINBO GUI

Wähle rechts das Werkzeug-Icon

aus.

Abb. 26: Tools Icon

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.

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.

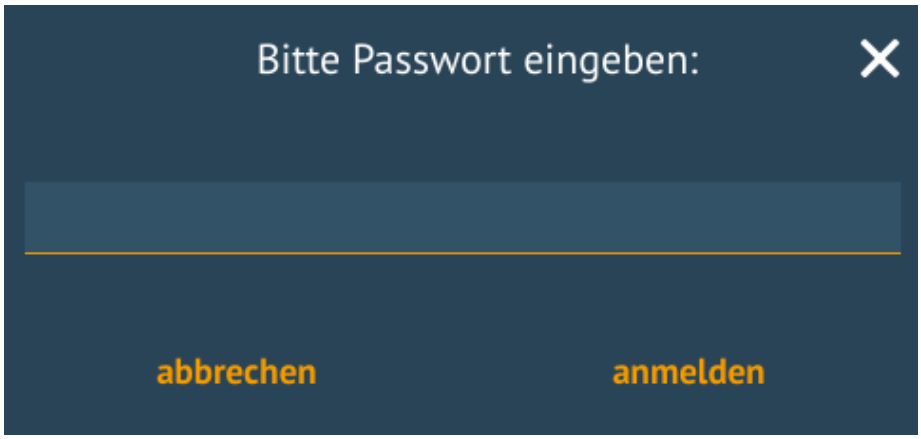


Abb. 27: LINBO Passwort

Abb. 28: LINBO Image Menü

Abb. 29: Icon neues Image

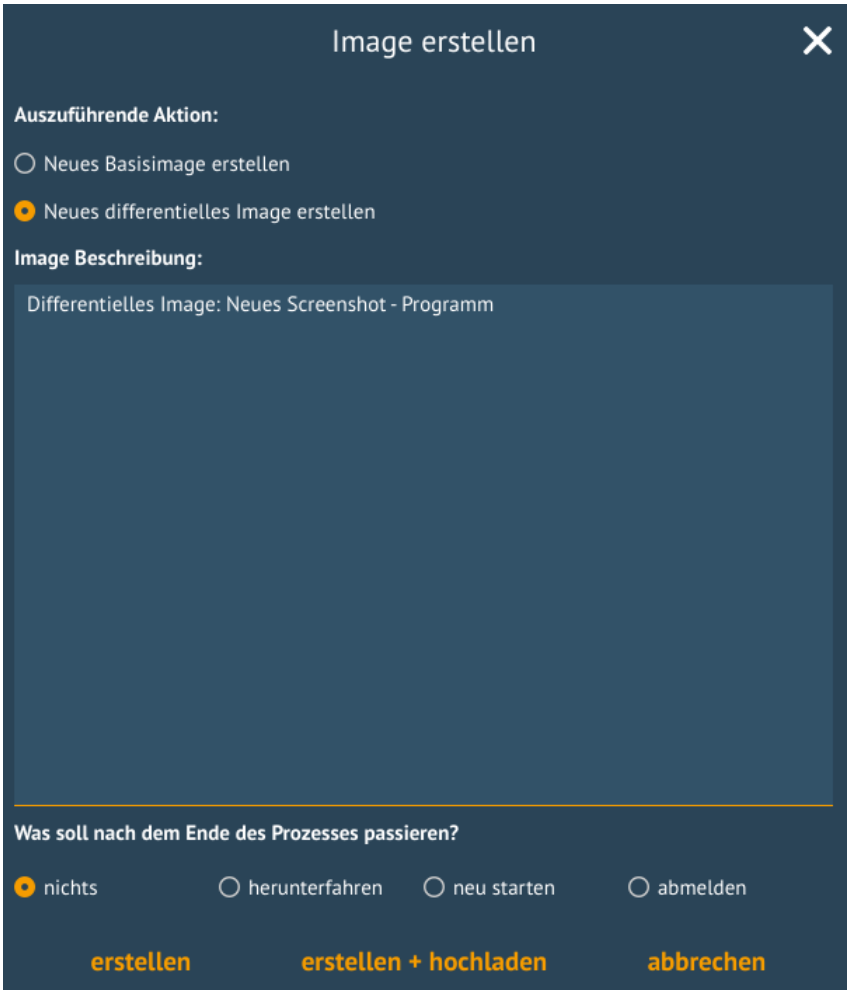


Abb. 30: LINBO Image erstellen

Abb. 31: 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. 32: LINBO Image erstellt

Starte im Anschluss LINBO neu, indem Du das entsprechende Icon auswählst:

Abb. 33: Icon neu starten

Image synchronisieren

Nachdem LINBO neu gestartet wurde, erscheint wieder die LINBO-GUI.

Abb. 34: LINBO-GUI: Boot-Icons

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.

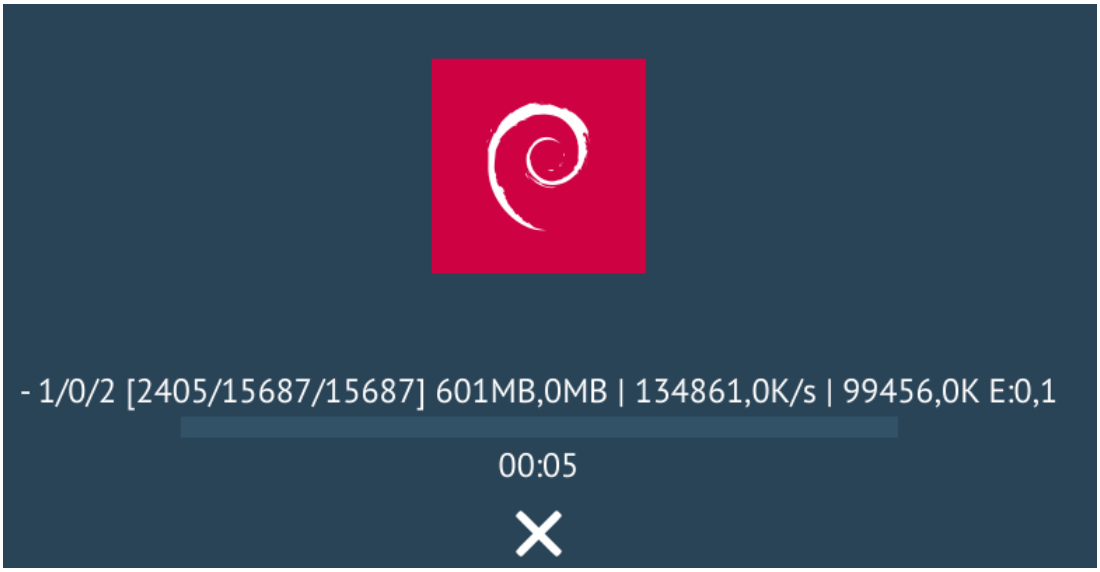


Abb. 35: Fortschrittsbalken

Imageverwaltung aufrufen

Abb. 36: 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.

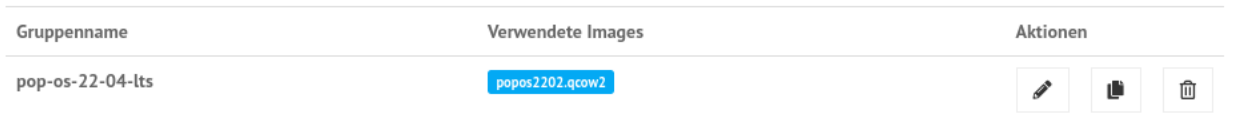


Abb. 37: LINBO Hardwaregruppen

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 Dateiendung `.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.

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.

Abb. 38: Überblick der LINBO-Images

Basis-Image

Abb. 39: 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. 40: 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 Dateiendung `.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).

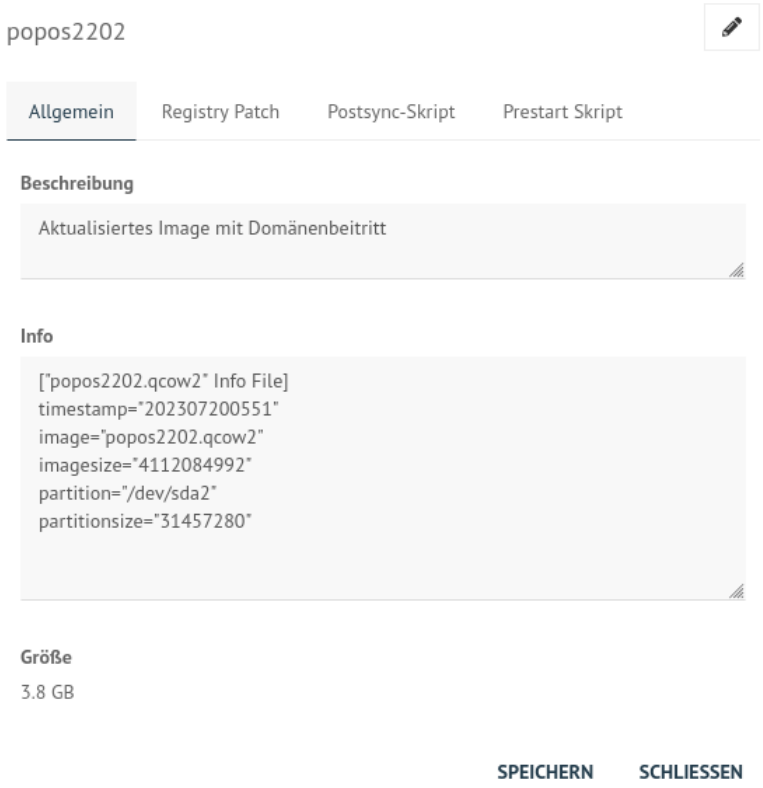


Abb. 41: Informationen zum Image

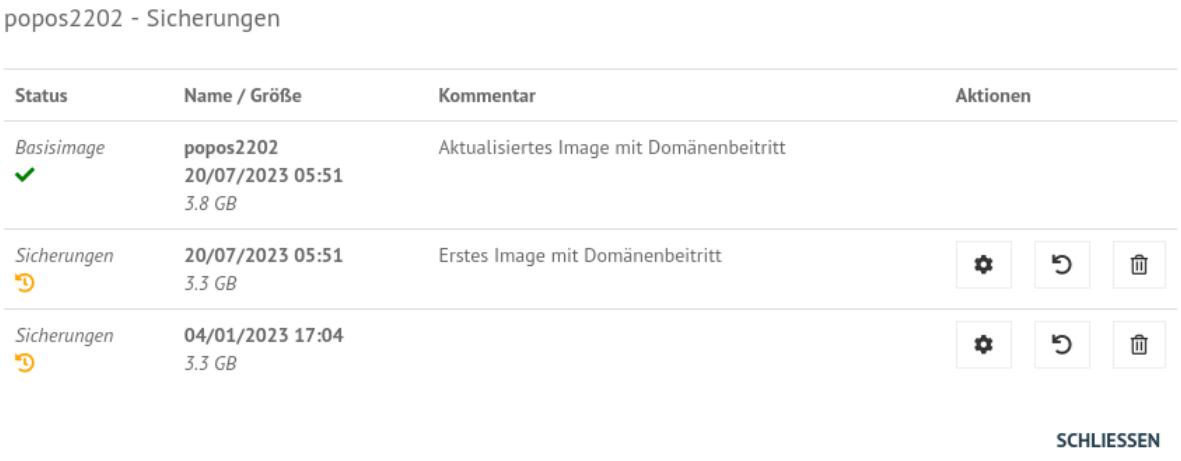
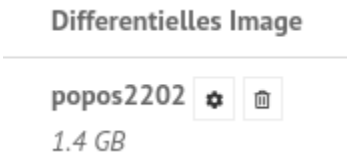


Abb. 42: Image-Sicherungen

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:

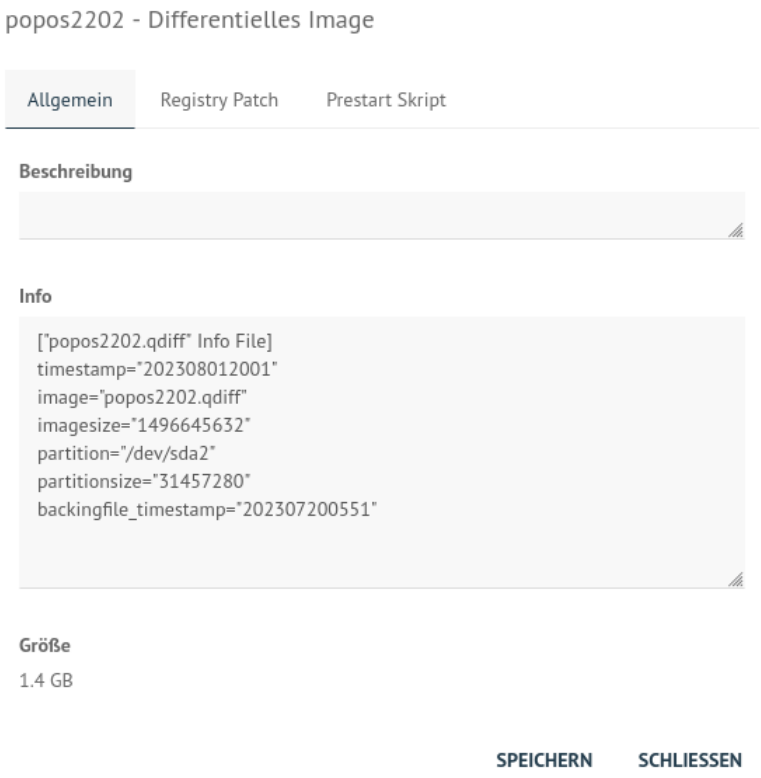


Abb. 43: Informationen zum diff. Image

Unter der Reiterkarte `Allgemein` findest Du Informationen zu dem differentiellen Image wie z.B. den Zeitstempel oder den Imagenamen. Die Dateiendung `.qdiff` steht für ein differentielles Image.

Hier kannst Du Änderungen bzw. Ergänzungen vornehmen und diese mithilfe des Buttons `SPEICHERN` dauerhaft anwenden.

4.17.5 Boot-Bildschirme in LINBO

Beim Booten in LINBO sind folgende Bildschirme sichtbar:

Bootvorgang via Netzwerk

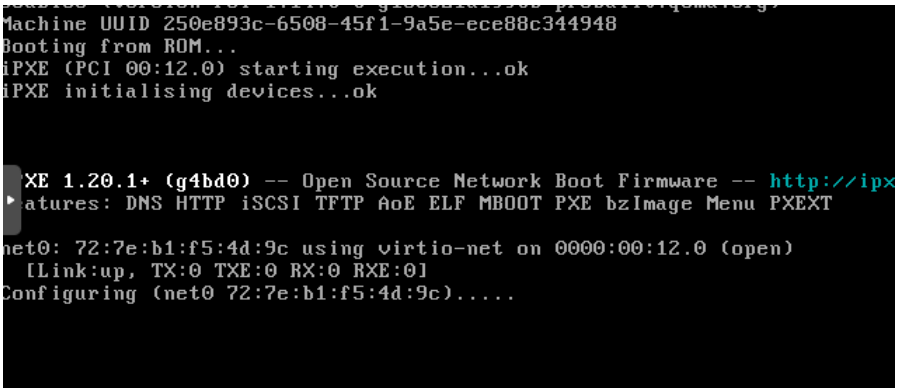


Abb. 44: Initialmeldungen beim Bootvorgang via Netzwerk (PXE)

Egal ob über die lokale Festplatte gebootet wurde oder nach dem Bootvorgang via Netzwerkkarte (PXE) wird mit der Gruppenkonfiguration der Kernel geladen.

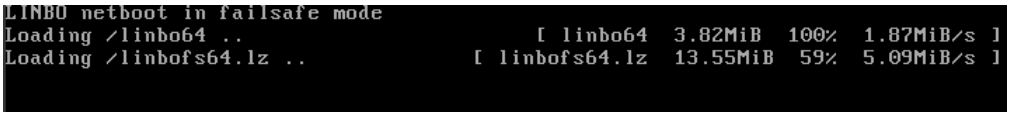


Abb. 45: Bootbildschirm: Laden des Kernels

Der gebootete LINBO-Kernel erscheint als ASCII-Art.

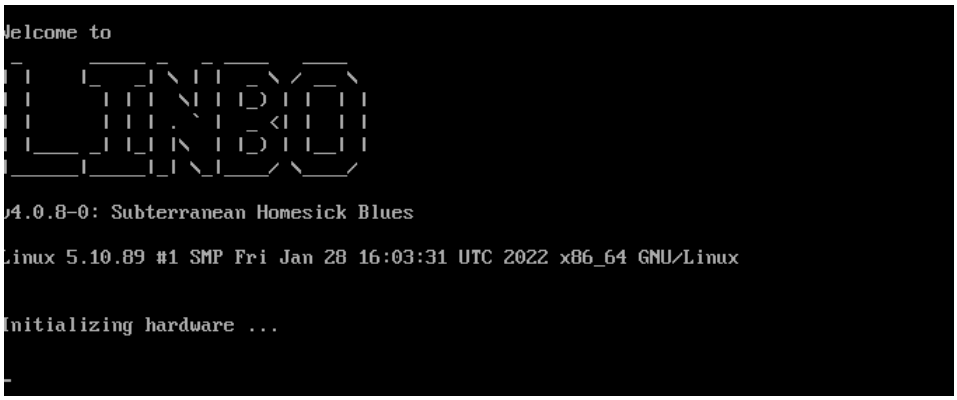


Abb. 46: LINBO-Kernelboot ASCII-Art

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.

Abb. 47: Login WebUI

Wähle danach links den Menüpunkt `LINBO4` aus.

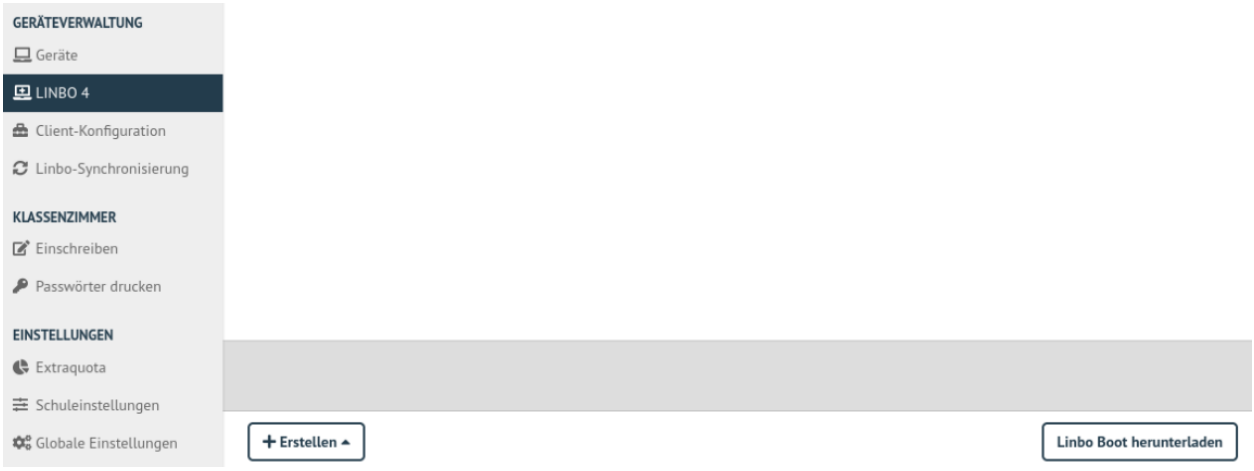


Abb. 48: LINBO4 Menüeintrag

Rechts im Fenster erscheinen ganz unten zwei Buttons. Klicke nun den Button `Linbo Boot herunterladen`.

Es erscheint ein Fenster zum Download des ISO-Images.

Das Booten eines Rechers 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

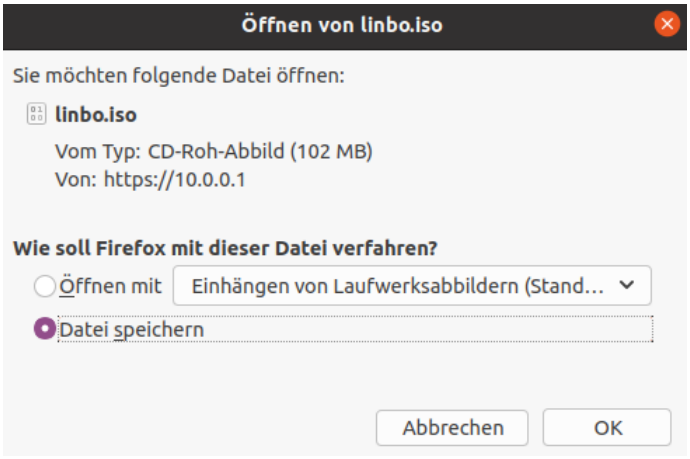


Abb. 49: Download des LINBO-Images

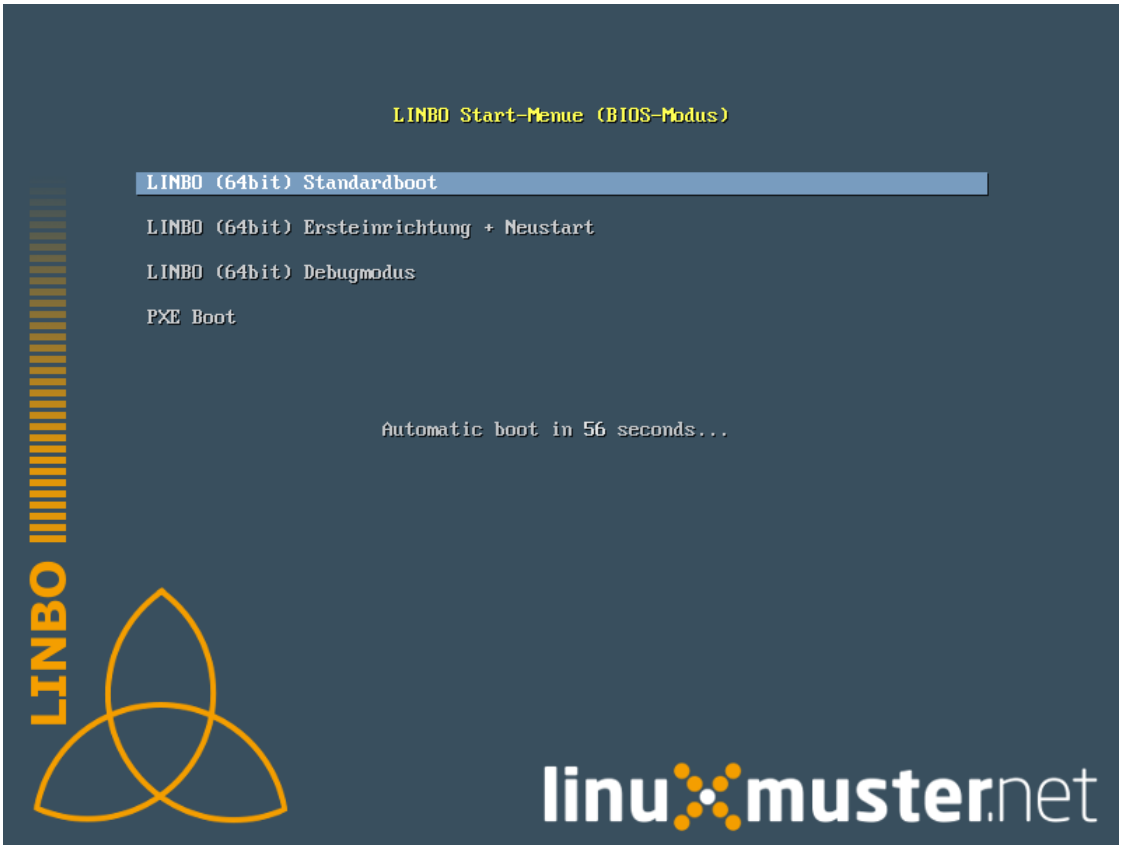


Abb. 50: LINBO Screen

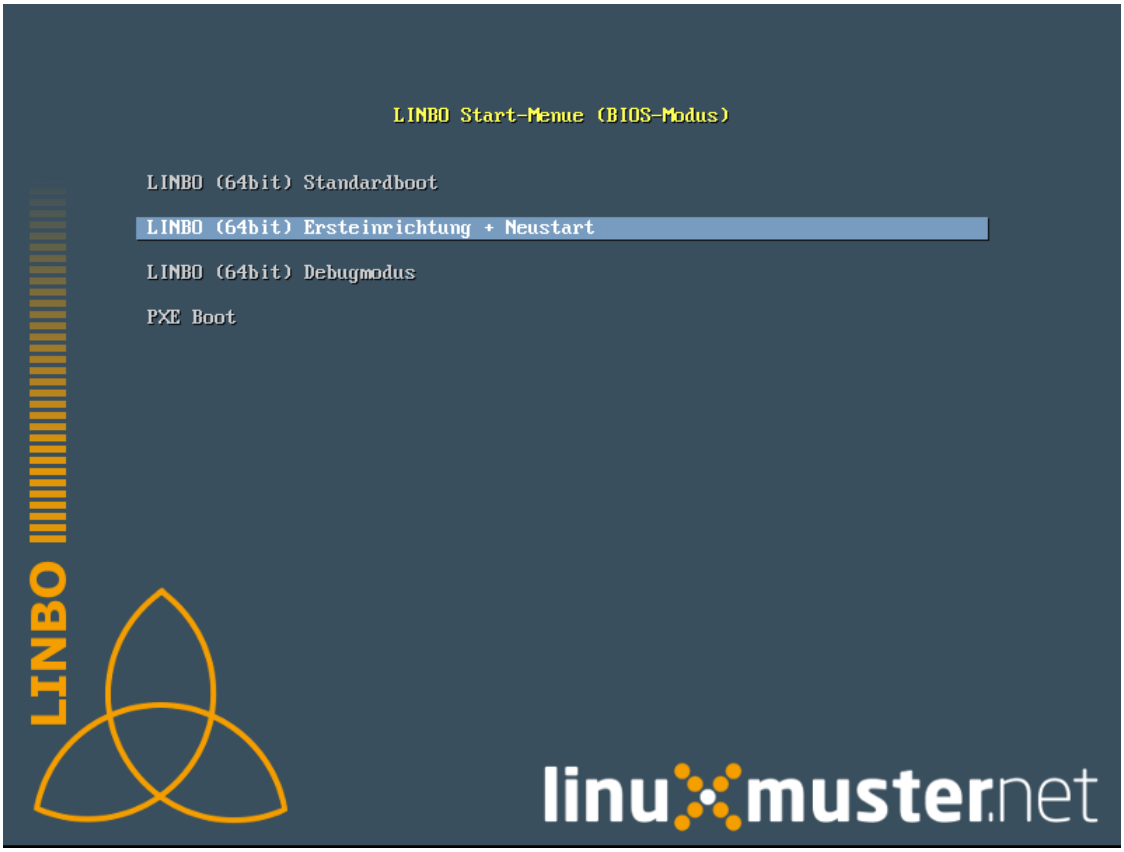


Abb. 51: LINBO Start-Menü

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.

4.17.7 LINBO4-Cache: Hinweise

Linbo4 nutzt auf jedem Client eine lokale Cache-Partition, um ein oder mehrere Image/s eine 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 Geruppe r101 gesendet, um diese „aufzuwecken“. Nach einer Wartezeit von 60 Sekunden werden die angegebenen Befehle an dien 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 Betriebsysystem, das in der start.conf an der angegebenen <#> Position eingetragen wurde.

- start:<#>: Startet das Betriebsyssystem, das in der start.conf an der angegebenen <#> Position eingetragen wurde.

4.17.8 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/
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
↪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.

4.18 Linux-Client - Anpassungen mit Postsync-Scripten

Linux-Clients können in linuxmuster.net mithilfe sogenannter Postsync-Scripte an besondere Nutzungssituationen sehr variabel angepasst werden.

Nach erfolgreicher Synchronisation mit dem Client-Image, das auf dem Server liegt, werden weitere Scripte 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-Scripte

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-Script 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-Script ?

Ein Beispiel für ein universelles Postsync-Script liegt im Verzeichnis `/srv/linbo/examples/postsync`.

Das Postsync-Script ist in dem Verzeichnis abzulegen, in dem sich das Image befindet, auf das das Script angewendet werden soll. Der Name für das Postsync-Script 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-Scriptes

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-Scripte

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 Imagenamen (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 Rechnermane: 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 Scripte ausgeführt werden können.

So können z.B. spezielle Anpassungen von PCs in einem bestimmten Raum vorgenommen werden. Alle abzuarbeitenden Scripte müssen im Verzeichnis `postsync.d` liegen.

Sollen Scripte für die `Patchklasse focalfossa` und dann nur auf `PCs im Raum r100` angewendet werden, so müssen die Scripte in folgendem Verzeichnis liegen:

```
/srv/linbo/linuxmuster-client/focalfossa/r100/postsync.d/
```

Die Skripte müssen sh-Scripte sein, da Linbo keine BASH als Shell kennt. In diesen Scripten ist der Shebang `#!/bin/sh` voranzustellen. Diese Scripte müssen zur Anwendung für die gewünschte Patchklasse in das jeweilige Verzeichnis kopiert und angepasst werden. Diese Scripte 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-Scripte finden sich unter `./common/postsync.d/` und werden in lexikalischer Reihenfolge abgearbeitet. Zudem wird für den `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
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
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
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
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
    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"

# 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
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
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 $LOG
  for pack in /cache/${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
 # wenn es /mnt/tarpacks gibt - löschen
 rm -rf /mnt/tarpacks

# hostname in /etc/hosts patchen
    sed -i "s/HOSTNAME/$HOSTNAME/g" /mnt/etc/hosts
     sed -i "s/#SERVERIP/$SERVERIP/g" /mnt/etc/hosts
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
# 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
# diese auch auf den Client übertragen werden.
# Achtung: Imageverzeichnis und Imagename 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.

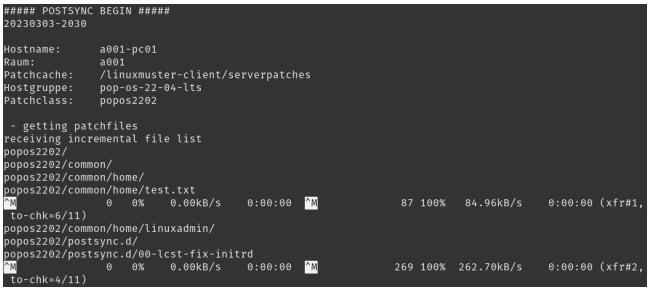
Auf dem linuxmuster.net Server gibt man hierzu folgendes an, um den Client zu starten, zu synchronisieren und dann in den Linbo-Bildschirm zu gelangen, um die Log-Datei einzusehen:

```
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:



Hier kann kontrolliert werden, ob der gewünschte Rechner, Raum, die korrekte Patchklasse und Hostgruppe ausgewählt wurden. Zudem wwerden 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/updaten

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 ausfindig 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
```

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 Betriebsystem.

`/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
```

Scripte 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
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/$USER/Schueler_auf_Server"
fi
# Link zu Schülerhomes Schueler_auf_Server in /media, wenn vorhanden (nur für␣
↪Lehrkräftte)
# muss vorher als root gelöscht werden /etc/linuxmuster-linuxclient7/onLoginAsRoot.d/03_
↪link-media-tausch.sh
if [ -L /home/$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 Scripte 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 Machine (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.
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 MASCHINENNAME 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).

Betriebsystemeinstellungen

Unter `Allgemein`, Reiter Basis muss der Betriebsystemtyp 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 Konfiguationsdateien 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'.
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
Wenn Sie die vollständige virtuelle Maschine in ein anderes Verzeichnis
umziehen wollen, starten Sie das Script 'leoclient2-vm-move'.
```

Weitere Schritte

Nachdem das Betriebsystem 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 Betriebsystem. Anleitungen finden sie bei „Weitere Informationen zu leoclient2“ und dem jeweiligen Gastbetriebsystem 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
```

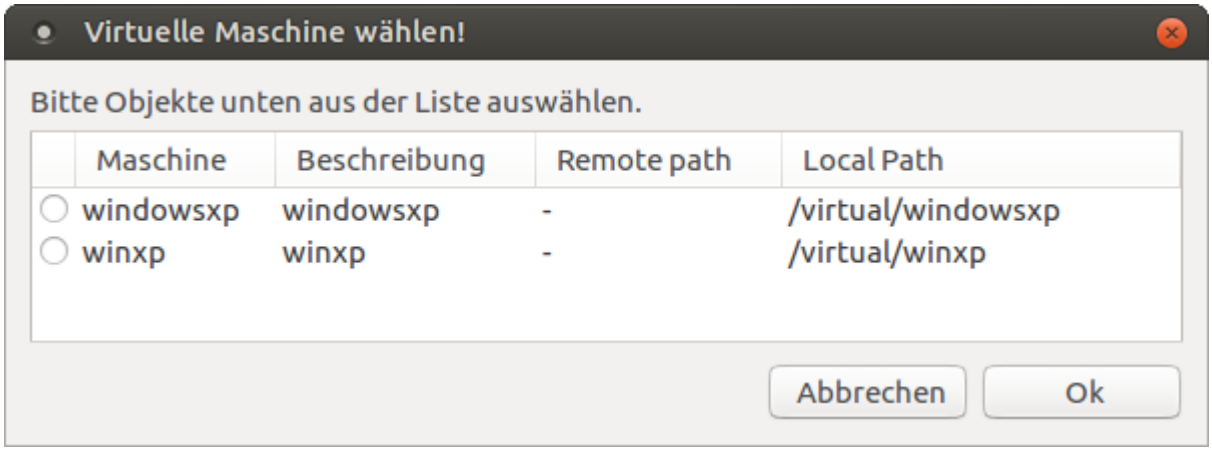


Abb. 52: Wählen Sie eine virtuelle Maschine

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

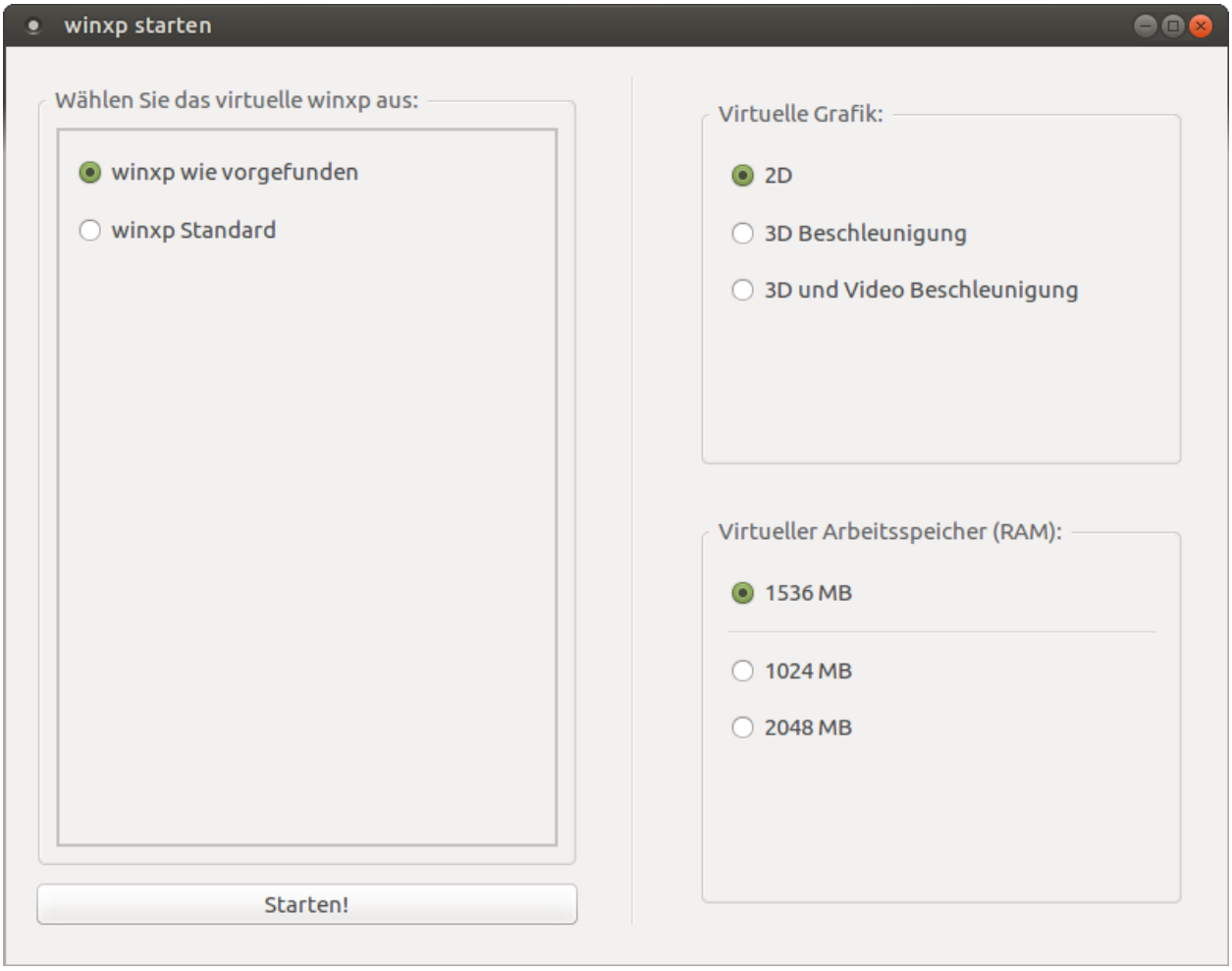


Abb. 53: Optionen zum Starten der virtuellen Maschine

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.

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 Verbinungen erscheint, kann ignoriert werden. Die Ursache ist z.B. bei dem vorkonfigurierten Ubuntu von linuxmuster.net die fehlende Verbindung zu den Homes als linuxadmin.

- 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/MASCHINENNAME/MASCHINENNAME.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.

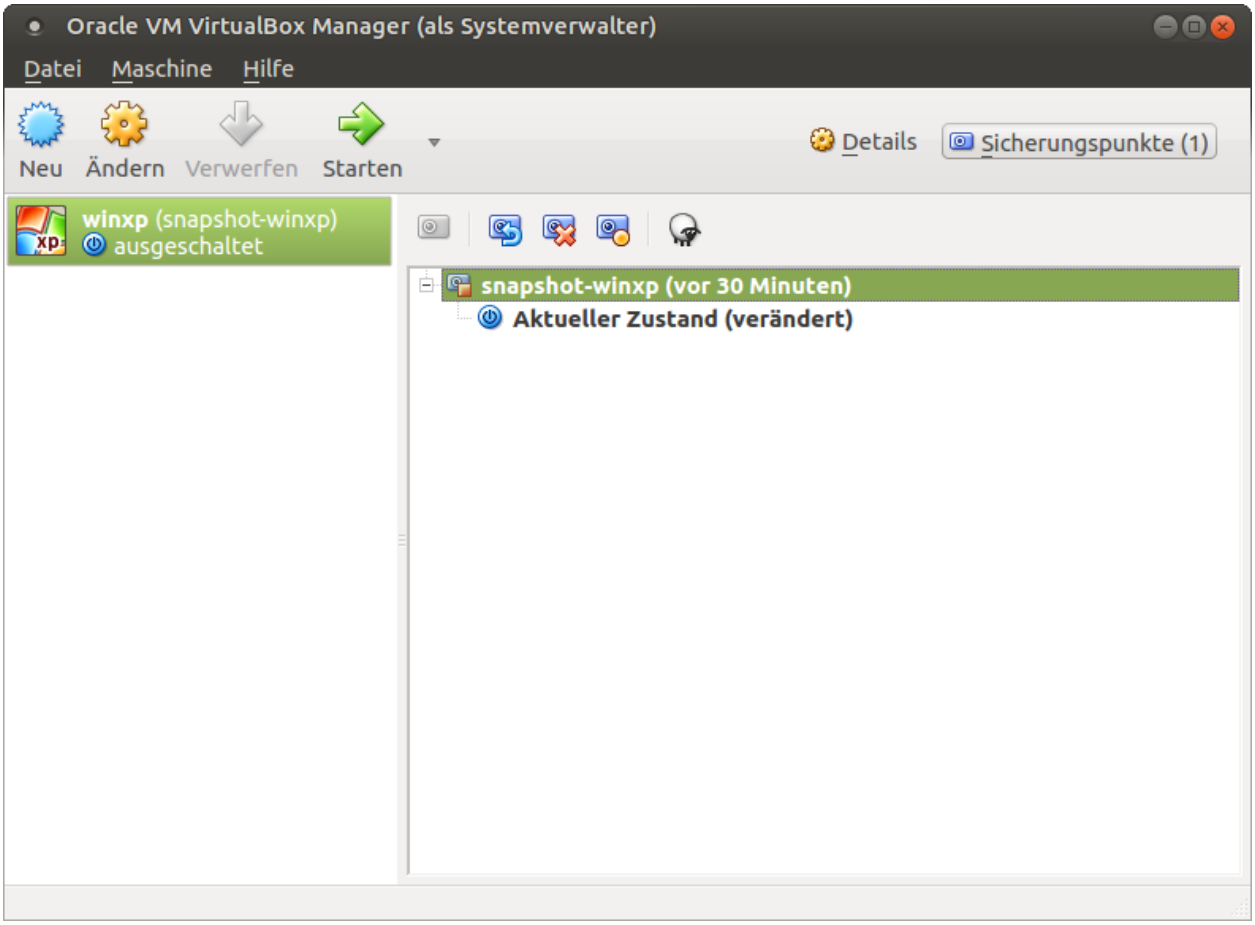


Abb. 54: VirtualBox-Optionen für Snapshots

```
...
##### 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/MASCHINENNAME/{..alterSnapshot..}.vdi*`

```
$ ls -1 /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 -1 /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 Betriebssystem 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 registiert 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 genutzen 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-Ordnern 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-Ordnern 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

- PDFXLiteHome9 installieren
- PDFXChange 9.0.354.0 - complete
- Druckerverwaltung
- Benutzerdefinierte Filter → Alle Drucker → Rechtsklick auf PDF-XChangeLite
- Eigenschaften → Allgemein → Einstellungen
- Speichern: Pfad: H:
- Name: ausdruck-winxp (.pdf wird ergänzt)
- Dialog zeigen: Aus
- Ausführen: Aus
- Drucker entfernen: alle außer PDFXLite9 (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 kein.

- Als linuxadmin im Terminal ausführen um die Basisfestplatte zu schrinken:

```
# 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-Datein schrinken. Dateien vom Typ .vmdk müssen zuerst in .vdi-Datein umgewandelt werden und danach ge-shrinked 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 Script 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 Netzwereinstellungen 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>/<MACHINENAME>/`snapshot-store`/<SNAPSHOT>/`network.conf` vorhanden, so wird diese benutzt.
- Danach wird die Datei auf dem Server für die VM <SERVERDIR>/<MACHINENAME>/`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 Snapshotnamen {...}.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 empfielt 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

```
# Berechtigugen 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 `MASCHINENNAME.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

- `MASCHINENNAME.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 exisiert)
- `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 Scripte/Befehle zum leoclient2

leoclient2-init:
legt eine neue lokale VM an

leovirtstarter2
startet das grafische Auswahlfenster und anschließend die VM mit Optionen

```
--info     listet alle VMs auf der Konsole auf
--vbox     startet das grafische Auswahlfenster 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.lan` 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.

Klicke auf der Hauptseite auf „Passwort ändern“

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`

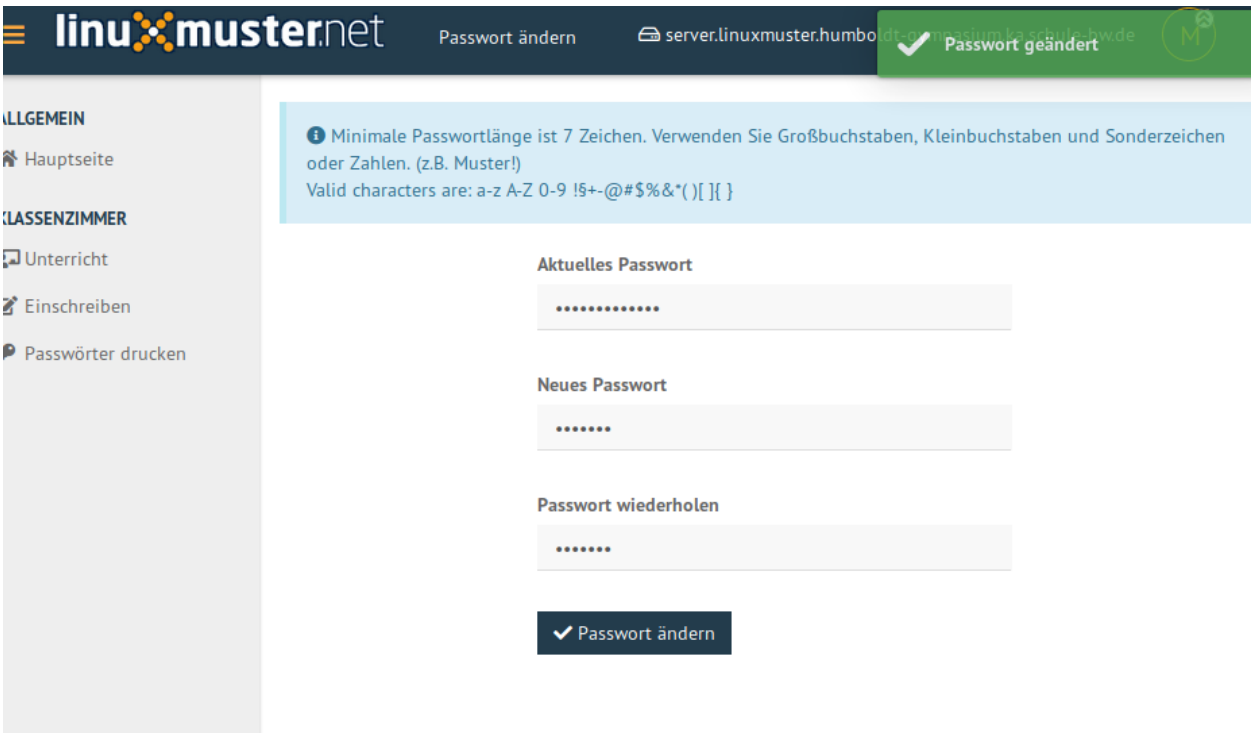
Das erfolgreiche Ändern des Passwortes wird mit einer Meldung bestätigt.

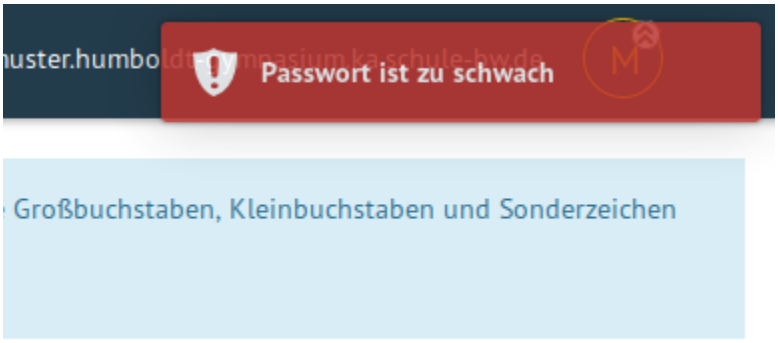
Falls die Änderung nicht erfolgreich war, erhalten Sie eine Fehlermeldung mit einem Hinweis auf den Fehler.

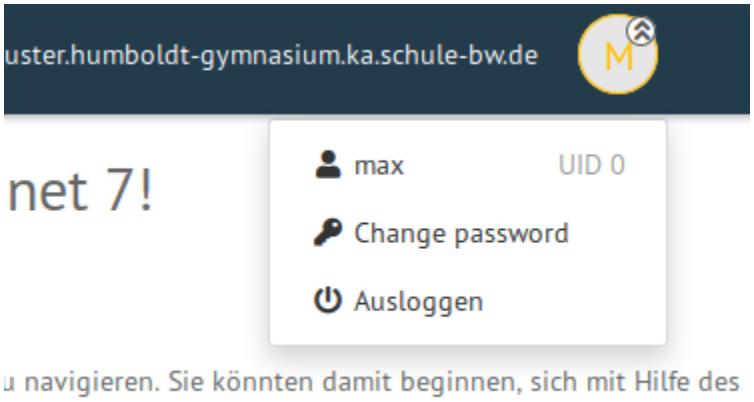
In dieser Beispielfehlermeldung bestand das Passwort nur aus Kleinbuchstaben, Zahlen und Sonderzeichen. Es enthielt keine Großbuchstaben.

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.


linuxmuster.net
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
Passwort ändern


Passwort ist zu schwach
Großbuchstaben, Kleinbuchstaben und Sonderzeichen


uster.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.lan` 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 lmn7 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

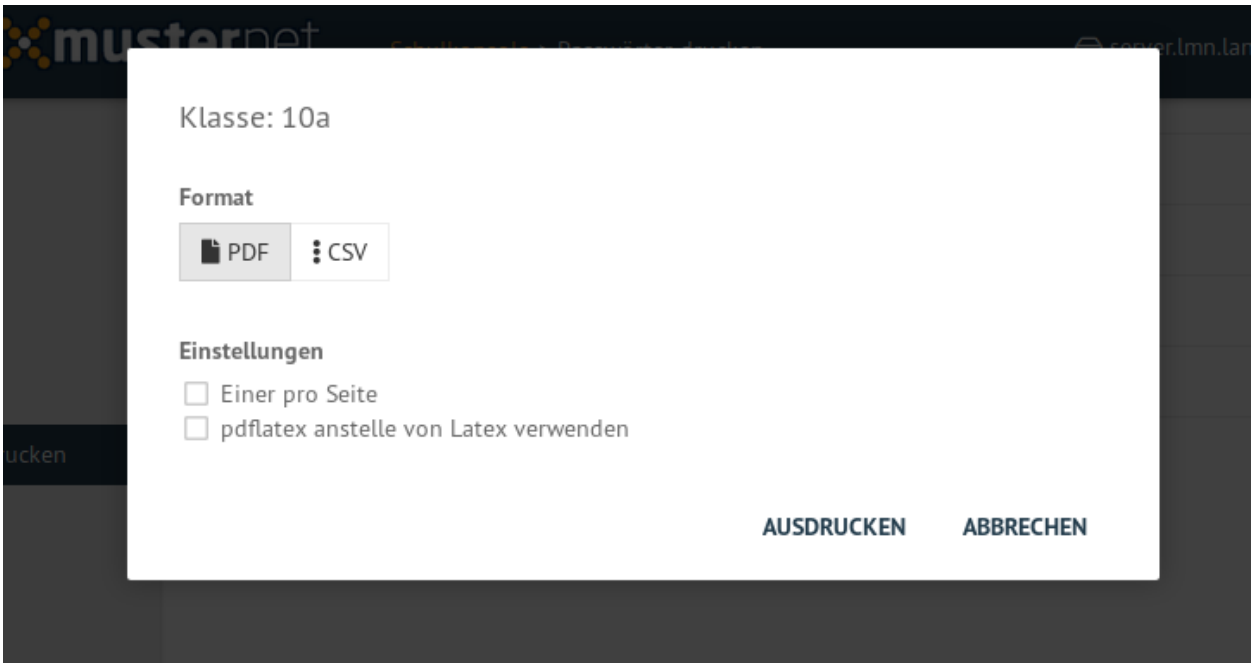
Es werden meist beide Kategorien für den täglichen Umgang benötigt.

Solange ein Lehrer nur den automatisch angelegten Tauschordner der Klasse verwenden will, muss er keine Kurse einrichten. Die Konfiguration findet sich unter *KLASSENZIMMER/Einschreiben*.

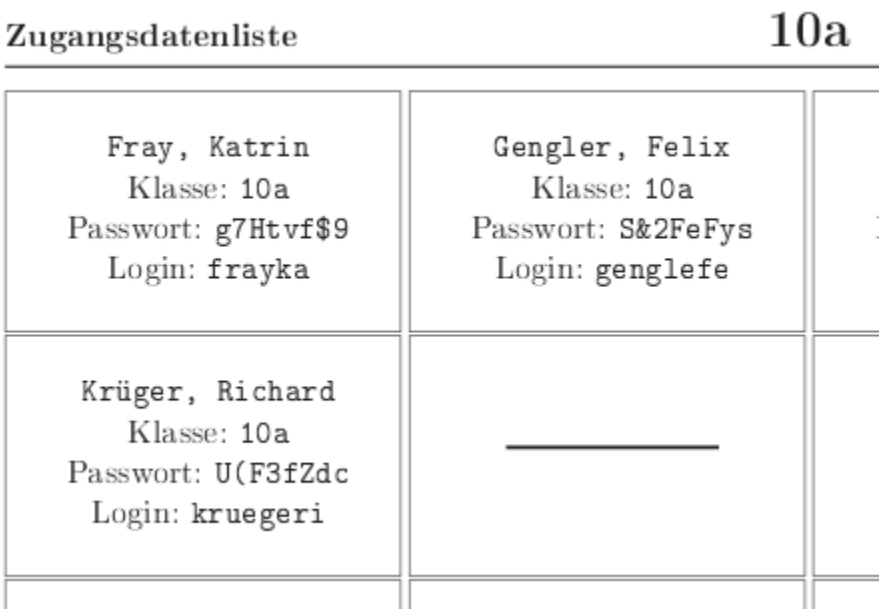
Sobald ein Lehrer die Unterrichtsfunktionen verwenden will, die über einen Tauschordner hinausgehen, muss er einen Kurs anlegen und die gewünschten Schüler hinzufügen. Die Konfiguration findet sich unter *KLASSENZIMMER/Unterricht*.

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.

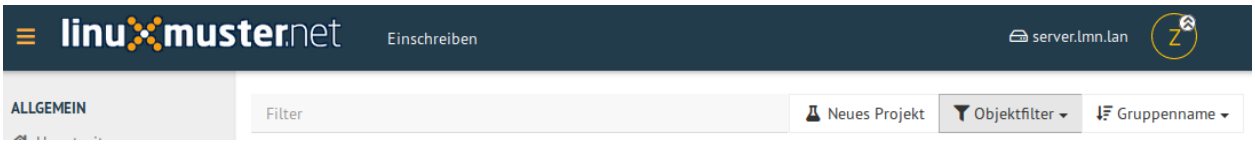
In Klassen einschreiben

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`.



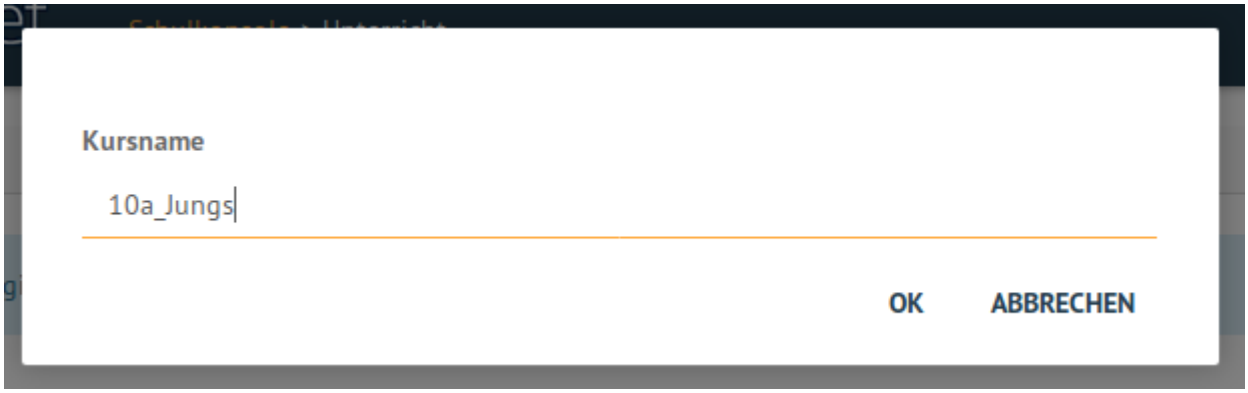
In dem sich öffnenden Eingabefeld kann der Projektname mit kleinen Buchstaben (a-z, keine Umlaute oder Sonderzeichen) und Zahlen (0-9) festgelegt werden. Die Schulkonsole meldet zurück, wenn das Projekt erfolgreich erstellt wurde und es erscheint in der Liste der Projekte.

fixme
Rest der Erstellung der Projekte

4.21.4 Unterrichtskurs einrichten

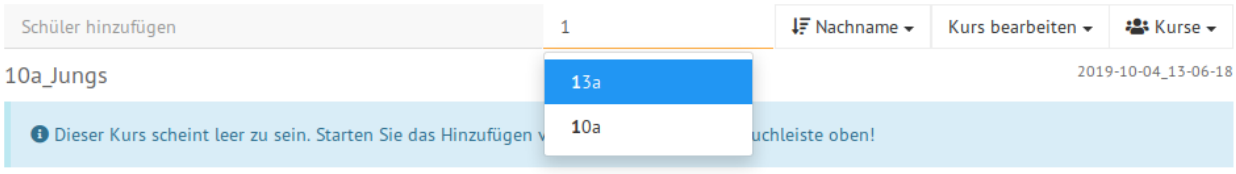
Die folgende Anleitung brauchst Du für alle Unterrichtsfunktionen (außer dem Tauschordner) und dafür musst Du nicht in der Klasse eingeschrieben sein.

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.

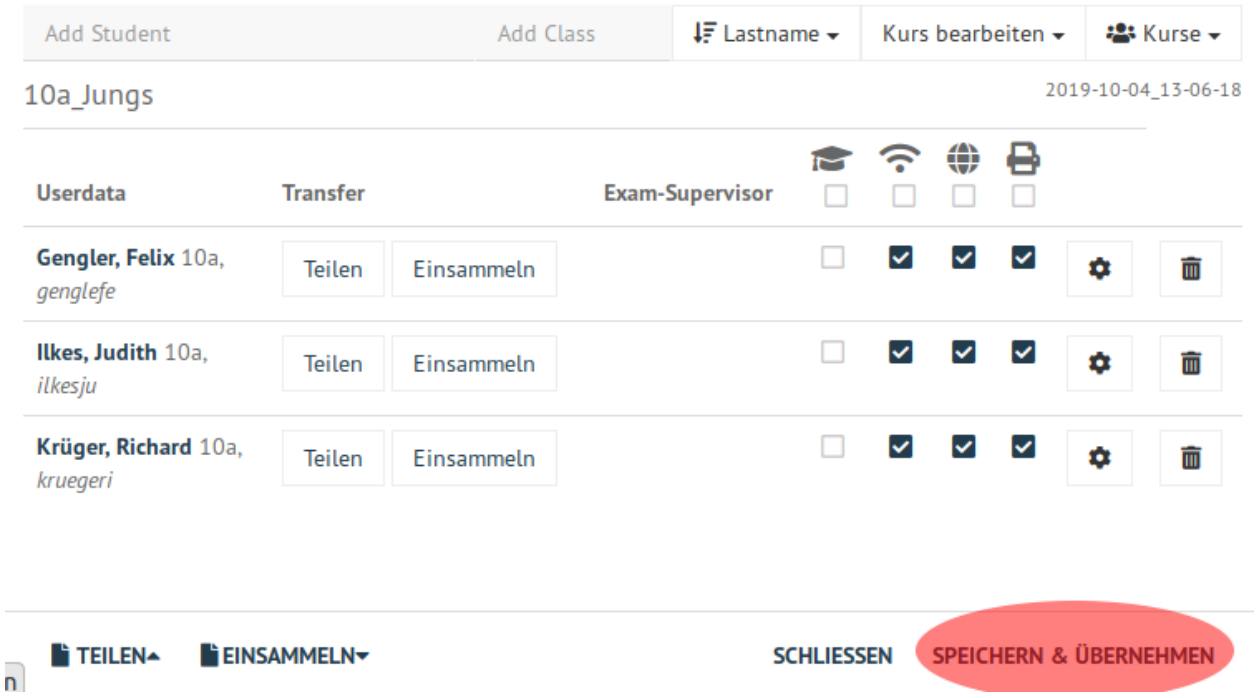
Ist die Liste vollständig klicke unten rechts auf *SPEICHERN & ÜBERNEHMEN*.

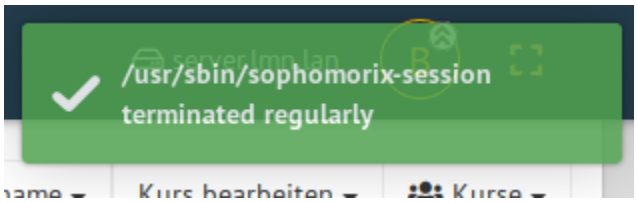
Rechts oben wird das erfolgreiche Speichern mit einem grünen Haken zurückgemeldet.

Der Kurs kann später an dieser Stelle auch umbenannt oder gelöscht werden.

Folgende Unterrichtsfunktionen können jetzt genutzt werden:

- *Prüfungs-/Klassenarbeitsmodus, austeilen und einsammeln*


Add Student
Add Class
Lastname
Kurs bearbeiten
Kurse
10a_Jungs
2019-10-04_13-06-18
Userdata
Transfer
Exam-Supervisor
Gengler, Felix 10a, genglefe
Teilen
Einsammeln
Ilkes, Judith 10a, ilkesju
Teilen
Einsammeln
Krüger, Richard 10a, kruegeri
Teilen
Einsammeln
TEILEN
EINSAMMELN
SCHLIESSEN
SPEICHERN & ÜBERNEHMEN

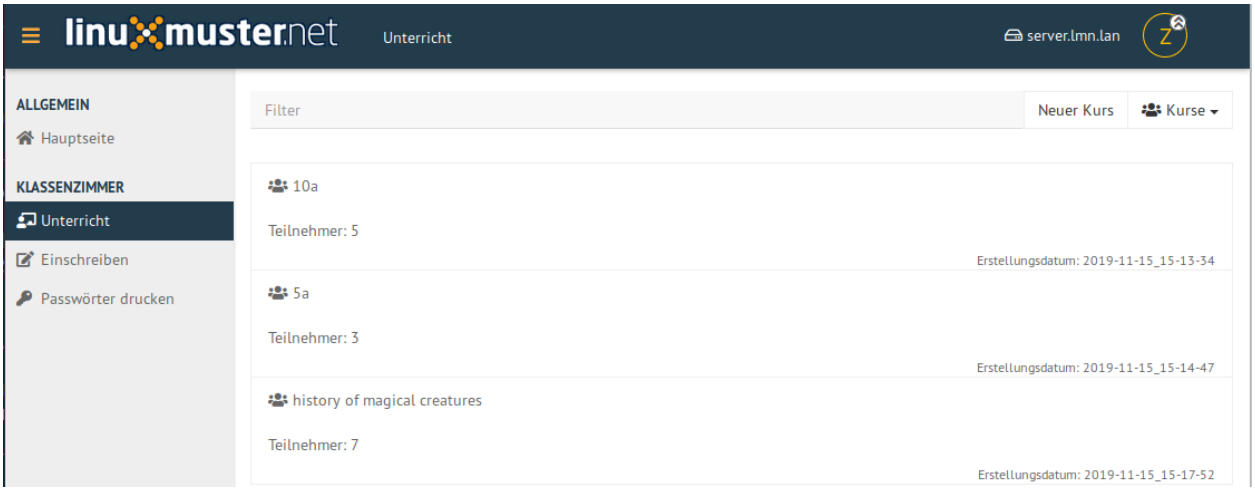

/usr/sbin/sophomorix-session
terminated regularly

- *Zugriff auf WLAN, Internet und Drucker regeln*

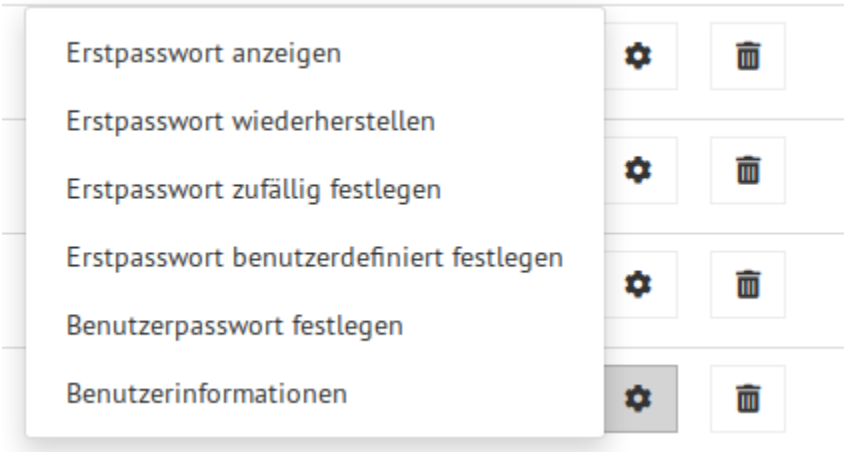
Passwörter zurücksetzen

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 Benutzerveraltun 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 Schulungsnetzs 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 Prüfvorgang 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

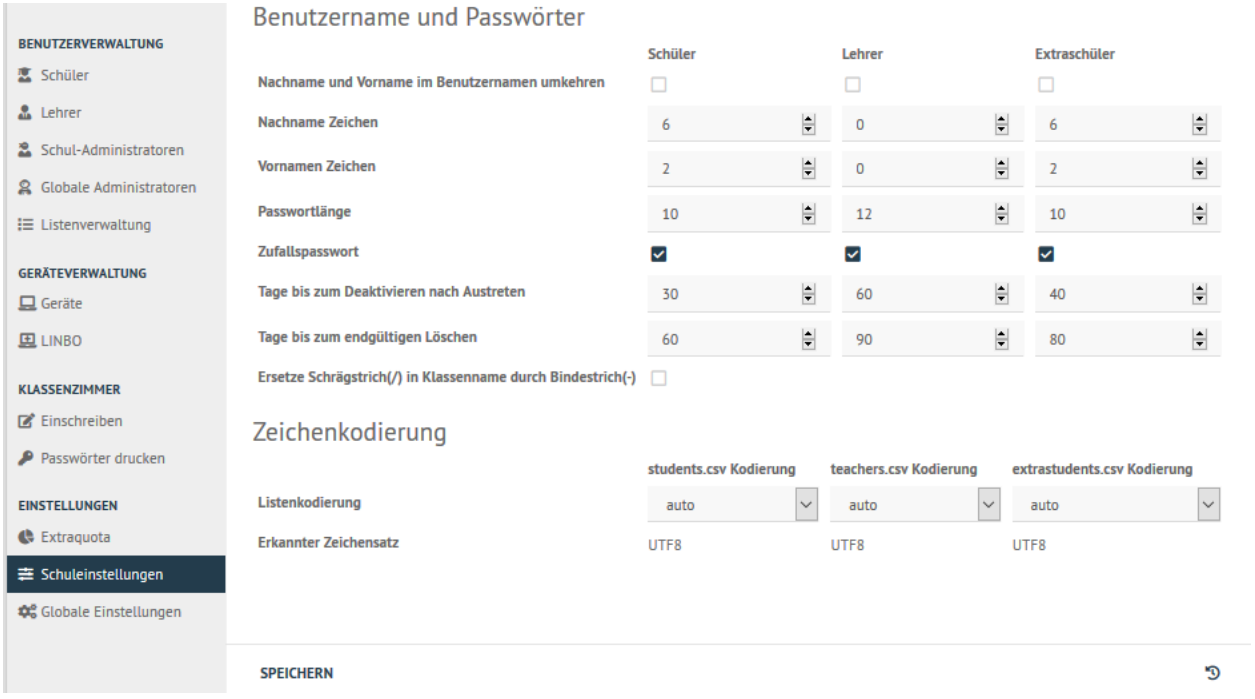
Autor des Abschnitts: @cweikl

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.



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.

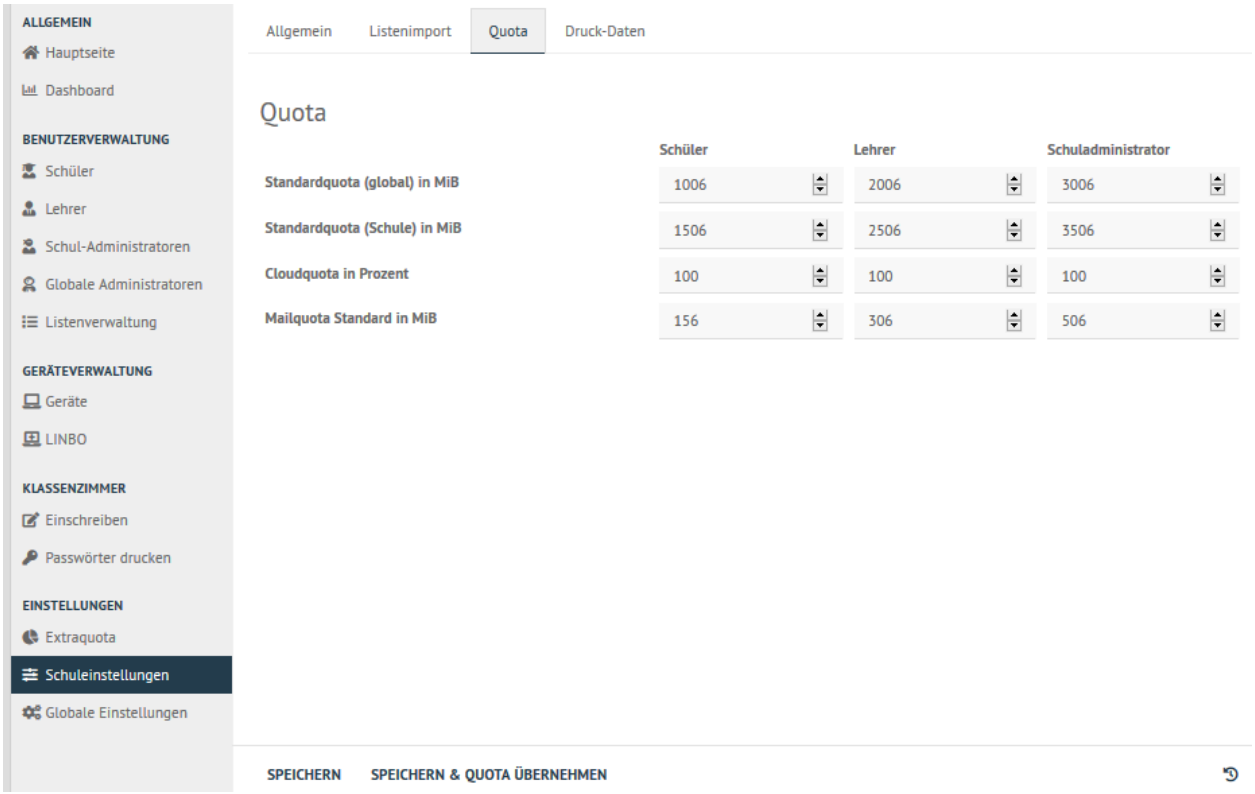
Es kann festgelegt werden, ob beim Import ein Zufallskennwort pro Benutzer erstellt wird, oder ob ein Kennwort später in der Schulkonsole gesetzt wird. Zudem wird hier festgeschrieben, wie mit Benutzern verfahren wird, die gelöscht werden sollen. Es wird hier mit einem Duldungszeitraum gearbeitet, so 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.

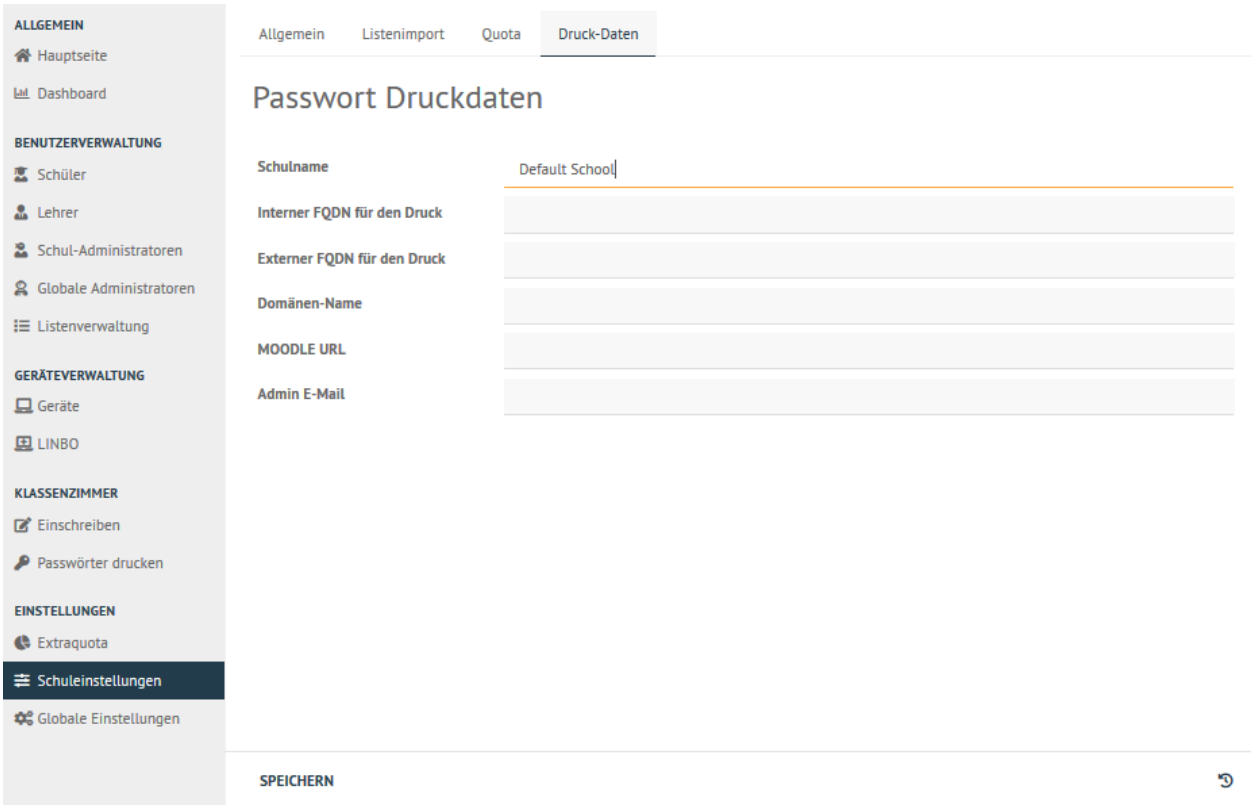
Zur Ermittlung des belegten Speicherplatzes werden alle Dateien des Benutzers über alle sog. Partitionen hinweg gezählt. Dies bedeutet, dass der belegte Speicherplatz aller Dateien des Benutzers im Verzeichnis der Klasse oder Schule als auch Dateien in seinem eigenen Home-Laufwerk, das ebenfalls auf dem Server liegt, ermittelt wird.



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*.

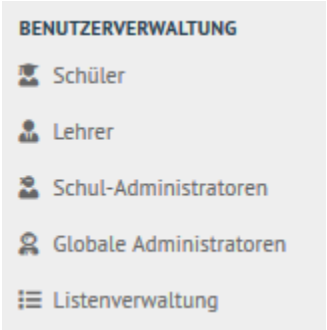
Mit der *Schulkonsole* gibt es für den Netzwerkbetreuer ein webbasiertes Werkzeug, das ihm die Bedienung von *sophomorix4* sehr erleichtert. Die einzelnen Schritte werden im Folgenden erläutert. Der Netzwerkbetreuer muss nur noch in Ausnahmefällen mit der Kommandozeile arbeiten.

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 üblichweise eine automatische Erkennng der Kodierung festgelegt.

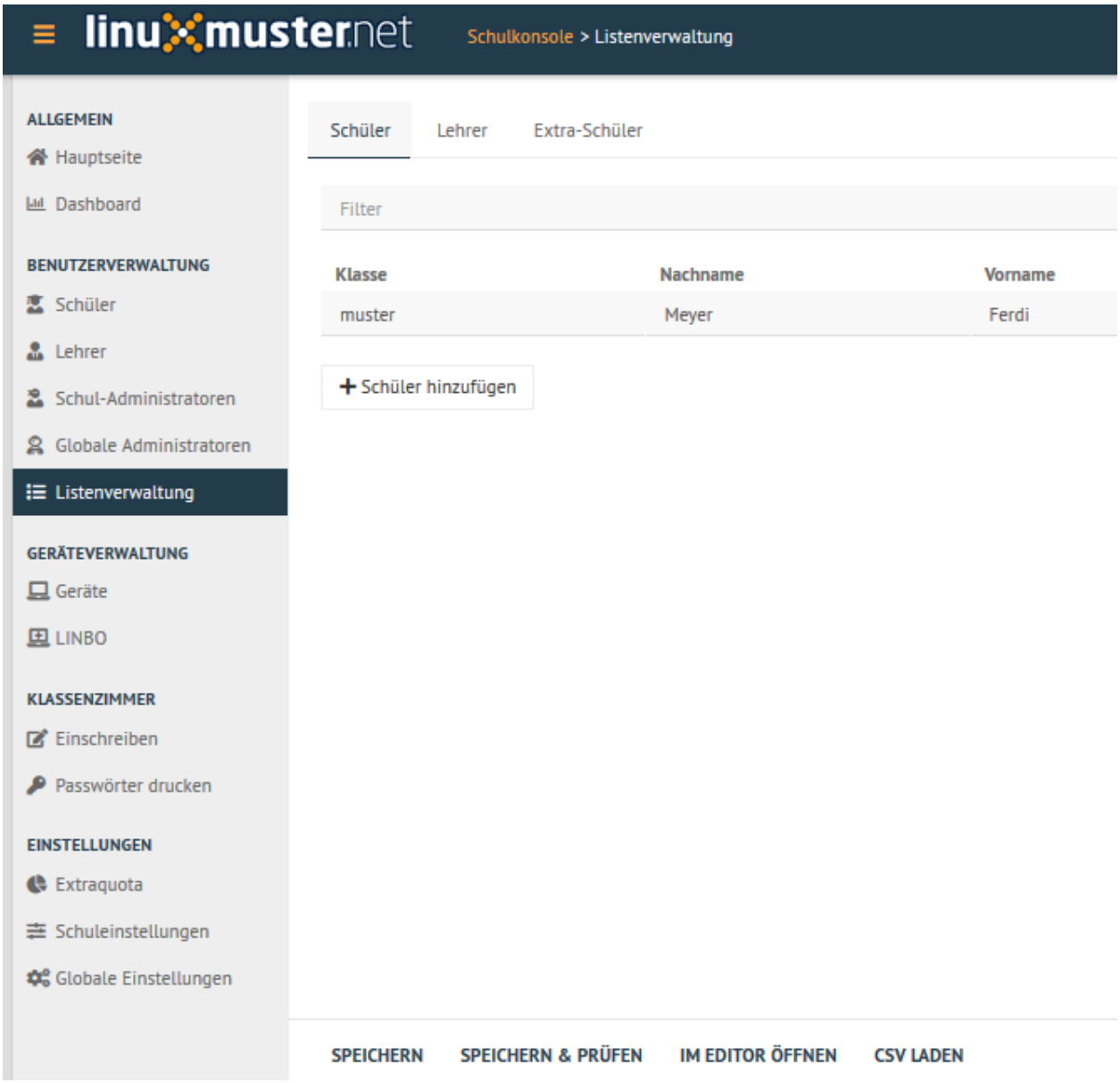
Hinweis: Die nachstehend dargestellten Benutzer sind alles *fiktive Testnutzer*, die nur zur Illustration eingetragen und auf den Screenshots dargestellt werden. Es handelt um keine lebenden Personen. Die Daten dienen nur zu Test- und Dokumentationszwecken.

Pflege der Schülerdatei

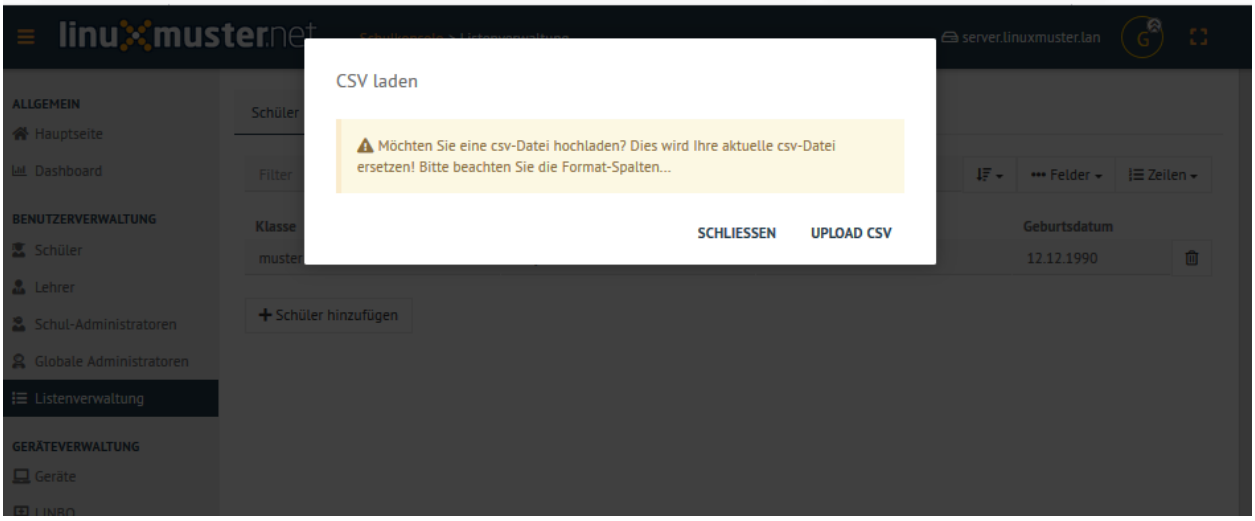
Die Schüler können Sie erstmals in das System aufnehmen, in dem Sie die vorbereitete students.csv Datei mithilfe der Schulkonsole hochladen.

Gehen Sie hierzu in der Schulkonsole unter `Benutzerveraltung` in das Menü `Listenverwaltung` und klicken Sie auf die obere Reiterkarte `Schüler` und dann unten auf den Eintrag `CSV Laden`.

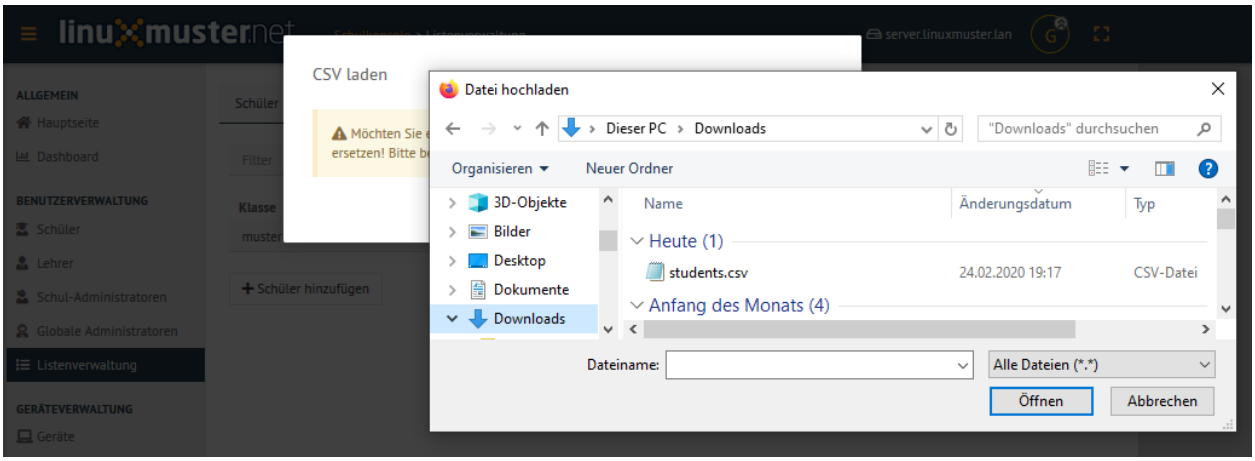
Es erscheinen dann schrittweise folgende Eingabefenster:



Es ercheint 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.

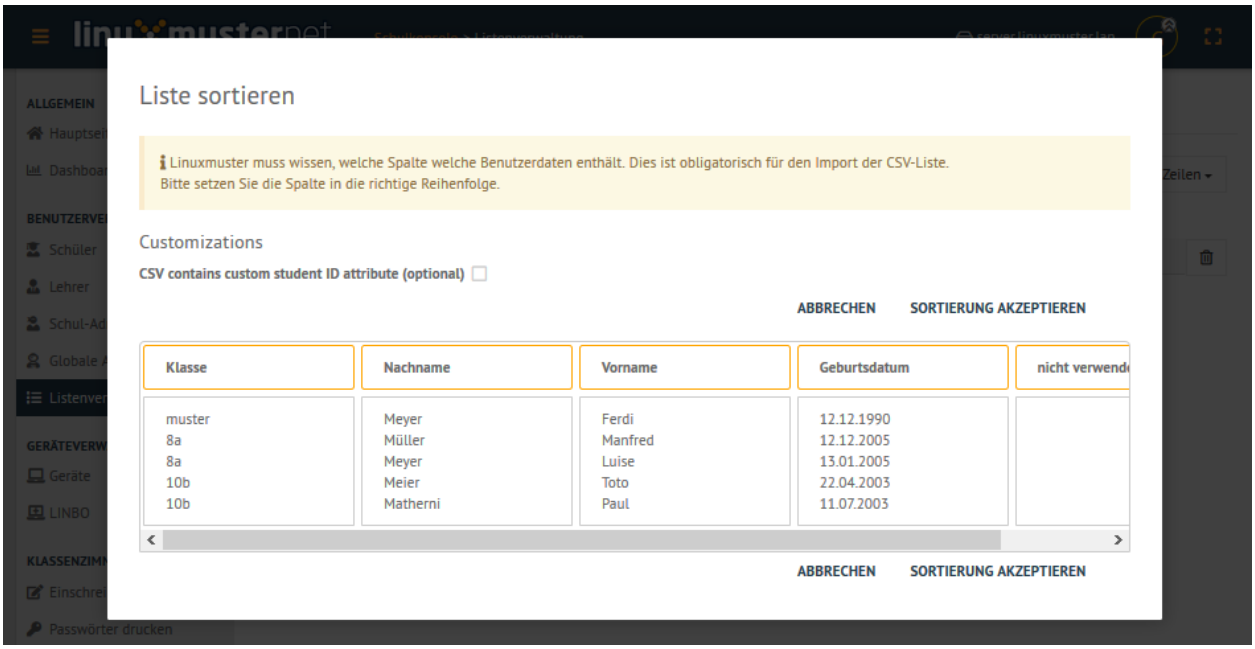
Nach der Bestätigung der Sortierreihenfolge werden die Benutzer temporär importiert. Das Ergebnis wird Ihnen wie in der nachstehenden Abbildung angezeigt.

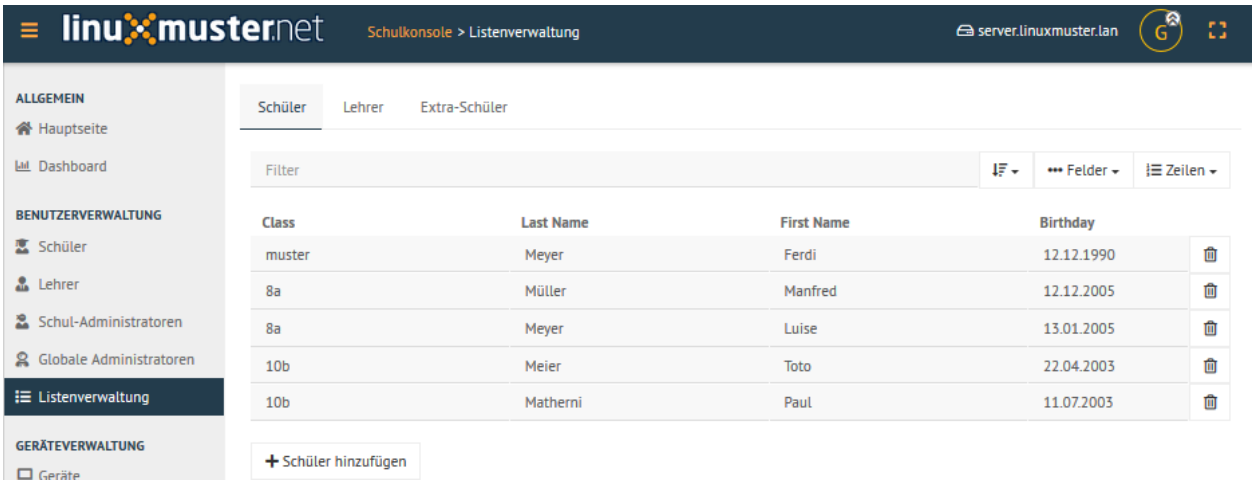
Entspricht dies dem gewünschen Import, so müssen Sie die Benutzer nun mithilfe des Eintrags `Speichern & prüfen` übernehmen. Das Prüfergebnis wird Ihnen angezeigt und Sie müssen nun die Übernahme der neuen Benutzer bestätigen.

