SCHULNETZ®

QUALIFIZIERUNG
VON SYSTEMBETREUERINNEN
UND SYSTEMBETREUERN

LINUX-SERVER

LABORÜBUNGEN

AKADEMIE FÜR LEHRERFORTBILDUNG
UND PERSONALFÜHRUNG DILLINGEN

IMPRESSUM

Die im Laborbuch „Linux-Netzwerke“ beschriebenen Übungen wurden im Rahmen der Fortbildungsinitiative SCHULNETZ zur Qualifizierung von Systembetreuerinnen und Systembetreuern von IT-Multiplikatoren erarbeitet.

Herausgeber: Akademie für Lehrerfortbildung und Personalführung
Kardinal-von-Waldburg-Str. 6-7
89407 Dillingen

Dokumentation: Georg Schlagbauer, Akademie Dillingen
Barbara Maier, Akademie Dillingen

URL: http://alp.dillingen.de/schulnetz
Mail: schlagbauer@alp.dillingen.de
Stand: November 2017

INHALT

LABORÜBUNG 01 - INSTALLATION EINES LINUX-SERVERS

Ein Linux-Server soll installiert und eingerichtet werden. Es werden nur die unbedingt erforderlichen Programme installiert. Auf eine grafische Oberfläche wird verzichtet.

Aufgaben

1. Installieren Sie die Linux-Distribution Debian (Stabile Version). Verwenden Sie zur Partitionierung folgende Vorgaben:
   - eine Partition: swap (2 GB)
   - eine Partition: / (10 GB)
   - eine Partition: /tmp (2 GB)
   - eine Partition: /var (15 GB)
   - eine Partition: /home (Rest)
2. Wählen Sie einen „Netzwerkspiegel“ aus, damit Sie später auf aktuelle Pakete zugreifen können.
3. Deaktivieren Sie im Menüfenster „Softwareauswahl“ die gesamte Software, so dass nur das Minimalsystem installiert wird.
4. Aktualisieren Sie Ihr Betriebssystem.
5. Installieren Sie, wann immer im laufenden Betrieb erforderlich, die notwendigen Programme nach.
6. Vergeben Sie eine statische IP-Adresse und überprüfen Sie die Netzwerkfunktionalität:
   - IP-Konfiguration
   - ping auf das Gateway
   - ping auf einen anderen PC
   - ping auf den DNS-Server
   - ping auf alp.dillingen.de (Überprüfung der Namensauflösung)
7. Richten Sie einen ssh-Zugriff auf den Linux-Server ein.

Hinweise

Überlegungen zur Partitionierung

- Für den Auslagerungsbereich (swap) ist eine eigene (primäre) Partition sinnvoll.
- Verzeichnisse, die bei einem Betriebssystem-Update erhalten bleiben sollen, werden in einen eigenen Bereich ausgelagert (z. B. Benutzerdaten).
- Verzeichnisse in denen Benutzer direkte oder indirekte Schreibrechte haben, werden in einen eigenen Bereich ausgelagert.

swap	Swap-Partition (Auslagerungsdatei)
/var	Variable Daten, z. B. Log-Dateien, Webseiten, Druckerwarteschlange, Datenbanken
/tmp	Temporäre Daten
/home	Homeverzeichnisse der Benutzer

Als Dateisystem wird heute vorzugsweise ext4 verwendet.

Infomationen zum Dateisystem

`fdisk -l`	Anzeige der Partitionierungsdaten
`df -h`	Freier und belegter Platz im Dateisystem (disk free)
`df -hT`	Anzeige des Dateisystemtyps
`du -hs *`	Belegter Festplattenpatz der einzelnen Verzeichnisse

Aktualisieren des Betriebssystems

`aptitude update`	Aktualisierung der Softwarelisten
`aptitude upgrade`	Aktualisierung der installierten Software

Installation eines Kommandozeilen-Texteditors

`vim`	Komfortversion des Editors vi (vi improved)
`nano`	Einfacher Texteditor

Informationen zum Netzwerk

`ip address`	IP-Adresse der Netzwerkkarten
`ip route`	Anzeige der Routing-Tabelle
`ip neighbour`	Anzeige des arp-cache
`ip neighbour flush all`	Löschen des des arp-cache
`ip –s link show`	Informationen zur Netzwerkkarte

Zu den ip-Befehlen sind abkürzende Schreibweisen zulässig, z. B.

`ip address, ip addr, ip a`

`ip neighbour, ip neigh, ip n`

Viele weiter klassische Netzwerkbefehle sind im Paket net-toos enthalten.

