Netzwerktechnik

Mag. Ing. Thomas Höllerer

2021/22

HTL Krems

Felix Schneider

25.05.2022

**Inhaltsverzeichnis:**

[1 Aufgabenstellung 3](#_Toc105151255)

[1.1 Debian Expert Install aufsetzen 3](#_Toc105151256)

[1.2 Debian Server Pakete installieren 3](#_Toc105151257)

[2 Vorbereitungen 3](#_Toc105151258)

[2.1 Debian Expert Install aufsetzen 3](#_Toc105151259)

[3 Übungsdurchführung 4](#_Toc105151260)

[3.1 Virtuelle Debian Maschine 4](#_Toc105151261)

[3.2 Aptitude + Putty 11](#_Toc105151262)

[3.3 wichtige Befehle zum Herausfinden von Informationen 14](#_Toc105151263)

[3.4 Virtuelle Windows Maschine 17](#_Toc105151264)

[3.5 Virtuelle Debian Maschine Kopie 20](#_Toc105151265)

[3.6 Windows Internet 27](#_Toc105151266)

[3.7 DHCP Server 28](#_Toc105151267)

[3.8 Firewall 31](#_Toc105151268)

[3.9 IPv6 35](#_Toc105151269)

[3.10 Apache2 38](#_Toc105151270)

[3.11 Samba 39](#_Toc105151271)

[3.12 DNS-Server 42](#_Toc105151272)

[4 Abbildungsverzeichnis 48](#_Toc105151273)

[5 Codeverzeichnis 50](#_Toc105151274)

[6 Ergebnisse 51](#_Toc105151275)

[7 Kommentar 51](#_Toc105151276)

# Aufgabenstellung

## Debian Expert Install aufsetzen

Wir legen eine neue virtuelle Maschine mithilfe der Software **VMWare Workstation Player** an und setzen darauf eine Debian Maschine ohne grafische Oberfläche auf. Dafür verwenden wir eine ISO-Datei mit Debian Version 11.0.0.

Wir benötigen einen root- und einen normalen Benutzeraccount.

## Debian Server Pakete installieren

# Vorbereitungen

## Debian Expert Install aufsetzen

Die **ISO-Datei** kann man vom Internet herunterladen:

* 64-Bit-Version: <https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/debian-11.1.0-amd64-netinst.iso>
* 32-Bit-Version: <https://cdimage.debian.org/debian-cd/current/i386/iso-cd/debian-11.1.0-i386-netinst.iso>

Die App **VMWare Workstation 16 Pro Player** kann hier heruntergeladen werden:

* <https://www.vmware.com/go/getworkstation-win>

# Übungsdurchführung

## Virtuelle Debian Maschine

### Virtuelle Maschine erstellen

Um eine virtuelle Maschine zu erstellen, öffnen Sie die App VMWare Worstation Player und drücken auf Player 🡪 File 🡪 New Virtual Maschine…

Anschließend wählen Sie in dem Fenster, das aufgegangen ist, „Installer disc image file (iso):“ aus und suchen nach der auf ihrem Computer installierten Debian 11 ISO-Datei. Wählen Sie diese aus und klicken Sie auf „Next🡪“.



Abbildung : ISO Datei auswählen

Wählen Sie beim nächsten Fenster „Linux“ bei „Guest operating system“ und „Debian 10.x 64-bit“ unter „Version“ aus. Wenn Sie über einen 32-bit Rechner verfügen, wählen Sie statt „Debian 10.x 64-bit“ „Debian 10.x 32-bit“ aus. Klicken Sie auf Next🡪.

zusätzliche Informationen: Auch wenn Sie eine Debian 11 ISO File heruntergeladen haben und virtuell eingelegt haben, wählen wir hier Debian 10 aus, weil dies die letzte Version ist, die VMWare unterstützt (Stand 2021).

Beim nächsten Fenster geben Sie einen sinnvollen Namen der neuen virtuellen Maschine ein. Dieser wird nach Abschluss der Erstellung in der List in VMWare Workstation Player angezeigt. Außerdem wählen Sie den Speicherort der Installation. Beachten Sie, dass Sie ein Laufwerk mit genügend Speicherkapazität auswählen sollten!

Anschließend werden Sie aufgefordert, die Speicherkapazität der Virtuellen Maschine einzustellen. Es wird empfohlen mindestens die empfohlene Größe des Speichers einzuhalten. Wenn die empfohlene Größe also 20GB beträgt, sollten Sie keine 18GB verwenden, sondern mindestens 20GB, besser mehr als weniger. Beachten Sie hierbei, dass Sie nicht zu viel Kapazität freigeben, sondern nur maximal so viel wie auf dem vorhin eingestellten Laufwerk verfügbar ist. Die Kapazität wird nicht direkt von der Virtuellen Maschine verwendet, erst wenn der Speicherplatz benötigt wird.

Außerdem können Sie wählen, ob Sie diese Kapazität in einer einzigen Datei speichern möchten oder in mehreren kleineren Dateien speichern möchten. Das Teilen der virtuellen Disk hat den Vorteil, dass die einzelnen Dateien kleiner sind, dadurch können Sie auch FAT32 als Speicherart verwenden. FAT32 hat nämlich eine Dateigrößenbegrenzung von 4GB.

### Hardwareeinstellungen konfigurieren

Konfigurieren Sie die Hardwareeinstellungen folgendermaßen:

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : Hardwareeinstellungen

Wichtig sind hierbei folgende Einstellungen:

* der Arbeitsspeicher bzw. RAM 🡪 Sie müssen nicht 4GB wählen; mind. 2GB wird empfohlen
* der Netzwerkadapter: damit Sie ins Internet kommen benötigen Sie eine Netzwerkkarte mit NAT
* Wenn Sie eine bessere Performance wollen, können Sie (falls Ihr Computer das unterstützt) mehrere CPU-Kerne hinzufügen

zusätzliche Informationen: NAT – Network Address Translation – ersetzt die IP-Adresse der Virtuelle Maschine mit der IP-Adresse des Hosts. Somit kommen Sie ins Internet. Ein außenstehender PC kann nicht unterscheiden, ob der Internetzugriff vom Host oder der Virtuelle Maschine kommt (die IP-Adressen sind ja identisch). Über die Portnummer kann der Host allerdings das Paket wieder zur Virtuellen Maschine zurückleiten.

### Expert Install starten

Starten Sie die gerade eben neu erstellte Virtuelle Maschine. Die Virtuelle Maschine lädt nun Daten der ISO Datei, dies kann ca. eine Minute dauern. Wenn die Daten fertig geladen sind, erscheint ein Fenster mit verschiedenen Optionen. Wählen Sie „Advanced options“ und anschließend „Expert Install“ aus.

Die Installation wurde jetzt gestartet. Das Protokoll führt Sie nun durch die einzelnen Schritte, die Sie durchführen müssen, um die Installation zu vollenden.

### Sprache und Tastatur auswählen

Als erstes wählen Sie die richtige Sprache aus. **Mit den Pfeiltasten können Sie navigieren, mit Enter wählen Sie dann die Option aus.** Wählen Sie „Choose language“ aus und suchen Sie nach Ihrer Sprache (wahrscheinlich German, ansonsten würden Sie dieses Protokoll nicht lesen 😊). Anschließend werden Sie nach dem Land und dem Gebietsschema gefragt, hier wählen Sie bitte jeweils das Land oder Gebiet aus, in dem Sie wohnen.

zusätzliche Information: UTF-8, die Kodierung für Unicode Zeichen, ist in allen deutschsprachigen Ländern gleich. Jedoch variiert die Kennung.

Nachdem die Sprache konfiguriert wurde, werden Sie jetzt „Tastatur konfigurieren“ auswählen und das Layout Ihrer Tastatur heraussuchen.

### Installer-Komponenten vom Installationsmedium laden

Laden Sie das Installationsmedium, das erkannt wurde, und binden Sie dieses ohne zusätzliche Komponenten ein.

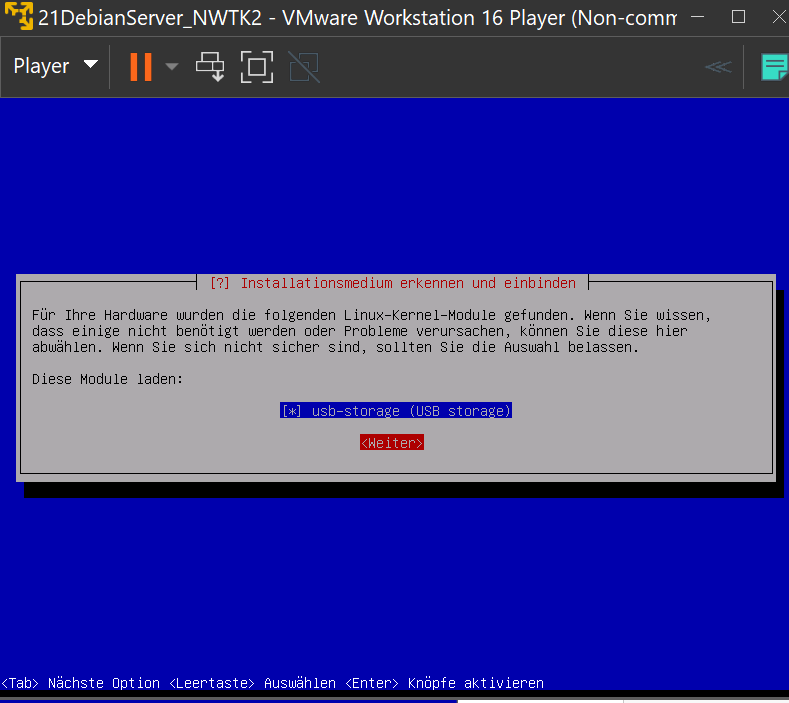


Abbildung : Medium einbinden/laden

### Netzwerk einrichten

Wieder im Hauptmenü zurück, klicken Sie auf „Netzwerk-Hardware erkennen“. Wenn keine Fehlermeldung auftritt, wurde die Netzwerk-Hardware erfolgreich erkannt und Sie können „Netzwerk einrichten“ aufrufen.

Sie wollen das Netzwerk automatisch einrichten, für die Wartezeit und den Rechnernamen am besten die voreingestellten Einträge so lassen, wie sie sind, und als Domain-Name **<IhrenNamen>.local** eintragen.

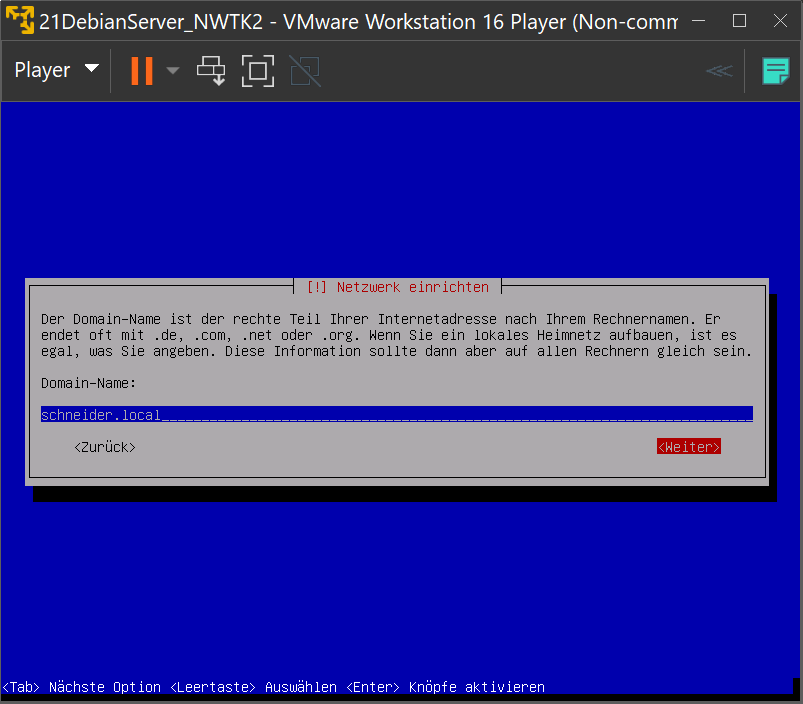


Abbildung : Name der Domain eingeben

zusätzliche Information: Der Domain-Name endet mit .local, weil Sie ein privates Netzwerk aufbauen wollen und .local auf den Rechner selbst verweist.

### Benutzer und Passwörter einrichten

Als nächstes richten Sie Benutzer mit zugehörigem Passwort ein. Es wird empfohlen Shadow-Passwörter zu verwenden, eine Methode, die die verschlüsselten Passwörter in der /etc/shadow-Datei speichert und nicht, wie früher, in der /etc/passwd-Datei.

zusätzliche Information: Das war nämlich eine Sicherheitslücke, wenn Programme einen Benutzernamen oder bestimmte Gruppen herausfinden wollten. Diese Informationen stehen nämlich ebenfalls verschlüsselt in der /etc/passwd-Datei. Das bedeutet, wenn ein Programm die entschlüsselte /etc/passwd-Datei ausgelesen hat, stand das Passwort direkt dabei (unverschlüsselt!). Bei Shadow-Passwörtern steht das Passwort dann in /etc/shadow.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : Shadow-Passwörter

Erlauben Sie die Anmeldung als root, Sie können auf der Virtuellen Maschine sowieso nicht viel kaputtmachen. Geben Sie ein sicheres Root-Passwort ein und bestätigen Sie dieses im nächsten Schritt. Erstellen Sie auch mindestens ein normales Benutzerkonto, für den Fall, dass Sie sich mit dem Root-Account nicht einloggen können.