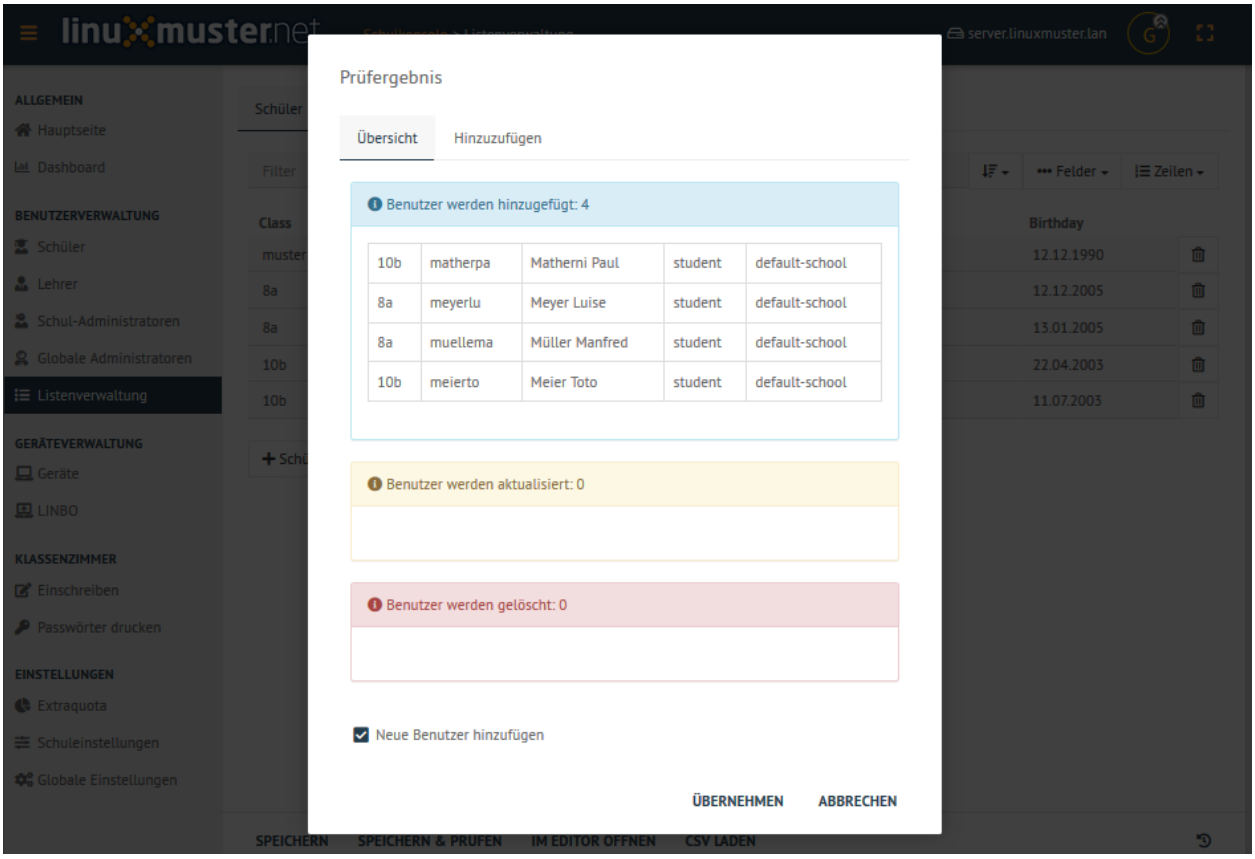
Nach der Bestätigung zur Übernahme der neuen Benutzer werden diese auf dem Server angelegt und eingerichtet. Nach Abschluss des Imports sehen Sie im dargestellten Konsolenfenster einen Eintrag wie `4 users added` - wir in der Abbildung zu erkennen ist.

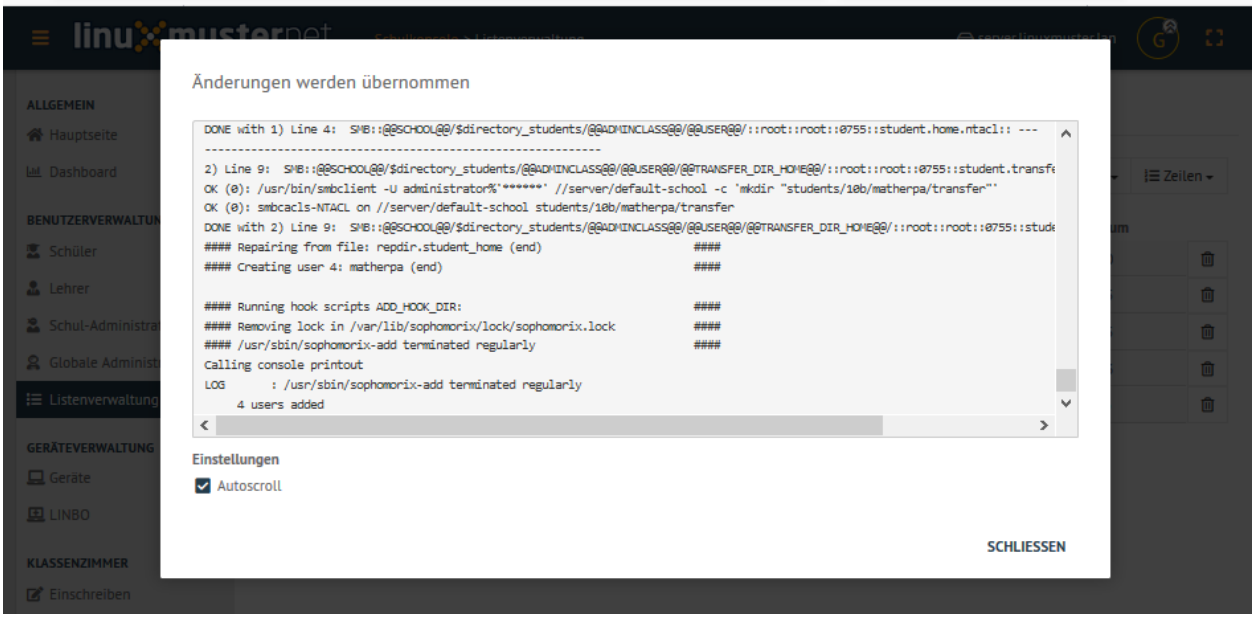
Die CSV-Dateien finden sich auf dem Server in folgendem Verzeichnis: `/etc/linuxmuster/sophomorix/default-school`

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 verwend
muster
8a
8a
10b
10b
Meyer
Müller
Meyer
Meier
Matherni
Ferdi
Manfred
Luise
Toto
Paul
12.12.1990
12.12.2005
13.01.2005
22.04.2003
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
Felder
Zeilen
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
Hinzuzufügen
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 meierto 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: SMB::@@SCHOOL@@/$directory_students/@@ADMINCLASS@@/@@USER@@/::root::root::0755::student.home.ntacl:: ---
2) Line 9: SMB::@@SCHOOL@@/$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: SMB::@@SCHOOL@@/$directory_students/@@ADMINCLASS@@/@@USER@@/@@TRANSFER_DIR_HOME@@/::root::root::0755::stud
Repairing from file: repdir.student_home (end)
Creating user 4: matherpa (end)
Running hook scripts ADD_HOOK_DIR:
Removing lock in /var/lib/sophomorix/lock/sophomorix.lock
/usr/sbin/sophomorix-add terminated regularly
Calling console printout
LOG : /usr/sbin/sophomorix-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 Schulkonsle 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.

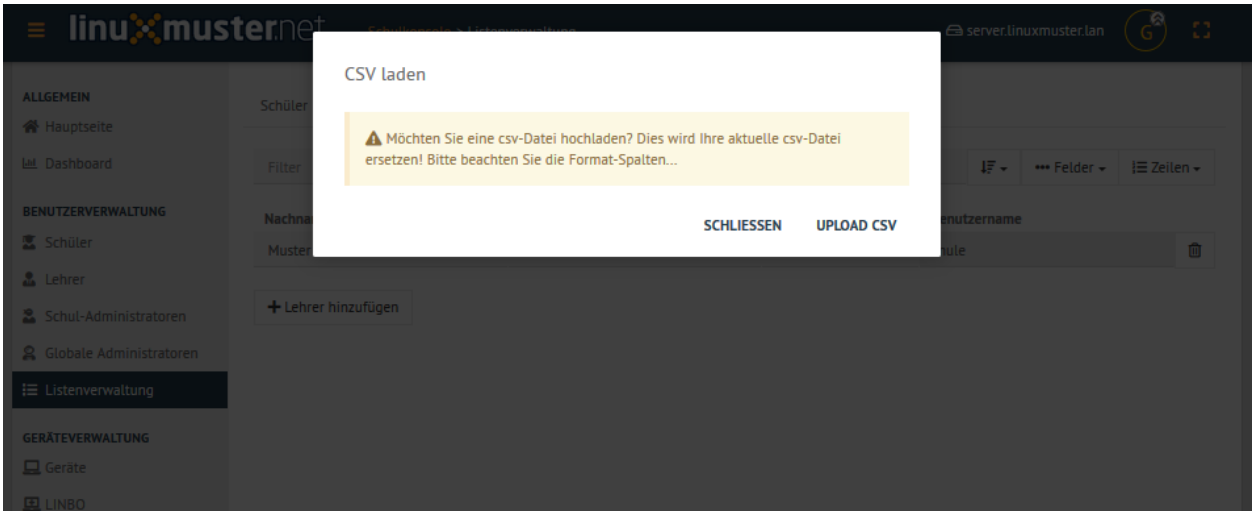
Der Import der teachers.csv erfolgt analog zu dem Vorgehen wie es zuvor bereits für die students.csv beschrieben wurde.

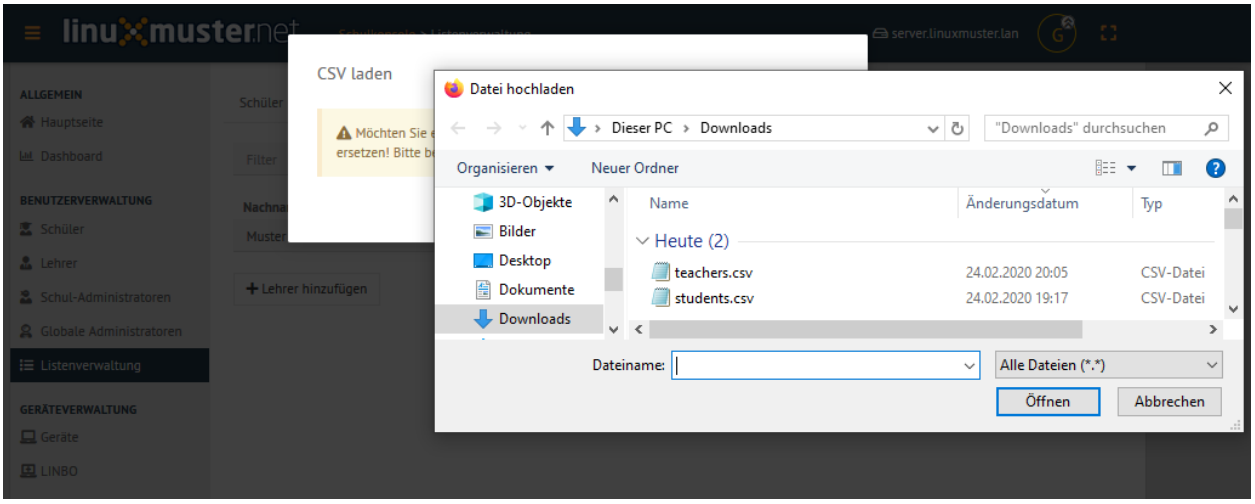
Rufen Sie im Menü unter der Benutzerverwaltung den Eintrag `Listenverwaltung -> Lehrer -> CSV Laden` auf.

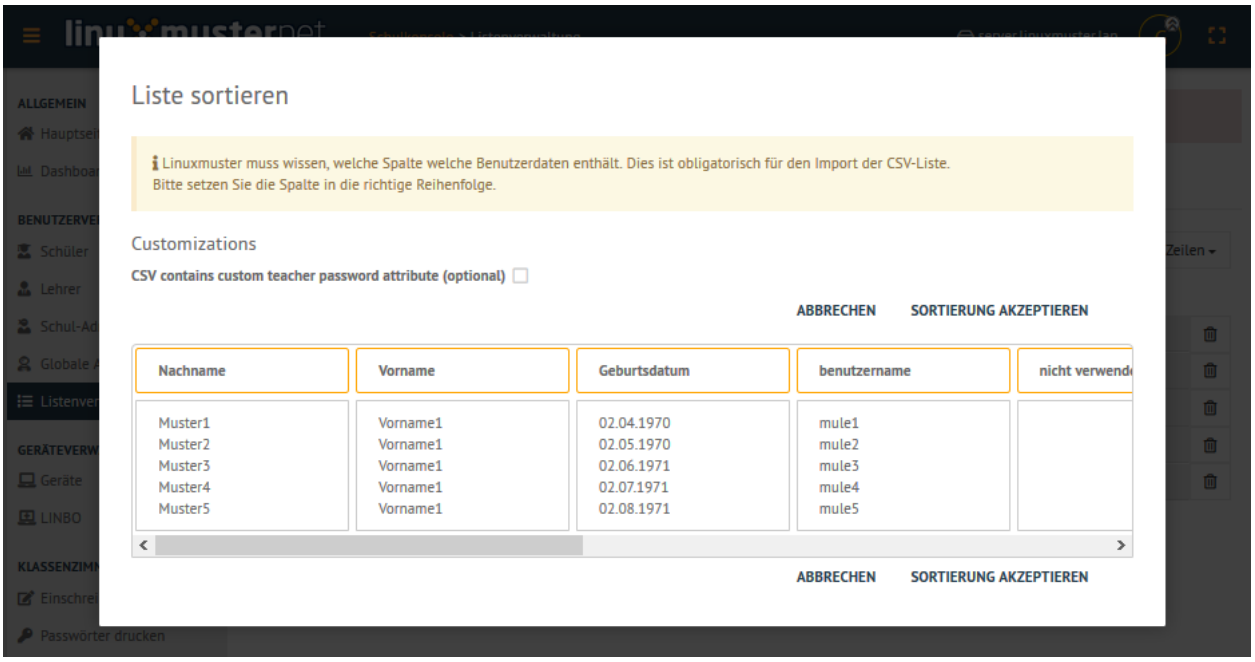
Danach wählen Sie dort den Dateinamen der hochzuladenden CSV-Datei aus.

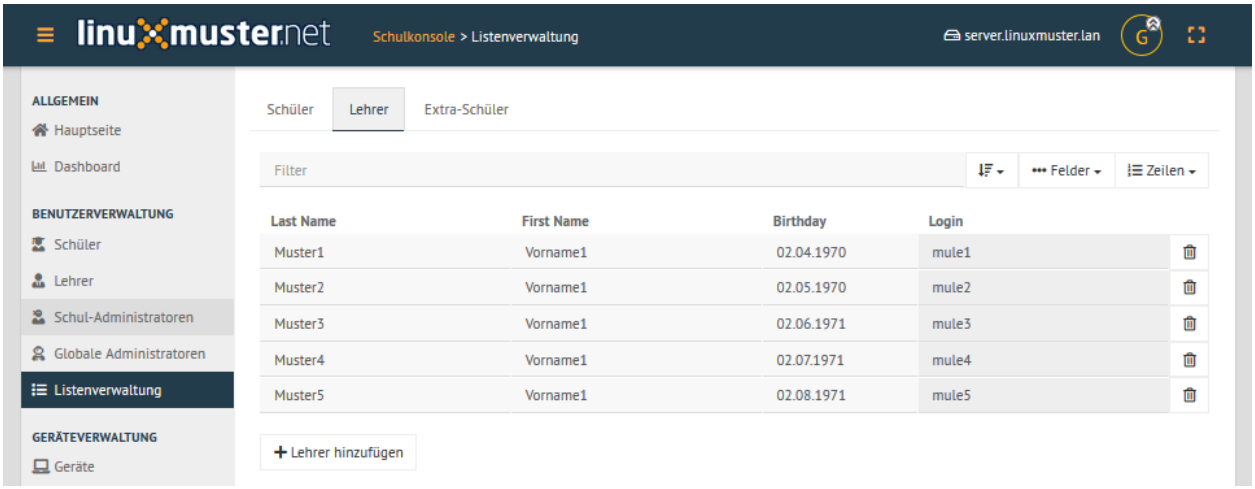
Die Einträge werden nun geprüft und das Prüfergebnis wird Ihnen angezeigt. Hier können Sie bereits falsche Spaltenzuordnungen oder eine abweichende Spaltenreihenfole erkennen. Stimmt das dargestellte Ergebnis, so übernehmen Sie die Sortierreihenfolge.

Nach dem Import der CSV-Datei werden die zu importierenden Lehrer wie folgt dargestellt:


CSV laden
Möchten Sie eine csv-Datei hochladen? Dies wird Ihre aktuelle csv-Datei ersetzen! Bitte beachten Sie die Format-Spalten...
SCHLIESSEN
UPLOAD CSV


CSV laden
Datei hochladen
Dieser PC › Downloads
"Downloads" durchsuchen
Organisieren
Neuer Ordner
3D-Objekte
Bilder
Desktop
Dokumente
Downloads
Name
Änderungsdatum
Typ
Heute (2)
teachers.csv 24.02.2020 20:05 CSV-Datei
students.csv 24.02.2020 19:17 CSV-Datei
Dateiname:
Alle Dateien (*.*)
Öffnen
Abbrechen


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 teacher password attribute (optional)
ABBRECHEN
SORTIERUNG AKZEPTIEREN
Nachname
Vorname
Geburtsdatum
benutzername
nicht verwend
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
ABBRECHEN
SORTIERUNG AKZEPTIEREN