`aptitude install net-tools`	Installation von net-tools
`ifconfig`	IP-Adresse
`route -n`	Routing-Tabelle
`arp -n`	Anzeige des arp-cache
`netstat -r`	Routing-Tabelle
`netstat -atn`	aktive Netzverbindungen

Einrichten einer statischen IP-Adresse

```
/etc/network/interfaces


iface eth1 inet static
            address 10.1.1.100
            netmask 255.255.255.0
            gateway 10.1.1.1
            dns-nameservers 10.36.102.31 10.36.102.32
```

Der PC muss neu gestartet werden, damit die Änderungen wirken. Zur Auswertung des Eintrags „dns-nameservers“ muss das Paket resolvconf installiert sein.

SSH-Zugriff vom Arbeitsplatzrechner auf den Server

```
ssh root@10.1.1.100
```
Zugriff auf den Server als Benutzer „root“

ssh-Zugriff für den Benutzer root erlauben

In vielen Linux-Distributionen ist der ssh-Zugriff für den Benutzer root standardmäßig deaktiviert.

```
Konfigurationsdatei /etc/ssh/sshd_config

# Authentication
PermitRootLogin yes
```

Anschließend ssh-Dämon neu starten:

```
/etc/init.d/ssh restart
```

Alternative:

```
systemctl restart sshd
```


LABORÜBUNG 02 - RECHTE EINES BENUTZERS

Welche Rechte hat ein Benutzer (z. B. der Benutzer „standard“) in den einzelnen Verzeichnissen?

Aufgaben

1. Geben Sie an, welches das Homeverzeichnis des Standardbenutzers ist und welche Rechte der Benutzer in seinem Homeverzeichnis hat.

   Homeverzeichnis: _____

   Rechte im Homeverzeichnis: _____

2. Geben Sie an, welche Bedeutung die folgenden Verzeichnisse haben und welche Rechte der Standardbenutzer in diesen Verzeichnissen hat:

   /etc: _____

   /root: _____

   /usr: _____

   /var: _____

   /tmp: _____

   Legen Sie in den Verzeichnissen, in denen Sie als Standardbenutzer Schreibrechte haben, Testdateien an.

3. Ändern Sie gegebenenfalls die Rechte des Verzeichnisses /root, so dass nur der Systemadministrator root Zugang zu seinem Homeverzeichnis hat (Standardeinstellung bei vielen Linux-Systemen). Andere Benutzer sollen in diesem Verzeichnis kein Leserecht haben.
4. Erstellen Sie als root im Verzeichnis /home das Unterverzeichnis Daten. Welche Möglichkeiten gibt es, dem Standardbenutzer Schreibrechte in diesem Verzeichnis zu geben?

Hinweise

Zugriffsrechte

Jede Datei und jedes Verzeichnis hat unter Unix verschiedene Zugriffsrechte. Auf der Kommandozeile zeigt der Befehl `ls -l` die Zugriffsrechte an.

`ls -l`	Zeigt den Inhalt eines Verzeichnisses ausführlich an (long listing).

```
Server:/home/standard# ls -l
drwxr-xr-x 2 standard standard 4096 2007-03-02 14:28 Daten
drwx------ 2 standard standard 4096 2007-03-02 14:29 Privat
drwxr-xr-x 2 standard standard 4096 2007-03-02 14:29 Projekte
-rw-r--r-- 1 standard standard  298 2007-03-02.14:30 vorlage.txt
```

`d`	Es handelt sich um ein Verzeichnis (directory).
`rwx r-x r-x`	Rechte für Besitzer, Gruppe und Andere
`standard standard`	Besitzer und Gruppe
`2007-03-02 14:28`	Datum der letzten Änderung
`Daten`	Name der Datei bzw. des Verzeichnisses

Besitzer

Jede Datei und jedes Verzeichnis gehört einem Besitzer. Wird eine Datei neu erzeugt, wird der erzeugende Benutzer der Besitzer. Dieser Besitzer kann auch die Rechte an der Datei bzw. dem Verzeichnis verändern.

Gruppe

Jede Datei und jedes Verzeichnis gehört einer Gruppe. Wird eine Datei neu erzeugt, wird ihr die primäre Gruppe des erzeugenden Benutzers zugeordnet.

Standardrechte unter Linux

`rwx r-x r-x` Die Rechte sind in drei Bereiche unterteilt für Besitzer, Gruppe und Andere:

Der erste Block gibt dabei die Rechte des Besitzers an, im zweiten Block stehen die Rechte für die Mitglieder einer Gruppe und der dritte Block umfasst die Rechte aller übrigen Benutzer (others).

`r` (read) Der Benutzer kann die Datei lesen bzw. sich das Inhaltsverzeichnis eines Verzeichnisses anzeigen lassen.