Es ist wichtig, dass man neben dem root-Account zusätzlich auch noch ein Benutzerkonto anlegt, für den Fall, wenn man mit dem root-Account nicht einsteigen kann, hat man immer noch die Möglichkeit mit dem Benutzerkonto einzusteigen.

### Uhr einstellen

Im nächsten Schritt stellen Sie die Uhr ein. Verwenden Sie kein NTP (Network Time Protocol), weil der Host die Uhrzeit bereits richtig eingestellt hat. Anschließend müssen Sie nur noch Ihre Zeitzone auswählen.

### Festplatte partitionieren

Der nächste große Schritt ist die Festplattenpartitionierung. Klicken Sie hierzu vorerst auf „Festplatten erkennen“, wodurch das Installationsprogramm nach Festplatten sucht. Anschließend wählen Sie „Festplatten partitionieren“ und „manuell“ aus.

Nun sollten Sie ungefähr so eine Auswahl sehen:

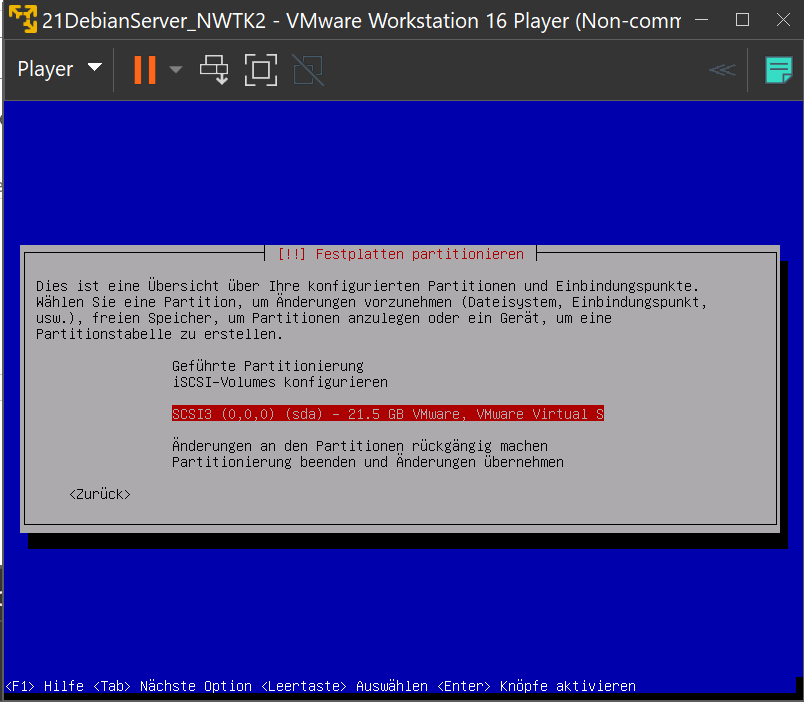


Abbildung : Übersicht – Festplatte partitionieren

Wählen Sie die gefundene Festplatte aus und erstellen Sie eine neue leere Partitionstabelle. Der Partitions-Typ soll msdos sein, Sie können allerdings auch andere Typen verwenden. Wie Sie dann sehen können, hat die Festplatte eine neue Partitionstabelle bekommen:

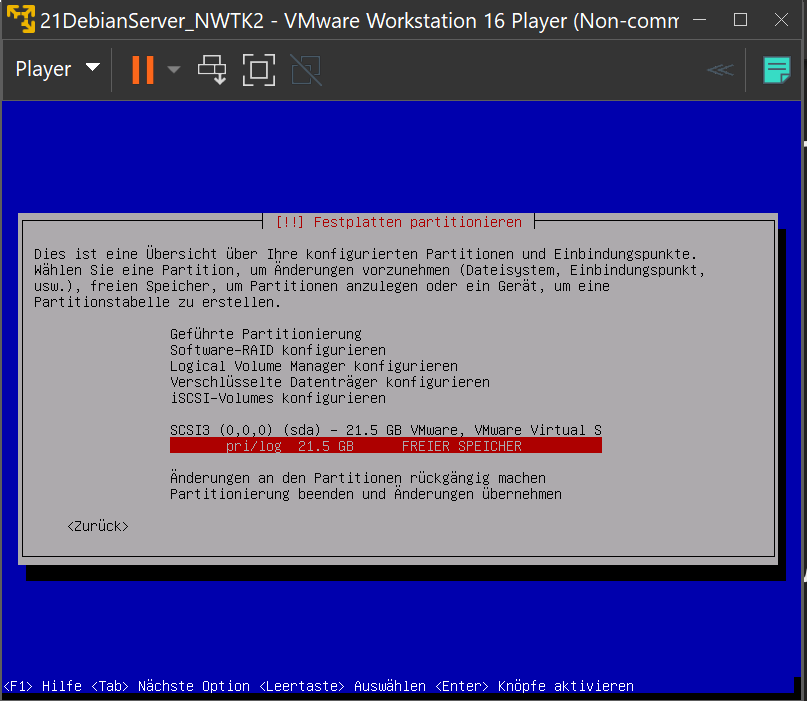


Abbildung : Partitionstabelle

Wählen Sie diese (rot hinterlegt) aus und erstellen Sie darauf eine neue Partition.

Die Größe dieser Partition kann hierbei ruhig die gesamte Größe der Virtuellen Maschine betragen.

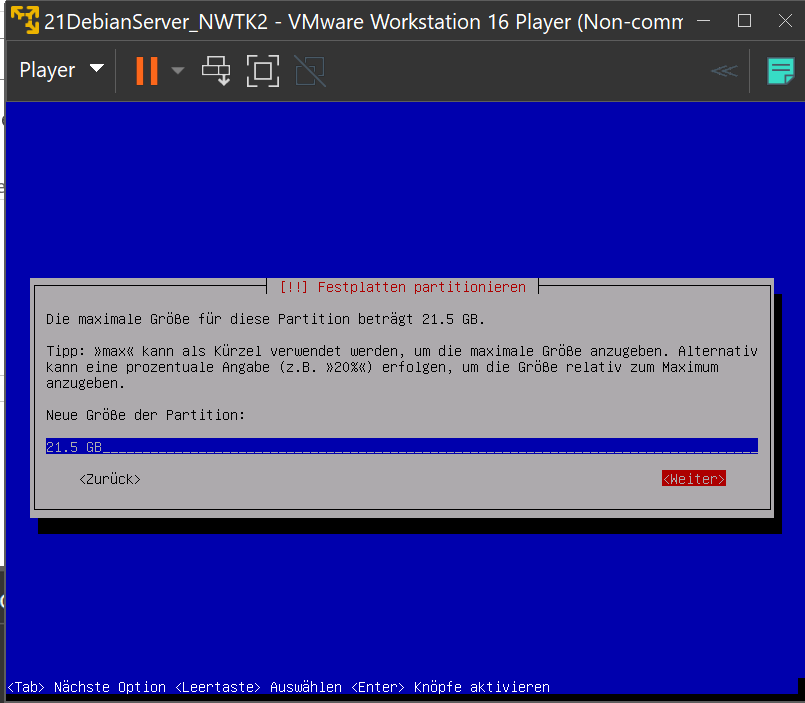


Abbildung : Größe der Partition

Erstellen Sie diese Partition mit dem Typen „primär“.

zusätzliche Information: Dies bedeutet, dass die Partitionierung nicht nur logisch getrennt wird, sondern mit Dateien. Außerdem stellt dieser Typ sicher, dass das Betriebssystem von der Partition booten kann. Aus diesem Grund sollte die erste Partition immer primär sein.

Die Partition sollte das Ext4-Journaling-Dateisystem nutzen, root (/) als Einbindungspunkt haben, 5% oder mehr reservierte Blöcke beinhalten und Boot-Flag aktiviert haben.

zusätzliche Information: Es ist wichtig, dass mindestens 5% der Partition für ext-Dateisysteme reserviert sind, weil im Falle des Volllaufens der Festplatte die Anmeldung mit root ansonsten nicht mehr möglich wäre. Für mehr Informationen: <https://wiki.ubuntuusers.de/ext/>

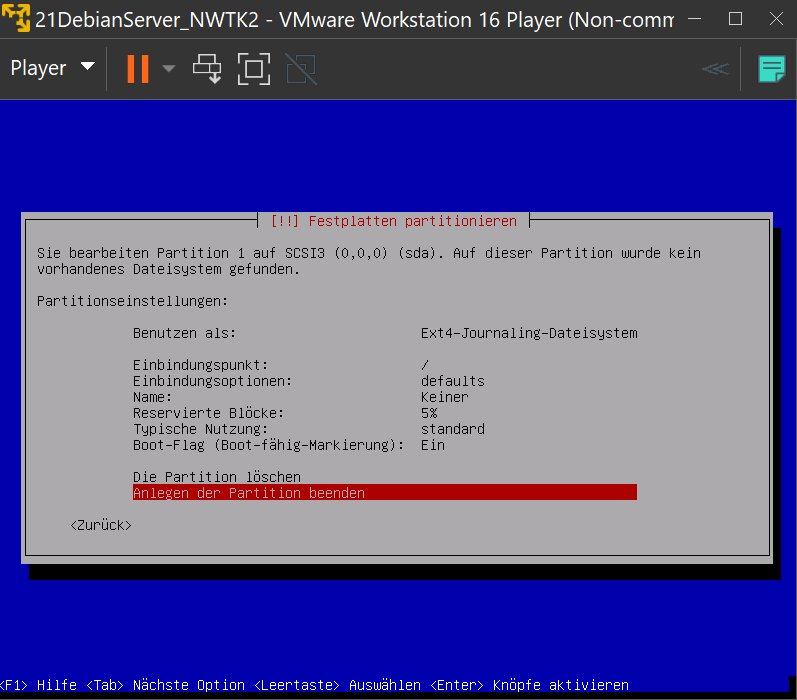


Abbildung : Partitionseinstellungen

Anschließend beenden Sie das Anlegen der Partition und speichern die Änderungen der Partitionierung. Kehren Sie zum Partitionierungsmenü zurück und schreiben Sie die Änderungen auf die Festplatte.

### Basissystem installieren

Der nächste Schritt ist das Basissystem. Wählen Sie diesen Kernel aus:

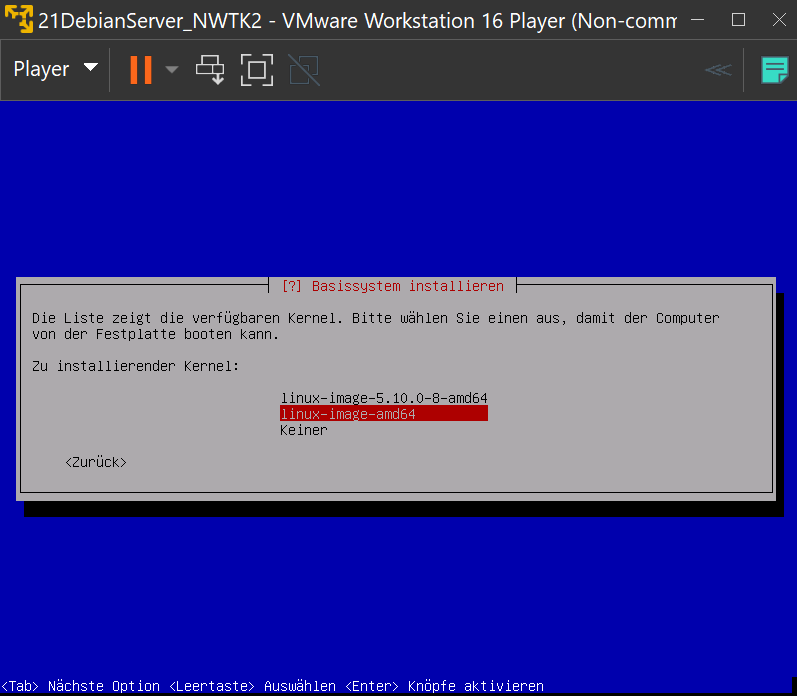


Abbildung : Kernel des Basissystems

Installieren Sie die Treiber **generisch**.

zusätzliche Information: Treiber generisch zu installieren, bedeutet, dass alle verfügbaren Treiber eingebunden werden. Treiber angepasst zu installieren, bedeutet, dass nur die Treiber installiert werden, die für das System gebraucht werden. Dadurch, dass Sie später noch weiter Zusatzpakete installieren wollen, ist es einfacher, wenn Sie bereits im Vorhinein alle verfügbaren Treiber installieren und danach nicht suchen müssen.