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. Gastschüler 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;
```

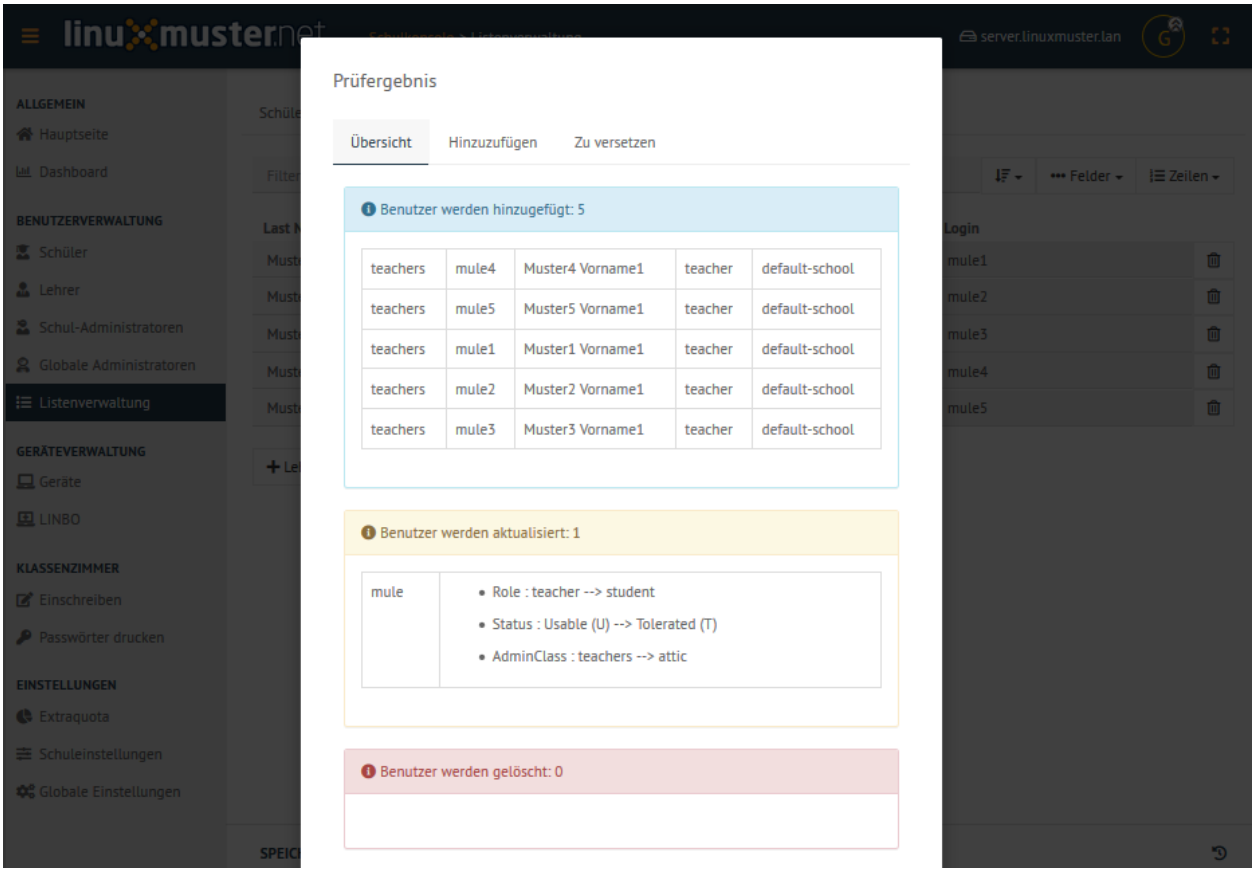
Der Name für die Klasse ist frei wählbar, z.B: *koop* (für Kooperation) oder *at* (für Austausch). Es können aber, gerade auch bei Kooperationsschülern, die **bestehenden** Klassennamen verwendet werden. Dies ist wichtig, falls der Zugriff auf das Klassentauschverzeichnis der Klasse ermöglicht werden soll. Bei neuen Gruppennamen, wird auch ein neues Klassentauschverzeichnis angelegt.

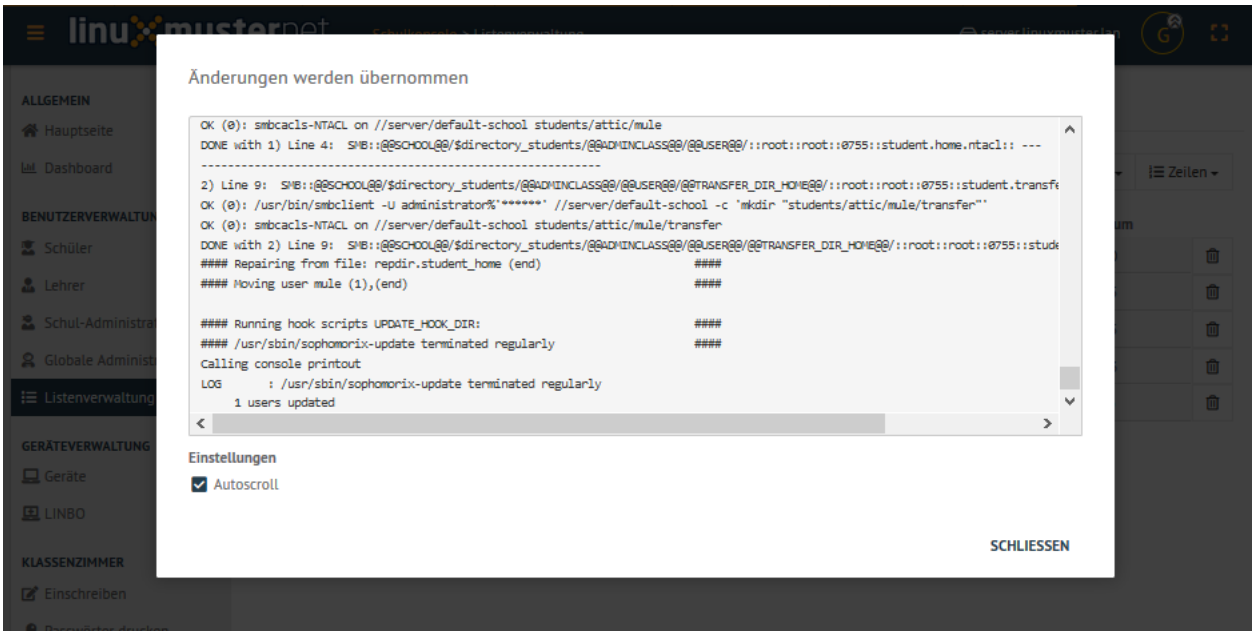
Analog zu dem Import der CSV-Dateien für die Schüler und Lehrer erfolgt auh für die Extra-Schüler der Upload bzw. die Bearbeitung der Datei extrastudents.csv.

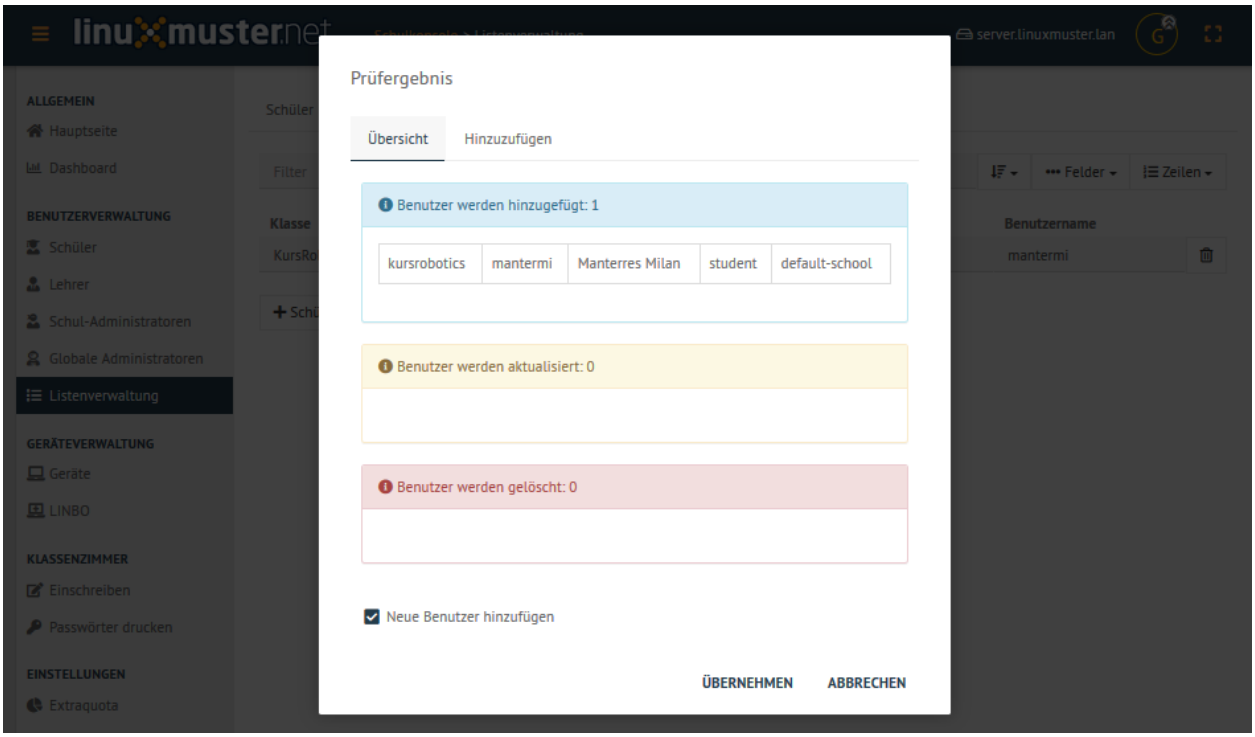
Die Benutzer werden wiederum mit `Speichern & prüfen` übernommen. Hierbei wird Ihnen wiederum das Prüfergebnis angezeigt:

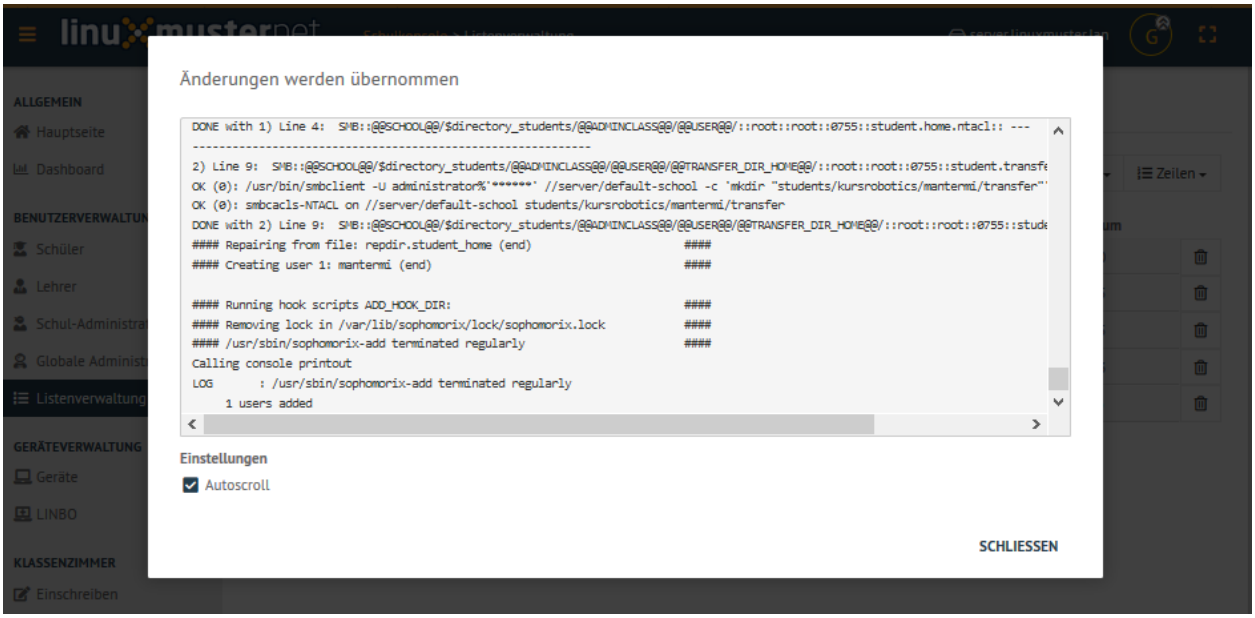
Nach dem Import sehen Sie in der dargestellten Konsole Hinweise wie `1 users added`.

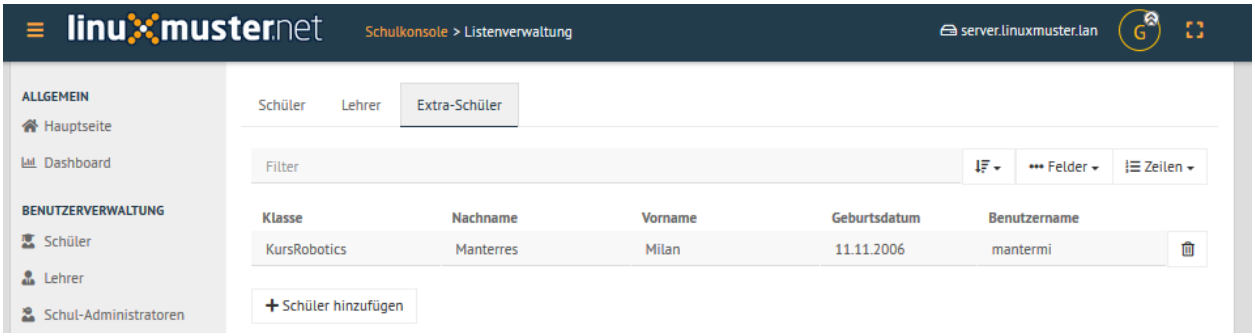
Die Extra-Schüler werden im System dann wie folgt dargestellt:


Prüfergebnis
Übersicht
Hinzuzufügen
Zu versetzen
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
Benutzer werden aktualisiert: 1
mule
Role : teacher --> student
Status : Usable (U) --> Tolerated (T)
AdminClass : teachers --> attic
Benutzer werden gelöscht: 0


Änderungen werden übernommen
OK (0): smbcacls-NTACL on //server/default-school students/attic/mule
DONE with 1) Line 4: SMB::@@SCHOOL@@/$directory_students/@@ADMINCLASS@@/@@USER@@/::root::root::0755::student.home.ntacl:: ---
2) Line 9: SMB::@@SCHOOL@@/$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/attic/mule/transfer"'
OK (0): smbcacls-NTACL on //server/default-school students/attic/mule/transfer
DONE with 2) Line 9: SMB::@@SCHOOL@@/$directory_students/@@ADMINCLASS@@/@@USER@@/@@TRANSFER_DIR_HOME@@/::root::root::0755::stude
Repairing from file: repdir.student_home (end)
Moving user mule (1),(end)
Running hook scripts UPDATE_HOOK_DIR:
/usr/sbin/sophomorix-update terminated regularly
Calling console printout
LOG : /usr/sbin/sophomorix-update terminated regularly
1 users updated
Einstellungen
Autoscroll
SCHLIESSEN


Prüfergebnis
Übersicht
Hinzuzufügen
Benutzer werden hinzugefügt: 1
kursrobotics
mantermi
Manterres Milan
student
default-school
Benutzer werden aktualisiert: 0
Benutzer werden gelöscht: 0
Neue Benutzer hinzufügen
ÜBERNEHMEN
ABBRECHEN


Änderungen werden übernommen
Einstellungen
Autoscroll
SCHLIESSEN


linuxmuster.net
Schulkonsole > Listenverwaltung
server.linuxmuster.lan
ALLGEMEIN
Hauptseite
Dashboard
BENUTZERVERWALTUNG
Schüler
Lehrer
Schul-Administratoren
Schüler
Lehrer
Extra-Schüler
Filter
Felder
Zeilen
Klasse
Nachname
Vorname
Geburtsdatum
Benutzername
KursRobotics
Manterres
Milan
11.11.2006
mantermi
Schüler hinzufügen

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.

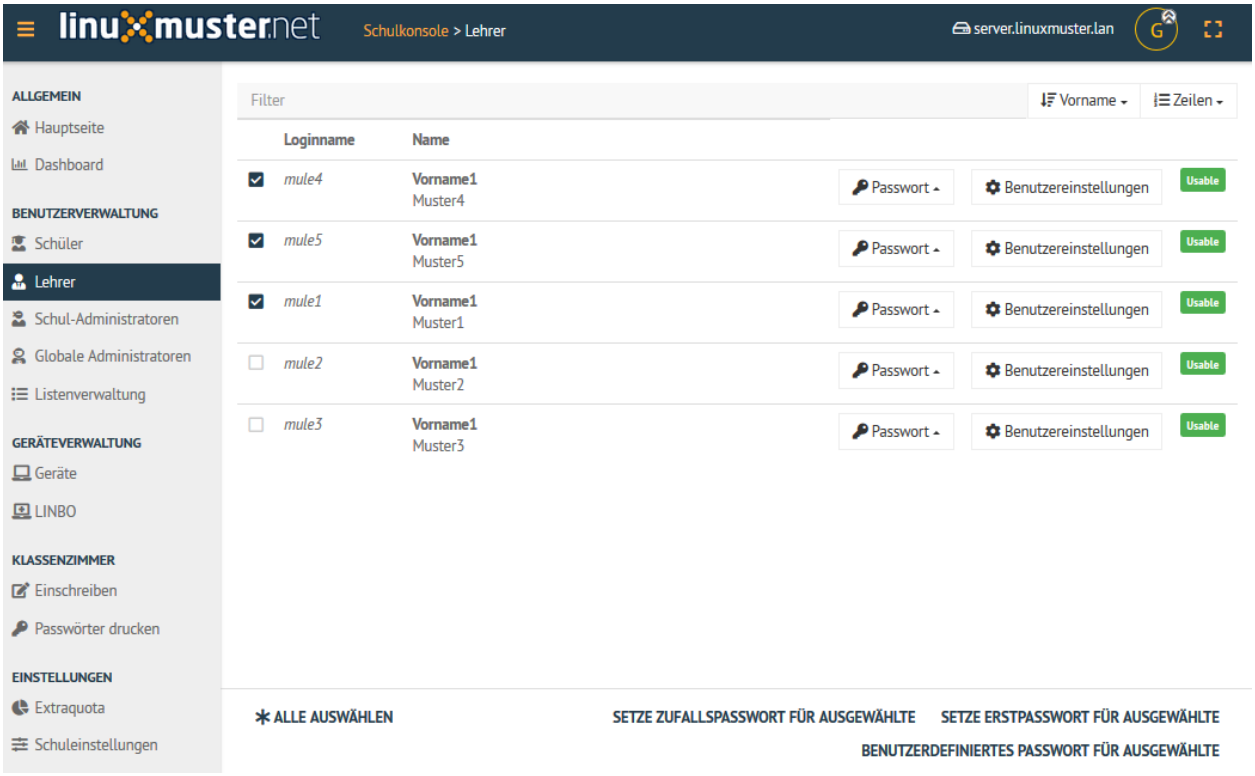
Um für Lehrer Kennwörter neu zu setzen, melden Sie sich an der Schulkonsole als `global-admin` an. Klicken Sie im Menü Benutzerverwaltung auf den Eintrag `Lehrer`. Sie sehen dann alle derzeit im System angelegten Lehrer-Accounts.

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!`



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.

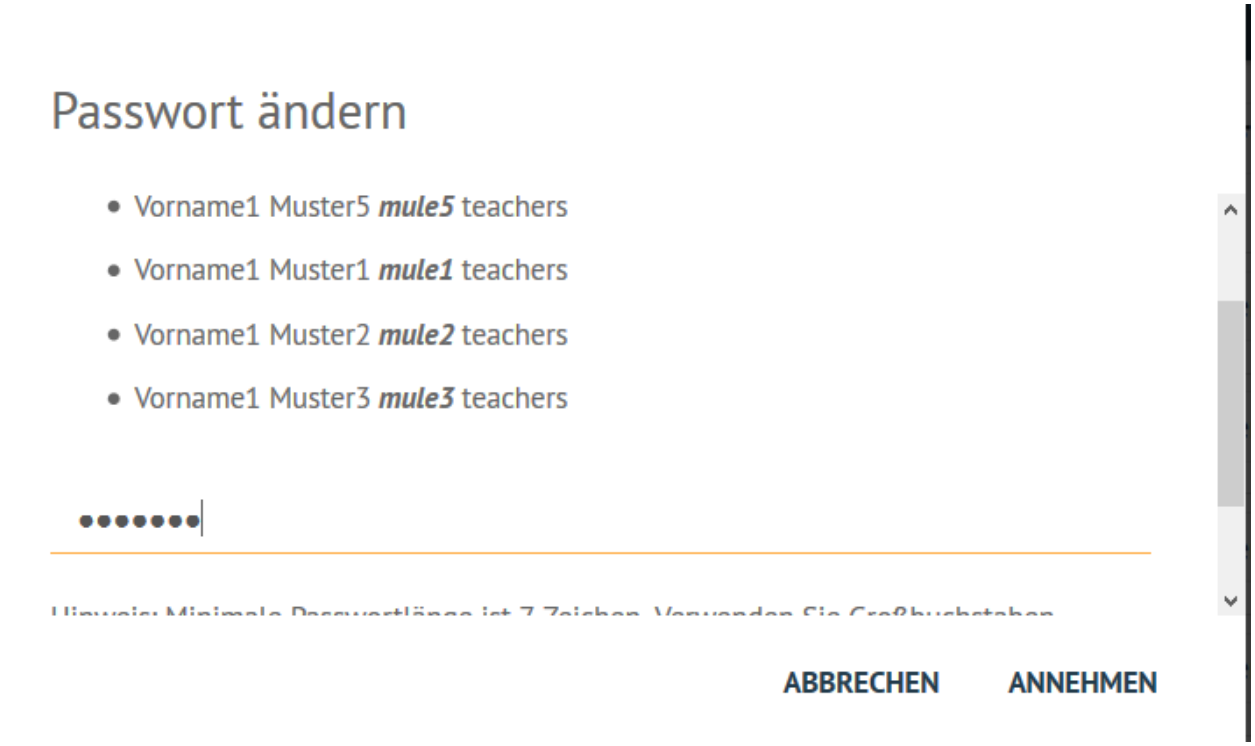
Dies können Sie auch über den Aufruf einzelner Lehrer, wie nachstehend beschrieben, kontrollieren.

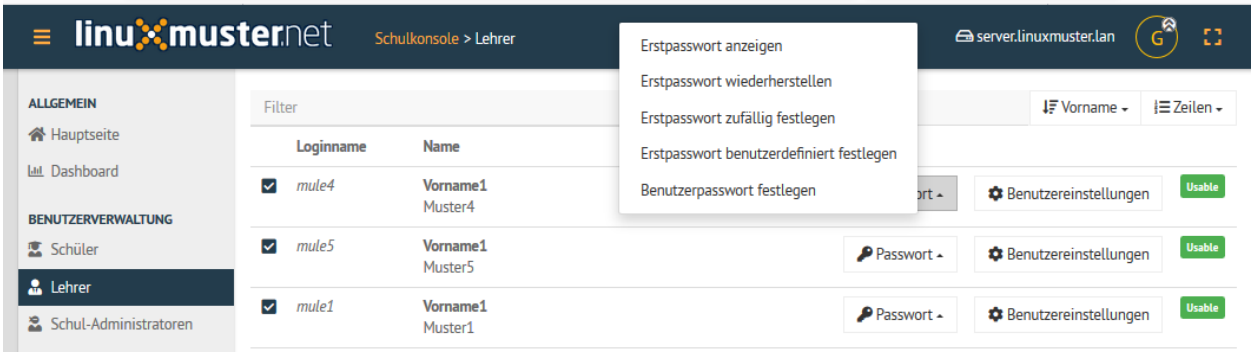
4.23.3 Einzelne Lehrer

In der Schulkonsole können Sie in der Benutzerverwaltung im Menü `Lehrer` als `global-admin` alle im System eingerichteten Lehrer-Accounts einsehen.

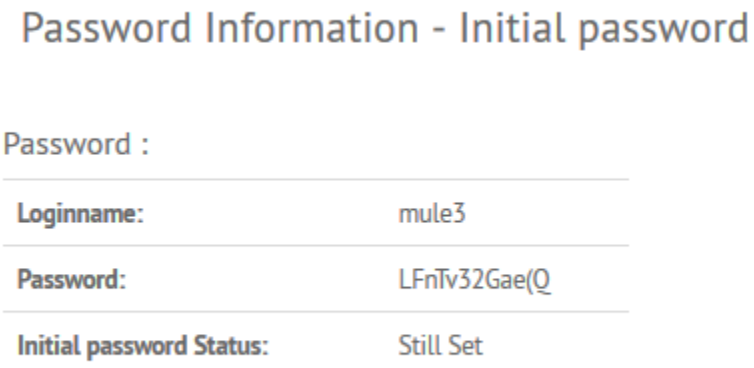
Um nun einzelne Kennworter zurückzusetzen, Benutzerinformationen zu erhalten, oder stichprobenartig einzelne Kennwörter zu prüfen (z.B. nach dem Zurücksetzen vieler ausgewählter Lehrer) nutzen Sie hier pro Lehrer die Untermenüs des Eintrags `Passwort` oder das Untermenü zu dem Eintrag `Benutzereinstellungen`.

Klicken Sie auf den Eintrag `Password`, erscheint ein Untermenü bei dem Sie mehrere Optionen für das Erstpasswort haben. Zudem git 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
ABBRECHEN
ANNEHMEN


linuxmusternet
Schulkonsole > Lehrer
server.linuxmuster.lan
Erstpasswort anzeigen
Erstpasswort wiederherstellen
Erstpasswort zufällig festlegen
Erstpasswort benutzerdefiniert festlegen
Benutzerpasswort festlegen
ALLGEMEIN
Hauptseite
Dashboard
BENUTZERVERWALTUNG
Schüler
Lehrer
Schul-Administratoren
Filter
Vorname
Zeilen
Loginname
Name
mule4
Vorname1 Muster4
mule5
Vorname1 Muster5
mule1
Vorname1 Muster1
Passwort
Benutzereinstellungen
Usable

Wählen Sie den Eintrag Erstpasswort anzeigen aus, so erscheinen nachfolgende Informationen für den jeweiligen Lehrer:

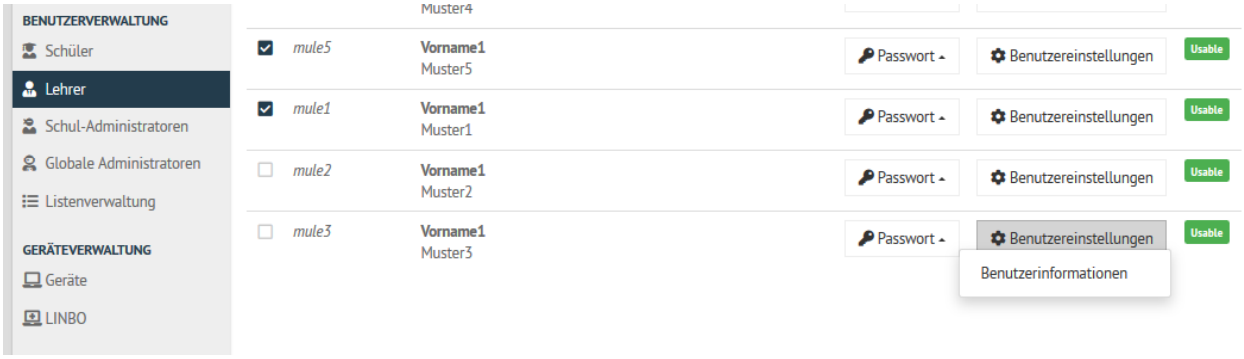


Die weiteren Einträge sind analog zu o.g. Erklärungen zu nutzen.

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.

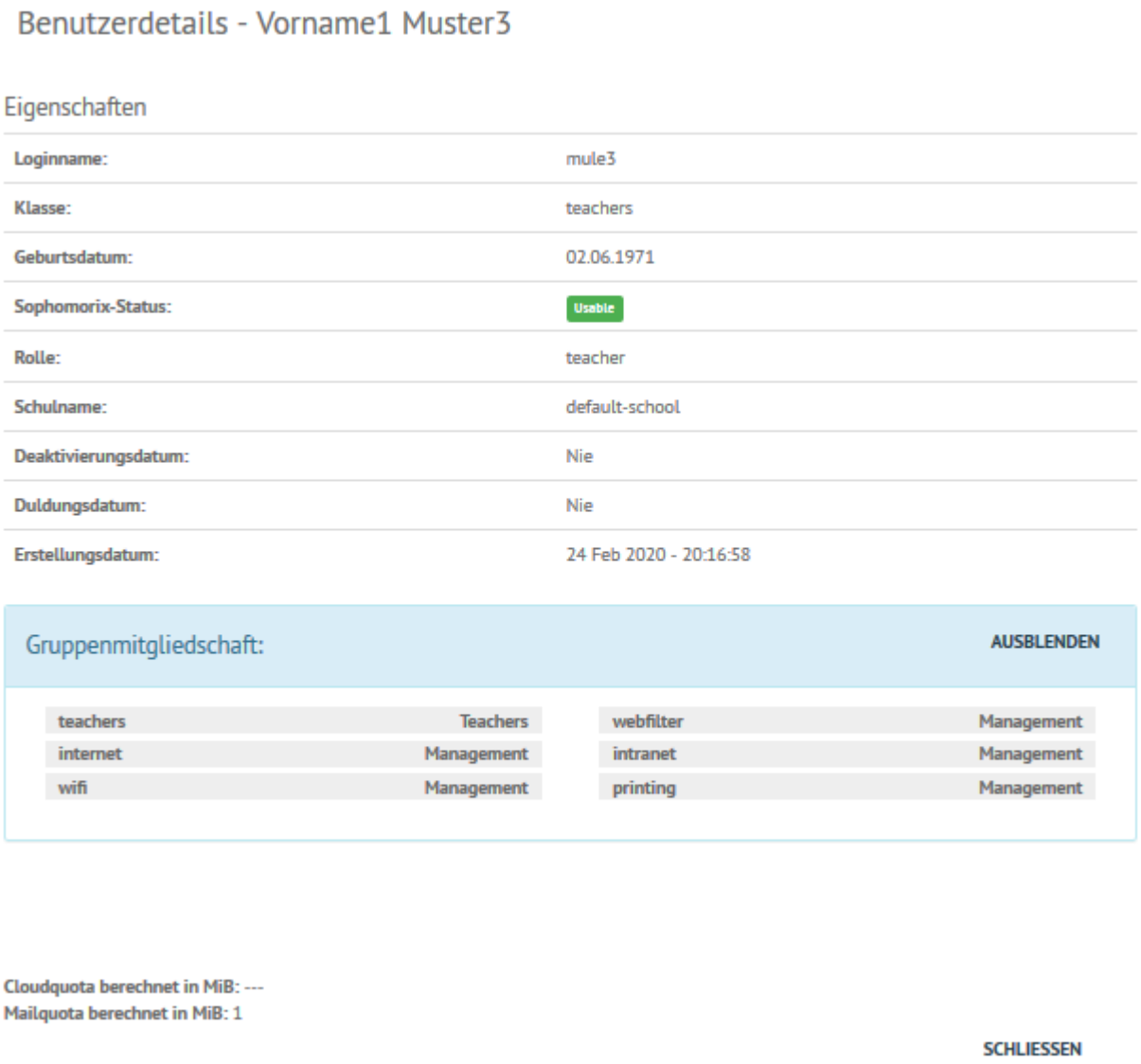
Für jeden Benutzer können Sie die die `Benutzerinformationen` anzeigen lassen.

Klicken Sie auf `Benutzereinstellngen`.



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
internet Management
wifi Management
webfilter Management
intranet 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 veschiedenen Partitionen - zur Verfügung steht. Danach ist zu planen, welche Obergrenzen zur Belegung des Festplattenplattes 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 ich an der Schulkonsole als `global-admin` an.

Gehen Sie im Menü der Schulkonsole unter dem Menüpunt `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`.

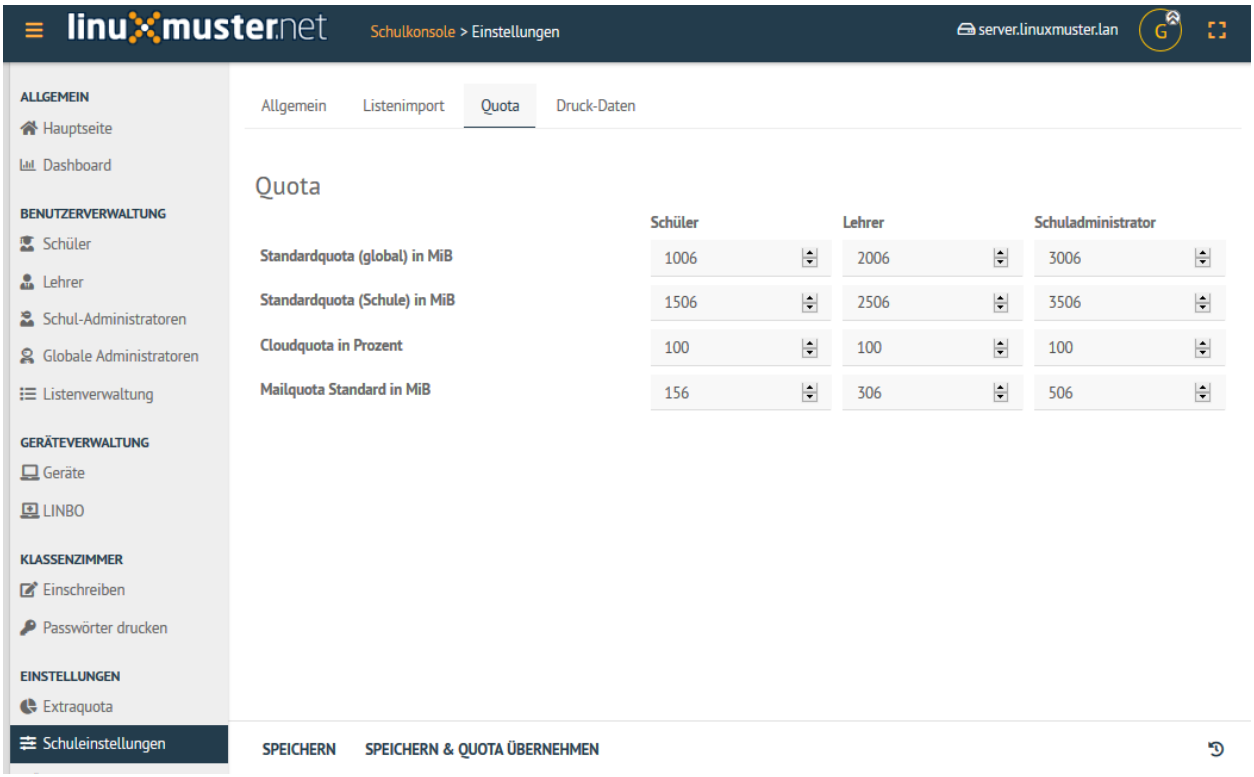
4.24.2 Quotas kontrollieren

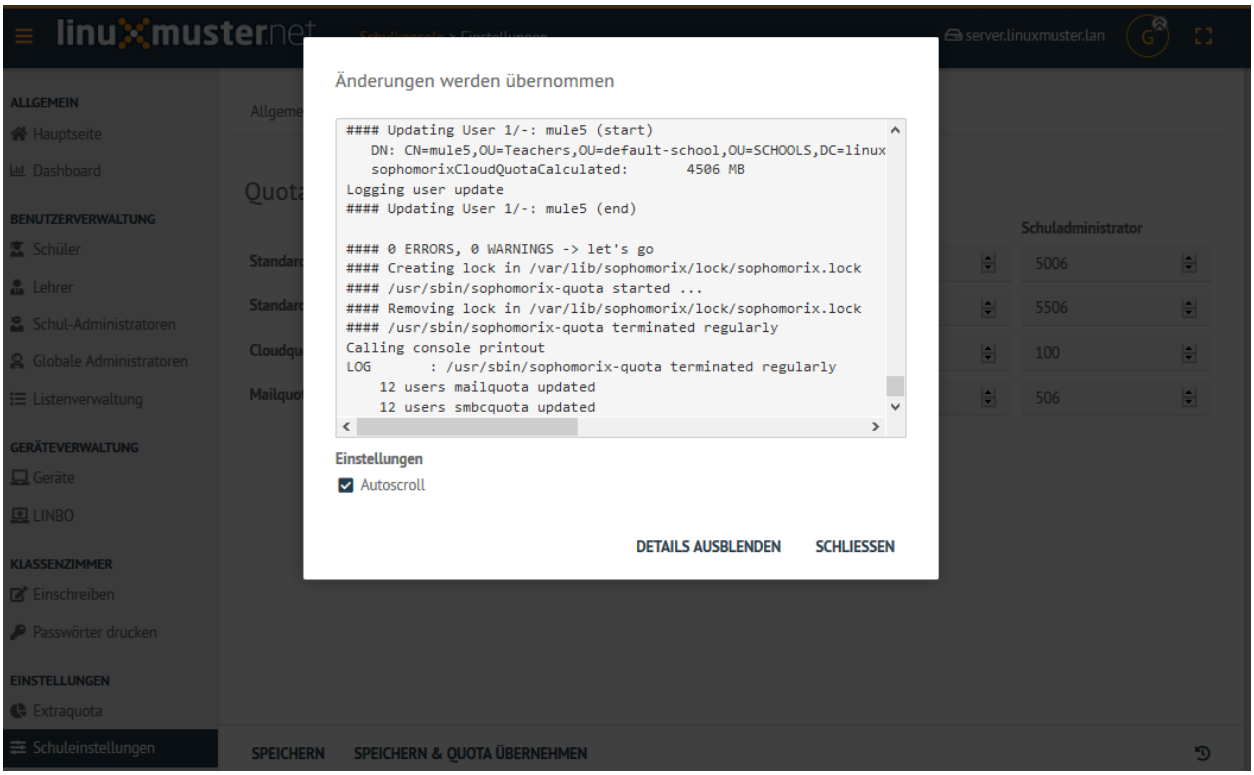
Nachdem die Änderungen angewendet wurden, sehen Sie die neuen Quotas in der Übersicht `Schuleinstellungen -> Quota`.

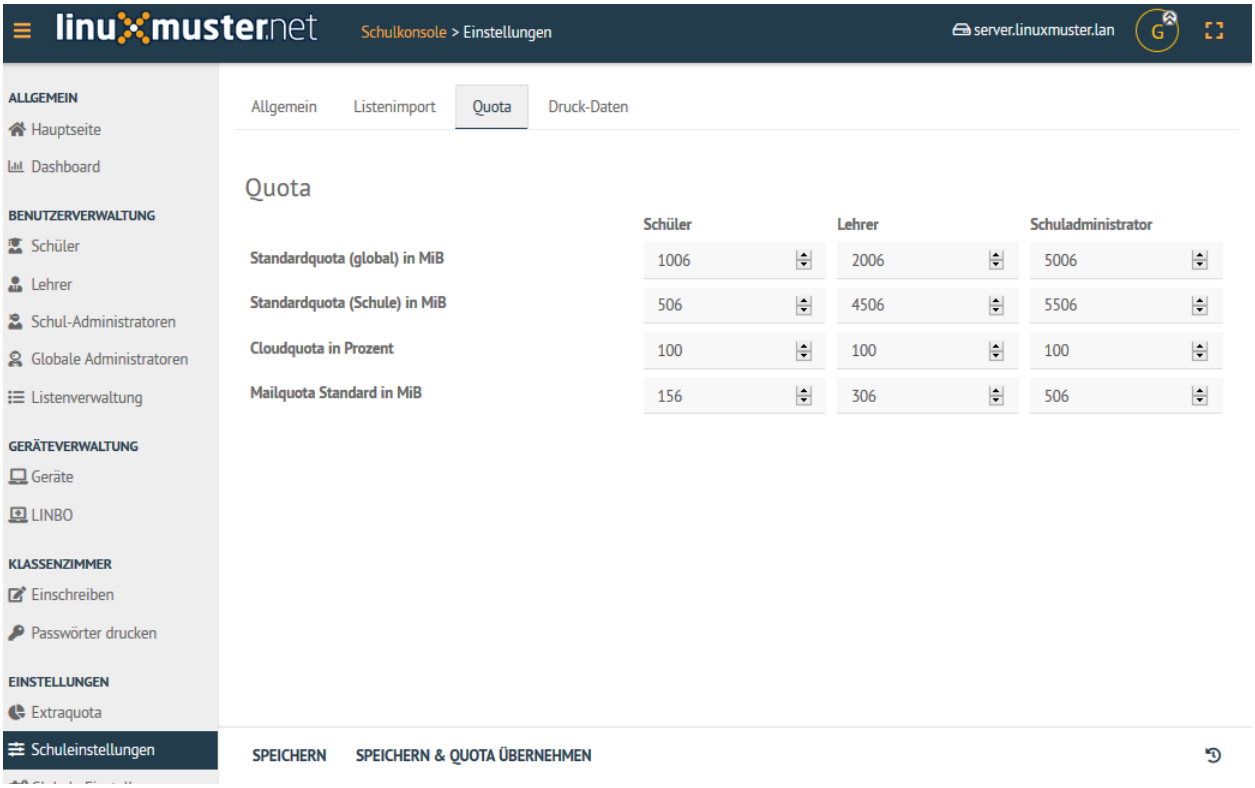
Die Quotas können Sie nun pro Benutzer kontrollieren.

Hierzu wählen Sie im Menü der Schulkonsole im Bereich der Benutzerveraltung 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


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 smbcquota updated
Einstellungen
Autoscroll
DETAILS AUSBLENDEN
SCHLIESSEN



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.

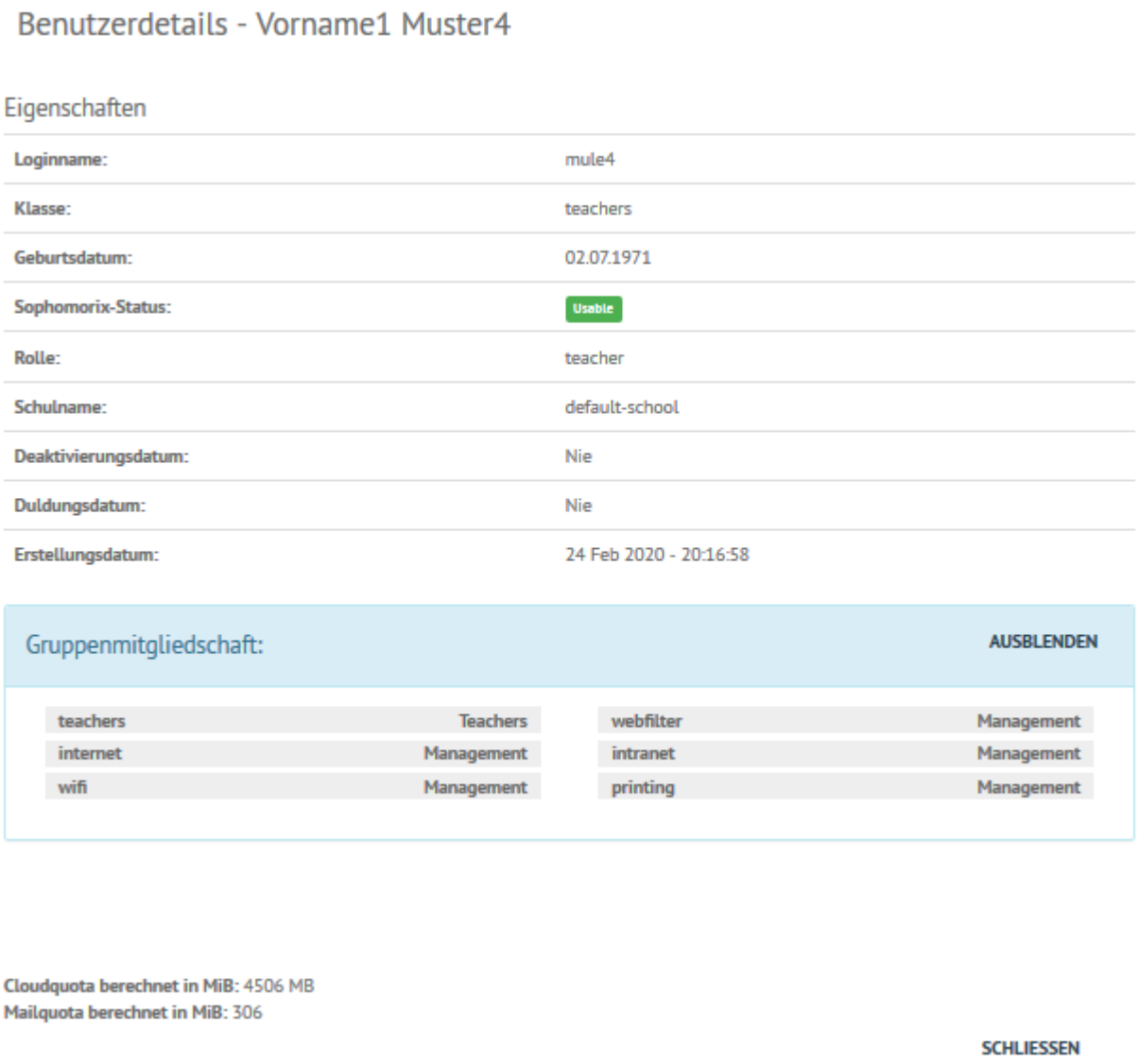
Lehrer

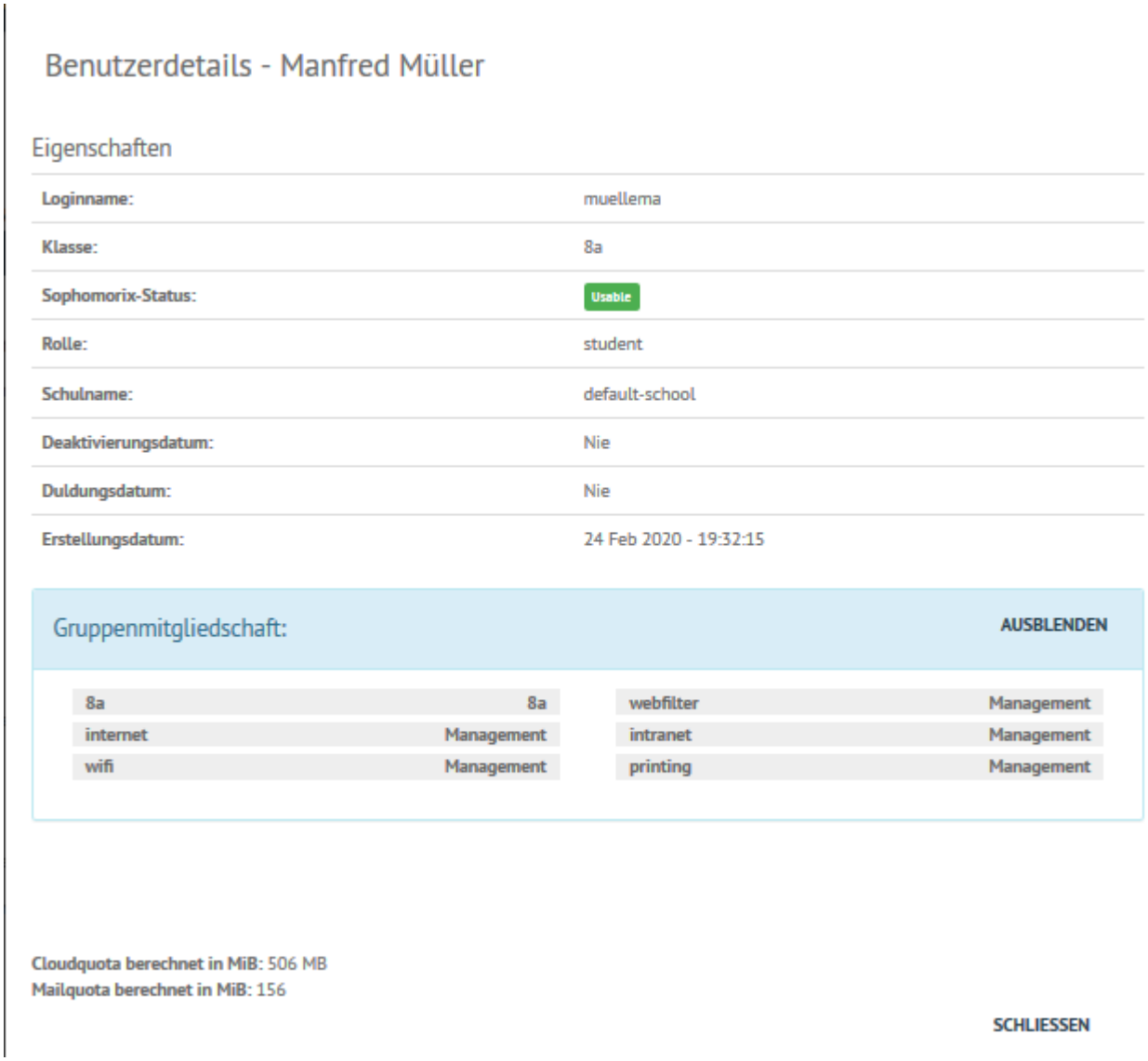
Haben Sie die Reiterkarte `Lehrer` gewählt, klicken Sie unten auf `Search & add user`. Es erscheint ein Konsolenfenster, in dem Sie einen Suchbegriff eingeben sollen, so dass passende Lehrer gefunden werden.

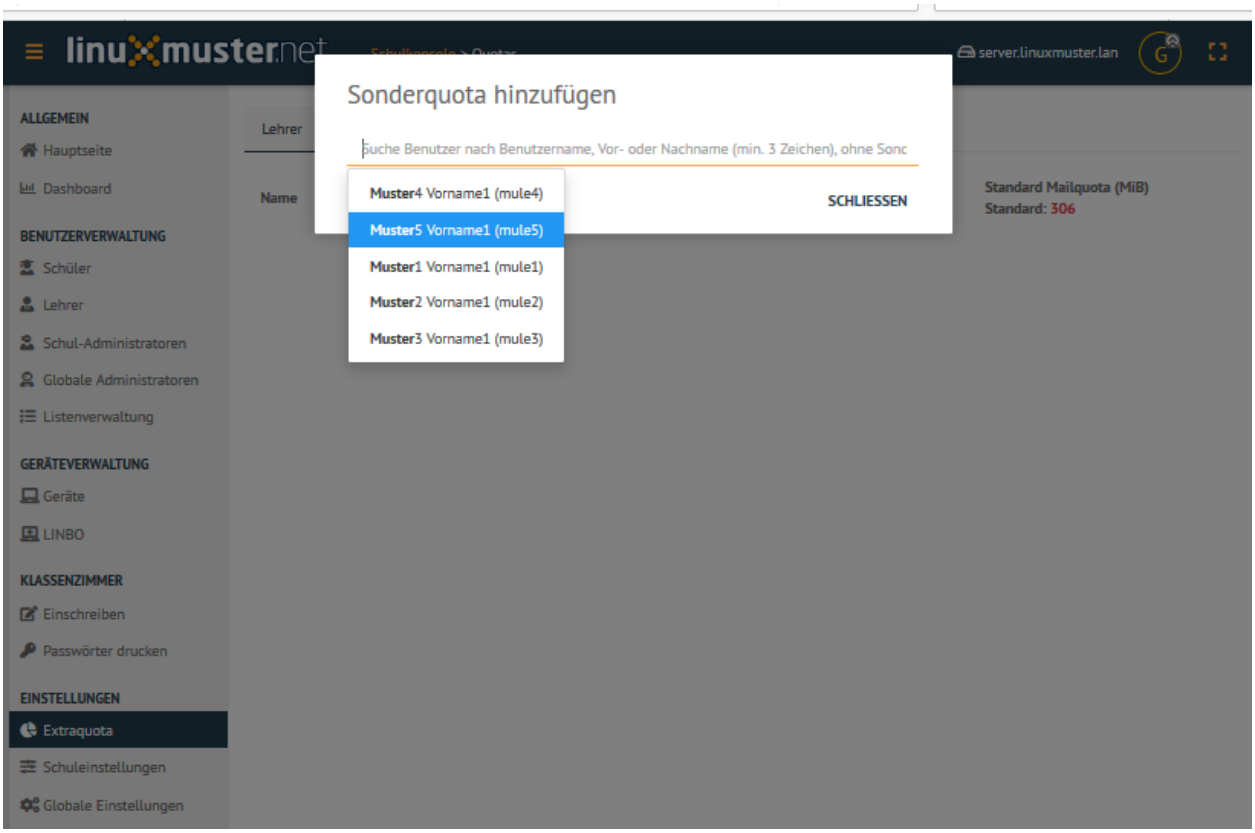
Wählen Sie aus der angezeigten Liste den gewünschten Benutzer aus und bestätigen Sie dies mit `Schliessen`.

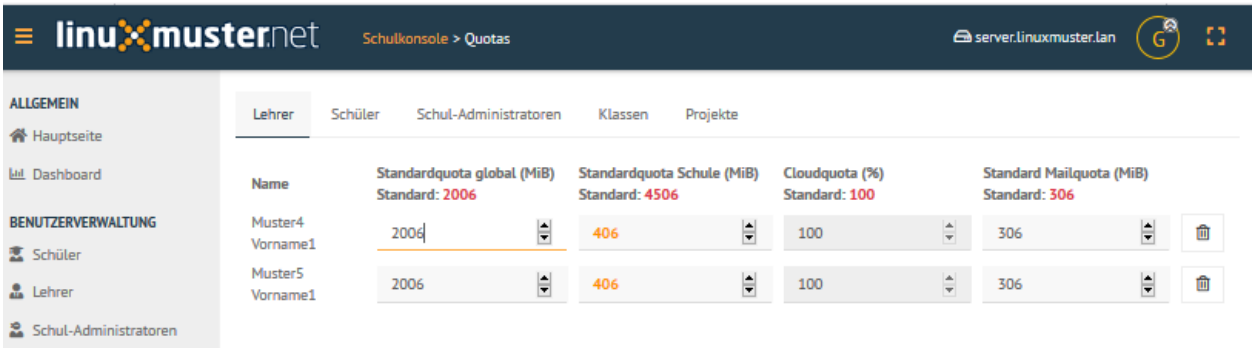
Danach sehen Sie in der Quota-Übersicht für Lehrer den Benutzer mit seinen bisherigen Quota-Eintragungen.

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
internet Management
wifi Management
webfilter Management
intranet Management
printing Management
Cloudquota berechnet in MiB: 4506 MB
Mailquota berechnet in MiB: 306
SCHLIESSEN

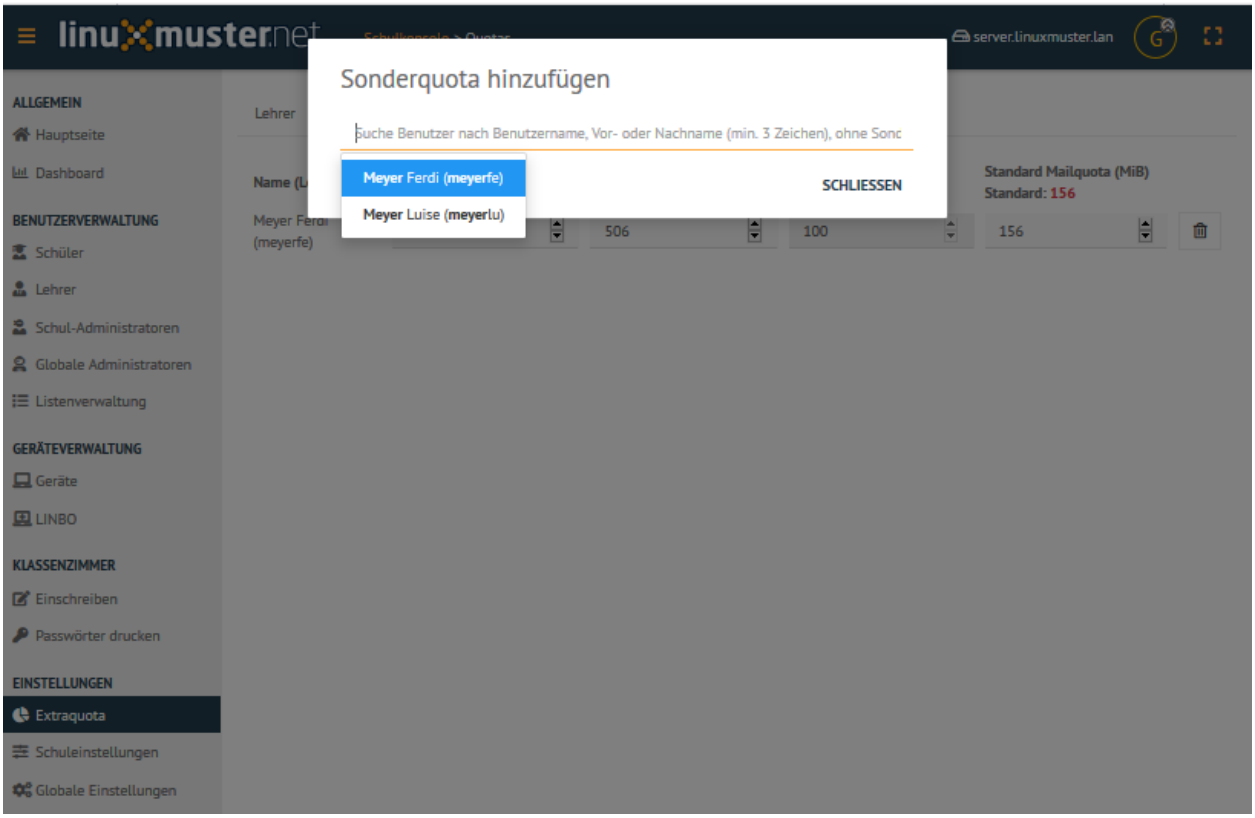

Benutzerdetails - Manfred Müller
Eigenschaften
Loginname: muellema
Klasse: 8a
Sophomorix-Status: Usable
Rolle: student
Schulname: default-school
Deaktivierungsdatum: Nie
Duldungsdatum: Nie
Erstellungsdatum: 24 Feb 2020 - 19:32:15
Gruppenmitgliedschaft:
AUSBLENDEN
8a 8a
internet Management
wifi Management
webfilter Management
intranet Management
printing Management
Cloudquota berechnet in MiB: 506 MB
Mailquota berechnet in MiB: 156
SCHLIESSEN


Sonderquota hinzufügen
Suche Benutzer nach Benutzername, Vor- oder Nachname (min. 3 Zeichen), ohne Sonc
Muster4 Vorname1 (mule4)
Muster5 Vorname1 (mule5)
Muster1 Vorname1 (mule1)
Muster2 Vorname1 (mule2)
Muster3 Vorname1 (mule3)
SCHLIESSEN
Lehrer
Name
Standard Mailquota (MiB)
Standard: 306
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


Schulkonsole > Quotas
server.linuxmuster.lan
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
2006
406
100
306
Muster5 Vorname1
2006
406
100
306

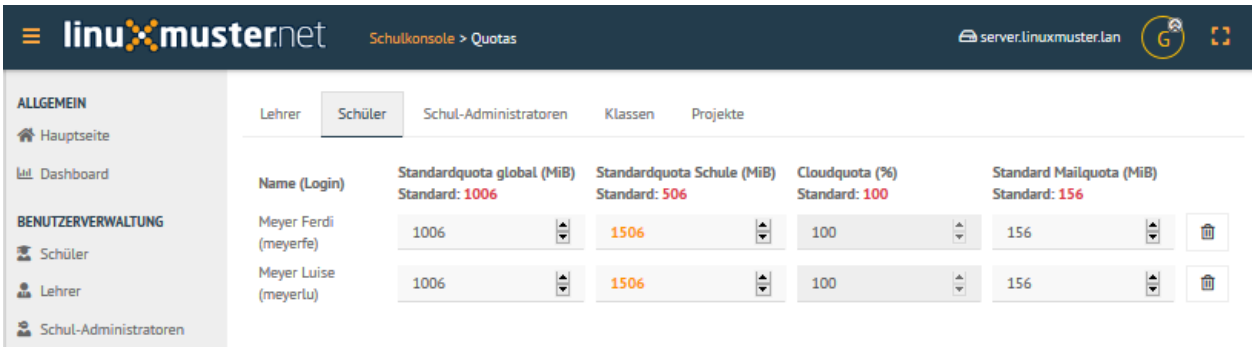
Schüler

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.

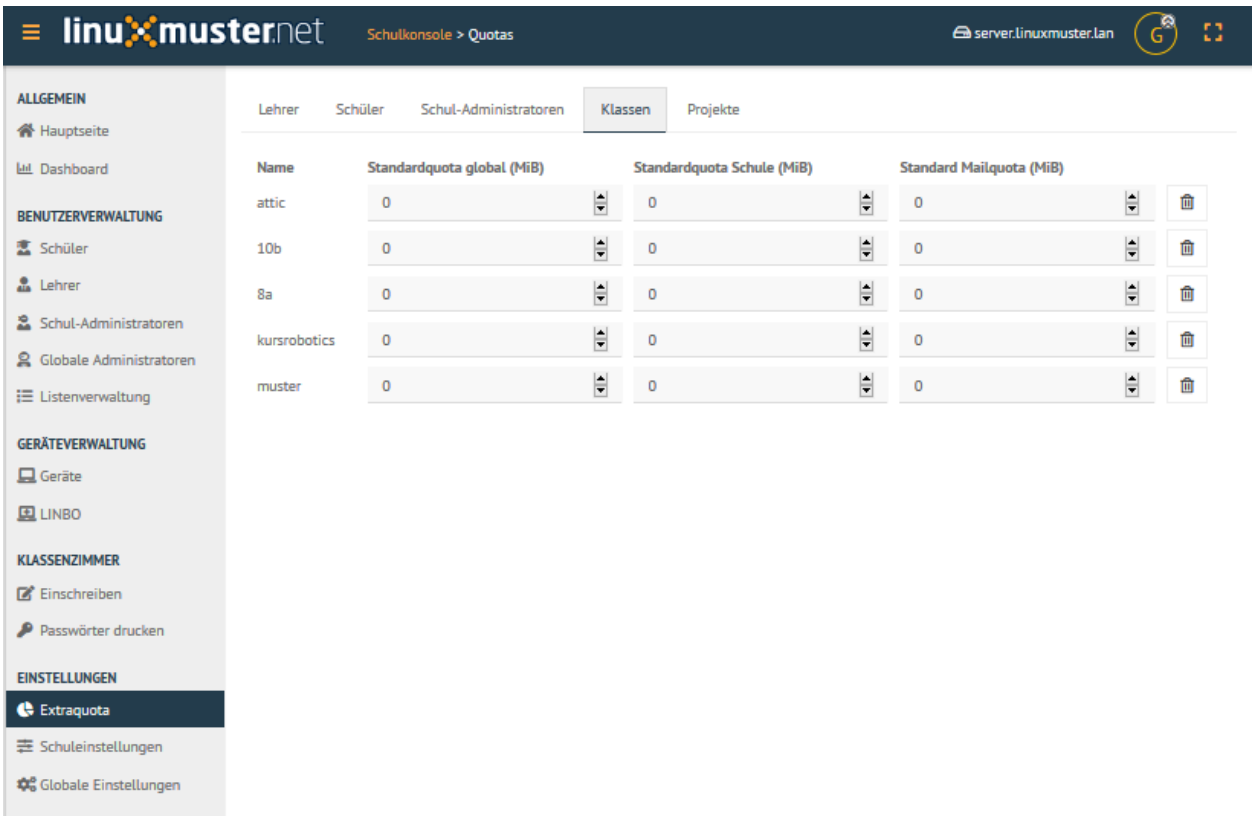


Passen Sie nun für die jeweiligen Benutzer, die Quotas wie gewünscht an. Änderungen gegenüber den bisherigen Vorgaben werden farblich abgesetzt.

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.

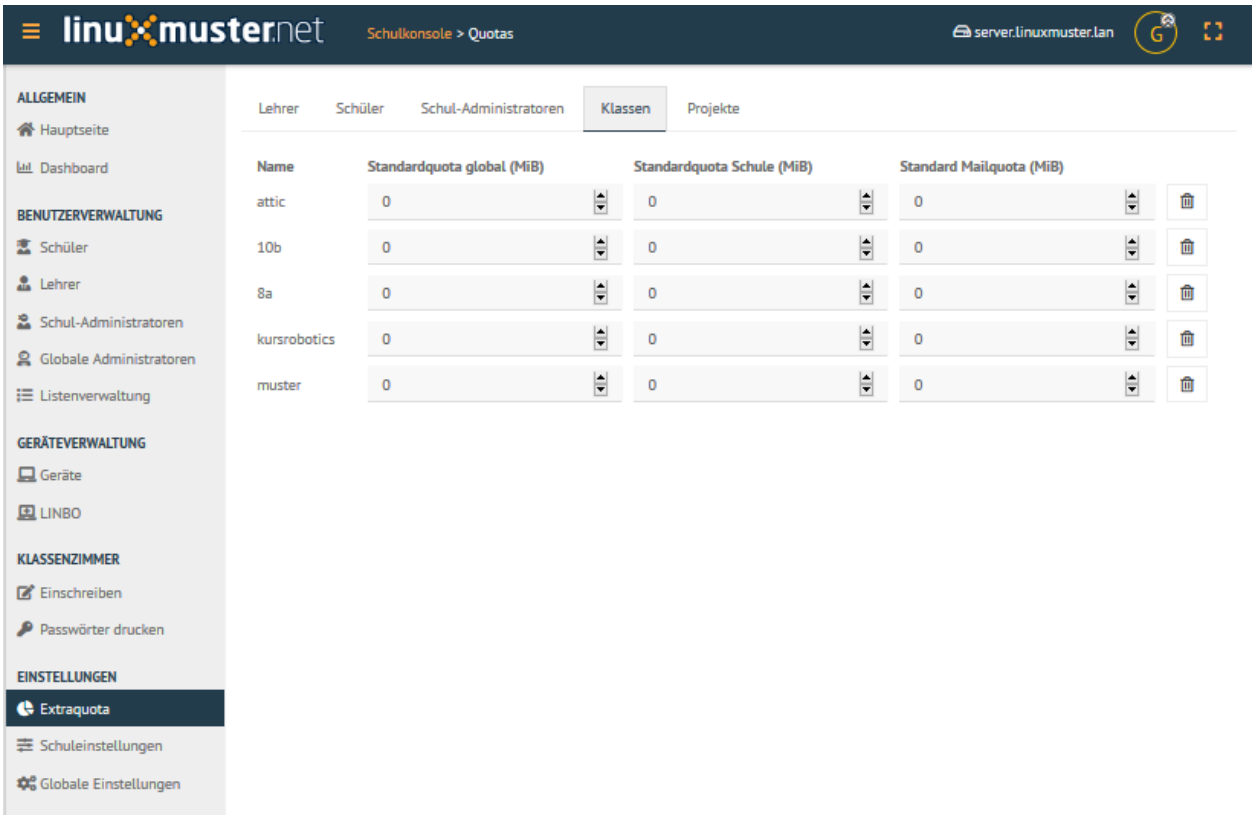


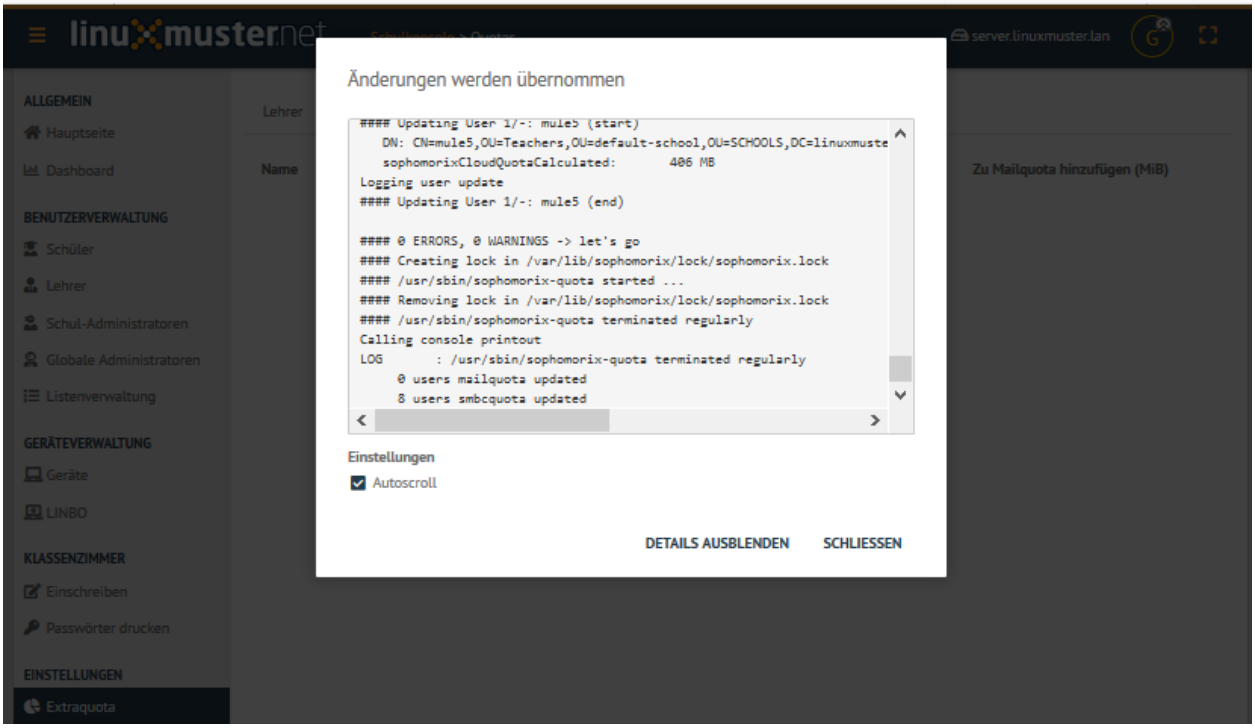
Nehmen Sie hier nun wie gewünscht die neuen Eintragungen für die Quotas der Klassen vor. Änderungen gegenüber den bisherigen Vorgaben werden farblich abgesetzt.

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`


linuxmusternet
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
10b
8a
kursrobotics
muster


Änderungen werden übernommen
Updating User 1/-: mule5 (start)
DN: CN=mule5,OU=Teachers,OU=default-school,OU=SCHOOLS,DC=linuxmuste
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 smbcquota updated
Einstellungen
Autoscroll
DETAILS AUSBLENDEN
SCHLIESSEN

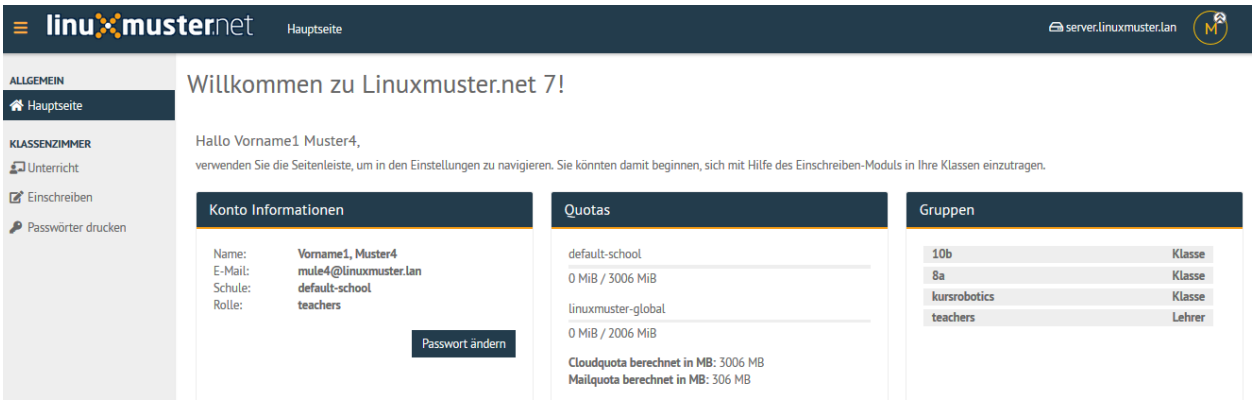
4.25 Vorbereitung am Schuljahresanfang

Autor des Abschnitts: @cweikl

4.25.1 Klassenliste aktualisieren

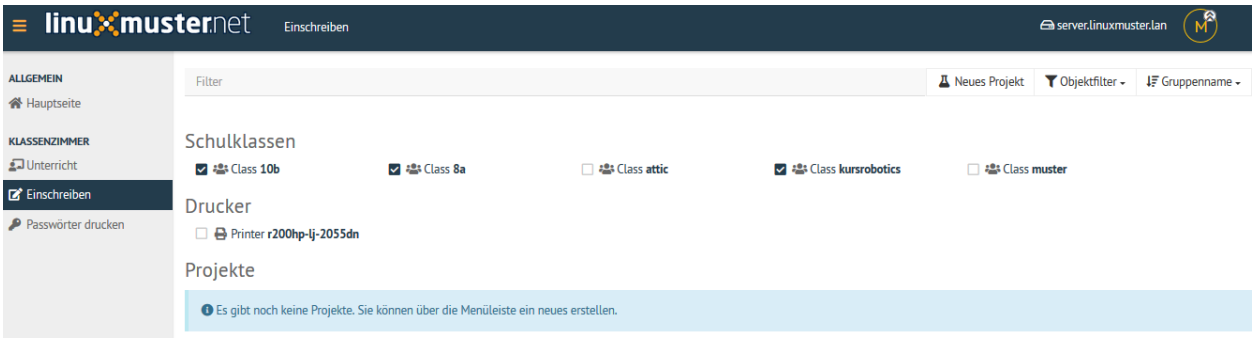
Zu Schuljahresbeginn muss jeder Lehrer seine Klassenliste aktualisieren. Neu zu unterrichtende Klassen sind hinzuzufügen und nicht mehr unterrichtete Klassen sind auszutragen. Voraussetzung für die Zuordnung neuer Klassen ist, dass diese im linuxmuster.net System bereits existieren. Ihr Schuladministrator 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.

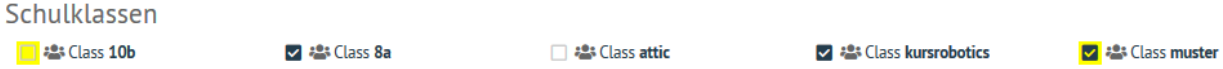


4.25.2 Klassenliste auswählen

Um Klassenlisten zu aktualisieren, ist nach erfolgreicher Anmeldung als Lehrer das Menü `Klassenzimmer` -> `Einschreiben` auszuwählen.

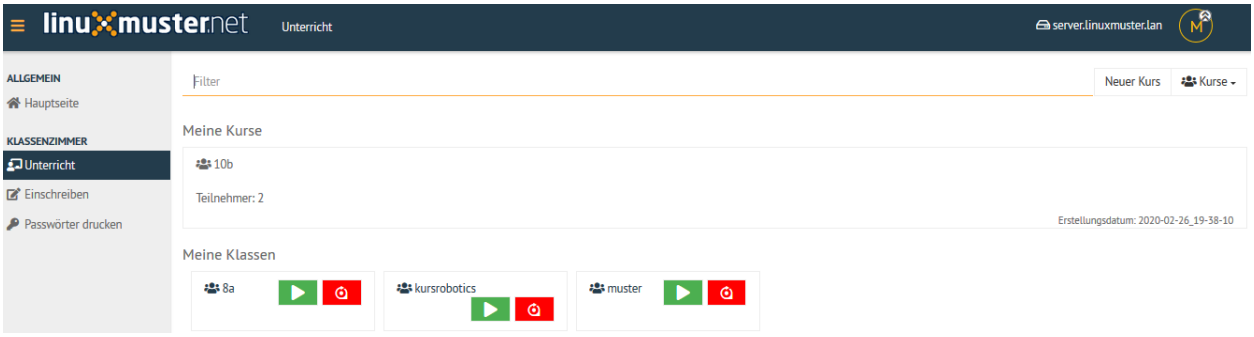


Jede Klasse, die dem Leher zugeordnet ist, ist mit einem Auswahlhäkchen markiert. Für Klassen, die nun dem Lehrer neu hinzugefügt werden sollen, ist das Häkchen vor der betreffenden Klasse zu setzen. Für Klassen, die im neuen Schuljahr nicht mehr dem Lehrer zugeordnet sein sollen, ist das Häkchen zu deaktivieren.



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

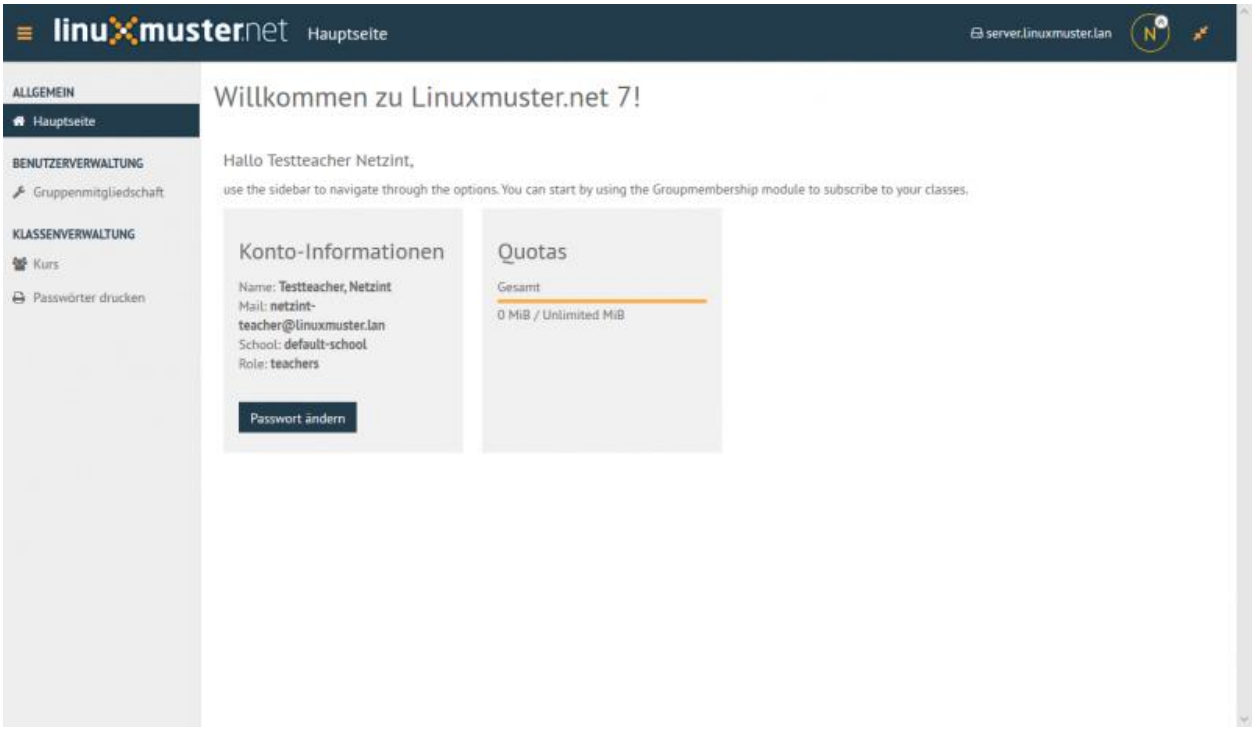
Abschließend müssen Sie sich von Ihrem Client abmelden und wieder neu anmelden, damit die Netzlaufwerke korrekt zugeordnet werden.

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

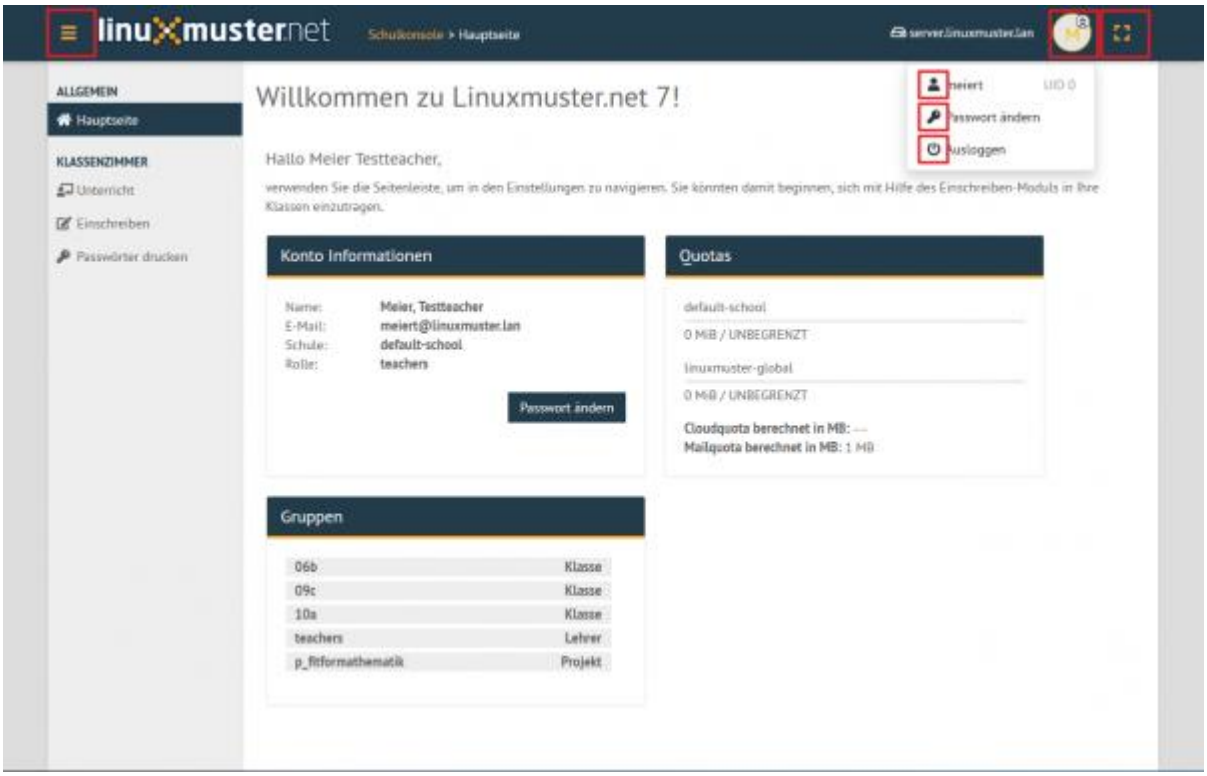
Autor des Abschnitts: @Maurice, @cweikl, @MachtDochNix (pics)

Haben Sie in linuxmuster.net v7 einen Lehrer-Account, so können Sie die Steuerung des Unterrichts web-basiert mithilfe der Schulkonsole in einem Browser vornehmen.



4.26.1 Allgemeine Bedienung

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:

- 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.

Die Schulkonsole des Lehrers teilt sich auf einen `Übersichtsbereich Allgemein` sowie auf `pädagogische Funktionen` im Bereich Klassenzimmer auf.

4.26.2 Allgemein

Hauptseite

Eine generelle Übersicht über Account- & Speicherinformationen des angemeldeten Benutzer. Möglichkeit zur Änderung des eigenen Passworts über `Passwort ändern`-Funktion.

Klassenzimmer

Unterricht

Kurse, in denen Sie Mitglied sind, werden hier aufgelistet.

Der Kurs „Dieser Raum“ wird dynamisch zusammengestellt mit angemeldeten Nutzern in einem Raum. Nur der Button zum neu starten der Sitzung ist auswählbar.

Bei Kursen unter „Meine Klassen“ kann unter 2 Button gewählt werden:

- Sitzung unverändert starten

Die Sitzung wird wie vorgefunden gestartet. Es kann also sein, dass hier Schüler, die nicht mehr in diese Klasse gehören, noch angezeigt werden oder hinzugekommene fehlen. Man kann Schüler aus anderen Klassen hinzufügen und entfernen. Das bleibt dann solange, bis die Sitzung neu erstellt wird.

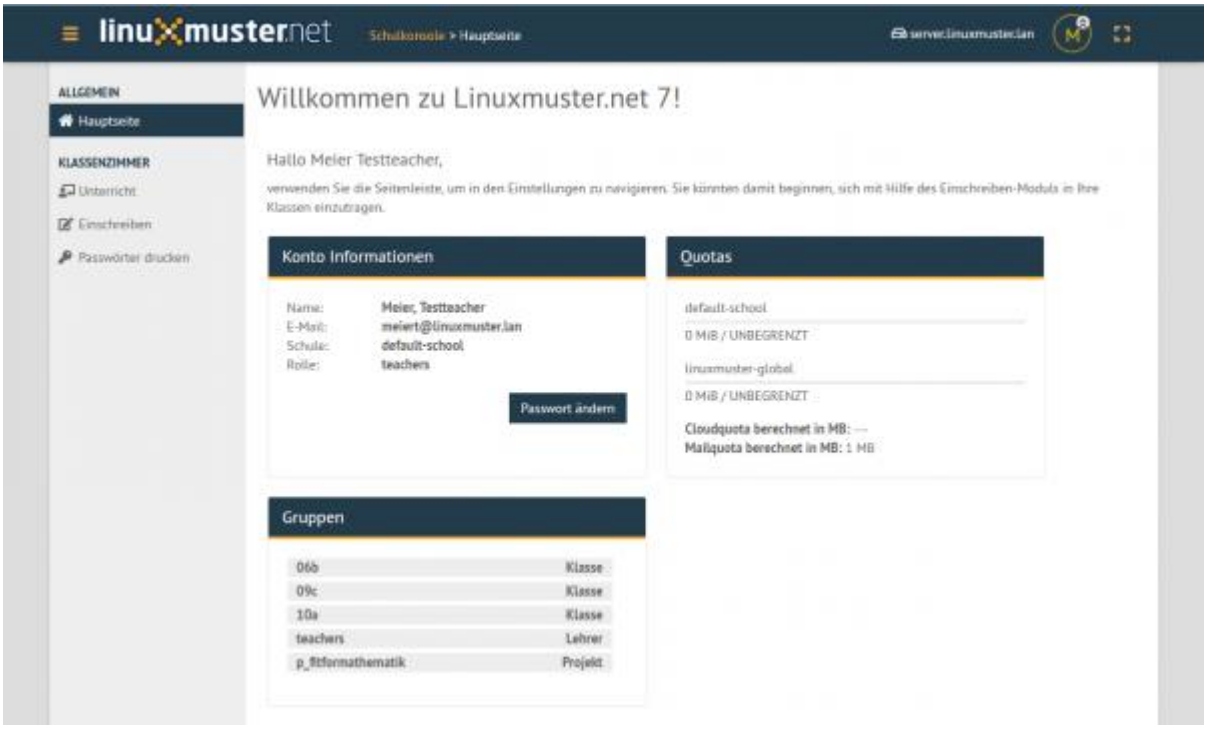
- Sitzung neu erstellen

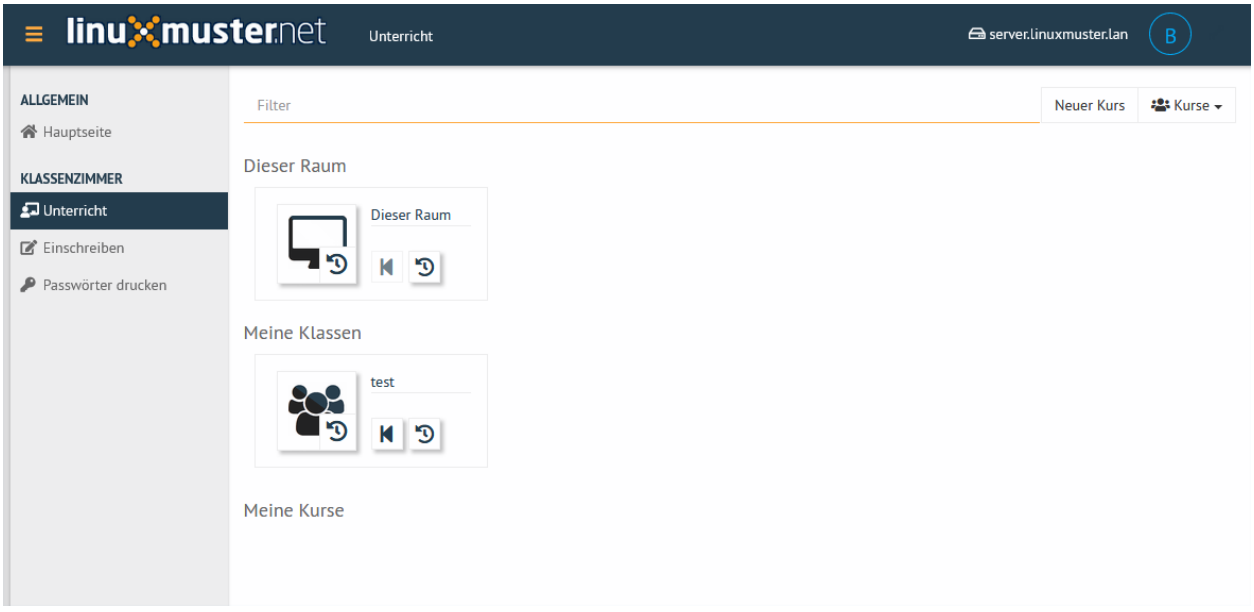
Es handelt sich hier um den aktuellen Stand der Schüler wie er im AD zu finden ist. Das erstellen dauert einen Moment länger.

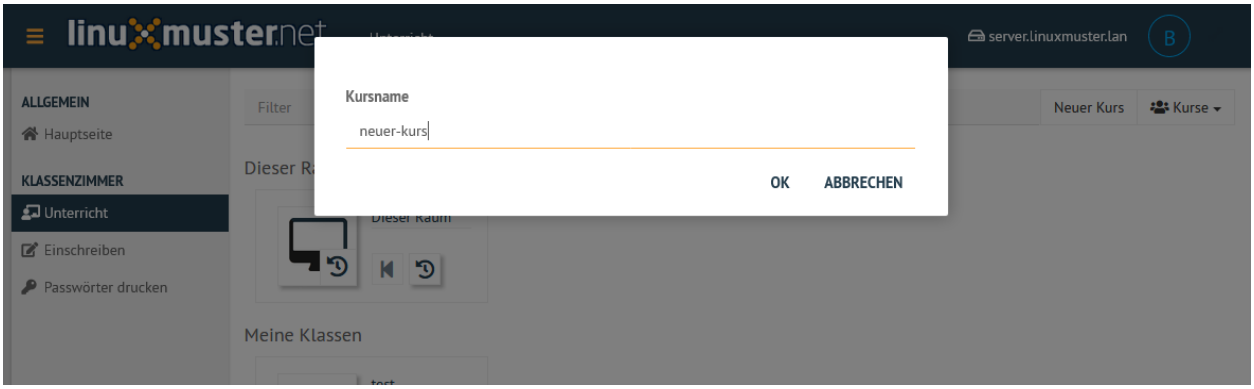
Unterhalb von „Meine Kurse“ finden Sie ihre selbst erstellten Kurse.

Kurse erstellen

Unter Kurse können Sie über die Funktion oben rechts `Neuer Kurs` einen neuen Kurs anlegen. Geben Sie dazu den Kursnamen ein und bestätigen mit OK.

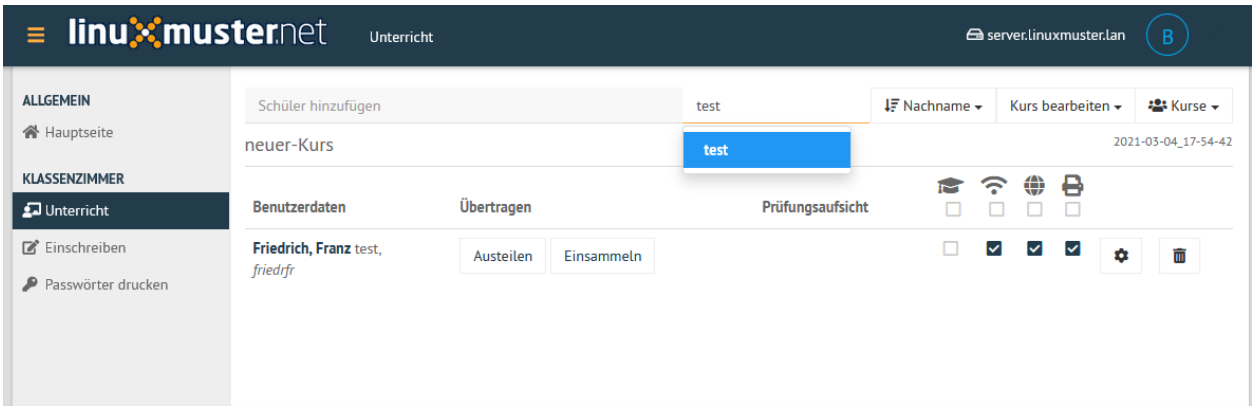

linuxmuster.net
Schulkonsole > Hauptseite
server.linuxmuster.lan
ALLGEMEIN
Hauptseite
KLASSENZIMMER
Unterricht
Einschreiben
Passwörter drucken
Willkommen zu Linuxmuster.net 7!
Hallo Meier Testteacher,
verwenden Sie die Seitenleiste, um in den Einstellungen zu navigieren. Sie könnten damit beginnen, sich mit Hilfe des Einschreiben-Moduls in Ihre Klassen einzutragen.
Konto Informationen
Name: Meier, Testteacher
E-Mail: meiert@linuxmuster.lan
Schule: default-school
Rolle: teachers
Passwort ändern
Quotas
default-school
0 MiB / UNBEGRENZT
linuxmuster-global
0 MiB / UNBEGRENZT
Cloudquota berechnet in MB: —
Mailquota berechnet in MB: 1 MB
Gruppen
06b Klasse
09c Klasse
10a Klasse
teachers Lehrer
p_fitformathematik Projekt


linuxmuster.net
Unterricht
server.linuxmuster.lan
B
ALLGEMEIN
Hauptseite
KLASSENZIMMER
Unterricht
Einschreiben
Passwörter drucken
Filter
Neuer Kurs
Kurse
Dieser Raum
Dieser Raum
Meine Klassen
test
Meine Kurse



Schüler einem Kurs hinzufügen

Um Schüler einem Kurs hinzuzufügen, den jeweiligen Kurs auswählen. In den oberen Zeilen gibt es nun die Möglichkeit über `Schüler hinzufügen` einzelne Schüler hinzuzufügen oder über `Klasse hinzufügen` eine ganze Schulklasse. Um die Übernahme der ausgewählten Benutzer in den Kurs anzuwenden, unten rechts mit `Speichern & Übernehmen` bestätigen.



Wählen Sie nun einen bestimmten Kurs aus, finden Sie eine Ansicht nach folgendem Schema vor.

In dieser Übersicht können die pädagogischen Funktionen WLAN-, Internet- & Drucker-Freigabe, Dateien-Übertragungs- Funktion und Prüfungsmodus genutzt werden.

WLAN-, Internet-Freigabe & Drucker-Freigabe

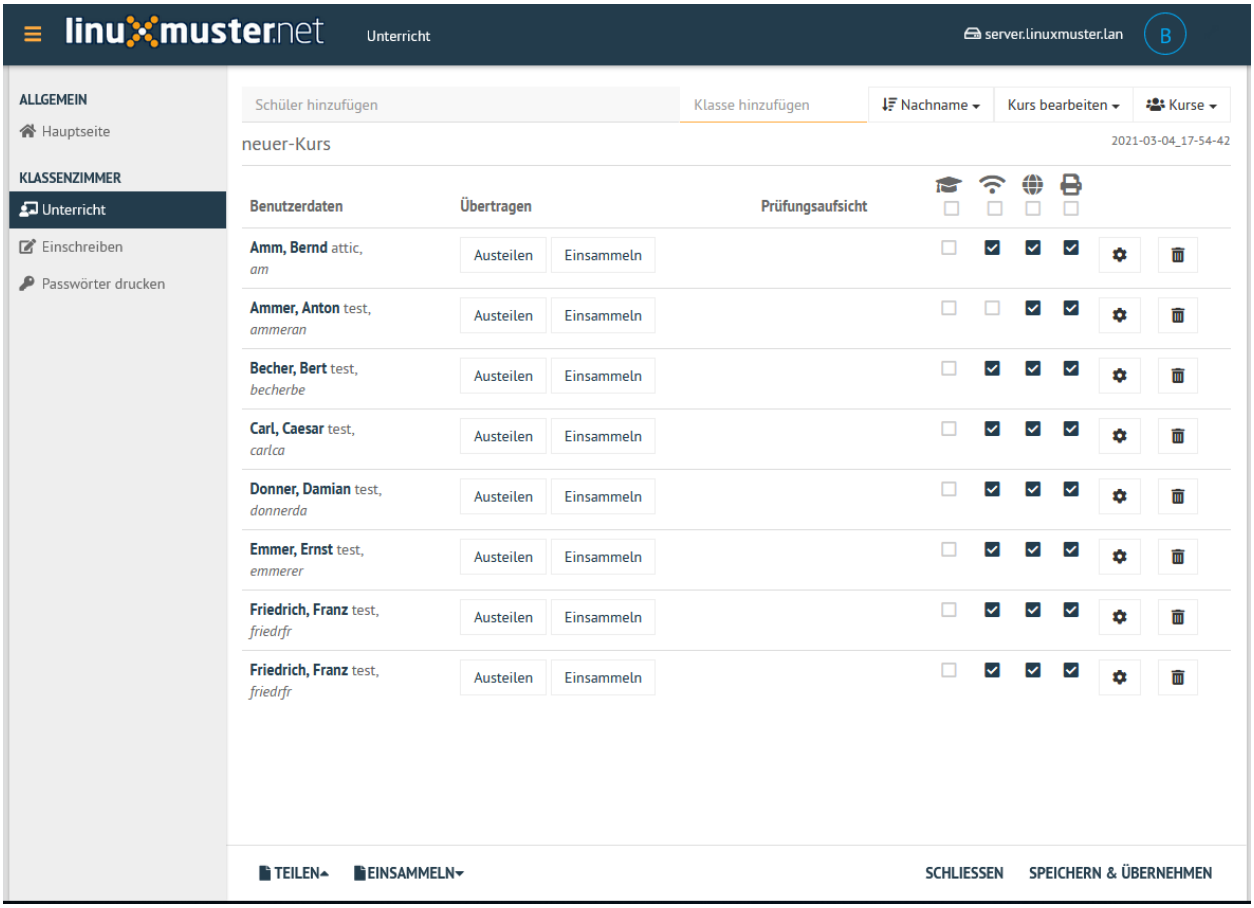
- WLAN-Freigabe
- Internet-Freigabe
- Drucker-Freigabe

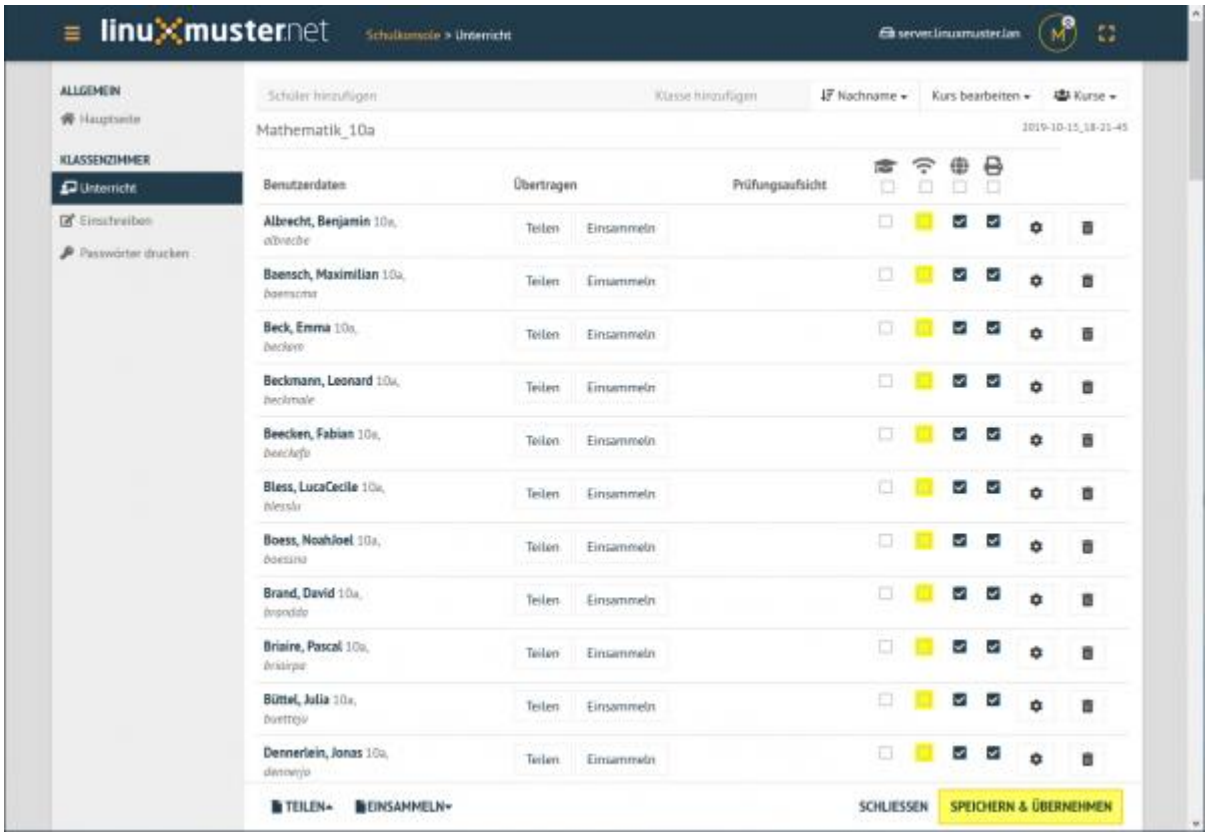
Freigaben zu den jeweiligen Diensten können über `Haken setzen oder entfernen` für jeweilige Benutzer freigegeben oder gesperrt werden. Über das Kästchen direkt unter einem Dienstsymbol kann die Freigabe zu dem jeweiligen Dienst mit `Speichern & Übernehmen` auf alle Benutzerangewendet werden. Beispielsweise wurde hier mit einem Klick unter das WLAN-Symbol für jeden Benutzer des aktuellen Kurses der WLAN-Zugang gesperrt.

- Einstellungen (Zahnrad)

Unter Einstellungen sind verschiedene Optionen zum Passwort des Benutzers zu finden.

- Löschen (Mülleimer)


linuxmuster.net
Unterricht
server.linuxmuster.lan
B
ALLGEMEIN
Hauptseite
KLASSENZIMMER
Unterricht
Einschreiben
Passwörter drucken
Schüler hinzufügen
Klasse hinzufügen
Nachname
Kurs bearbeiten
Kurse
neuer-Kurs
2021-03-04_17-54-42
Benutzerdaten
Übertragen
Prüfungsaufsicht
Amm, Bernd attic, am
Ammer, Anton test, ammeran
Becher, Bert test, becherbe
Carl, Caesar test, carlca
Donner, Damian test, donnerda
Emmer, Ernst test, emmerer
Friedrich, Franz test, friedrfr
Friedrich, Franz test, friedrfr
Austeilen
Einsammeln
TEILEN
EINSAMMELN
SCHLIESSEN
SPEICHERN & ÜBERNEHMEN


linuxmusternet
Schulkonsole > Unterricht
ALLGEMEIN
Hauptseite
KLASSENZIMMER
Unterricht
Einschreiben
Passwörter drucken
Schüler hinzufügen
Klasse hinzufügen
Nachname
Kurs bearbeiten
Kurse
Mathematik_10a
Benutzerdaten
Übertragen
Prüfungsaufsicht
Albrecht, Benjamin 10a
Baensch, Maximilian 10a
Beck, Emma 10a
Beckmann, Leonard 10a
Beecken, Fabian 10a
Bless, LucaCecile 10a
Boess, Noahjoel 10a
Brand, David 10a
Brinire, Pascal 10a
Büttel, Julia 10a
Dennerlein, Jonas 10a
Teilen
Einsammeln
TEILEN
EINSAMMELN
SCHLIESSEN
SPEICHERN & ÜBERNEHMEN

Mit Hilfe des Löschen Button können einzelne Schüler aus dem Kurs entfernt werden. Dies gilt, bis die Sitzung neu erstellt wird.

Sämtliche Änderungen müssen mit `Speichern & Übernehmen` übernommen werden!

Dateien-Übertragungs-Funktion

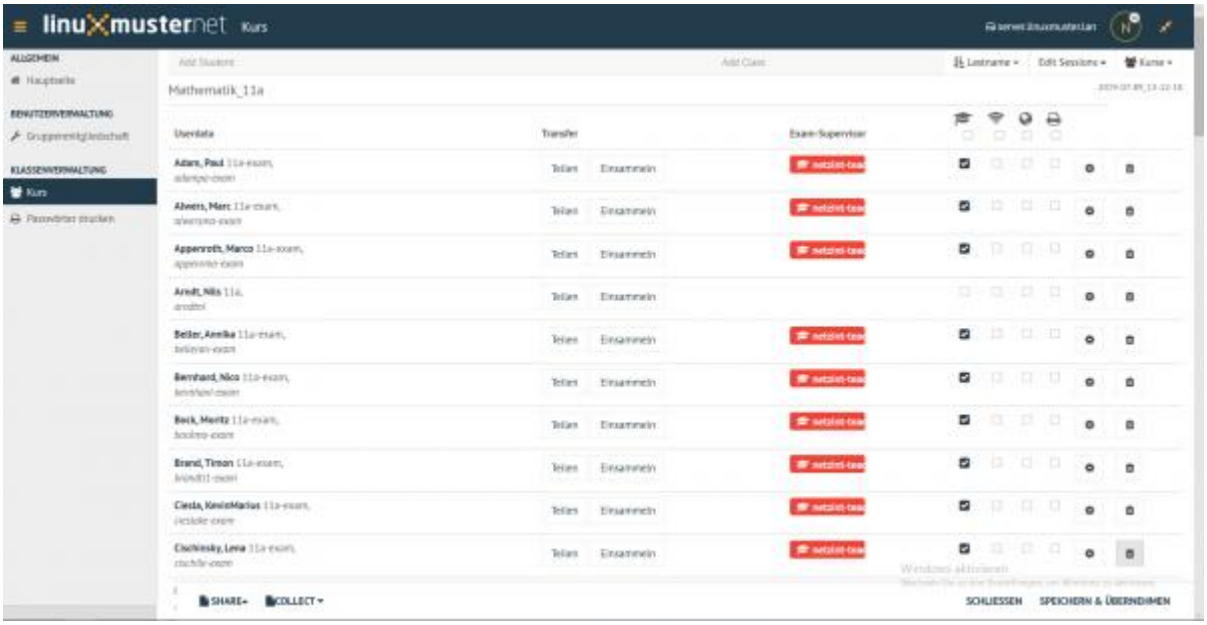
Eine nützliche Funktion für Unterrichtsarbeit mit Dateien bietet linuxmuster.net mit der `Austeilen- & Einsammeln-Funktion`. Auf der Kursseite finden Sie im unteren Bereich die `Teilen` und `Einsammeln` Funktionen, welche sich auf alle Kursteilnehmer beziehen. Neben jedem Benutzer selbst gibt es `Austeilen` und `Einsammeln` Funktionen, welche auf einzelne Benutzer angewendet werden.

Weitere Erläuterungen sind im Abschnitt Austeilen und Einsammeln zu finden.

Prüfungsmodus

Das Absolventenkappen-Symbol

stellt den Prüfungsmodus dar. Ausgewählte Schüler können dadurch in diesen Modus gesetzt werden (nach Speichern & Übernehmen unten rechts). Im aktivierten Prüfungsmodus wird die Seite in folgendem Schema angezeigt.

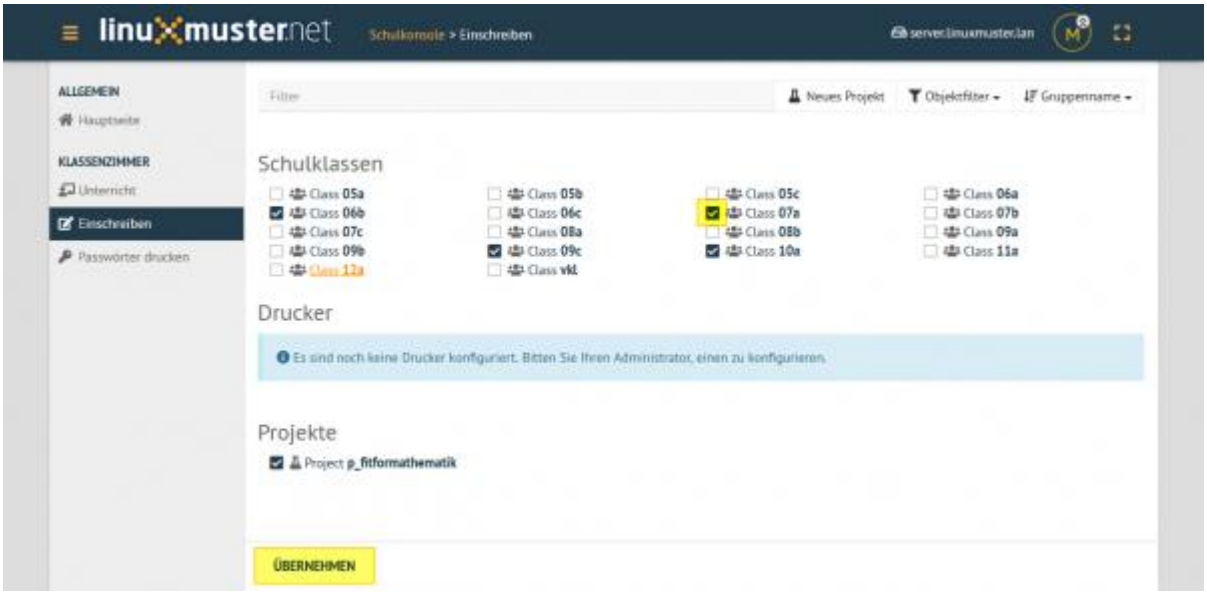


Schülern im Prüfungsmodus ist automatisch die WLAN-, Internet- & Drucker-Freigabe gesperrt. Dies kann jedoch angepasst werden. Um den Prüfungsmodus zu terminieren, den Haken bei jedem Kursmitglied entfernen und `Speichern & Übernehmen` ausführen.

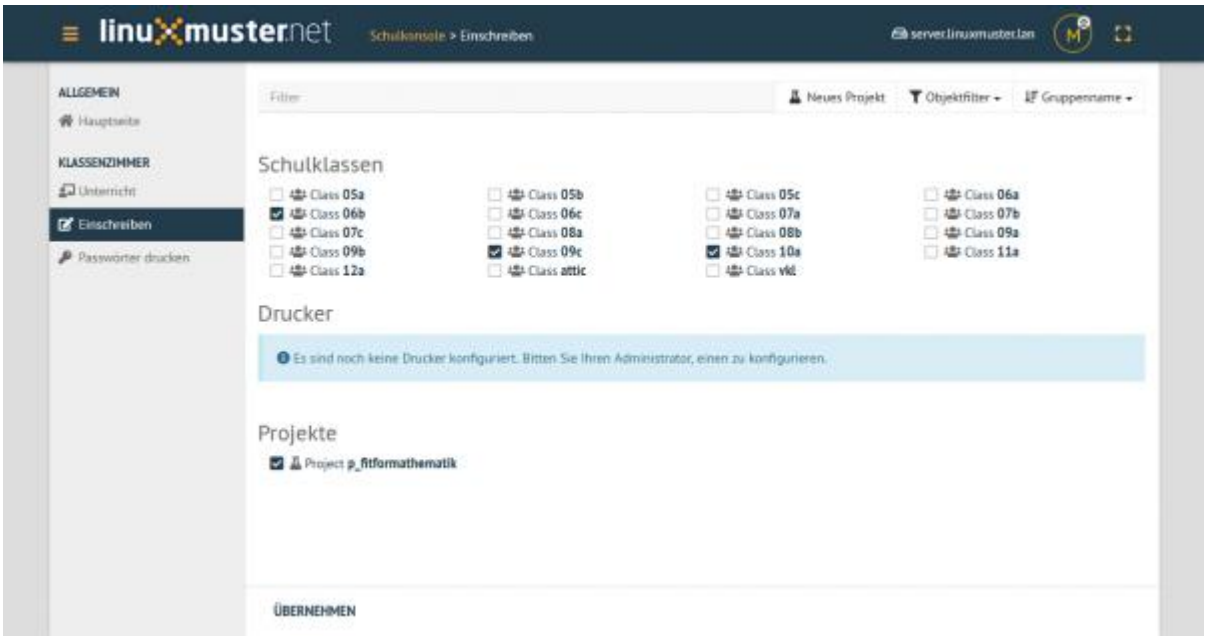
Weitere Hinweise sind im Abschnitt Prüfungsmodus Klassenarbeitsmodus zu finden.

Einschreiben

Dieser Abschnitt dient Lehrern dazu sich in Schulklassen, Projekte oder zu Druckern einzuschreiben. Lehrer ordnen sich hier beispielsweise zu Beginn des Schuljahres den jeweiligen Klassen zu.

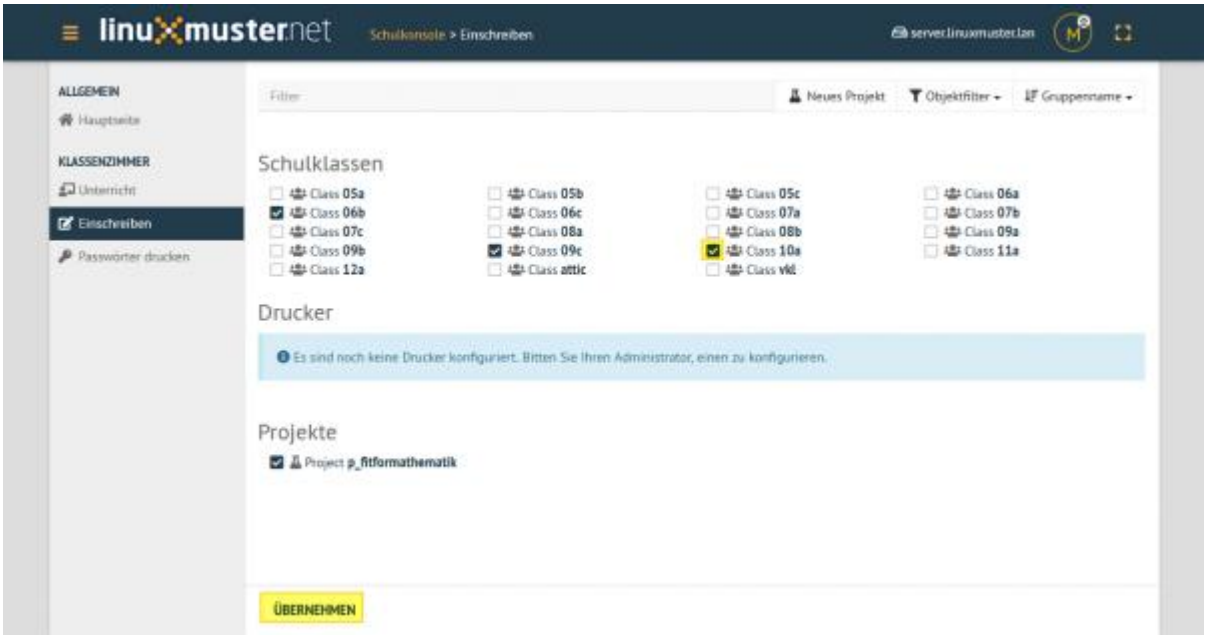


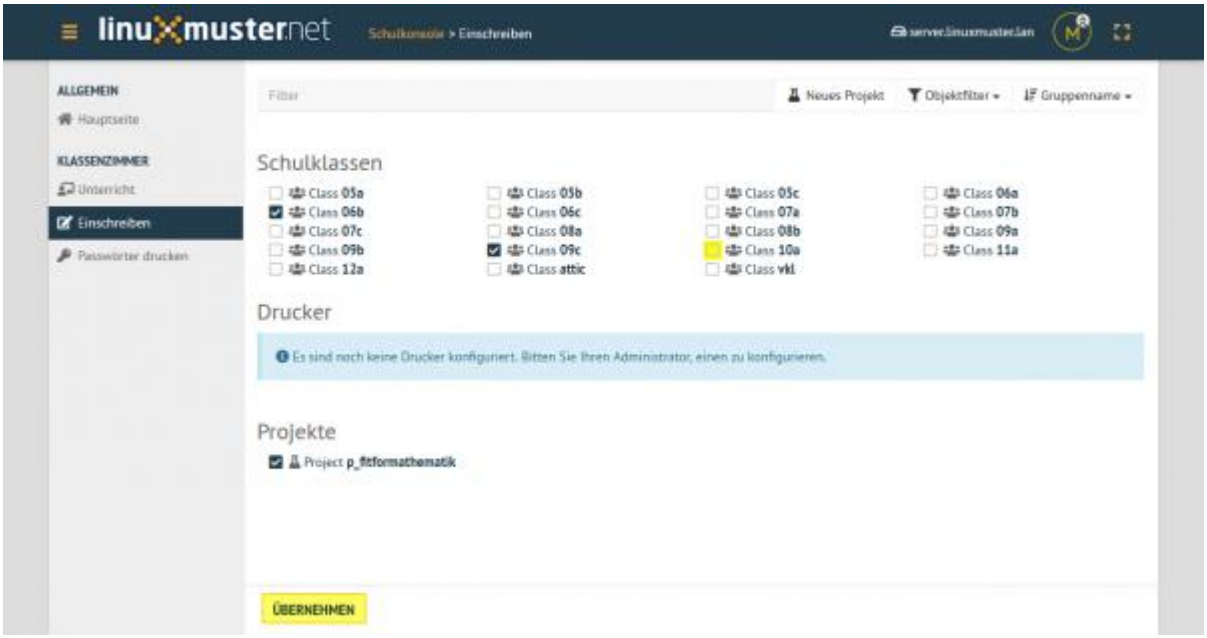
Ein jeweiliges Objekt zum Einschreiben auswählen oder den Haken entfernen um daraus auszutreten. Geänderte Einstellungen werden gelb angezeigt. Um die Änderungen anzuwenden, auf `Übernehmen` klicken. In diesem Abschnitt finden Sie eine übersichtliche Darstellung zu zugehörigen Schulklassen, Druckern und Projekten. Für detaillierte Informationen zu einem Objekt, dieses anklicken.



Objekt beitreten: Das jeweilige Objekt durch Anhaken auswählen und anschließend mit der Übernehmen-Taste unten links bestätigen.

Aus Objekt austreten: Den Haken des jeweiligen Objektes entfernen und anschließend mit der `Übernehmen-Taste` unten links bestätigen.


linuxmusternet
Schulkonsole > Einschreiben
server.linuxmuster.lan
ALLGEMEIN
Hauptseite
KLASSENZIMMER
Unterricht
Einschreiben
Passwörter drucken
Filter
Neues Projekt
Objektfilter
Gruppenname
Schulklassen
Class 05a
Class 05b
Class 05c
Class 06a
Class 06b
Class 06c
Class 07a
Class 07b
Class 07c
Class 08a
Class 08b
Class 09a
Class 09b
Class 09c
Class 10a
Class 11a
Class 12a
Class attic
Class vkl
Drucker
Es sind noch keine Drucker konfiguriert. Bitten Sie Ihren Administrator, einen zu konfigurieren.
Projekte
Project p_fitformathematik
ÜBERNEHMEN


linuxmusternet
Schulkonsole > Einschreiben
server.linuxmuster.lan
ALLGEMEIN
Hauptseite
KLASSENZIMMER
Unterricht
Einschreiben
Passwörter drucken
Filter
Neues Projekt
Objektfilter
Gruppenname
Schulklassen
Class 05a
Class 05b
Class 05c
Class 06a
Class 06b
Class 06c
Class 07a
Class 07b
Class 07c
Class 08a
Class 08b
Class 09a
Class 09b
Class 09c
Class 10a
Class 11a
Class 12a
Class attic
Class vkl
Drucker
Es sind noch keine Drucker konfiguriert. Bitten Sie Ihren Administrator, einen zu konfigurieren.
Projekte
Project p_fitformathematik
ÜBERNEHMEN

Schulklassen

Hier werden alle Schulklassen aufgelistet. Durch Anklicken werden weitere Informationen angezeigt, wie etwa die dazugehörigen Schüler.

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

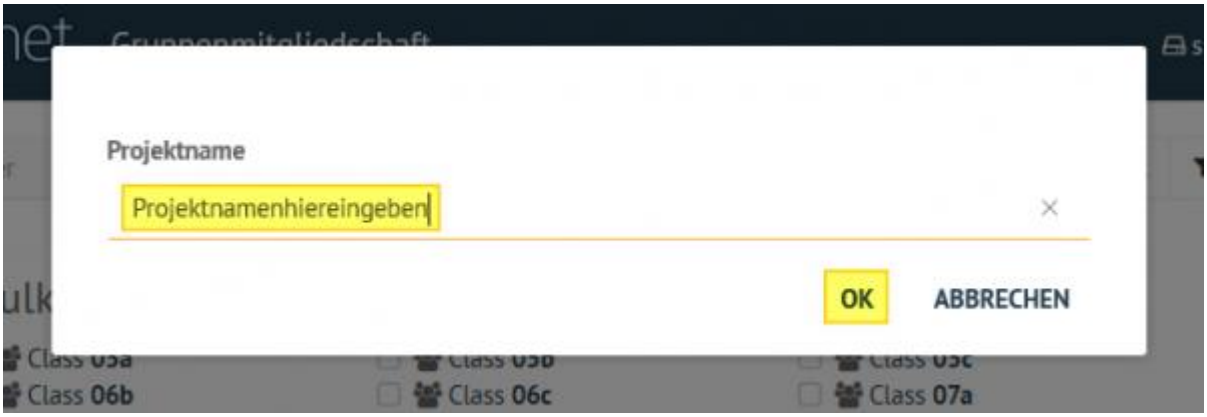
Hier werden alle Projekte aufgelistet. Projekte unterscheiden sich von Kursen:

- Mehrere Lehrer können in eine Projektgruppe aufgenommen werden.
- Projekte verfügen über eigene Tauschverzeichnisse
- Projekte können wiederverwendet werden.
- Unterrichtssteuerung (Passwörter ändern, Internet sprerren, etc.) ist nicht möglich

Projekt anlegen: Über

mit `OK` erstellen.

Im rechten oberen Bereich, können Sie ein neues Projekt benennen und mit `OK` erstellen.

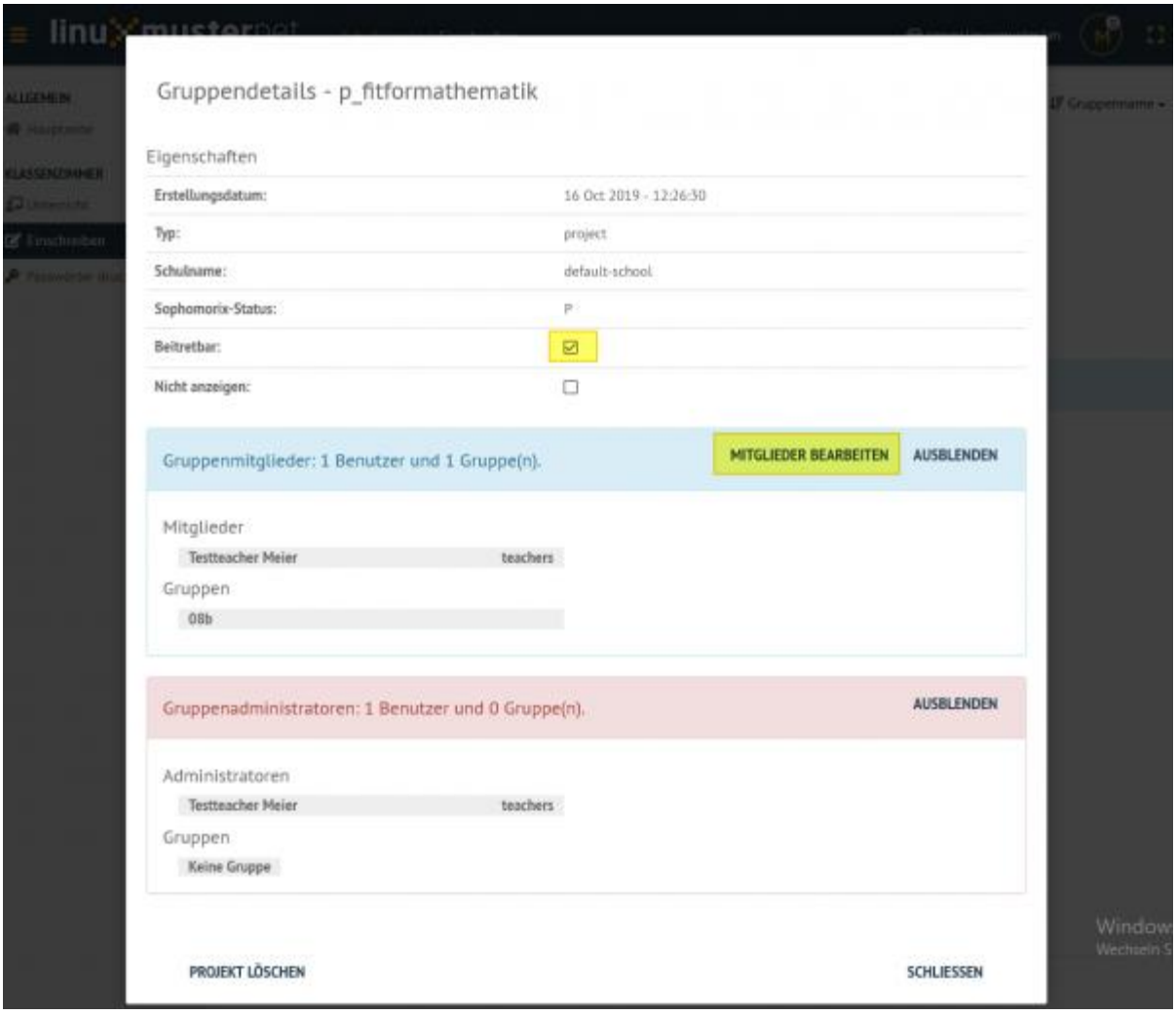


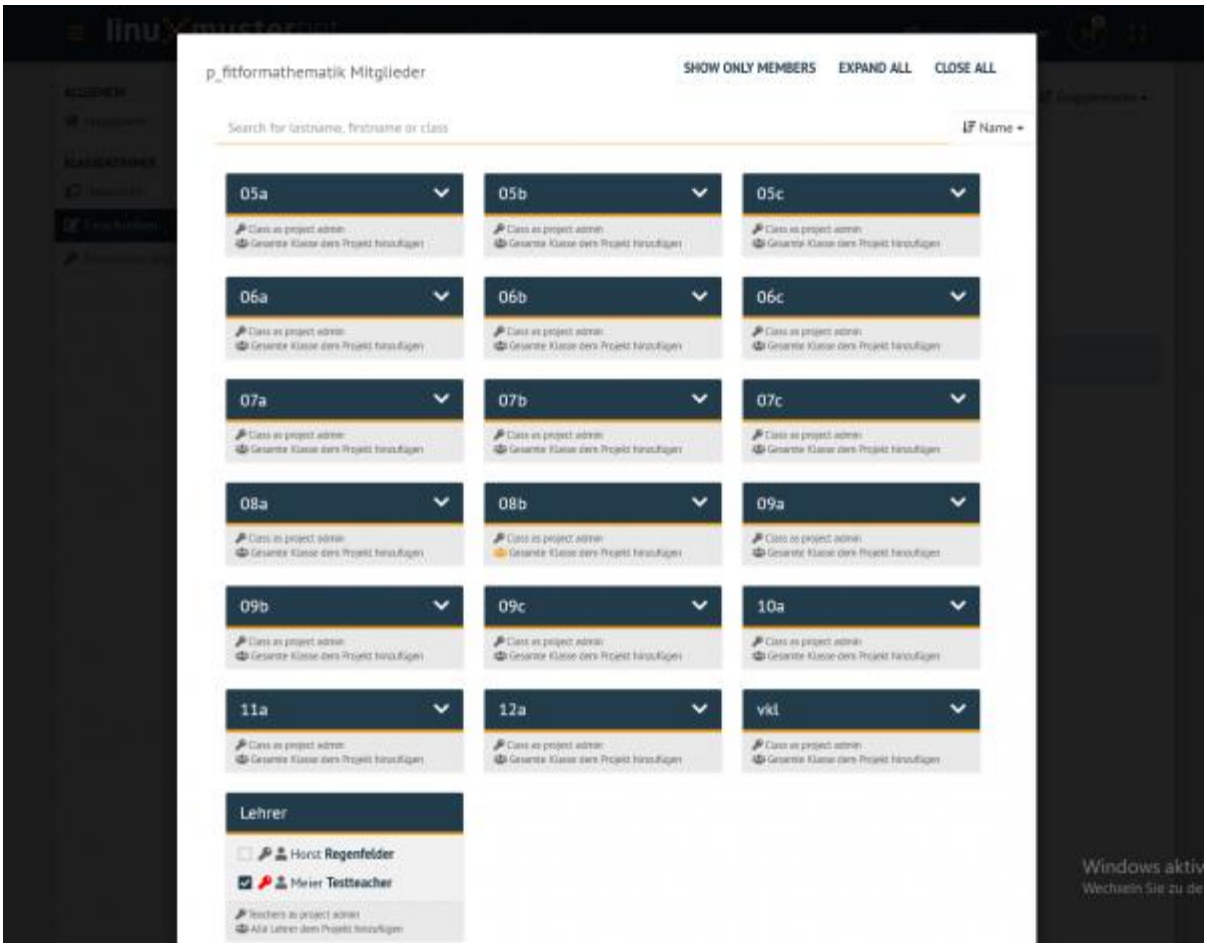
Projektmitglieder verwalten: Durch Anklicken eines bestimmten Projektes, werden weitere Informationen angezeigt, wie etwa die dazugehörigen Mitglieder und Administratoren: Über die Funktion `Beitretbar` kann die Beitrittmöglichkeit und über die Funktion `Nicht anzeigen` die Sichtbarkeit eingestellt werde. Mitglieder können hier über die Mitglieder `bearbeiten`-Funktion gleichzeitig auch hinzugefügt oder entfernt werden.

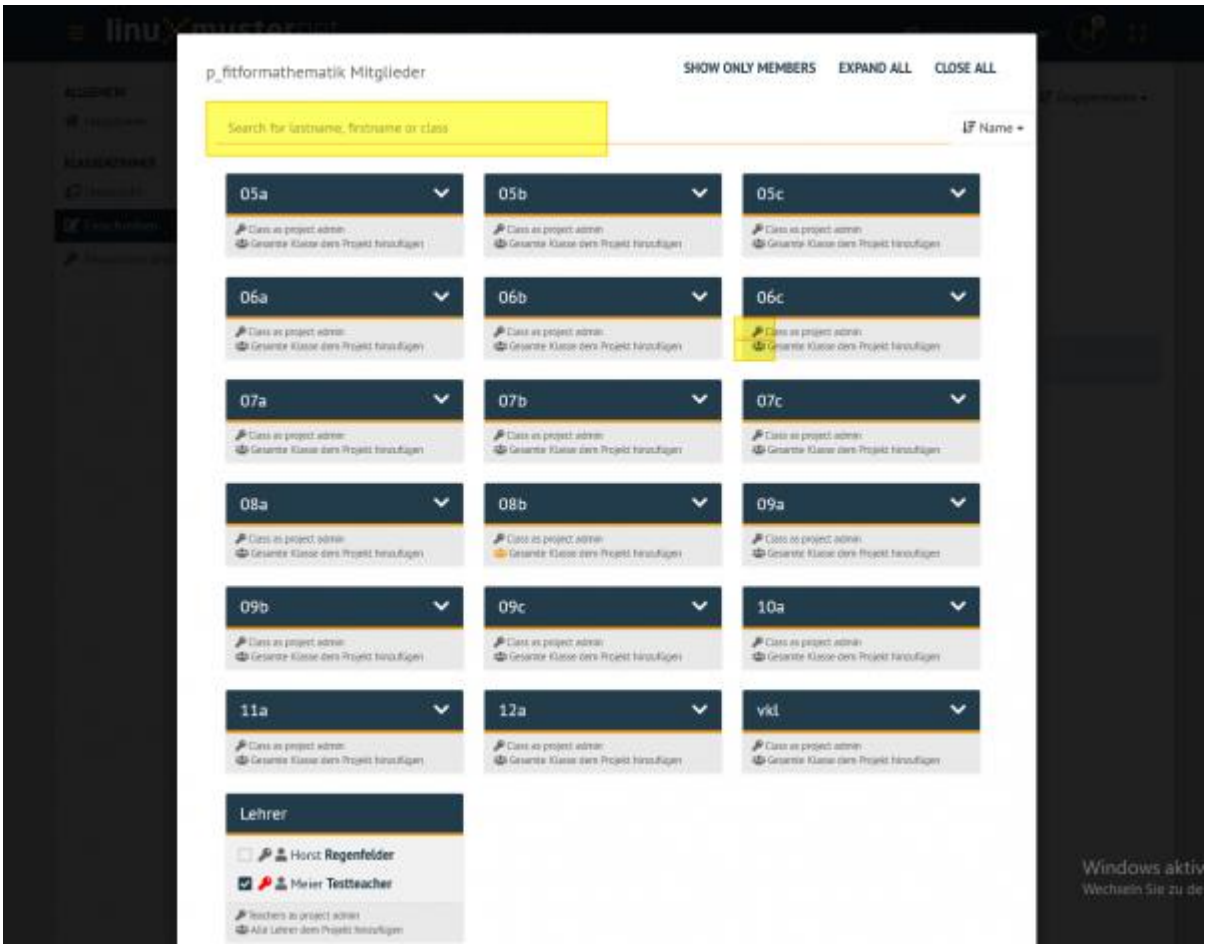
eine Übersicht aller Klassen-Benutzer, die hinzugefügt werden können, erscheint.

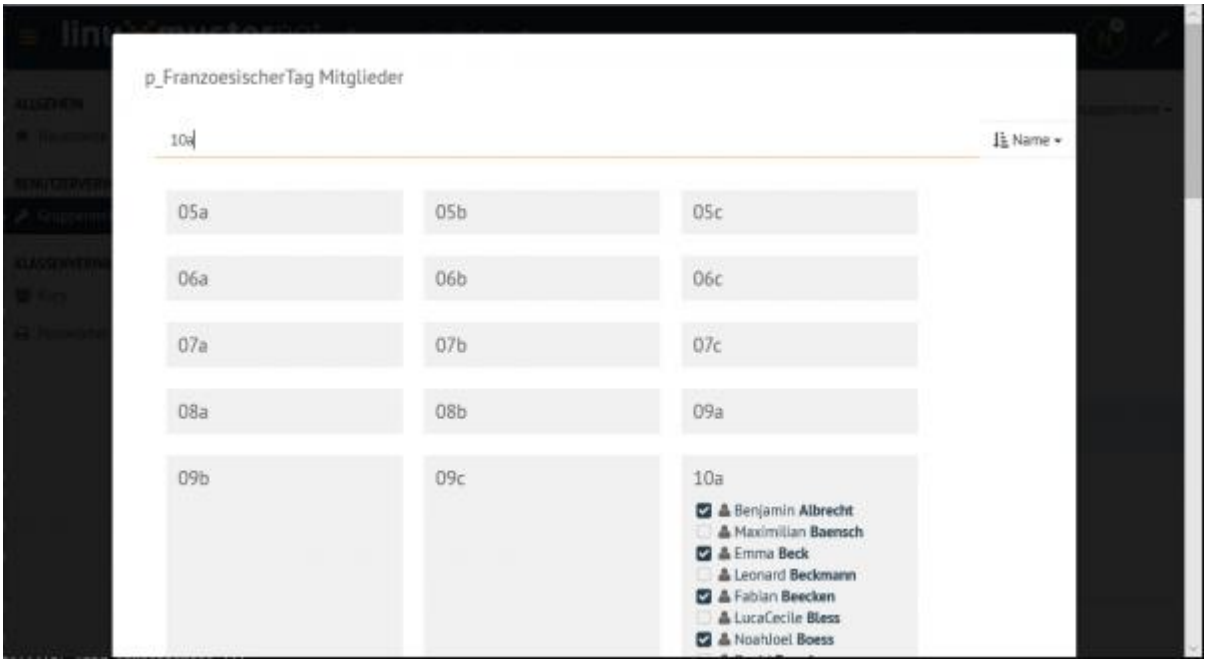
Um bestimmte Benutzer besser finden zu können, gibt es eine Filterfunktion. Ebenso ist es möglich eine ganze Klasse als Projektadmin zu ernennen oder alle Mitglieder einer Klasse auf einmal auszuwählen. Dafür einfach das Symbol links neben „Class as project admin“ oder das Symbol links neben „Gesamte Klasse dem Projekt hinzufügen“ unter derjenigen Klasse klicken:

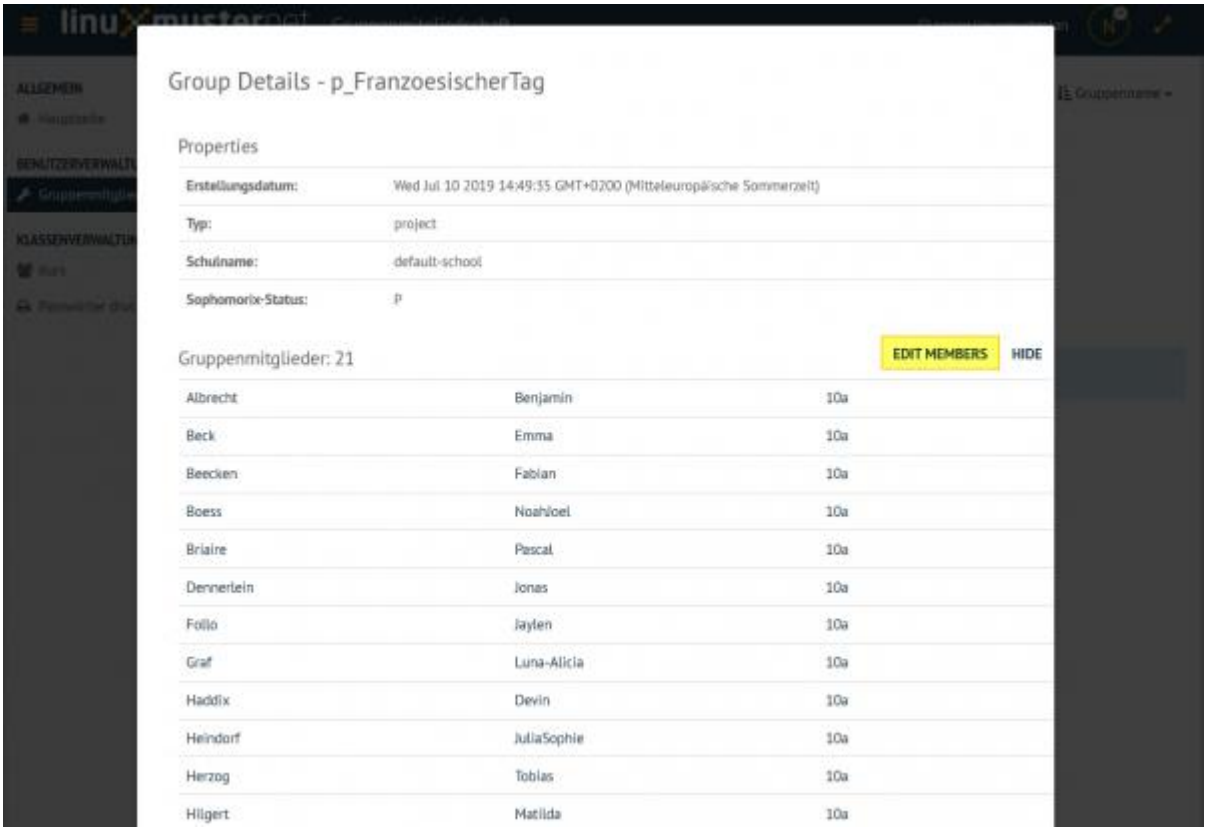
Haben Sie alle Projektschüler aus- oder abgewählt, unten über Speichern die Auswahl übernehmen.


Gruppendetails - p_fitformathematik
Eigenschaften
Erstellungsdatum:
16 Oct 2019 - 12:26:30
Typ:
project
Schulname:
default-school
Sophomorix-Status:
P
Beitretbar:
Nicht anzeigen:
Gruppenmitglieder: 1 Benutzer und 1 Gruppe(n).
MITGLIEDER BEARBEITEN
AUSBLENDEN
Mitglieder
Testteacher Meier
teachers
Gruppen
08b
Gruppenadministratoren: 1 Benutzer und 0 Gruppe(n).
AUSBLENDEN
Administratoren
Testteacher Meier
teachers
Gruppen
Keine Gruppe
PROJEKT LÖSCHEN
SCHLIESSEN


p_fitformathematik Mitglieder
SHOW ONLY MEMBERS
EXPAND ALL
CLOSE ALL
Search for lastname, firstname or class
Name
05a
05b
05c
06a
06b
06c
07a
07b
07c
08a
08b
09a
09b
09c
10a
11a
12a
vkl
Lehrer
Horst Regenfelder
Meier Testteacher


p_fitformathematik Mitglieder
SHOW ONLY MEMBERS
EXPAND ALL
CLOSE ALL
Search for lastname, firstname or class
Name
05a
05b
05c
06a
06b
06c
07a
07b
07c
08a
08b
09a
09b
09c
10a
11a
12a
vkl
Lehrer
Horst Regenfelder
Meier Testteacher


p_FranzoesischerTag Mitglieder
10a
Name
05a
05b
05c
06a
06b
06c
07a
07b
07c
08a
08b
09a
09b
09c
10a
Benjamin Albrecht
Maximilian Baensch
Emma Beck
Leonard Beckmann
Fabian Beecken
LucaCecile Bless
Noahloel Boess



Projekt löschen: klicken Sie das jeweilige Projekt an und wählen unten links Projekt löschen und bestätigen mit Löschen.

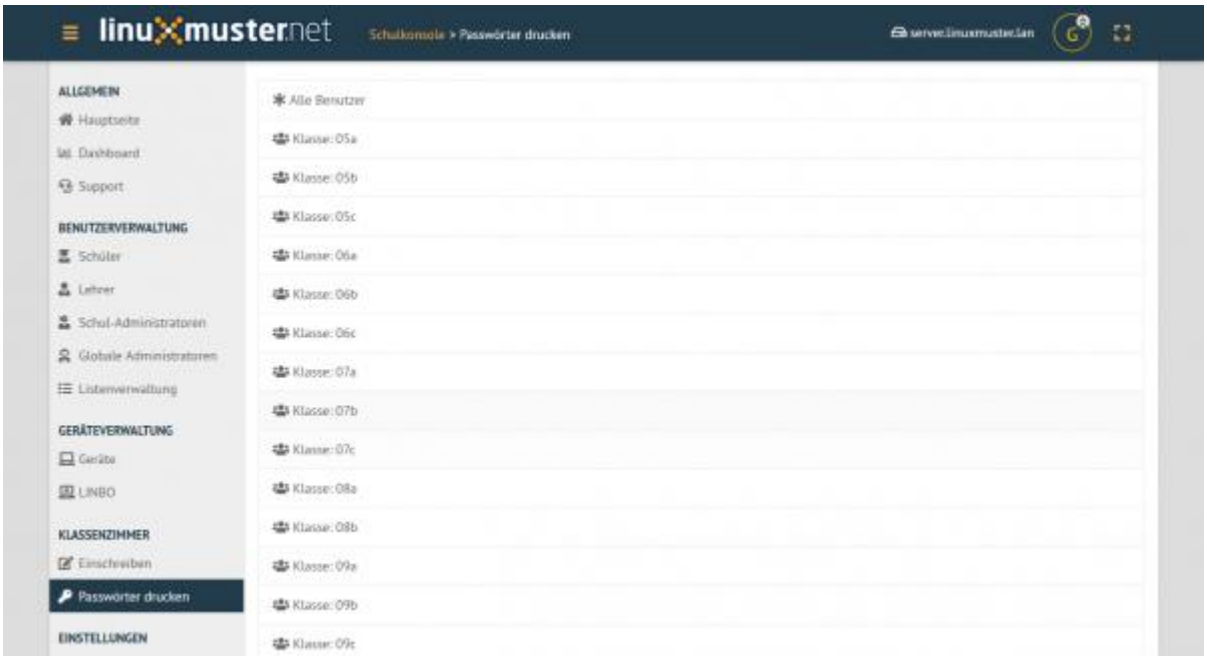
Projektansicht: Für eine übersichtlichere Ansicht, gibt es die Möglichkeit, über den Objektfilter die Objektekategorie auszuwählen, welche angezeigt werden soll. Daneben können Sie die Sortierweise auf Gruppenname oder Mitgliedschaft anwenden (bei nochmaligem Auswählen der selben Kategorie ändert sich die Auflistungsrichtung).

Passwörter drucken

Hier gibt es die Möglichkeit, eine übersichtliche Liste von Benutzer- & Passwortinformationen per PDF oder CSV-Format ausdrucken zu lassen.

Dies 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.



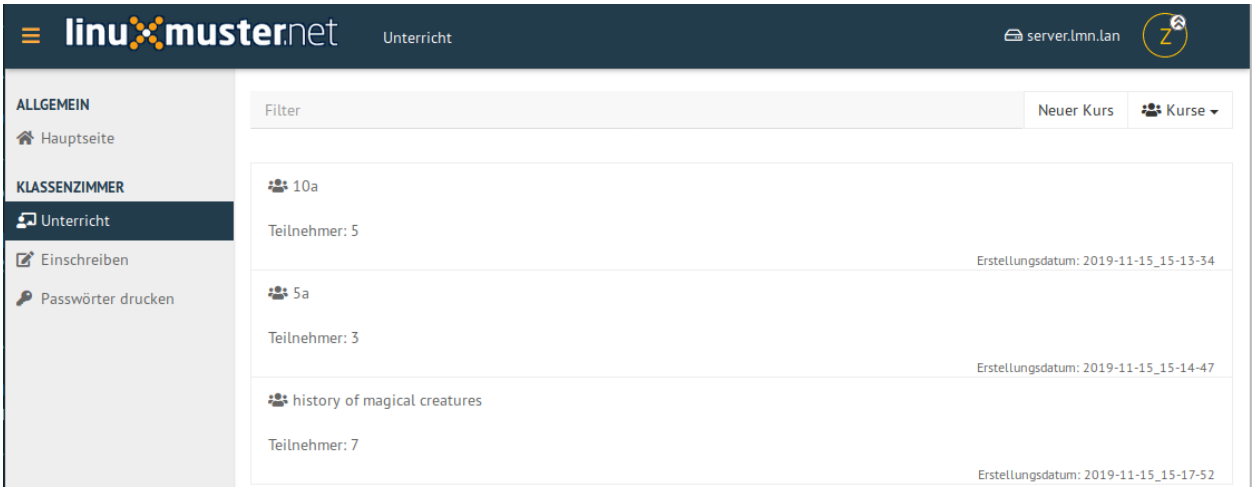
Zugangsdatenliste **10a** 29. April 2019

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	———	———	———

4.27 Prüfungs-/Klassenarbeitsmodus, austeilen und einsammeln

In einem Kurs 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/Unterricht` den angelegten Kurs.

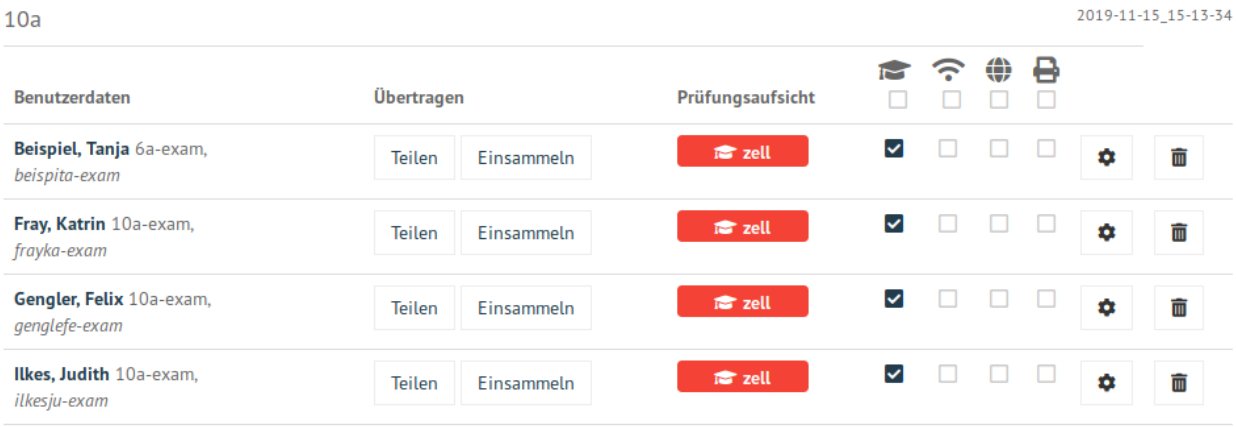


Die Liste mit Schülern des Kurses wird angezeigt. Der Prüfungsmodus wird aktiviert durch Anklicken in der ersten Spalte.

Änderungen werden gelb hinterlegt bis sie mit *SPEICHERN & ÜBERNEHMEN* übernommen werden.

4.27.1 Prüfungsmodus = Klassenarbeitsmodus

Während 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.



Die Prüfungsaufsicht zu diesem Konto übernimmt der Lehrer. Der Prüfungsmodus bleibt so lange erhalten, bis der Lehrer (oder auch ein anderer Lehrer) den Haken bei dem Schülerkonto entfernt.

Der Schüler meldet sich am Computer mit seinem Examenskonto und seinem Passwort an. Dann hat er ein leeres Profil und keine Daten im Home-Laufwerk (`Home_auf_Server` bzw. `H:\\`). Der Internetzugang, der WLAN-Zugang und der Druckerzugriff sind standardmäßig zunächst deaktiviert.

fixme
Internetsperrung funktioniert momentan nicht mit der Firewall OPNsense®.

4.27.2 Austeilen und Einsammeln

Im Home-Laufwerk aller Benutzer (`Home_auf_Server` bzw. *H:*\) gibt es einen Ordner für den Transfer `transfer`. Über diesen Ordner wird ausgeteilt und eingesammelt. Folgende Anleitung funktioniert mit und ohne Prüfungssituation.

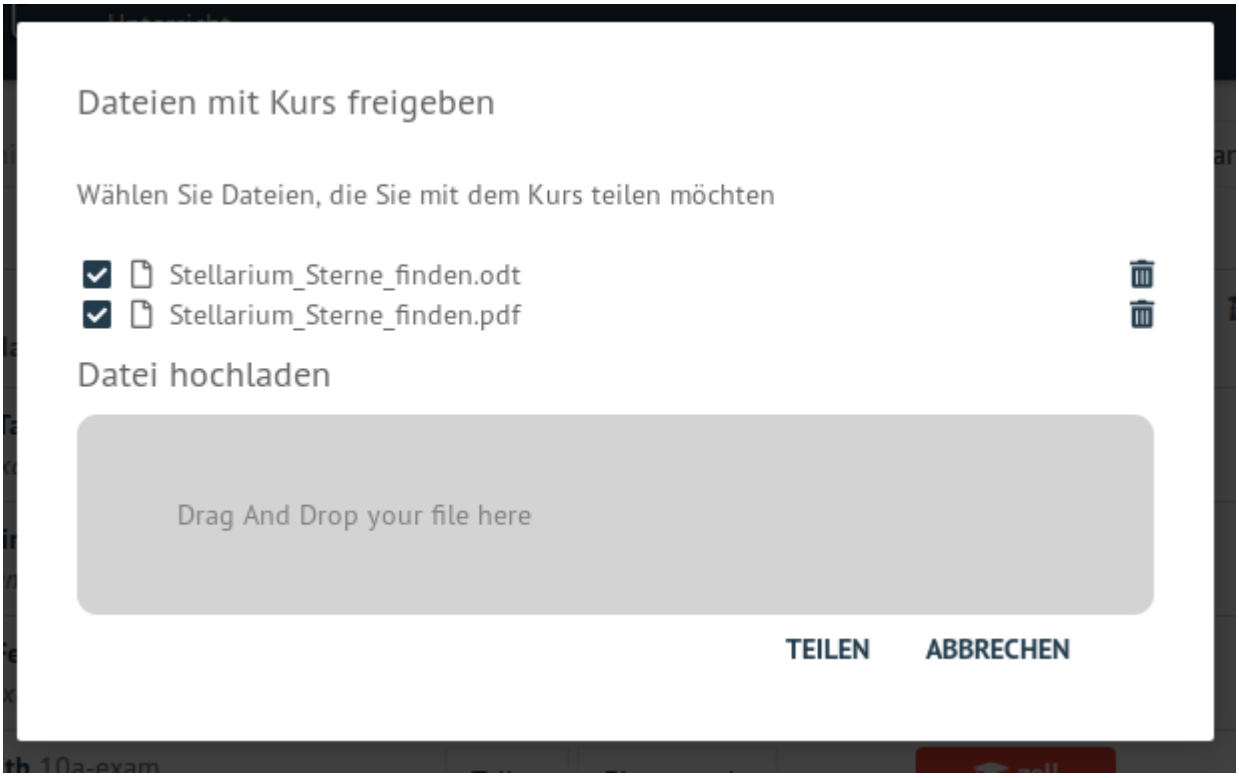
Es gibt zwei Arten Daten an Schüler im aktuellen Kurs auszuteilen. Zum einen kann man Ordner und Dateien im Ordner `transfer` ablegen. Zum anderen kann man im folgenden Dialog per Drag and Drop *einzelne* Dateien hochladen. Klickt man nun bei einzelnen Schülern oder unten auf der Seite für alle Schüler des Kurses auf `Teilen`, kann man im folgenden Dialog neben dem Hochladen auch die zum Teilen gewünschten Daten auswählen und das Austeilen anstoßen.

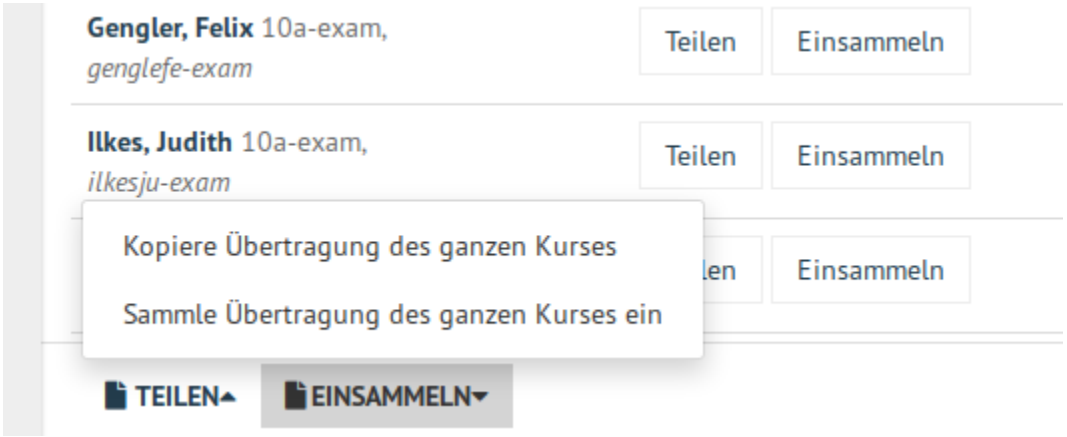
Die ausgeteilten Daten landen nun als Kopien im Ordner `transfer\Lehrername-Kursname` der entsprechenden Schüler.

Die Schüler speichern ihre Daten ebenso im Ordner `transfer\Lehrername-Kursname`.

Der Lehrer hat nun während dieser Phase die Möglichkeit die Daten einzusammeln. Dabei gibt es die Variante, die Daten zu kopieren oder einzusammeln (und damit auf Benutzerseite zu löschen). Die eingesammelten Daten findet man im Ordner `transfer\collected\Zeitstempel-Kursname`.

Das Beenden des Prüfungsmodus sammelt automatisch die Daten von den Schülern ein, verschiebt die Benutzer zurück auf ihre normalen Benutzernamen und aktiviert die Internet-, WLAN- und Druckzugriffe. Die Änderung muss ebenso durch `SPEICHERN & ÜBERNEHMEN` quittiert werden.

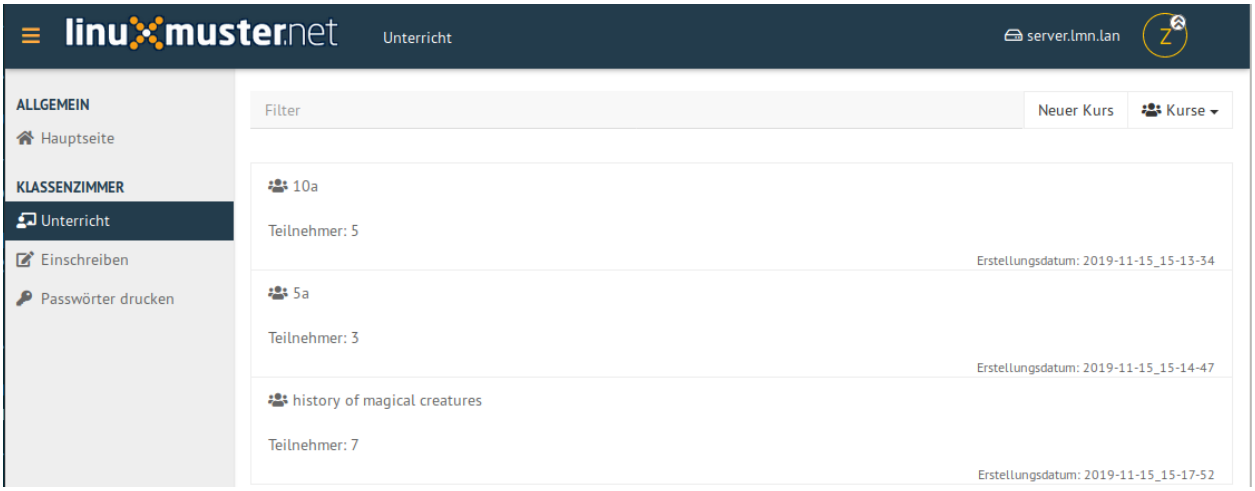

Dateien mit Kurs freigeben
Wählen Sie Dateien, die Sie mit dem Kurs teilen möchten
Stellarium_Sterne_finden.odt
Stellarium_Sterne_finden.pdf
Datei hochladen
Drag And Drop your file here
TEILEN
ABBRECHEN


Gengler, Felix 10a-exam,
genglefe-exam
Teilen
Einsammeln
Ilkes, Judith 10a-exam,
ilkesju-exam
Teilen
Einsammeln
Kopiere Übertragung des ganzen Kurses
Sammle Übertragung des ganzen Kurses ein
Einsammeln
TEILEN
EINSAMMELN

4.28 Zugriff auf WLAN, Internet und Drucker regeln

In einem Kurs kann einzelnen Personen oder dem gesamten Kurs 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/Unterricht` den angelegten Kurs.



Die Liste mit Schülern des Kurses wird angezeigt. Es gibt Auswahlfelder bei den Schülern und oberhalb des ersten Schülers für alle Schüler für

- den Prüfungsmodus (siehe *nächstes Kapitel*)
- WLAN-Zugang
- Internetzugang
- Druckerzugriff

Änderungen werden gelb hinterlegt bis sie mit *SPEICHERN & ÜBERNEHMEN* übernommen werden.

4.29 Anzeigen des eigenen Plattenplatzes

Autor des Abschnitts: @cweikl

Jeder Benutzer kann sich auf der Startseite der *Schulkonsole* über ihren verbrauchten Speicherplatz und die ihnen zugewiesenen Speicherplatzbegrenzungen (Quotas) informieren.

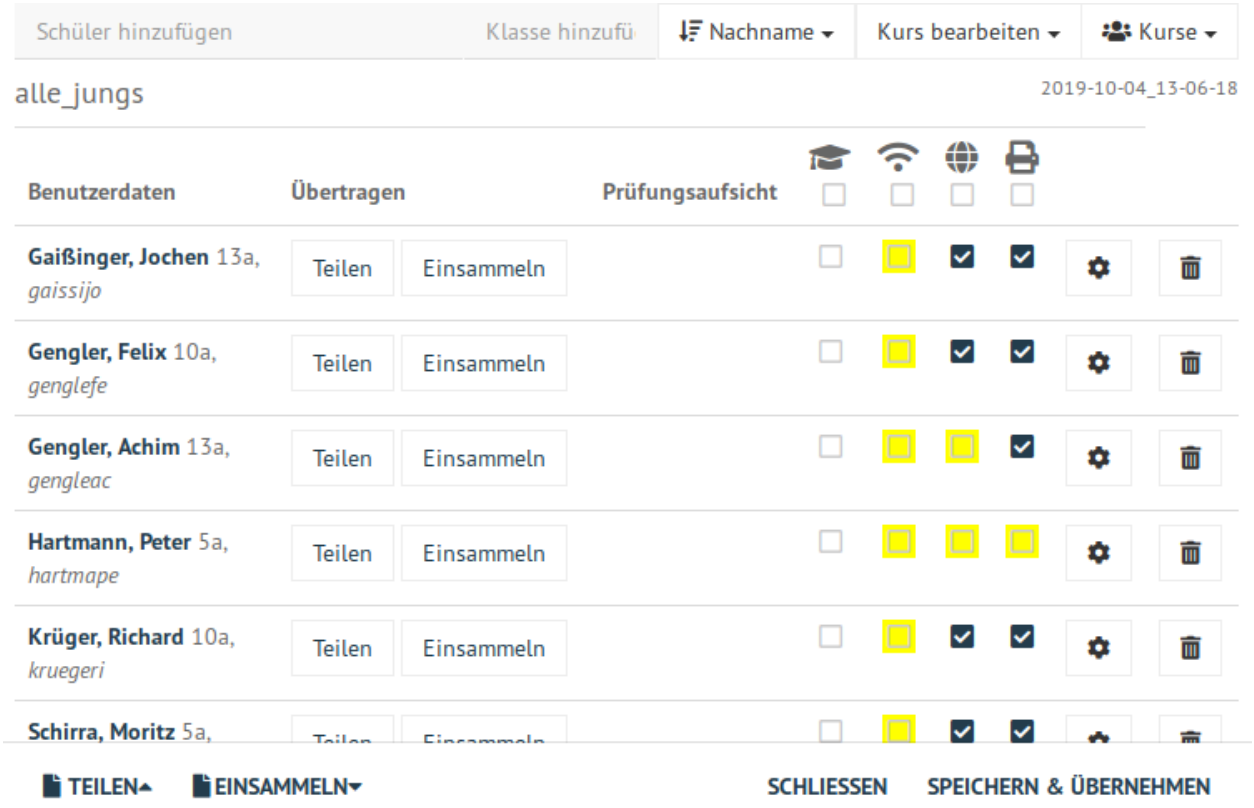
4.29.1 Lehrer: Prüfen der eigenen Quota

Melden Sie sich z.B. als Lehrer in der Schulkonsole an. Es erscheint zunächst die Hauptseite mit den Konto-Informationen, den Quotas und denjenigen Gruppen, denen Sie zugeordnet sind.

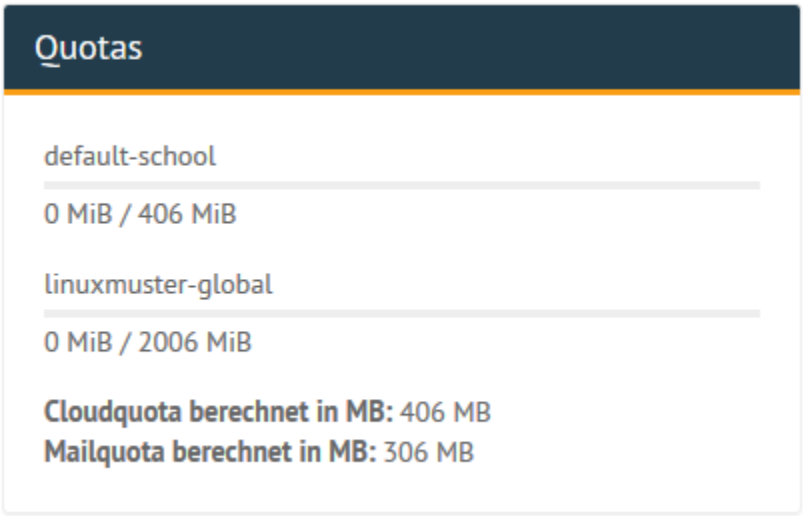
Es sind verschiedene Quotas voneinander abzugrenzen:

Wie in obiger Abbildung dargestellt, sind folgende Quotas 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


Schüler hinzufügen
Klasse hinzufü
Nachname
Kurs bearbeiten
Kurse
alle_jungs
2019-10-04_13-06-18
Benutzerdaten
Übertragen
Prüfungsaufsicht
Gaißinger, Jochen 13a, gaissijo
Gengler, Felix 10a, genglefe
Gengler, Achim 13a, gengleac
Hartmann, Peter 5a, hartmape
Krüger, Richard 10a, kruegeri
Schirra, Moritz 5a,
Teilen
Einsammeln
TEILEN
EINSAMMELN
SCHLIESSEN
SPEICHERN & ÜBERNEHMEN


linuxmuster.net
Schulkonsole > Hauptseite
server.linuxmuster.lan
ALLGEMEIN
Hauptseite
KLASSENZIMMER
Unterricht
Einschreiben
Passwörter drucken
Willkommen zu Linuxmuster.net 7!
Hallo Vorname1 Muster4,
verwenden Sie die Seitenleiste, um in den Einstellungen zu navigieren. Sie könnten damit beginnen, sich mit Hilfe des Einschreiben-Moduls in Ihre Klassen einzutragen.
Konto Informationen
Name: Vorname1, Muster4
E-Mail: mule4@linuxmuster.lan
Schule: default-school
Rolle: teachers
Passwort ändern
Quotas
default-school
0 MiB / 406 MiB
linuxmuster-global
0 MiB / 2006 MiB
Cloudquota berechnet in MB: 406 MB
Mailquota berechnet in MB: 306 MB
Gruppen
teachers
Lehrer



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.

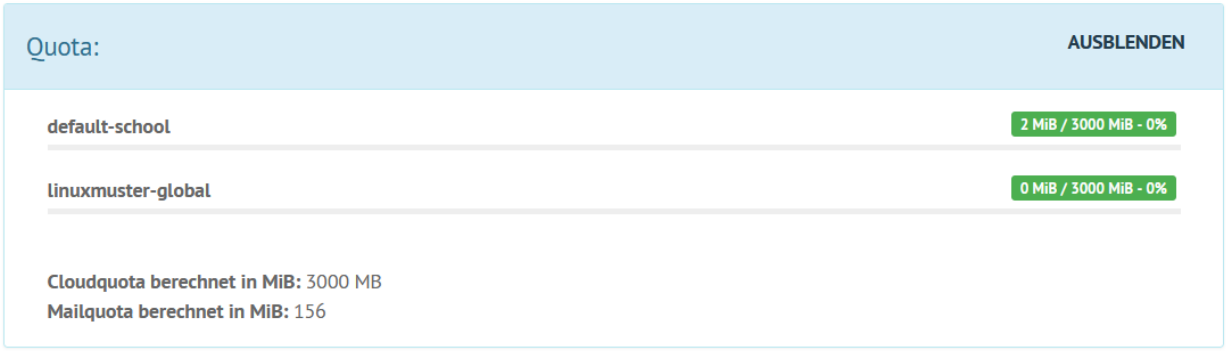
4. **Mailquota**: Zeigt den verfügbaren Plattenplatz zur Ablage von E-Mails an.

Beachte auch, dass die gesetzte Quota immer für eine ganze Festplattenpartition auf dem Linux-Server gilt, d.h. in den meisten Fällen zählen auch Dateien auf den Tauschverzeichnissen zum verbrauchten Speicherplatz.

Sollte der Netzwerkbetreuer dir eine neue Quota eingerichtet haben, so erkennst du dies in deiner Übersicht nach der Anmeldung wie in nachstehender Abbildung dargestellt:

4.29.2 Lehrer: Prüfen der Schüler-Quota

Um in der unterrichteten Klasse zu prüfen, welche Schülerinnen und Schüler ihren zugewiesenen Speicherplatz ausgeschöpft haben, rufe in der Schulkonsole „Unterricht“ auf. Wähle eine Klasse oder Kurs aus. Klicke auf das Zahnrad-Symbol in der Zeile eines Schülers und wähle „Benutzerinformation“. Ganz unten wird die Quota des Schülers angezeigt:



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 18.04.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:

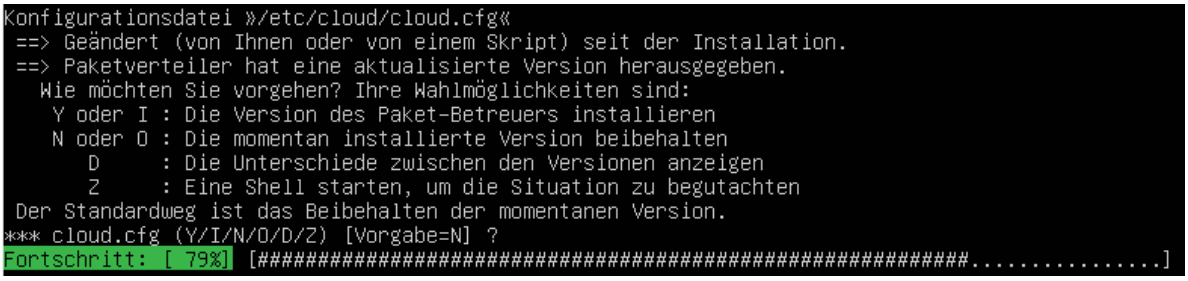
1. Logge Dich als Benutzer root auf einer Serverkonsole ein.
2. Aktualisiere die Paketlisten:

```
# apt update
```

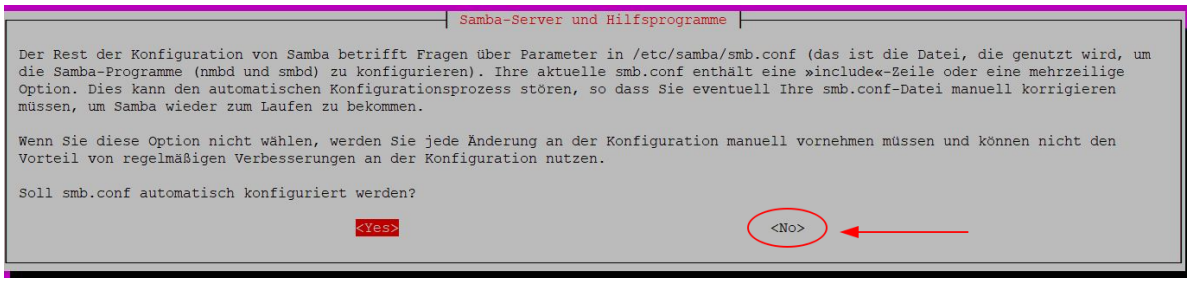
3. Installiere nun Aktualisierungen und weitere Software-Pakete über das Internet:

```
# apt dist-upgrade
```

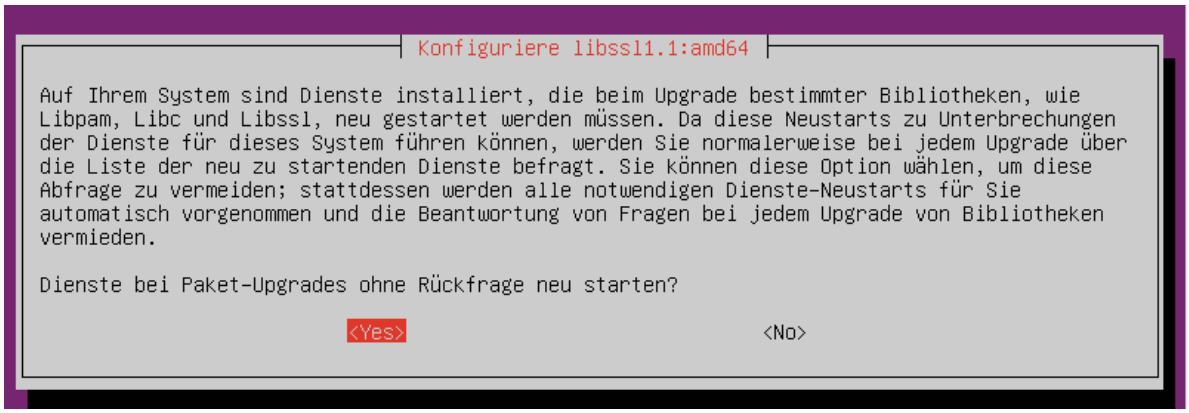
4. Es wird aufgelistet, welche Pakete aktualisiert werden. Bestätige die Aktualisierung mit der Eingabe von **Y**
5. Während des Aktualisierungsverlaufs fragen manchmal Pakete nach, ob eine neue Konfigurationsdatei installiert werden soll. Gib hier **N** oder **ENTER** für „Beibehalten“ an.



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)



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:



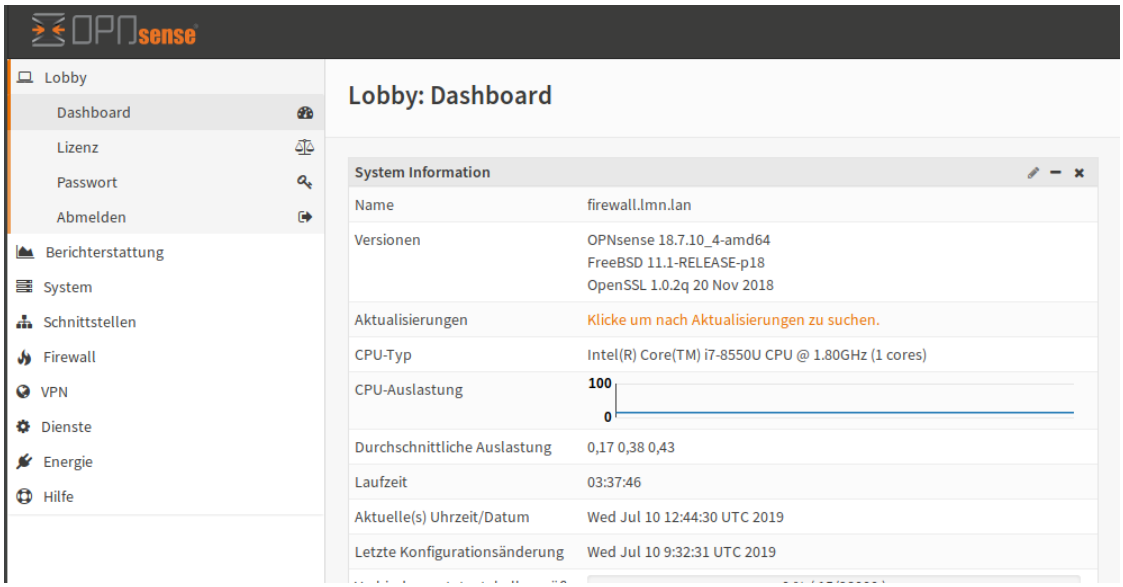
4.30.4 Aktualisierung der Firewall OPNsense®

Um die Firewall OPNsense® zu aktualisieren, beachte bitte Hinweise.

Achtung: Führe Updates bitte regelmäßig manuell durch.

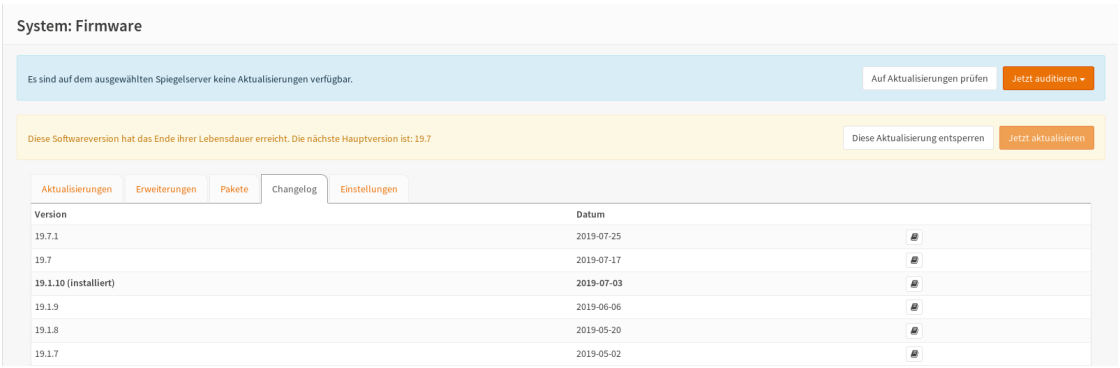
Im Gegensatz zur bisherigen Firewall-Implementierung unter Linuxmuster 6.2, ist in der neuen Linuxmuster 7.x die Firewall relativ unabhängig vom eigentlichen Server zu warten. Dementsprechend werden die Updates über die Weboberfläche der Firewall eingespielt.

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.



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.

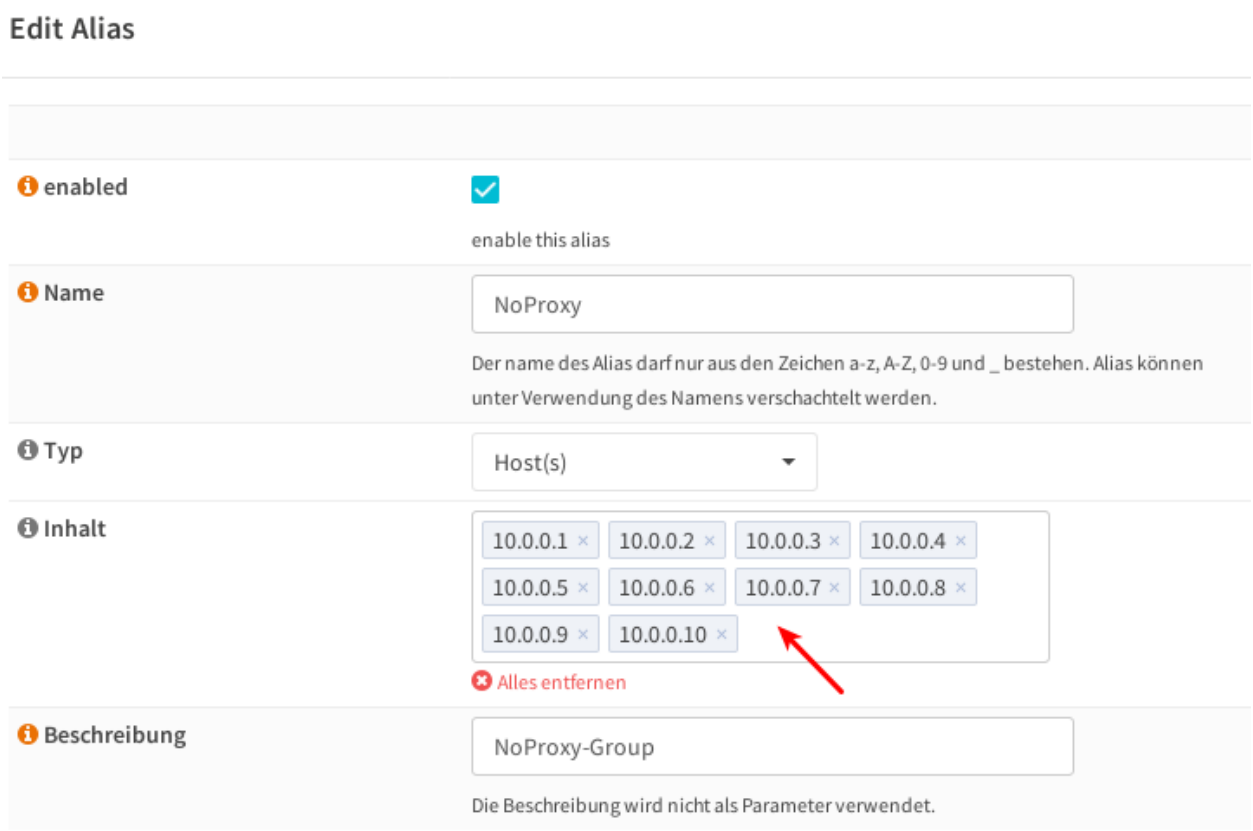
linuxmuster.net verwendet hier standardmäßig das Kerberos-Ticketsystem. Dieses SSO-Verfahren ist auf der Firewall OPNsense® aktiviert und muss auf den Arbeitsplatzrechnern eingerichtet werden.

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.



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 Virtualisierungsumgebung 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.

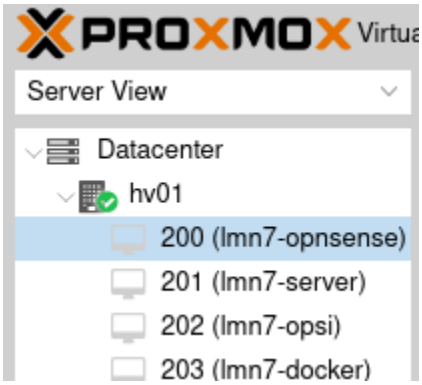
Vorbereiten der Proxmox Festplatten

1. Snapshots der VMs anfertigen

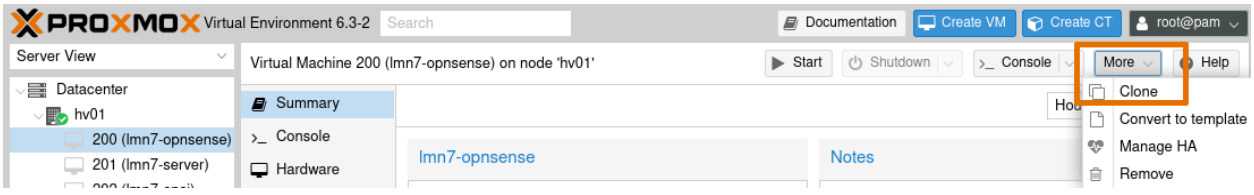
Autor des Abschnitts: @toheine, @MachtDochNix, @cweikl

Am Beispiel der OPNsense®-VM werden die Anpassungen nachstehend erläutert.

Wähle als Erstes die VM aus, die geklont werden soll.

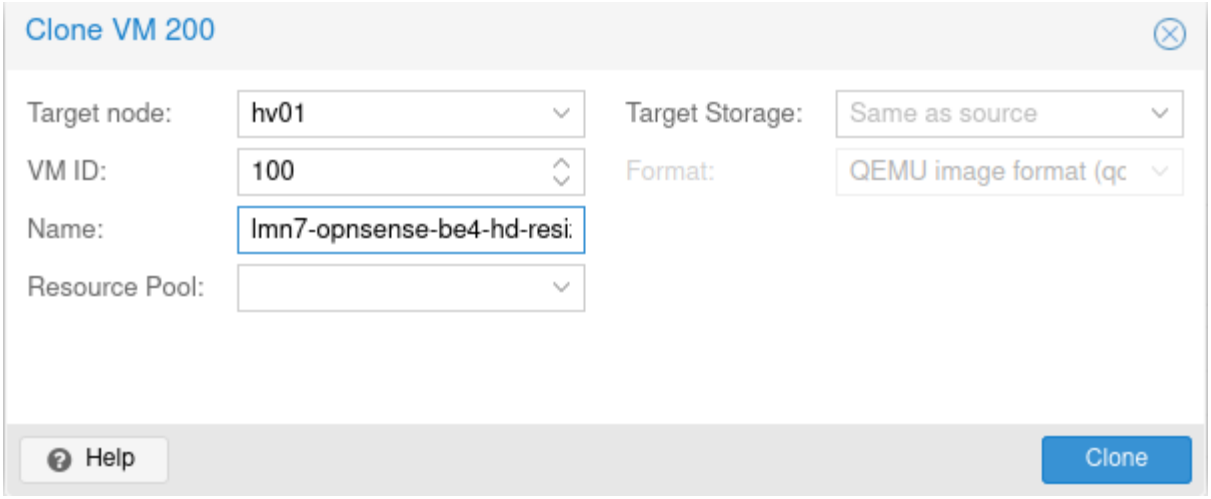


Unter `More` findest Du den Button zum Starten des Klon-Vorganges



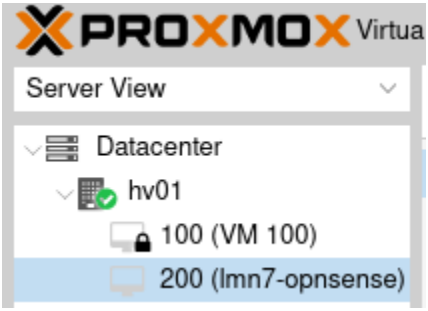
In dem sich öffnen Fenster siehst Du welche VM geklont werden wird und deren neuer ID.

Im Feld *Name* kannst Du einen eigenen angeben, ansonsten wird einer nach dem Muster „Copy of VM . . . “ verwendet.

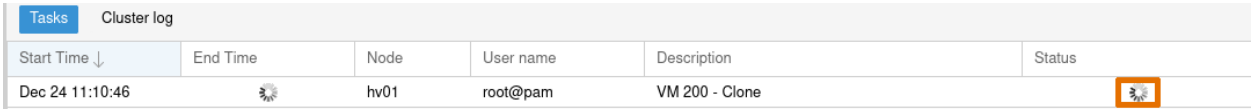


Der Klon-Vorgang wird mit *Clone* gestartet.

Das wird sichtbar daran, dass die VM mit der neuen ID in der linken Übersicht mit einem Schloss erscheint.



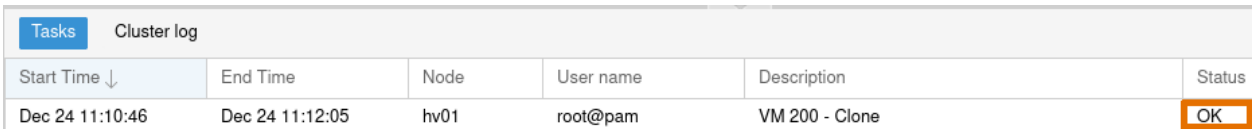
Das Schloss zeigt an, dass das Kopieren der VM gestartet ist. Dieses siehst Du auch in den *Tasks* am unteren Bildschirmrand.

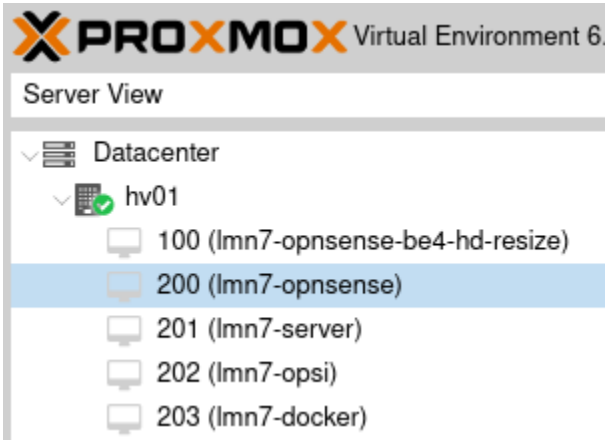


Dort erkennst Du, wann der Vorgang abgeschlossen ist.

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.





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!

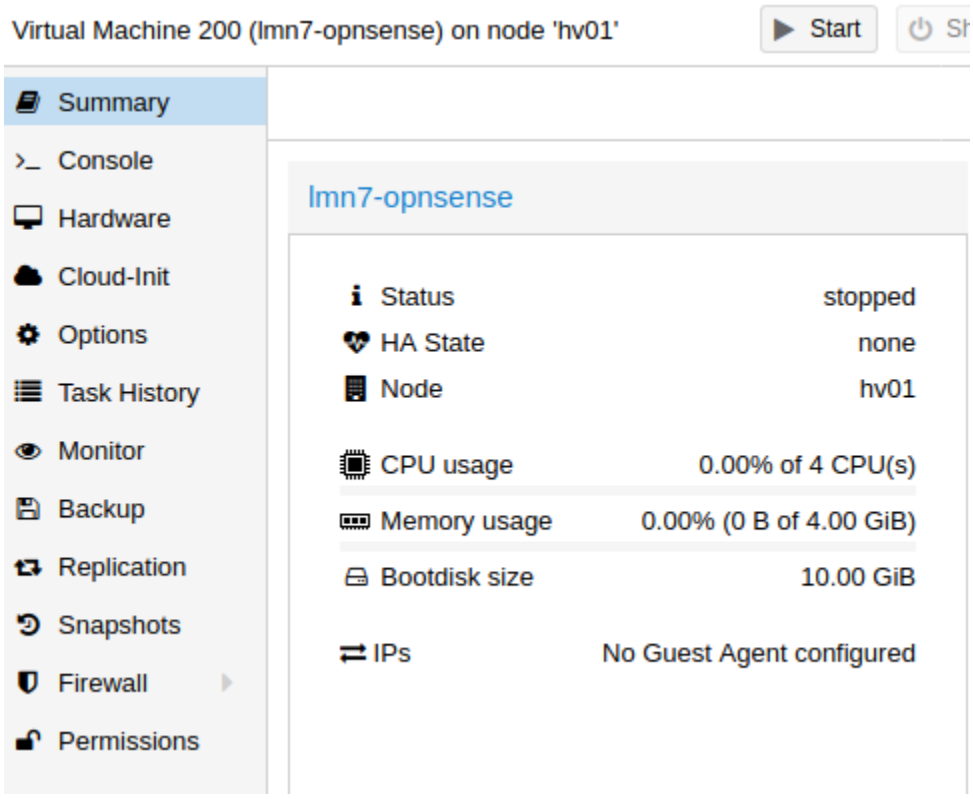
---

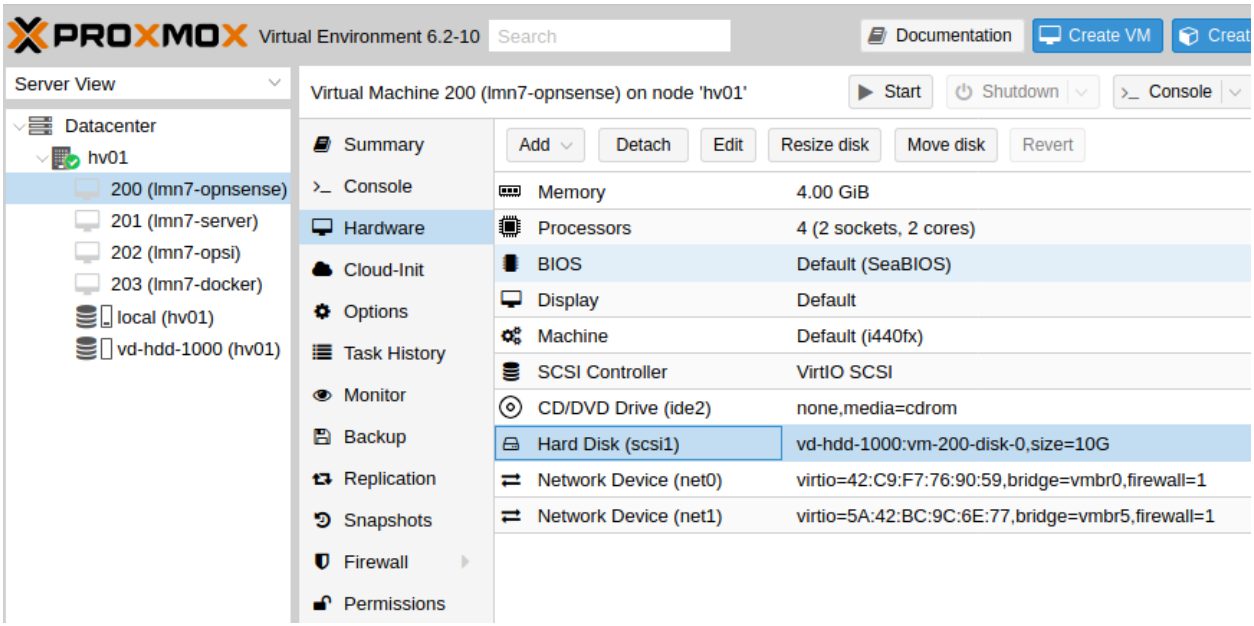
4. Es erscheint ein neues Fenster, in dem Du angeben must, um wieviel GiB Du die Festplatte vergrößern willst.
5. In dem Beispiel sind 10 GByte gegeben, um auf 50 GByte zu kommen, trägst Du nun 40 GByte ein. Danach siehst Du folgenden Eintrag:

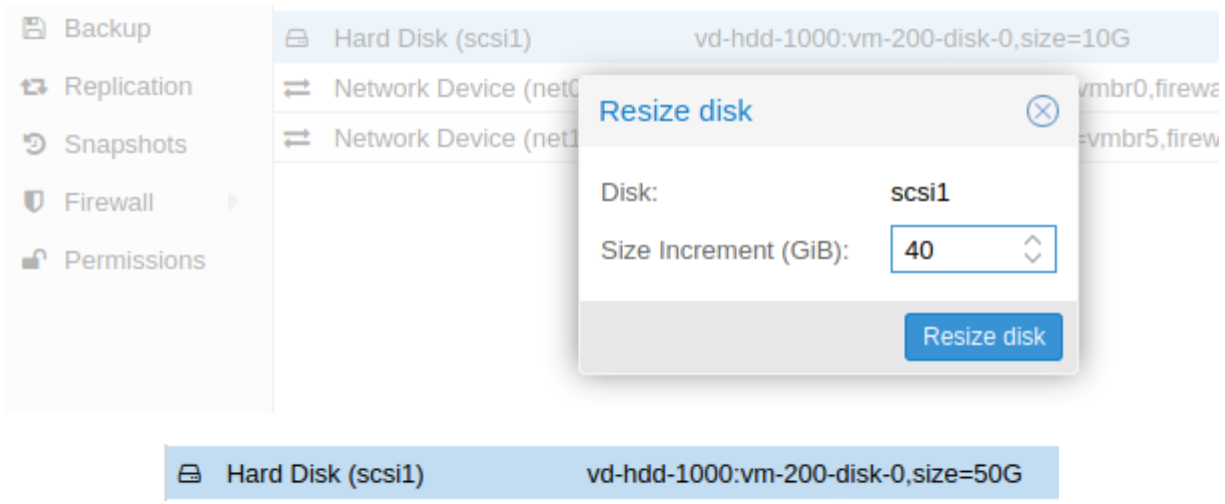
Hinweis: Für die anderen VMs werden die Festplatten in gleicher Weise vergrößert.

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 (lmn7-opnsense) on node 'hv01'
Start
Summary
Console
Hardware
Cloud-Init
Options
Task History
Monitor
Backup
Replication
Snapshots
Firewall
Permissions
lmn7-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

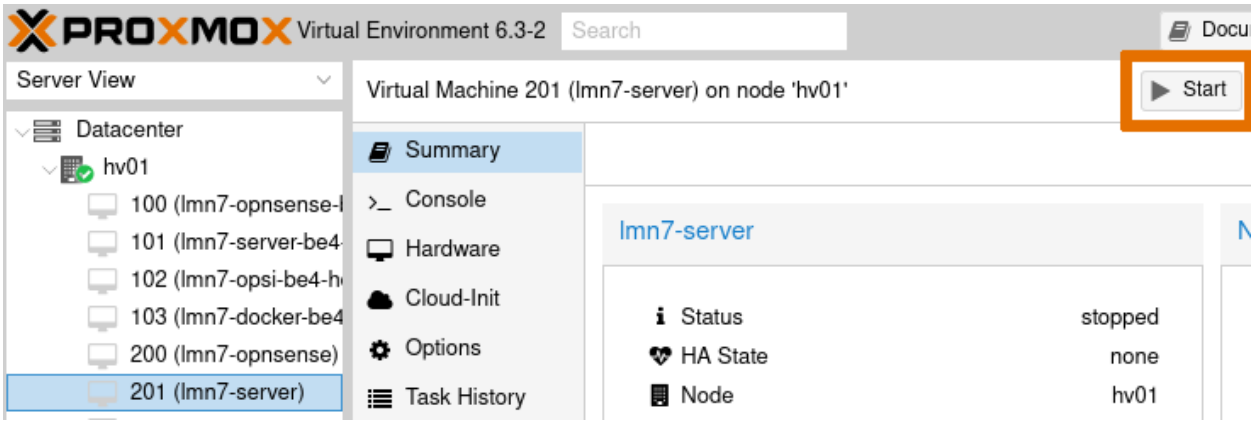

PROXMOX Virtual Environment 6.2-10
Search
Documentation
Create VM
Server View
Datacenter
hv01
200 (lmn7-opnsense)
201 (lmn7-server)
202 (lmn7-opsi)
203 (lmn7-docker)
local (hv01)
vd-hdd-1000 (hv01)
Virtual Machine 200 (lmn7-opnsense) on node 'hv01'
Start
Shutdown
Console
Summary
Console
Hardware
Cloud-Init
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=vmbr0,firewall=1
Network Device (net1) virtio=5A:42:BC:9C:6E:77,bridge=vmbr5,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 ensprechend 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
/dev/mapper/vg_srv-var           9,8G    1,2G  8,1G   13% /var
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 Eingabekonsole 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/Ignoiren/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 vorhanden 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.

```
Partionsnummer (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
Mon 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 5zinhXXOawj1Q2N0AxtZ+i5YDrlu3rI/j85pPILUy1c (ECDSA)
 SSH:   SHA256 r2Ij7n3jlq1hRYSB+dEog/rVs0lwq+U2uyGUYdduU5U (ED25519)
 SSH:   SHA256 uRGfVm13RxPaSR+K0u0RuggDpLWRw9+ErQPRfycdJHQ (RSA)

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

login: root
Password:
```

```
| Forums:       https://forum.opnsense.org/  |         @@@///   \\\@@@
| Lists:        https://lists.opnsense.org/  |        @@@@          @@@@
| Code:         https://github.com/opnsense  |         @@@@@@@@@@@@@@@@
-----------------------------------------------

*** 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 5zinhXXOawj1Q2N0AxtZ+i5YDrlu3rI/j85pPILUy1c (ECDSA)
 SSH:   SHA256 r2Ij7n3jlq1hRYSB+dEog/rVs0lwq+U2uyGUYdduU5U (ED25519)
 SSH:   SHA256 uRGfVm13RxPaSR+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 Festplate 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
OM_PART: da0s1 was automatically resized.
Use `gpart commit da0s1` to save changes or `gpart undo da0s1` to revert them.
0s1 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 Authentification 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 berechtigte Nutzer Zugriff haben. Der Zugriff kann zudem auch auf bestimmte Endgeräte beschränkt werden. Um die Authentifizierungsdaten zu übertragen, wird oftmals das Protokoll EAP (Extensible Authentification 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 berechtigte 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 lmn-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 lmn-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:

```
sophomorix-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 entferns 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. Sophomorix-Befehl übergeben werden:

```
sophomorix-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 dem lmn-Server ist in der Datei `/etc/linuxmuster/allowed_ports` der Radiusport 1812 einzutragen:

```
udp domain,netbios-ns,netbios-dgm,9000:9100,1812
```

Danach ist der lmn-Server neu zu starten.

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 erhälst 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 Netzbereich (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 Sktipt 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 Applicance (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

```
./lmn71-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

- emo/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-Applicance

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 müste 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-/Netzwerkonfiguration 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
- Domänename: 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 datenschutzrechtichen Überlegungen ist ein schulisches Netzwerk in drei Bereiche mit unterschiedlichen Absicherungen und Berechtigungsstufen zur Verarbeitung und Speicherung von personenbezogenen Daten zu unterteilen:

- Verwaltungsnetz (Veraltungsprogramme, 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. Ein 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-Switche, die VLANs verwalten können. Hierzu können Switche beliebiger Hersteller genutzt werden.

Die Konfigurationsschritte für den L3-Switch werden anhand eines `Cisco SG300-300-28` besipielhaft dargstellt. Für die Konfiguration der L2-Switche werden die Schritte anhand eines `Cisco SF200-24` exemplarisch verdeutlicht. Bei dem Einsatz anderer Switche sind die dargestellten Konfigurationsschritte entsprechend anzupassen.

Am Ende des Kapitels findest Du weitere Konfigurationen für andere L3-Switche, 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 Netzsegemente 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

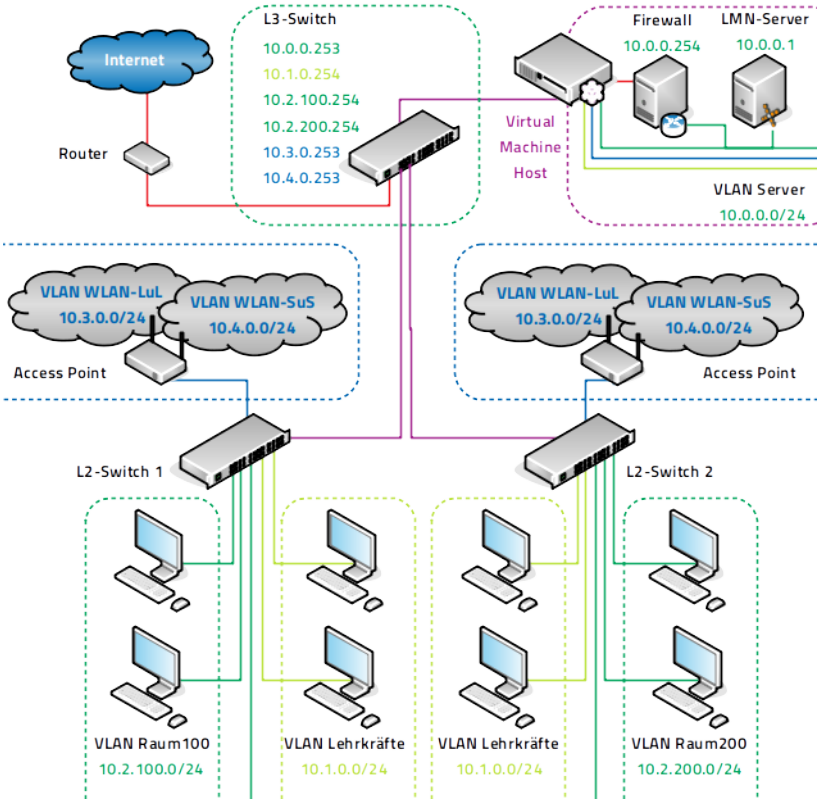
In dieser Dokumentation werden folgende VLAN-IDs und Gateway-IPs verwendet:

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-Switche 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 identiizieren).
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 Brdige 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

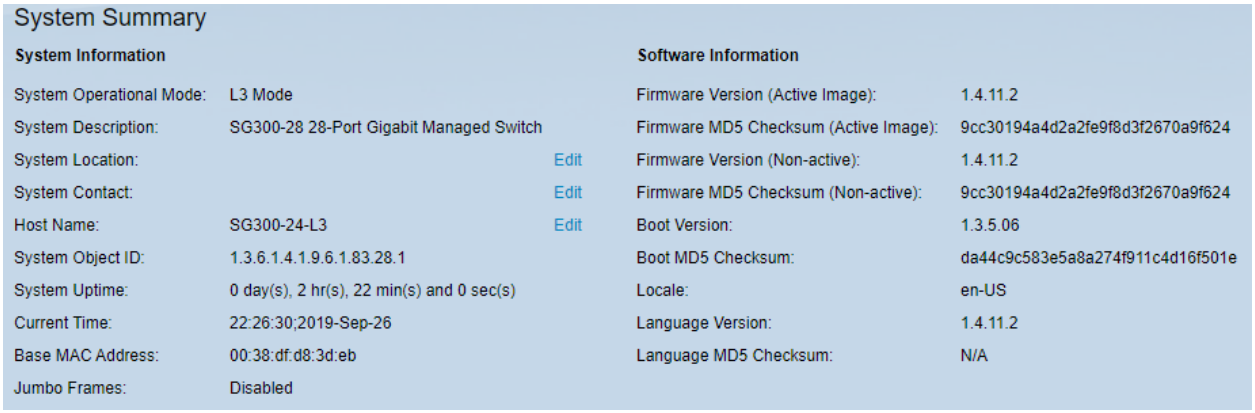
Konfigurationsschritte auf dem Layer-3-Switch:

- 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			

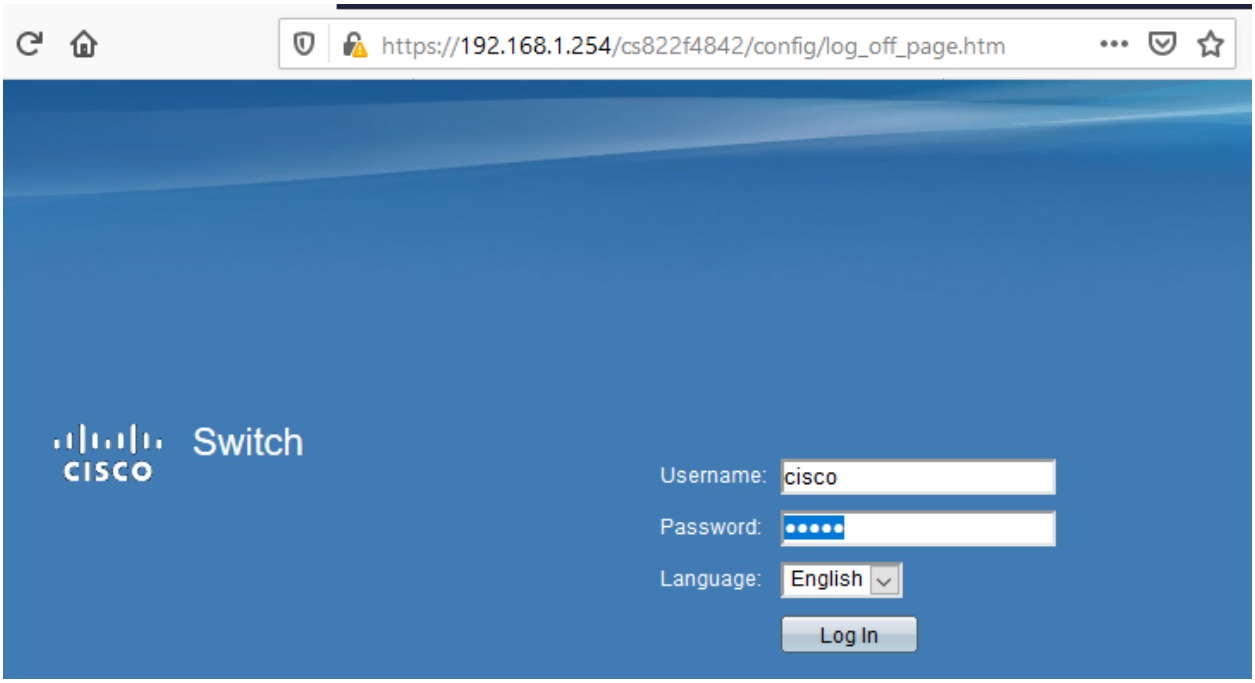
Für den L3-Switch Cisco SG300-28 steht die vorbereitete Konfigurationsdatei zur Verfügung, die die Konfiguration auf dem L3-Switch so einspielt, wie diese in dieser Dokumentation beschrieben wird.

Download

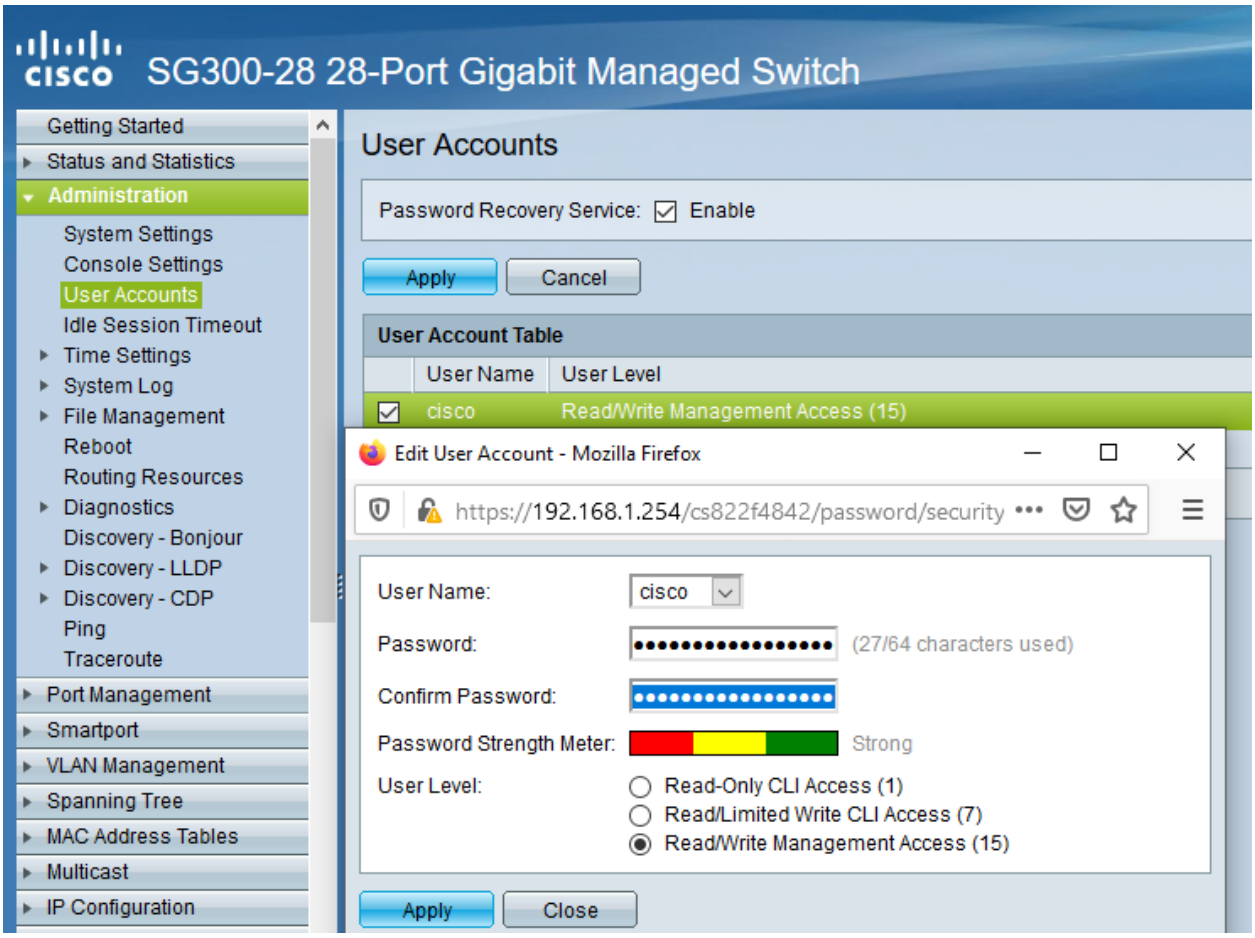
- `Konfiguration für v7.1 mit Server-IP 10.0.0.1/24`.

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.

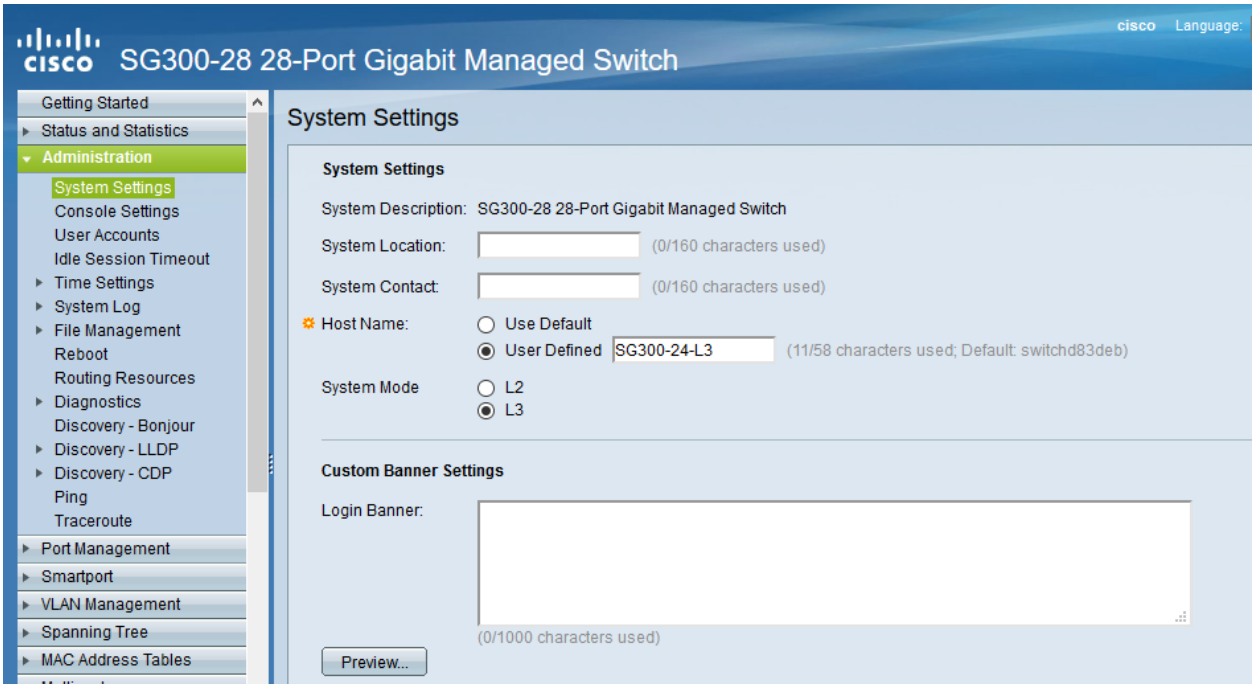


Meldest Du Dich als Benutzer `cisco` mit dem Kennwort `cisco` (Voreinstellungen) an.

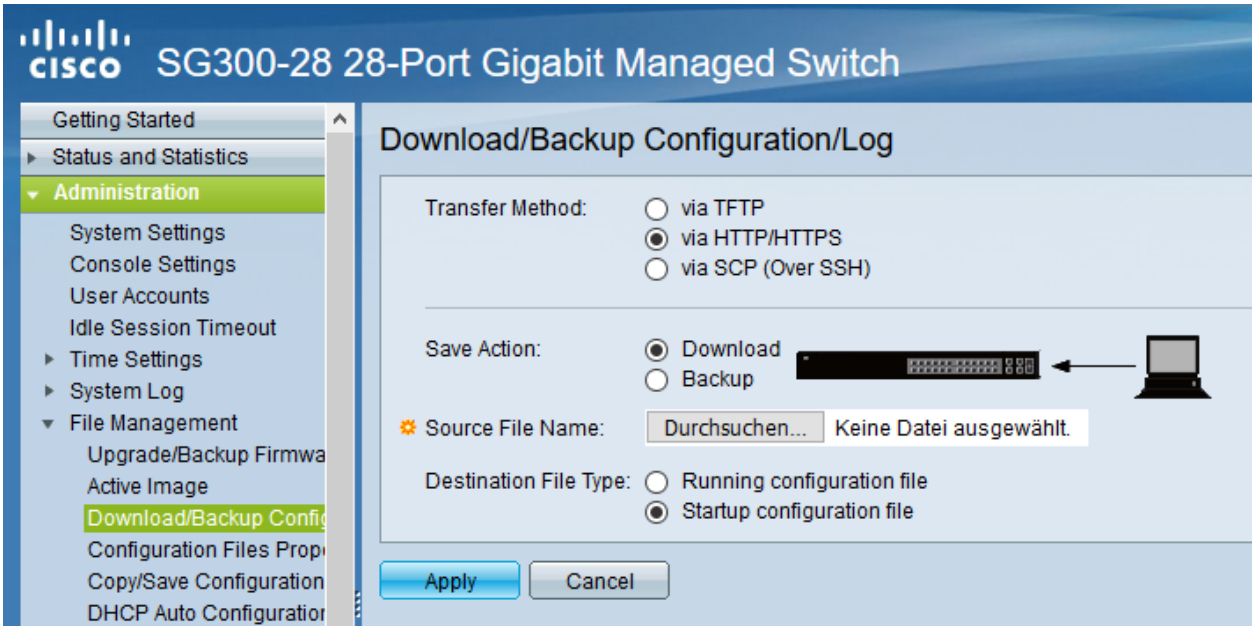


Danach erfolgt der Wechsel in das Menü `Administration --> User Accounts`. Dort ist der betreffende Benut-

zer auszuwählen, mit dem Menüpunkt `Edit` ist das Kennwort des Benutzers neu zu setzen. Die neueren Firmware-Versionen geben eine Kennwort-Komplexität vor.

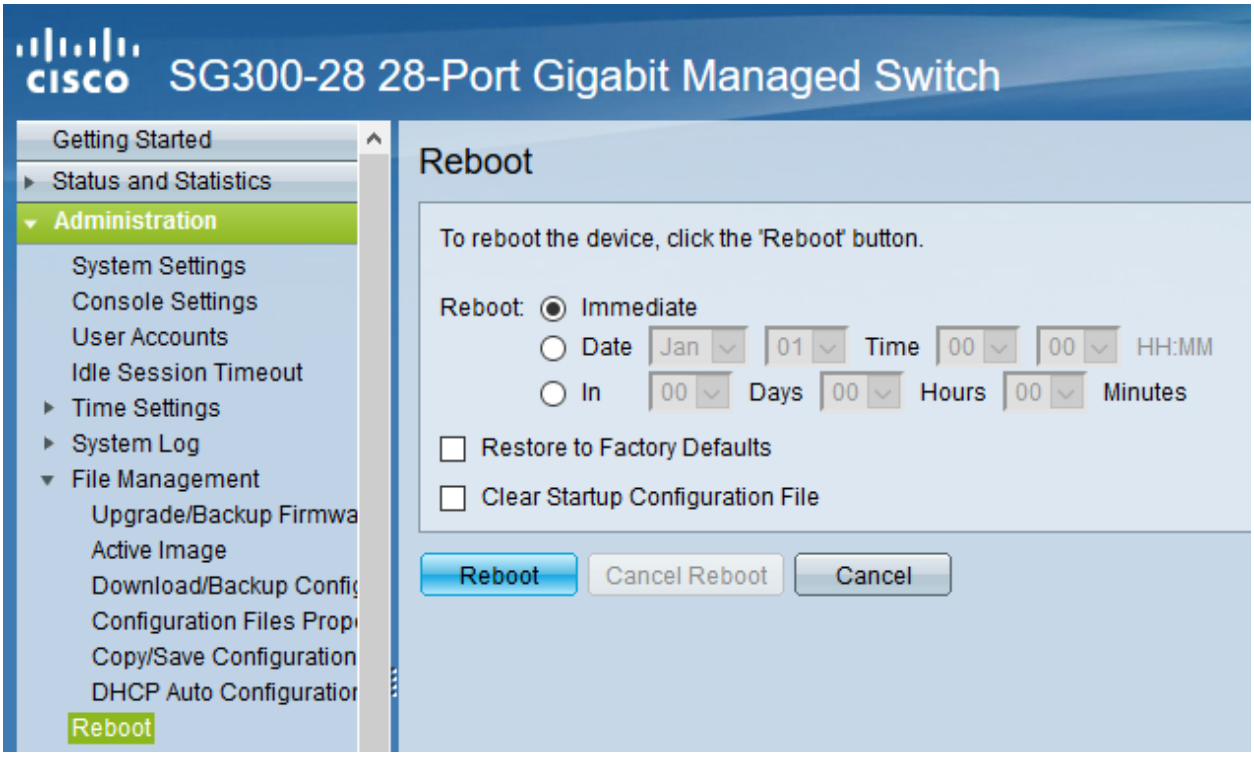


Im Menü `Administration --> System Settings` ist der Name für den Switch zu vergeben und der System-Modus ist auf L3 zu ändern. Die Änderungen sind dann mit `Apply` zu übernehmen.



Dies erfolgt im Menü `Administration --> File Management --> Download/BackupConfig`. Die hochzuladende Datei ist als sog. `Startup configuration file` hochzuladen. Mit `Durchsuchen` ist die heruntergeladende 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 ausgschlossen, 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.

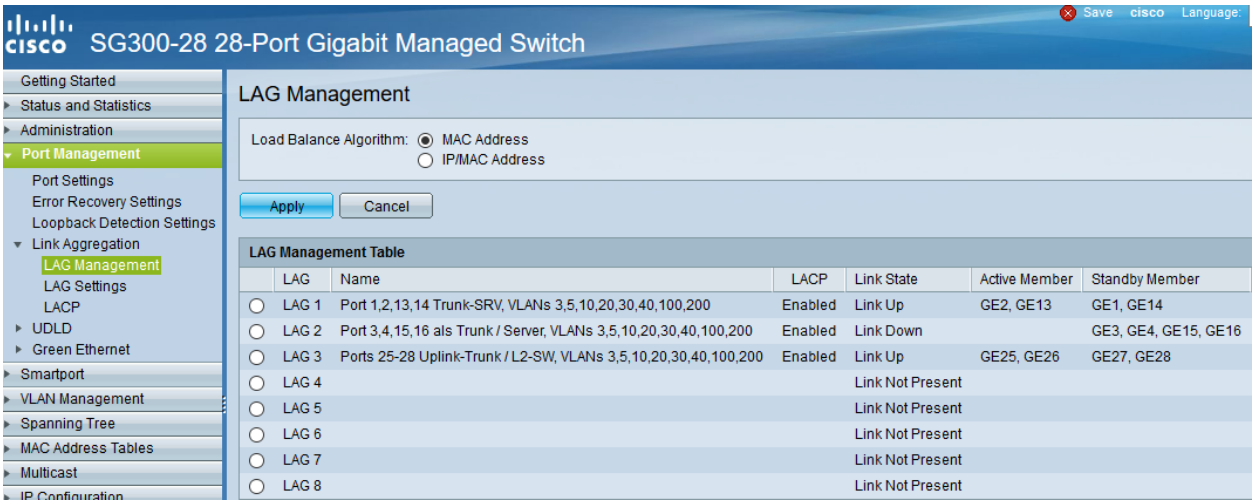
- `ausgeschlossen`: Datenpakete, die mit der VLAN-ID x getaggt sind, werden verworfen.
- `tagged`: Datenpakete, die mit der VLAN-ID x getaggt sind, werden weitergeleitet.
- `untagged`: Von Datenpaketen, die mit der VLAN-ID x getaggt sind, wird die VLAN-ID entfernt und zum Client weitergeleitet. Die meisten Clients können mit getaggten 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.

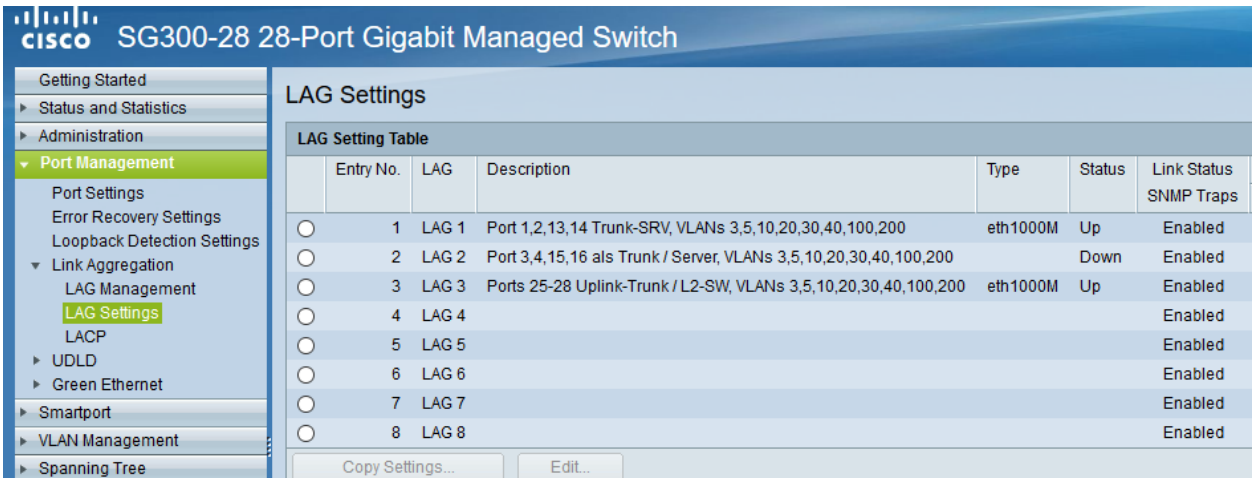
Anwendung auf das Ausgangsbeispiel

Nachstehende Ausführungen, dienen dazu, die eingespielte Konfiguration zu prüfen oder ggf. Anpassungen für abweichend eingesetzte Hadrware 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

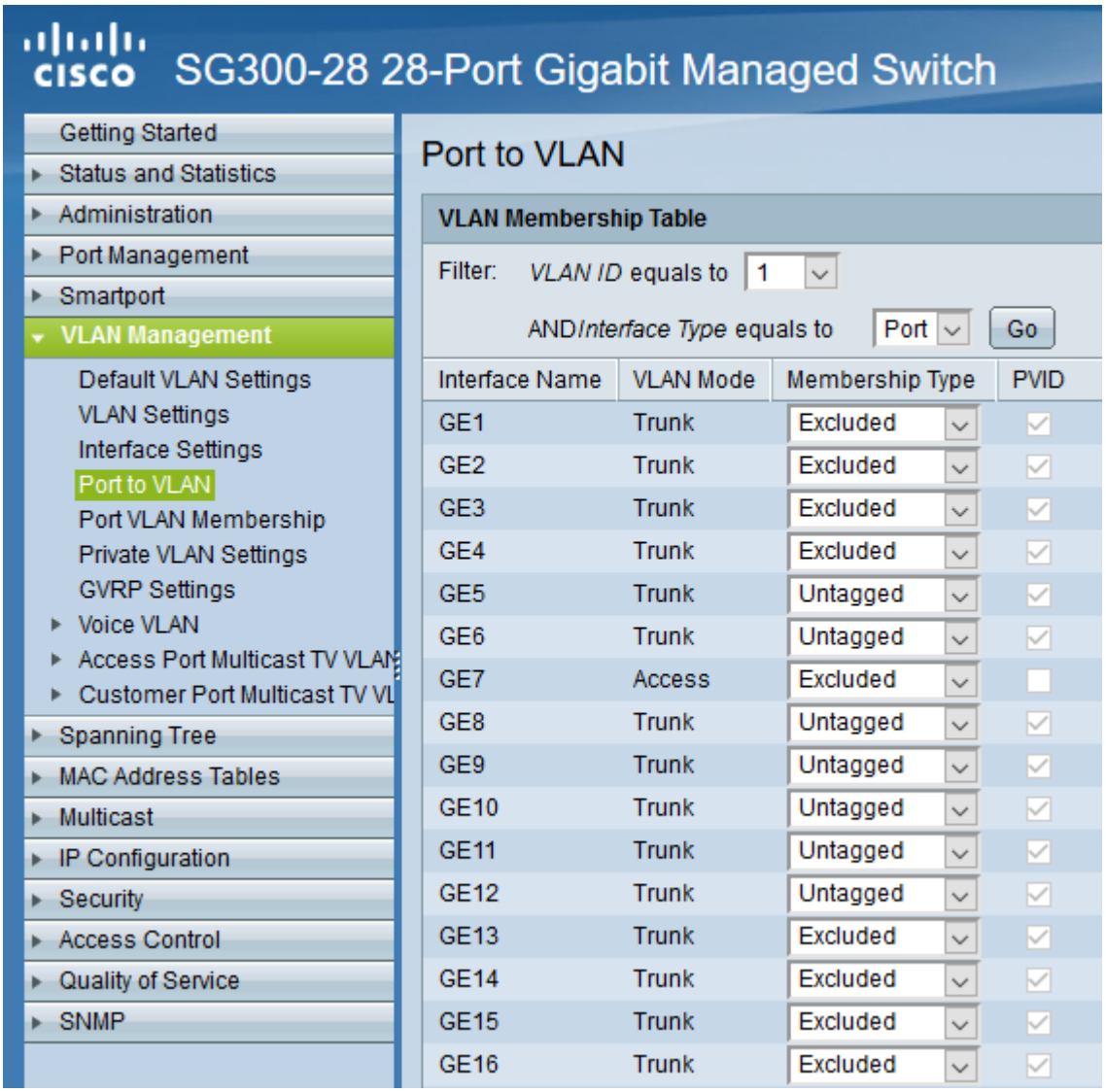


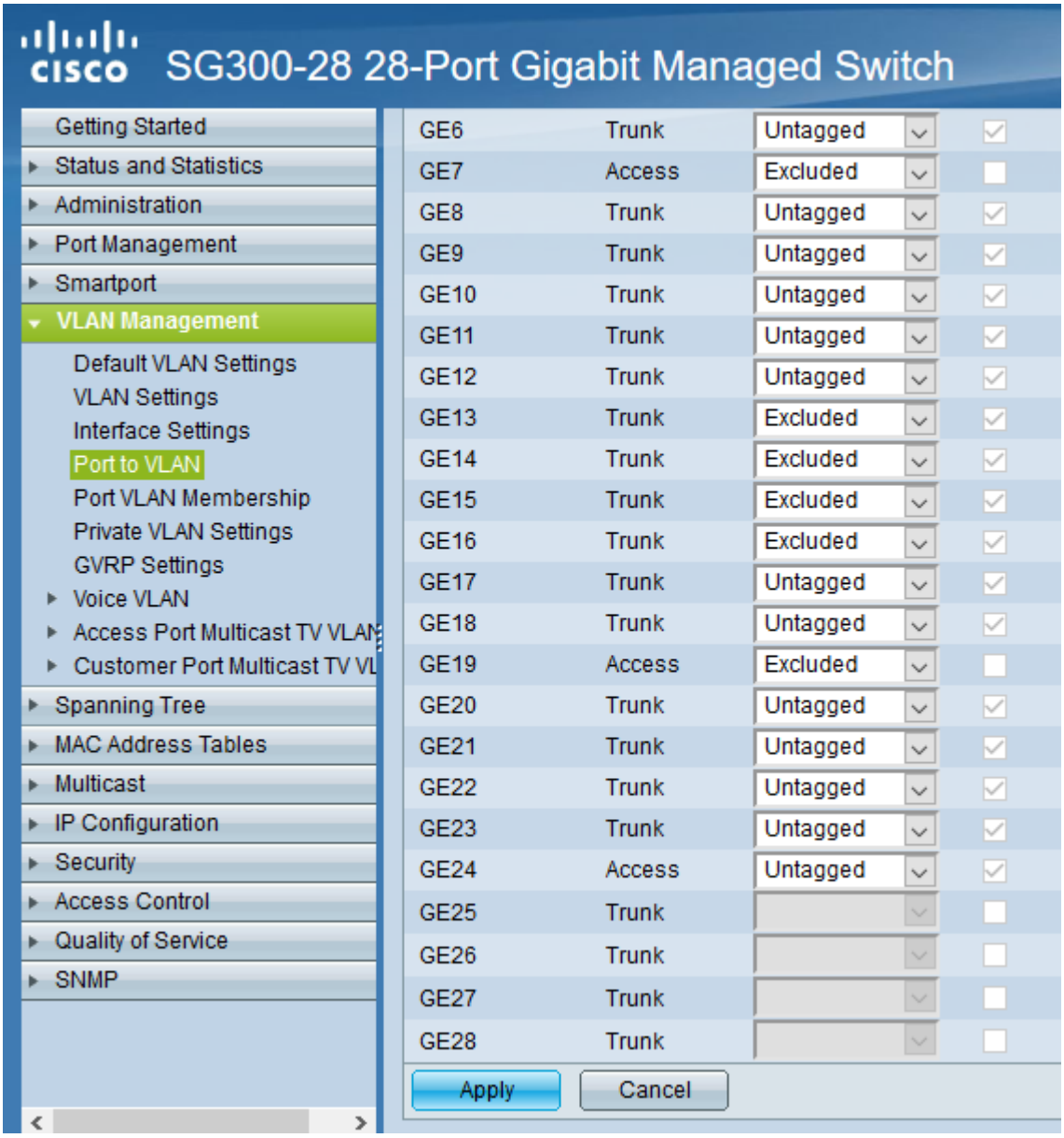


Definition der Access Ports (port-based VLAN)

- `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).

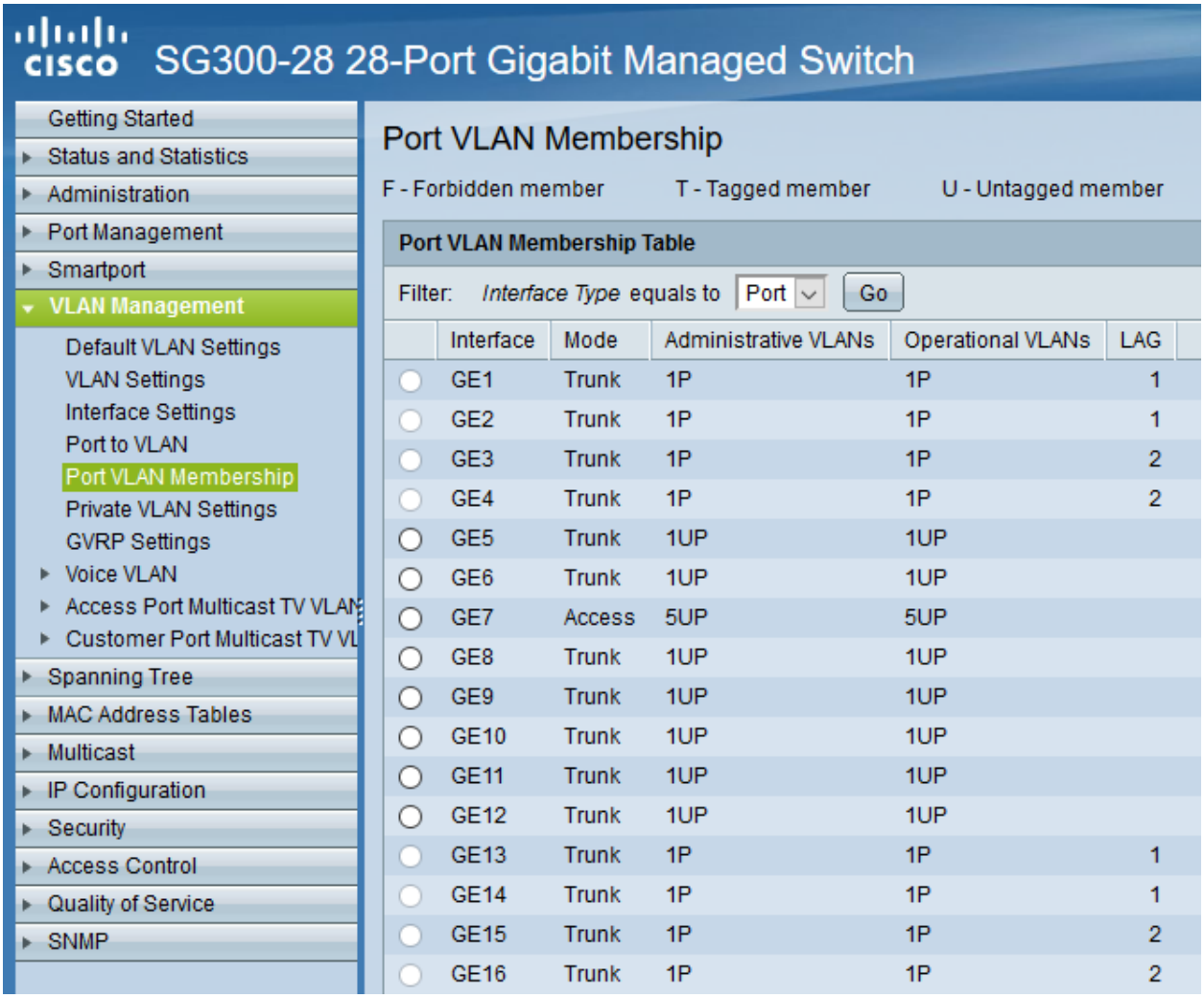
Werden auf dem Switch weitere Ports z.B. für Testzwecke im Server VLAN benötigt, so sind diese unter `VLAN Management --> Interface Settings` als Access-Ports und unter `Port-to-VLAN` dem korrekten VLAN zuzordnen. Nachstehende Abbildungen stellen die Zuordnung zu VLAN 1 dar.

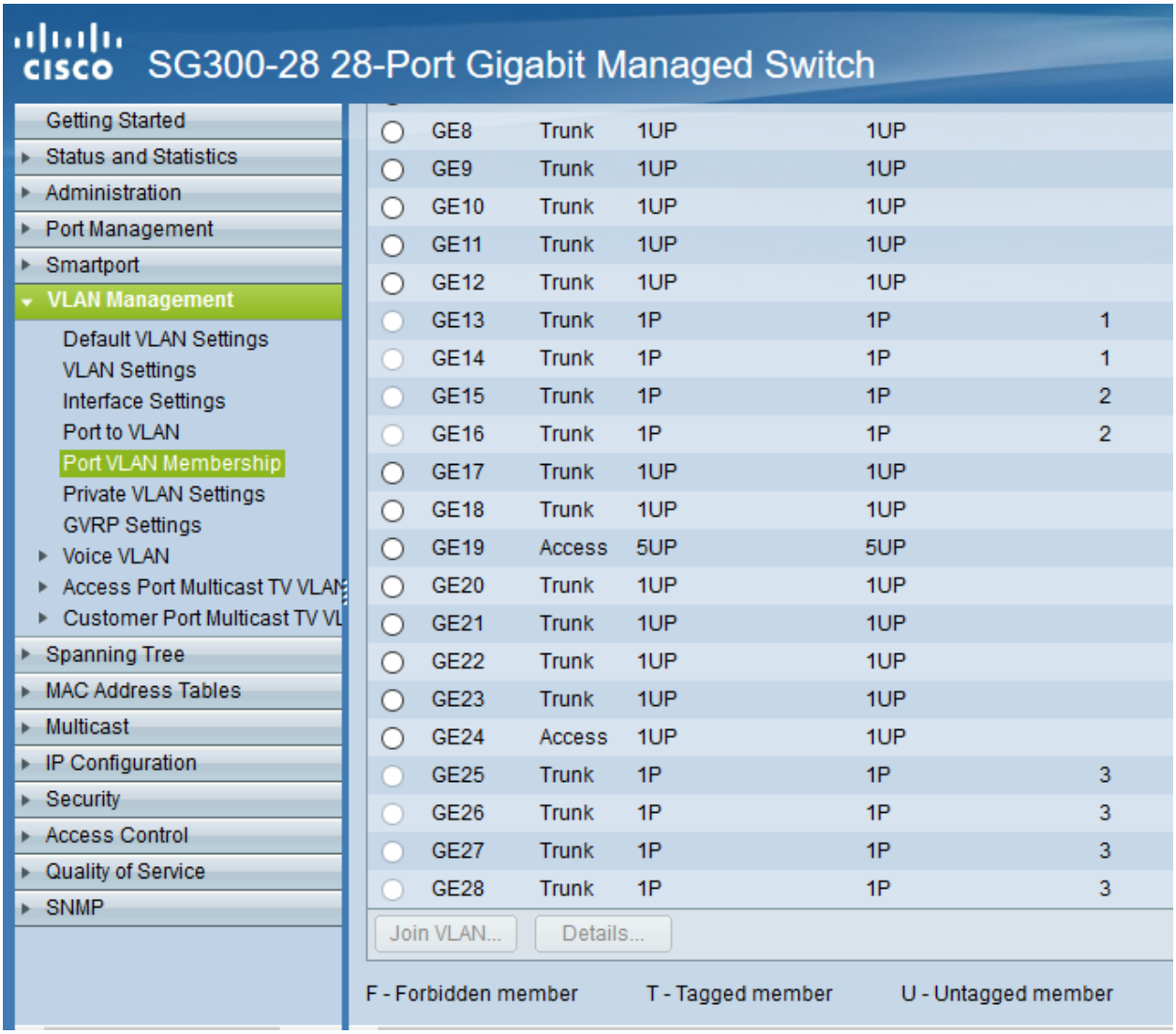


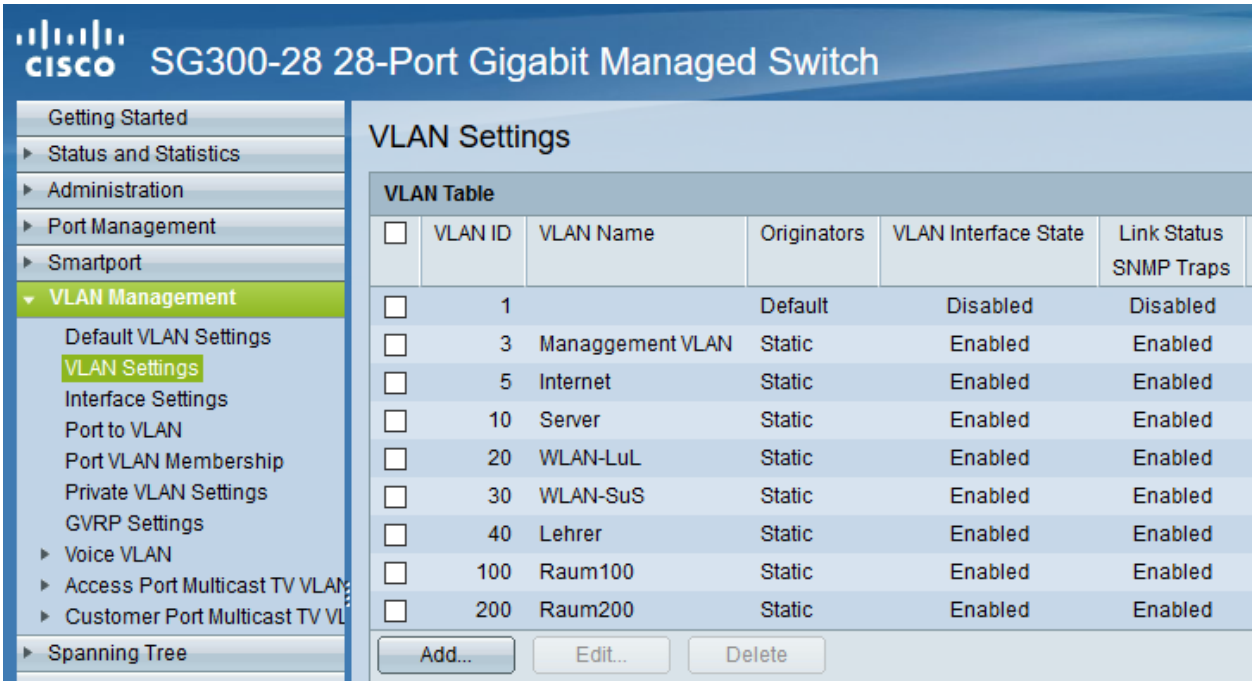


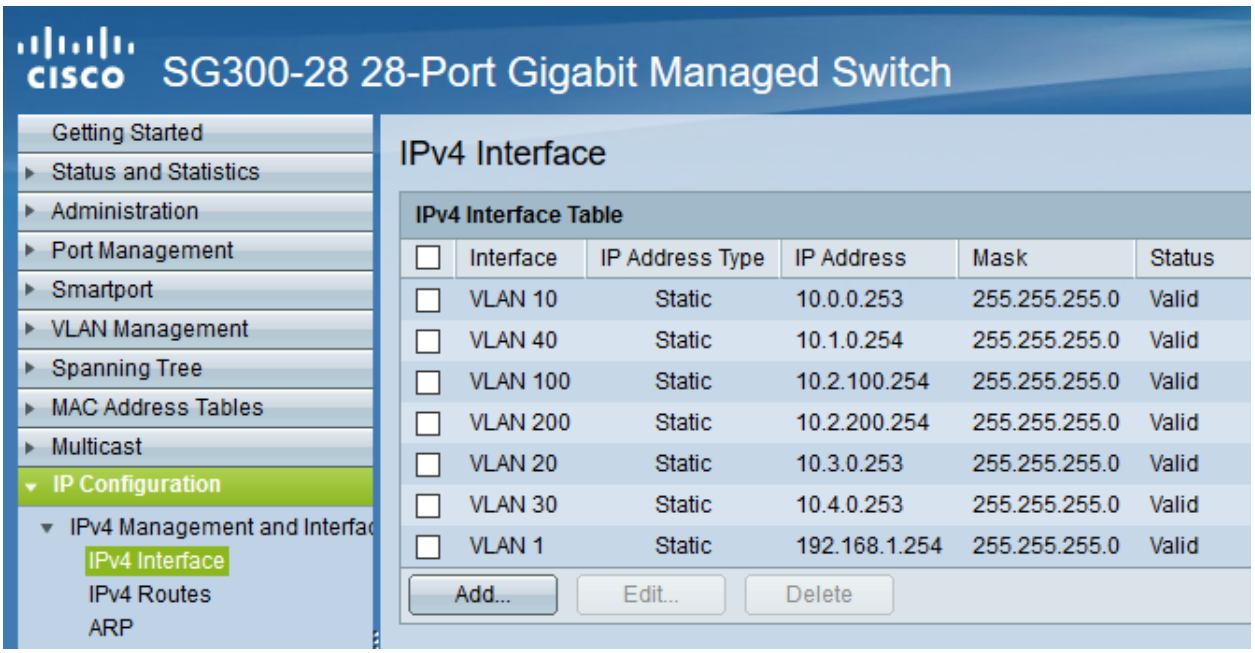
Definition / Zuordnung der VLANs

- `LAG1 (Port 1,2,13,14)`: Der Hypervisor ist über vier Netzwerkkabel mit Port 1,2,13,14 des Switches verbunden. Auf der Seite des Hypervisor sind ebenfalls vier Ports durch LinkAggregation definiert. LAG1 ist getaggtes Mitglied der VLANs 3,5,10,20,30,40,100,200.
- `LAG2 (Port 3,4,15,16)`: Der zweite Hypervisor ist über vier Netzwerkkabel mit Port 3,4,15,16 des Switches verbunden. Auf der Seite des Hypervisor sind ebenfalls vier Ports durch LinkAggregation definiert. LAG1 ist getaggtes 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. LA32 ist getaggtes 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).

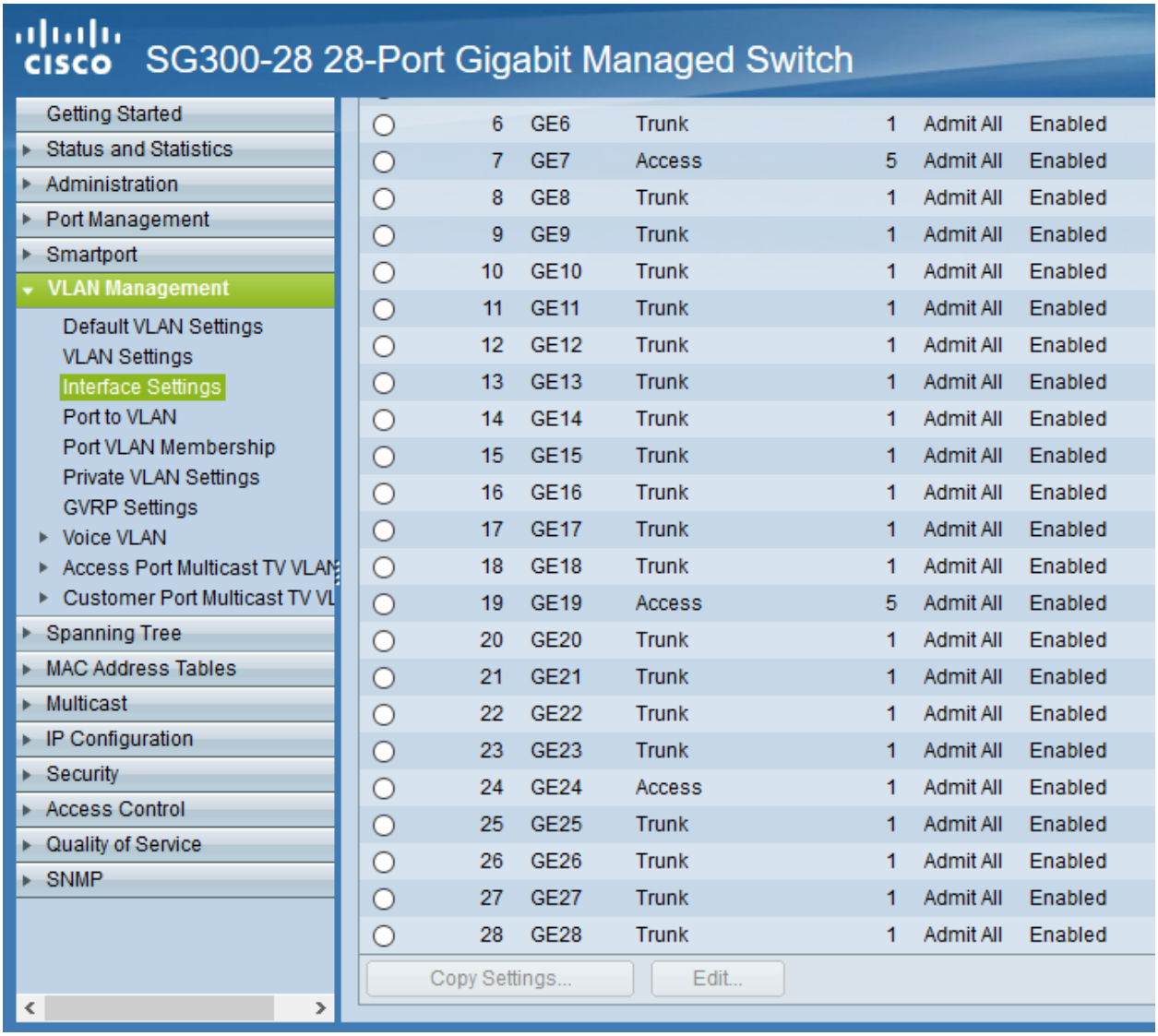

cisco
SG300-28 28-Port Gigabit Managed Switch
Getting Started
Status and Statistics
Administration
Port Management
Smartport
VLAN Management
Default VLAN Settings
VLAN Settings
Interface Settings
Port to VLAN
Port VLAN Membership
Private VLAN Settings
GVRP Settings
Voice VLAN
Access Port Multicast TV VLAN
Customer Port Multicast TV VL
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 Port Go
Interface Mode Administrative VLANs Operational VLANs LAG
GE1 Trunk 1P 1P 1
GE2 Trunk 1P 1P 1
GE3 Trunk 1P 1P 2
GE4 Trunk 1P 1P 2
GE5 Trunk 1UP 1UP
GE6 Trunk 1UP 1UP
GE7 Access 5UP 5UP
GE8 Trunk 1UP 1UP
GE9 Trunk 1UP 1UP
GE10 Trunk 1UP 1UP
GE11 Trunk 1UP 1UP
GE12 Trunk 1UP 1UP
GE13 Trunk 1P 1P 1
GE14 Trunk 1P 1P 1
GE15 Trunk 1P 1P 2
GE16 Trunk 1P 1P 2


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 VL
Spanning Tree
MAC Address Tables
Multicast
IP Configuration
Security
Access Control
Quality of Service
SNMP
GE8 Trunk 1UP 1UP
GE9 Trunk 1UP 1UP
GE10 Trunk 1UP 1UP
GE11 Trunk 1UP 1UP
GE12 Trunk 1UP 1UP
GE13 Trunk 1P 1P 1
GE14 Trunk 1P 1P 1
GE15 Trunk 1P 1P 2
GE16 Trunk 1P 1P 2
GE17 Trunk 1UP 1UP
GE18 Trunk 1UP 1UP
GE19 Access 5UP 5UP
GE20 Trunk 1UP 1UP
GE21 Trunk 1UP 1UP
GE22 Trunk 1UP 1UP
GE23 Trunk 1UP 1UP
GE24 Access 1UP 1UP
GE25 Trunk 1P 1P 3
GE26 Trunk 1P 1P 3
GE27 Trunk 1P 1P 3
GE28 Trunk 1P 1P 3
Join VLAN...
Details...
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 VL
Spanning Tree
VLAN Settings
VLAN Table
VLAN ID
VLAN Name
Originators
VLAN Interface State
Link Status SNMP Traps
1 Default Disabled Disabled
3 Managgement VLAN Static Enabled Enabled
5 Internet Static Enabled Enabled
10 Server Static Enabled Enabled
20 WLAN-LuL Static Enabled Enabled
30 WLAN-SuS Static Enabled Enabled
40 Lehrer Static Enabled Enabled
100 Raum100 Static Enabled Enabled
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 Interfac
IPv4 Interface
IPv4 Routes
ARP
IPv4 Interface
IPv4 Interface Table
Interface
IP Address Type
IP Address
Mask
Status
VLAN 10 Static 10.0.0.253 255.255.255.0 Valid
VLAN 40 Static 10.1.0.254 255.255.255.0 Valid
VLAN 100 Static 10.2.100.254 255.255.255.0 Valid
VLAN 200 Static 10.2.200.254 255.255.255.0 Valid
VLAN 20 Static 10.3.0.253 255.255.255.0 Valid
VLAN 30 Static 10.4.0.253 255.255.255.0 Valid
VLAN 1 Static 192.168.1.254 255.255.255.0 Valid
Add...
Edit...
Delete


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 VL
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 Port Go
Entry No. Interface Interface VLAN Mode Administrative PVID Frame Type Ingress Filtering Primary VLAN
1 GE1 Trunk 1 Admit All Enabled
2 GE2 Trunk 1 Admit All Enabled
3 GE3 Trunk 1 Admit All Enabled
4 GE4 Trunk 1 Admit All Enabled
5 GE5 Trunk 1 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



Access Listen definieren

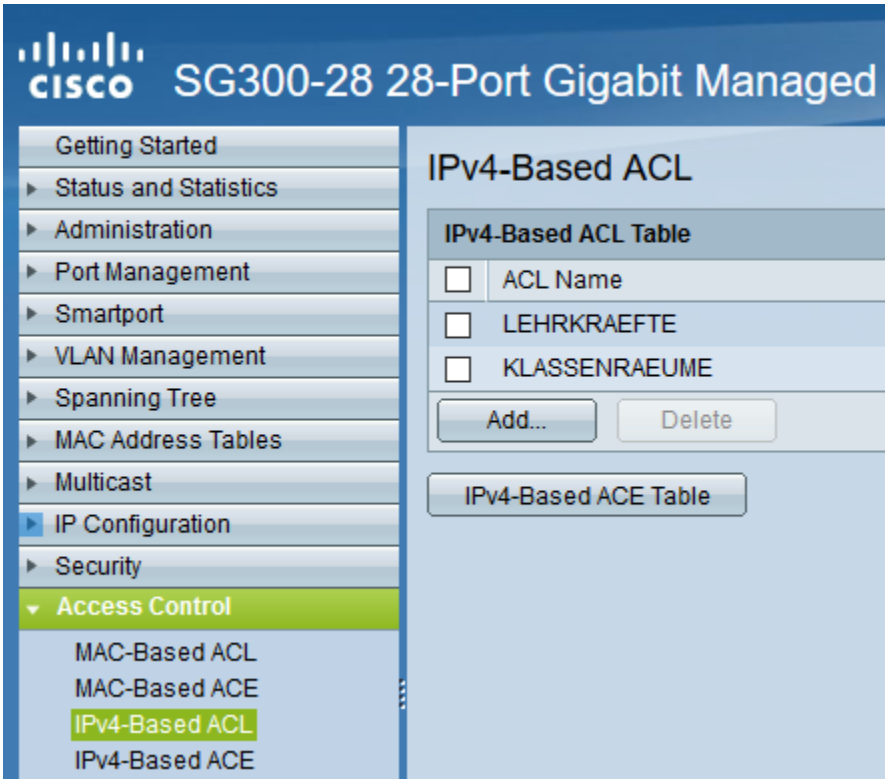
Hinweis: Der Cisco L3-Switch kann nur eingehenden Datenverkehr filtern. Dies ist relevant für die Definition und Anwendung der Listen für die Zugriffssteuerung (ACLs). **Achtung**: Die hier vorgestellten ACLs führen dazu, dass bsp. PCs aus zwei verschiednen Klassenräumen sich untereinander via ping nicht 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: Lehrkraefte und Klassenraeume

Es sind Zwei ACL anzulegen: Lehrkraefte und Klassenraume. Dies erfolgt im Menü unter: Zugriffssteuerung –> IPv4 basierte ACL –> Hinzufügen –> <Name der ACL>

ACEs hinzufügen

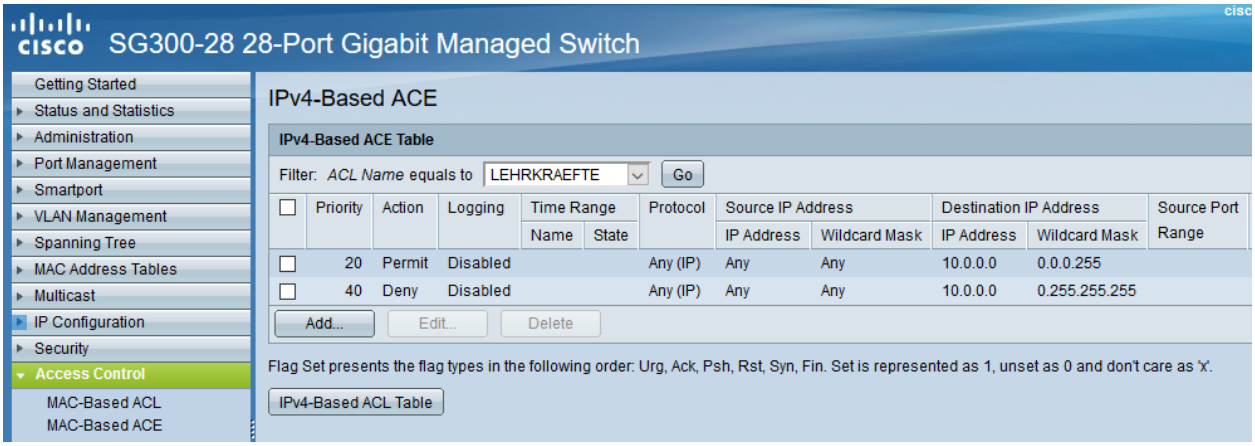
Für die zuvor genannten ACLs sind jetzt sog. Entries (Einträge) anzulegen. Hierfür wählst Du im Menü: Zugriffssteuerung –> IPv4 basiertes ACE –> <Name der ACL aus Liste auswählen - hier Lehrkraefte> –> Hinzufügen



Du gibst dann folgende Werte an:

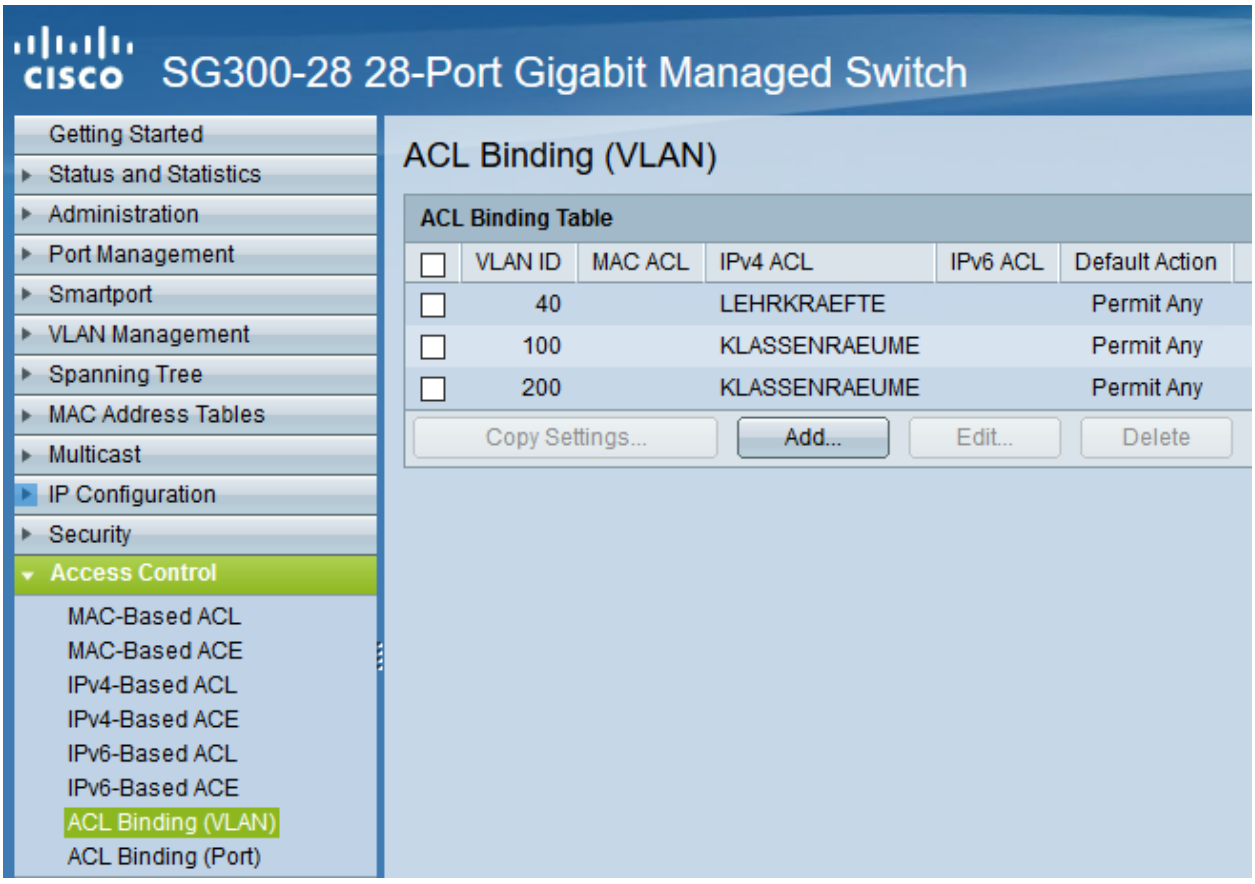
- Priorität: 20
- Aktion: Zulassen (permit)
- Protokoll: Beliebig (IP) (any)
- Quell-IP-Adresse: Beliebig (any)
- Ziel-IP-Adresse: Benutzerdefiniert (user defined)
- Wert der Ziel-IP-Adresse: 10.16.1.0 (Servernetz-IP)
- Ziel-IP-Platzhaltermaske: 0.0.0.255 (invertierte Netzmaske)

Danach legst Du eine zweite ACE für die ACL Lehrkraefte an. Im Ergebnis solltest Du für die Lehrkraefte dann nachstehenden Einträge haben:



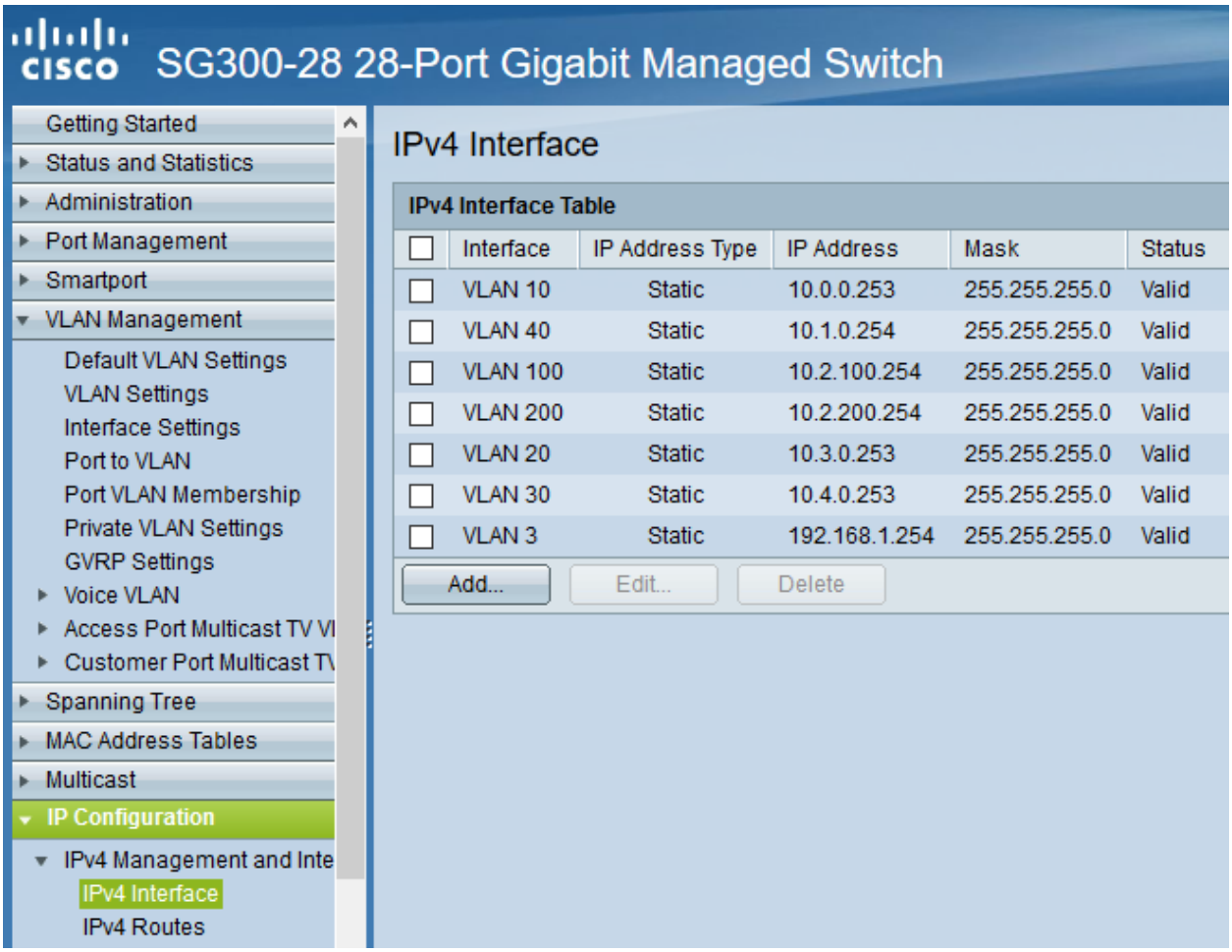
Danach lest Du ACEs für die `ACL Klassenraeume` an. Danach solltest Du nachstehende Einträge haben:

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:



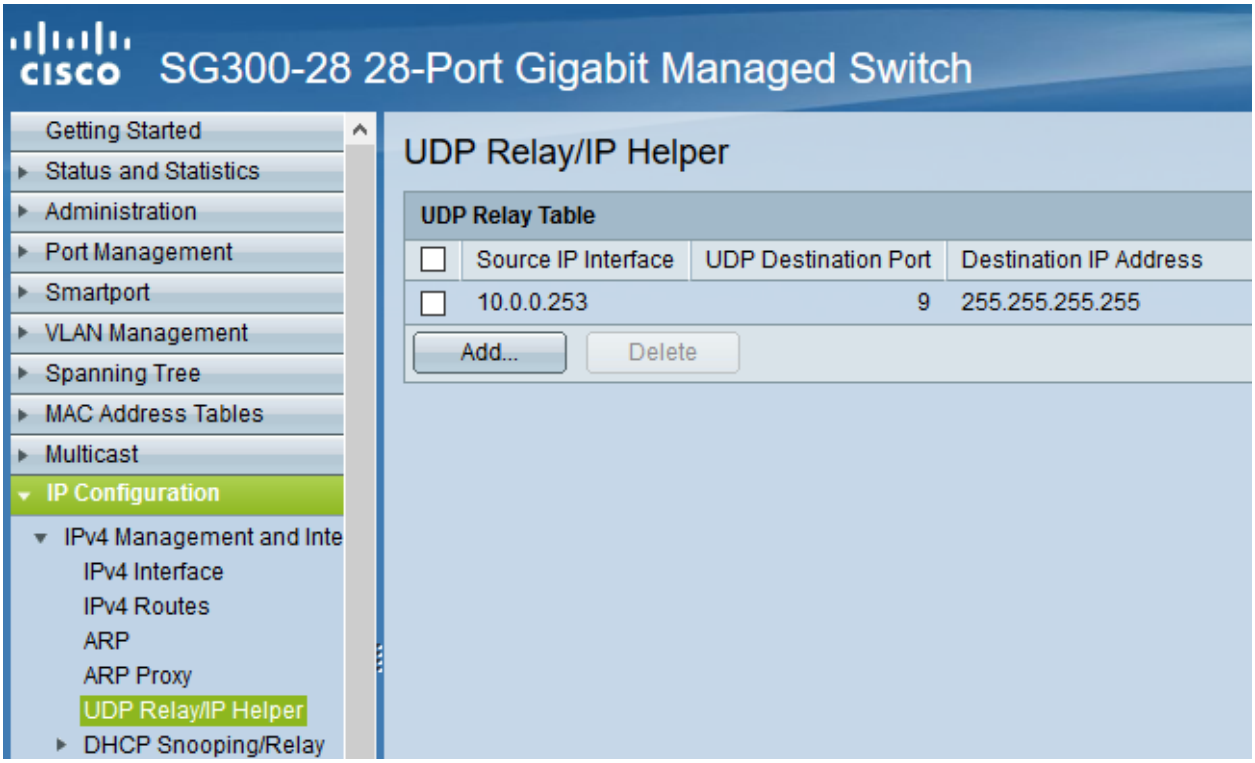
DHCP-Relay konfigurieren

Die Einstellungen für das DHCP-Relaying sollten wie folgt aussehen:

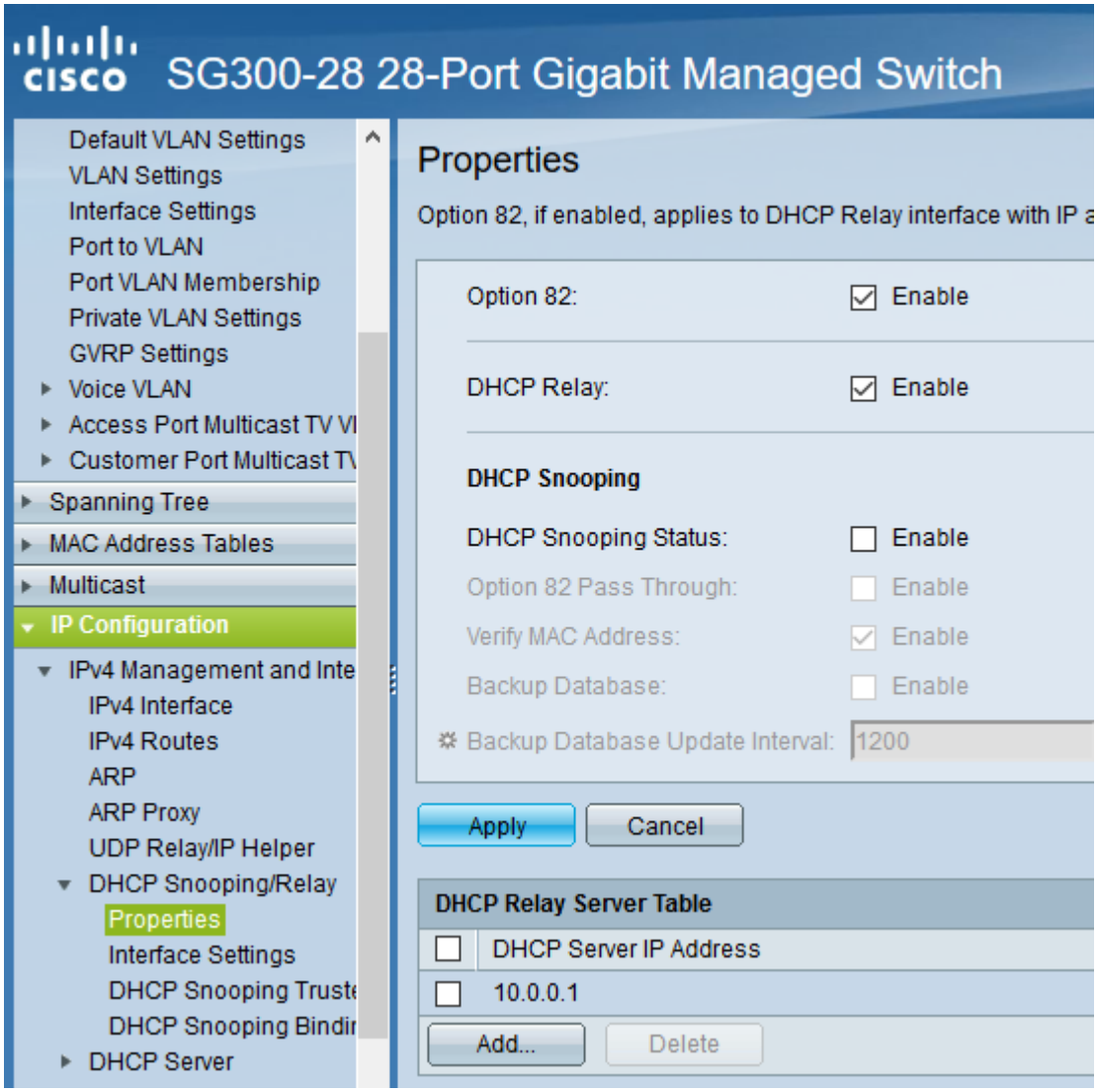


Hierdurch wird sichergestellt, dass DHCP-Anfragen aus den genannten VLANs auch beim linuxmuster.net Server ankommen und bedient werden können.

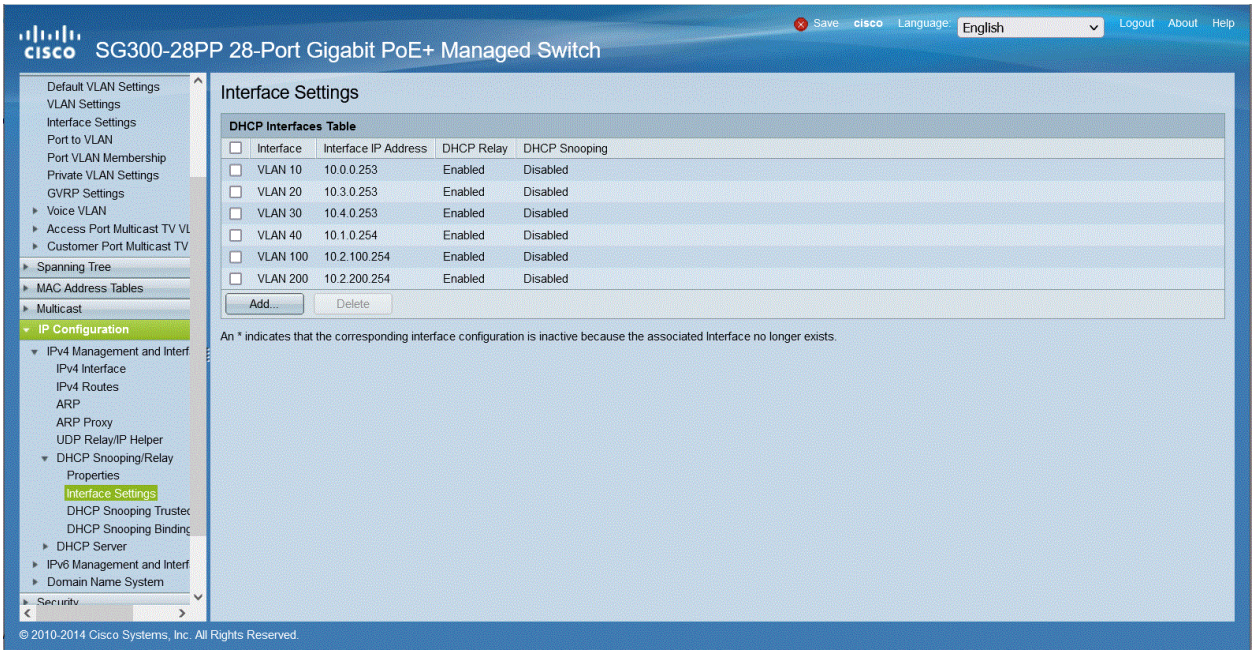
Um Wake-on-LAN über Subnetze hinweg zu nutzen, muss ein sog. UDP-Relaying eingerichtet werden. Hierdruch können dann z.B. Clients via `linbo-remote` aufgeweckt werden.



Für das DHCP-Relaying/Snooping muss zudem die Option 82 aktiviert werden.



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 Switche abhängt.

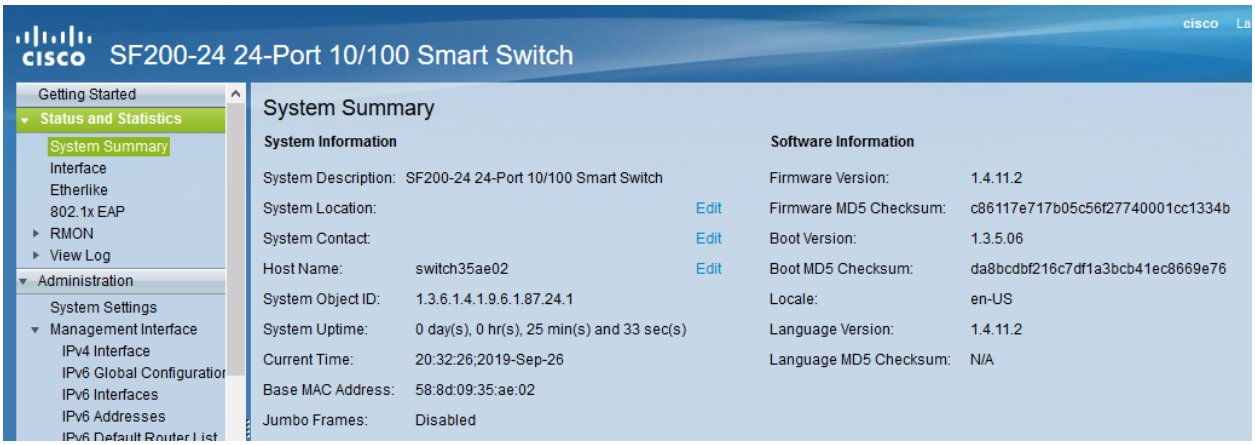
Exemplarisch erfolgt die Darstellung zur Einrichtung der VLANS auf L2-Switches anhand des Modells Cisco SF200-24. Für andere Modelle sind die Konfigurationsschritte entsprechend anzupassen.

SF200-24 Startup-Config

Für das hier dokumentierte Netzwerkszenario wurde ein Switch des o.g. Models für Raum 200 vorkonfiguriert, um das Vorgehen zur Konfiguration der L2-Switche besser darstellen zu können. Die Konfiguration wird zur schnelleren Umsetzung des Szenarios unten bereitgestellt.

`Startup-config-SF200-24-L2-Raum200`.

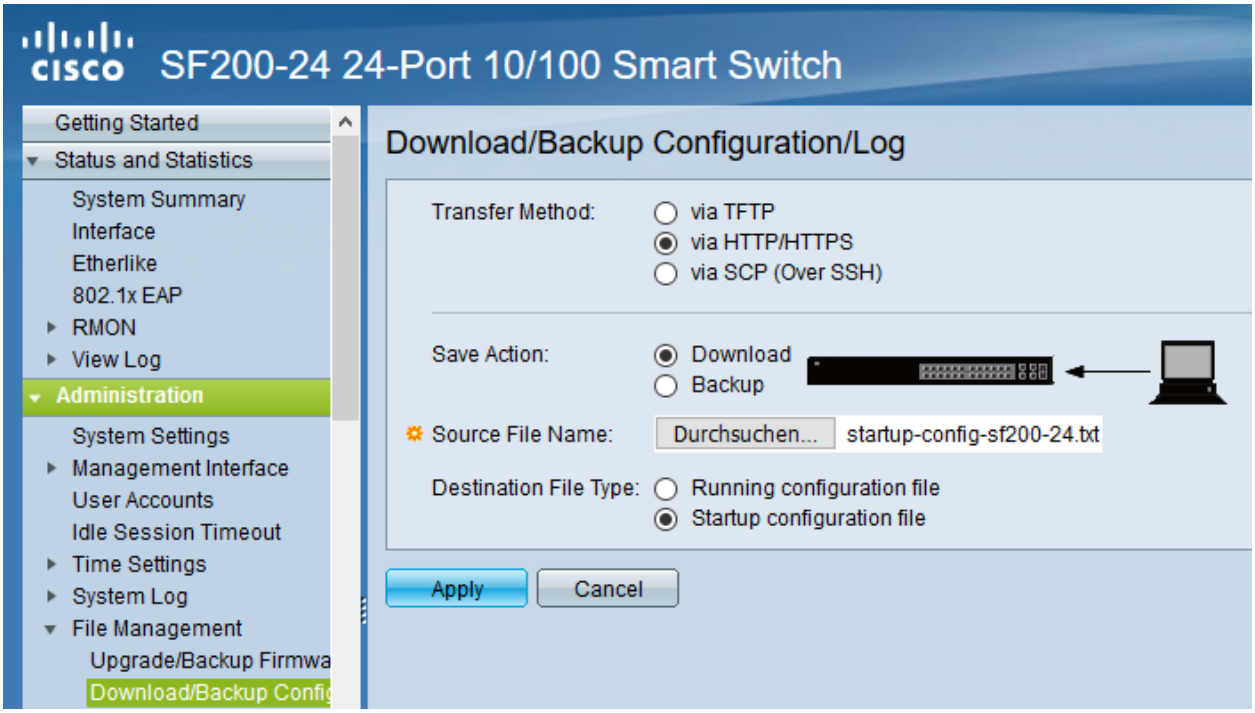
Hinweis: Die Firmware des Cisco L2-Switches ist vorab auf die aktuellste Version (hier: 1.4.11.2) zu aktualisieren. Ist eine ältere FW-Version noch installiert, so kann es erforderlich sein, die Aktualisierung in Etappen vorzunehmen (z.B. 1.1.2.0 -> 1.3.7.18 -> 1.4.7.5 -> 1.4.11.2). Um die Boot Version zu aktualisieren, ist die RTB-Datei desFW-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.



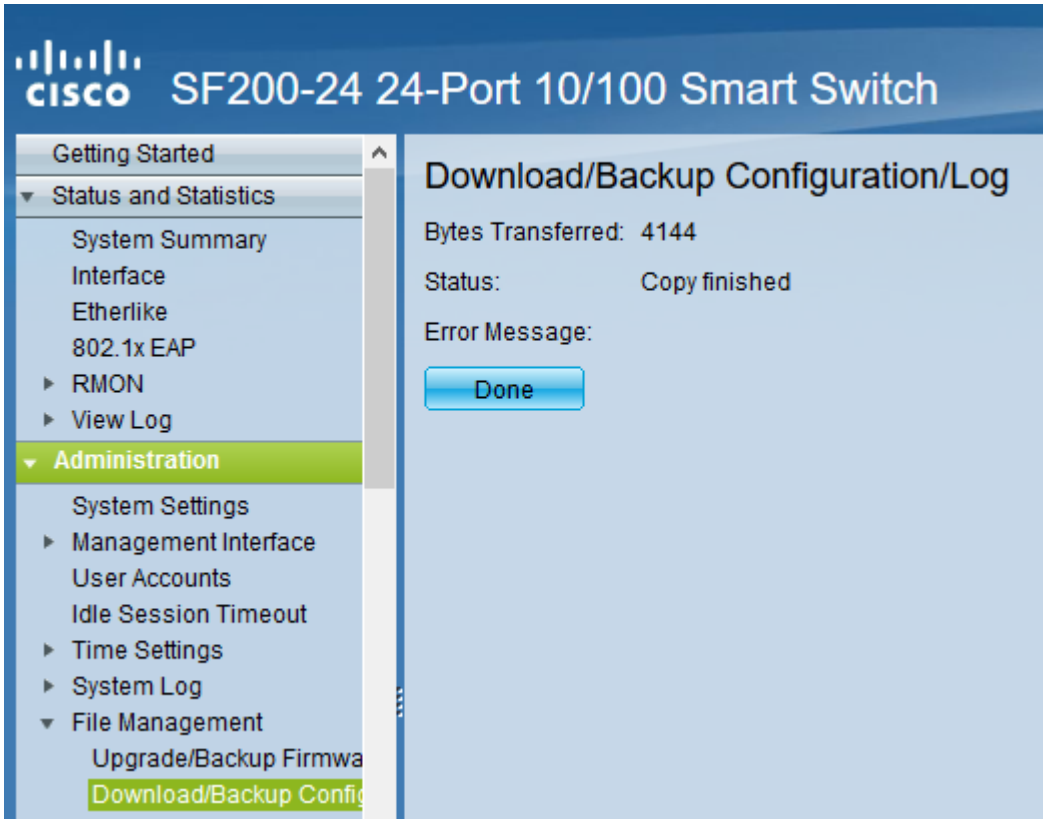
Die heruntergeladene Konfigurationsdatei ist nun auf den Switch zu laden und dieser ist dann neu zu starten.

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.



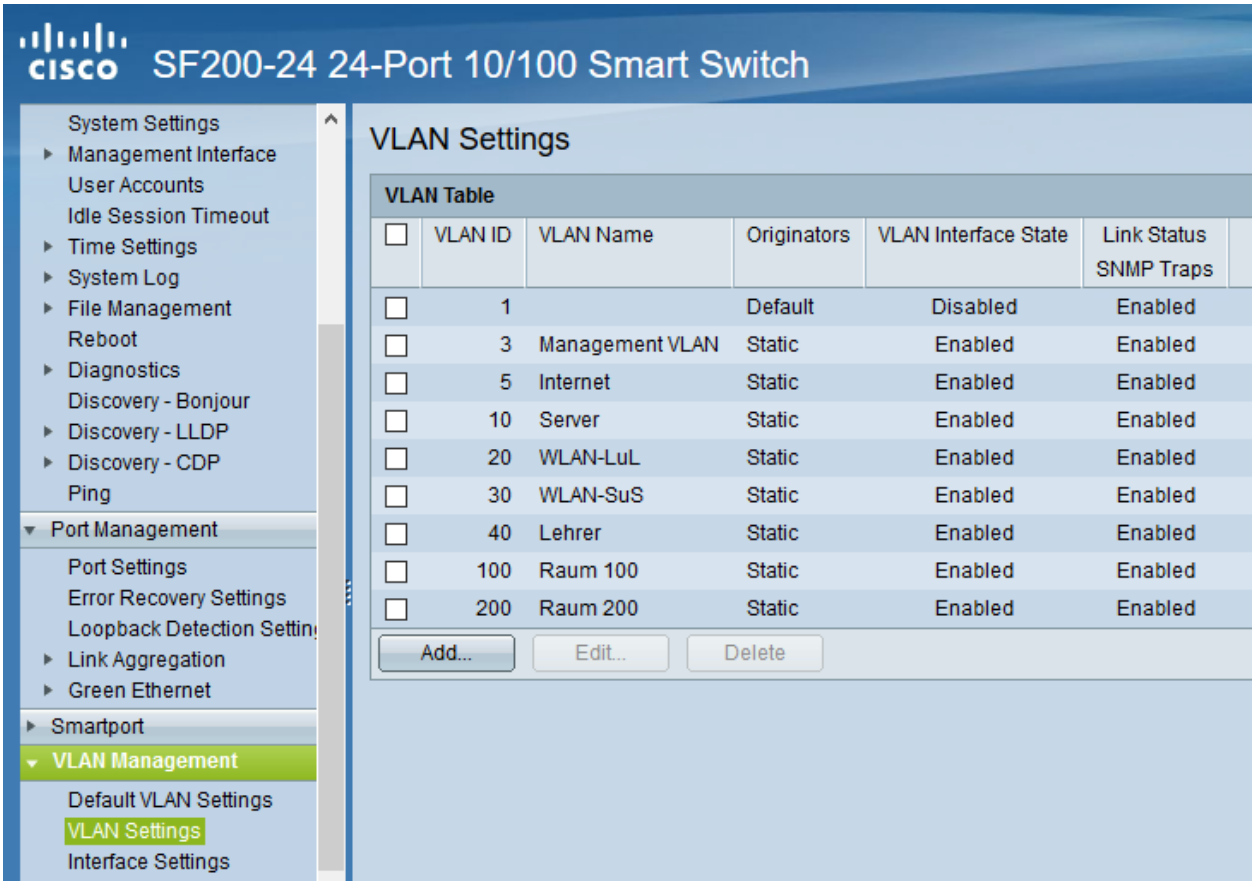
Danach ist der Switch neu zu starten (siehe Hinweise wie bei Cisco L3-Switch). Nach dem Neustart sind nachstehende Hinweise zur weiteren Konfiguration des Switches zu beachten.

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.

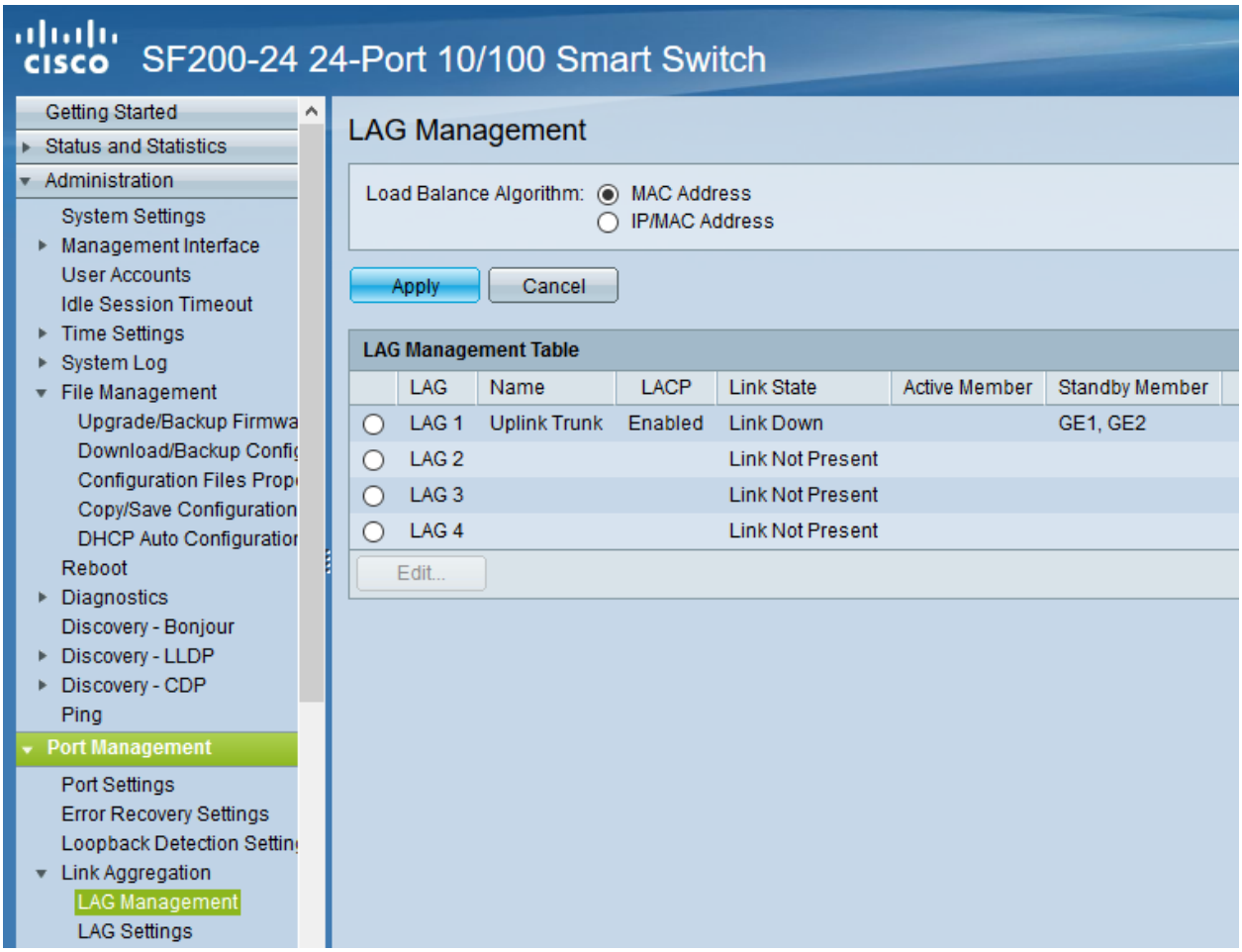
Durch den Import der Konfigurationsdatei sind bereits alle Konfigurationseinstellungen für den Switch eingetragen, der als Raum-Switch für Raum 200 (VLAN 200) für einen PC-Raum dienen soll.

Nachstehend dargestellte Konfigurationsschritte visualisieren die jeweiligen Einstellungen, die so auch manuell eingestellt werden können.

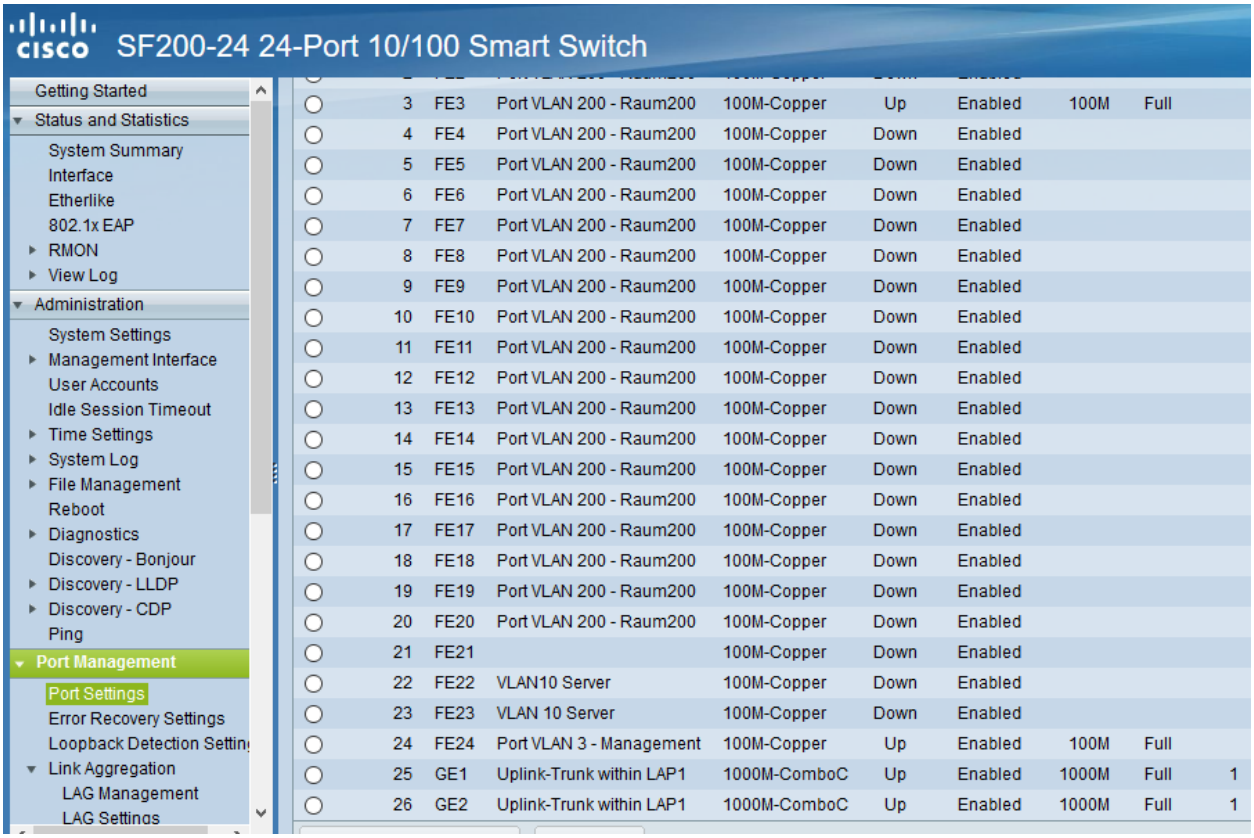
Zunächst sind die VLANs mit identischen IDs und Bezeichnungen auf allen L2 - Switchen analog zum L3-Switch anzulegen.



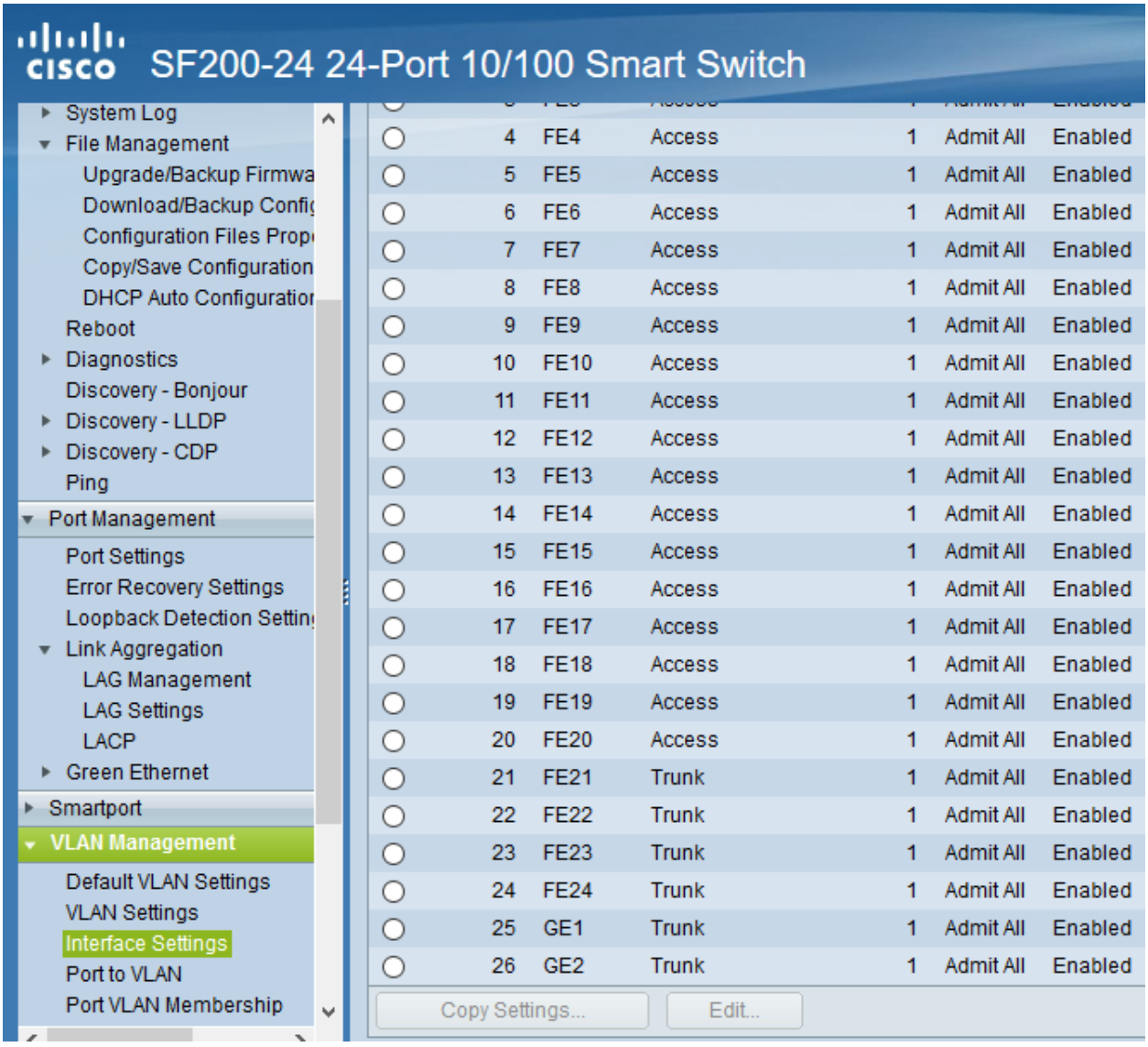
Danach ist der LACP-Bond bestehend aus den Ports 25 & 26 zu definieren.



Die Nutzung der jeweiligen Ports wird in der Beschreibung pro Port dokumentiert.

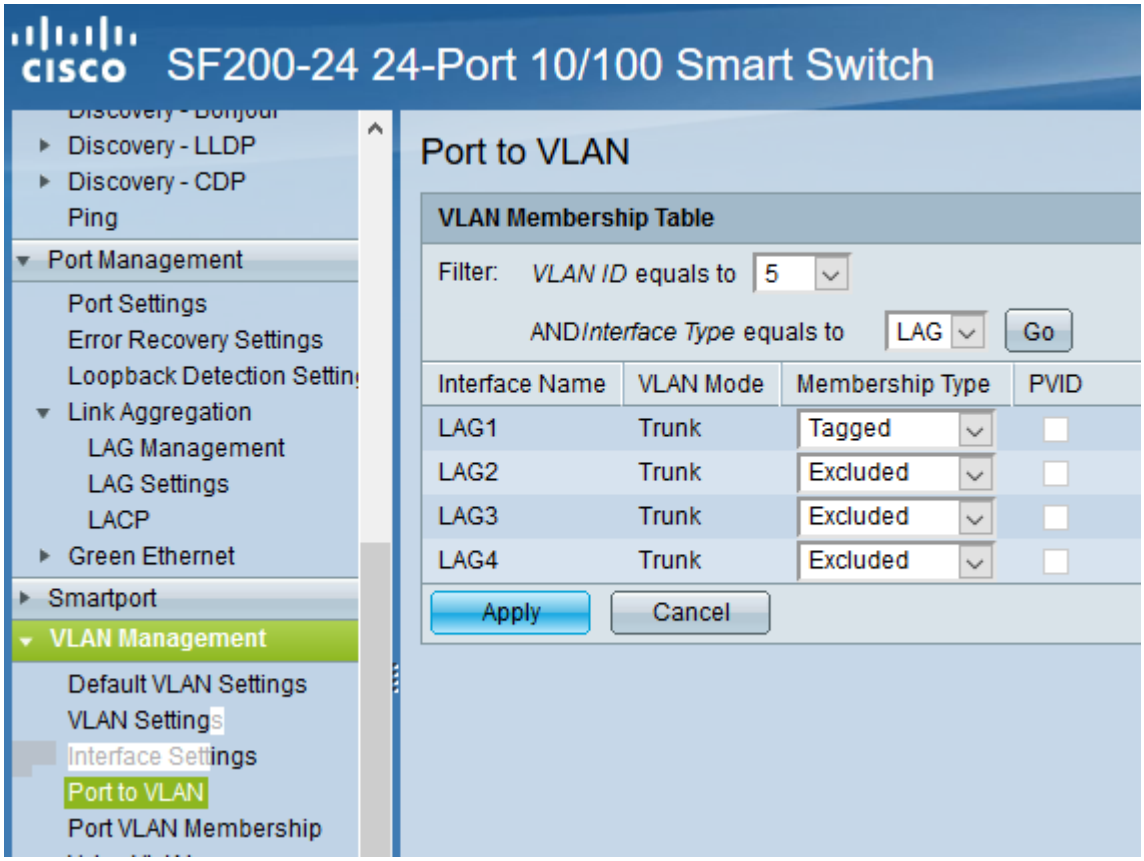


Die VLAN - Nutzung der Ports (Access, Trunk) ist festzulegen.

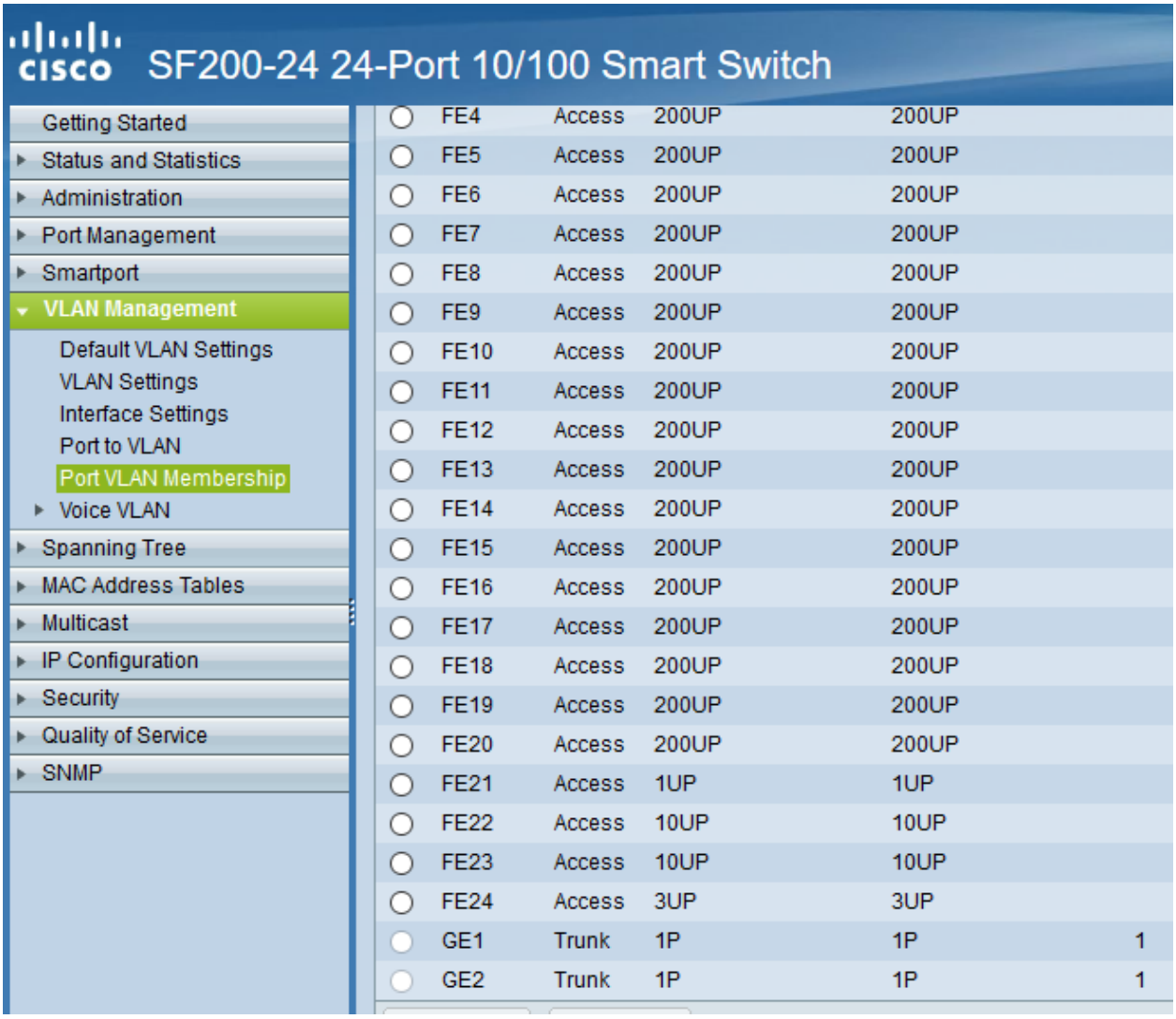


Die Ports sind den VLANs zuzuordnen in denen diese arbeiten sollen. So soll der Switch die Ports 1-20 als Access Ports im VLAN 200 nutzen.

Die Darstellung der Zuordnung kann pro VLAN kontrolliert werden. Hier als Beispiel die Darstellung für das VLAN 5.



Die Zuordnung der Ports zu den VLANs inkl. Darstellung deren Funtkion ist im Menü `VLAN Management --> Port VLAN Membership` dargestellt.



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 Netzszenario 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
       brdige_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
       brdige_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
       brdige_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
       brdige_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
       brdige_ageing 0
       bridge_maxwait 0
#VLAN 40 Lehrernetz
```