`w` (write) Der Benutzer kann die Datei verändern. In einem Verzeichnis kann der Benutzer neue Dateien oder Verzeichnisse anlegen.

`x` (execute) Der Benutzer kann eine Datei ausführen. Bei einem Verzeichnis kann der Benutzer in dieses Verzeichnis wechseln.

Oktale Darstellung der Rechte

Die Rechte der drei Bereiche Besitzer, Gruppe und Andere lassen sich auch als Oktalzahlen darstellen:

```
r ⇔ 4
w ⇔ 2
x ⇔ 1

rwx r-x r-x ⇔ 755
rw- r-- r-- ⇔ 644
rwx --- --- ⇔ 700
```

Üblicherweise wird die oktale Darstellung 4-stellig angegeben (0755 statt 755). Die erste Stelle ist für eine Erweiterung mit Spezialbits vorgesehen.

Ändern von Rechten (oktale Zahlendarstellung)

`chmod` (change modus) Standardprogramm unter Linux zum Verändern von Rechten.

`chmod 0700 Privat` Die Rechte des Verzeichnisses Privat werden auf 700 (Besitzer darf alles, Gruppe und Andere dürfen nichts) gesetzt.

`chmod 0644 Testdatei` Die Rechte der Datei werden auf `rw- r-- r--` gesetzt.

Ändern von Rechten (symbolische Darstellung)

`chmod u=rw,g=r,o=r Testdatei`	Die Rechte der Datei werden auf `rw- r-- r--` (644) gesetzt.
`chmod g-w,o-w Testdatei`	Eventuell gesetzte Schreibrechte für Gruppe und Andere werden entfernt.
`chmod -R g-rwx,o-rwx Privat`	Im Verzeichnis Privat und in allen darin enthaltenen Dateien und Unterverzeichnissen werden die Rechte für Gruppe und Andere entfernt.
`chmod -R g=,o= Privat`	Genau das Gleiche.
`chmod g+rw *`	Alle Dateien im aktuellen Verzeichnis werden für die Gruppe les- und schreibbar.

Modifikatoren

`u`	Einstellungen betreffen nur den Besitzer
`g`	Einstellungen betreffen nur die Gruppe
`o`	Einstellungen betreffen nur Andere
`a`	Einstellungen betreffen Besitzer, Gruppe und Andere
`=`	Rechte setzen
`+`	Rechte hinzufügen
`-`	Rechte entfernen