### Paketmanager konfigurieren

Nun konfigurieren Sie den Paketmanager. Der Paketmanager von Debian heißt **apt**. Sie lesen kein weiteres Installationsmedium ein und verwenden den Netzwerkspiegel.

zusätzliche Information: Der Netzwerkspiegel bzw. Spiegelserver ist der Server, von dem sich apt seine Pakete installiert. Es wird daher empfohlen einen Spiegelserver in der Nähe, also im gleichen Land zu verwenden, damit das Downloaden schneller funktioniert.

Als Datei-Download-Protokoll verwenden Sie am besten http, weil es keine Probleme mit Firewalls verursacht. Anschließend wählen Sie einen netztopologisch gesehen, sinnvollen Spiegelserver aus. Verwenden Sie keinen Proxy, es sei denn, Sie benötigen einen, um ins Internet zu kommen. Damit Sie später alle Softwarepakete sehen können, wählen Sie die Option „<Ja>“ aus, wenn Sie nach „Non-free-Software“ gefragt werden. Paketdepots sollten Sie aktivieren. Verwenden Sie folgende Dienste (mit \* markiert):

ACHTEN Sie darauf, dass mit Enter zum nächsten Fenster springen und mit Leertaste die einzelnen Dienste aktivieren bzw. deaktivieren können!



Abbildung : Dienste auswählen

### Software auswählen und installieren

Dieser Schritt ist optional.

Automatische Updates können Sie deaktivieren und an der Paketverwendungserfassung wollen Sie auch nicht teilnehmen. Zusätzliche Software müssen Sie auch keine installieren. Natürlich können Sie bei allen 3 Auswahlmöglichkeiten auch auf ja klicken oder Zusatzsoftware installieren. Sie benötigen sie allerdings nicht.

### den GRUB-Bootloader installieren

Im Gegensatz zum vorherigen Schritt ist dieser Schritt wieder unbedingt notwendig.

Installieren Sie den GRUB-Bootloader auf dem primären Laufwerk /dev/sda und deaktivieren Sie die Erzwingung von EFI.

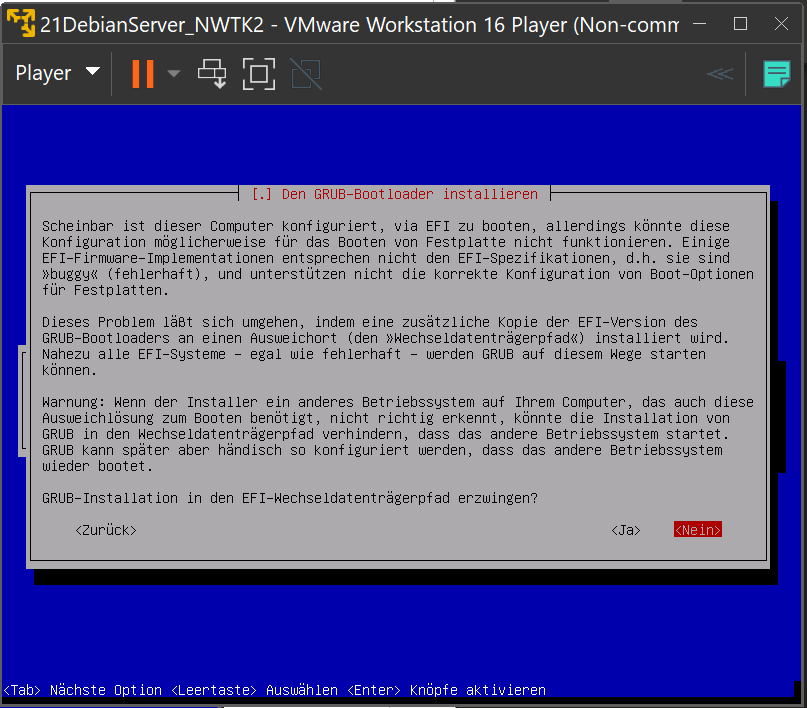


Abbildung : EFI Erzwingung deaktivieren

### Installation abschließen

Schlussendlich müssen Sie nur noch die Installation abschließen. Stellen Sie ein, dass die Systemzeit nicht auf UTC eingestellt werden soll. Bestätigen Sie den Neustart und warten Sie, bis die Virtuelle Maschine neu gestartet hat.

Überprüfen Sie, ob Sie sich mit root anmelden können und fahren Sie anschließend die Virtuelle Maschine herunter.

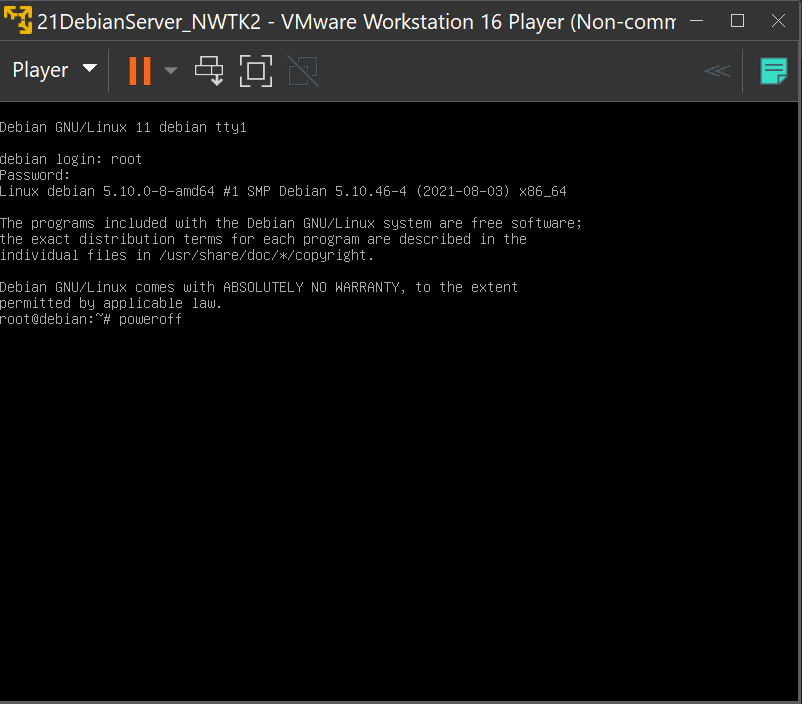
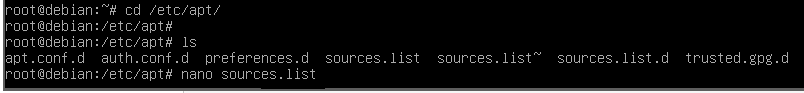


Abbildung : Root-Anmeldung möglich

## Aptitude + Putty

Öffnen Sie die Datei /etc/apt/sources.list.



Code : # nano sources.list

Überprüfen Sie, ob die beiden Zeilen, in denen „cdrom“ vorkommt, auskommentiert sind. Das sollten Zeile 1 und 3 sein. Die Zeilen sind dann auskommentiert, wenn eine Raute (#) am Beginn steht.



Abbildung : sources.list

### Aptitude installieren

Aktualisieren Sie die Datenbank mit „apt-get update“.



Code : # apt-get update

Installieren Sie Aptitude.

zusätzliche Information: Aptitude ist ein Programm, mit dem Sie ganz einfach Zusatzpakete installieren können. Der große Vorteil im Gegensatz zu Apt ist, dass Aptitude Ihnen vor der Installation eine Liste aller Pakete auflistet, die neben dem vom Ihnen ausgewählten Paket installiert werden müssen.



Code 3: # apt-get install aptitude

Führen Sie Aptitude aus.



Code : # aptitude

Nun sollte sich ein Fenster öffnen, das ungefähr so aussieht:

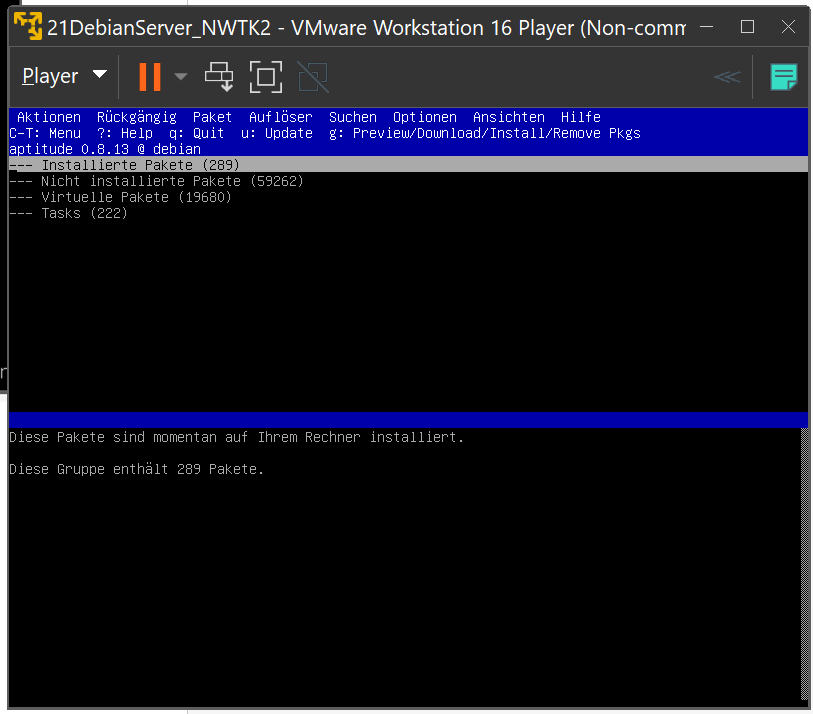


Abbildung : Aptitude

Hier haben Sie eine Liste mit den wichtigsten Aktionen:

* STRG+T: Menu
* q: beendet die Software Aptitude
* u: aktualisiert die Datenbank
* U: zeigt Ihnen alle Pakete an, die aktualisiert werden können
* /: öffnet ein Fenster, wo Sie nach Paketnamen suchen können
* n: springt zum nächsten Paket
* +: markiert ein Paket zum Installieren mit i   
  (zusammenhängende Pakete werden mit iA markiert)
* g: installiert alle markierten Pakete

Unter den Aktionen können Sie sich Ihre installierten Pakete auflisten lassen. Außerdem kann man über das Menu Minesweeper spielen.

### Openssh und man-db installieren

Öffnen Sie Aptitude, suchen Sie nach „openssh“, springen Sie die Pakete durch, bis Sie das „openssh“-Paket gefunden haben und markieren Sie dieses mit +. Installieren Sie diese Pakete.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : nach openssh suchen

Das gleiche Prinzip der Installation führen Sie nun bei man-db ebenfalls durch.

### Putty einrichten

Wenn Sie mit VMWare öfters arbeiten, haben Sie vielleicht schon bemerkt, dass es schwierig ist, zwischen dem Fenster der Virtuellen Maschine und Windows bzw. dem laufenden Betriebssystem schnell zu wechseln. Aus diesem Grund ist **Putty** sehr hilfreich. So können Sie viel einfacher zwischen den Fenstern wechseln.

Laden Sie Putty über einen dieser Links herunter:

* 64-Bit-Version: <https://the.earth.li/~sgtatham/putty/latest/w64/putty.exe>
* 32-Bit-Version: <https://the.earth.li/~sgtatham/putty/latest/w32/putty.exe>

Falls die Links nicht mehr funktionieren sollten, suchen Sie im Internet nach putty.org 🡪 Download 🡪 und suchen Sie sich die für Sie passende Version heraus.

Öffnen Sie die putty.exe Datei über den Explorer. Schreiben Sie in das Feld „Host Name (or IP address)“ die IP-Adresse der Virtuellen Maschine ein. Diese finden Sie mit dem [„ip -c a“-Befehl](#_ip_-c_a) heraus.

Wählen Sie als Verbindungstyp SSH und speichern Sie diese Einstellungen am besten unter einem sinnvollen Namen.