(Fortsetzung auf der nächsten Seite)

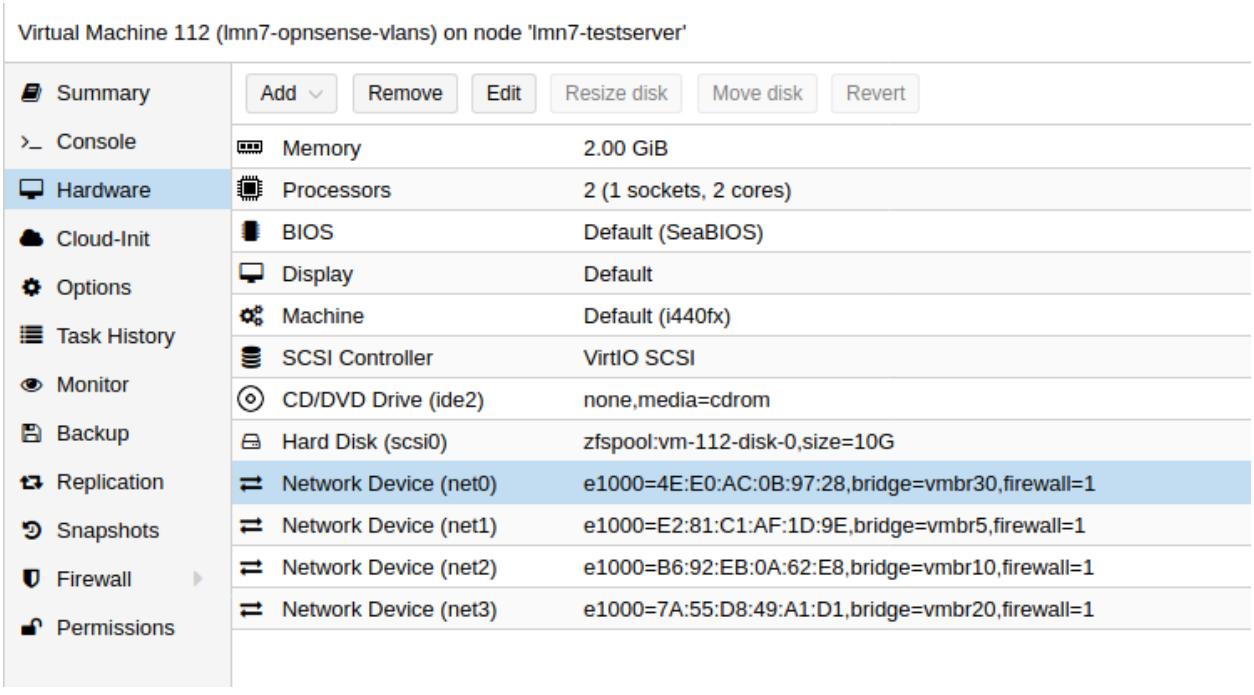
(Fortsetzung der vorherigen Seite)

```
auto vmbr100
iface vmbr100 inet manual
       bridge-ports bond0.100
       bridge-stp off
       bridge-fd 0
       bridge_maxage 0
       brdige_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
       brdige_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:



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: 10.4.0.0.0/24, 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
```

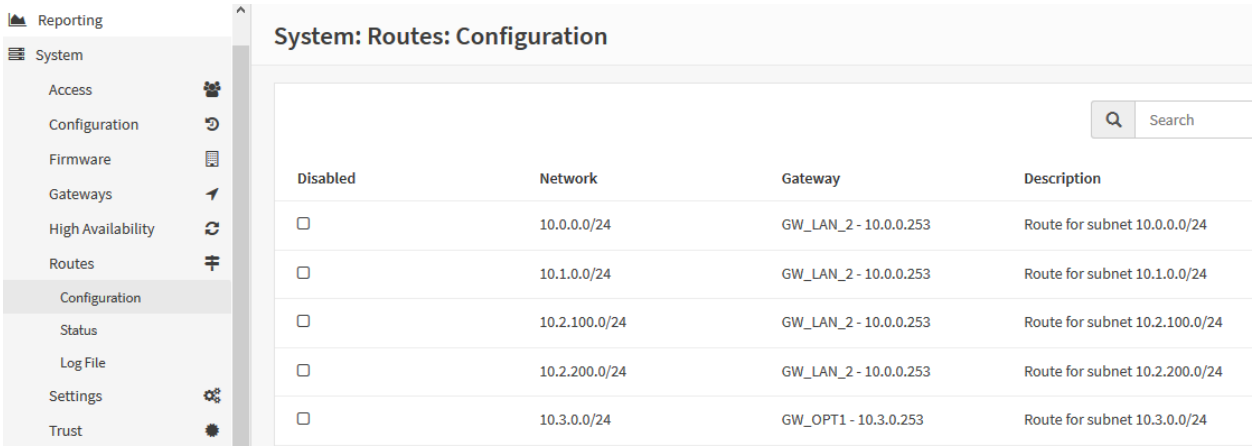
Hinweise:

- 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-Swich 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.

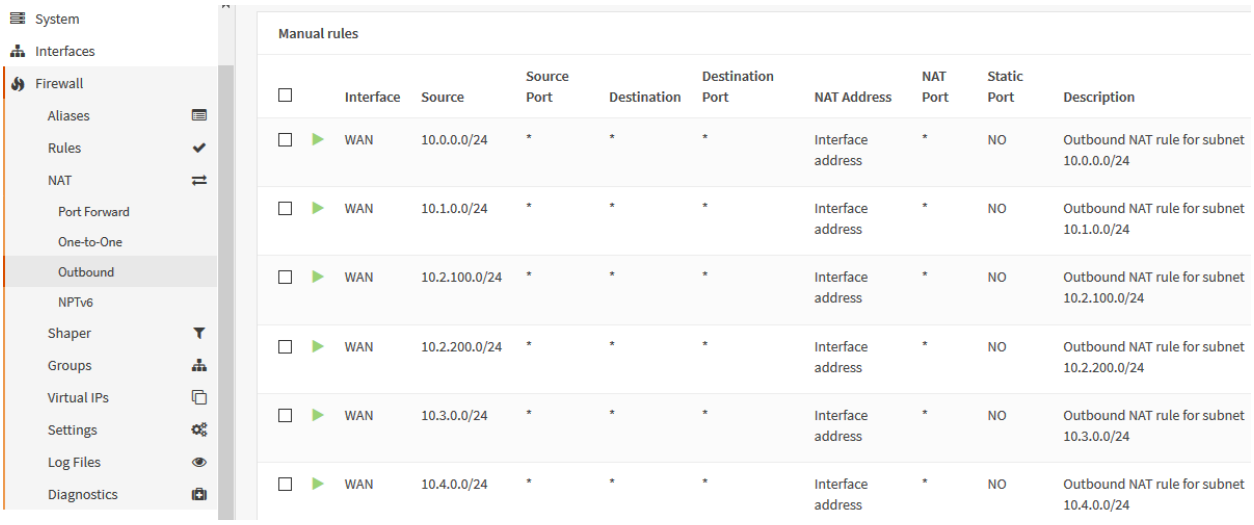
Subnetze importieren

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.

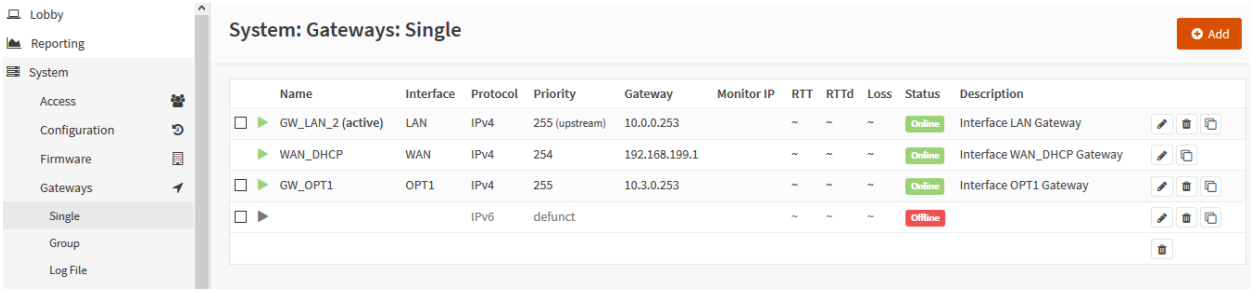
Firewall-Beispiel



Auf der Firewall werden zusätzlich ausgehende NAT-Regeln für jedes Subnetz angelegt:



und das LAN-Gateway angepasst.



netplan auf VMs prüfen

Der Import ändert die Netzwerkeintragungen 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:

Wichtig ist, dass die Routen zu den jeweileigen 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 Zugrff 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/sophomorix/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
l001;l001-pc01;ubu18;01:60:66:3F:A6:1A;10.1.0.1;;;;computer;;2
l001;l001-pc02;ubu18;01:60:66:3F:A6:1B;10.1.0.2;;;;computer;;2
l001;l001-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 geignete 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-Switche 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 Druckermodells
- mögliche Treiber für Linux, Windows und ggf. andere Clients
- MAC-Adresse des Druckers
- Raum / Standort des Druckers
- IP-Adresse gemäß des genutzen Adressschema

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.

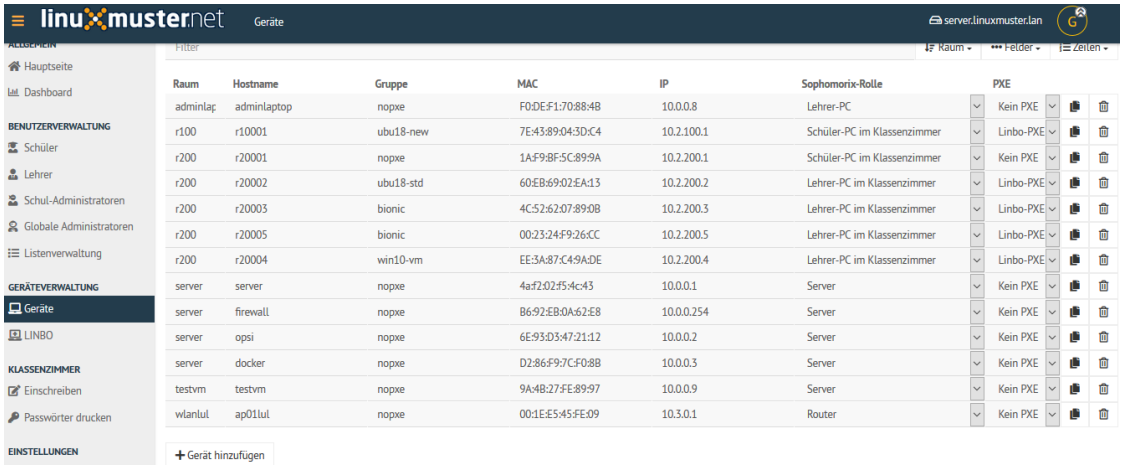
4.35.2 Drucker via Schulkonsole hinzufügen

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.

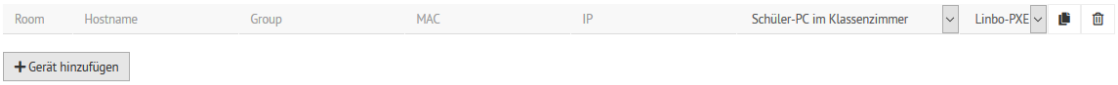
Für das folgende Beispiel nehmen wir an, der Drucker stehe in Raum „r200“, bekomme den Namen „r200-pr01“, habe die MAC-Adresse „00:11:22:33:44:55“ und bekomme entsprechend einem IP-Adressschema die IP-Adresse 10.2.200.101.

Melde Dich als `global-admin` in der Schulkonsole (https://10.0.0.1) an. Wähle dort links im Menü `Geräteverwaltung` das Untermenü `Geräte` aus.



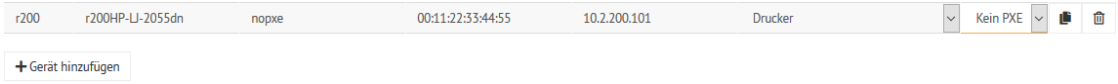
Klicke unterhalb der Geräteliste auf den Eintrag `Gerät hinzufügen`.

Es wird eine leere Zeile zur Liste hinzugefügt.



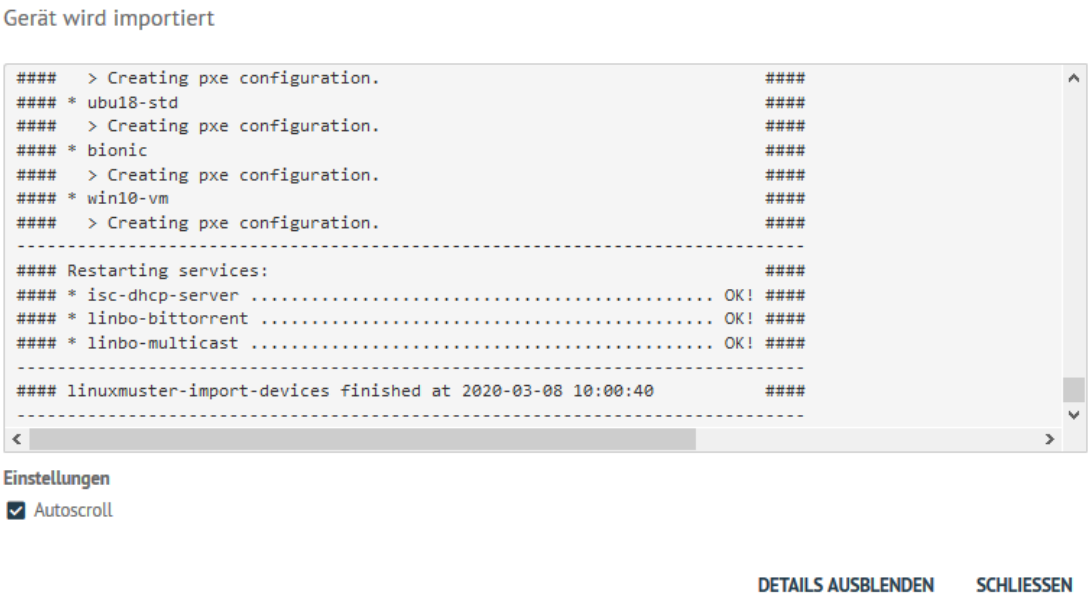
Die Option PXE ist zu deaktivieren, da die Drucker nicht via PXE starten. Als Gruppe ist `nopxe` einzutragen.

Für o.g. Beispieldrucker stellt sich der Eintrag wie folgt dar:



Bestätige den Eintrag mit `speichern & importieren`.

Es erscheint ein Fenster, in dem der Vorgang bestätigt wird.



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

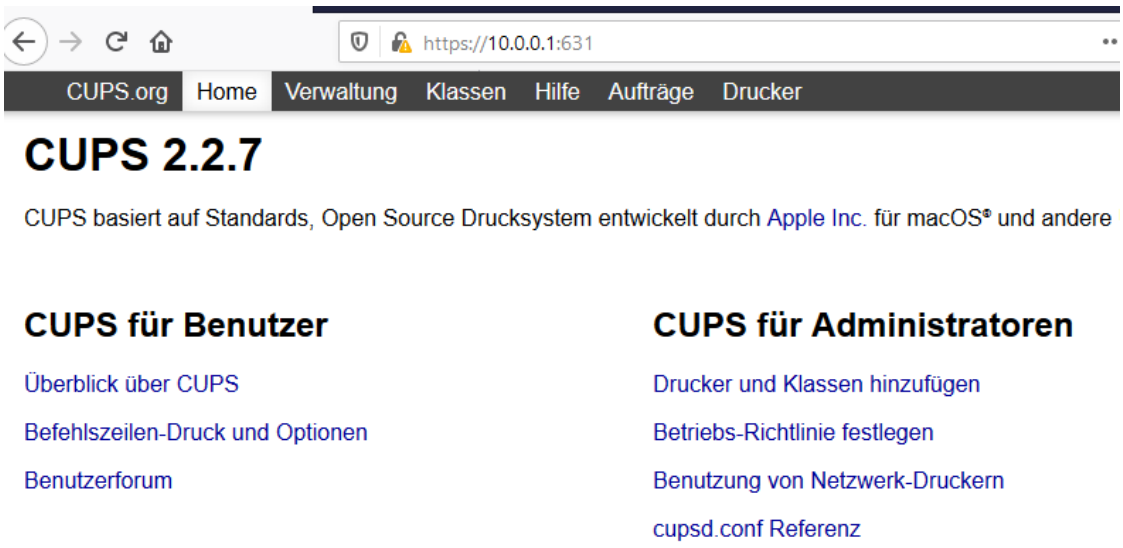
Autor des Abschnitts: @cweikl

Um die als Geräte bereits importieren 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.

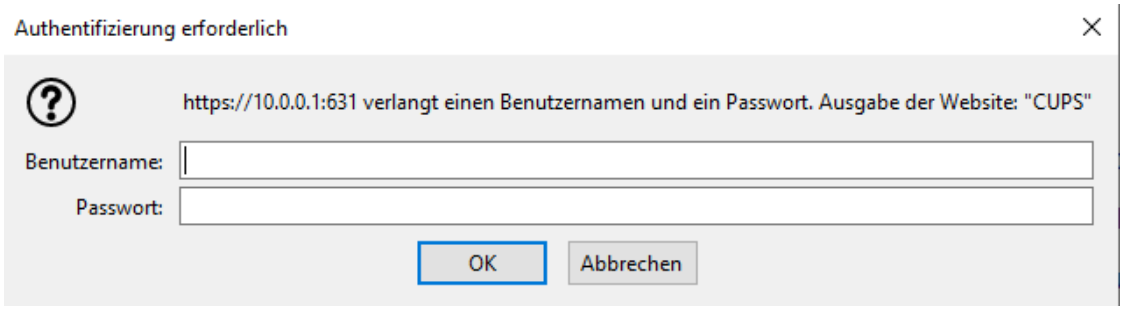
Starte auf einem Rechner einen Browser, um das sog. CUPS-Webinterface des Servers zur weiteren Einrichtung der Drucker aufzurufen. Hierzu füge nachstehende URL in der Adresszeile Deines Browsers ein:

```
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).



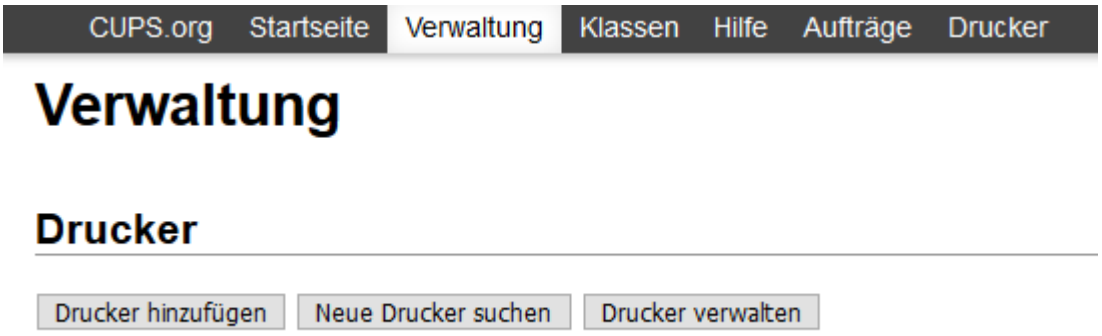
Es erscheint die Login-Aufforderung von CUPS auf dem Server:



Melde Dich als `root` dort an.

Drucker hinzufügen

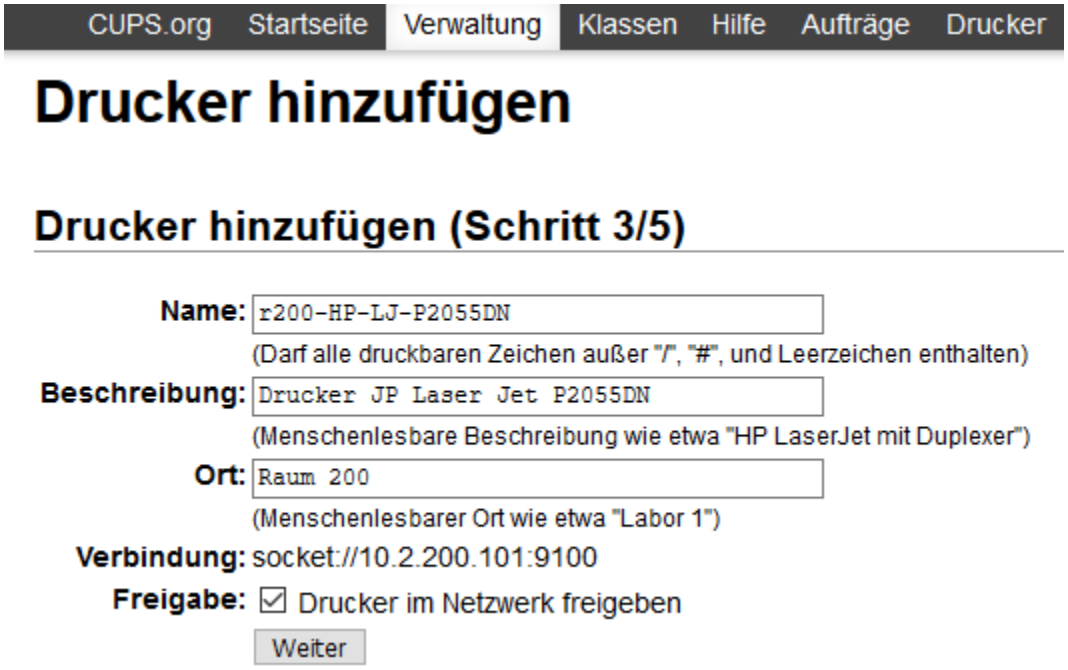
Nach der Anmeldung an CUPS wähle den Menüpunkt `Verwaltung` aus.



Rufe den Untermenüpunkt `Drucker hinzufügen` aus. Es erscheint nachstehende Maske. Wähle als Netzwerkdrucker i.d.R. LPD/LPR-Host aus und klicke auf `weiter`.

Gib als Verbindung die IP-Adresse und den Port des LPD-Druckers wie in der Abb. an:

Klicke auf `weiter`. Wähle nun den geeigneten Druckertreiber für Deinen Drucker aus:



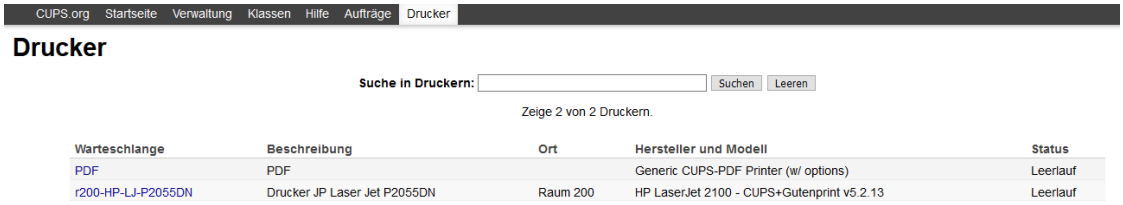
Hierzu wähle den Hersteller aus, dann erscheint eine Liste mit den verfügbaren Druckertreibern. Wähle in der Liste den korrekten Drucker aus. Sollte dieser in der Liste nicht enthalten sein, so klicke auf `PPD-Datei bereitstellen -> Durchsuchen`. Wähle nun die PPD-Datei mit dem korrekten Druckertreiber aus, den Sie zuvor von der Website des Herstellers heruntergeladen hast.

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.

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.



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

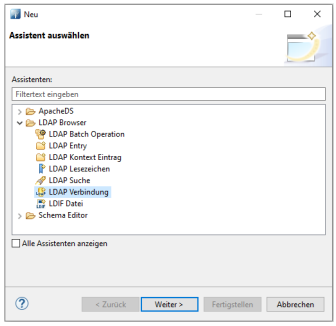
Achtung: Sobald diese Funktion in der Schulkonsole zur Verfügung steht, wird dieser Teil der Dokumentation ergänzt.

Für die Raumzuweisung von Druckern eignet sich am besten das *Apache Directory Studio*. Das *Apache Direktory 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 Direktory Studios* herunter und installiere sie ebenfalls.

Hinweis: Auf dem Ubuntu-Client kann das *Apache Directory Studio* direkt ausgeführt werden.

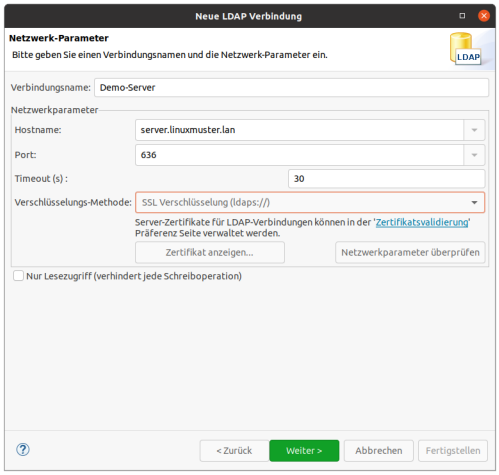
Schauen wir uns mit dem *Apache Directory Studio* die AD-Struktur etwas genauer an. Dazu müssen wir zunächst eine Verbindung zum Server aufbauen.

Starte das *Apache Directory Studio* und gehe in der Menü-Leiste auf `Datei` → `Neu`.

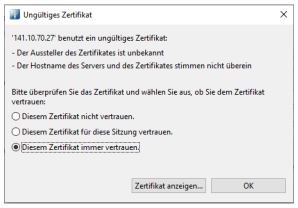


Wähle `LDAP-Verbindung` und klicke auf `weiter`.

Gib der Verbindung einen Namen und trage die Verbindungsdaten des Servers ein.

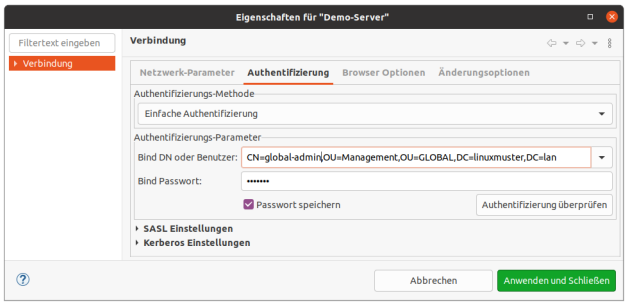


Klicke auf Netzwerkparameter überprüfen. Falls der Server nur ein selbst signiertes Zertifikat hat, erscheint der folgende Dialog:



Wähle `Diesem Zertifikat immer vertrauen` und klicke auf `ok`. Wenn Du jetzt auf Netzwerkparameter überprüfen klicken, 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`.

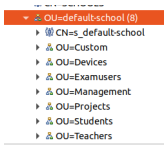
Hinweis: Du nutzt hier den global-admin, weil Du Schreibrechte brauchst. Sicherheitshalber solltest Du vor Deiner Arbeit einen Snapshot des Servers machen.

Klicke auf `Anwenden und Schließen`.

Der Baum des AD wird geladen und angezeigt.

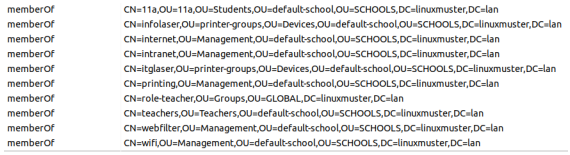
Schreib Dich in der Schulkonsole bei den Druckern ein.

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.

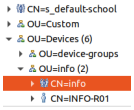
Im Eintrag des Benutzers sind die Drucker als memberOf eingetragen.



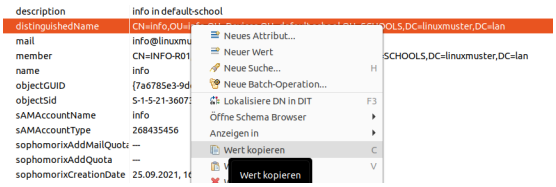
Beim Eintrag des Druckers ist der Benutzer als member eingetragen.

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.

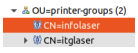
Navigiere zum Gruppeneintrag des Informatik-Raums.



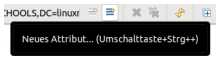
Im mittleren Fenster werden die Einträge der Gruppe info angezeigt. Kopiere mit einem Rechtsklick den `distinguishedName`.



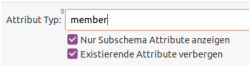
Navigiere zur Gruppe des Druckers.



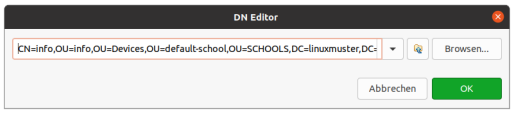
und klicke auf `Neues Attribut...`



Als Attribut-Typ gibst Du `member` ein und klickst anschließend auf `Fertigstellen`.



Jetzt Fügst 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.

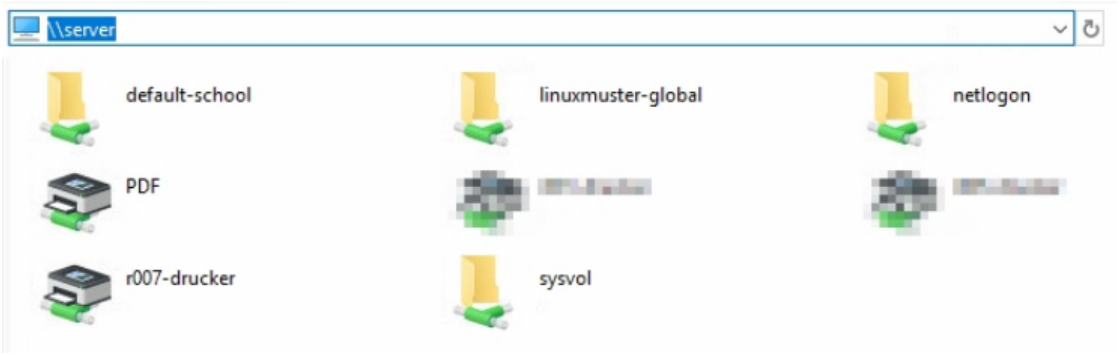
Markiere einen Drucker, klicke mit der rechten Maustaste und wähle im Kontextmenü den Punkt `Eigenschaften` aus. Klicke unterhalb von `Tests und Wartungen` den Button `Testseite drucken` aus.

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

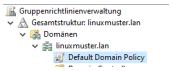
Bevor es losgehen kann, müssen wir dem *global-admin* noch die nötigen Rechte auf dem Server einräumen. Melde Dich dazu als *root* auf dem Server an und führen Sie die folgenden Befehle aus:

```
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/
```

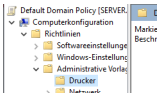
Dem Server vertrauen

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:

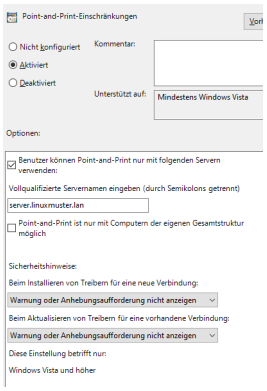
Melde Dich als global-admin am Windows-Client an und starte die Gruppenrichtlinienverwaltung (Wie Du sie installierts kannst Du *hier* nachlesen). Navigiere zur Default Domain Policy von linuxmuster.lan.



Wähle mit einem Rechtsklick `Bearbeiten`. Es öffnet sich der Gruppenrichtlinien-Editor. Navigiere zu `Computerkonfiguration` → `Richtlinien` → `Administrative Vorlagen` → `Drucker`.



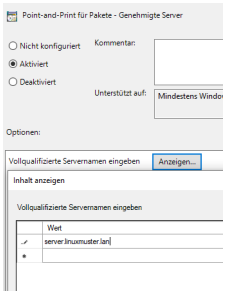
Doppelkilicke auf `Point and Print Einschränkungen`, aktiviere die Richtlinie und setzen folgende Einstellungen:



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

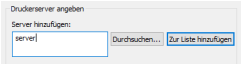
Starte den Rechner neu.

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.

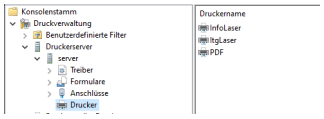
Jetzt können wir die Druckertreiber auf dem Server installieren.

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.



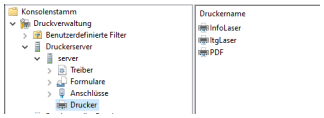
Mache einen Rechtsklick auf `Treiber` und wähle `Treiber hinzufügen`. Gehe zu `Weiter` → `Weiter` → `Datenträger... Durchsuchen` → `Ok` und wähle den richtigen Druckertreiber. Es werden nur Microsoft zertifizierte Treiber akzeptiert. Falls Du mit einem Treiber Probleme haben solltest, versuche es eventuell mit einem etwas älteren Treiber. Die werden sehr oft akzeptiert.

Klicke abschließend auf `Fertigstellen`.

Einem Drucker einen Druckertreiber zuweisen

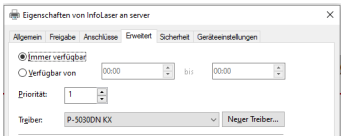
Jetzt müssen wir nur noch den Druckern die Druckertreiber zuweisen.

Öffne als global-admin das Programm `mmc.exe` und navigiere zu `Drucker`.



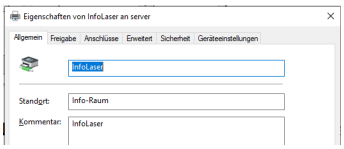
Mache einen Rechtsklick auf den Drucker, dem Du einen Druckertreiber zuweisen möchtest und wähle `Eigenschaften...` Falls Du gefragt wirst, ob Du einen Druckertreiber lokal installieren möchtest, antworte mit Nein.

Gehe zum Reiter `Erweitert`, wähle bei Treiber den passenden Treiber für den Drucker und bestätige mit `OK`.



Leider ändert Windows den Namen des Drucker 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 installieret 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 hinzufügt 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-Protokol 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 veschrieben: 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

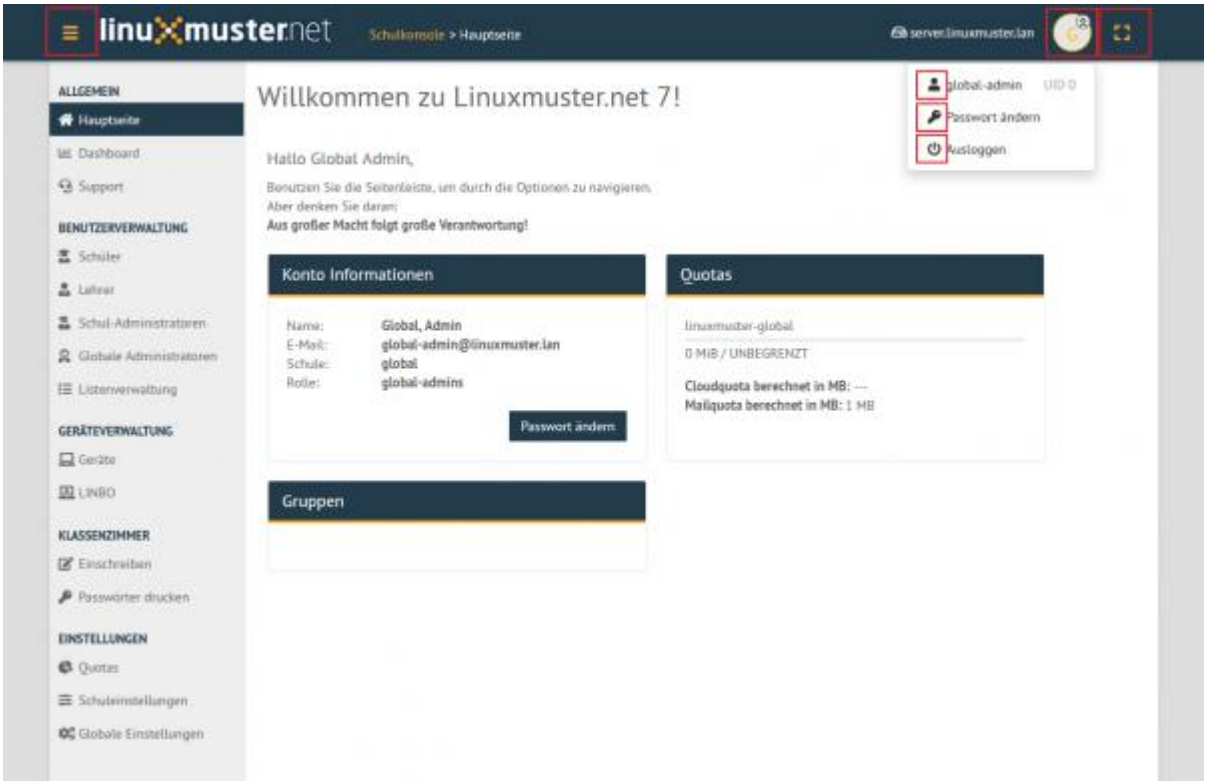
Die Schulkonsole wird im Browser über https://10.0.0.1 aufgerufen. Je nachdem welcher Benutzer angemeldet ist, erscheinen zugehörige Menüpunkte. Alle verwaltungsspezifischen Menüpunkte stehen dem Benutzer ‚global-admin“ bereit. Lehrer haben Zugriff auf alle pädagogischen Funktionen.

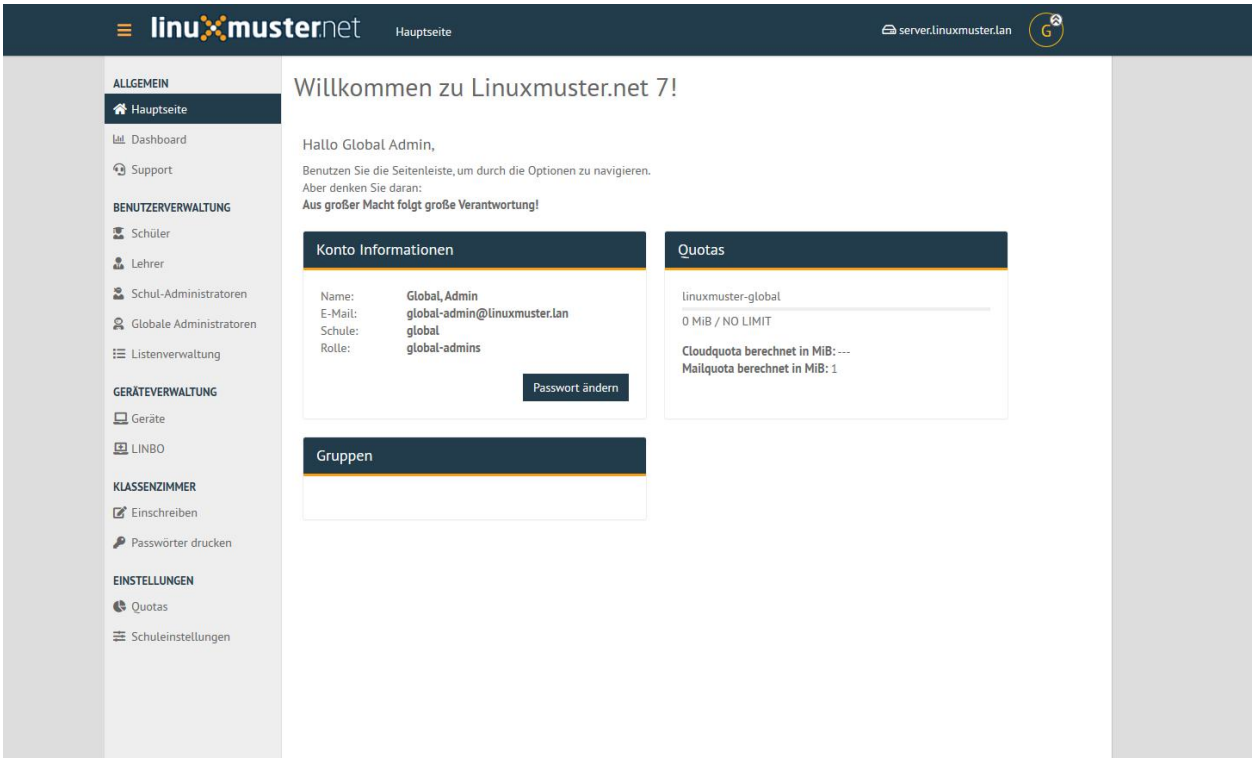
Die Icons haben folgende Bedeutung:

- 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.


linuxmuster.net
Schulkonsole > Hauptseite
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
Willkommen zu Linuxmuster.net 7!
global-admin
UID 0
Passwort ändern
Ausloggen
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.lan
Schule: global
Rolle: global-admins
Passwort ändern
Quotas
linuxmuster-global
0 MiB / UNBEGRENZT
Cloudquota berechnet in MB: ---
Mailquota berechnet in MB: 1 MB
Gruppen


linuxmuster.net
Hauptseite
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
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.lan
Schule: global
Rolle: global-admins
Passwort ändern
Quotas
linuxmuster-global
0 MiB / NO LIMIT
Cloudquota berechnet in MiB: ---
Mailquota berechnet in MiB: 1
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 hinzufügt/entfernt werden. Im Bereich Globale Administratoren können globale Admins verwaltet und hinzugefügt/entfernt werden.

Schüler, Lehrer, Schul-Administratoren, Globale Administratoren: Funktionen

Suche

In den jeweligen Benutzer-Bereichen kann in der intelligenten Filterleiste nach Benutzern mit Kriterien wie Namen, Klassen, Projekten gefiltert und gesucht werden.

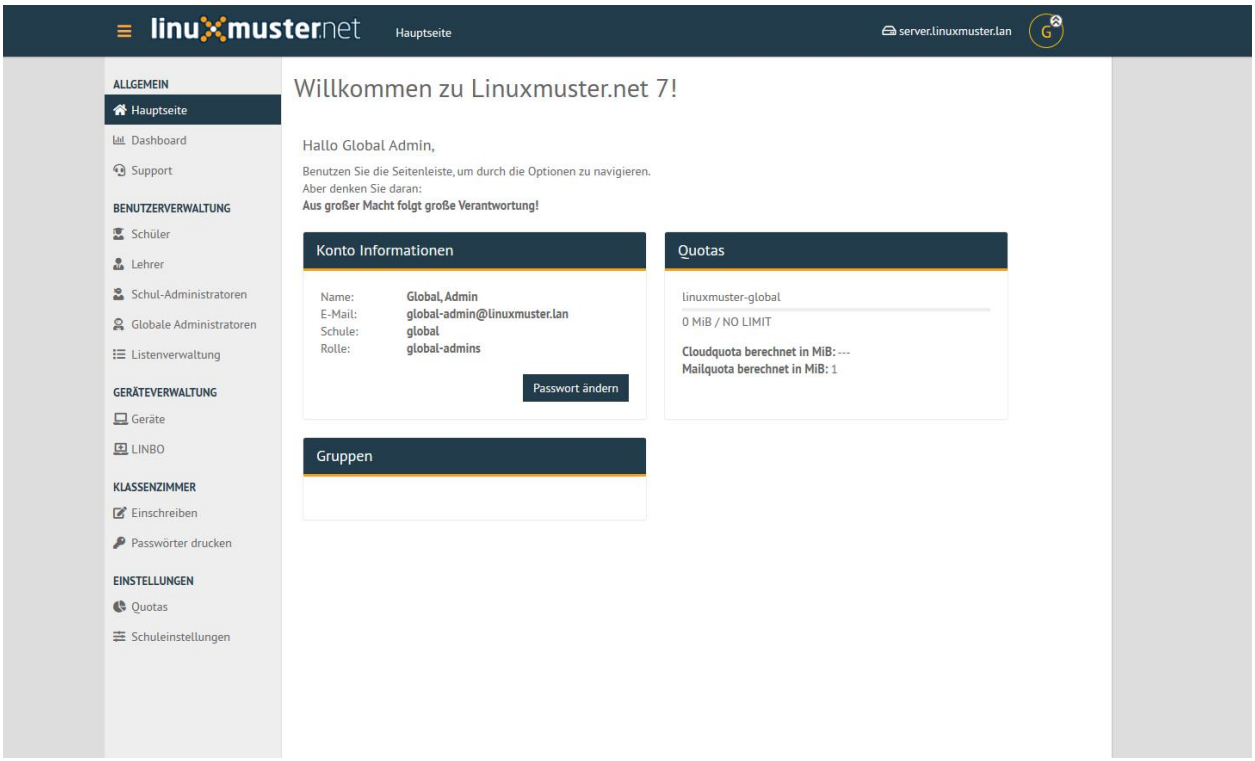
Passwort-Verwaltung

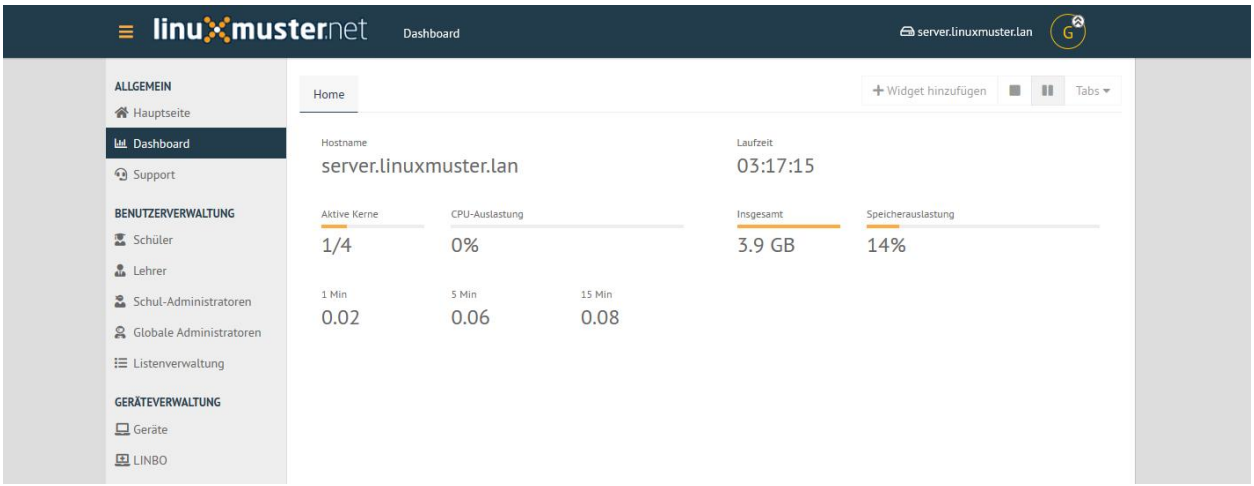
Zu einzelnen Benutzern gibt es die Möglichkeiten über das Passwort-Menü rechts neben dem jeweiligen Namen.

- Erstpasswort anzeigen
- Erstpasswort wiederherstellen
- Erstpasswort zufällig festlegen
- Erstpasswort benutzerdefiniert festlegen
- Benutzerpasswort festlegen

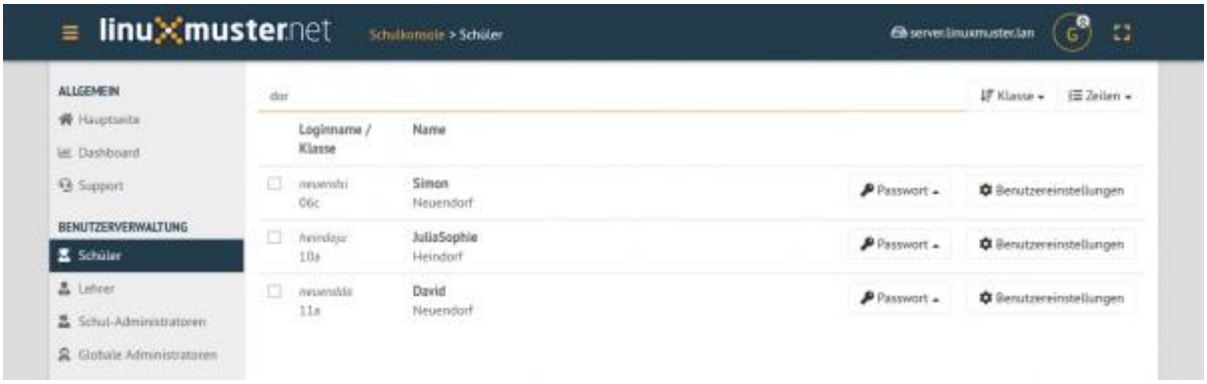
Durch Auswählen von mehreren Benutzern über Anklicken des Quadrats links neben dem Loginnamen oder über die Funktion `Alle auswählen`, können Funktionen auf mehrere Benutzer gleichzeitig angewendet werden.

- Setze Zufallspasswort für Ausgewählte
- Setze Erstpasswort für Ausgewählte


linuxmusternet
Hauptseite
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
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.lan
Schule: global
Rolle: global-admins
Passwort ändern
Quotas
linuxmuster-global
0 MiB / NO LIMIT
Cloudquota berechnet in MiB: ---
Mailquota berechnet in MiB: 1
Gruppen


linuxmusternet
Dashboard
server.linuxmuster.lan
ALLGEMEIN
Hauptseite
Dashboard
Support
BENUTZERVERWALTUNG
Schüler
Lehrer
Schul-Administratoren
Globale Administratoren
Listenverwaltung
GERÄTEVERWALTUNG
Geräte
LINBO
Home
+ Widget hinzufügen
Tabs
Hostname
server.linuxmuster.lan
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


BENUTZERVERWALTUNG
Schüler
Lehrer
Schul-Administratoren
Globale Administratoren
Listenverwaltung

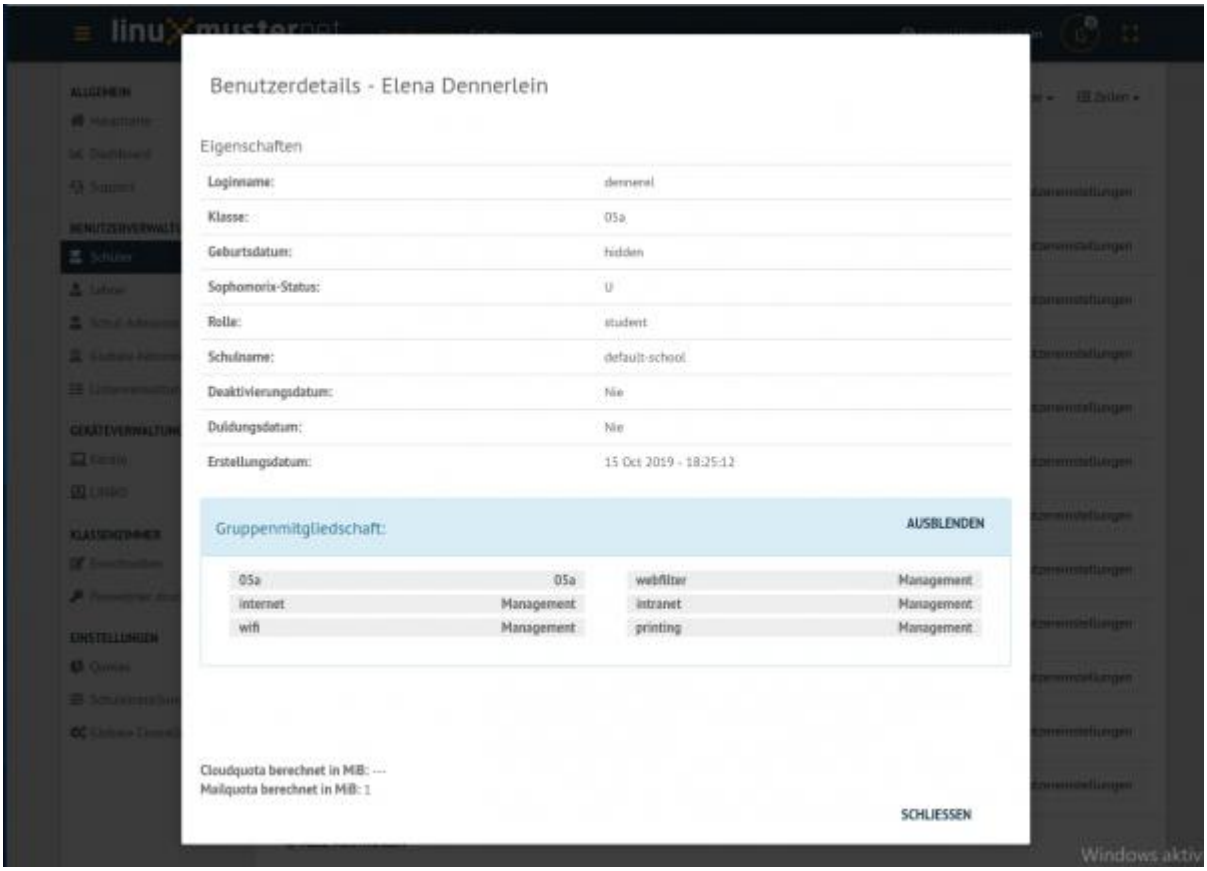

linuxmuster.net
Schulkonsole > Schüler
server.linuxmuster.lan
ALLGEMEIN
Hauptseite
Dashboard
Support
BENUTZERVERWALTUNG
Schüler
Lehrer
Schul-Administratoren
Globale Administratoren
Klasse
Zeilen
Loginname / Klasse
Name
Simon
Neuendorf
Passwort
Benutzereinstellungen
JuliaSophie
Heindorf
David
Neuendorf


Klasse
Zeilen
Loginname / Klasse
Name
Erstpasswort anzeigen
Erstpasswort wiederherstellen
Erstpasswort zufällig festlegen
Erstpasswort benutzerdefiniert festlegen
Benutzerpasswort festlegen
Simon
Neuendorf
Benutzereinstellungen
JuliaSophie
Heindorf
Benutzereinstellungen
David
Neuendorf
Passwort
Benutzereinstellungen

- 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.

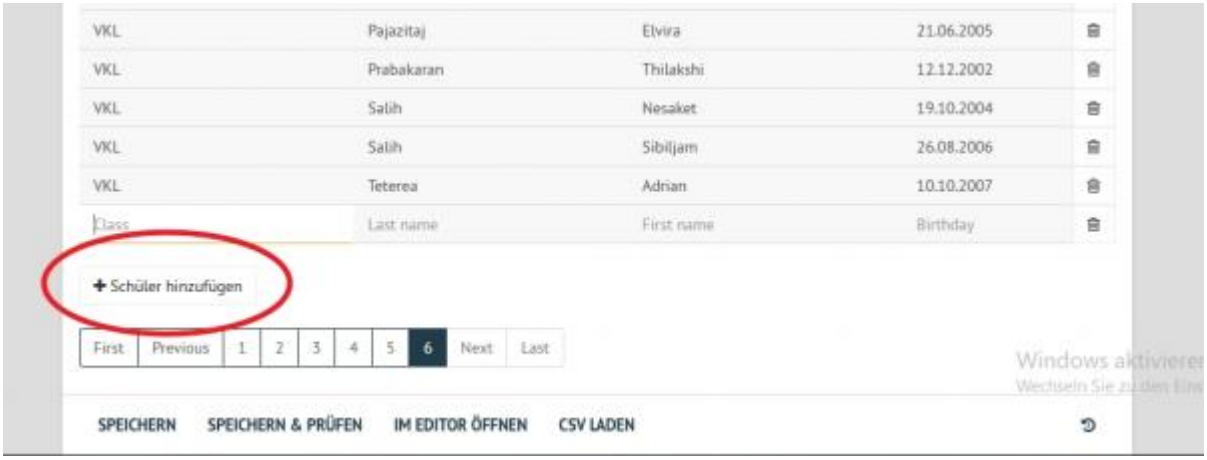


Listenverwaltung

In der Listenverwaltung können Benutzer von Schülern, Lehrern, und Extra-Schülern verwaltet werden, das bedeutet hinzugefügt, entfernet 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.



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.

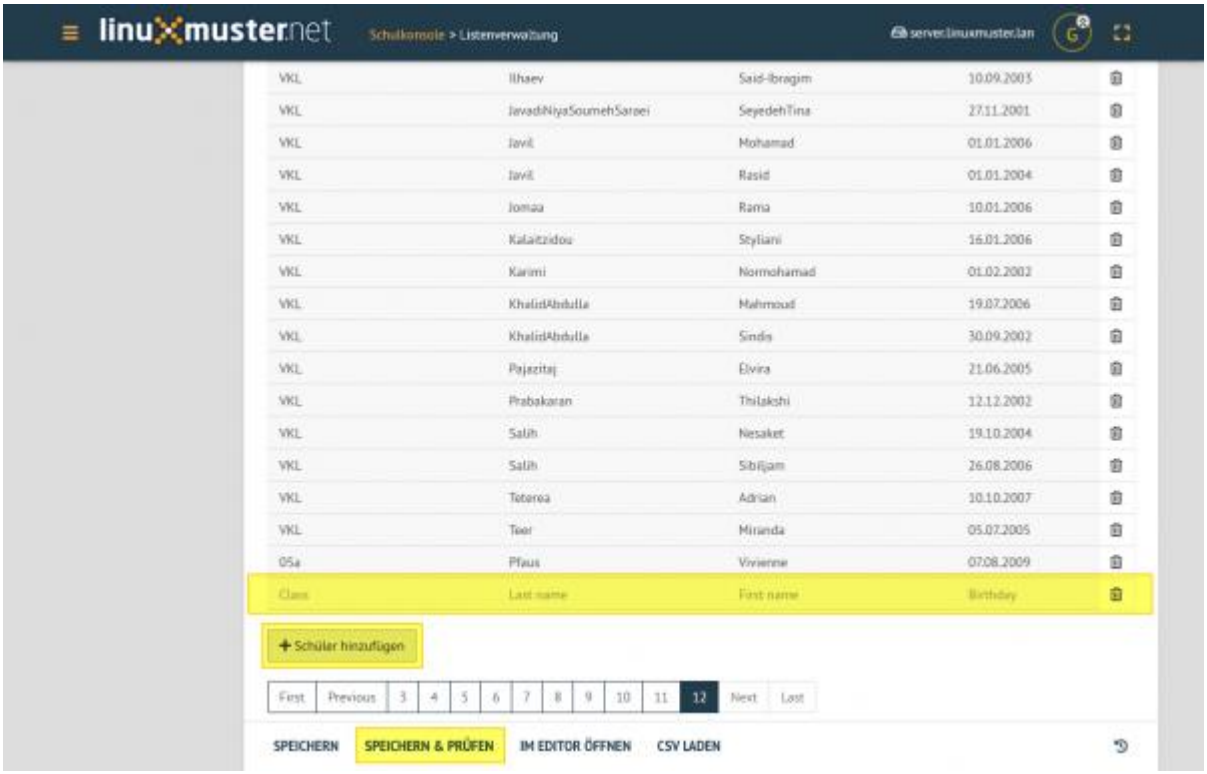
Benutzeraufnahme über vorhandene CSV-Datei

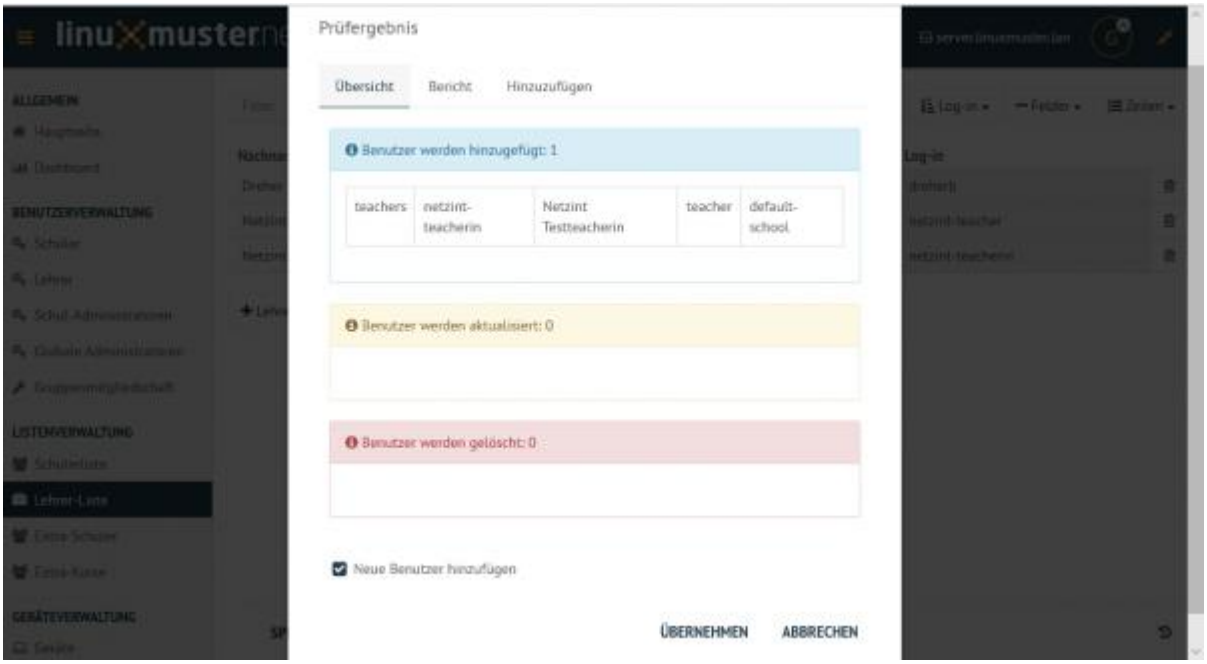
Über die integrierte Funktion, Benutzer simpel über eine CSV-Datei zu übernehmen und anzupassen, können so zahlreiche Benutzer schnell aufgenommen werden. Dafür in einer bestimmten Benutzerliste über die Funktion in der unteren Menüleiste CSV laden auswählen und die CSV-Datei hochladen.

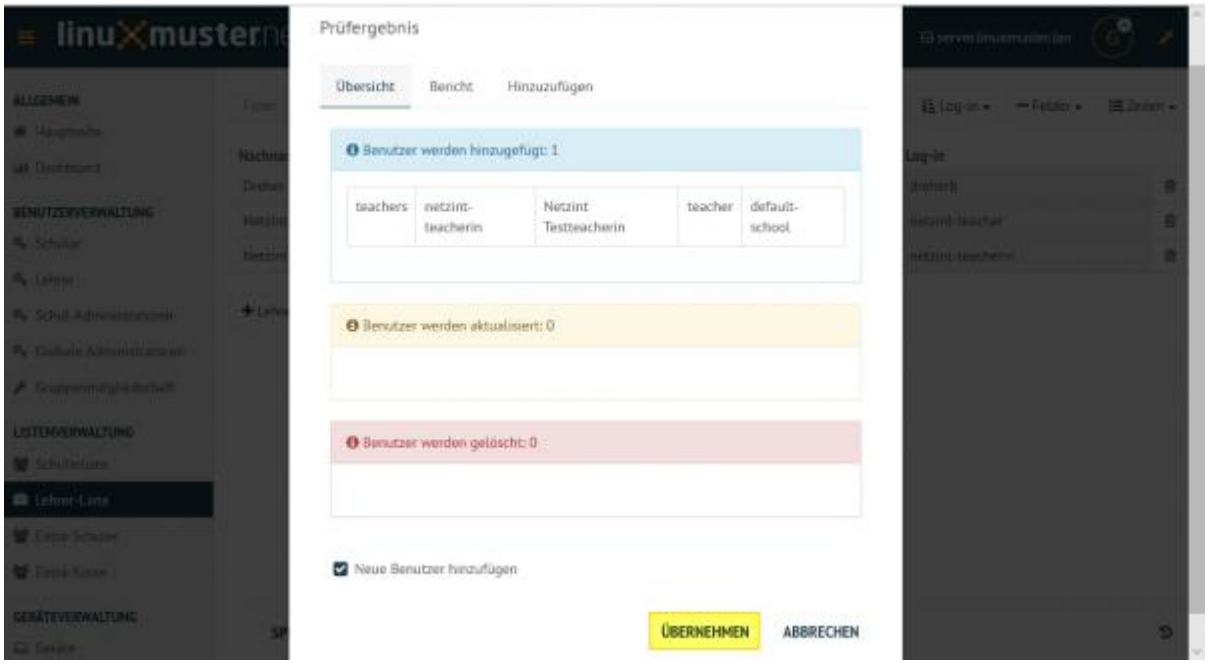
Falls die Spalten nicht in der richtigen Reihenfolge aufgelistet sind, gibt es die Möglichkeit diese graphisch per Ziehen mit der Maus umzuordnen, bevor sie mit Sortierung akzeptieren in die Liste übernommen werden.

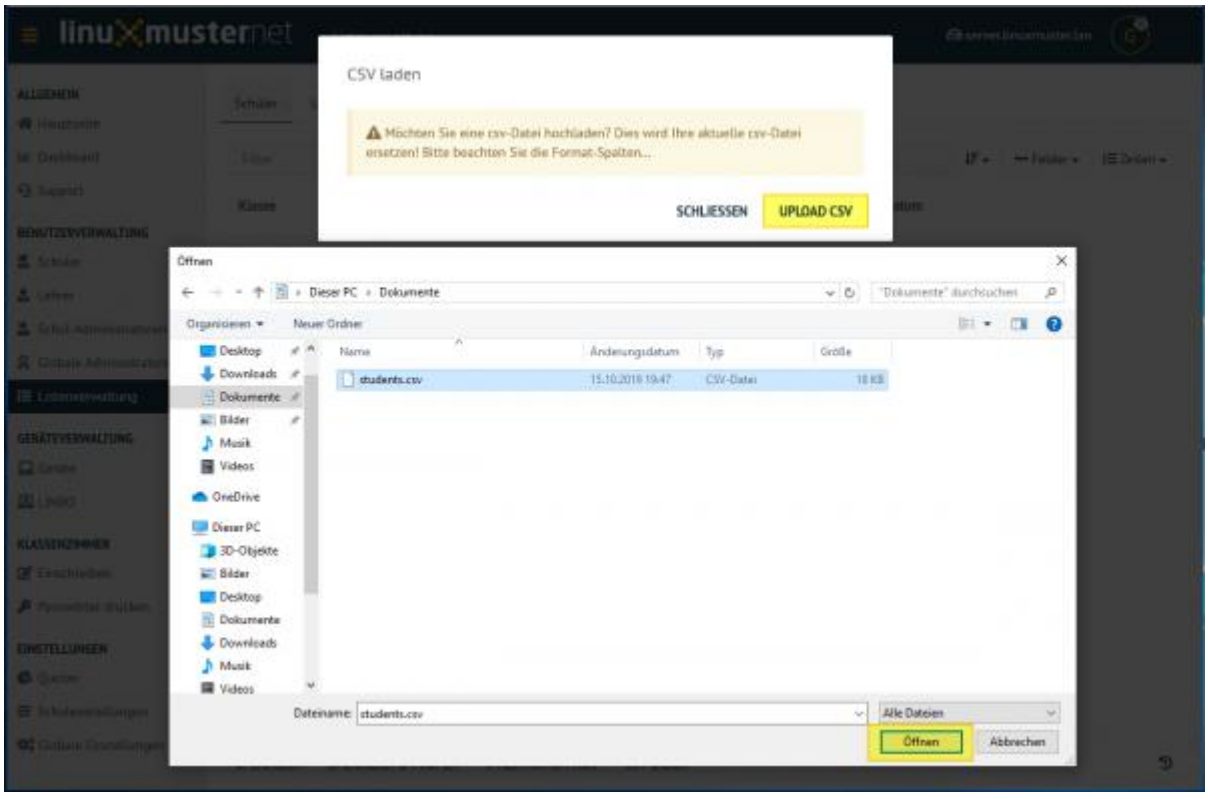
Falls die Spalten nicht in der richtigen Reihenfolge aufgelistet sind, gibt es die Möglichkeit diese graphisch per Ziehen mit der Maus umzuordnen, bevor sie mit Sortierung akzeptieren in die Liste übernommen werden.

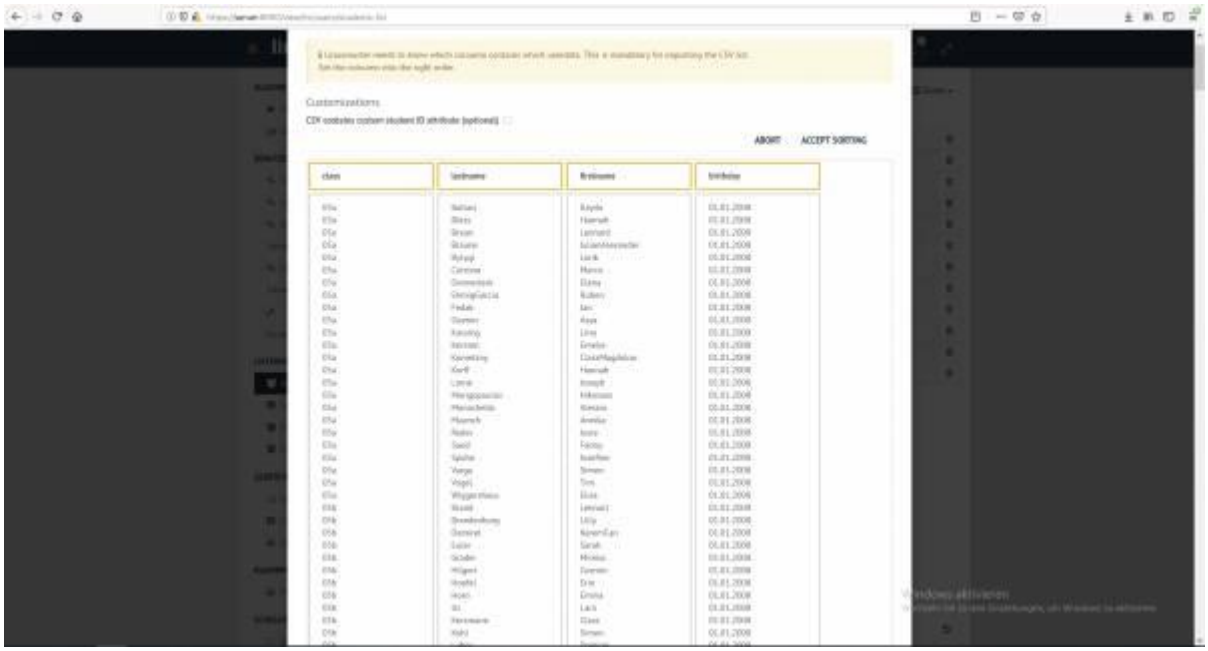
Anschließend `Speichern & Überprüfen` und ganz unten auf der Listenübersicht (gegebenfalls runterscrollen) Übernehmen.


linuxmuster.net
Schulkonsole > Listenverwaltung
server.linuxmuster.lan
VKL Ilhaev Said-Ibragim 10.09.2003
VKL JavadiNiyaSoumehSaraei SeyedehTina 27.11.2001
VKL Javil Mohamad 01.01.2006
VKL Javil Rasid 01.01.2004
VKL Jomaa Rama 10.01.2006
VKL Kalaitzidou Styliani 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 Sibiljam 26.08.2006
VKL Toterea Adrian 10.10.2007
VKL Teer Miranda 05.07.2005
05a 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


Prüfergebnis
Übersicht
Bericht
Hinzuzufügen
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


Prüfergebnis
Übersicht
Bericht
Hinzuzufügen
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

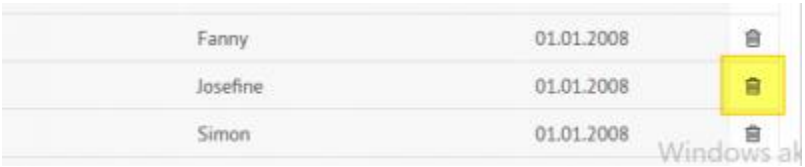

CSV laden
Möchten Sie eine csv-Datei hochladen? Dies wird Ihre aktuelle csv-Datei ersetzen! Bitte beachten Sie die Format-Spalten...
SCHLIESSEN
UPLOAD CSV
Öffnen
Dieser PC › Dokumente
Organisieren
Neuer Ordner
Desktop
Downloads
Dokumente
Bilder
Musik
Videos
OneDrive
Dieser PC
3D-Objekte
Name
Änderungsdatum
Typ
Größe
students.csv
15.10.2018 19:47
CSV-Datei
18 KB
Dateiname: students.csv
Alle Dateien
Öffnen
Abbrechen



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 angebunden Geräte inklusiver Informationen und der Möglichkeit diese zu ändern, weitere Geräte hinzuzufügen oder zu entfernen. Weiter finden Sie das LINBO-Menü zu desen 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)

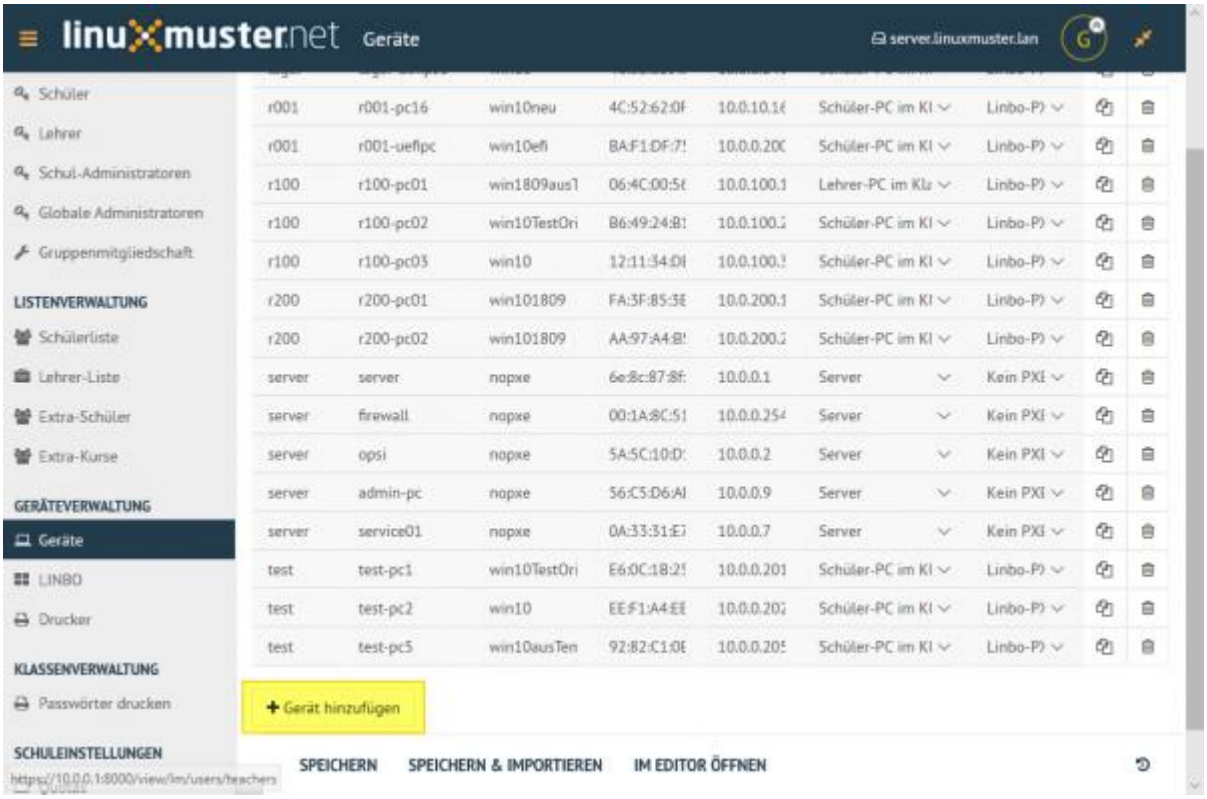
Gerät hinzufügen

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.

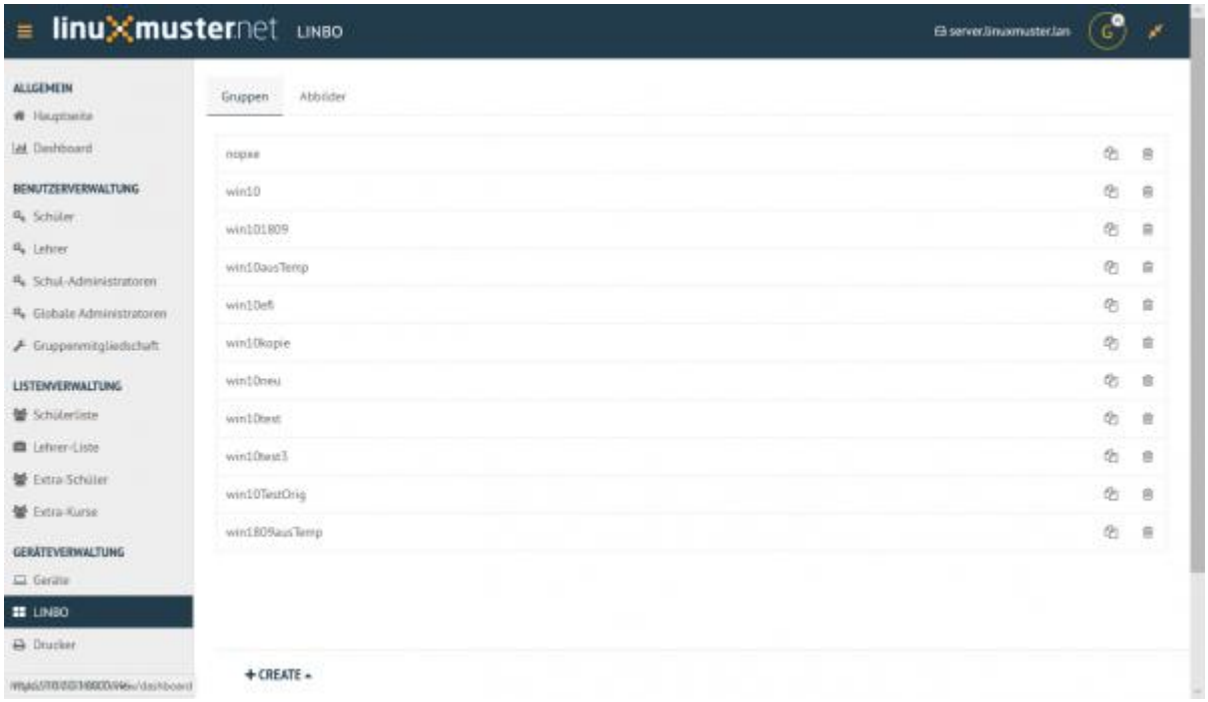
Geräteansicht

- 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.


linuxmusternet
Geräte
server.linuxmuster.lan
Schüler
Lehrer
Schul-Administratoren
Globale Administratoren
Gruppenmitgliedschaft
LISTENVERWALTUNG
Schülerliste
Lehrer-Liste
Extra-Schüler
Extra-Kurse
GERÄTEVERWALTUNG
Geräte
LINBO
Drucker
KLASSENVERWALTUNG
Passwörter drucken
SCHULEINSTELLUNGEN
r001 r001-pc16 win10neu 4C:52:62:0F 10.0.10.1 Schüler-PC im KI Linbo-P)
r001 r001-ueflpc win10efi BA:F1:DF:7! 10.0.0.20 Schüler-PC im KI Linbo-P)
r100 r100-pc01 win1809aus1 06:4C:00:5 10.0.100.1 Lehrer-PC im Klz Linbo-P)
r100 r100-pc02 win10TestOri B6:49:24:B 10.0.100.2 Schüler-PC im KI Linbo-P)
r100 r100-pc03 win10 12:11:34:D 10.0.100.3 Schüler-PC im KI Linbo-P)
r200 r200-pc01 win101809 FA:3F:85:3 10.0.200.1 Schüler-PC im KI Linbo-P)
r200 r200-pc02 win101809 AA:97:A4:B 10.0.200.2 Schüler-PC im KI 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:A 10.0.0.9 Server Kein PXI
server service01 nopxe 0A:33:31:E 10.0.0.7 Server Kein PXI
test test-pc1 win10TestOri E6:0C:18:2 10.0.0.201 Schüler-PC im KI Linbo-P)
test test-pc2 win10 EE:F1:A4:E 10.0.0.202 Schüler-PC im KI Linbo-P)
test test-pc5 win10ausTen 92:82:C1:0 10.0.0.205 Schüler-PC im KI Linbo-P)
+ Gerät hinzufügen
SPEICHERN
SPEICHERN & IMPORTIEREN
IM EDITOR ÖFFNEN


Filter
Raum
Felder
Zeilen
Raum Hostname Gruppe MAC IP Sophomorix-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 Gerätelistenverwaltung 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.

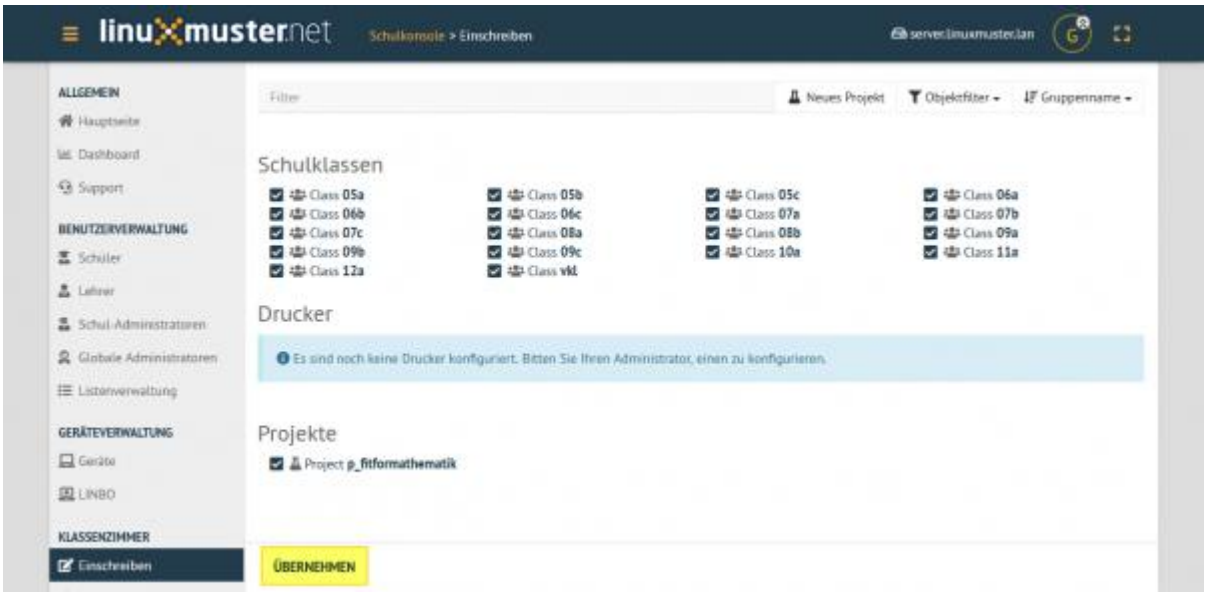
Ein jeweiliges Objekt zum Einschreiben auswählen oder den Haken entfernen um daraus auszutreten. Geänderte Einstellungen werden gelb angezeigt. Um die Änderungen anzuwenden, auf **Übernehmen** klicken.

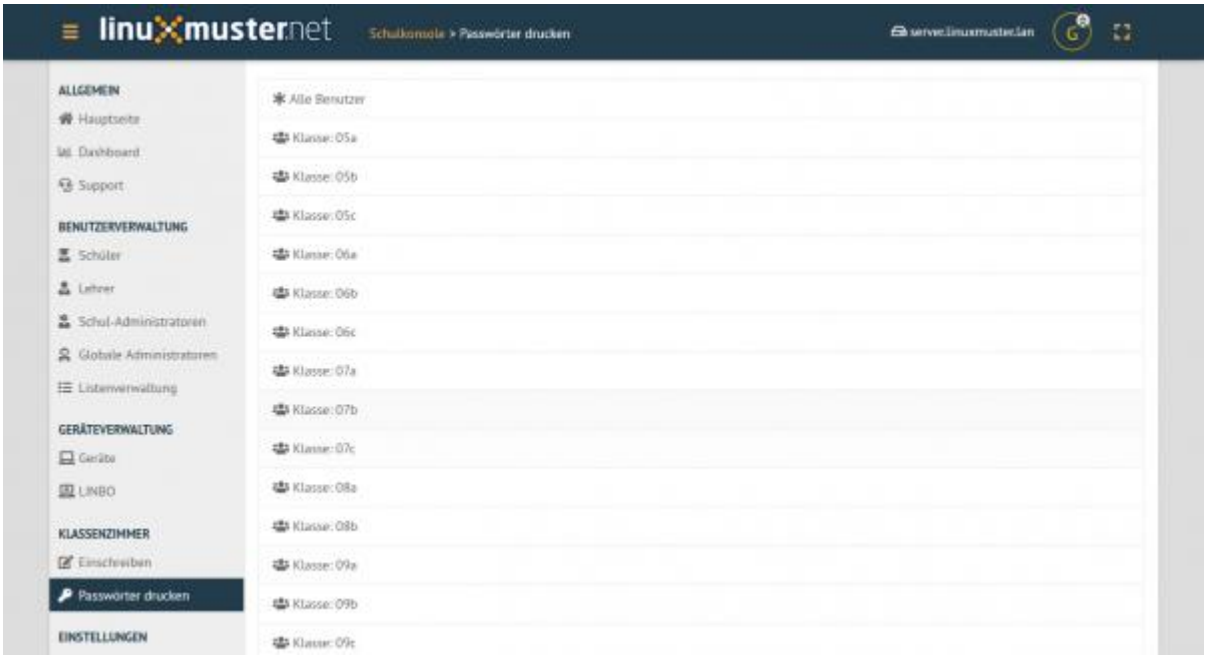
Passwörter drucken

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
Schulkonsole > Einschreiben
server.linuxmuster.lan
ALLGEMEIN
Hauptseite
Dashboard
Support
BENUTZERVERWALTUNG
Schüler
Lehrer
Schul-Administratoren
Globale Administratoren
Listenverwaltung
GERÄTEVERWALTUNG
Geräte
LINBO
KLASSENZIMMER
Einschreiben
Filter
Neues Projekt
Objektfilter
Gruppenname
Schulklassen
Class 05a
Class 05b
Class 05c
Class 06a
Class 06b
Class 06c
Class 07a
Class 07b
Class 07c
Class 08a
Class 08b
Class 09a
Class 09b
Class 09c
Class 10a
Class 11a
Class 12a
Class vkl
Drucker
Es sind noch keine Drucker konfiguriert. Bitten Sie Ihren Administrator, einen zu konfigurieren.
Projekte
Project p_fitformathematik
ÜBERNEHMEN


linuxmuster.net
Schulkonsole > Passwörter drucken
server.linuxmuster.lan
ALLGEMEIN
Hauptseite
Dashboard
Support
BENUTZERVERWALTUNG
Schüler
Lehrer
Schul-Administratoren
Globale Administratoren
Listenverwaltung
GERÄTEVERWALTUNG
Geräte
LINBO
KLASSENZIMMER
Einschreiben
Passwörter drucken
EINSTELLUNGEN
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

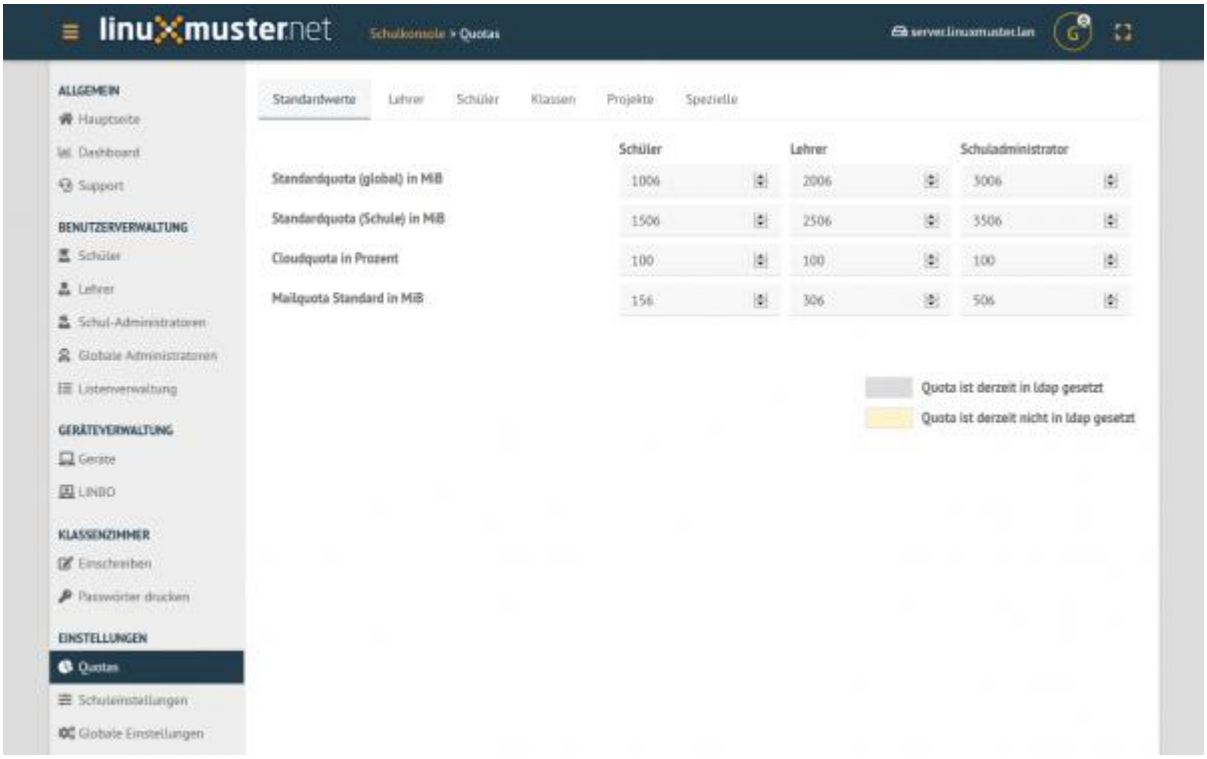
Zugangsdatenliste 10a 29. April 2019

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.

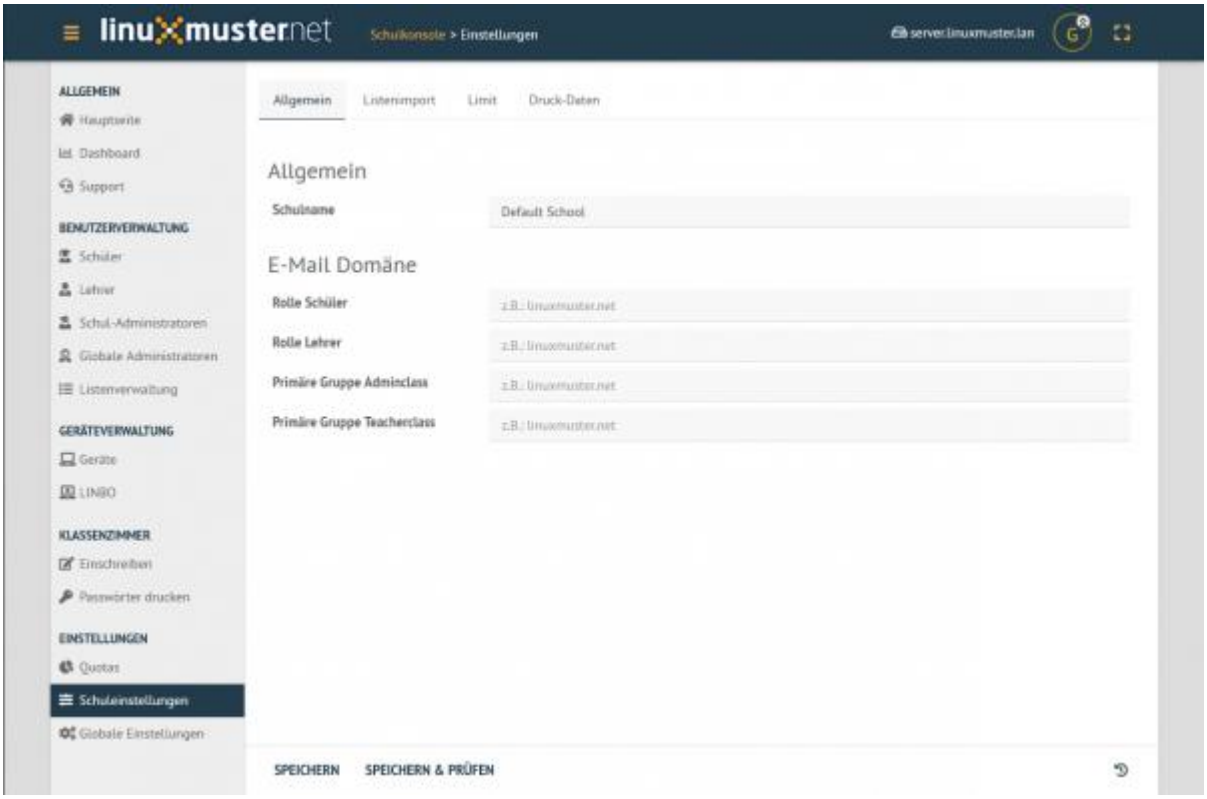


In den Bereichen **Lehrer** und **Schüler** daneben können von den Standwartwerten abweichend pro Benutzer eigene Werte eingestellt werden. Ebenso kann unter **Klassen** und **Projekte** einer jeweiligen Schulklasse/einem jeweiligen Projekt die Speichergröße festgelegt werden.

4.36.7 Schuleinstellungen

Allgemeine Informationen, Einstellungen zum Linstenimport, 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.

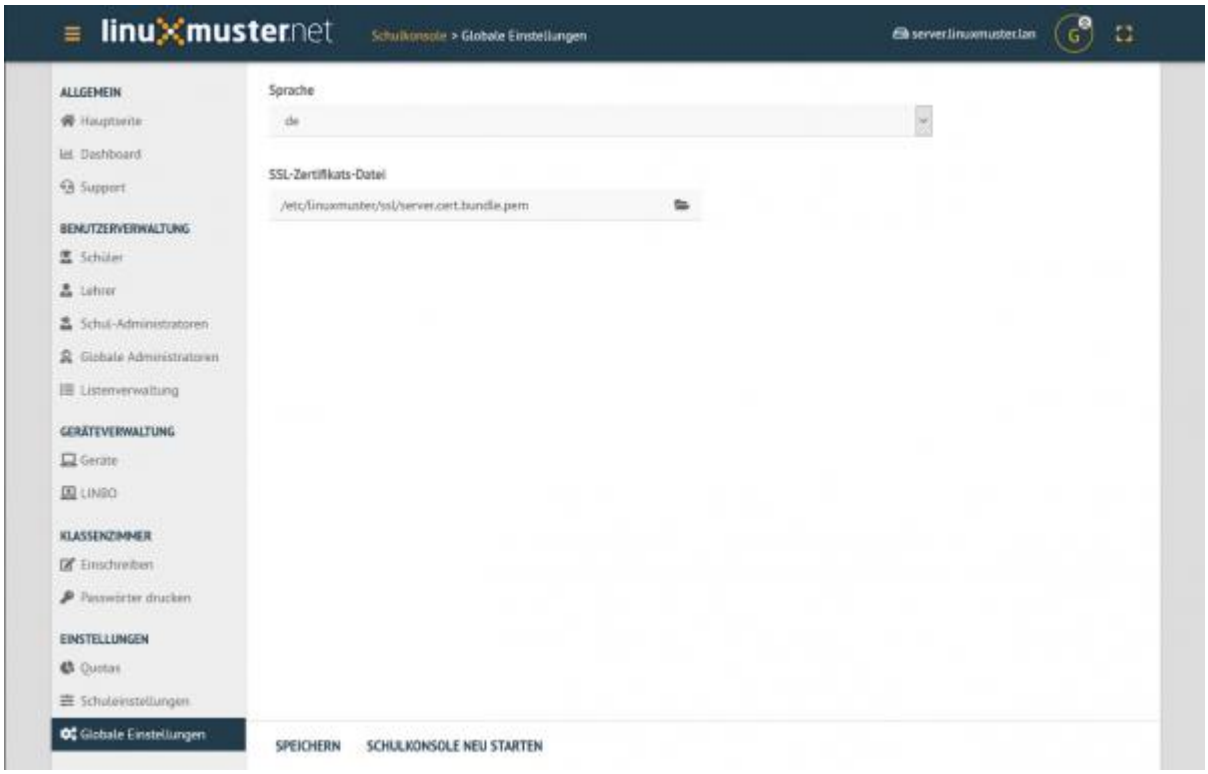


Änderungen über Speichern & Prüfen und anschließend Übernehmen anwenden. Unter Listenimport können Standardwerte festgelegt werden, die beim Import einer CSV-Datei angewendet werden. Wird ein Haken unter der Funktion Nachname und Vorname im Benutzernamen umkehren für eine jeweilige Rolle, werden die 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)

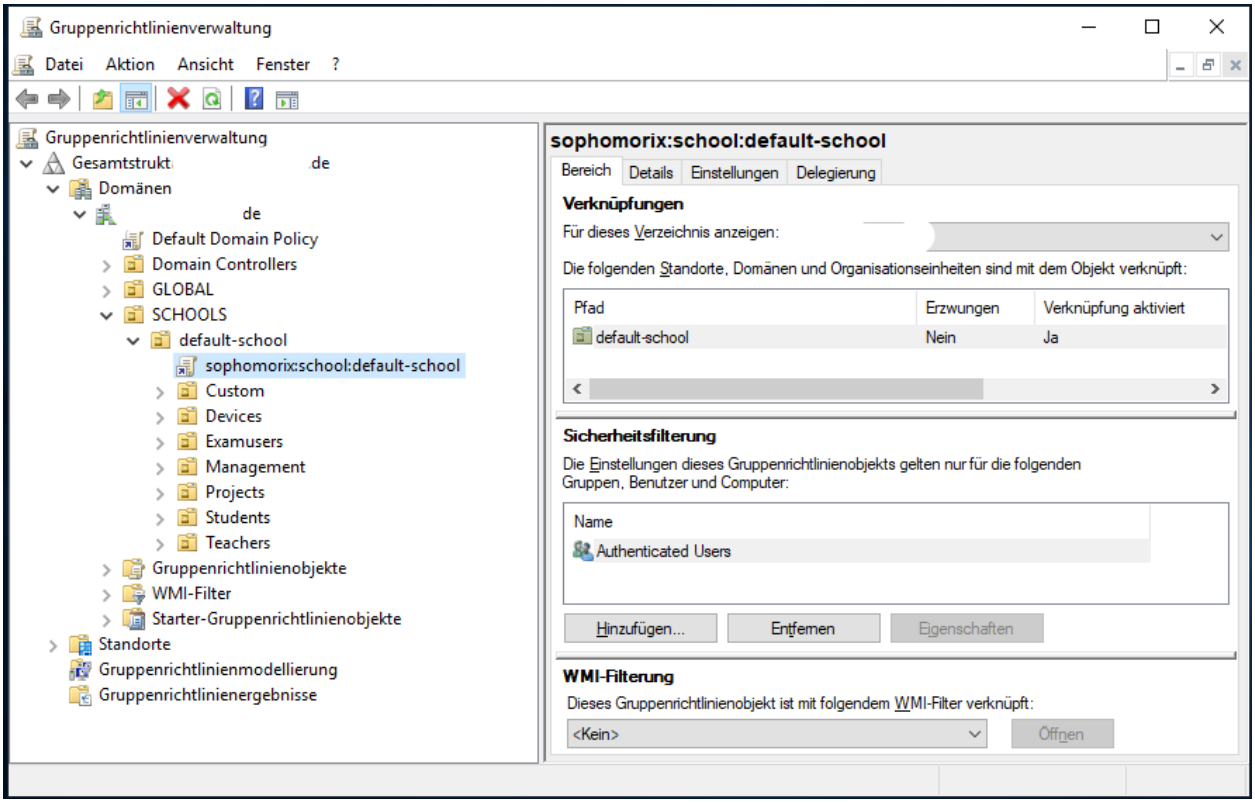
Zur Verwaltung des Active Directory (AD) benötigt man die Microsoft Remote Server Administration Tools (RSAT). Diese werden von Microsoft bereitgestellt. (Home-Versionen von Windows werden nicht unterstützt!)

Für Windows10-Versionen vor 1809 müssen diese noch als separtes Installationspaket heruntergeladen werden: https://www.microsoft.com/en-us/download/details.aspx?id=45520

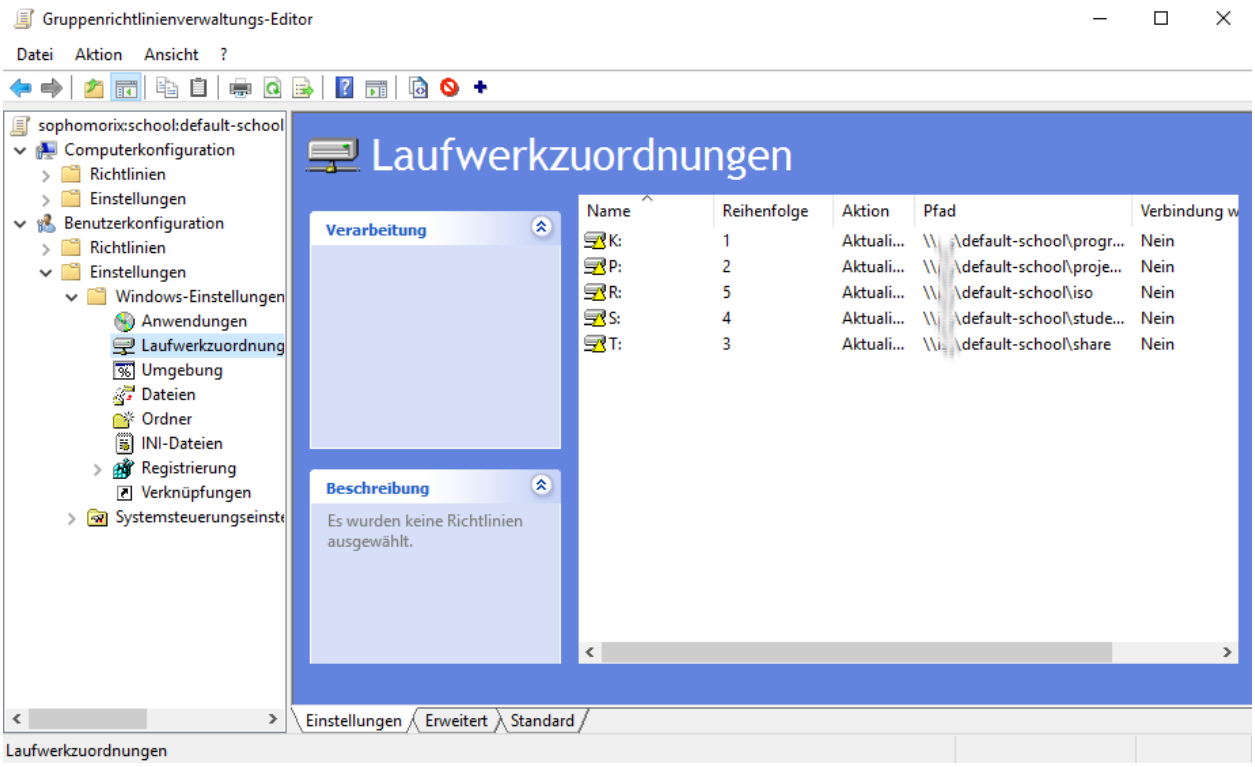
Ab Version 1809 sind die RSAT ein optionales Feature. Die Installation erfolgt über `Start` -> `Apps und Features` -> `optionale Features` -> `Feature hinzufügen` -> `RSAT: Group Policy Management Tools`.

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:

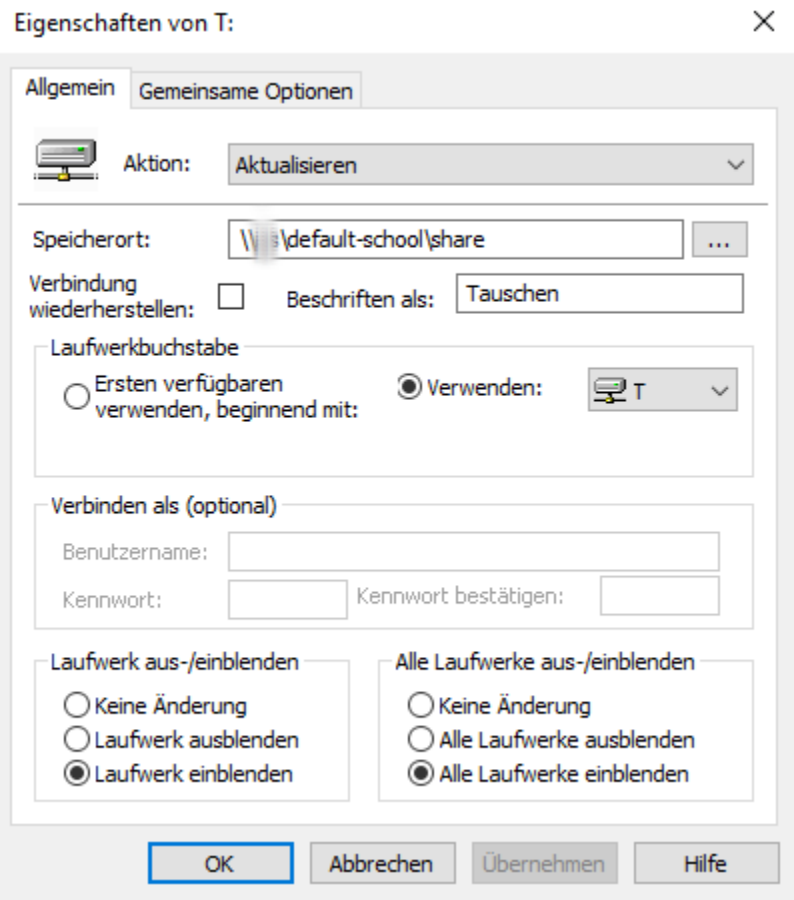


Hinweis: Sollte die Standard-GPO „sophomorix:school:default-school“ nicht vorhanden sein, dann kann diese auf dem Server erzeugt werden durch Eingabe von: `sophomorix-school --gpo-create default-school`.

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

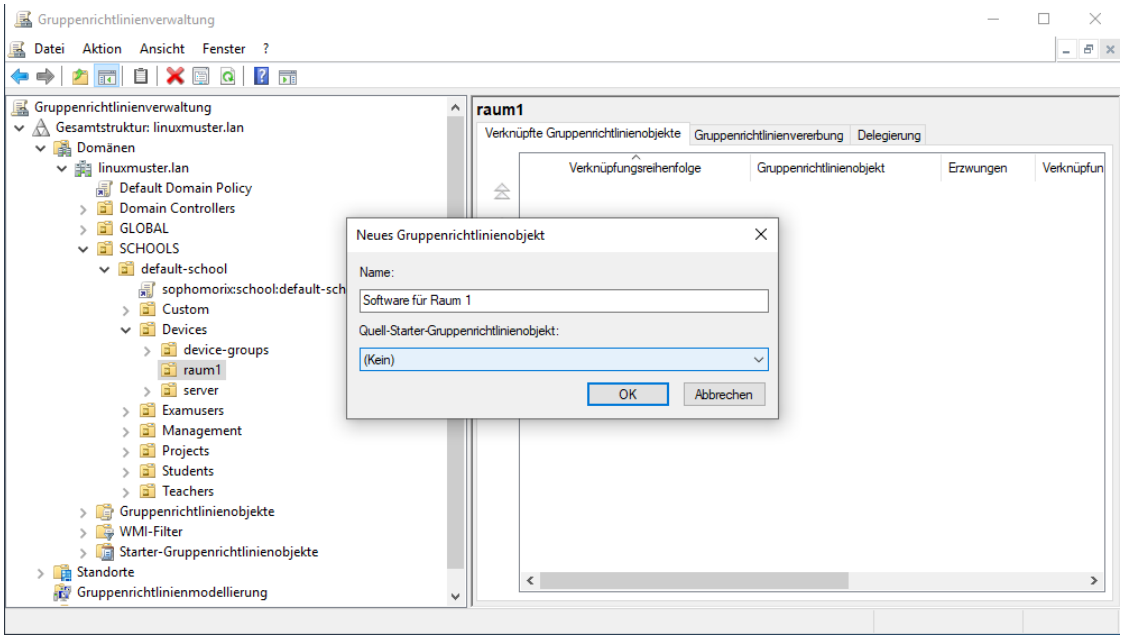
Über GPOs können drei Arten von Paketen installiert werden: Windows-Installationspakete mit der Dateiendung .MSI, Transformationsdateien mit der Dateiendung .MST und Patch-Dateien, die auf .MSP enden.

Software kann an Computer oder User verteilt werden. In diesem Beispiel erfolgt die Verteilung an die Computer in einem bestimmten Raum.

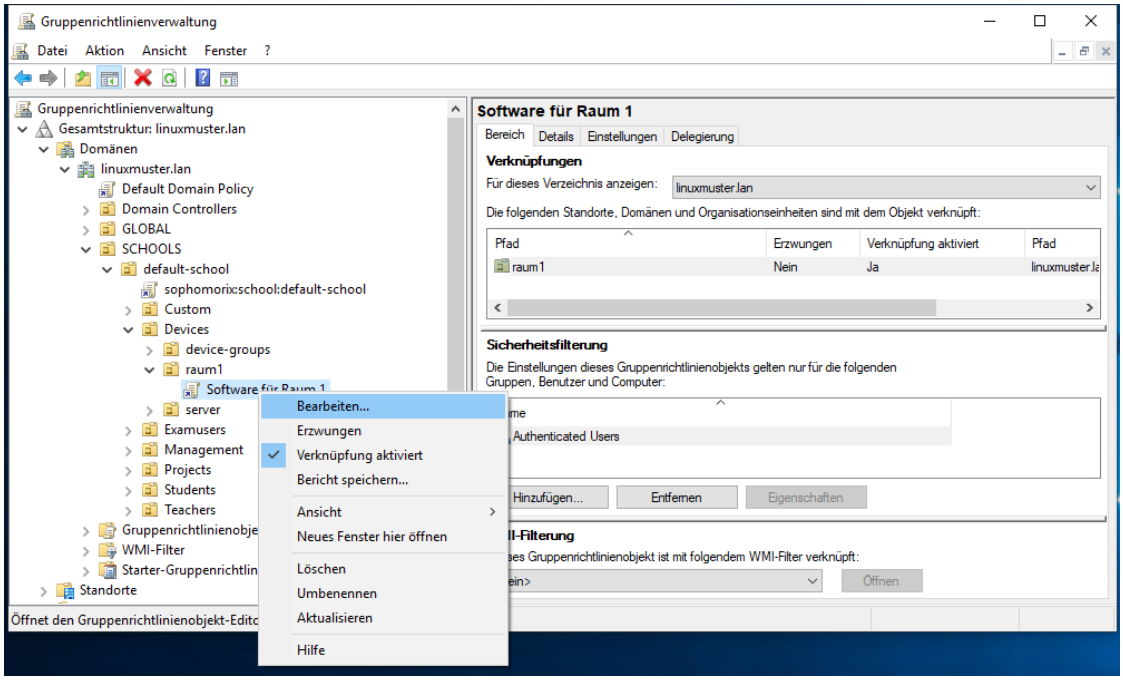
Zunächst sollte die Software auf einem UNC-Pfad abgelegt werden, von dem aus die Installation ausgeführt werden kann. Das Server-Share `\\server\default-school\program` ist ungeeignet. Besser: `\\server\sysvol\domänenname\`. Hier einen Unterordner `Software` erstellen und die MSI-Pakete ablegen.

4.38.1 Neue GPO erzeugen

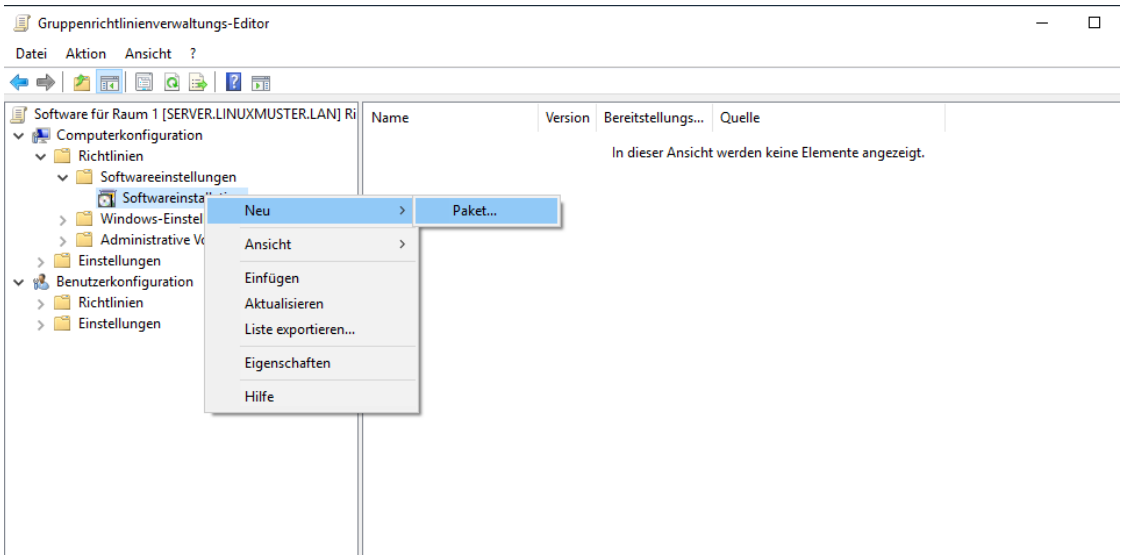
Melde Dich an einem PC mit `global-admin` an und starte die `Gruppenrichtlinienverwaltung`. Klappe den Baum auf bis zum gewünschten Raum. Mache einen Rechtsklick auf den gewünschten Raum und wähle `Gruppenrichtlinienobjekt hier erstellen und verknüpfen`. Im folgenden Fenster einen sinnvollen Namen vergeben (z.B. Software für Raum X) und mit `OK` bestätigen.



Nun muss die neue GPO noch bearbeitet werden. Mache dazu einen Rerchtsklick darauf und wähle `Bearbeiten`.



Der Gruppenrichtlinienverwaltungs-Editor öffnet sich. Gehe zu: `Computerkonfiguration` -> `Richtlinien` -> `Softwareeinstellungen` -> `Softwareinstallation`



Mache einen Rechtsklick auf `Softwareinstallation` und wähle `Neu` -> `Paket`. Gibt den UNC-Pfad zum Paket ein. Wichtig: Das Paket muss an einer Stelle liegen, auf die der Ziel-Computer Zugriff hat! Darauf weißt 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.

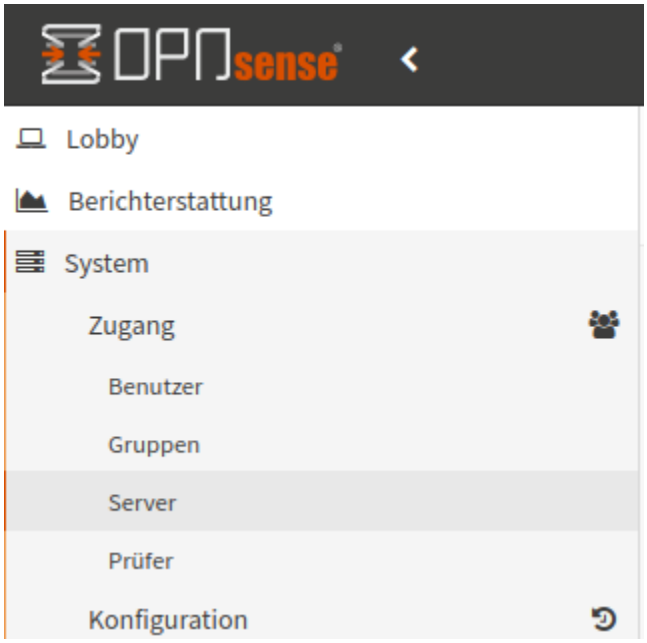
4.39.1 Voraussetzungen

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:

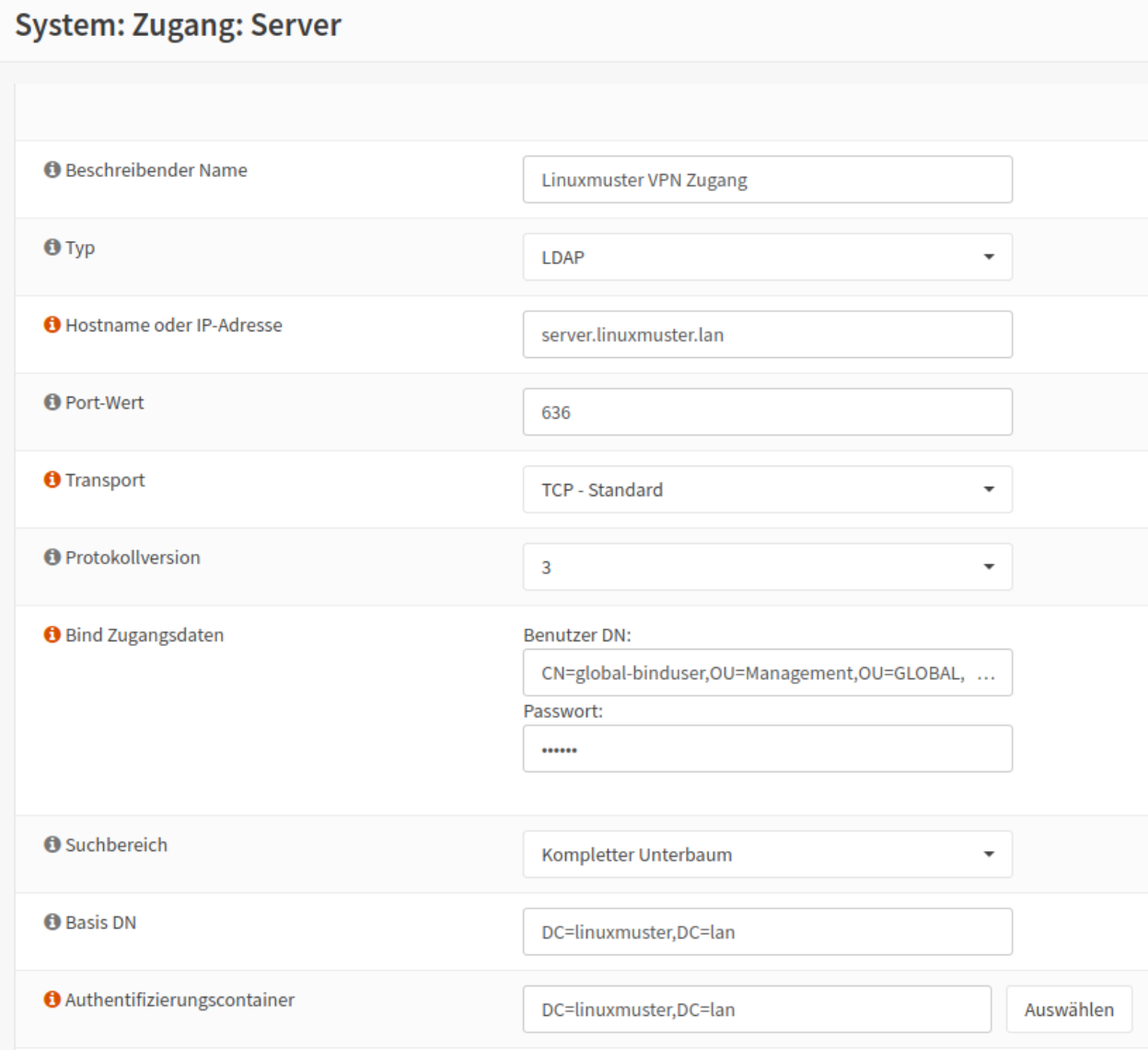
```
Benutzer DN: CN=global-binduser,OU=Management,OU=GLOBAL,DC=linuxmuster,DC=lan
Suchbereich: Kompletter Unterbaum
```

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:



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)
```

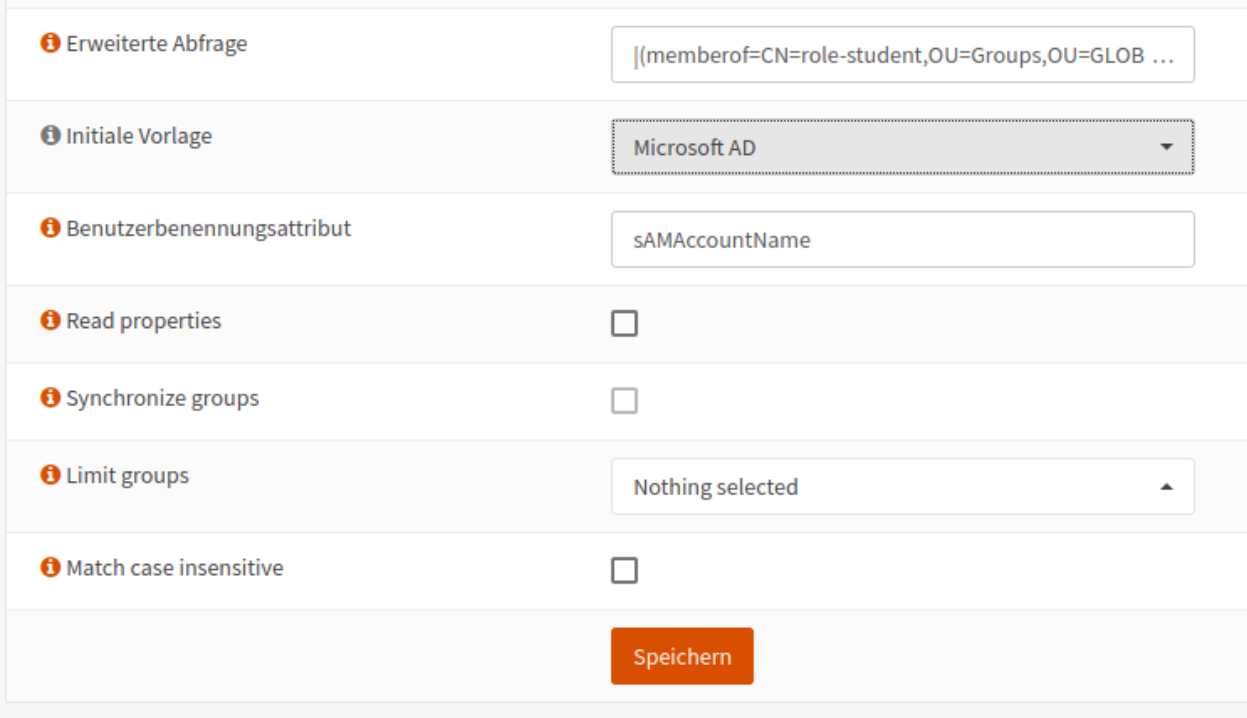
O D E R

Erweiterte Abfrage: `Nur Lehrer`:

```
(memberof=CN=role-teacher,OU=Groups,OU=GLOBAL,DC=linuxmuster,DC=lan)
```

11. Benutzerbennenungsattribut: `sAMAccountName`

Nachstehende Abb. verdeutlicht die Anwendung der o.g. Einstellungen:



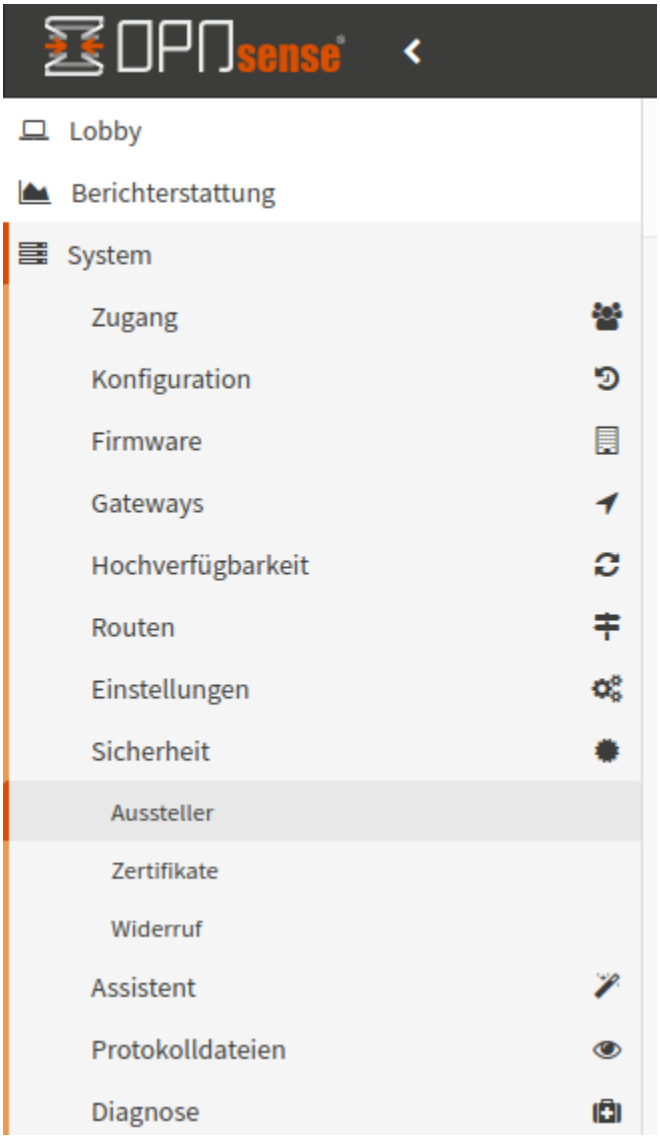
Danach sollte der Login mit beliebigen Nutzern getestet werden. Erst nachdem die Tests erfolgreich waren fortgahren. Dies kann unter `System > Zugang > Prüfer` und der Auswahl des vorhin angelegten Authentifizierungsservers für den Linuxmuster VPN-Zugang erfolgen.

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.