Ändern eines Besitzers

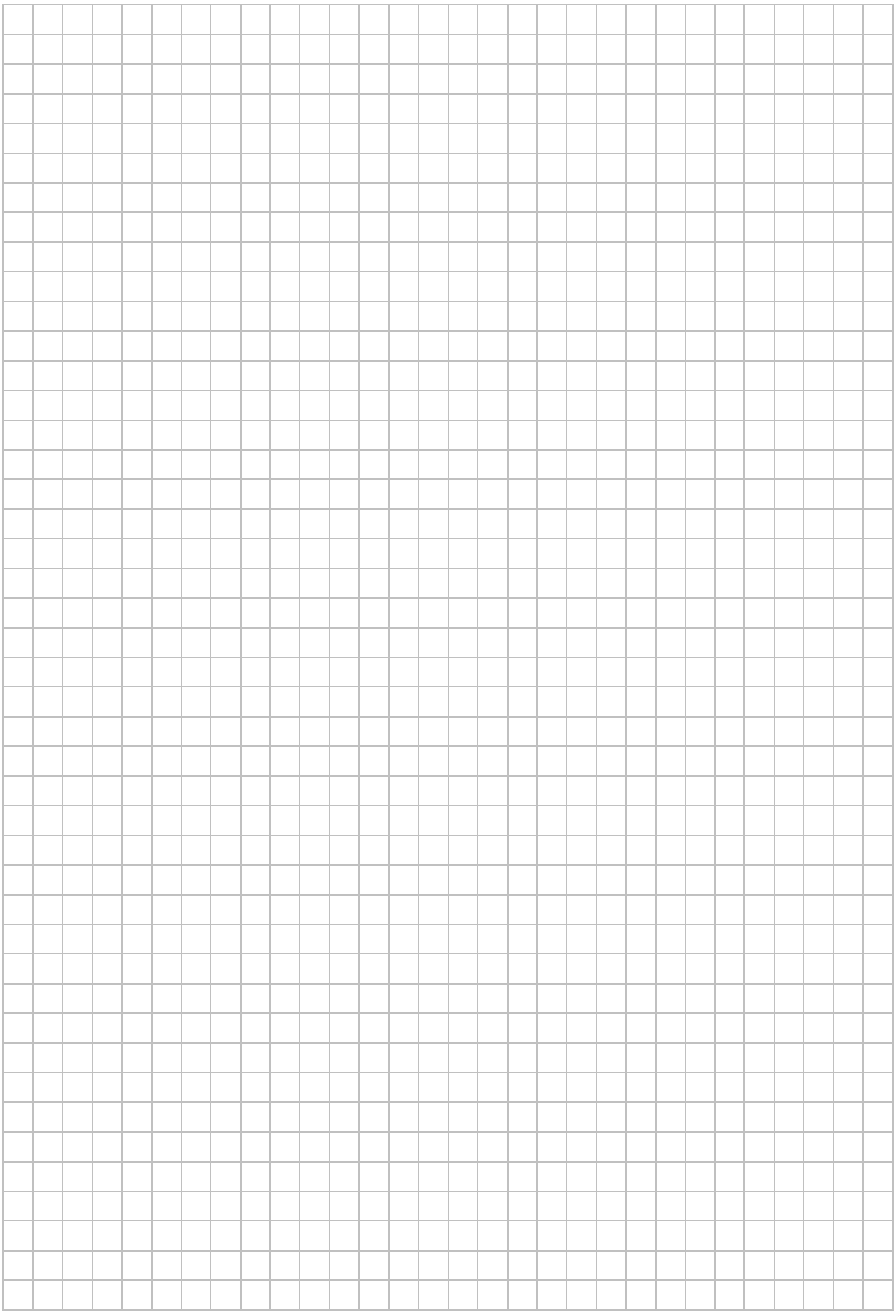
`chown`	(change owner) Ändern des Besitzers einer Datei.
`chgrp`	(change group) Ändern der Gruppe einer Datei.
`chown standard Privat`	Das Verzeichnis Privat erhält als Besitzer den Benutzer standard.
`chown –R standard Privat`	Das Verzeichnis Privat und alle darin enthaltenen Unterverzeichnisse und Dateien erhalten als Besitzer den Benutzer standard.
`chgrp –R standard Privat`	Das Verzeichnis Privat und alle darin enthaltenen Unterverzeichnisse und Dateien erhalten als Gruppe die Gruppe standard.
`chown –R standard.standard Privat`	Das Verzeichnis Privat und alle darin enthaltenen Unterverzeichnisse und Dateien erhalten als Besitzer den Benutzer standard und als Gruppe die Gruppe standard.

Der Typ einer Datei

Die erste Spalte beim Listing `ls –l` gibt den Typ des Eintrages an:

`-`	Normale Datei
`l`	Soft-Link
`d`	Verzeichnis
`c`	Zeichenorientiertes Gerät
`b`	Blockorientiertes Gerät
`s`	Socket
`p`	Pipe

Notizen



LABORÜBUNG 03 - BENUTZERVERWALTUNG AUF EINEM FILESERVER

In der Schule wird ein Fileserver eingerichtet, auf dem Lehrer und Schüler Daten ablegen können. Jeder Schüler und Lehrer soll ein Homeverzeichnis haben. Daneben gibt es auch Austausch- und Vorlagenverzeichnisse mit unterschiedlichen Zugriffsrechten.

Aufgaben

1. Legen Sie am Linux-Fileserver die Benutzer s1, s2, l1 und l2 an und geben Sie jedem Benutzer ein Homeverzeichnis. Überprüfen Sie, ob sich die Benutzer lokal am Fileserver anmelden können und Zugriff auf ihre Homeverzeichnisse haben.
2. Erstellen Sie im Verzeichnis /home ein neues Verzeichnis Austausch, in dem alle Benutzer Schreibrechte haben.
3. Überprüfen Sie, ob ein Benutzer im Ordner Austausch die Daten eines anderen Benutzers verändern oder löschen kann. Unterscheiden Sie dabei folgende Fälle:

   s2 kann Dateien von s1 löschen: (ja/nein) _____

   s2 kann leere Ordner von s1 löschen: _____

   s2 kann Ordner mit Inhalt von s1 löschen: _____

   s2 kann in Ordnern von s1 Daten ablegen: _____

   s2 kann Ordner mit Inhalt umbenennen: _____

4. Verändern Sie die Rechte im Ordner Austausch so, dass ein Benutzer die Dateien eines anderen Benutzers nicht löschen kann.
5. Erstellen Sie entsprechend dem Ordner Austausch einen neuen Ordner Vorlagen, in dem nur die Lehrer Schreibrechte haben.