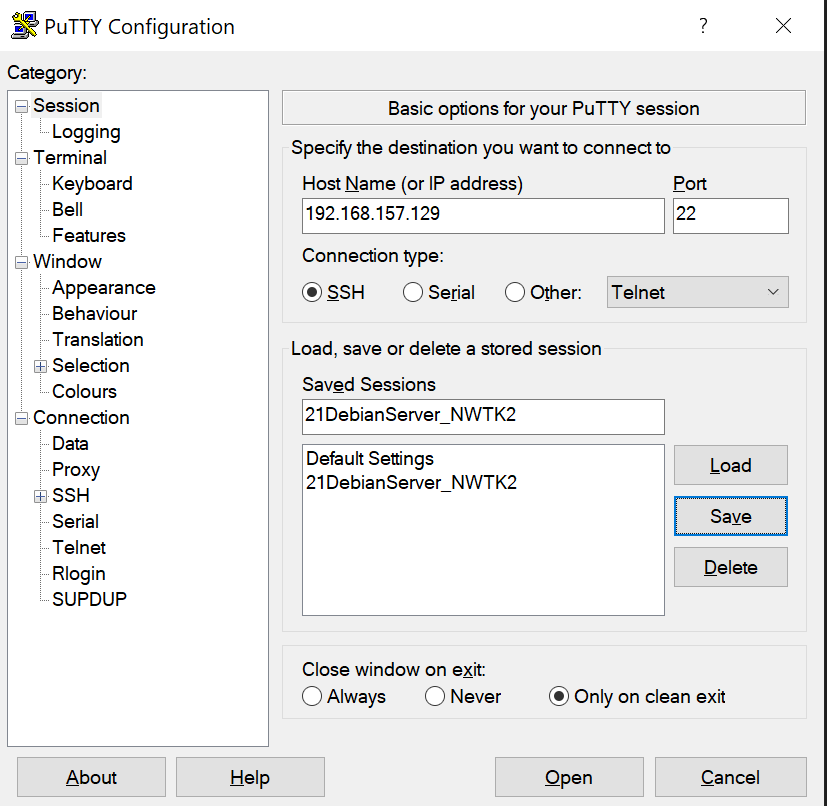


Abbildung : Putty Configuration

Nachdem Sie auf „Open“ geklickt haben, öffnet sich ein Fenster. Versuchen Sie einmal, sich mit dem root-Account anzumelden. Sie werden merken, dass dies nicht möglich ist, weil in der sshd\_config-Datei nicht eingeschalten ist, dass man sich mit dem root-Benutzer anmelden kann. Aus diesem Grund war es auch wichtig, dass Sie mindestens einen normalen Benutzeraccount erstellen.

Melden Sie sich nun mit dem Benutzerkonto an. Führen Sie den Befehl



Code : # su - root

aus und geben Sie Ihr Passwort ein, um root-Berechtigungen zu erhalten.

zusätzliche Information: Den Bindestrich benötigen Sie, damit Sie auch root-Befehle ausführen können.

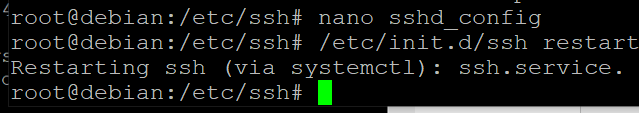
Öffnen Sie die Datei /etc/ssh/sshd\_config.



Code : # nano sshd\_config

Entfernen Sie die Raute **#** in der Zeile „PermitRootLogin yes“ bzw. ändern Sie das „no“ auf ein „yes“.

Starten Sie den SSH-Service neu, indem Sie diesen Befehl eingeben:



Code : # /etc/init.d/ssh restart

Anschließend können Sie sich mit dem root-Account anmelden.

### SSH Verbindung herstellen

Um eine SSH Verbindung aufbauen zu können, benötigen Sie einen Benutzernamen, dessen Passwort und die IP-Adresse der Virtuellen Maschine.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

## wichtige Befehle zum Herausfinden von Informationen

### ip -c a



Code : # ip -c a

Mit diesem Befehl können Sie IP-Adressen herausfinden. Egal, ob decimal oder hexadecimal, die Antwort finden Sie mit diesem Befehl. Wegen dem „-c“ sind alle IP-Adressen in pink bzw. orange. Das „a“ ist die Kurzschreibweise für address.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : ip -c a Ausgabe

### route -n



Code : # route -n

Mit diesem Befehl können Sie herausfinden, welche IP-Adressen über welche Router auf welchen Interfaces hinaus gehen. Hierbei können Router auf andere Rechner, also IP-Adressen bzw. Ziele, verweisen.

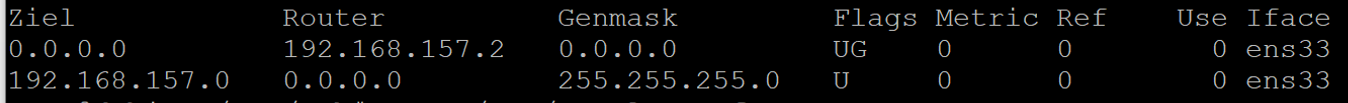


Abbildung : route -n Ausgabe

### more [path]



Code 10: # more /etc/resolv.conf

Mit diesem Befehl kann man den DNS-Server des Rechners und die Domain herausfinden.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : more /etc/resolv.conf Ausgabe



Code 11: # more /etc/network/interfaces

Mit diesem Befehl kann man herausfinden, welche Netzwerkkarte welche IP-Adresse, Subnetzmaske und Gateway hat.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : more/etc/network/interfaces Ausgabe

### tail -f [path]



Code : # tail -f /var/log/syslog

Mit diesem Befehl kann man sich immer die aktuellen log-Einträge ansehen. Das bedeutet, dass auf dem Fenster, wo man den Befehl aktiv ausführt, immer die neuesten Zeilen der syslog-Datei stehen. Sie können das Auslesen der syslog-Datei mit STRG+C beenden und zur Console zurückkehren.

zusätzliche Information: In dieser Datei stehen alle Meldungen bzw. Warnungen mit Ausnahme von Meldungen der auth oder authpriv Facilities. Diese Datei eignet sich daher gut zur Analyse von vielen Problemen.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : Beispiel für Ausgabe von # tail -f /var/log/syslog

### tracert -d [ip-address]

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

tracert -d 192.168.157.2 zeigt die Routenverfolgung bis zum Ziel.

## Virtuelle Windows Maschine

### Virtuelle Windows Maschine aufsetzen

Laden Sie sich eine Windows 10 - ISO-Datei, oder wenn Sie wollen Windows 11 - ISO-Datei, vom Internet oder von hier: <https://www.microsoft.com/de-de/software-download/windows11> herunter.

Erstellen Sie eine neue Virtuelle Maschine in VMWare mit sinnvollem Namen, genügend RAM und Festplattenspeicher und fügen Sie die heruntergeladene ISO-Datei ein. Führen Sie den Installationsprozess durch.

### Virtuelle Debian Maschine fürs Pingen einrichten

Als zweites schließen Sie die Virtuelle Debian Maschine, falls diese noch läuft. Gehen Sie in die Einstellungen der Virtuellen Debian Maschine und fügen Sie eine zweite Netzwerkkarte hinzu.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : LAN Segment

Diese soll auf „LAN segment“ gestellt werden. Geben Sie dem Segment einen Namen, speichern Sie und fahren Sie die Virtuelle Debian Maschine wieder hoch.

Als nächstes ändern Sie auf der Virtuellen Debian Maschine die „/etc/network/interfaces“-Datei. Öffnen Sie die Datei mit „nano“ mit Root-Berechtigungen, um den Inhalt der Datei ändern zu können.



Code : # nano /etc/network/interfaces

Sie werden feststellen, dass diese Datei bereits einige geschrieben Zeilen beinhaltet. Das sind Voreinstellungen.

Sie müssen jetzt die Netzwerkeinstellungen von der neuen Netzwerkkarte hinzufügen. Um herauszufinden, wie die Netzwerkkarte heißt benötigen Sie den Befehl [ip -c a](#_ip_-c_a). In hellblau bzw. türkis sehen Sie die Netzwerkkarten. Die Netzkarte, die Sie noch konfigurieren müssen, hat noch keine IP-Adresse. Konfigurieren Sie sie statisch mit IP-Adresse und Subnetzmaske.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : /etc/network/interfaces

Außerdem schreiben Sie den Namen dieser Netzwerkkarte bei der Zeile „auto lo“ hinten dazu, damit die Änderungen bei Ausführung des Befehls „service networking restart“ auch übernommen werden.

zusätzliche Informationen: „iface“ schreiben Sie, weil Sie ein Interface konfigurieren. „ens37“ ist bei mir der Name der Netzwerkkarte. Als Protokoll verwenden Sie am besten „inet“ und weil Sie die IP-Adresse statisch, also per Hand, eintragen wollen, schreiben Sie „static“.

Als nächstes starten Sie das Netzwerk neu. Dies können Sie mit mehreren verschiedenen Befehlen erzielen. Hier zwei Beispiele:

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Code 14: # /etc/init.d/networking restart



Code : # service networking restart

### Windows Einstellungen konfigurieren

#### IPv4 Konfiguration

Auf der Virtuellen Windows Maschine müssen Sie die IPv4-Adresse, die Subnetzmaske und das Gateway, also den Router, richtig konfigurieren, damit eine Verbindung überhaupt stattfinden kann.

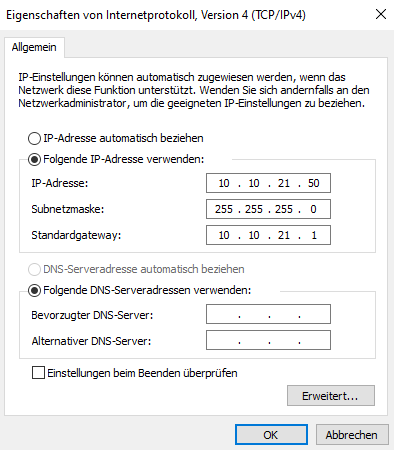
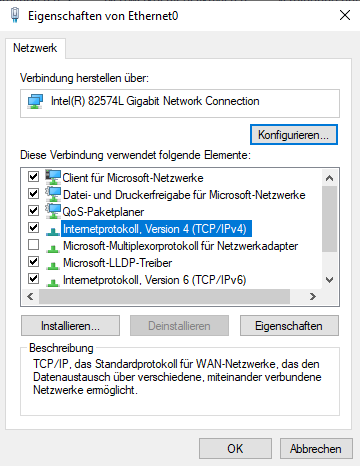
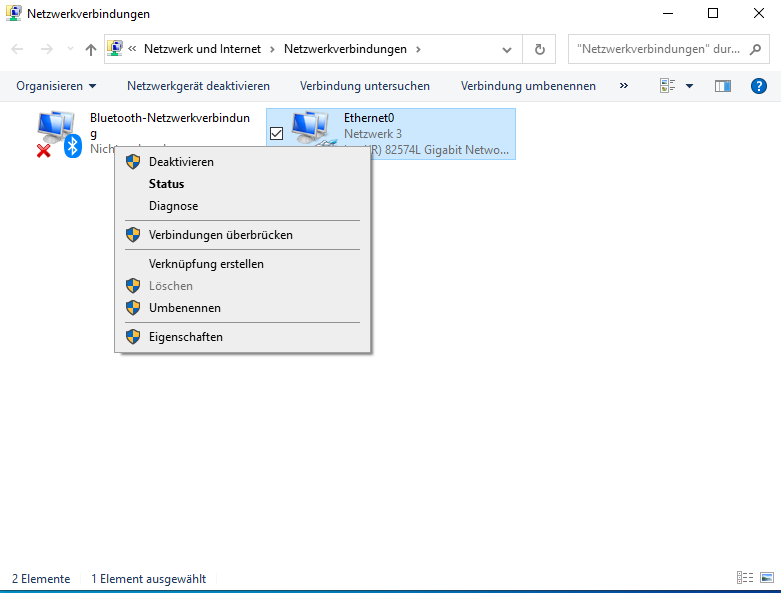
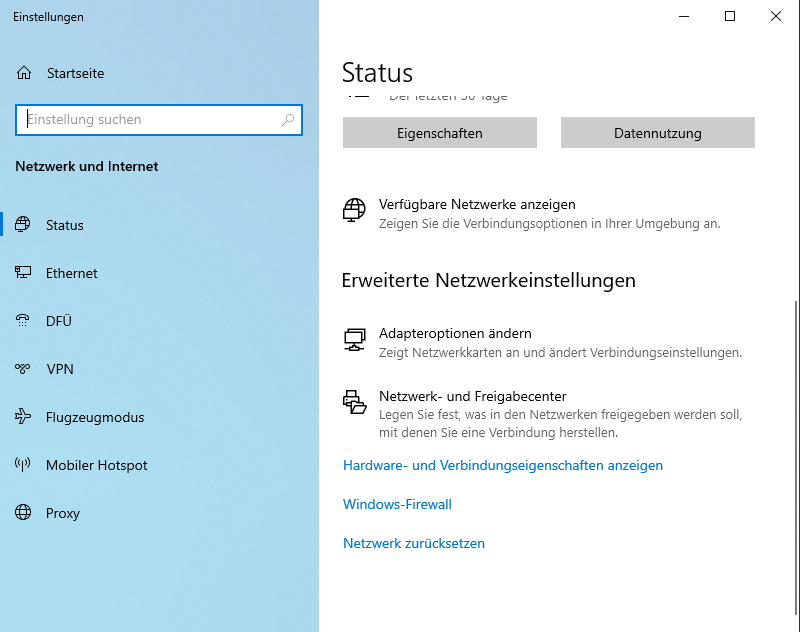
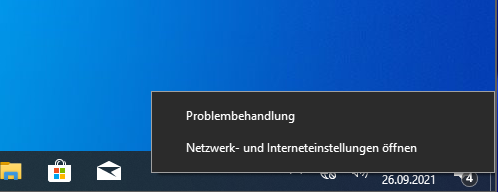


Abbildung : IPv4-Adressen Einstellungen Windows

Zu beachten ist hierbei, dass die dritte Dekade der IPv4-Adresse und des Standardgateways mit der IPv4-Adresse der Virtuellen Debian Maschine übereinstimmen (Interface ens37).