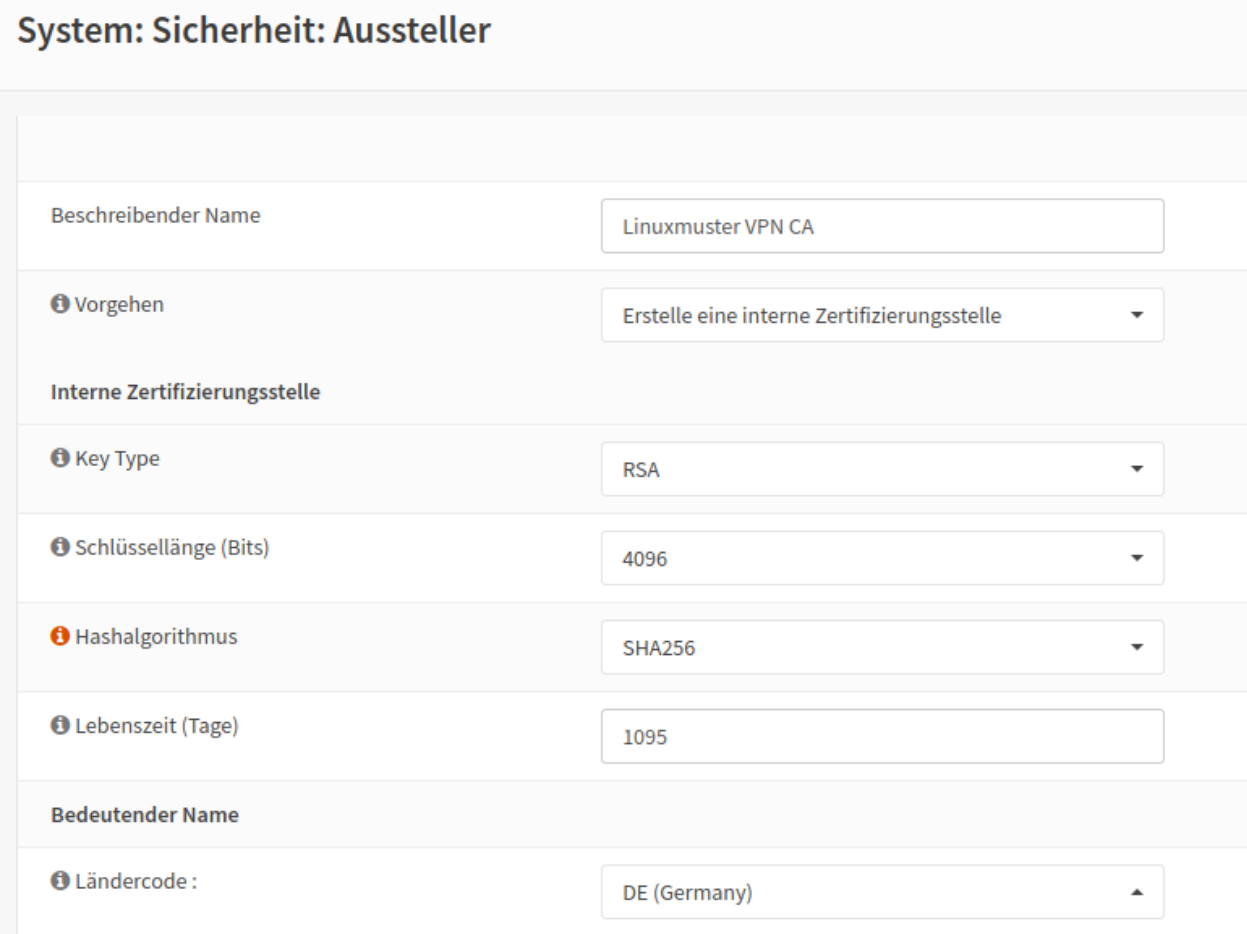
CA erstellen

Unter `System –> Zugang –> Sicherheit –> Aussteller`



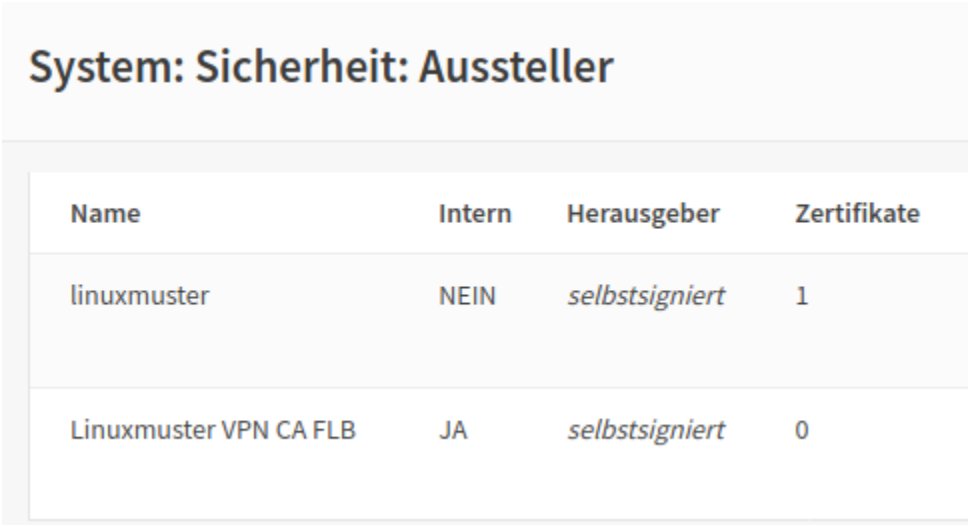
ist ein Aussteller hinzuzufügen (oben rechts). Es sind folgende Einstellungen vorzunehmen:

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>



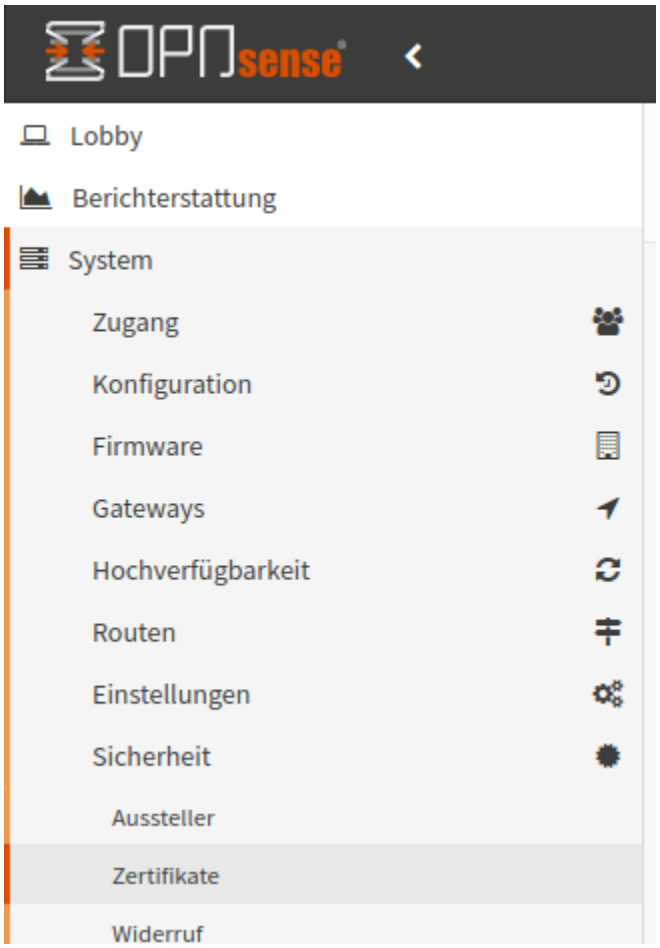
7. Bedeutender Name: <dein bedeutender Name für die CA>

Die erstellte CA findet sich unter `System` –> `Zugang` –> `Sicherheit` –> `Aussteller` wie in nachstehender Abb. dargestellt:



Zertifikat hinzufügen

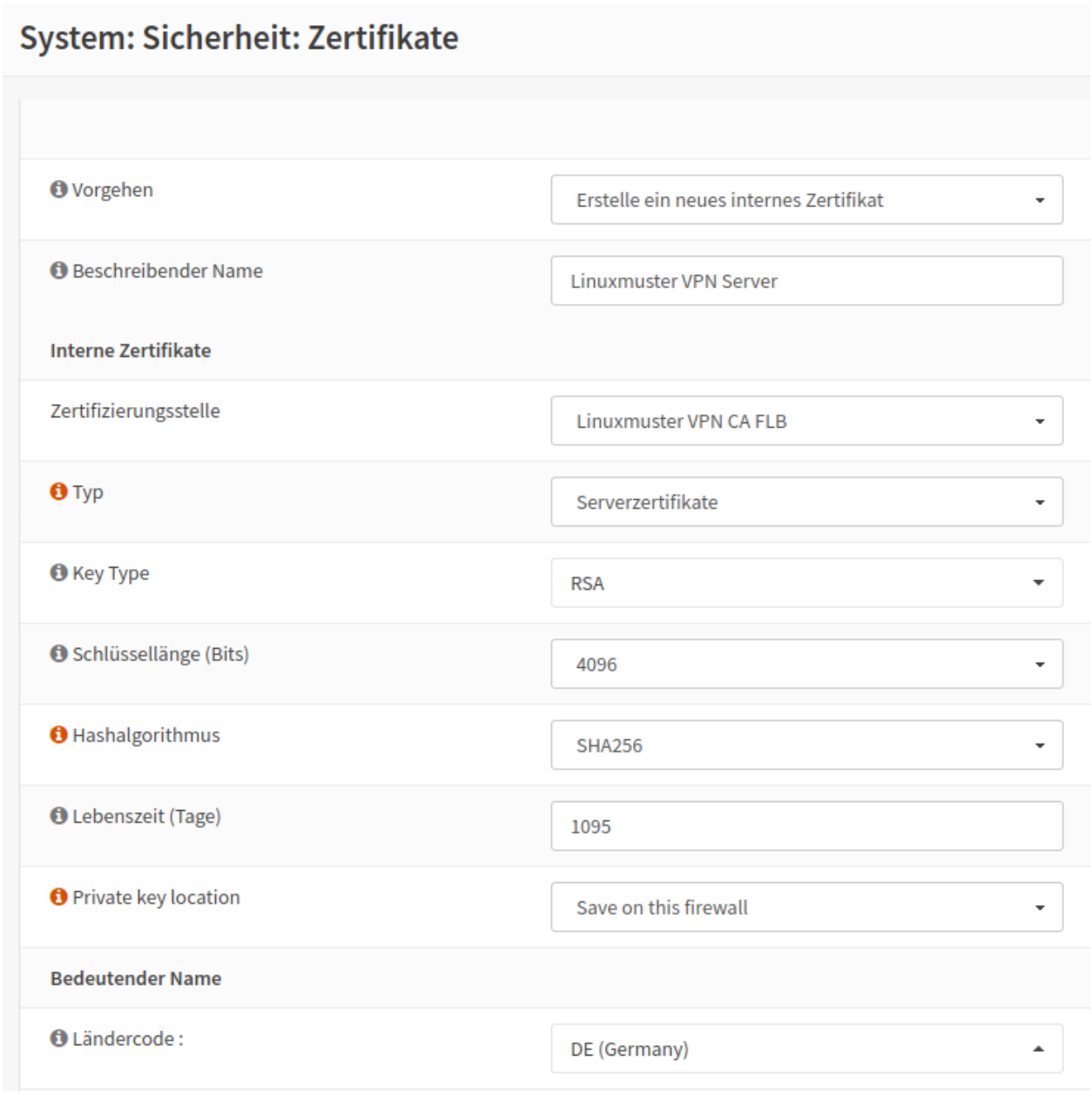
Danach ist unter Unter `System` –> `Sicherheit` –> `Zertifikate` ein Zertifikat hinzuzufügen (oben rechts).



Folgende Eingaben sind zu treffen:

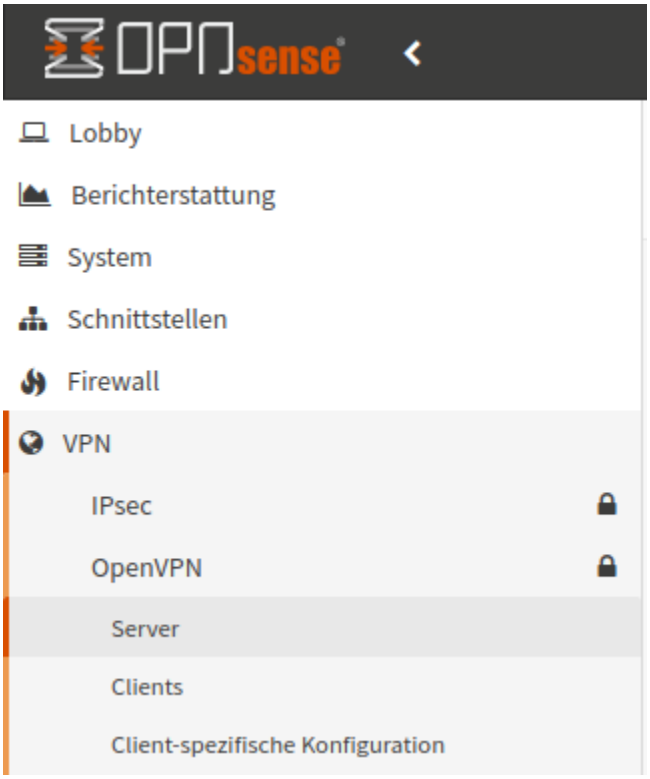
1. Vorgehen: Erstelle ein neues internes Zertifikat
2. Beschreibender Name: Linuxmuster VPN Server
3. Zertifizierungsstelle: Linuxmuster VPN CA
4. Type: Serverzertifikate
5. Key Type: RSA
6. Schlüssellänge: 4096
7. Hash-Algorithmus: SHA512
8. Lebenszeit (Tage): frei wählbar!
9. Private Key Location: Save on this firewall
10. Bedeutender Name: <dein bedeutender Name für das Zertifikat>

Folgende Abb. gibt diese Einstellungen wieder:



4.39.4 OpenVPN-Server erstellen

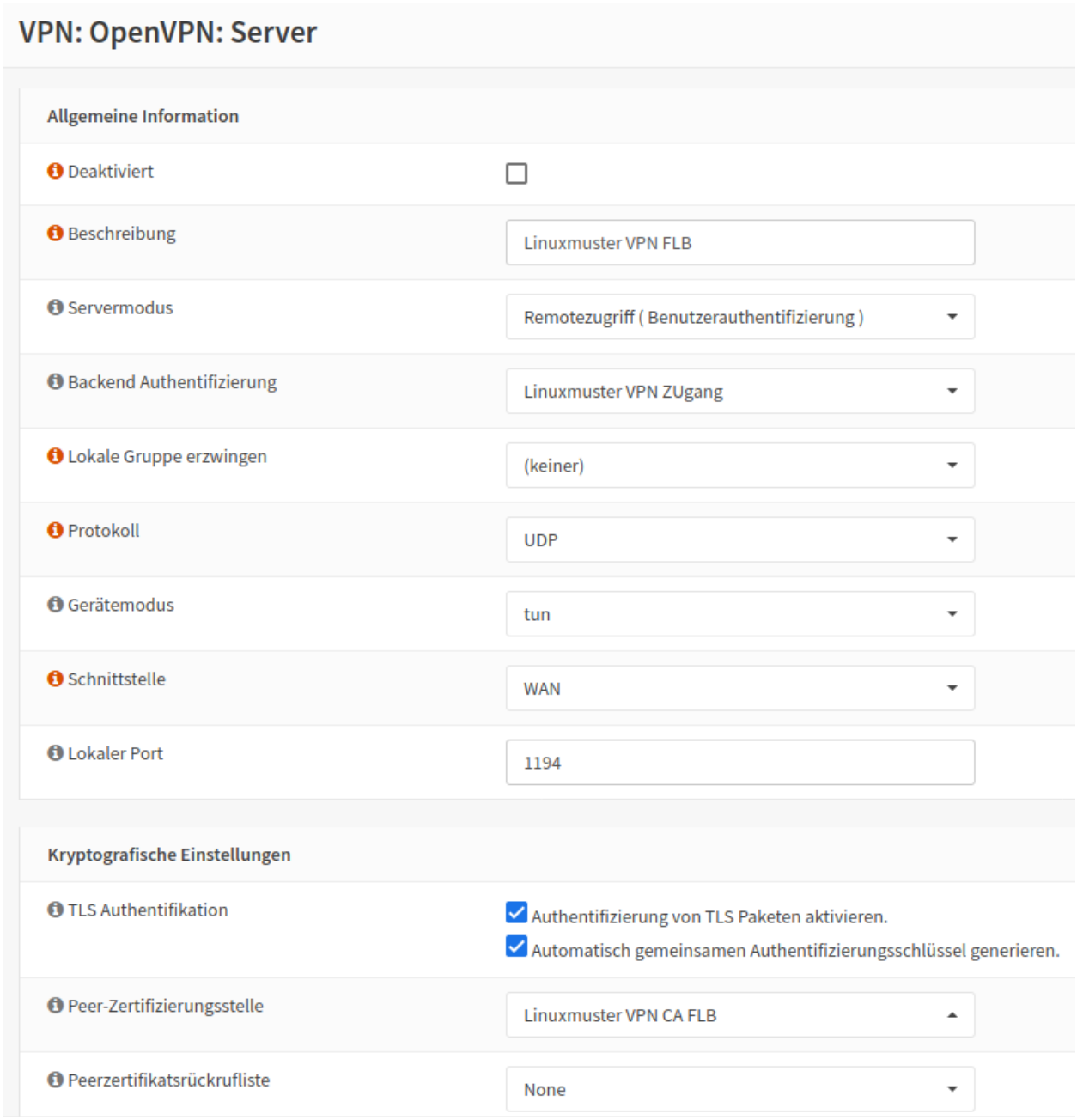
Unter `VPN` –> `OpenVPN` –> `Server` ist ein OpenVPN-Server zu erstellen (oben rechts).



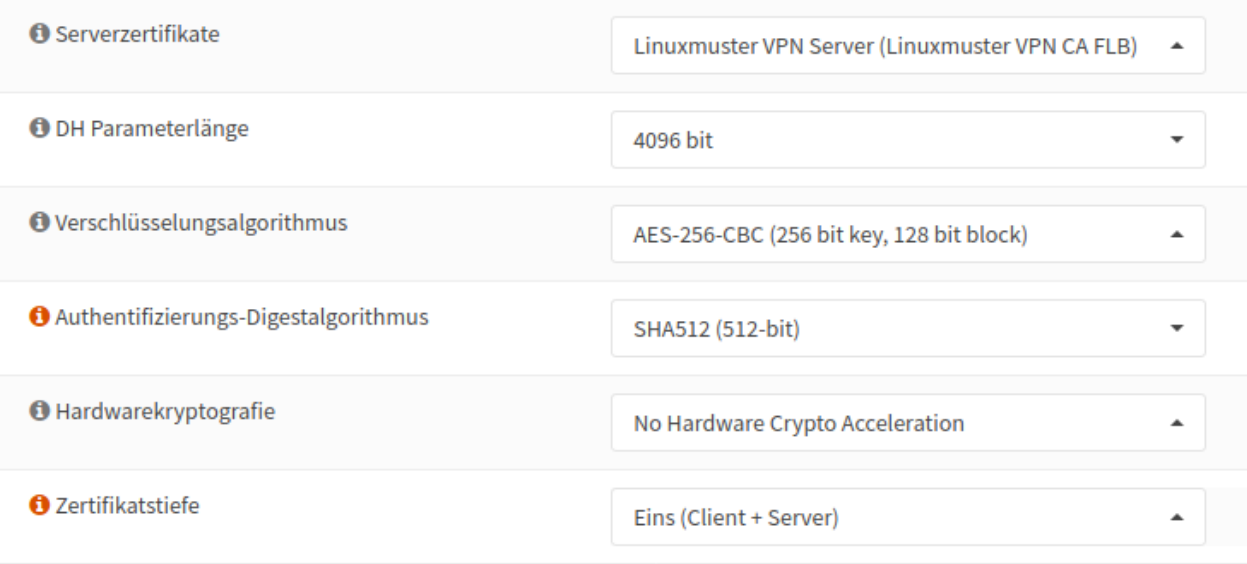
Es sind folgende Eingaben sind zu treffen:

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

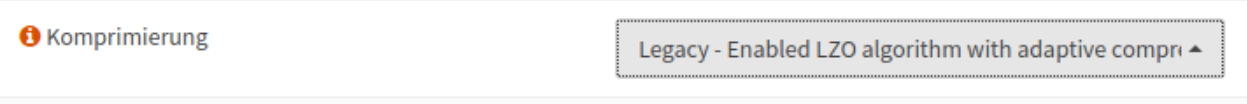
Nachstehende Abb. verdeutlicht diese Einstellungen:



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)

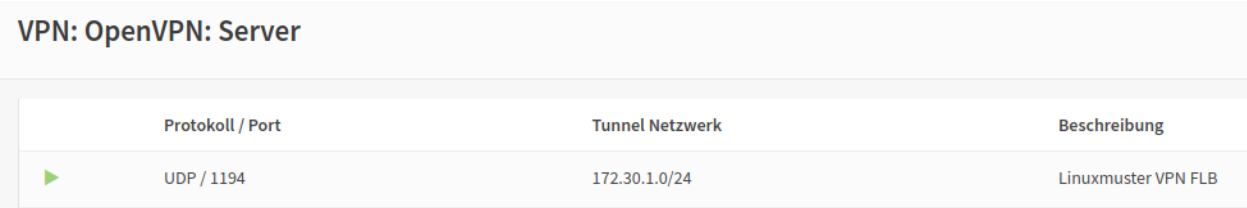


18. IPv4 Tunnelnetzwerk: Ein Netzbereich in dem die VPN Clients ihre IP bekommen z.B. 172.30.1.0/24 oder 192.168.100.0/24
19. IPv6 Tunnelnetzwerk:
20. Weiterleitungs Gateway:
21. Lokales IPv4-Netzwerk: 10.0.0.0/16 –> hier ist das beim Setup gewählte linuxmuster-Netz anzugeben
22. Lokales IPv6-Netzwerk:
23. Fernes IPv4-Netzwerk:
24. Fernes IPv6-Netzwerk:
25. Konkurrierende Verbindungen:
26. Komprimierung: Aktiviert mit adaptiver Kompression



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.



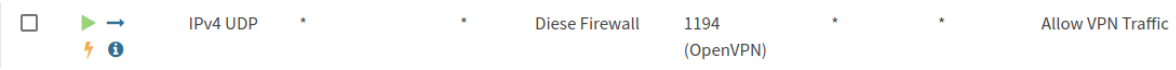
4.39.5 Firewall Regeln

Es müssen nun Regeln definiert werden, die die VPN-Anfragen an die Firewall weitergeben und nach erfolgreicher Authentifizierung den VPN-Datenverkehr zulassen.

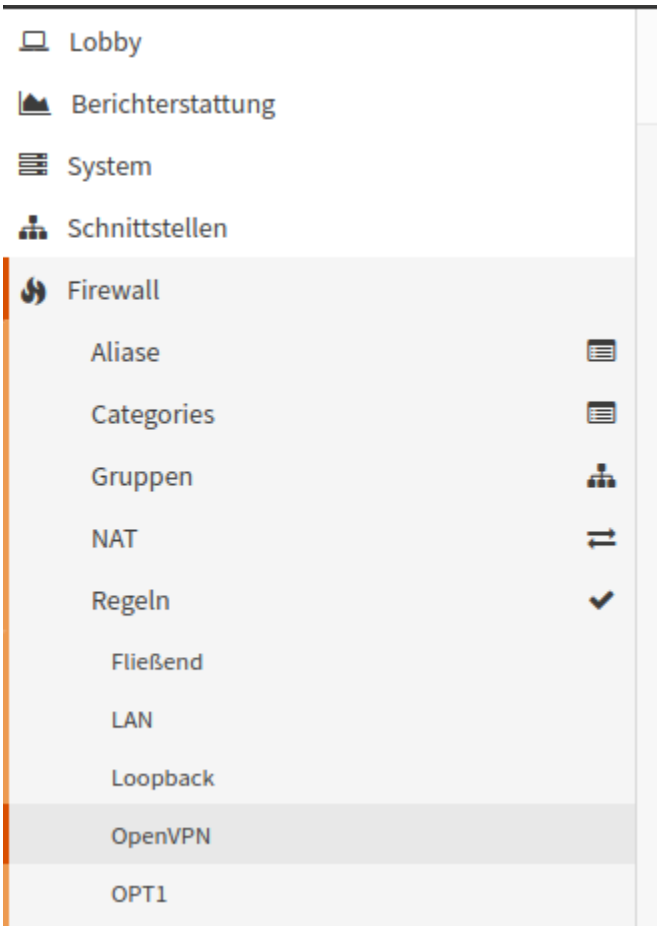
Unter `Firewall` –> `Regeln` –> `WAN` eine neue Regel anlegen (oben rechts). Folgende Eingaben sind zu treffen:

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:



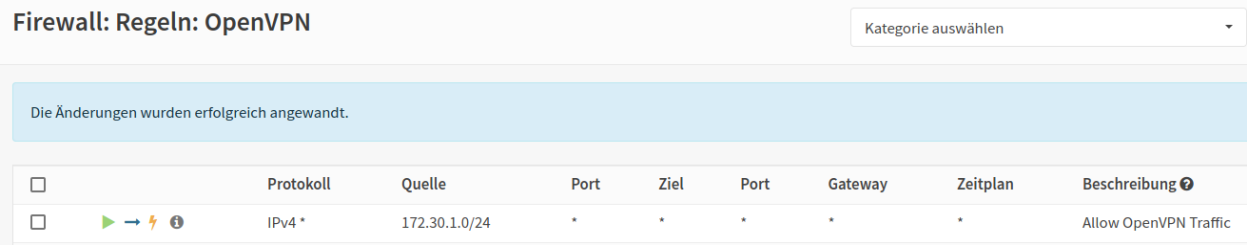
Danach unter `Firewall` –> `Regeln` –> `OpenVPN` eine neue Regel anlegen (oben rechts). Hier findet sich jetzt nach der Anlage des VPN-Servers eine neuer Menüeintrag für OpenVPN:



Es sind folgende Eingaben vorzunehmenn:

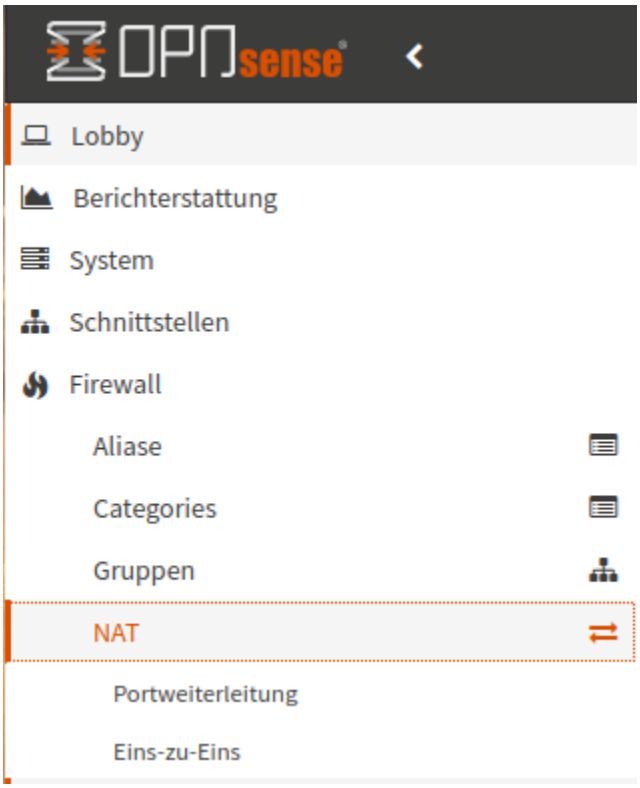
1. Quelle: 172.30.1.0/24 -> das VPN-Netz, das Du für den OpenVPN-Server zuvor eingerichtet hast.
2. Für den Rest: <Standardwerte>

Änderungen übernehmen (rechts im blauen Kasten).



Sollte ein Router das externe Netz bedienen und befindet sich die OPNsense® „hinter“ dem Router, so 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:

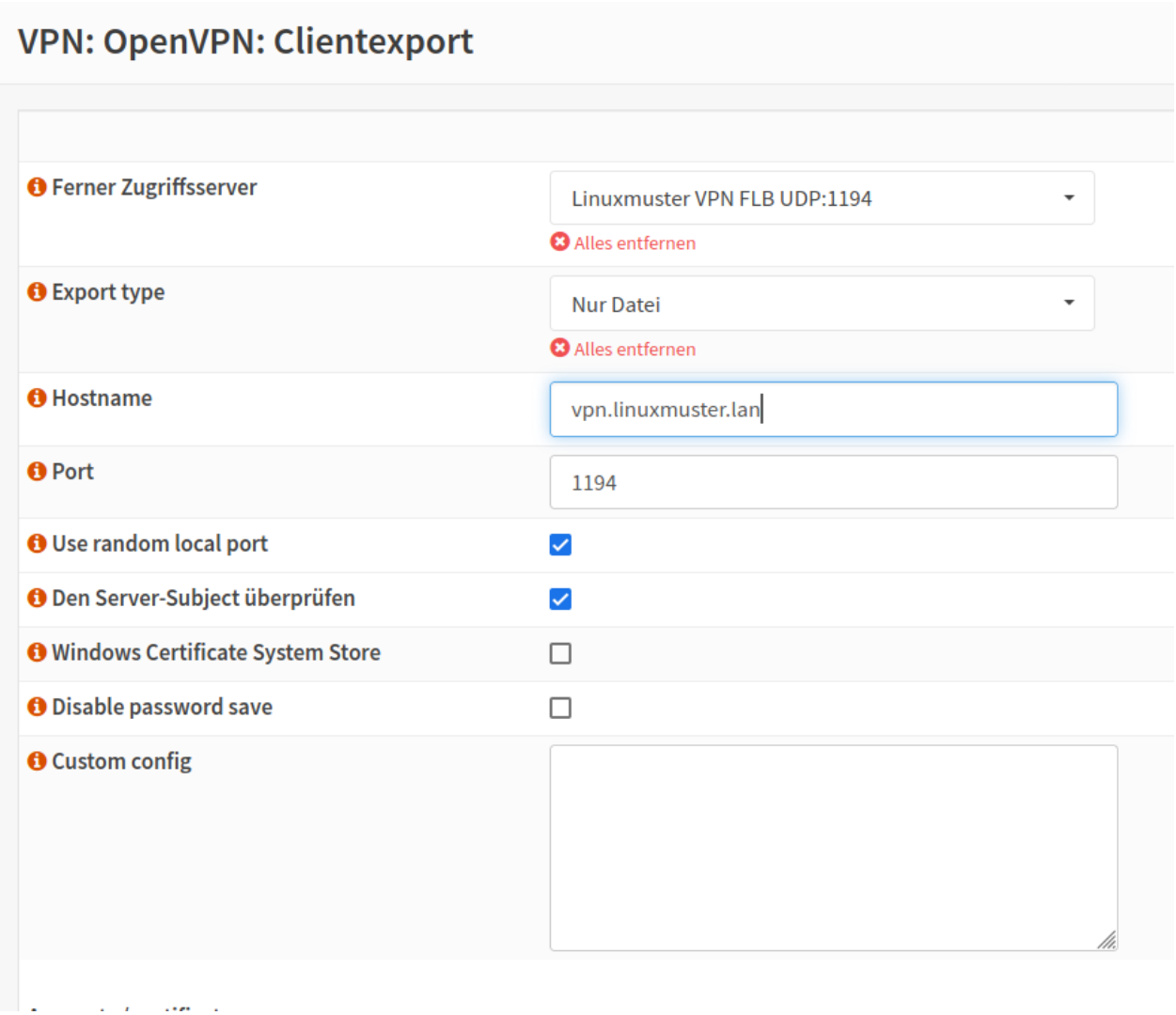
Zwischen dem Router, der die externe Verbindung bedinet und der externen Schnittstelle der Firewall wird i.d.R. ein privates Netz (z.B. 192.168.200.0/24) verwendet. Daher muss hier eine Weiterleitungsregel für NAT angelegt werden, sonst werden die eingehenden Pakete vom Router nicht an die Firewall weitergegeben.

4.39.6 Konfiguration exportieren

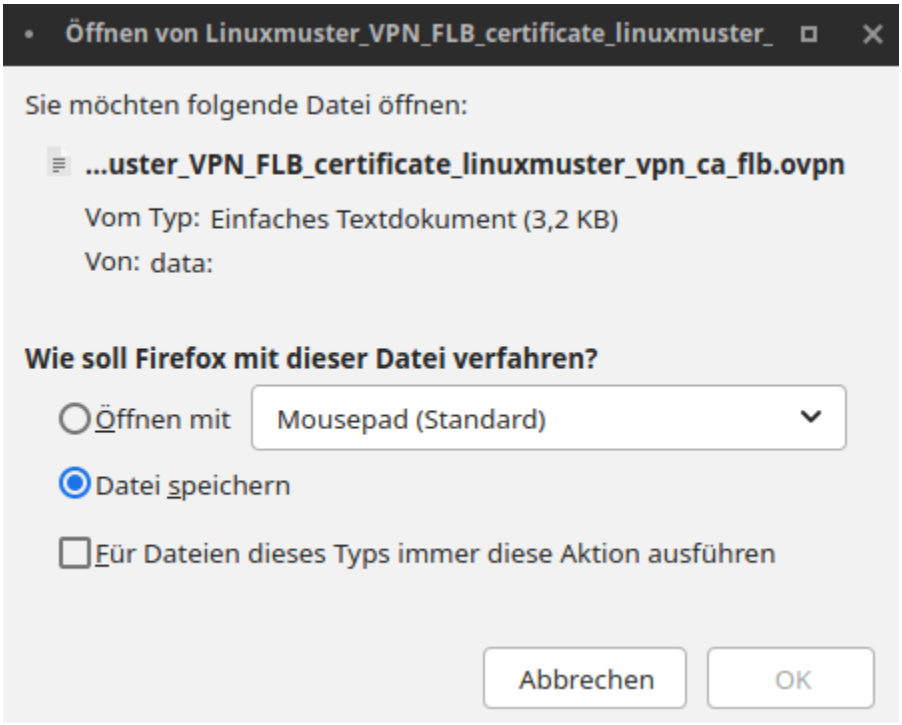
Für die Verbidnung mit den Clients muss nun ein Export des Profils für den Benutzer erfolgen.

Dazu gehst Du zu `VPN` –> `OpenVPN` –> `Clientexport`. Dort gibst Du Folgerndes 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>



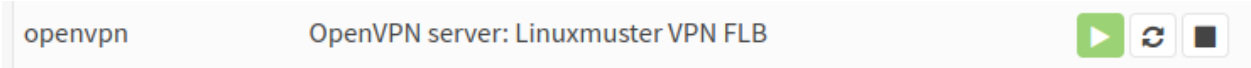
Danach drückst Du unter `Accounts / certificates` bei Linuxmuster VPN Server ganz rechts auf das Download-symbol.



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

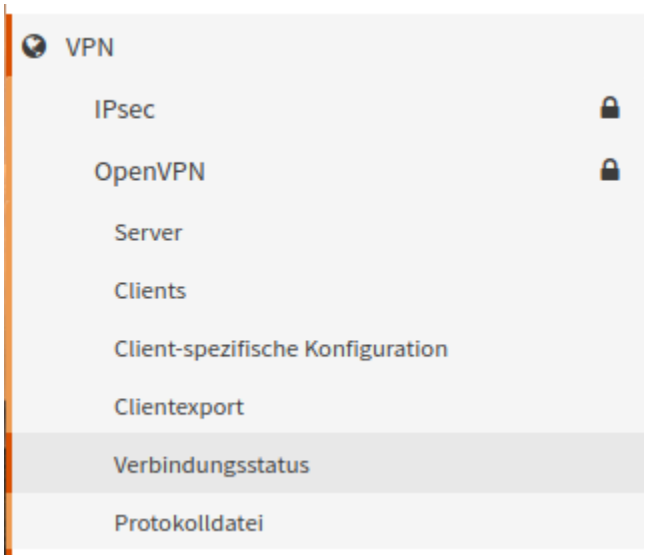
Bevor Du nun die Verbindung mit einem Client zum VPN-Server testest, überprüfe zuerst, ob der Dienst läuft. In der GUI der OPNsense® klickst Du links auf den Menüeintrag `Lobby` und siehst rechts alle Dienste mit ihrem Status aufgelistet. Hier muss für OpenVPN Server ein `grünes` Dreieck zu sehen sein. Dies weist daraufhin, dass der Dienst läuft.



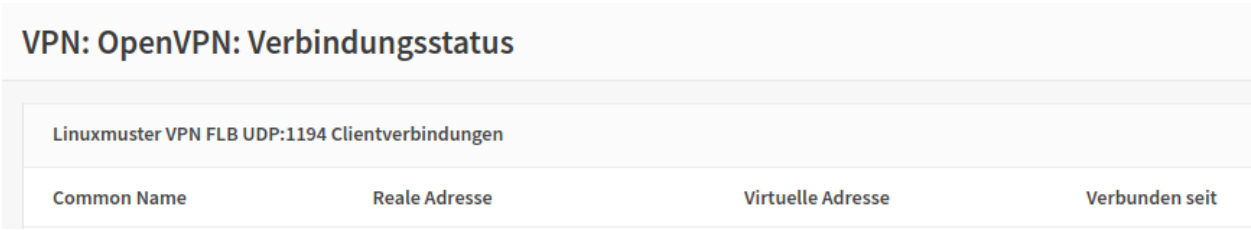
OpenVPN Client

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:



Troubleshooting

Sollte die Verbindung nicht erfolgreich aufgebaut werden können, prüfe Folgendes ab:

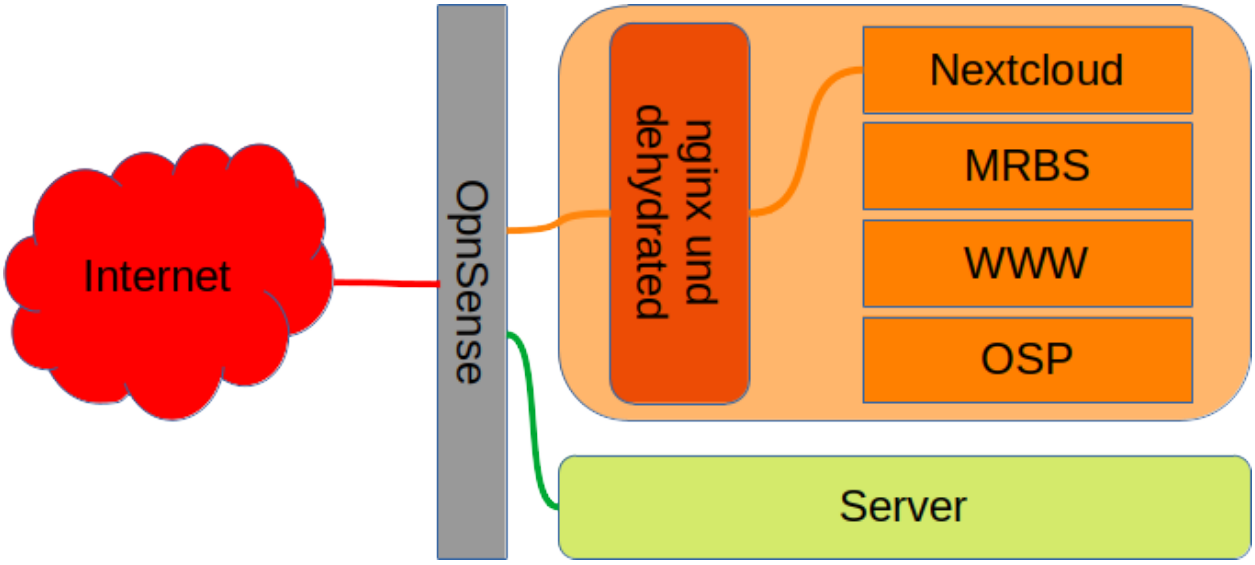
1. Ist die OPNsense® von extern via URL erreichbar ?
2. Antwortet die OPNsense® auf dem eingestellten VPN Port ?
3. Kommen die VPN - Pakete (ggf. Prot-Forwarding) auf der OPNsense® an?
4. Werden die VPN-Pakete auf der WAN-Schnittstelle zugelassen (siehe Live-Logs)?

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 intalliert werden können.

Angenommen wir möchten an einer Schule eine Nextcloud, ein MRBS, eine Website und eventuell noch ein OpenSchulPortfolio 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.

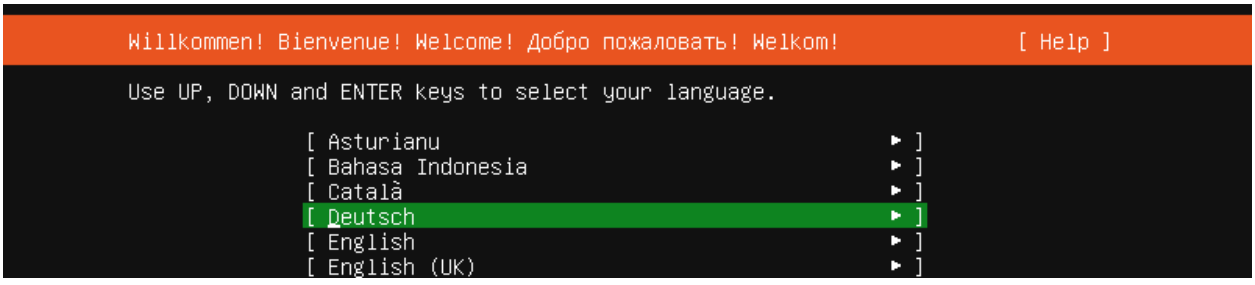
Installiere zunächst einen ubuntu 20.04 Server.

4.40.1 Installation des Ubuntu Servers

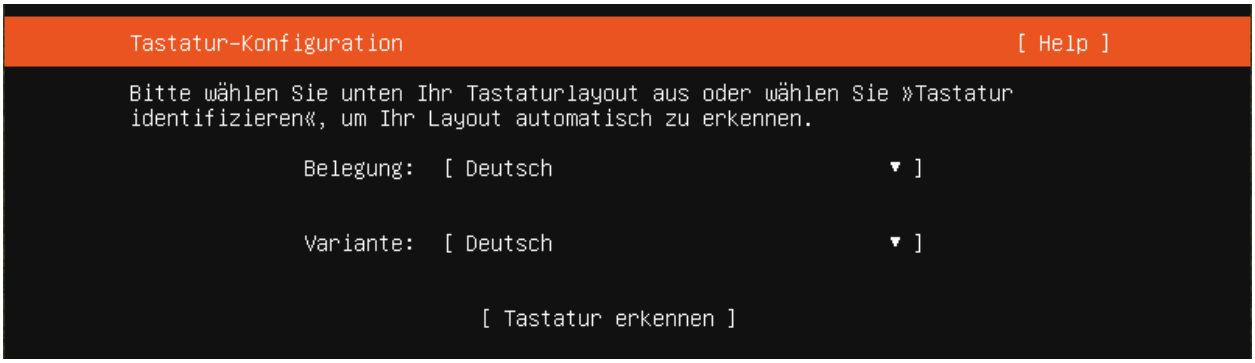
Lade die iso-Datei für den Ubuntu-Server von https://ubuntu.com/download/server herunter und starte Deinen Server vom Installationsmedium.

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.

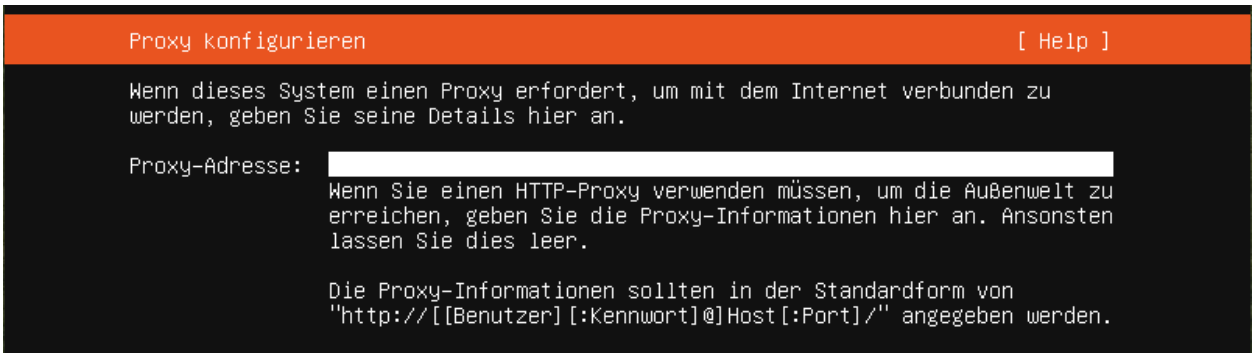


Wähle Deine bevorzugte Sprache

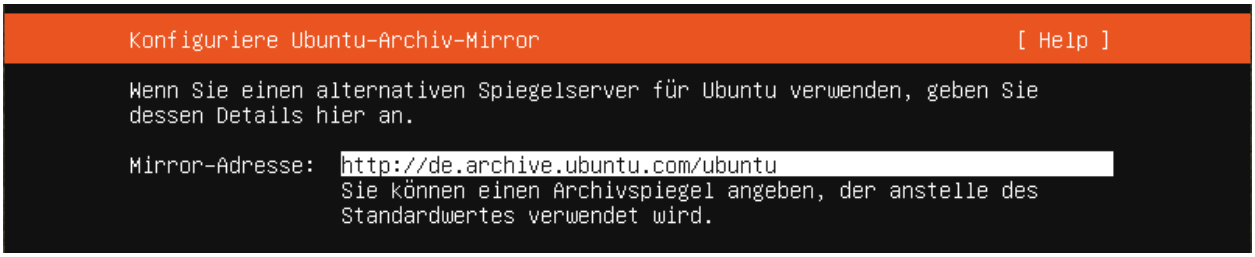


und Tastatur.

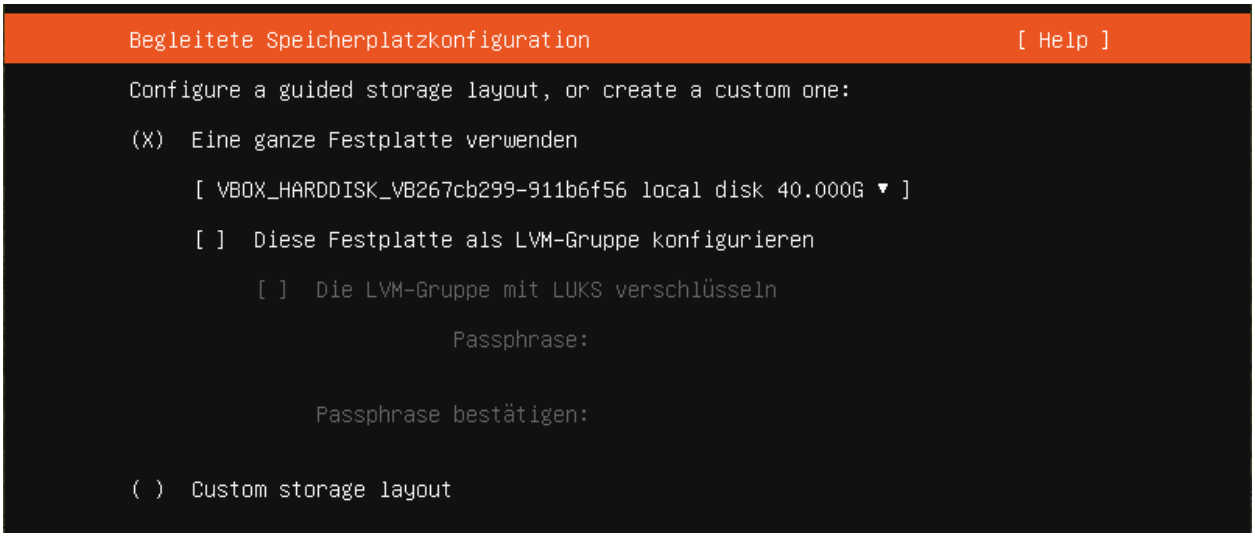
Da der neue Docker-Host per DHCP seine IP-Adresse bekommt, kannst Du die Vorgaben übernehmen.



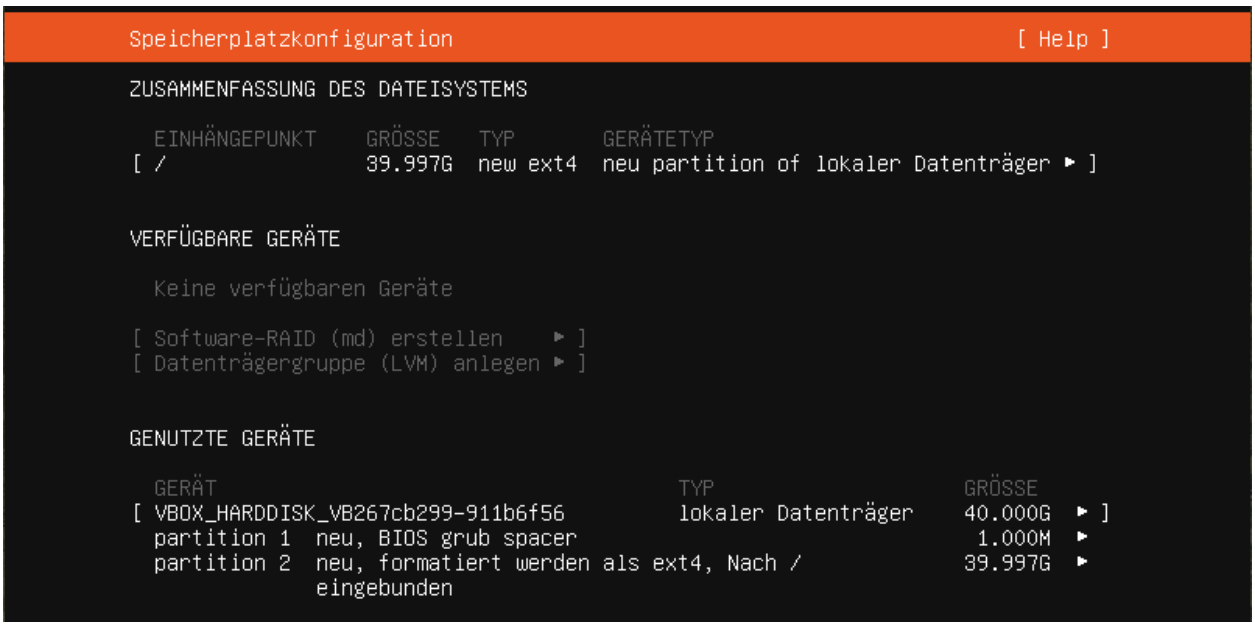
Die Proxy-Adresse und



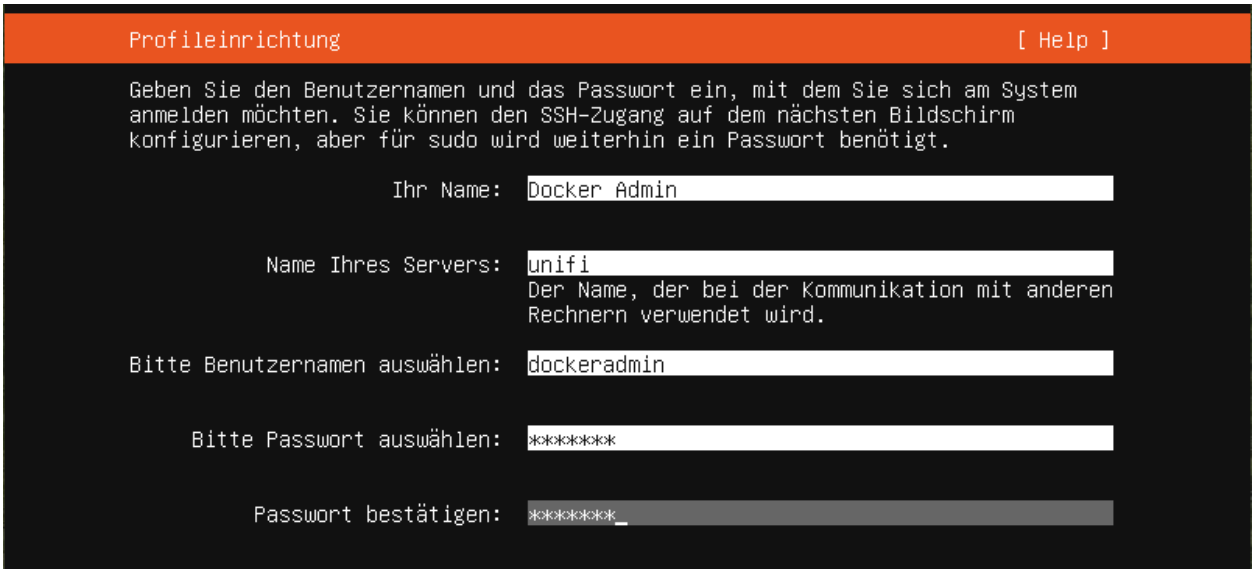
die Mirror-Adresse übernimmst du.



Die Speicherplatzkonfiguration

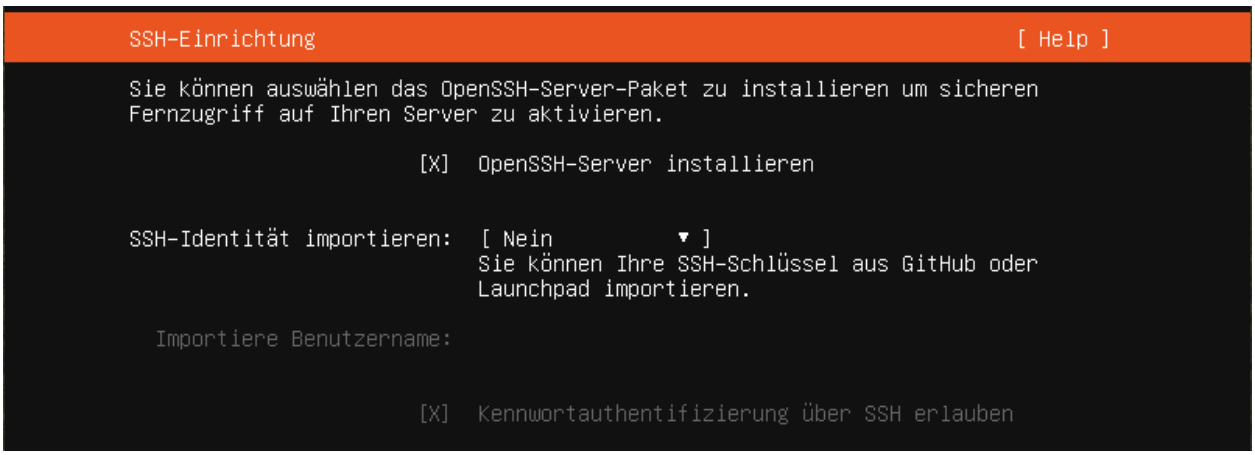


kannst Du auch übernehmen.



Der Name des Servers sollte so, wie in */etc/linuxmuster/sophomorix/default-school/devices.csv* gewählt werden.

Der Benutzername ist frei wählbar.



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 Firewalleinstellungen

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.

Die Regel muss nun noch aktiviert

und anschliessend übernommen werden:

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/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 (`moodle-binduser`) für den Bind-Zugriff zu definieren. Das zufällig erzeugte Kennwort wird in einer Datei auf dem Server hinterlegt.

```
# sophomorix-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.

```
# sophomorix-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
	DC=linuxmuster,DC=lan sind mit den Angaben der eigenen Domäne zu ersetzen.
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:

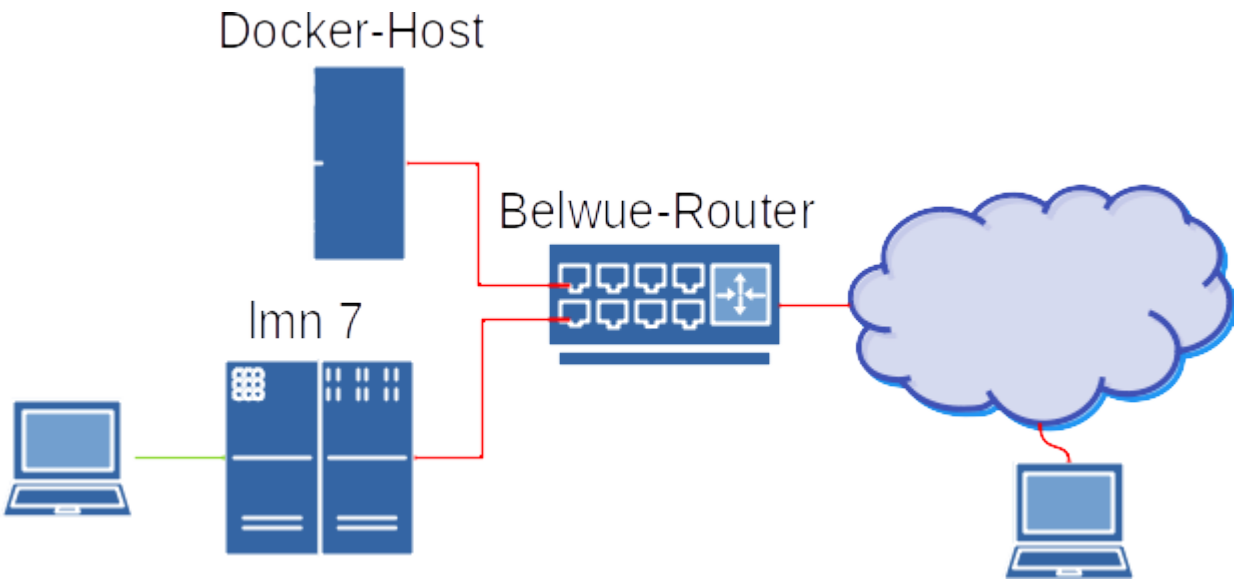
4.42.1 Vorüberlegungen zum Standort des Nextcloud-Services

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 verzeichtet werden und ist die Anbindung der Schule nur mit begrenzter Bandbreite gegeben, so könnte eine externer Docker-Host besser für die Schule geeignet sein.

Beide Szenarien werden nachstehend kurz dargestellt.

Nextcloud auf einem internen Docker-Host

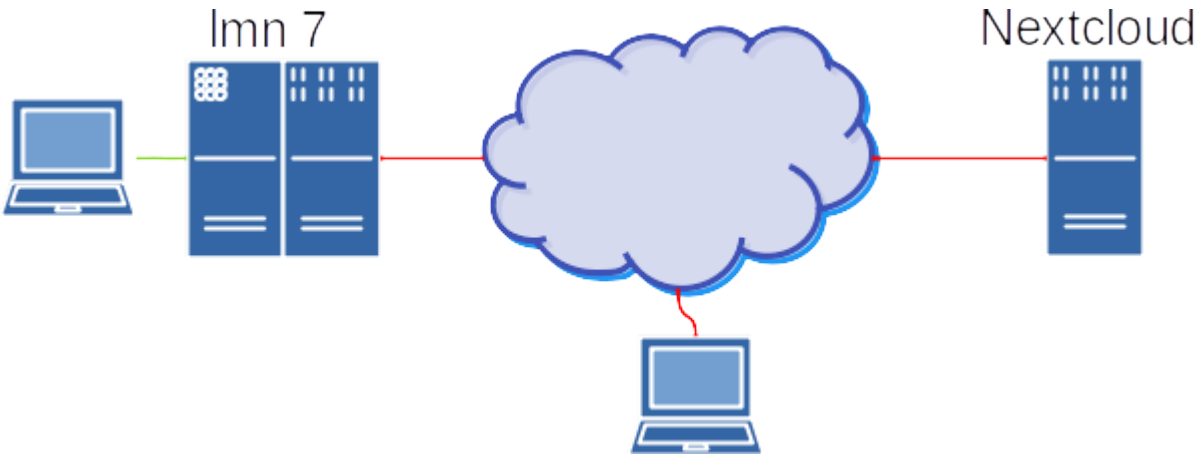


In der Grafik ist der Nextcloud-Service auf dem Docker-Host der Schule installiert. Da der Docker-Host Web-Services wie das Medien- und Raumbuchungssystem und die Nextcloud zur Verfügung stellt, ist er ein völlig eigenständiger Server, der außerhalb der linuxmuster.net steht. Er sollte also direkt an 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, leistungsstärker 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 Kaptitel *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. Ingesamt müssen diese vor der Einrichtung bewertet werden.

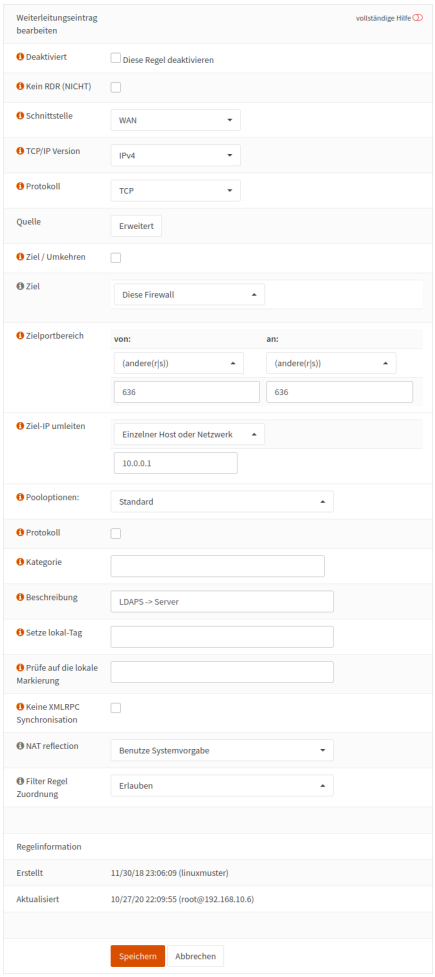
Firewallregel für den Zugriff auf das AD

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`.

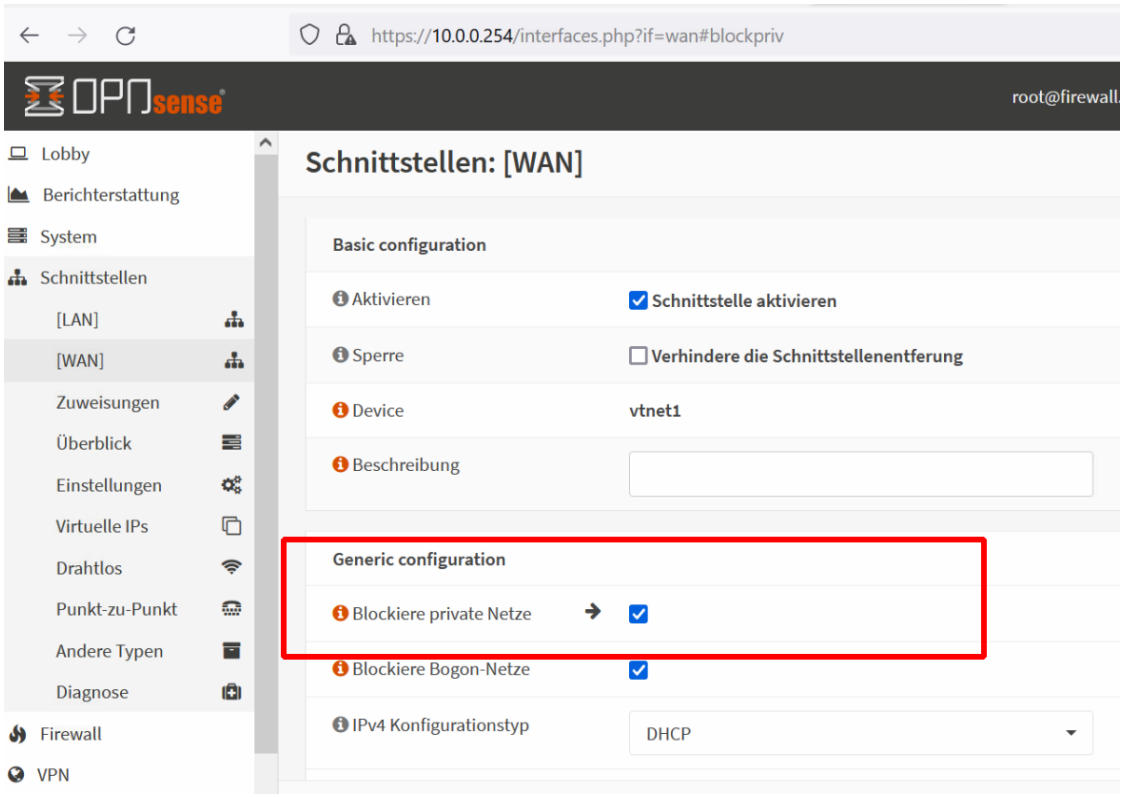
Klicke auf Hinzufügen um eine neue Firewallregel hinzuzufügen und trage die folgenden Werte ein.



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:

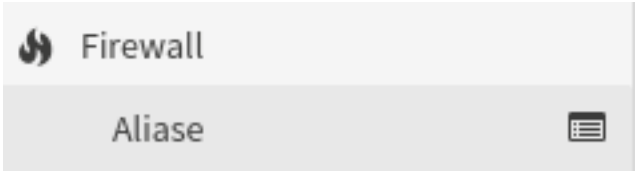


Firewallregel für den Zugriff über Samba

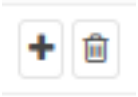
Hinweis: Sollte der Nextcloud-Servicve extern stehen, so sollten diese Ports nicht weitergeleitet werden.

Für den Zugriff über Samba müssen die Ports `139` und `445` an den Server weiter geleitet werden. Dazu legst Du erst mal einen Alias an.

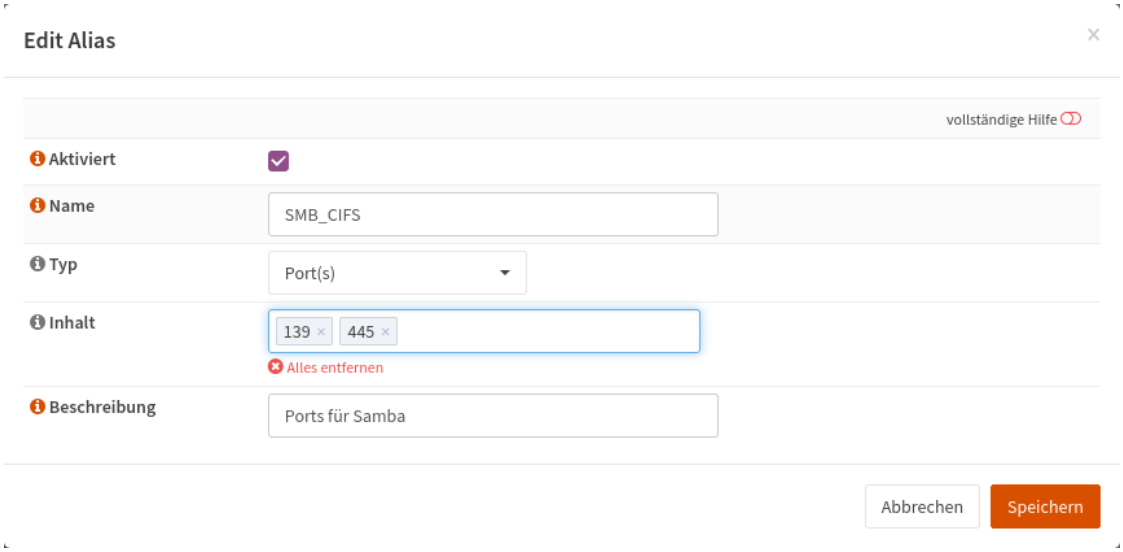
Navigiere auf Firewall -> Aliase.



In der Zeile unter dem letzten Alias klickst Du auf + um einen neuen Alias anzulegen.



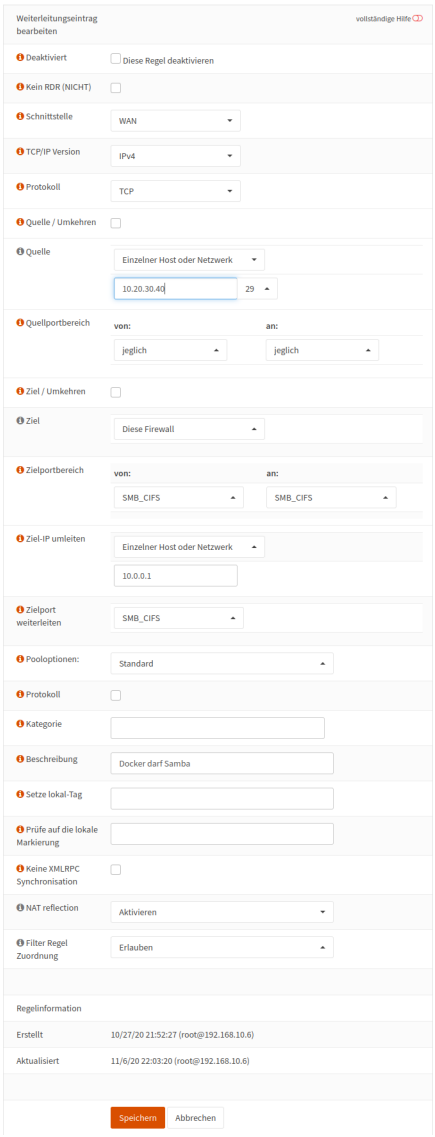
Und trage die folgenden Werte ein.



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:



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/carddav {
    return 301 $scheme://$host/remote.php/dav;
  }
  location /.well-known/caldav {
    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 angelegen, 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.

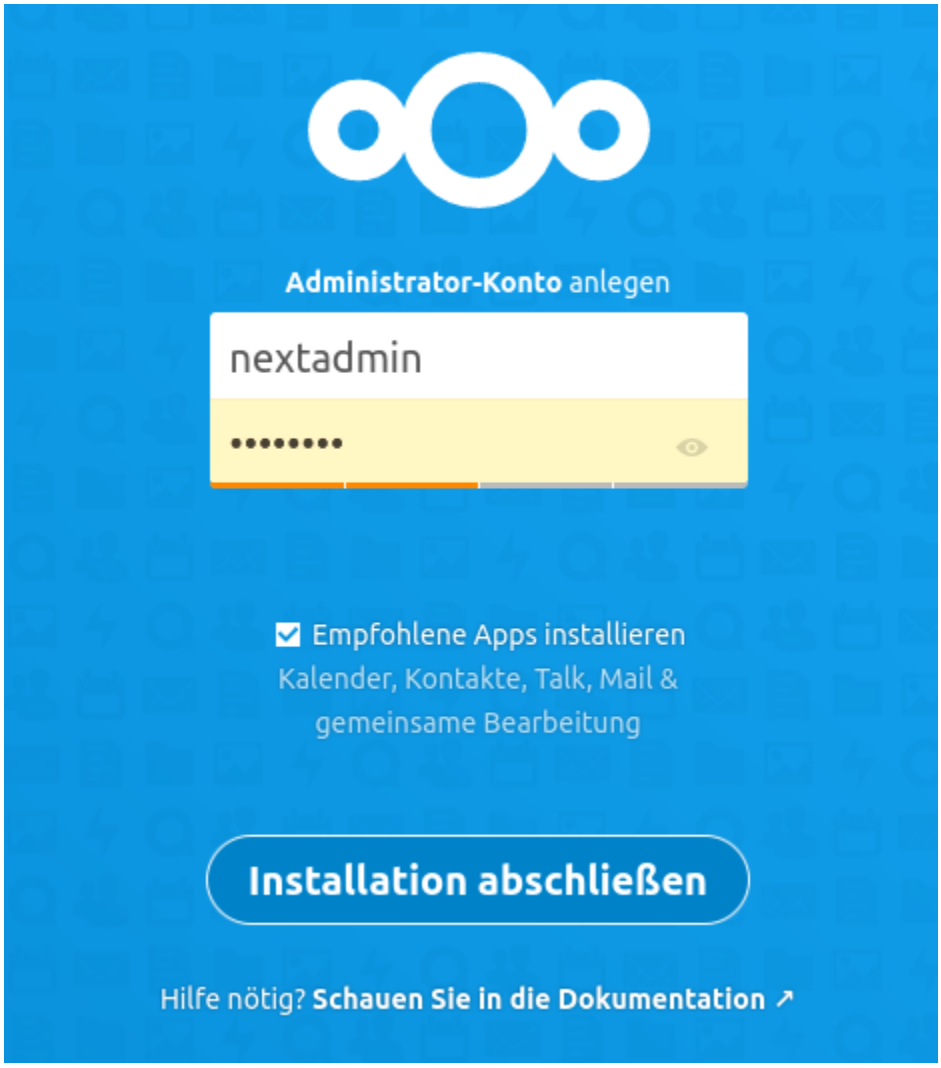
Das Verzeichnis `/var/www/html` des Webservers wird unter dem Verzeichnis `/srv/docker/nextcloud/nextcloud` auf dem Docker-Host abgelegt. Und das Datenverzeichnis `/var/lib/mysql` der Maria Datenbank wird unter dem Verzeichnis `/srv/docker/nextcloud/db` auf dem Docker-Host abgelegt.

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 `deaktiverte 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 Nextloud-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.

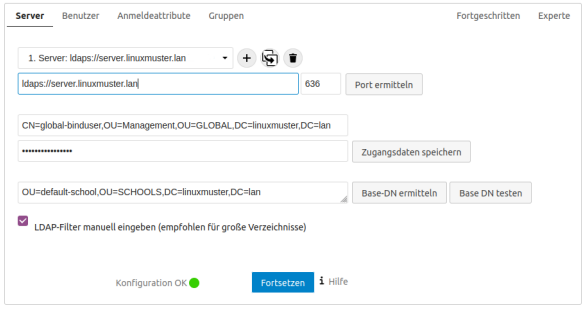
```
# sophomorix-user -u nextcloud-binduser --comment "AD access from nextcloud"
```

3. Lasse nun die Daten für den neu angelegten Benutzer anzeigen, die dann in den Nextcloud-Einstellungen als bind-user einzutragen sind.

```
# sophomorix-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 erhälst Du mit dem Befehl unter 3., den Du auf dem linuxmuster.net Server absetzen musst. Dass 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 `sophomorixRole=teacher`.

Bei Schüler-Accounts ist `sophomorixRole=student`.

Daraus ergibt sich die Filterregel:

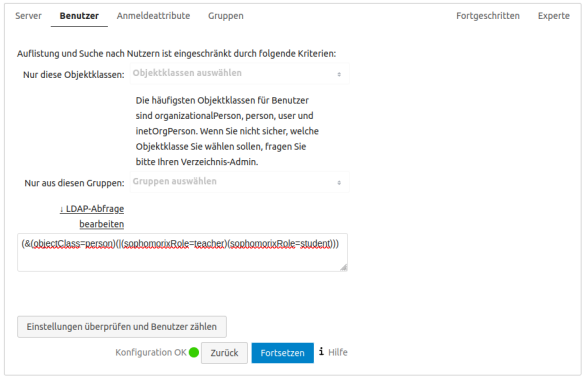
```
(&
  (objectClass=person)
  (|
    (sophomorixRole=teacher)
    (sophomorixRole=student)
  )
)
```

Trage also unter Benutzer in die LDAP-Abfrage folgendes ein:

```
(&(objectClass=person)(|(sophomorixRole=teacher)(sophomorixRole=student)))
```

Um den Zugriff auf die Nextcloud auf Lehrer zu begrenzen, ist unter `Benutzer` diese LDAP-Abfrage einzutragen.

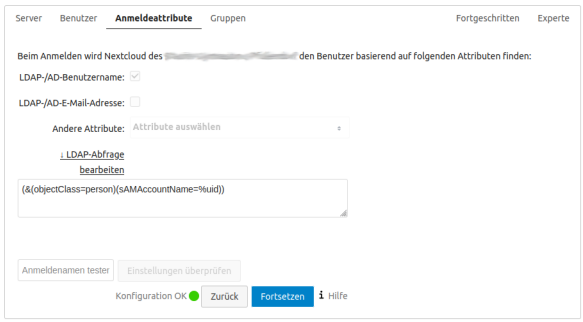
```
(&(objectClass=person)(sophomorixRole=teacher))
```



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:



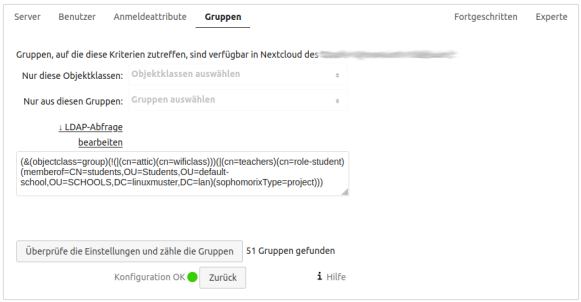

```
(&(objectClass=person)(sAMAccountName=%uid))
```

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)
    (sophomorixType=project)
  )
)
```

Nehme folgende Einstellungen vor:



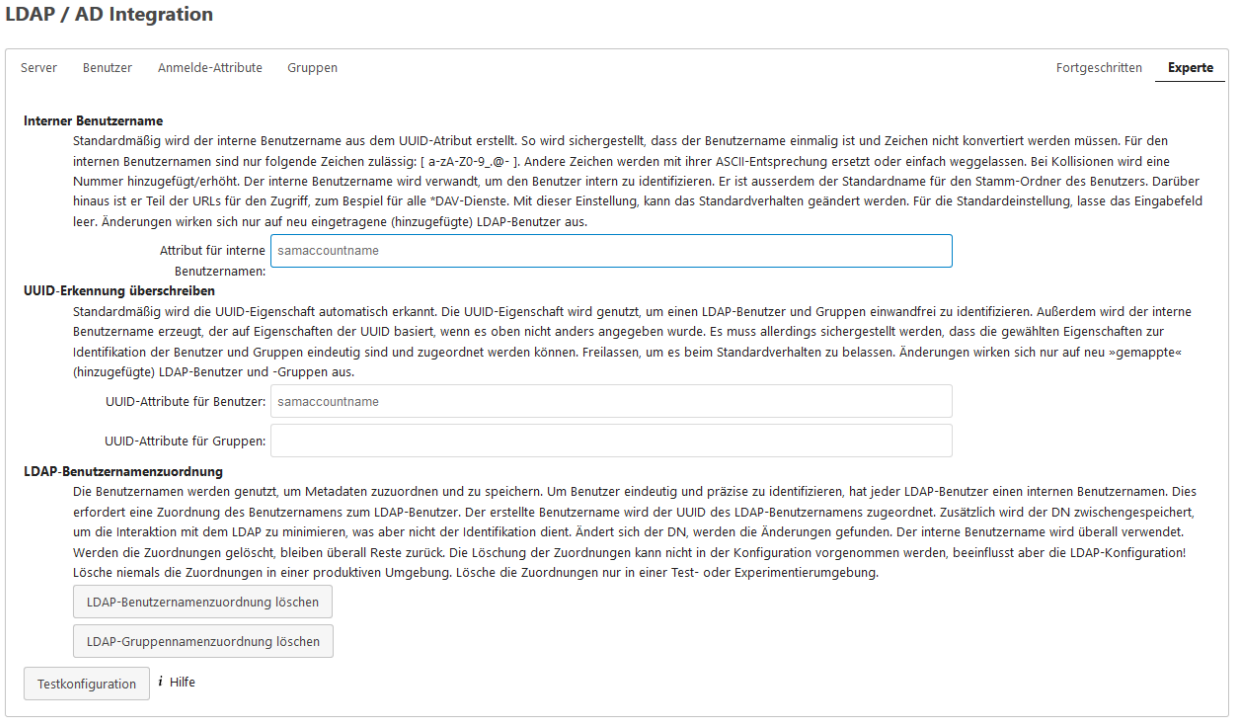

```
(&(objectclass=group)(!(|(cn=attic)(cn=wificlass)))(|(cn=teachers)(cn=role-
↪student)(memberof=CN=students,OU=Students,OU=default-school,OU=SCHOOLS,DC=linuxmuster,
↪DC=lan)(sophomorixType=project)))
```

Die nachstehende Abfrage liefert nur die Gruppe der Lehrer:

```
(&(objectclass=group)(cn=teachers))
```

Einstellungen Experte

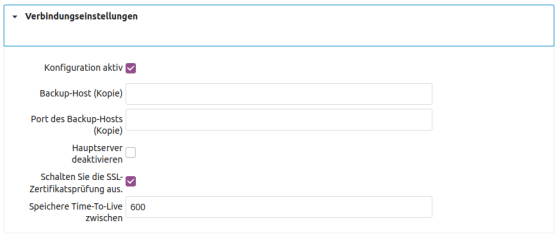
Klicke in dem Einstellungsmenü oben rechts auf den Eintrag `Experte` und trage nachstehende Werte ein:



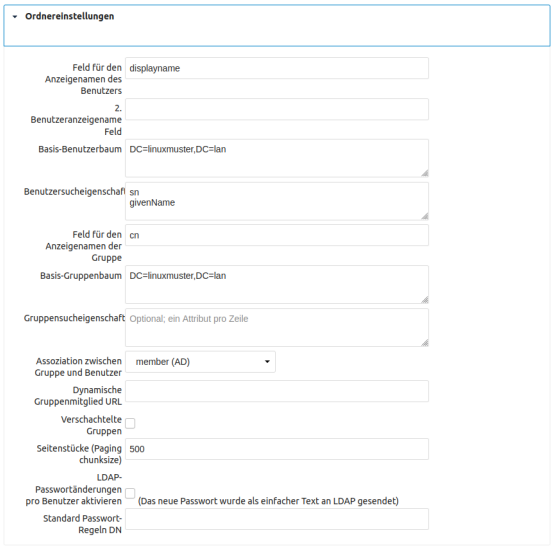
Trage dort folgenden Wert ein:

```
samaccountname
```

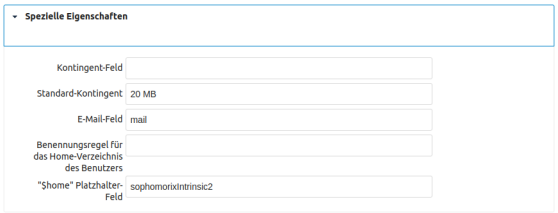
Einstellungen Fortgeschritten



Setze eine Häkchen bei `Konfiguartion aktiv` und, falls Dein Server mit einem selbstsigniertem Zertifikat arbeitet, auch bei `Schalten Sie die SSL-Zertifikatsprüfung aus`.



In `Benutzersucheigenschaften` gibst Du `sn` und `givenName` ein. So können Benutzer über ihren Vor- und Nachnamen gefunden werden.



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, hälst 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-Benutzernamenzuordung` und `Lösche LDAP-Gruppennamenzuordung`.

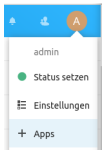
4.42.6 Zugriff auf die Home-Verzeichnisse

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.

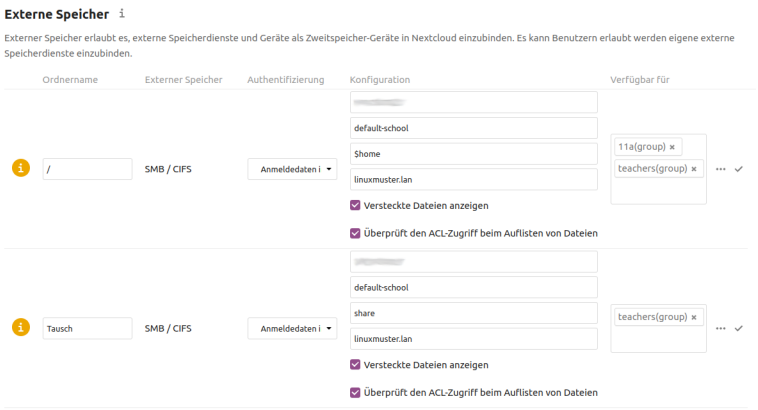


Gehe dazu auf A -> + Apps. Auf der Seite ganz unten findest Du die deaktivierten Apps. Aktiviere `External storage support`.

Einbindung der Home- und Tauschverzeichnisse

Sollte der Nextloud-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.

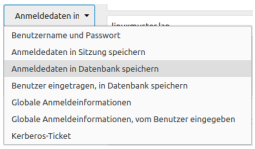


In den Einstellungen von `Externer Speicher` kannst Du jetzt, wie oben im Bild zu sehen ist, die Tauschverzeichnisse und das Home-Verzeichnis `/` der Benutzer einbinden.

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

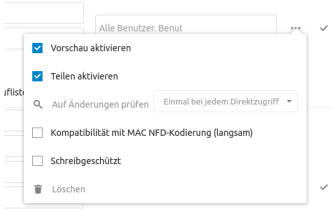
Dateien oder Verzeichnissen Änderungen vornehmen, wird die Desktop-App diese Änderungen bei anderen Benutzern nicht aktualisieren. Das passiert nicht, wenn Du als Lehrer über die Nextcloud diese Tauschverzeichnisse mit den Schülern/Gruppen teilst. Dann arbeitet die Desktop-App einwandfrei.



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` duchzuführen.

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`.

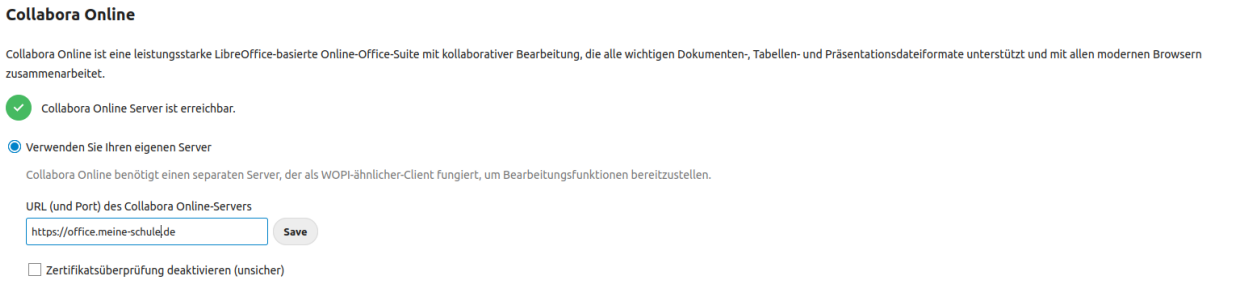
Collabora updaten

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.



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. aleksis.org

Folgende Funktionen bietet Aleksis an:

- Stundenplan Verwaltung
- Vertretunsplan
- 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 Anbidung 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 betrtrieben 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.

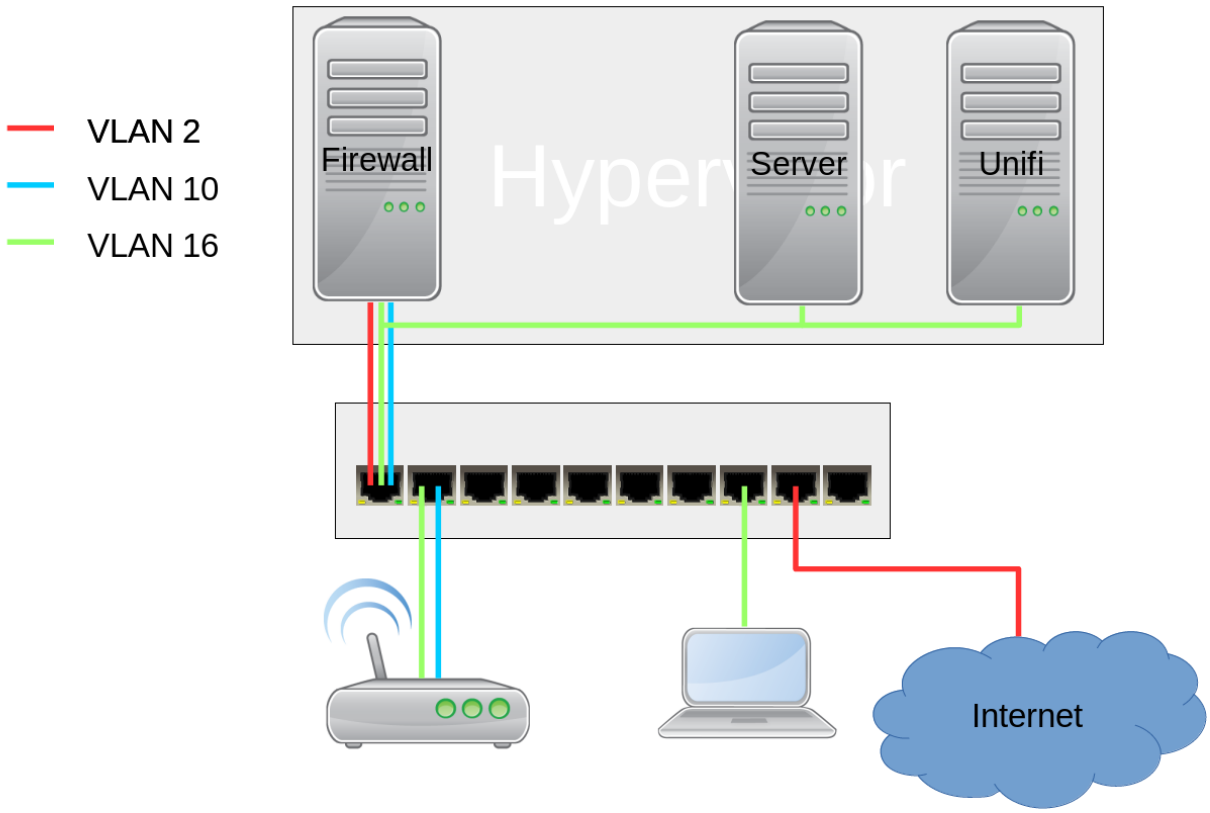
Jetzt sollte der Benutzer in der Lage sein sich anzumelden. Die LDAP Anbindung ist hiermit abgeschlossen.

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.

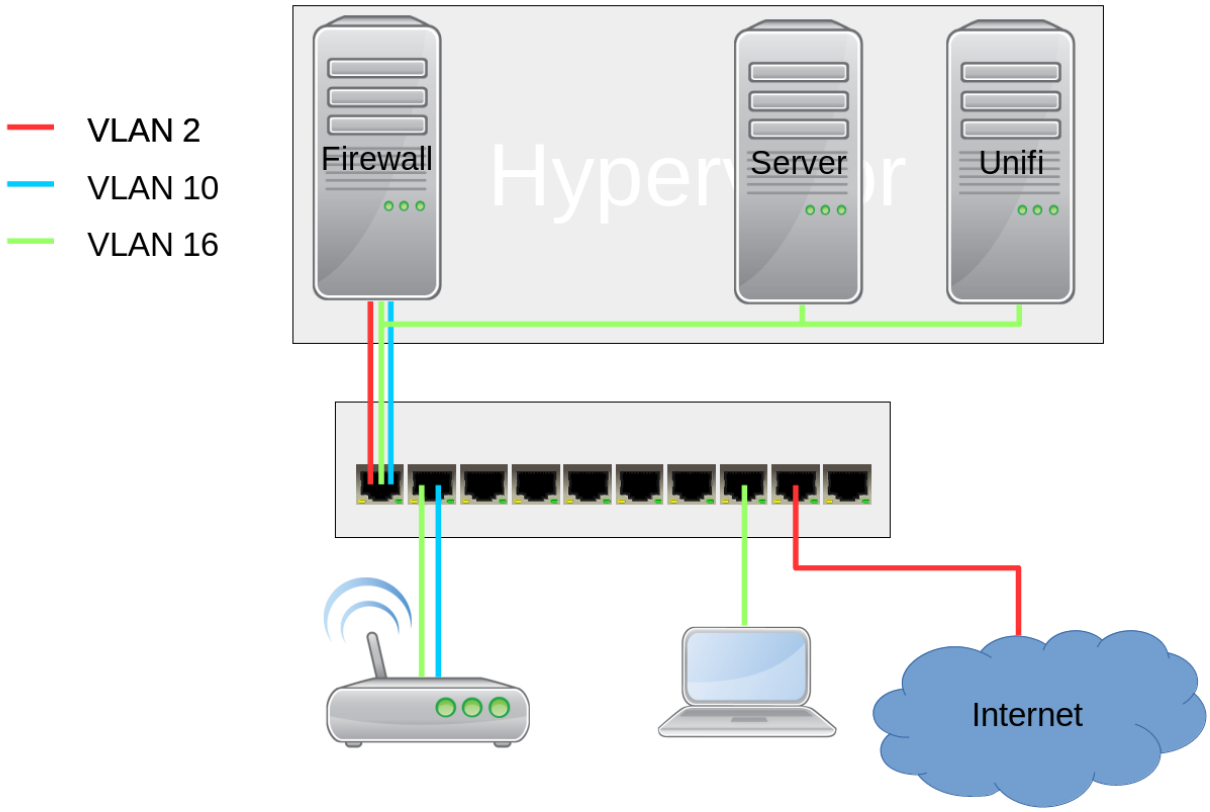
Die Geräte im Lehrernetz werden in die Datei */etc/linuxmuster/sophomorix/default-school/devices.csv* aufgenommen. Das Lehrernetz ist ein Teil des Schulnetzes. Damit können sich beispielsweise Benutzer mit einem Schullaptop per WLAN wie gewohnt anmelden und auf ihre Daten zugreifen.

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

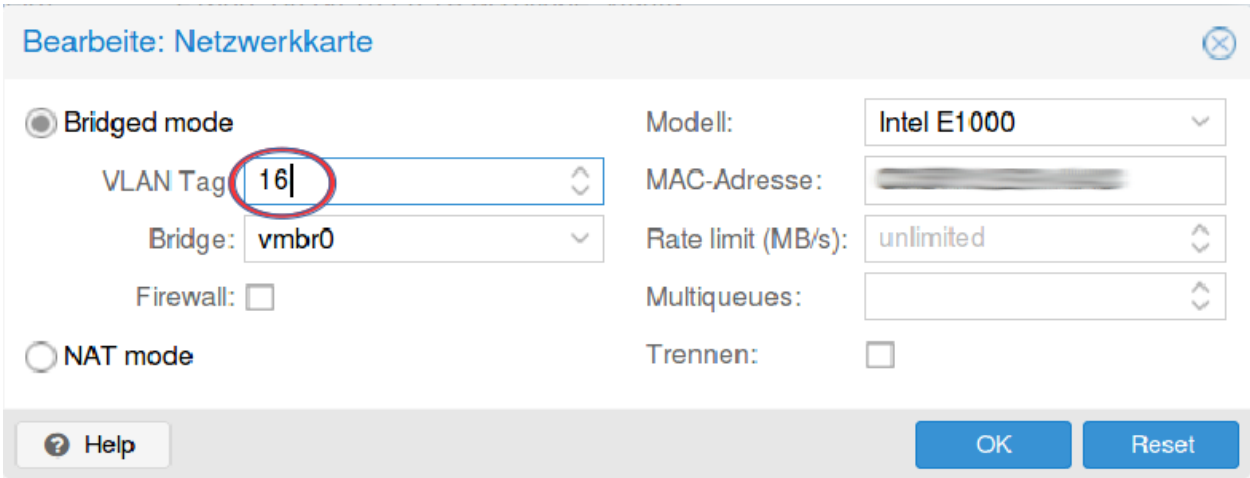
Sollen 2 WLANs über einen Accesspoint (AP) ausgestrahlt werden, muss mindestens ein Netzwerk ein getaggtes VLAN sein.