Hinweise

Anlegen und Löschen von Benutzern

Je nach Distribution ordnet Linux einen neuen Benutzer einer Standardgruppe zu (z. B. users) oder legt eine eigene Gruppe mit dem Namen des Benutzers an.

`useradd`	Standardwerkzeug unter Linux zum Anlegen von Benutzern.
`useradd standard`	Anlegen des Benutzers standard
`useradd -m standard`	Anlegen des Benutzers standard und automatisches Anlegen des Homeverzeichnisses für den Benutzer standard.
`userdel standard`	Löschen des Benutzers standard
`adduser`	Interaktives Kommandozeilenwerkzeug zum Anlegen von Benutzern auf Debian-Systemen.
`adduser standard`	Anlegen des Benutzers standard

Ändern eines Passwortes

`passwd`	Standardwerkzeug unter Linux zum Ändern eines Passwortes.
`passwd standard`	Ändern des Passwortes des Benutzers standard.

Umgang mit Gruppen

`groupadd`	Standardwerkzeug unter Linux zum Anlegen von Gruppen.
`groupdel`	Standardwerkzeug unter Linux zum Löschen von Gruppen.
`groups`	Zeigt alle Gruppen an, zu welchen der gerade angemeldete Benutzer gehört.
`groups standard`	Zeigt die Gruppen an, zu welcher der Benutzer standard gehört.
`adduser standard lehrer`	Fügt den Benutzer standard der Gruppe lehrer hinzu.
`deluser standard lehrer`	Entfernt den Benutzer standard aus der Gruppe lehrer.
`usermod -G audio,video standard`	Der Benutzer standard wird Mitglied der Gruppen audio und video. Er gehört keinen weiteren Gruppen an.

Erweiterung der Zugriffsrechte durch Spezialbits

user-id-bit	Ein Programm mit diesem Bit wird so gestartet, als ob es der Besitzer des Programms starten würde.
group-id-bit	In einem Verzeichnis mit gesetztem group-id-bit werden neu angelegte Dateien der Gruppe des Verzeichnisses zugeordnet und nicht der primären Gruppe des erzeugenden Benutzers.
sticky-bit	In einem Verzeichnis mit gesetztem sticky-bit kann nur der Besitzer einer Datei diese löschen (Löschschutz).

Oktale Darstellung der Spezialbits

```
user-id-bit   ⇔ 4
group-id-bit ⇔ 2
sticky-bit    ⇔ 1
```

Die oktale Darstellung der Dateirechte wird üblicherweise 4-stellig angegeben, wobei die erste Stelle die Spezialbits symbolisiert. Bei der Darstellung im Listing (ls –l) werden die Spezialbits mit der üblichen Darstellung (rwx) vermischt.

`- rws r-x r-x ⇔ 4755`	Ausführbare Datei mit Besitzerrechten
`d rwx rws r-x ⇔ 2775`	Verzeichnis mit Gruppen-id-bit
`d rwx rwx rwt ⇔ 1777`	Verzeichnis mit Sticky-bit

Standardrechte für neue Dateien

Die Rechte, die eine neu angelegte Datei oder ein neu erstelltes Verzeichnis erhält, sind in der umask festgelegt. Üblich ist eine umask von 0022 oder von 0002.

```
umask 0022
```

`0644 ⇔ rw- r-- r--`	Rechte einer neuen Datei
`0755 ⇔ rwx r-x r-x`	Rechte eines neuen Verzeichnisses

```
umask 0002
```

`0664 ⇔ rw- rw- r--`	Rechte einer neuen Datei
`0775 ⇔ rwx rwx r-x`	Rechte eines neuen Verzeichnisses

LABORÜBUNG 04 - SSH-ZUGRIFF AUF EINEN SERVER

Die Administration eines Linux-Servers soll von einem Linux- oder Windows-Client aus über eine verschlüsselte ssh-Verbindung (secure shell) erfolgen.

Aufgaben

1. Überprüfen Sie, ob am Server der SSH-Dienst installiert ist und läuft.
2. Beschränken Sie den SSH-Zugriff auf bestimmte Benutzer. Verhindern Sie, dass sich der Benutzer root direkt über ssh einloggen kann.
3. Kopieren Sie über die verschlüsselte SSH-Verbindung eine Datei vom Client zum Server.
4. Laden Sie am Server (auf Kommandozeile) eine Datei aus dem Internet

Weiterführende Aufgaben

5. Lassen Sie den SSH-Dienst nicht auf dem Standard-Port 22, sondern auf einem Port > 1024 laufen.
6. Binden Sie ein Serververzeichnis in den Dateibaum ein und testen Sie den Zugriff mit verschiedenen Anwendungen aus.

Hinweise

SSH ermöglicht eine sichere verschlüsselte Verbindung zwischen zwei Computern.