Mit dem Befehl „ipconfig“ können Sie Ihre Einstellungen auf Ihre Korrektheit prüfen.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : ipconfig

Code : # ipconfig

Damit wir von Debian Windows auch pingen können, müssen wir die Windows Firewall deaktivieren. Dies folgt in den nächsten Schritten:

#### Firewall deaktivieren

Im nächsten Schritt müssen Sie die Firewall der Virtuellen Windows Maschine deaktivieren, weil ansonsten diese die Pakete möglicherweise nicht von der Virtuellen Debian Maschine zu der Virtuellen Windows Maschine durchlässt.

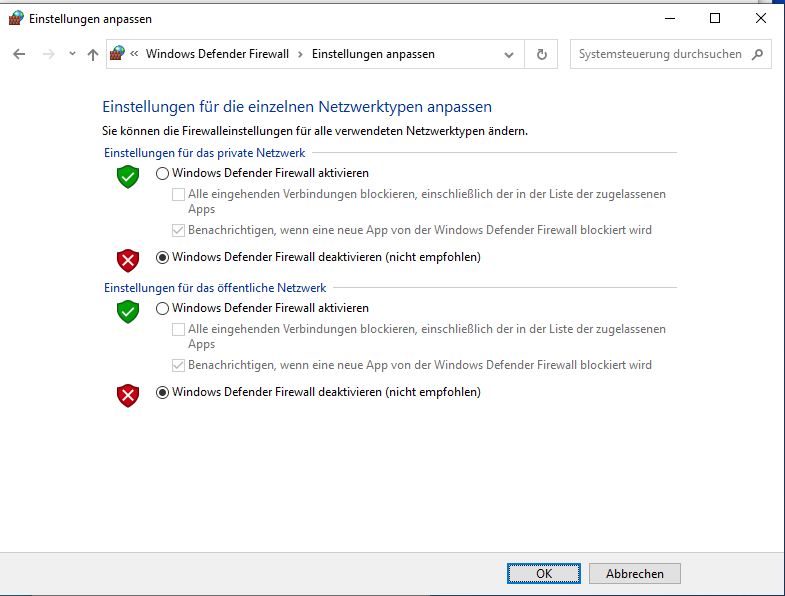
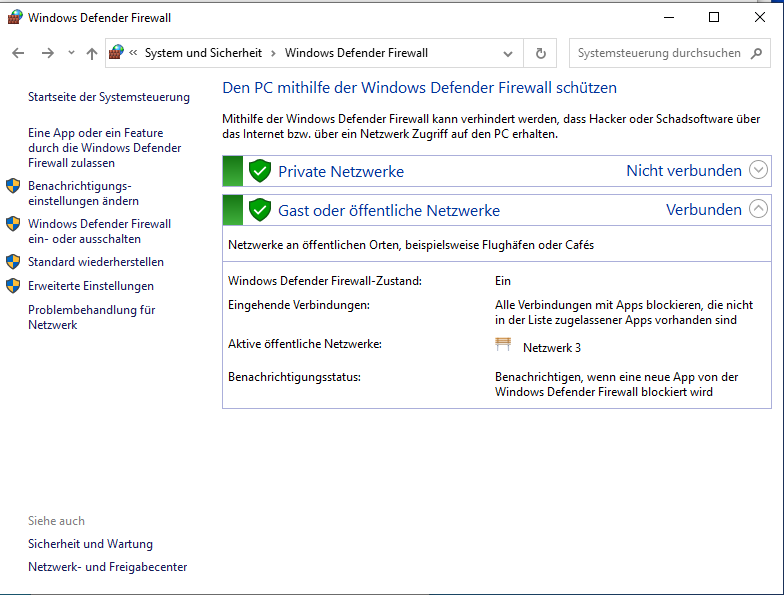
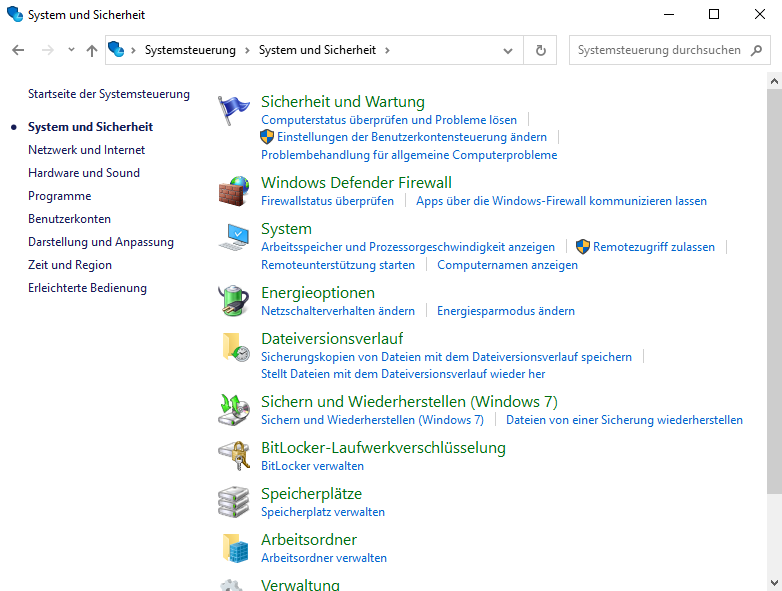
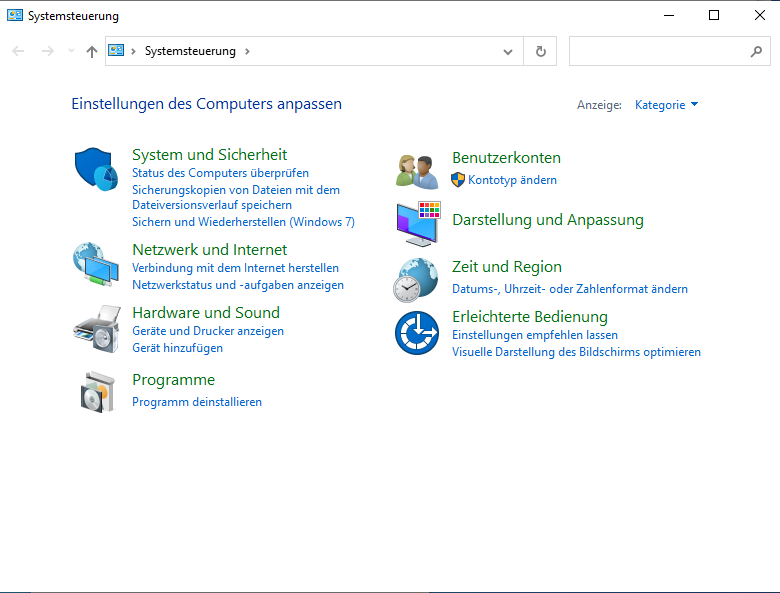
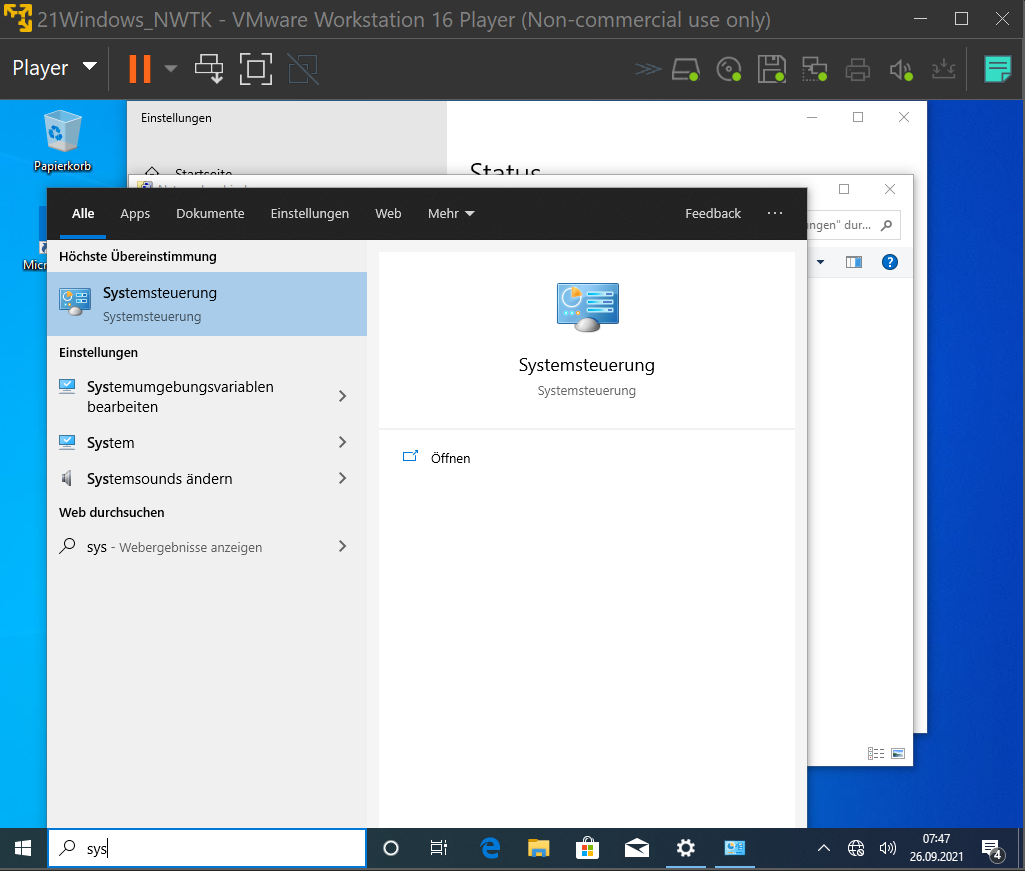


Abbildung : Firewall deaktivieren

Wenn wir die Netzwerkkonfigurationen auf der Virtuellen Debian Maschine neu starten, sollte das Pingen in beide Richtungen funktionieren.

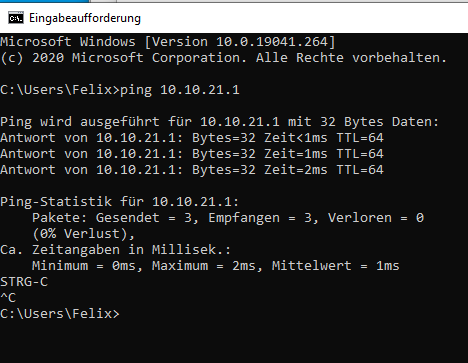
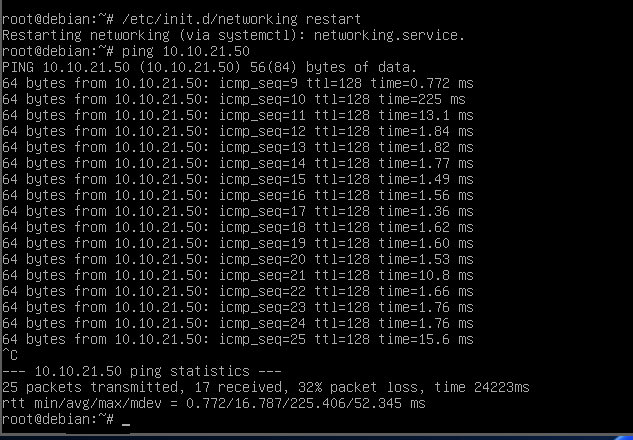


Abbildung (links): Debian – ping Windows

Abbildung (rechts): Windows – ping Debian

## Virtuelle Debian Maschine Kopie

### Virtuelle Debian Maschine klonen

Klonen Sie die Virtuelle Debian Maschine. Dies können Sie erreichen, indem Sie folgende Schritte befolgen:

Tätigen Sie einen Rechtsklick auf die Virtuelle Maschine in VMWare Workstation Player und klicken Sie auf „Settings…“ beziehungsweise „Einstellungen…“. Klicken Sie auf die Abteilung „Hard Disk (SCSI)“ und kopieren Sie den Pfad, wo die Virtuelle Debian Maschine gespeichert ist (im Bild rot markiert).

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : Pfad der Virtuellen Debian Maschine finden

Öffnen Sie Ihren Explorer und fügen Sie den kopierten Pfad in die Adressleiste ein. Wichtig ist, dass Sie anschließend den Namen am Ende der Adressleiste und die Dateiendung löschen, ansonsten starten Sie die Virtuelle Debian Maschine. Drücken Sie dann Enter und Sie werden zu dem Ordner geführt, indem sich die Virtuelle Debian Maschine befindet.

In diesem Ordner befindet sich eine Datei, die den Namen der Virtuellen Debian Maschine und die Dateiendung „.vmdk“ enthält. Diese Datei ist im nachstehenden Bild grau hinterlegt.

Ein Bild, das Text, Computer, Monitor, Screenshot enthält.