Im Beispiel ist der Hypervisor (z.B. Proxmox) mit einem Netzwerkkabel 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.



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.

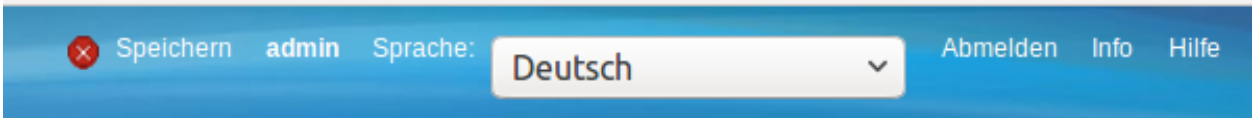
Grundsätzliches

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.

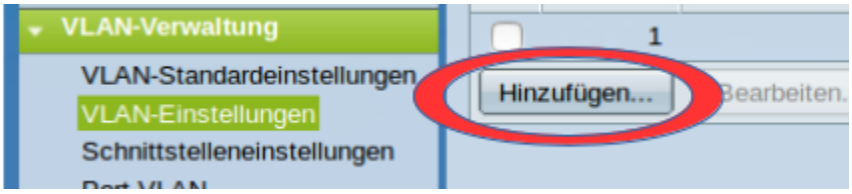
Wenn Du sich also mit einer Einstellung ausgeschlossen hast, starte den Switch einfach neu und Du hast den zuletzt in die *Startkonfiguration* gespeicherten Stand.

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.

Füge die VLANs wie im Bild hinzu.

Sobald alle VLANs hinzugefügt sind, schließe das Fenster. Die VLANs sollten jetzt aufgeführt sein.

Jetzt wäre ein guter Zeitpunkt, um die *Ausgeführte Konfiguartion* 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.

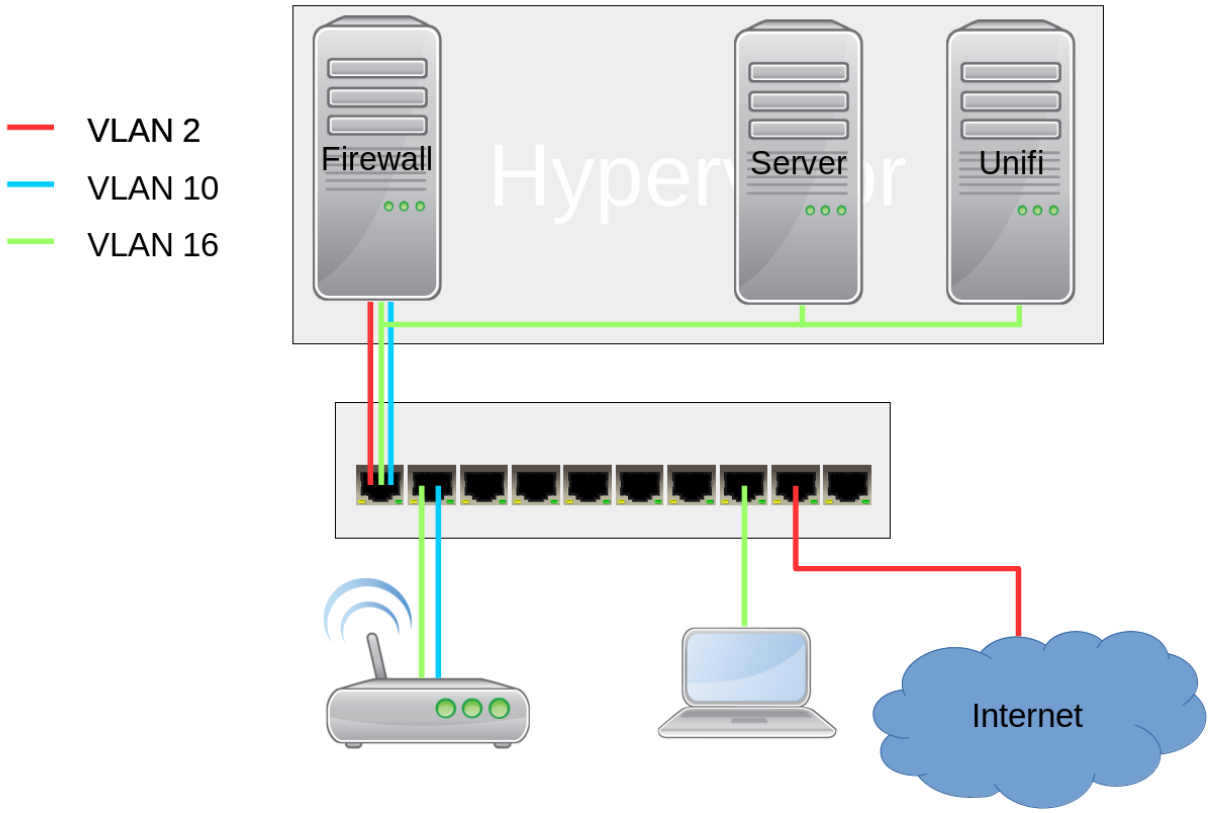
Ausgeschlossen:
Datenpakete, die mit der VLAN-ID x getaggt sind, werden verworfen.

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 getaggten 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 Netzwerkkabel mit Port 1 des Switches verbunden. Der Port 1 ist getaggtes Mitglied der VLANs 2, 10 und 16.

Port 2-5:
Die APs sind im Schulnetz und werden über ein ungetaggtes 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.

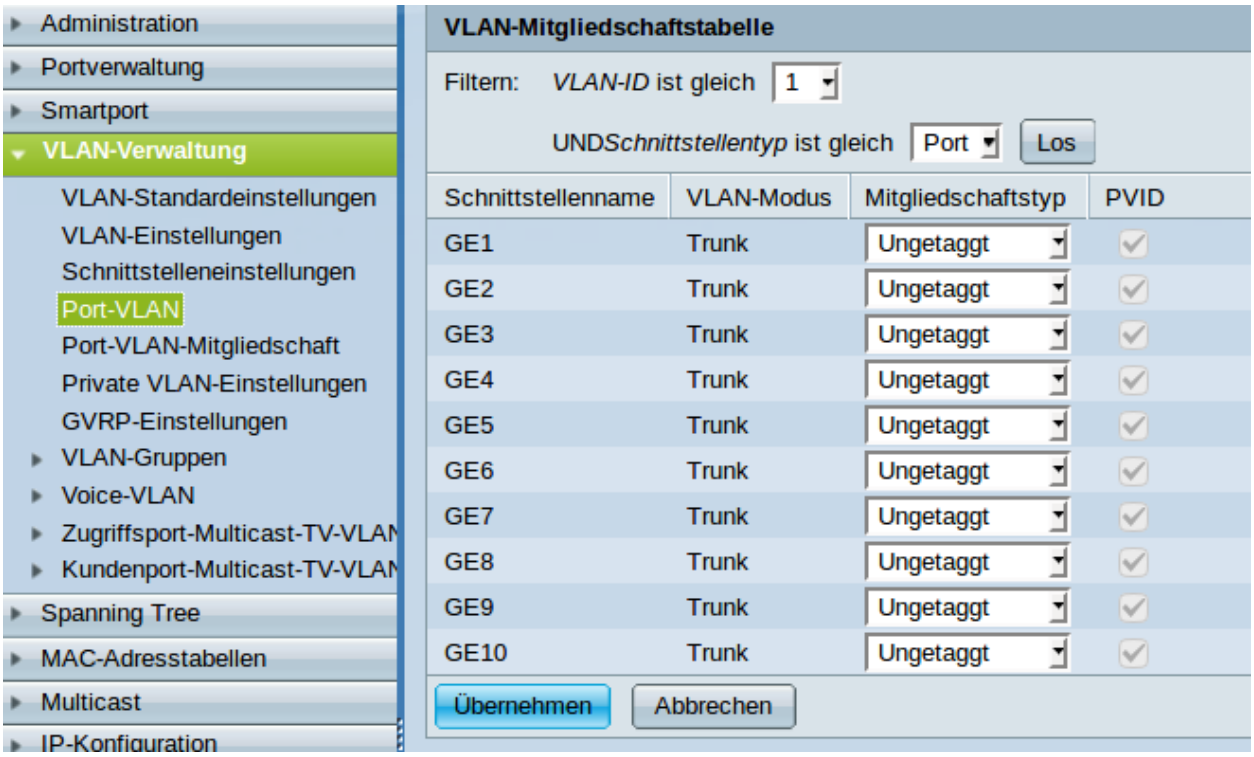
Port 7-8:
Die Clients sind nur im Schulnetz und arbeiten mit ungetaggten Datenpaketen. VLAN 16 ist ungetaggt und PVID ist 16.

Port 9:
Auch der Router arbeitet mit ungetaggten 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.



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.

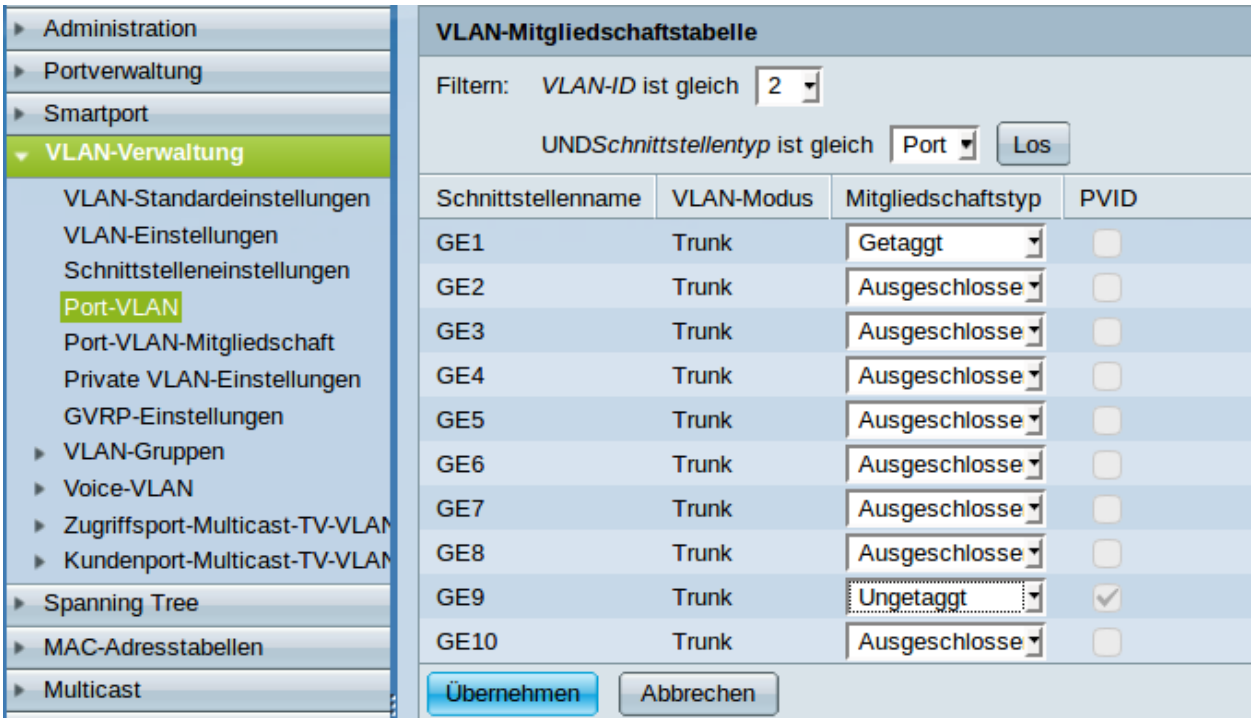
Für die Ports 1 bis 5 wählst Du getaggt.

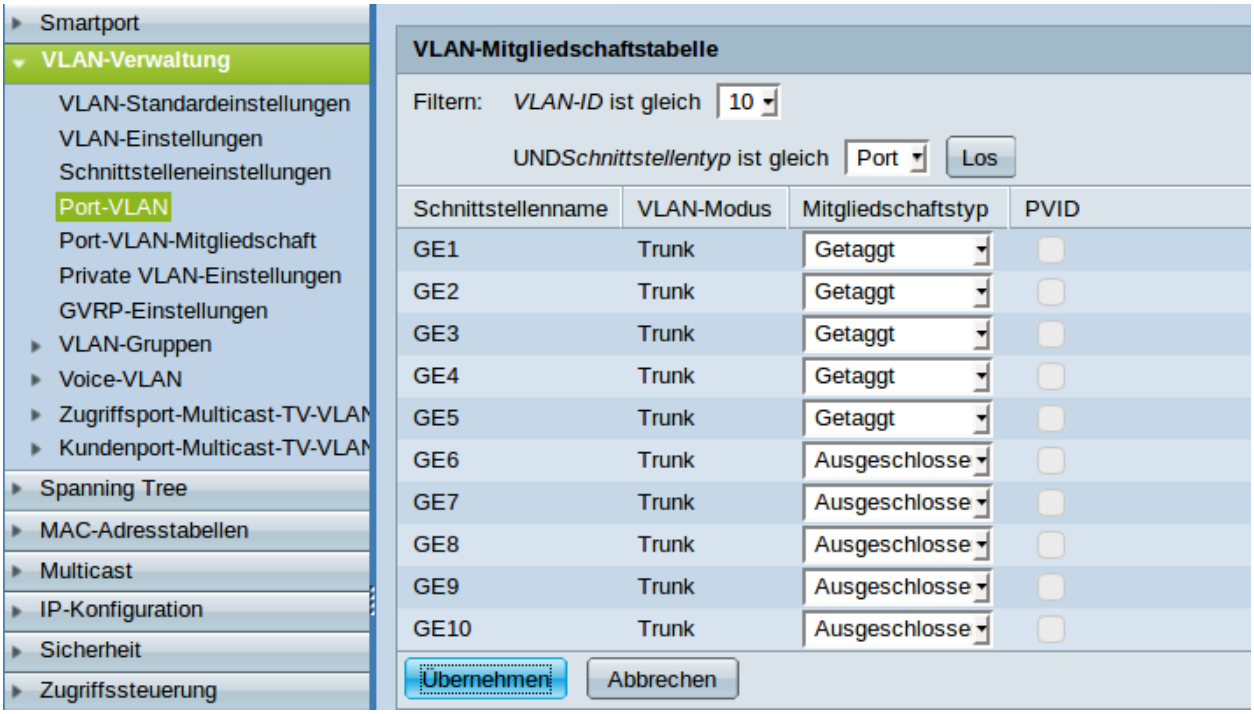
Und schließlich noch VLAN 16.

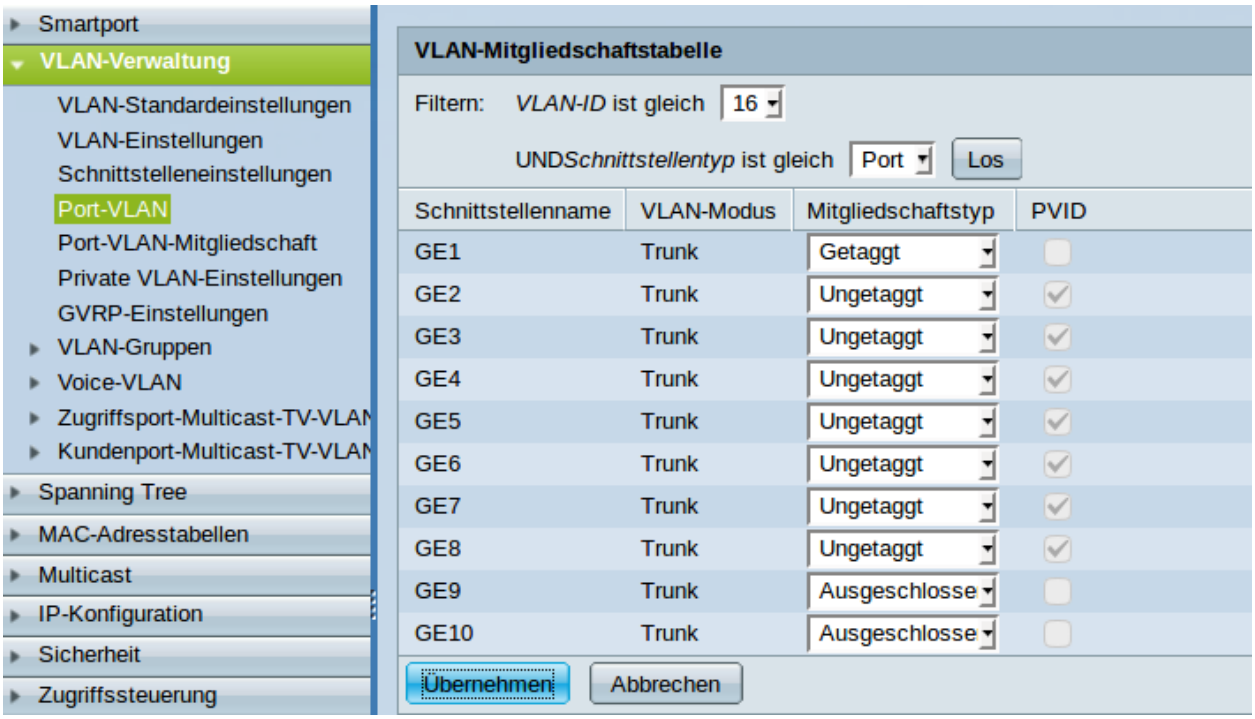
Da die APs und die Clients im Schulnetz sind, sind die Ports 2 bis 8 ungetaggt und PVID ist gesetzt.

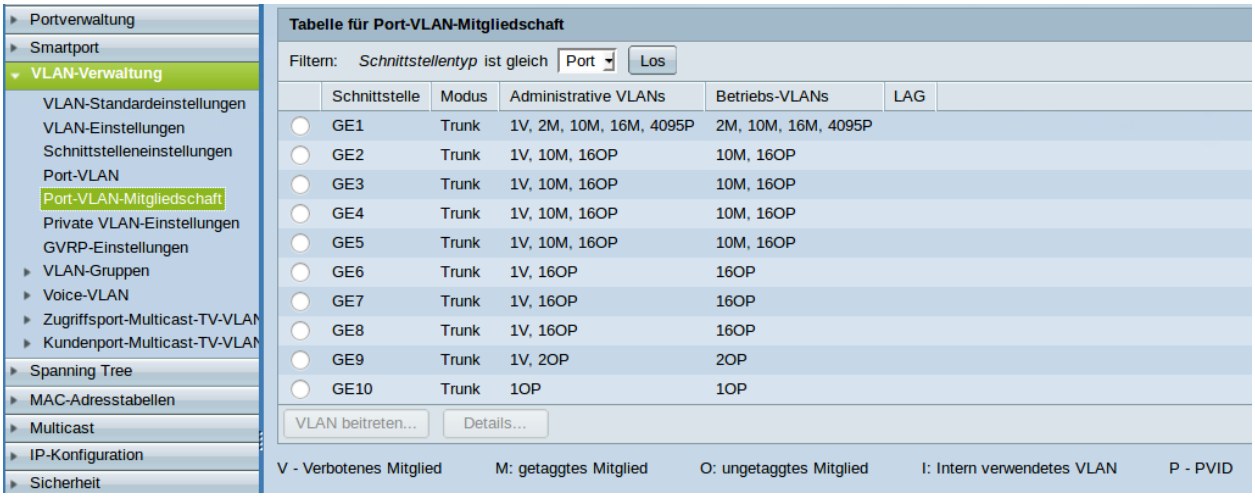
Über *VLAN-Verwaltung* -> *Port-VLAN-Mitgliedschaft* erhält man eine Zusammenfassung.

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 2
UNDSchnittstellentyp ist gleich Port
Los
Schnittstellenname
VLAN-Modus
Mitgliedschaftstyp
PVID
GE1 Trunk Getaggt
GE2 Trunk Ausgeschlosse
GE3 Trunk Ausgeschlosse
GE4 Trunk Ausgeschlosse
GE5 Trunk Ausgeschlosse
GE6 Trunk Ausgeschlosse
GE7 Trunk Ausgeschlosse
GE8 Trunk Ausgeschlosse
GE9 Trunk Ungetaggt
GE10 Trunk Ausgeschlosse
Übernehmen
Abbrechen


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 10
UNDSchnittstellentyp ist gleich Port
Los
Schnittstellenname
VLAN-Modus
Mitgliedschaftstyp
PVID
GE1 Trunk Getaggt
GE2 Trunk Getaggt
GE3 Trunk Getaggt
GE4 Trunk Getaggt
GE5 Trunk Getaggt
GE6 Trunk Ausgeschlosse
GE7 Trunk Ausgeschlosse
GE8 Trunk Ausgeschlosse
GE9 Trunk Ausgeschlosse
GE10 Trunk Ausgeschlosse
Übernehmen
Abbrechen


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 16
UNDSchnittstellentyp ist gleich Port
Los
Schnittstellenname
VLAN-Modus
Mitgliedschaftstyp
PVID
GE1 Trunk Getaggt
GE2 Trunk Ungetaggt
GE3 Trunk Ungetaggt
GE4 Trunk Ungetaggt
GE5 Trunk Ungetaggt
GE6 Trunk Ungetaggt
GE7 Trunk Ungetaggt
GE8 Trunk Ungetaggt
GE9 Trunk Ausgeschlosse
GE10 Trunk Ausgeschlosse
Übernehmen
Abbrechen


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 Port
Los
Schnittstelle Modus Administrative VLANs Betriebs-VLANs LAG
GE1 Trunk 1V, 2M, 10M, 16M, 4095P 2M, 10M, 16M, 4095P
GE2 Trunk 1V, 10M, 16OP 10M, 16OP
GE3 Trunk 1V, 10M, 16OP 10M, 16OP
GE4 Trunk 1V, 10M, 16OP 10M, 16OP
GE5 Trunk 1V, 10M, 16OP 10M, 16OP
GE6 Trunk 1V, 16OP 16OP
GE7 Trunk 1V, 16OP 16OP
GE8 Trunk 1V, 16OP 16OP
GE9 Trunk 1V, 2OP 2OP
GE10 Trunk 1OP 1OP
VLAN beitreten...
Details...
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 .

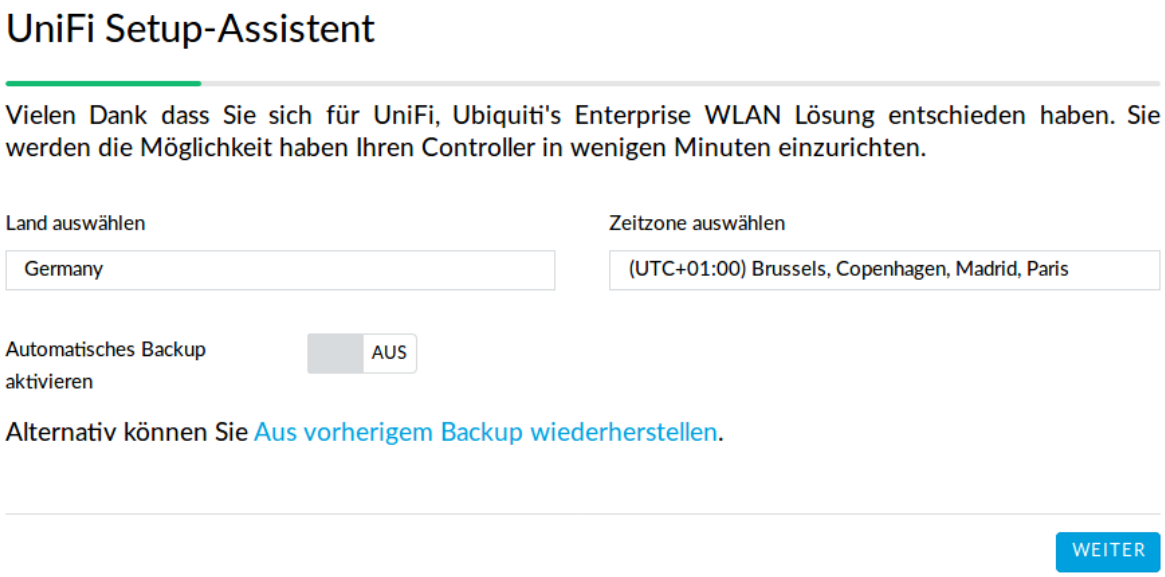
Die Grundkonfiguration

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.



Wähle Germany als Land und klicke auf *weiter*.

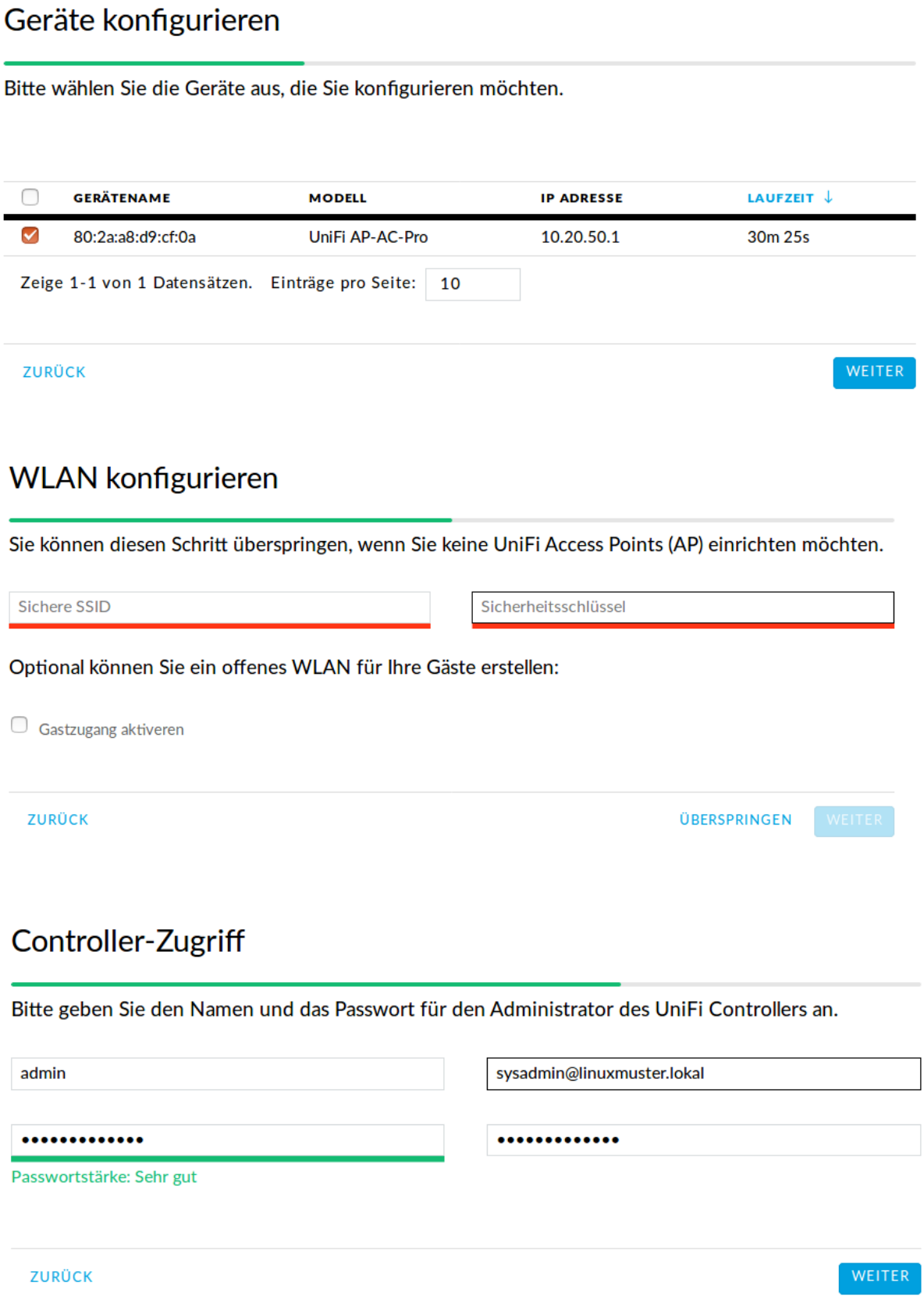
Wähle die Geräte aus, die Du mit dem Unifi-Kontroller managen wöchtest (also alle) und klicke auf *WEITER*.

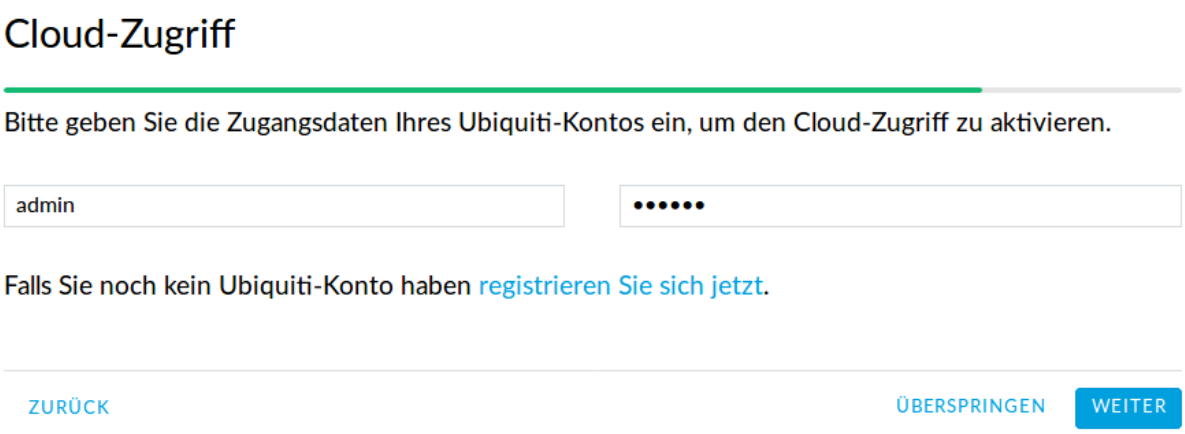
An dieser Stelle überspringst Du die Einrichtung eines WLANs. Das wird später ausführlich beschrieben.

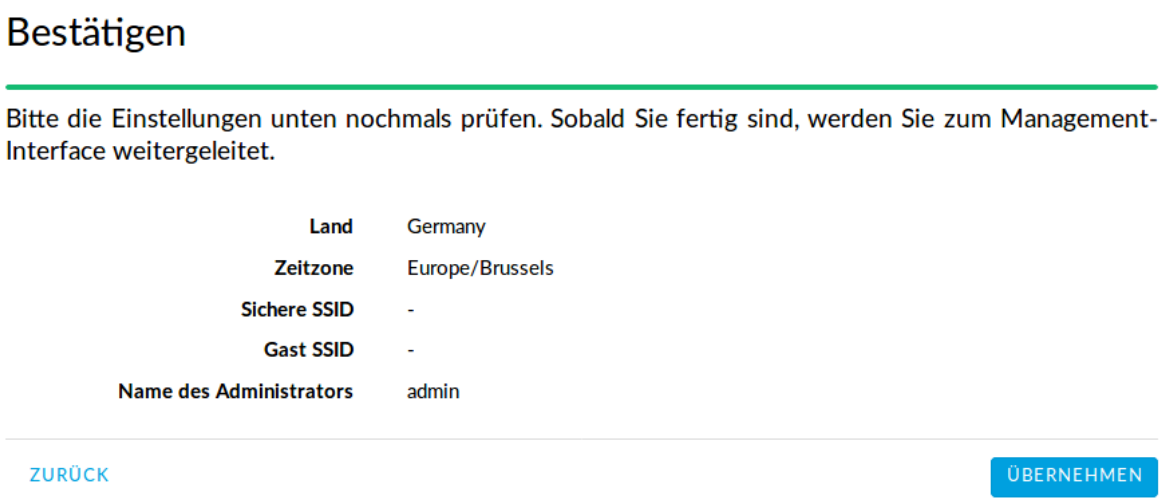
An dieser Stelle wird ein Administrator-Zugang angelegt.

Überspringe auch diesen Schritt.

Bestätige schließlich Deine Einstellungen.


Geräte konfigurieren
Bitte wählen Sie die Geräte aus, die Sie konfigurieren möchten.
GERÄTENAME
MODELL
IP ADRESSE
LAUFZEIT
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:
10
ZURÜCK
WEITER
WLAN konfigurieren
Sie können diesen Schritt überspringen, wenn Sie keine UniFi Access Points (AP) einrichten möchten.
Sichere SSID
Sicherheitsschlüssel
Optional können Sie ein offenes WLAN für Ihre Gäste erstellen:
Gastzugang aktiveren
ZURÜCK
ÜBERSPRINGEN
WEITER
Controller-Zugriff
Bitte geben Sie den Namen und das Passwort für den Administrator des UniFi Controllers an.
admin
sysadmin@linuxmuster.lokal
Passwortstärke: Sehr gut
ZURÜCK
WEITER


Cloud-Zugriff
Bitte geben Sie die Zugangsdaten Ihres Ubiquiti-Kontos ein, um den Cloud-Zugriff zu aktivieren.
admin
••••••
Falls Sie noch kein Ubiquiti-Konto haben registrieren Sie sich jetzt.
ZURÜCK
ÜBERSPRINGEN
WEITER

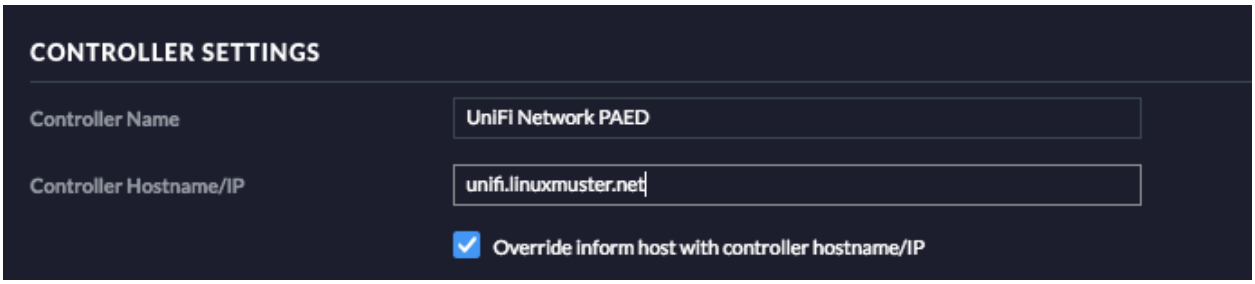

Bestätigen
Bitte die Einstellungen unten nochmals prüfen. Sobald Sie fertig sind, werden Sie zum Management-Interface weitergeleitet.
Land
Germany
Zeitzone
Europe/Brussels
Sichere SSID
-
Gast SSID
-
Name des Administrators
admin
ZURÜCK
ÜBERNEHMEN

Einstellungen zur Aufnahme der APs

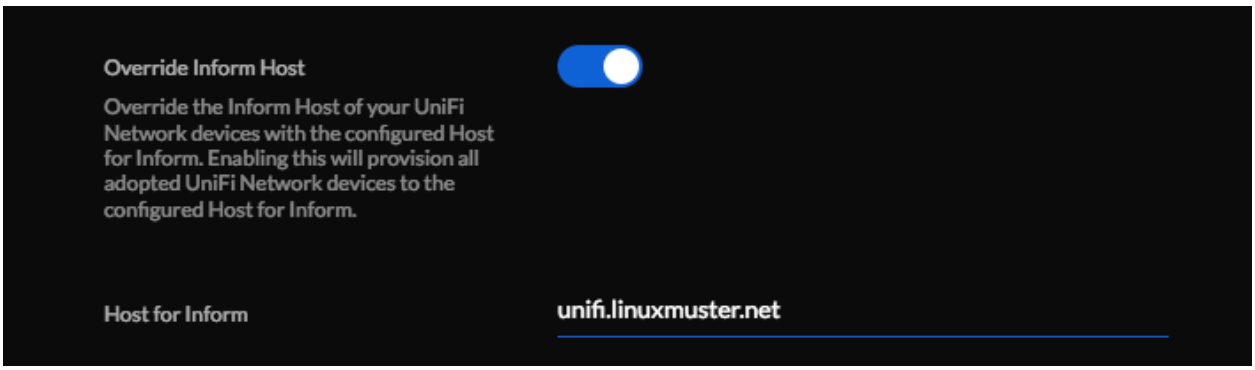
Damit der Unificontroller die angeschlossenen Access Points (APs) aufnehmen kann und mit diesen kommuniziert, sind noch folgende Einstellungen zu treffen:

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:



In der neuen UI des Unifi Controllers entspricht dies folgender Einstellung:



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.

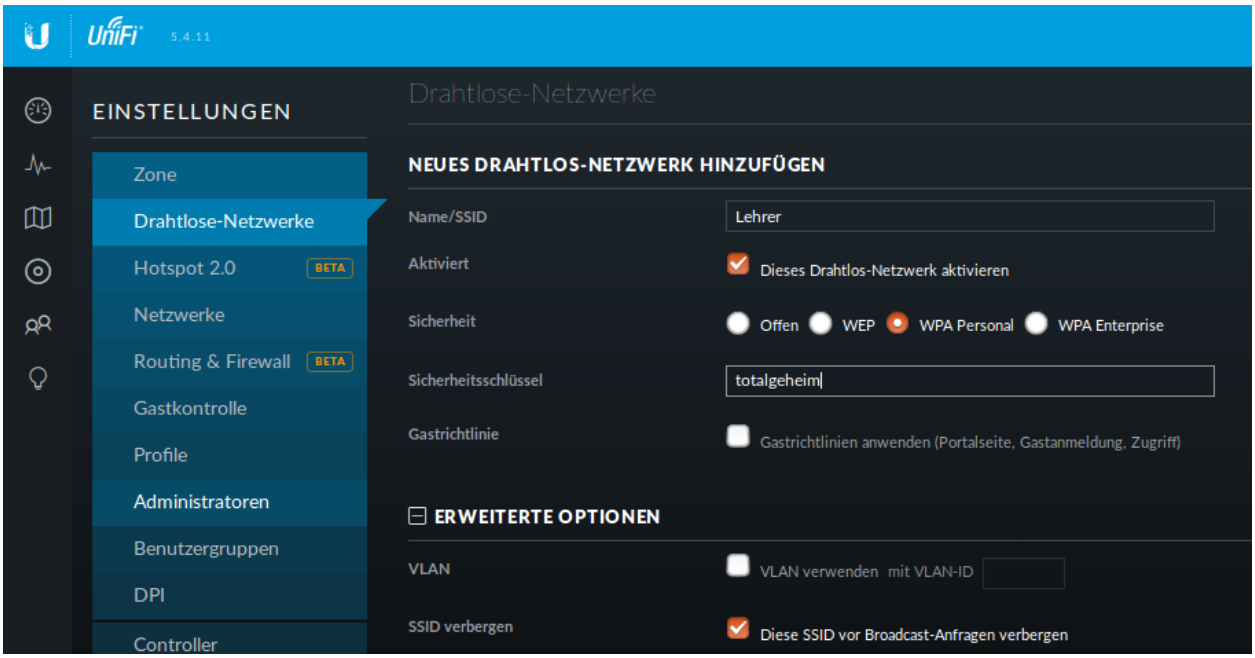
Schritt für Schritt

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 DRAHTLOSES 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

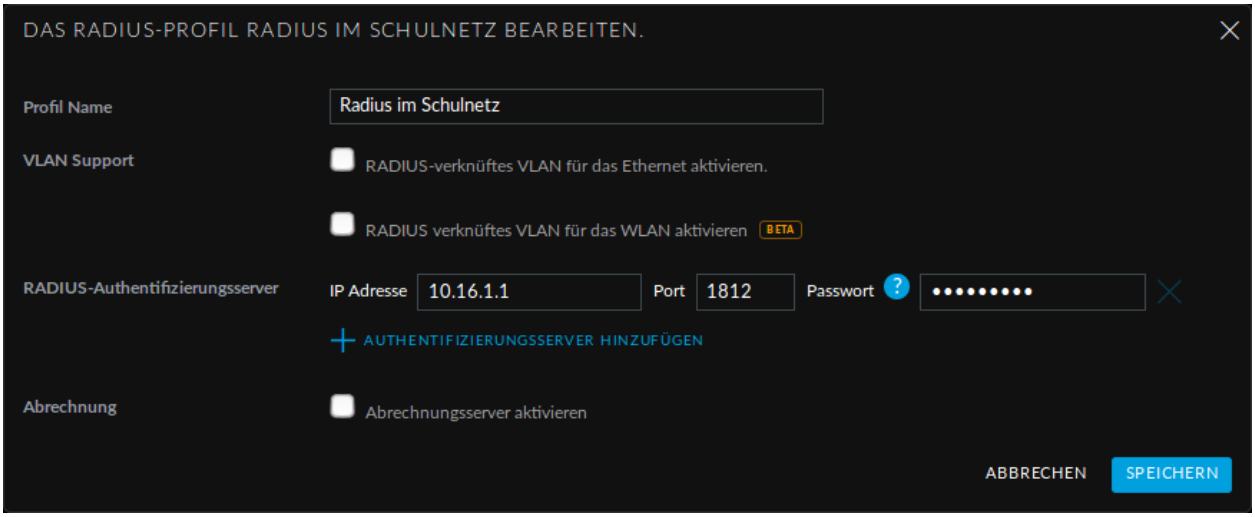
Im Schüler-WLAN sind die Geräte der Schüler. Es liegt im blauen Netz der OPNsense®. Der Netzwerk-Schlüssel des Schüler-WLANs basiert auf ihrem Benutzernamen und ihrem Kennwort.

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*.



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.

Speiche die Einstellungen.

Gehe zu *Einstellungen* -> *Drahtlose-Netzwerke* -> *NEUES DRAHTLOSES NETZWERK HINZUFÜGEN*.

Gib dem Schüler-WLAN einen Namen.

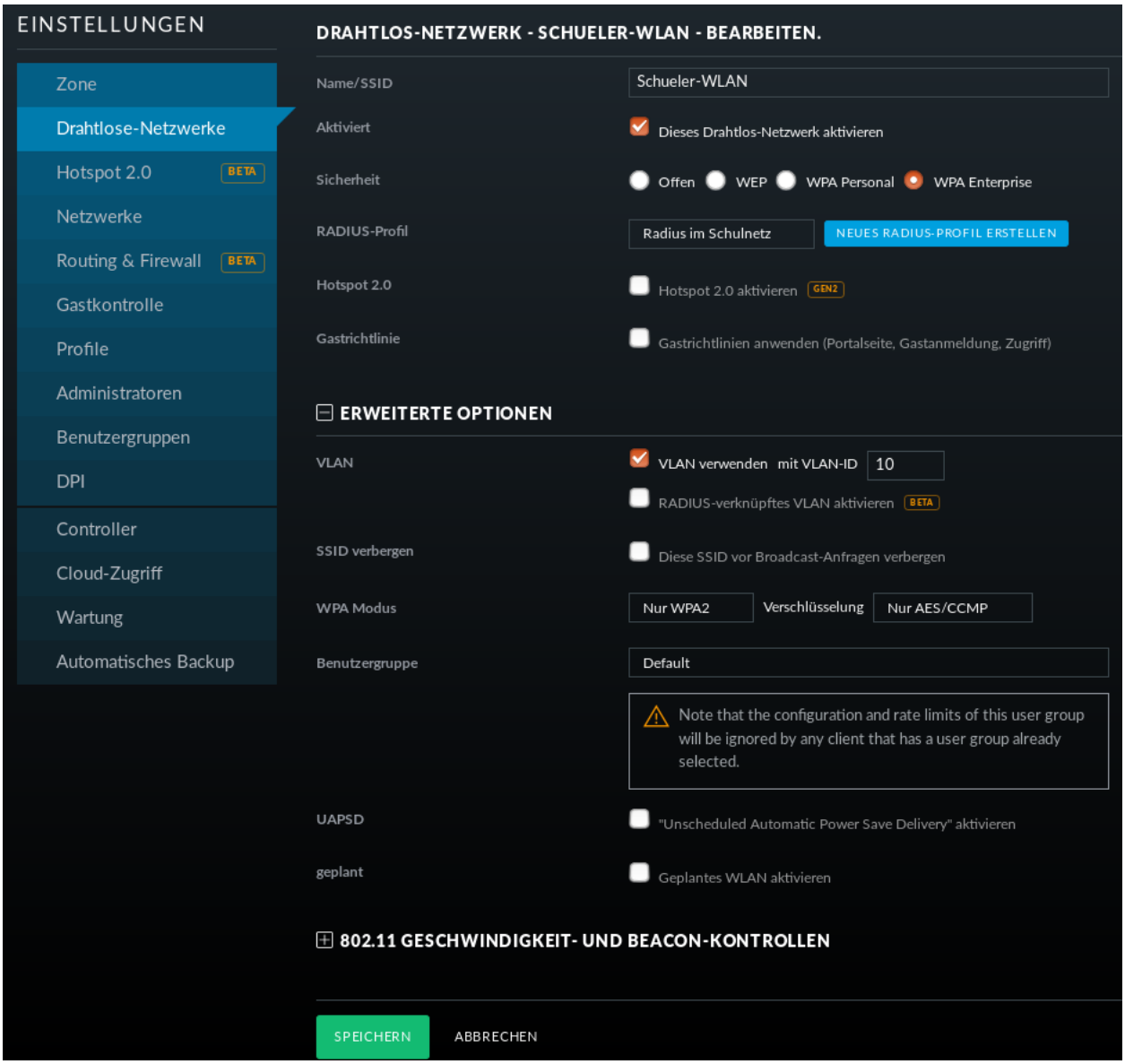
Sicherheit ist *WPA Enterprise*.

Wähle das vorher definierte Radius-Profil.

Da das blaue Netz der OPNsense® als getaggtes VLAN mit der VLAN-ID 10 zu den APs kommt, setze ein Häkchen bei VLAN und gib als VLAN-ID 10 ein.

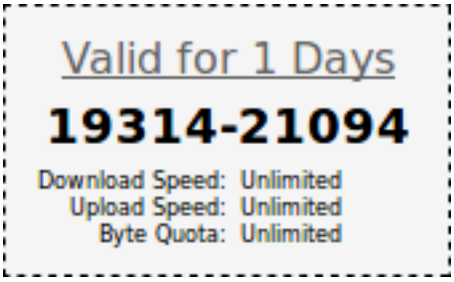
Speichere die Enstellungen.

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
SSID verbergen
Diese SSID vor Broadcast-Anfragen 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.

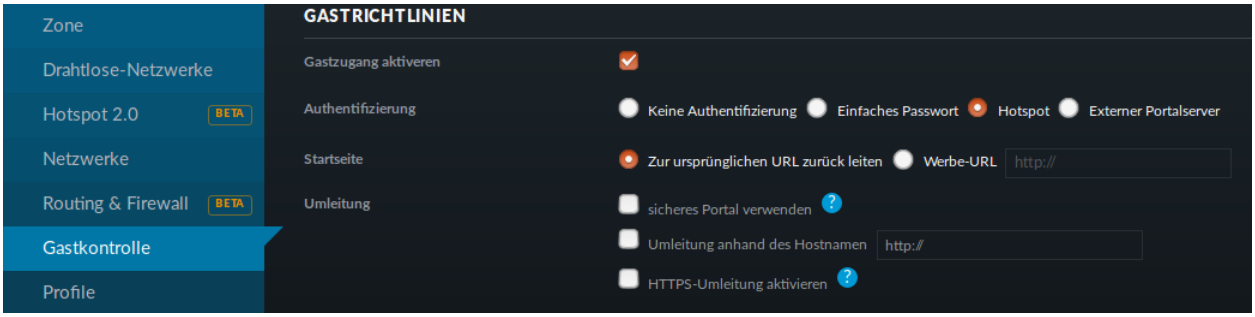
Der Unifi-Controller unterstützt zwei Arten von Gutscheinen:

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*.

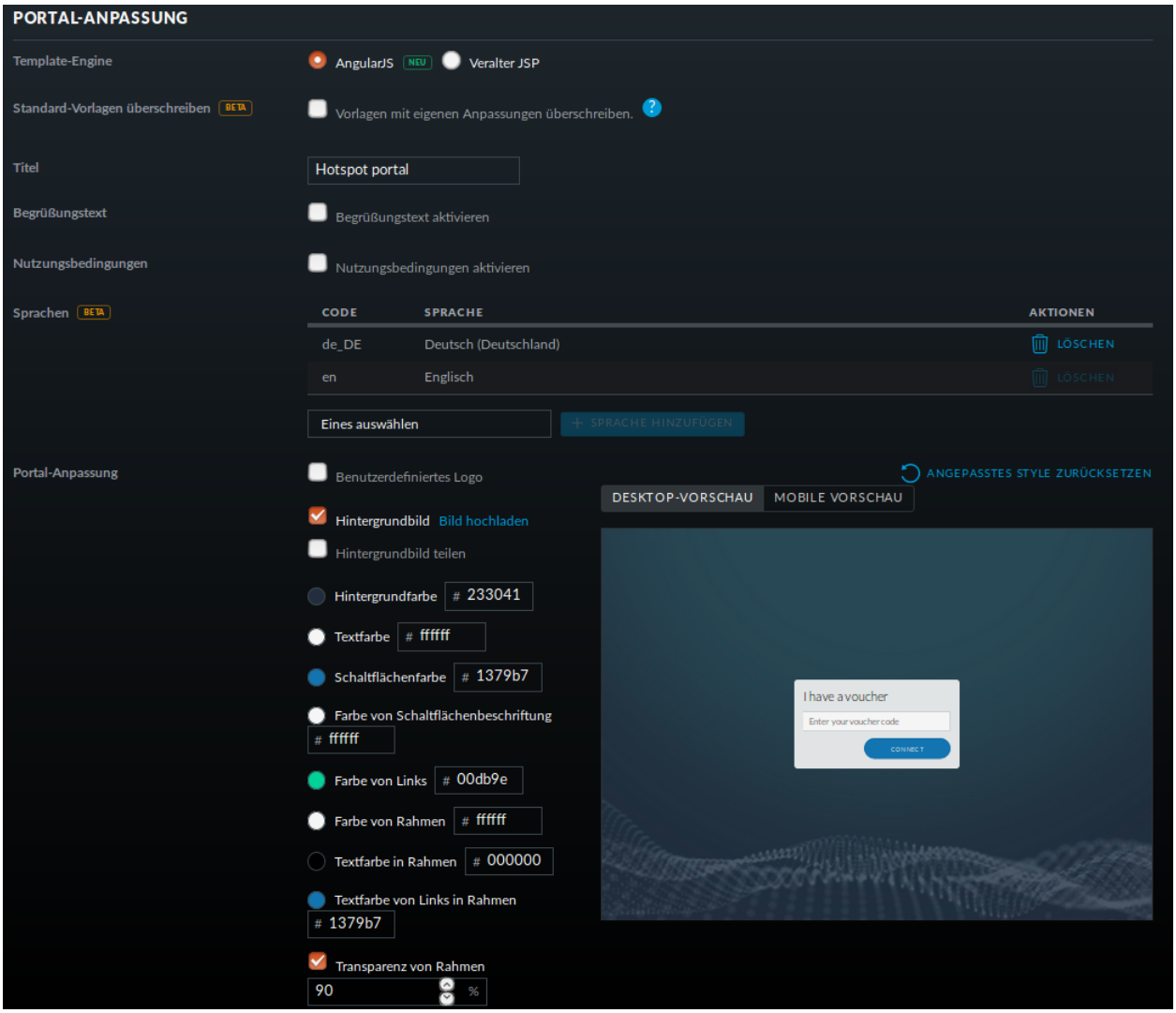
Bei *Authentifizierung* wählst Du *Hotspot*.

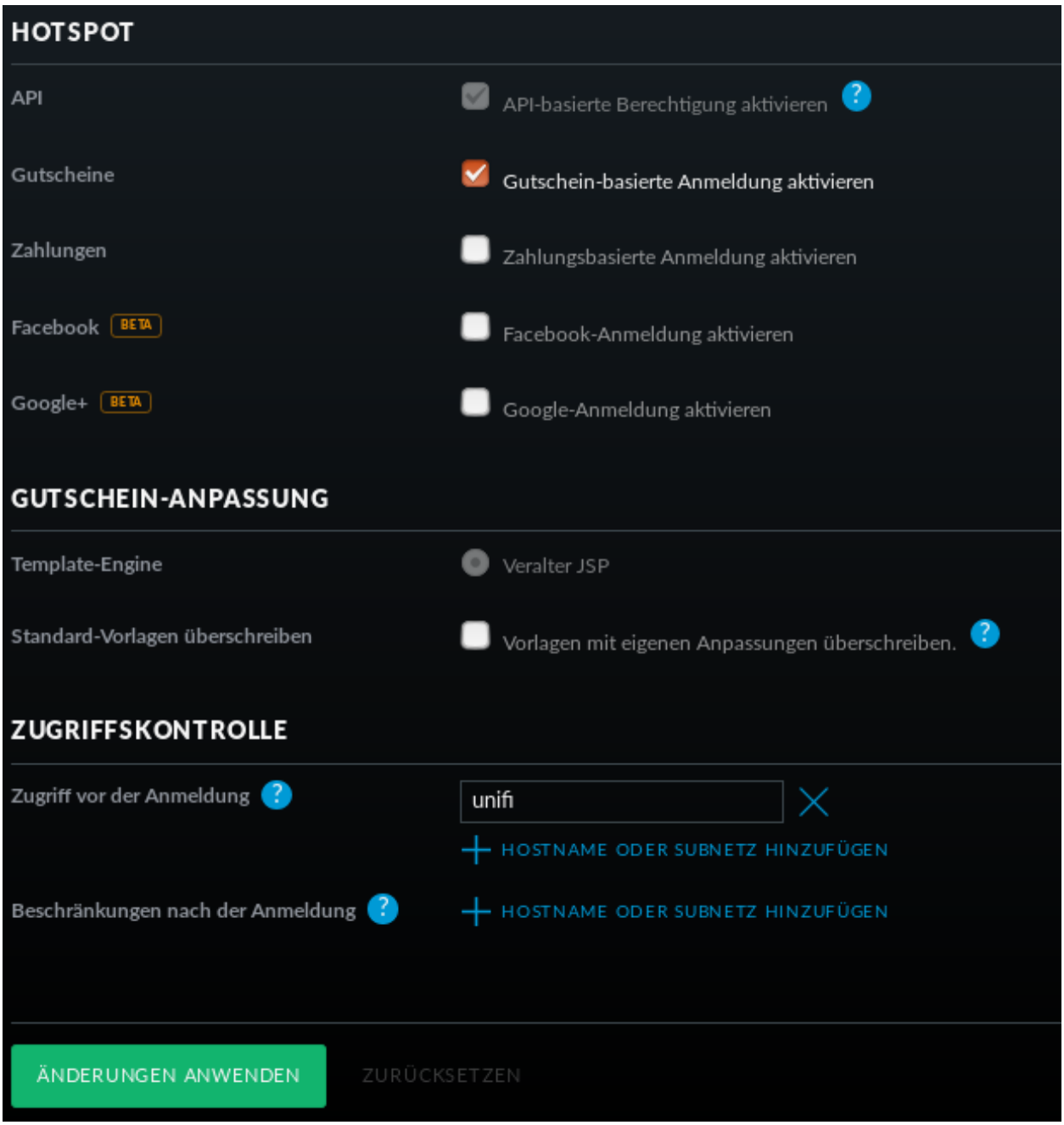
Hat *HTTPS-Umleitung aktivieren* ein Häkchen, so werden Clients auch dann umgeleitet, wenn Sie auf HTTPS-Seiten surfen. Leider erhält man dann eine Zertifikatswarnung, da der Unifi-Kontroller mit einem selbstsignierten Zertifikat arbeitet. Allerdings leiten viele Betriebsysteme von selbst auf das Gastportal 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* setz Du ein Häkchen bei Gutscheine.


PORTAL-ANPASSUNG
Template-Engine
AngularJS NEU
Veralter JSP
Standard-Vorlagen überschreiben BETA
Vorlagen mit eigenen Anpassungen überschreiben.
Titel
Hotspot portal
Begrüßungstext
Begrüßungstext aktivieren
Nutzungsbedingungen
Nutzungsbedingungen aktivieren
Sprachen BETA
CODE
SPRACHE
AKTIONEN
de_DE
Deutsch (Deutschland)
LÖSCHEN
en
Englisch
LÖSCHEN
Eines auswählen
SPRACHE HINZUFÜGEN
Portal-Anpassung
Benutzerdefiniertes Logo
ANGEPASSTES STYLE ZURÜCKSETZEN
DESKTOP-VORSCHAU
MOBILE VORSCHAU
Hintergrundbild
Bild hochladen
Hintergrundbild teilen
Hintergrundfarbe # 233041
Textfarbe # ffffff
Schaltflächenfarbe # 1379b7
Farbe von Schaltflächenbeschriftung # ffffff
Farbe von Links # 00db9e
Farbe von Rahmen # ffffff
Textfarbe in Rahmen # 000000
Textfarbe von Links in Rahmen # 1379b7
Transparenz von Rahmen
90 %
I have a voucher
Enter your voucher code
CONNECT


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.

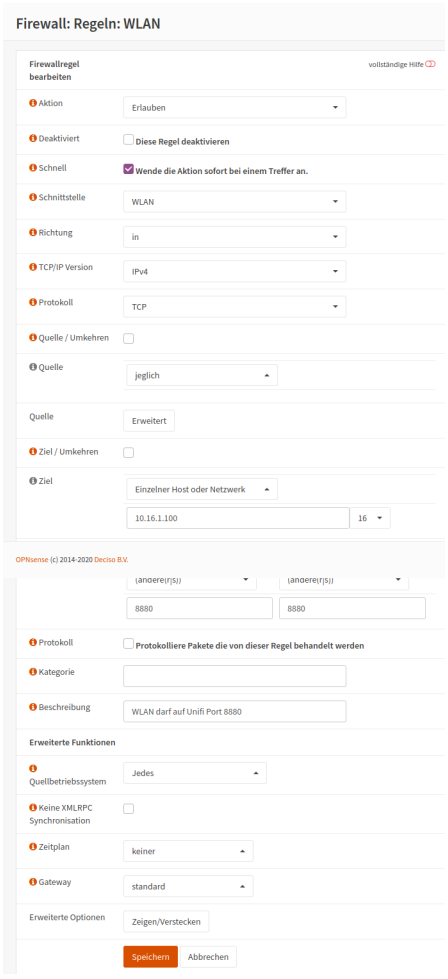
Firewall-Regeln für die OPNsense®

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*.



Mache die folgenden Eingaben:

Schnittstelle: WLAN

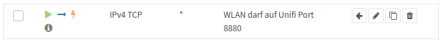
Protokoll: TCP

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*

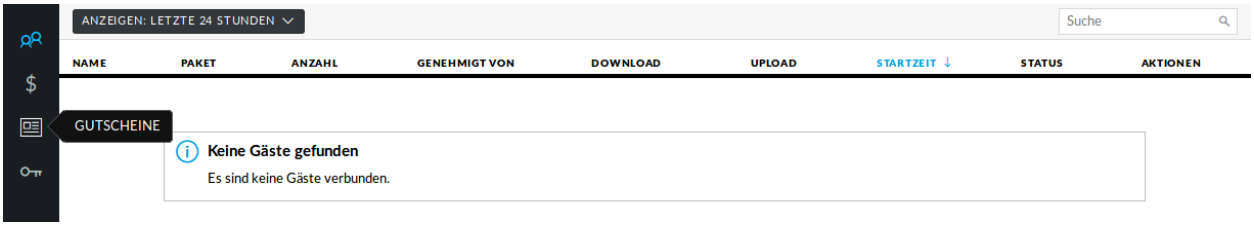
Steichere Deine Eingabe und übernimm die Änderungen.

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.

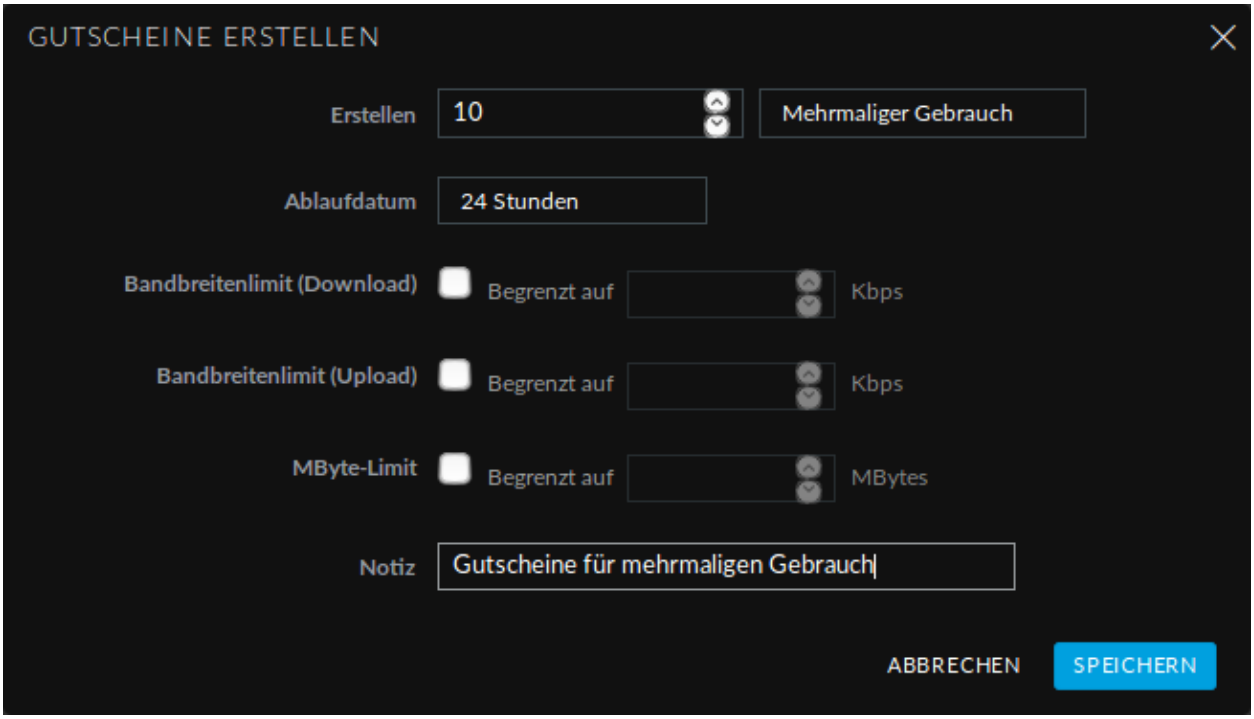
Hier kannst auch Gutscheine löschen.

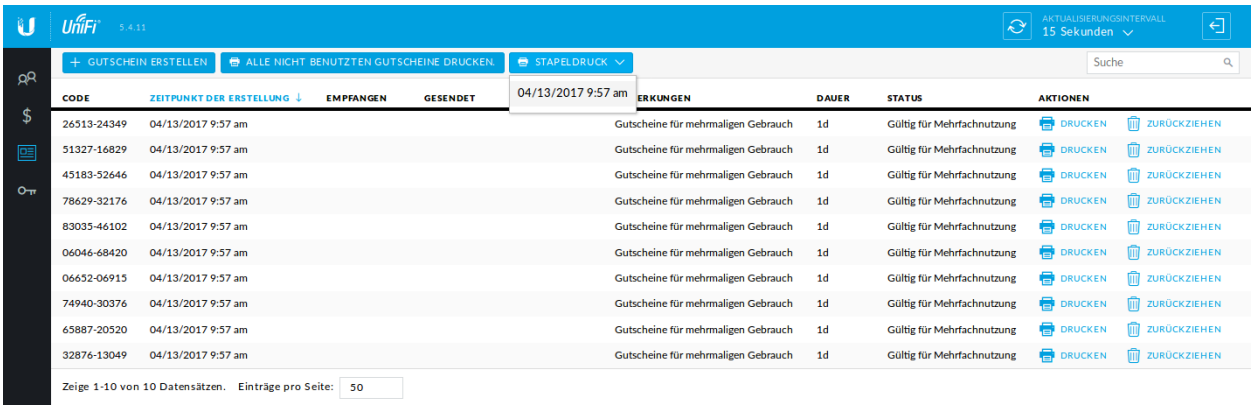
4.45 Mitarbeit linuxmuster.net

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


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.

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.

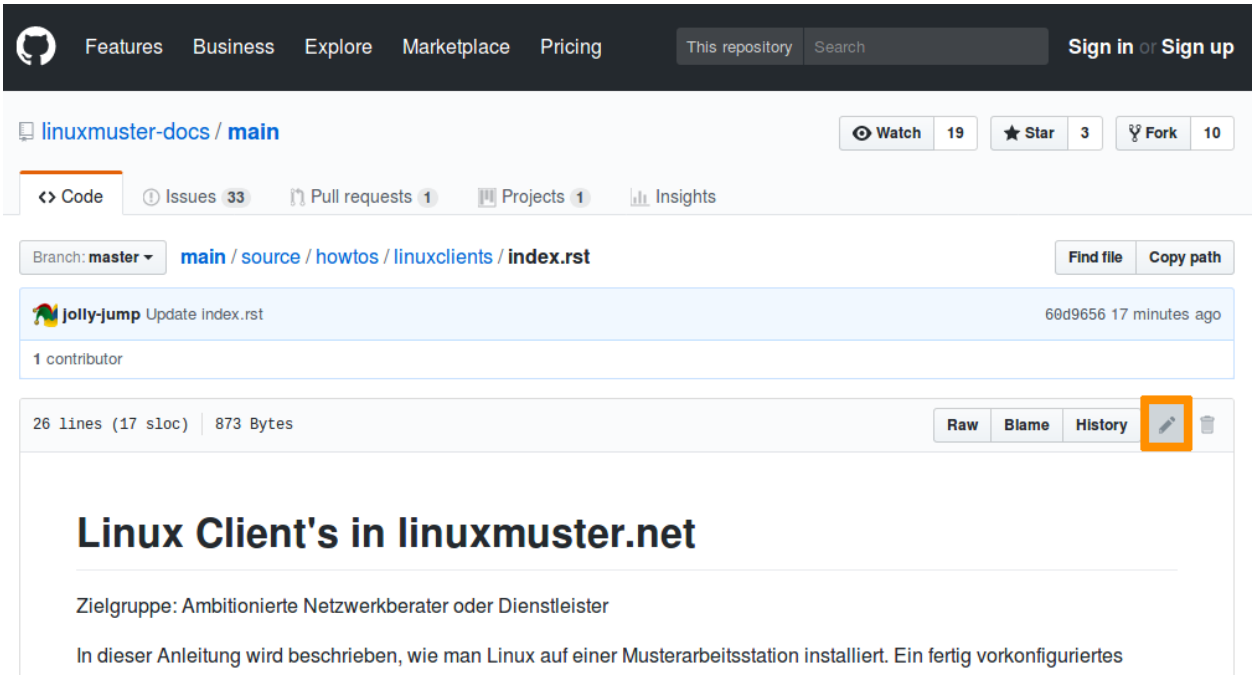
Im Beispiel wurde der Rechtschreibfehler und die Länge der zur Überschrift gehörenden Unterschreichung geändert.

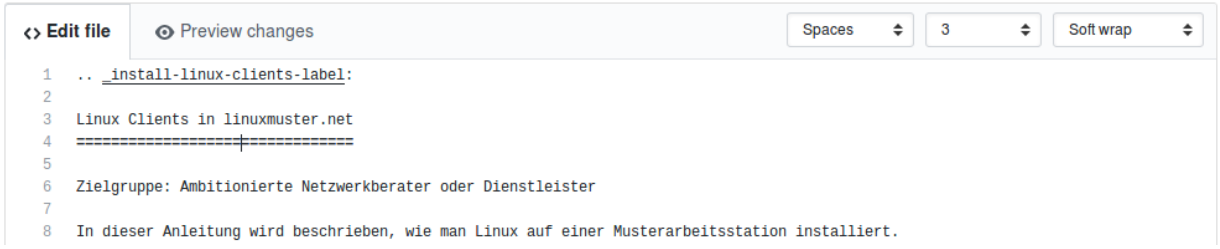
Nachdem Du alle Änderungen vorgenommen hast, gib unten einen Titel und einen Kommentar ein. Die Änderungen können nun mit einem Klick auf „Propose file changes“ eingereicht werden.

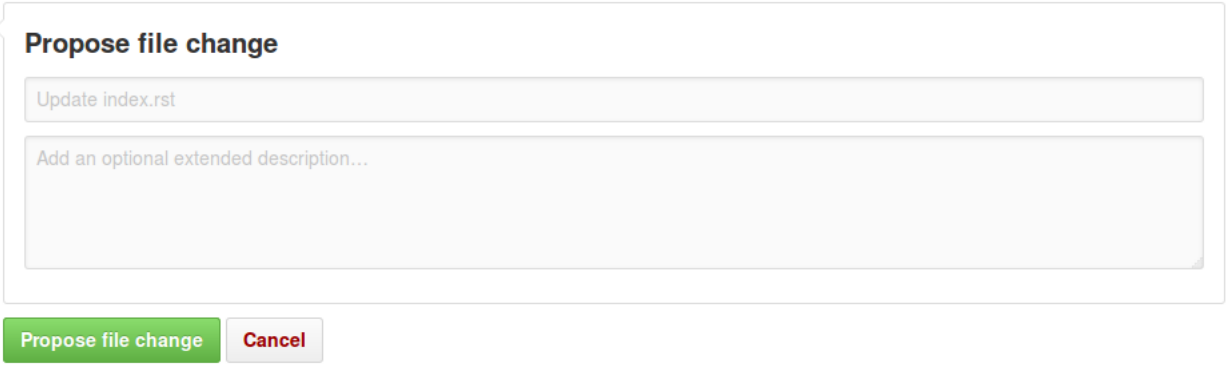
Dein Änderungsvorschlag wird dann vom Dokumentationsteam geprüft und gegebenenfalls übernommen. Sekunden später erscheint die Änderung dann auch hier in der offiziellen Dokumentation.

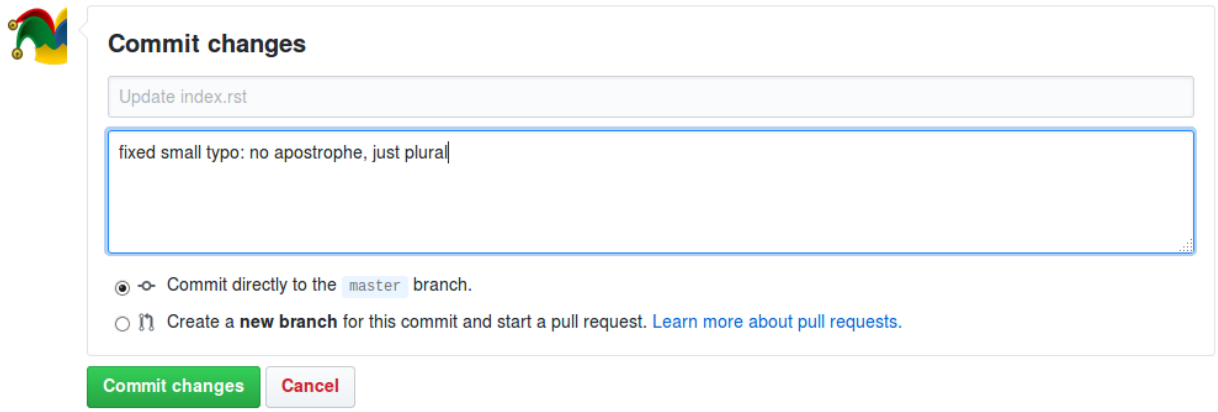
Hinweis: Bitte beachte auch unbedingt die *Leitlinien zur Dokumentation*, damit Deine Änderungen schnell eingepflegt werden könnnen!

Sollest 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
Search
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



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 16.04) Ubuntu-Distributionen git, python und sphinx nachinstallieren:

```
$ sudo apt install git
$ sudo apt install python3-pip
$ pip3 install sphinx
$ pip3 install sphinx_rtd_theme
```

Offizielle Dokumentation kompilieren

Hast Du bereits 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 v1.6.5
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.

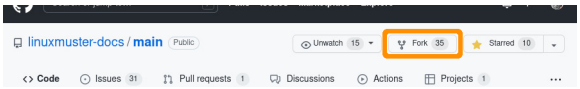
Verifiziere Deine E-Mail-Adresse. Natürlich kannst Du die Dokumentation zu GitHub durchlesen. Weiter geht es dann unter https://github.com/linuxmuster-docs/main

---

Hinweis: Im folgenden wird das Konto „lmn-docs-bot“ verwendet. Überall wo dieser auftaucht, ersetze ihn durch Dein Kontonamen bei GitHub.

Linuxmuster Dokumentation forken

Öffnen Sie die linuxmuster.net Dokumentation auf Github und klicken Sie auf „Fork“.



Öffne nun einen Terminal / Eingabeauffoderung (`Strg+Alt+t` in Ubuntu) and 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 finden Sie einen guten Überblick über die am häufigsten verwendeten Elemente.

Hinweis: Bitte beachten Sie auch unbedingt die *Leitlinien zur Dokumentation*, damit ihre Änderungen schnell eingepflegt werden könnnen!

Im Verzeichnis `source` und den entsprechenden Unterordnern befinden sich alle Dokumentationsdateien. Öffnen Sie einfach eine dieser Dateien und nehmen Sie die gewünschten Änderungen vor. Sie können auch eine neue Dokumentation in einem der Unterordner anlegen. Erstellen Sie dazu einfach einen Ordner mit einem passenden Namen und die notwendige `index.rst` Datei.

```
$ mkdir source/howto/foobar
$ touch source/howto/foobar/index.rst
```

Schaue 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 Sie neue Dateien oder Ordner erstellt haben, müssen diese noch hinzugefügt werden:

```
$ git add source/howto/foobar
```

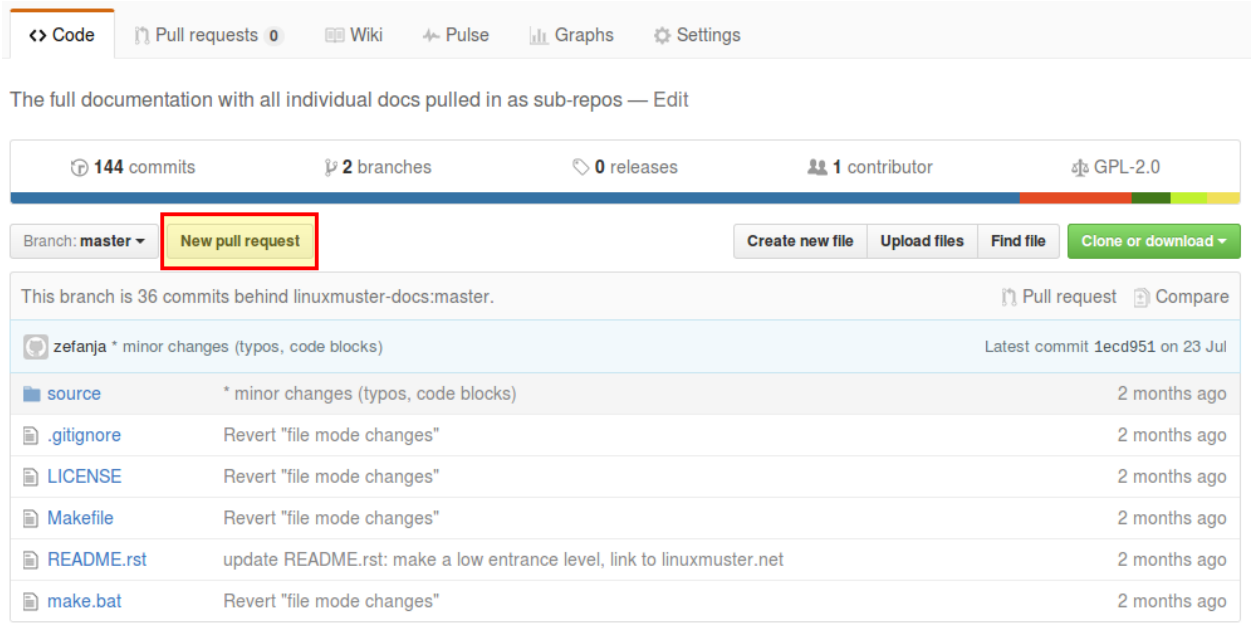
Gib nun noch einen Kommentar zu Deinen Änderungen ein und lade alles in Deinen Fork hoch:

```
$ 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.



Eigenen Fork aktualisieren

Um später weiter Änderungen vornehmen zu können, kann der eigene Fork bei GitHub komplett gelöscht werden 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, sollte man besser den Fork löschen und neu erzeugen. Andernfalls kann man jetzt die offiziellen Änderungen hochladen.

```
~/my-docs$ git push
```

- Jetzt kann man seine lokale 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`, dann gibt es nur Folgendes zu beachten:

1. Man muss einmalig den Zweig mit `git checkout v7` 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
Zu Branch 'v7' gewechselt
Ihr Branch ist auf demselben Stand wie 'origin/v7'.
linuxadmin@lmn-docs:~/my-docs$ git branch
master
* v7
```

   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.

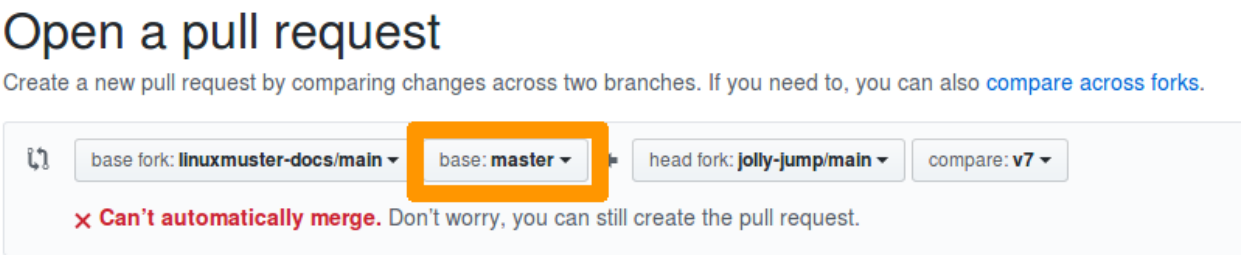


Abb. 55: Ein Pull-Request mit falsch gewähltem Zweig, die sich nicht automatisch zusammenführen lassen.

4. Aktualisiert man den eigenen Fork über das `upstream`-Repository, dann muss man den Befehl zum Zusammenführen anpassen. Ein Ablauf kann da 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         -> upstream/v7
linuxadmin@lmn-docs:~/my-docs$ git branch
master
* v7
linuxadmin@lmn-docs:~/my-docs$ git merge upstream/v7
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 versucht würde zusammenzuführen, was bei sich stark unterscheidenden Zweigen nicht erfolgreich wäre.

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-dargestelltem
```

  - (unter)kapitelbezeichnung <– Titel des Kapitels bzw. des Unterkapitels in dem die Medien-Datei verwendet wird
  - laufende-nummer <– Bilder ihrer Verwendung nach von oben nach unten fortlaufend durchnummeriert; eine führende Null
  - beschreibung-des-dargestelltem <– 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 die wird um eine neu aufsteigende Nummerierung ergänzt.

Medien und Bilder, die in der Dokumentation mehrfach genutzt werden.

Sie sollten von diesem Schema abweichen, da sie nur in dem root-Verzeichnis vorhanden sein müssen. Indem auf die laufenden Nummer und Kapitelbezeichnung 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.

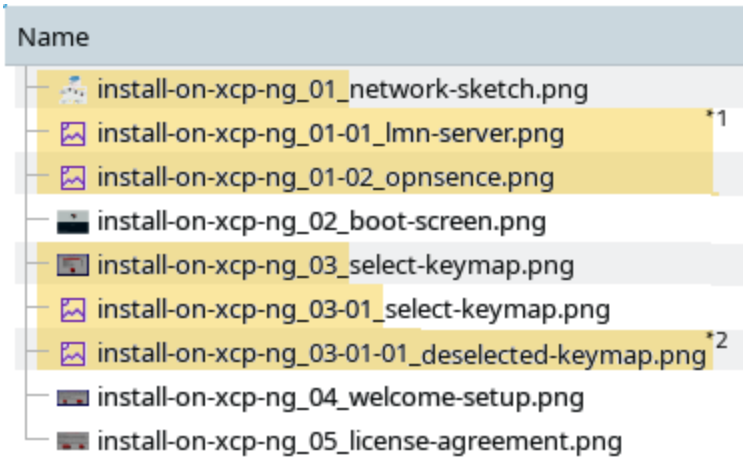


Abb. 56: Beispiel: *1 erste Ergänzung; *2 zweite Ergänzung

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
===============
```

  Bennungen dieser Sprungpunkte sollen immer mit `-label` enden

- Mit diesem Sprungpunkt kann man an anderer Stelle auf ihn verweisen

```
Bitte lesen Sie :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	Rabararabararabara

einzustellen, nutze folgende einfache Syntax

```
========== ============ ==================
Überschrift Überschrift  Überschrift
Spalte A    Spalte B     Spalte C
========== ============ ==================
Bla         Balbla       Blablabla
Blub        Blubblub     Blubblubblub
Rababa      Rababarababa Rabararabararabara
========== ============ ==================
```

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.

Sie »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, sie können auch mehreren anderen Einträgen entsprechen und sogar rekursiv auf andere Einträge verweisen, indem sie Einträge wie CNAME verwenden.

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 »samdom.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 Domänennamen handelt, der durch einen Punkt am Ende des Domänennamens angegeben wird, z. B. »www.samdom.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. »samdom.example.com«, und allen Namen unterhalb dieser Ebene, z. B. »www.samdom.example.com«, »ftp.samdom.example.com« oder »server.samdom.example.com«.

DNS-Server geben autoritative oder endgültige Antworten auf Anfragen mit den Zonen, für die sie konfiguriert sind.

Weitere Einzelheiten zu diesem Verfahren finden Sie auf der [http://en.wikipedia.org/wiki/DNS#Address_resolution_mechanism Wikipedia DNS-Seite].

Warum das wichtig ist?

Der Domänenname, den Sie für Ihre Active Directory-Domäne auswählen, 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 Sie unter anderem Ihre 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 Sie www.samba.org anfragen würden, wäre das auch kein Problem. Der Server würde erkennen, dass er für die Domäne samba.org nicht maßgeblich ist, und die Anfrage an den Server weiterleiten, der für den Namen zuständig ist, und Ihnen dann die Antwort zurückschicken.

Was aber, wenn Sie auch eine externe Website wie »www.samdom.example.com« haben, die wahrscheinlich von einem anderen externen DNS-Server verwaltet wird? Wenn Sie diesen Namen anfordern, wird der DNS-Server feststellen, dass er für die Domäne »samdom.example.com« zuständig ist, und eine Antwort für Sie suchen. Wenn er keine Antwort hat, wird er die Anfrage nicht an einen anderen Server weiterleiten, weil er glaubt, dass er die letzte Autorität für diese Domäne ist. Daher wird er Ihnen 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 Domänennamen 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 sollten Sie keine DNS-Anfragen für interne Namen außerhalb des internen Netzwerks senden. Selbst wenn Sie dem DNS-Server, an den Sie sie senden, vertrauen, 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, den er möchte.

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 sie nur Ihren 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 sie 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 Sie 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 Sie PCs mit doppelten Namen haben, aber nicht, dass Sie 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 Domänennamen akzeptabel sind, können Sie nur wenig tun, um mögliche Namenskonflikte zu vermeiden.

Typischerweise wird empfohlen, den ersten Teil des Domänennamens für die NetBIOS-Domäne zu verwenden (Anmerkung: dies ist ein anderer Name für „Arbeitsgruppe“). Wenn Ihr Domänenname zum Beispiel „samdom.example.com“ lautet, können Sie den NetBIOS-Namen „SAMDOM“ wählen.

Was auch immer Sie für Ihren NetBIOS-Namen verwenden, achten Sie darauf, dass er 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 sie 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, lassen Sie 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 Domänennamen 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 Sie kontrollieren (weil Sie der eingetragene Eigentümer sind), hilft, böswillige Nutzung zu verhindern. Die Registrierung eines Domänennamens ist billig und für jedes Unternehmen ohnehin wünschenswert.
- Der Domänenname sollte immer noch ein gültiger Domänenname sein, sodass Sie auf Wunsch SSL-Zertifikate von Drittanbietern dafür erhalten können.
- Der FQDN für einen Active-Directory-Domänennamen ist auf 64 Byte begrenzt, einschließlich der Punkte, ein Active-Directory-Servername zum Beispiel: »s4ad01.office.example.tld«
- Welchen Domänennamen Sie auch immer verwenden, er 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 würden Sie Ihre Domäne nach dem Muster »subdomain.domainyouown.tld« benennen, z. B. »samdom.example.com«. Dies ist in der Regel die beste Option, die Sie wählen können! Sie 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 Domänennamen aufgestellt haben, vor allem aber:

- Er ist weltweit einzigartig. Da Sie die Registrierung der Domäne im Netz (und vermutlich auch deren DNS-Einträge) kontrollieren, können Sie sicherstellen, dass die von Ihnen intern verwendete Domäne nicht nach außen hin aufgelöst wird.
- Es handelt sich um einen gültigen Domänennamen 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-Domänennamen.

Standardmäßig sind dies die ersten 15 Zeichen des Domänennamens ganz links.

Wenn Ihre Domäne also „ad.example.com“ heißt, dann wäre der Standardvorschlag einfach „AD“.

Die Auswahl eines solchen NetBIOS-Domänennamens 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 Sie jemals eine Vertrauensbeziehung zwischen diesen beiden Domänen einrichten müssten. Wählen Sie stattdessen einen benutzerdefinierten Namen, der auf Ihrem Domänennamen 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. Sie können [https://technet.microsoft.com/en-us/library/cc772007.aspx konfigurieren], was immer Sie wollen, 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 Sie es wünschen (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 Sie ein Zertifikat für einen internen Server ausstellen können, das für »https://server/« anstelle von »https://server.samdom.example.com« gilt, wenn Sie möchten. Und wenn Sie irgendwann einmal die Verwendung des DNS-Such-Suffixes bei einer DNS-Anfrage vermeiden müssen, können Sie das tun, indem Sie den FQDN angeben und dabei daran denken, das abschließende ».« 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 Sie ihn bitten, den Namen „www.example.com“ aufzulösen, wird er erkennen, dass er 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. Sie können jeden beliebigen NetBIOS-Namen wählen. Die Wahl eines Namens, der auf Ihrem Domänennamen basiert, könnte eine gute Alternative sein, oder wählen Sie 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 Ihres Netzes aufzulösen, als Sie ihn außerhalb Ihres Netzes auflösen könnten. 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 Sie 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, zu viel für sie sein. Auf mobilen Geräten ist dieses Schema möglicherweise nicht einmal praktikabel. Zum Glück gibt es einige Lösungen für dieses Problem:

- Erlauben Sie, 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.

- Erstellen Sie eine DNS-Zone, die nur den gewünschten Namen auflöst.:

  Es gibt einen cleveren Trick, mit dem Sie in AD DNS nur einen einzigen Host innerhalb einer Zone auflösen können, während der Rest der Hosts normal vom externen Server aufgelöst wird. Erstellen Sie eine DNS-Zone mit dem Namen „host.domain.tld“, zum Beispiel „mail.example.com“. Erstellen Sie innerhalb der Zone einen einzelnen A- oder CNAME-Eintrag (CNAME ist wahrscheinlich vorzuziehen), wobei Sie den Namen des Eintrags leer lassen. Wie Sie im Dialogfeld sehen, wird dieser Name zur Auflösung der übergeordneten Domäne verwendet, in diesem Fall „host.domain.tld“.

  Dies wird genau das tun, was Sie wollen. „host.domain.tld“ wird wie von Ihnen 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 Sie einen CNAME als übergeordneten Eintrag verwenden, können Sie diesen auf den Eintrag in Ihrem internen Domänennamen zurückverweisen.

4.46.7 Verwendung einer ungültigen TLD

In diesem Szenario würden Sie Ihre Domäne im Format „domain.invalid.tld“ benennen, z. B. »SAMDOM.loca«. 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 sie eine Domäne in Form von „domain.local“ verwendeten. Da die TLD .local offiziell von der ICANN reserviert ist, können Sie 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 können Sie jetzt kein Zertifikat für diese Namen erwerben, wenn sie 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 Sie jetzt verwenden, 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 verwenden Sie 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 Sie die Einträge auf dem externen Server auf Ihrem internen Server duplizieren. Dies kann jedoch unpraktikabel sein, wenn Sie viele externe DNS-Einträge haben oder diese häufig wechseln. Sie können und sollten 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 verwenden Sie einen anderen, nicht verwendeten Domänennamen als Ihren primären Internet-Domänennamen. Sie könnten 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 clevere DNS-Tricks (siehe oben) erzielt werden. Außerdem besteht jedes Mal, wenn Sie Namen extern anders auflösen 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 B E T A: Update auf lmn 7.2

Autor des Abschnitts: @cweikl

> **Achtung:** Die Version linuxmuster.net 7.2 ist noch im Beta-Stadium und n i c h t für den produktiven Einsatz geeignet.

Die Version linuxmuster.net 7.2 bringt

- volle Unterstützung von Ubuntu 22.04 LTS
- Linbo 4.1 mit einem akuellen Linux-Kernel 6.1.* und einem nativen NTFS-Kernel Treiber
- Linbo 4.1: NEW - jetzt mit Option auch differentielle Images zu erstellen

4.47.1 Update auf lmn 7.2

Vorbereitungen

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`.

Gebe 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 erhälst 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.

Zudem müssen nach der Installation einiger neuerer Bibliotheken einige Dineste 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:

```
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 (Achtung: testing) wie folgt hinzu:

Importiere zuerst die Schlüsseldatei:

```
sudo wget -qO- "https://deb.linuxmuster.net/pub.gpg" | gpg --dearmour -o /usr/share/
↪keyrings/linuxmuster.net.gpg
```

Füge danach das Linuxmuster 7.2 Testing-Repro 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 nun die Paketquellen:

```
sudo apt update
```

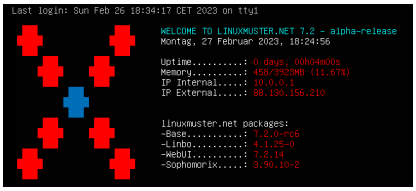
7. Aktualisiere die installierten Pakete und führe anschließend ein Reboot durch:

```
sudo apt dist-upgrade
sudo 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 4.1 aktualisiert.
10. Synchronisiere das Betriebssystem und melde Dich danach mit einem Domänen-Benutzer an.



Hinweis: Glückwunsch ! Du hast Dein System nun auf lmn 7.2 aktualisiert. Du kannst nun alle Neuerungen testen. Denke daran, dass die Version noch im Beta-Stadium ist. Bei Fragen oder Auffälligkeiten schaue unter https://ask.linuxmuster.net/t/lmn-7-2-testing/9732