SSH-Dienst auf dem Linux-Server

`ps aux | grep ssh`	Überprüft, ob der SSH-Dienst läuft.
`/etc/init.d/ssh stop`	SSH-Dienst anhalten.
`/etc/init.d/ssh start`	SSH-Dienst starten.
`/etc/init.d/ssh restart`	SSH-Dienst neu starten.
`/etc/ssh/sshd_config`	Konfigurationsdatei des SSH-Dienstes.

Beschränkung des SSH-Zugriffs auf bestimmte Benutzer

In der Konfigurationsdatei /etc/ssh/sshd_config kann mit den Einträgen AllowUsers, AllowGroups, DenyUsers und DenyGroups der Zugriff beschränkt werden.

`PermitRootLogin yes`	Anmeldung für root erlauben
`AllowUsers root admin@10.1.* gs chris`	Nur die angegebenen Benutzer dürfen per ssh zugreifen.
`AllowGroups admin ssh`	Nur die Mitglieder der angegebenen Gruppen dürfen per ssh zugreifen.

SSH -Zugriff von einem Linux-Client auf den Server

`ssh root@10.1.1.100`	Zugriff auf den Server (10.1.1.100) als Benutzer root.
`ssh s1@10.1.1.10`	Zugriff auf den Server als Benutzer s1.
`scp datei.txt root@10.36.16.100:/root`	Kopiert die Datei datei.txt auf den Server (als Benutzer root) in das angegebenen Verzeichnis.

SSH -Zugriff unter Gnome

```
Orte – Verbindung zu Server – SSH
```

SSH -Zugriff von einem Windows-Client auf den Linux-Server

`putty.exe`	Kommandozeilenzugriff auf einen Server.
`pscp`	Kopieren von Dateien (entspricht scp).
`winscp`	Grafisches Tool zum Kopieren von Dateien.

Kopieren und Einfügen unter Putty

Eine Markierung mit der Maus wird automatisch in die Zwischenablage übernommen. Zum Einfügen genügt unter Putty ein rechter Mausklick.

Download einer Datei aus dem Internet

```
wget http://alp.dillingen.de/schulnetz/materialien/Systembetreuung.pdf
```

Die Adresse kann über “copy and paste” eingefügt werden. Im putty-Fenster genügt zum Einfügen ein rechter Mausklick.

Authentifizierung bei einer SSH-Verbindung

Beim ersten SSH-Zugriff auf einen Server stellt der Client fest, dass er den öffentlichen Schlüssel des Servers nicht hinterlegt hat und er deshalb die Authentizität des Servers nicht bestätigen kann. Man erhält eine Meldung ähnlich dieser:

```
The authenticity of host '10.1.1.100' can't be estab-
lished.
RSA key fingerprint is
e3:97:ce:00:0b:2f:7c:83:44:1c:87:9b:e1.
Are you sure you want to continue connecting (yes/no)?
```

Bestätigt man beim ersten Zugriff die Authentizität des Servers, so wird der öffentliche Schlüssel des Servers bei einem Windows-Client in der Registry, bei einem Linux-Client unter „known_hosts“ eingetragen und ist zukünftig bekannt.

`~/.ssh/known_hosts`	Datei, in der die öffentlichen Schlüssel aller bekannten Verbindungen gespeichert sind.

Stimmt beim SSH-Zugriff der öffentliche Schlüssel des Servers nicht mit dem am Client hinterlegten Schlüssel überein, wird die Verbindung verweigert. Man erhält eine Meldung der Art:

```
WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Host key verification failed.
```

Wenn man am Server nichts verändert hat, kann diese Meldung auf einen Angriff hindeuten. Falls man (z. B. durch eine Neuinstallation des Servers) die Schlüssel des Servers verändert hat, ist es notwendig, am Client den zugehörigen öffentlichen Schlüssel des Servers zu löschen oder den korrekten Schlüssel einzutragen.

Einbinden eines Verzeichnisses in den Dateibaum

`aptitude install sshfs`	Installation des ssh-Dateisystems (Client).
`sshfs s1@10.1.1.10: <mountpoint>`	Zugriff auf den Server als Benutzer s1. Der lokale Benutzer des Clients muss Eigentümer des Mountpoint sein.
`fusermount –u <mountpoint>`	Aushängen des ssh-Dateisystems.

Beispiel für ein Anmeldeskript

```
#!/bin/bash
read –p "Benutzername: " USER
sshfs $USER@10.1.1.10: ~/server
```

Das Verzeichnis server unterhalb des Homeverzeichnisses des Benutzers muss existieren.