Automatisch generierte Beschreibung

Abbildung : Virtuelle Debian Maschine - Datei

Kopieren Sie diese Datei in einen anderen Ordner und benennen Sie die Datei um, sodass der Name der neuen Virtuellen Debian Maschine drinnen steht, zum Beispiel: „21DebianClient\_NWTK2.vmdk“. Führen Sie die Datei aus.

Wenn Sie gefragt werden, ob Sie die Virtuelle Debian Maschine Kopie verschoben oder kopiert haben, klicken Sie auf kopiert, damit die neue Virtuelle Debian Client Maschine eine neue eigene MAC-Adresse bekommt.

Schließen Sie die Virtuelle Debian Client Maschine wieder und öffnen Sie die Einstellungen. Entfernen Sie das virtuelle LAN-Segment, das Sie bei der ersten Virtuellen Debian Maschine hinzugefügt haben.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : LAN-Segment entfernen

### Webserver einrichten

Richten Sie einen Webserver auf der Virtuellen Debian Client Maschine ein, den Sie auf den anderen Virtuellen Maschinen erreichen, indem Sie folgende Schritte befolgen.

#### Apache2 installieren

Laden Sie über Aptitude das Apache2-Paket, das PHP-Paket und alle zugehörigen Pakete auf der Virtuellen Debian Client Maschine herunter.

#### Skript PHP schreiben

Damit Sie von der Virtuellen Windows Maschine über einen Webserver die Virtuelle Debian Client Maschine erreichen können und eine IP-Adresse angezeigt bekommen, müssen Sie sich ein PHP-Skript schreiben.

Erstellen Sie die Datei „/var/www/html/ip.php“ und fügen Sie den untenstehenden PHP-Code in diese Datei ein.



Code : # nano /var/www/html/ip.php

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : ip.php

### Virtuelle Debian Client Maschine mit Virtuelle Windows Maschine verbinden

Es gibt zwei Möglichkeiten, wie Sie die Virtuelle Debian Client Maschine mit der Virtuelle Windows Maschine verbinden können:

* [NAT MASQUERADE](#_NAT_MASQUERADE)
* [Route IP-Weiterleitung](#_Route_IP-Weiterleitung)

NAT MASQUERADE verändert die IP-Adresse des Paketes und schickt es anschließen zu dieser Adresse. Die Route IP-Weiterleitung leitet das Pakete an die IP-Adresse weiter, die in der Tabelle eingetragen ist.

#### NAT MASQUERADE

Das ist der grundsätzliche Aufbau des neuen Netzwerks, wenn Sie NAT verwenden. In den folgenden Schritten werden Sie die Einstellungen dementsprechend konfigurieren.

zusätzliche Information: MASQUERADE ändert die ursprüngliche Quelladresse des Pakets in eine routbare IP-Adresse um.



Abbildung : Netzwerkaufbau NAT

##### „iptables“ installieren

Als erstes installieren Sie das „iptables“-Paket mittels Aptitude.

##### Nat richtig einstellen

Damit NAT richtig funktioniert, muss MASQUERADE auf alle Pakete vom Interface ens33 in der POSTROUTING-Chain auf MASQUERADE umgestellt werden. Iptables weiß dann automatisch, was es zu tun hat. Damit Sie das erreichen benötigen Sie folgenden Befehl:



Code : # iptables -t nat -A POSTROUTING -o ens33 -j MASQUERADE

Zur Kontrolle, ob Masquerade nun aktiviert ist, tippen Sie den Befehl „iptables -t nat -L“ ein. Dieser zeigt Ihnen die aktuellen IP-Tabelle-Einstellungen. In der letzten Zeile des Bildes sehen Sie, dass Masquerade für alle Pakete aktiviert ist.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : IP-Tabellen-Einstellungen

Code : # iptables -t nat -L

Wenn Sie glauben, die IP-Tabellen-Einstellungen kaputt gemacht zu haben, verwenden Sie den Befehl „iptables -t nat -F“, um die IP-Tabellen-Einstellungen für NAT zurückzusetzen.

##### Webserver erreichen

Öffnen Sie auf der Virtuellen Windows Maschine einen Browser Ihrer Wahl und tippen Sie die IP-Adresse der Virtuellen Debian Client Maschine, aus der kopierten Virtuellen Debian Maschine, in die URL-Leiste. Fügen Sie dann noch ein „/ip.php“ an, damit auch die Datei, die Sie [vorhin](#_Skript_PHP_schreiben) erstellt haben, aufrufen.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : Webserver erreichen NAT

#### Route IP-Weiterleitung

Das ist der grundsätzliche Aufbau des neuen Netzwerks, wenn Sie die Routing Variante verwenden. In den folgenden Schritten werden Sie die Einstellungen dementsprechend konfigurieren.

zusätzliche Information: ROUTING sucht in einer internen Tabelle nach der Zieladresse des Paketes. Wenn diese gefunden wurde, schickt Routing das Paket an die andere IPv4-Adresse, die in der Tabelle neben der Zieladresse steht.

##### IPv4-Adressen aktivieren

Damit die Variante mittels Router funktioniert, müssen Sie als allererstes, IPv4-Adressen am Router aktivieren. Öffnen Sie hierzu die Datei „/etc/sysctl.conf“ und einkommentieren Sie die Zeile „net.IPv4.ip\_forward=1“, indem Sie die Raute am Beginn der Zeile löschen.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : sysctl.conf - net.IPv4.ip\_forward=1

Speichern Sie die Datei mit STRG+O und verlassen Sie die Datei mit STRG+X. Mit dem Befehl „sysctl -p“ können Sie sich alle Zeilen, die nicht kommentiert sind, der Datei „sysctl.conf“ ausgeben lassen.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Code : # sysctl -p

##### Routing-Tabelle einstellen

Mit dem Befehl [„route -n“](#_route_-n) können Sie sich diese Routing-Tabelle anzeigen lassen.

Wenn Sie einen neuen Eintrag in die Tabelle machen wollen, verwenden Sie den Befehl „route add -net [Ziel-IP-Adresse des Pakets]/[Subnetzmaske] gw [neue Ziel-IP-Adresse des Routers]“



Code 21: # route add -net 10.10.21.0/24 gw 192.168.157.128

Damit sich die Virtuelle Debian Klon Maschine mit der Virtuellen Windows Maschine verbindet, stellen Sie die Router-Tabelle-Einstellungen der Virtuellen Debian Maschine so ein:

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : Route-Einstellungen von Virtueller Debian Maschine

Die Virtuelle Debian Klon Maschine – Router-Tabellen-Einstellungen müssen Sie so einstellen:

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : Route-Einstellungen von Virtuelle Debian Klon Maschine

##### Webserver erreichen

Öffnen Sie auf der Virtuellen Windows Maschine einen Browser Ihrer Wahl und tippen Sie die IP-Adresse der Virtuellen Debian Client Maschine, als der kopierten Virtuellen Debian Maschine, in die URL-Leiste. Fügen Sie dann noch ein „/ip.php“ an, damit auch die Datei, die Sie [vorhin](#_Skript_PHP_schreiben) erstellt haben, aufrufen.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

## Windows Internet

Damit Sie in der Virtuellen Windows Maschine Internetzugang haben tragen Sie in den IPv4-Einstellungen einen DNS-Server ein. Wichtig ist hierbei nur der bevorzugte DNS-Server, es funktioniert auch ohne den alternativen DNS-Server-Eintrag.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : Virtuelle Windows Maschine DNS-Server

WICHTIG: Dies funktioniert nur bei der [NAT Methode](#_NAT_MASQUERADE). Bei der [ROUTING Methode](#_Route_IP-Weiterleitung) funktioniert die Weiterleitung logischerweise nicht!

## DHCP Server

### DHCP Server konfigurieren

#### isc-dhcp-server Paket installieren

Installieren Sie mithilfe von Aptitude das „isc-dhcp-server“-Paket und alle dazugehörigen Pakete auf der Virtuellen Debian Maschine.

#### Interface einstellen

Schreiben Sie in die „/etc/default/isc-dhcp-server“-Datei bei INTERFACESv4=““ zwischen die Anführungszeichen ihre Netzwerkkarte, die zur Virtuellen Windows Maschine führt.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : Netzwerkkarte DHCP einstellen

#### dhcpd.conf Datei

In der „/etc/dhcp/dhcpd.conf“ stellen Sie folgende Einstellungen um:

1. die Domain-Name **Servers** sind 8.8.8.8 und 1.1.1.1
2. die Domain-Name ist grundsätzlich egal
3. Entkommentieren Sie **authoritative**, weil der DHCP Server der einzige DHCP Server in dem Netzwerk ist
4. Stellen Sie das Subnetz so ein:

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : Subnetz DHCP einstellen

#### DHCP Server neu starten

Starten Sie den DHCP Service neu, indem Sie diesen Befehl schreiben:



Code : # systemctl restart isc-dhcp-server.service

### Virtuelle Windows Maschine auf DHCP umstellen

#### umstellen

Navigieren Sie auf der Virtuellen Windows Maschine zu den Netzwerkeinstellungen des IPv4-Protokolls und schalten Sie „IP-Adresse automatisch beziehen“ ein. In anderen Worten ist dies die DHCP-Einstellung.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : IP-Adresse automatisch beziehen

#### überprüfen

Um festzustellen, ob die Einstellungen richtig konfiguriert wurden und DHCP funktioniert, lassen Sie sich die IP-Adresse der Virtuellen Windows Maschine anzeigen:



Code : # ipconfig /all

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : Ausgabe der Interneteinstellungen Windows

### syslog

Sie können auch auf der Virtuellen Debian Maschine in der /var/log/syslog-Datei nachsehen, ob DHCP Pakete ein- und ausgegangen sind.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : Syslog-Datei Ausgabe

### Virtuelle Windows Maschine mittels MAC-Adresse IP-Adresse zuordnen

#### dhcpd.conf konfigurieren

Die Datei dhcpd.conf müssen Sie folgendermaßen konfigurieren:

Wie Sie sehen können weisen Sie dem Windows Client dann immer eine fixe IP-Adresse mithilfe der MAC-Adresse zu. Die MAC-Adresse der Virtuellen Windows Maschine finden Sie mit dem Befehl „ipconfig /all“ heraus.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : dhcpd.conf mit fixer Adresse

#### Virtuelle Windows Maschine IPv4-Konfiguration erneuern

Mit dem Befehl „ipconfig /renew“ holt sich die Virtuelle Windows Maschine die neue IPv4-Adresse.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : IP-Konfiguration Virtuelle Windows Maschine

## Firewall

### iptables Befehl und Co.

#### Konfiguration in Datei speichern

„iptables-save -f <Dateiname>“ speichert die aktuelle iptables-Konfiguration in die neue Datei.

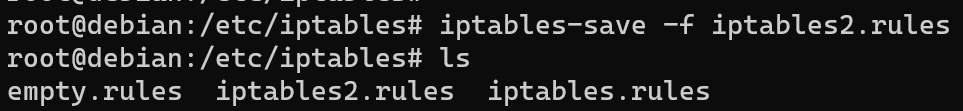


Abbildung : iptables-Konfiguration speichern

#### Konfiguration aus Datei laden

„iptables-restore <Dateiname>“ ladet die Konfigurationen aus der Datei in die aktuelle Konfiguration.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : iptables-Konfiguration laden

### Firewall konfigurieren (iptables)

#### Iptables konfigurieren

Führen Sie folgende Befehle durch:

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : Firewall iptables Befehle

#### Iptables-Konfiguration speichern

Speichern Sie die aktuelle Konfiguration ([Konfiguration in Datei speichern](#_Konfiguration_in_Datei)).

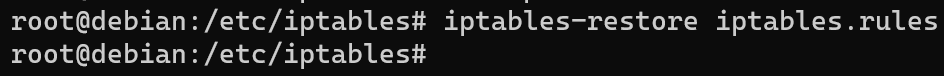
Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : Datei mit Konfiguration (iptables)

#### laden der Konfiguration

Sie können nun die Konfiguration immer nach dem Hochfahren der Virtuellen Debian Server Maschine laden ([Konfiguration aus Datei laden](#_Konfiguration_aus_Datei)).



Code : # iptables-restore iptables.rules

#### Autoladen der Konfiguration

Damit Sie nicht jedes Mal nach dem Hochfahren die Konfiguration per Hand laden müssen, können Sie auch einstellen, dass diese automatisch geladen wird, und die Firewall somit automatisch konfiguriert ist. Dies wird mithilfe eines „systemd“-Service umgesetzt.