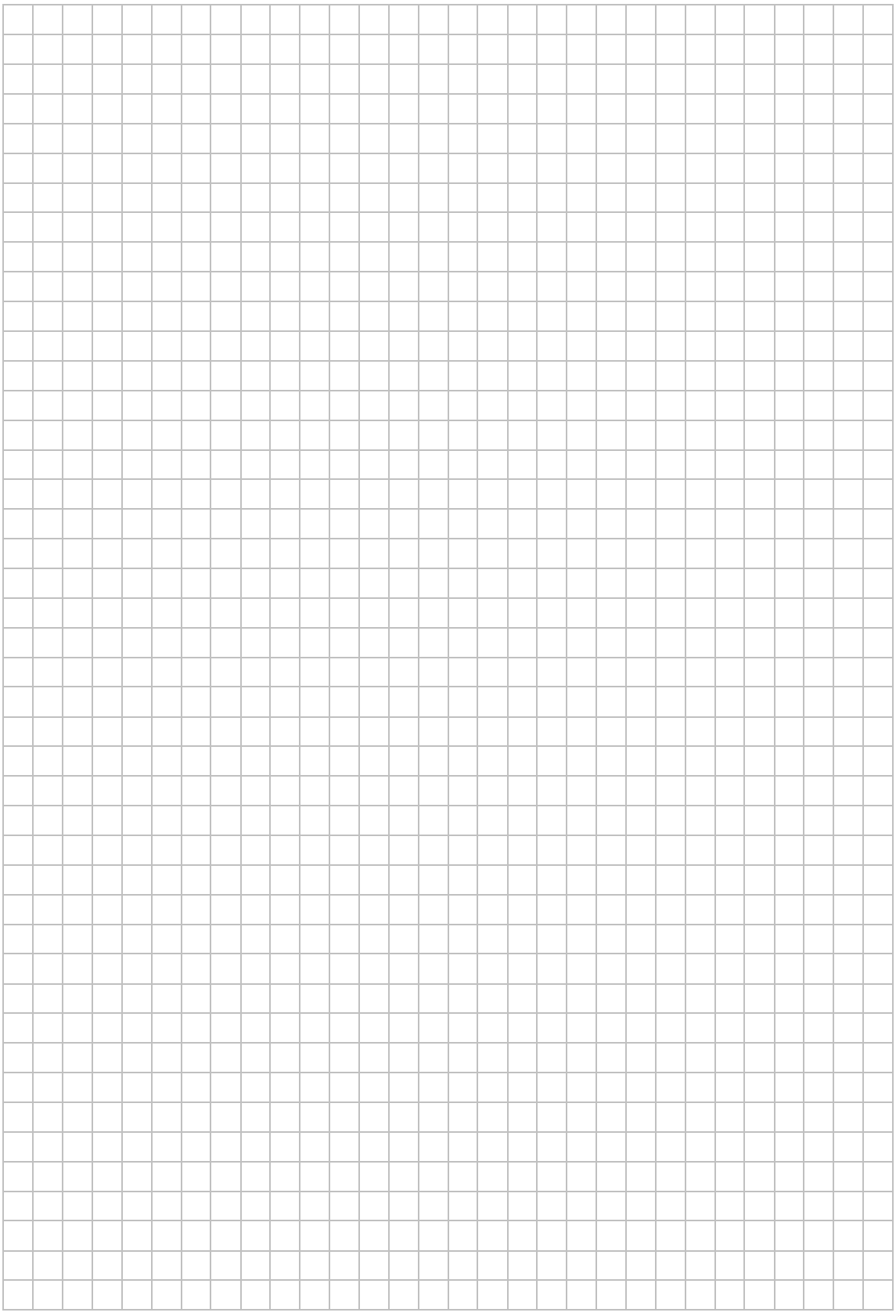
LABORÜBUNG 05 - SMB-ZUGRIFF AUF EINEN FILESERVER

Auf den Fileserver der Schule soll über das Netzwerk sowohl von den Windows- als auch von den Linux-Computern aus zugegriffen werden. Beim Zugriff müssen sich die Benutzer mit Benutzernamen und Passwort authentifizieren.

Aufgaben

1. Installieren Sie am Fileserver das Paket Samba.
2. Richten Sie für die Benutzer s1, s2, l1 und l2 einen Samba-Zugang ein und konfigurieren Sie Samba so, dass jeder Benutzer Zugriff auf sein Homeverzeichnis hat.
3. Überprüfen Sie den SMB-Zugriff auf den Fileserver von einem Windows- und einem Linux-Computer aus.
4. Ermitteln Sie am Fileserver, welche Benutzer mit dem Fileserver über Samba verbunden sind.
5. Geben Sie die Ordner Vorlagen und Austausch unter Samba frei und überprüfen Sie den Zugriff auf diese Freigaben von einem Windows- und einem Linux-Computer aus.
6. Melden Sie sich am Samba-Server mit falschem Passwort an. Werten Sie die Log-Dateien aus und interpretieren Sie die Fehlermeldungen.