Erstellen Sie eine neue Datei: „/etc/systemd/system/iptables.service“. Schreiben Sie den Inhalt des folgenden Screenshots ab.

zusätzliche Informationen: Bei [Unit] werden allgemeine Beschreibungen hinzugefügt und festgelegt, in welche Reihenfolge der Service ausgeführt werden soll. Bei [Service] wird eingestellt, welcher Service dahinter ausgeführt wird. [Install] managed, von welchem Target der Service ausgeführt werden soll.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : /etc/systemd/system/iptables.service

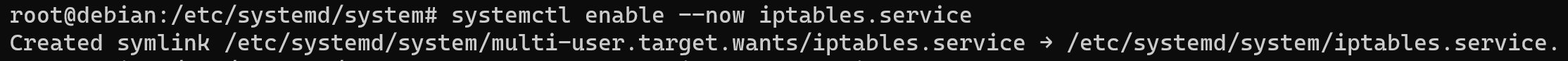
Anschließend können Sie den Service neu laden. Starten Sie den Service nun entweder per Hand oder stellen Sie ein, dass er jedes Mal beim Starten ausgeführt wird.



Code : # systemctl daemon-reload



Code : # systemctl start iptables.service



Code : # systemctl enable --now iptables.service

#### Firewall testen

Testen Sie die Firewall, indem Sie die Regeln, die Sie konfiguriert haben, ausprobieren. Zum Beispiel sollten Sie die Virtuelle Debian Maschine von der Virtuellen Windows Maschine nicht pingen.

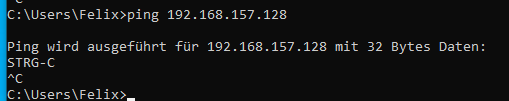


Abbildung : not-ping Debian

### Firewall konfigurieren (nftables)

Eine andere Variante, wie man die Firewall konfigurieren kann ist **NFTABLES**. Dazu muss man eine .conf-Datei erstellen, in der alle Regeln festgelegt werden. nftables verwendet hier ein wenig ein anderes Aussehen als iptables.

#### nftables.conf konfigurieren

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : Firewall NFTABLES Konfiguration

#### nftables.conf ersetzen

Nun müssen Sie im Ordner „/etc“ die alte nftables.conf (dort stehen noch die Konfigurationen von iptables drinnen) durch die neue nftables.conf (obirger SS) ersetzen. Machen Sie vorher jedoch eine Kopie der alten nftables.conf-Datei, z.B.: nftables.conf.bak

#### iptables stoppen

Falls Sie Probleme mit iptables haben, weil sich eventuell irgendetwas in einem .service-File verändert haben und iptables nun neu laden will, führen Sie diesen Befehl aus:



Code : # systemctl daemon-reload

Deaktivieren Sie iptables mit diesem Befehl:



Code : # systemctl disable --now iptables

#### nftables starten

Um nftables zu aktivieren, führen Sie diesen Befehl durch:



Code : # systemctl enable –now nftables

Kontrollieren Sie auch, ob die Regeln der Firewall nun richtig konfiguriert sind.



Code : # nft list ruleset

Der Output dieses Befehls sollten die eingestellten Regeln sein.

#### nftables stoppen

Mithilfe dieses Befehls kann man die NFTABLES-Regeln löschen. Beim nächsten Hochfahren werden die Regeln allerdings wieder ausgeführt, weil sie immer noch aktiviert sind.



Code : # nft flush ruleset

## IPv6

### Virtuelle Debian Server Maschine IPv6-Adresse zuweisen

Die Virtuelle Debian Maschine (also der Server) muss eine statische IPv6-Adresse bekommen (auf der richtigen Netzwerkkarte).

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : IPv6-Adresse Server (statisch) (/etc/network/interfaces)

### Netzwerkkarte IPv6 erlauben

Damit IPv6 funktioniert, muss man in der „/etc/default/isc-dhcp-server“ einstellen, welche Interfaces (Netzwerkkarten) verwendet werden.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : /etc/default/isc-dhcp-server

### DHCPv6 konfigurieren

Konfigurieren Sie DHCPv6 indem Sie in der Datei /etc/dhcp/dhcpd6.conf zwei Dinge ändern.

* Schreiben Sie eine beliebige Domain in die Options hinein.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : /etc/dhcp/dhcpd6.conf

* Entkommentieren Sie am Ende der Datei das folgende Subnetz und geben Sie den Adressbereich ein:

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : /etc/dhcp/dhcpd6.conf

#### radvd installieren und konfigurieren

Laden Sie mit Aptitude das radvd Paket herunter. Erstellen Sie in „/etc“ eine Datei namens „radvd.conf“.

Eine Beispielsdatei von radvd.conf finden Sie in „/usr/share/doc/radvd/examples/radvd.conf.example“.

zusätzliche Informationen: Durch die radvd-Konfiguration wird im Netzwerk fc00 eine stateful IP-Konfiguration vorgegeben.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : /etc/radvd.conf

#### Firewall anpassen

Damit man nun auch wirklich pingen kann, muss man in der NFTABLES Firewall-Konfiguration noch ein bisschen etwas umändern, nämlich 2 neue Zeilen (markiert) hinzufügen:

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : Firewall anpassen

#### Windows überprüfen

Um sicherzustellen, dass IPv6-DHCP funktioniert, starten Sie die Virtuelle Windows Maschine und überprüfen Sie die IPv6-Adressen. Hier sollte nun eine Adresse aus dem angegebenen Adressbereich stehen.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : Windows IPv6-Adresse

#### Ping

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : IPv6-Adressen pingen

## Apache2

Apache2 ist ein Webserver, der in unserem Fall auf der Debian Server Maschine laufen soll. Mithilfe dieses Webservers können wir überprüfen, ob das, was wir in der Theorie gelernt haben auch stimmt, nämlich: Muss man bei URLs wirklich eckige Klammern ([]) um die IPv6-Adresse herumschreiben, damit WWW das als IPv6-Adresse erkennt? Ansonsten würde es nämlich ein Problem geben, weil der Port bereits Doppelpunkte (:) als Trennzeichen verwendet.

Installieren Sie Apache2 mittels Aptitude und überprüfen Sie, ob Sie auf der Virtuellen Windows Maschine diesen Webserver erreichen.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : URL-Pfad IPv6

## Samba

Samba ist das Standardprogramm für die Interoperabilität von Windows mit Linux und Unix. Seit 1992 bietet Samba sichere, stabile und schnelle Datei- und Druckdienste für alle Clients, die das SMB/CIFS-Protokoll verwenden, wie z.B. alle Versionen von DOS und Windows, OS/2, Linux und viele andere.

### Installation

Als erstes muss man mithilfe von Aptitude das Samba-Paket installieren.

### Shared Folder

Anschließend erstellen wir einen Media-Ordner. In diesem Ordner befinden sich später alle Dateien, die öffentlich geteilt werden wollen. Dieser Ordner bekommt alle Berechtigungen, sodass jeder darin herumschreiben, lesen und ausführen kann.

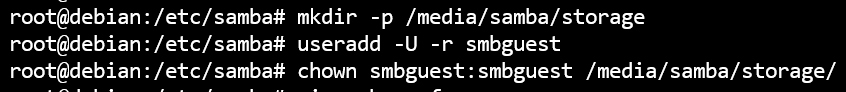


Abbildung : Shared Folder erstellen

### Konfiguration

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : Samba public folder

### Samba Service neu starten

Samba können Sie mit diesem Befehl neu starten:

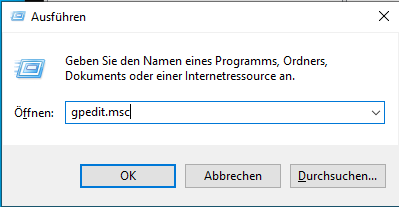
zusätzliche Informationen: Das d am Ende steht bei Services immer für Daemon.



Code : # systemctl restart smbd

### Unsichere Gastanmeldungen aktiveren

Bei Windows Education Versionen muss man anschließend noch unsichere Gastanmelungen aktivieren, damit die Verbindung mit einem „\public“-Folder hergestellt werden kann.

Diese Aktion kann folgendermaßen durchgeführt werden: + R drücken, damit ein unten links ein kleines Fenster aufpoppt, wo Sie gpedit.msc hineinschreiben. Das ist die schnellste Variante, die lokalen Gruppenrichtlinien bei Windows zu öffnen.

Anschließend klicken Sie die im Screenshot gelb markierten Ordner an und aktivieren Sie schlussendlich die unsicheren Gastanmeldungen. Somit sollte der UNC-Pfad funktionieren.

Abbildung : gpedit.msc

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : unsichere Gastanmeldungen aktivieren

### Fileshare funktioniert

Um zu überprüfen, ob der Fileshare funktioniert, gehen Sie zur Virtuellen Windows Maschine und tippen Sie im Explorer die IPv6-Adresse der Virtuellen Debian Server Maschine mit Bindestrichen (-) statt Doppelpunkten (:) ein. Anschließend sollten Sie Zugriff auf den Shared Folder erhalten.



Abbildung : IPv6-UNC-Pfad

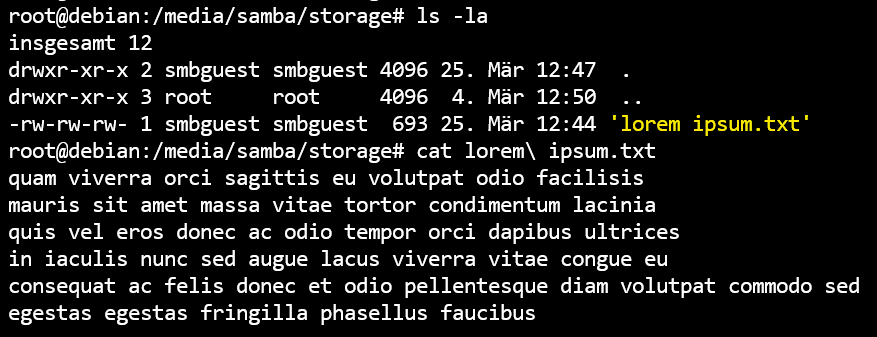
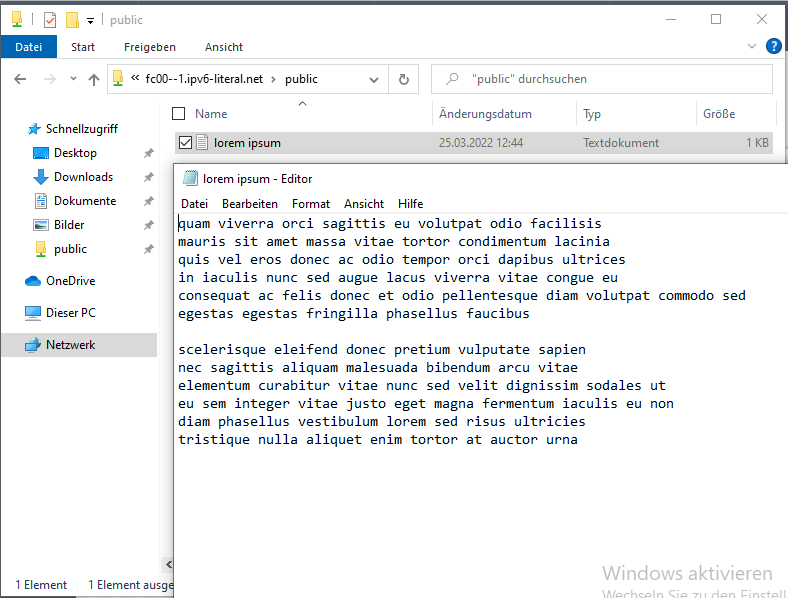


Abbildung : SAMBA funktioniert

### Firewallrules anpassen

Damit die Firewall auch eine verbindungsorientierte TCP-Verbindung auf Port 445 zulässt, müssen Sie noch die grau hinterlegte Zeile bei Ihren NFTABLES-Rules hinzufügen:

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung : Firewall anpassen

## DNS-Server

### Konfiguration

#### Options-Datei

Konfigurieren Sie die „/etc/bind/named.conf.options“ – Datei, damit DNS funktioniert. Dort können Sie auch einstellen, dass Sie einen Forwarder benötigen.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung 71: /etc/bind/named.conf.options

#### named.conf.local

Damit die Zonendateien auch gefunden werden können, müssen Sie in der named.conf.local die Zonen einbinden.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung 72: /etc/bind/namend.conf.local

#### Forward Zone

In der Forward Zone (db.schneider.local) stehen alle Umwandlungen von Namen in IP-Adressen drinnen.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung 73: /etc/bind/zones/db.schneider.local

Wie man sehen kann, funktioniert diese Zone:

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung 74: Forward-Zone funktioniert

Ein Bild, das Text enthält.

Automatisch generierte BeschreibungEin Bild, das Text enthält.

Automatisch generierte BeschreibungEin Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung 75: Überprüfung

#### IPv4 Reversed Lookup Zone

In der IPv4 Reversed Lookup Zone (db.21.10.10.in-addr.arpa) stehen alle Umwandlungen von IP-Adressen in Namen drinnen. Diese soll dann ungefähr so aussehen:

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung 76: /etc/bind/zones/db.21.10.10.in-addr.arpa

Wie man sehen kann, funktioniert die IPv4 Reverse Lookup Zone ebenfalls:

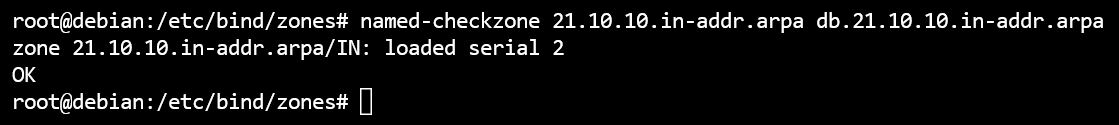


Abbildung 77: IPv4 Reversed Lookup Zone funktioniert

Ein Bild, das Text enthält.

Automatisch generierte BeschreibungEin Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung 78: Überprüfung

#### IPv6 Reversed Lookup Zone

In der IPv6 Reversed Lookup Zone (db.fc00.ip6.arpa) stehen alle Umwandlungen von IPv6-Adressen in Namen drinnen. Diese soll dann ungefähr so aussehen:

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung 79: /etc/bind/zones/db.fc00.ip6.arpa

Wie man sehen kann, funktioniert die IPv6 Reverse Lookup Zone ebenfalls:

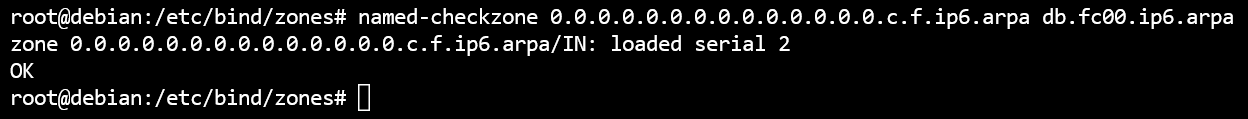


Abbildung 80: IPv6 Reversed-Lookup Zone funktioniert

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung 81: Überprüfung

#### DHCP anpassen

In der „/etc/dhcp/dhcpd.conf“ – Datei müssen Sie den Domain-Namen eintragen:

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung 82: /etc/dhcp/dhcpd.conf

Auch bei IPv6 müssen Sie den Server eintragen: „/etc/dhcp/dhcpd6.conf“



Abbildung 83: /etc/dhcp/dhcpd6.conf

### DNS-Server selbst nutzen

#### /etc/network/interfaces

Damit der DNS-Server selbst auch die Zonendateien am DNS-Server nutzen kann, muss man in der Datei „/etc/network/interfaces“ die beiden markierten Zeilen hinzufügen, damit in der „/etc/resolv.conf“ – Datei vom DNS-Server der Server selbst eingetragen ist.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung 84: /etc/network/interfaces

#### resolvconf installieren

Installieren Sie den Manager der Datei „/etc/resolv.conf“ 🡪 resolvconf



Code 34: # aptitude install resolvconf

#### /etc/resolv.conf

Überprüfen Sie die Datei „/etc/resolv.conf“.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung 85: /etc/resolv.conf

Nun sollte der Server selbst auch DNS-Abfragen auflösen können.

# Abbildungsverzeichnis

[Abbildung 1: ISO Datei auswählen 4](#_Toc104375342)

[Abbildung 2: Hardwareeinstellungen 5](#_Toc104375343)

[Abbildung 3: Medium einbinden/laden 6](#_Toc104375344)

[Abbildung 4: Name der Domain eingeben 7](#_Toc104375345)

[Abbildung 5: Shadow-Passwörter 7](#_Toc104375346)

[Abbildung 6: Übersicht – Festplatte partitionieren 8](#_Toc104375347)

[Abbildung 7: Partitionstabelle 8](#_Toc104375348)

[Abbildung 8: Größe der Partition 8](#_Toc104375349)

[Abbildung 9: Partitionseinstellungen 9](#_Toc104375350)

[Abbildung 10: Kernel des Basissystems 9](#_Toc104375351)

[Abbildung 11: Dienste auswählen 10](#_Toc104375352)

[Abbildung 12: EFI Erzwingung deaktivieren 10](#_Toc104375353)

[Abbildung 13: Root-Anmeldung möglich 10](#_Toc104375354)

[Abbildung 14: sources.list 11](#_Toc104375355)

[Abbildung 15: Aptitude 12](#_Toc104375356)

[Abbildung 16: nach openssh suchen 12](#_Toc104375357)

[Abbildung 17: Putty Configuration 13](#_Toc104375358)

[Abbildung 18: ip -c a Ausgabe 15](#_Toc104375359)

[Abbildung 19: route -n Ausgabe 15](#_Toc104375360)

[Abbildung 20: more /etc/resolv.conf Ausgabe 15](#_Toc104375361)

[Abbildung 21: more/etc/network/interfaces Ausgabe 16](#_Toc104375362)

[Abbildung 22: Beispiel für Ausgabe von # tail -f /var/log/syslog 16](#_Toc104375363)

[Abbildung 23: LAN Segment 17](#_Toc104375364)

[Abbildung 24: /etc/network/interfaces 18](#_Toc104375365)

[Abbildung 25: IPv4-Adressen Einstellungen Windows 19](#_Toc104375366)

[Abbildung 26: ipconfig 19](#_Toc104375367)

[Abbildung 27: Firewall deaktivieren 20](#_Toc104375368)

[Abbildung 28 (links): Debian – ping Windows 20](#_Toc104375369)

[Abbildung 29 (rechts): Windows – ping Debian 20](#_Toc104375370)

[Abbildung 30: Pfad der Virtuellen Debian Maschine finden 21](#_Toc104375371)

[Abbildung 31: Virtuelle Debian Maschine - Datei 21](#_Toc104375372)

[Abbildung 32: LAN-Segment entfernen 21](#_Toc104375373)

[Abbildung 33: ip.php 22](#_Toc104375374)

[Abbildung 34: Netzwerkaufbau NAT 23](#_Toc104375375)

[Abbildung 35: IP-Tabellen-Einstellungen 23](#_Toc104375376)

[Abbildung 36: Webserver erreichen NAT 24](#_Toc104375377)

[Abbildung 37: sysctl.conf - net.IPv4.ip\_forward=1 25](#_Toc104375378)

[Abbildung 38: Route-Einstellungen von Virtueller Debian Maschine 25](#_Toc104375379)

[Abbildung 39: Route-Einstellungen von Virtuelle Debian Klon Maschine 26](#_Toc104375380)

[Abbildung 40: Virtuelle Windows Maschine DNS-Server 27](#_Toc104375381)

[Abbildung 41: Netzwerkkarte DHCP einstellen 28](#_Toc104375382)

[Abbildung 42: Subnetz DHCP einstellen 28](#_Toc104375383)

[Abbildung 43: IP-Adresse automatisch beziehen 29](#_Toc104375384)

[Abbildung 44: Ausgabe der Interneteinstellungen Windows 29](#_Toc104375385)

[Abbildung 45: Syslog-Datei Ausgabe 29](#_Toc104375386)

[Abbildung 46: dhcpd.conf mit fixer Adresse 30](#_Toc104375387)

[Abbildung 47: IP-Konfiguration Virtuelle Windows Maschine 30](#_Toc104375388)

[Abbildung 48: iptables-Konfiguration speichern 31](#_Toc104375389)

[Abbildung 49: iptables-Konfiguration laden 31](#_Toc104375390)

[Abbildung 50: Firewall iptables Befehle 32](#_Toc104375391)

[Abbildung 51: Datei mit Konfiguration (iptables) 32](#_Toc104375392)

[Abbildung 52: /etc/systemd/system/iptables.service 33](#_Toc104375393)

[Abbildung 53: not-ping Debian 33](#_Toc104375394)

[Abbildung 54: Firewall NFTABLES Konfiguration 34](#_Toc104375395)

[Abbildung 55: IPv6-Adresse Server (statisch) (/etc/network/interfaces) 35](#_Toc104375396)

[Abbildung 56: /etc/default/isc-dhcp-server 36](#_Toc104375397)

[Abbildung 57: /etc/dhcp/dhcpd6.conf 36](#_Toc104375398)

[Abbildung 58: /etc/dhcp/dhcpd6.conf 36](#_Toc104375399)

[Abbildung 59: /etc/radvd.conf 37](#_Toc104375400)

[Abbildung 60: Firewall anpassen 37](#_Toc104375401)

[Abbildung 61: Windows IPv6-Adresse 38](#_Toc104375402)

[Abbildung 62: IPv6-Adressen pingen 38](#_Toc104375403)

[Abbildung 63: URL-Pfad IPv6 38](#_Toc104375404)

[Abbildung 64: Shared Folder erstellen 39](#_Toc104375405)

[Abbildung 65: Samba public folder 39](#_Toc104375406)

[Abbildung 66: gpedit.msc 40](https://htlkrems3500-my.sharepoint.com/personal/f_schneider_htlkrems_at/Documents/Schule/NWTK/NWTK_Protokoll_DebianServer.docx#_Toc104375407)

[Abbildung 67: unsichere Gastanmeldungen aktivieren 40](#_Toc104375408)

[Abbildung 68: IPv6-UNC-Pfad 40](#_Toc104375409)

[Abbildung 69: SAMBA funktioniert 40](#_Toc104375410)

[Abbildung 70: Firewall anpassen 41](#_Toc104375411)

[Abbildung 71: /etc/bind/named.conf.options 42](#_Toc104375412)

[Abbildung 72: /etc/bind/namend.conf.local 42](#_Toc104375413)

[Abbildung 73: /etc/bind/zones/db.schneider.local 43](#_Toc104375414)

[Abbildung 74: Forward-Zone funktioniert 43](#_Toc104375415)

[Abbildung 75: Überprüfung 43](#_Toc104375416)

[Abbildung 76: /etc/bind/zones/db.21.10.10.in-addr.arpa 44](#_Toc104375417)

[Abbildung 77: IPv4 Reversed Lookup Zone funktioniert 44](#_Toc104375418)

[Abbildung 78: Überprüfung 44](#_Toc104375419)

[Abbildung 79: /etc/bind/zones/db.fc00.ip6.arpa 45](#_Toc104375420)

[Abbildung 80: IPv6 Reversed-Lookup Zone funktioniert 45](#_Toc104375421)

[Abbildung 81: Überprüfung 45](#_Toc104375422)

[Abbildung 82: /etc/dhcp/dhcpd.conf 46](#_Toc104375423)

[Abbildung 83: /etc/dhcp/dhcpd6.conf 46](#_Toc104375424)

[Abbildung 84: /etc/network/interfaces 47](#_Toc104375425)

[Abbildung 85: /etc/resolv.conf 47](#_Toc104375426)

# Codeverzeichnis

[# nano sources.list 11](#_Toc104375427)

[# apt-get update 11](#_Toc104375428)

[# apt-get install aptitude 11](#_Toc104375429)

[# aptitude 11](#_Toc104375430)

[# su - root 14](#_Toc104375431)

[# nano sshd\_config 14](#_Toc104375432)

[# /etc/init.d/ssh restart 14](#_Toc104375433)

[# ip -c a 14](#_Toc104375434)

[# route -n 15](#_Toc104375435)

[# more /etc/resolv.conf 15](#_Toc104375436)

[# more /etc/network/interfaces 15](#_Toc104375437)

[# tail -f /var/log/syslog 16](#_Toc104375438)

[# nano /etc/network/interfaces 17](#_Toc104375439)

[# /etc/init.d/networking restart 18](#_Toc104375440)

[# service networking restart 18](#_Toc104375441)

[# ipconfig 19](#_Toc104375442)

[# nano /var/www/html/ip.php 22](#_Toc104375443)

[# iptables -t nat -A POSTROUTING -o ens33 -j MASQUERADE 23](#_Toc104375444)

[# iptables -t nat -L 24](#_Toc104375445)

[# sysctl -p 25](#_Toc104375446)

[# route add -net 10.10.21.0/24 gw 192.168.157.128 25](#_Toc104375447)

[# systemctl restart isc-dhcp-server.service 28](#_Toc104375448)

[# ipconfig /all 29](#_Toc104375449)

[# iptables-restore iptables.rules 32](#_Toc104375450)

[# systemctl daemon-reload 33](#_Toc104375451)

[# systemctl start iptables.service 33](#_Toc104375452)

[# systemctl enable --now iptables.service 33](#_Toc104375453)

[# systemctl daemon-reload 35](#_Toc104375454)

[# systemctl disable --now iptables 35](#_Toc104375455)

[# systemctl enable –now nftables 35](#_Toc104375456)

[# nft list ruleset 35](#_Toc104375457)

[# nft flush ruleset 35](#_Toc104375458)

[# systemctl restart smbd 39](#_Toc104375459)

[# aptitude install resolvconf 47](#_Toc104375460)

# Ergebnisse

Funktionierender Debian Server und angeschlossenem Windows und Debian Client. Folgende Protokolle / Programme wurden verwendet:

* DHCP (IPv4 + IPv6)
* Firewall (iptables + nftables)
* Apache2 + PHP
* Samba
* DNS

# Kommentar

Die Konfiguration der Firewall haben Clemens Schlipfinger und ich nicht mit einem Shell-Script gemacht, sondern mit einem SystemD-Service.