Notizen



Hinweise zur Installation von Samba

Paket Samba installieren

`aptitude install samba`	Installation des Samba-Servers

Die Samba-Konfigurationsdatei /etc/samba/smb.conf

Die Konfigurationsdatei smb.conf besteht aus einem Abschnitt [global], in dem allgemeine Einstellungen getroffen werden und den einzelnen Freigaben mit den Freigabenamen als Abschnittsbezeichnung.

```
[global]
  workgroup = Schulnetz
  log file = /var/log/samba.log
  log level = 1
  max log size = 1000
  server role = standalone server
  passdb backend = tdbsam

[Daten]
  comment = Alle Homeverzeichnisse
  path = /home
  browseable = yes
  writeable = yes
```

Auswahl der Benutzerdatenbank

`passdb backend = smbpasswd`	Klassische Benutzerdatenbank zur Kontenverwaltung
`passdb backend = tdbsam`	Derzeit empfohlene Benutzerdatenbank zur Verwaltung der SAM-Datenbank (Kontenverwaltung – Security Account Manager).
`passdb backend = ldapsam`	Directory-basierte Datenbank für umfangreiche Installationen.

Loglevel

`log level = 0`	Keine Protokollierung
`log level = 1`	Erfolgreiche An- und Abmeldevorgänge werden protokolliert.
`log level = 2`	Alle An- und Abmeldeversuche werden protokolliert.
`log level = 3`	Standardeinstellung

Syntaxüberprüfung der Konfigurationsdatei

`testparm`	Überprüft die Syntax der Samba-Konfigurationsdatei auf deren Richtigkeit.

Starten und Beenden von Samba

`/etc/init.d/samba start`	Startet den Samba-Dienst.
`/etc/init.d/samba stop`	Beendet den Samba-Dienst.
`/etc/init.d/samba restart`	Beendet und Startet den Samba-Dienst neu.

Passwortverwaltung

Passwörter werden sowohl unter Linux als auch unter Windows nicht im Klartext gespeichert, sondern als Hashwert, aus dem das Passwort nicht zurückgerechnet werden kann. Linux verwendet jedoch einen anderen Verschlüsselungsalgorithmus als Windows. Deshalb kann Samba nicht die Passwörter von Linux verwenden und baut eine eigene Passwortverwaltung auf.

Einrichten von Benutzern

`smbpasswd –a s1`	Neuer Samba-Zugang für den Benutzer s1.
`smbpasswd s1`	Ändern des Samba-Passworts für den Benutzer s1

Anlegen und Verwalten von Benutzern

`pdbedit`	Programm zur Verwaltung der SAM-Datenbank (Kontenverwaltung – Security Account Manager).
`pdbedit –L`	Auflisten aller Samba-Zugänge.
`pdbedit –u s1 –v`	Ausführliche Information zum Benutzer s1.
`smbstatus`	Gibt Information zu aktuellen Samba-Verbindungen aus.
`smbstatus –b`	(brief) Kurzinformation über Verbindungen.

Die Samba-Konfigurationsdatei /etc/samba/smb.conf

```
[global]
  workgroup = Schulnetz
  log file = /var/log/samba.log
  log level = 1
  max log size = 1000
  server role = standalone server
  passdb backend = tdbsam

[homes]
  comment = Homeverzeichnisse
  browseable = no
  writeable = yes
[Austausch]
  comment = Austauschverzeichnis
  path = /home/Austausch
  browseable = yes
  writeable = yes
[Vorlagen]
  comment = Vorlagenverzeichnis
  path = /home/Vorlagen
  browseable = yes
  writeable = yes
```


Troubleshooting

`/var/log/samba/`	Verzeichnis mit den Log-Dateien des Samba-Dienstes
`tail –f /var/log/samba/log.smbd`	Änderungen in der Log-Datei können sofort beobachtet werden.

Anzeige der verfügbaren SMB-Freigaben

`smbclient`	Client für den Zugriff auf SMB-/CIFS-Ressourcen auf Servern.
`smbclient –L 10.1.1.100 –N`	Zeigt die SMB-Freigaben eines Servers an.

Zugriff auf eine Freigabe unter Windows:

Explorer-Adressleiste: `\\ip-Adresse`

Explorer-Adressleiste: `\\10.36.16.200`

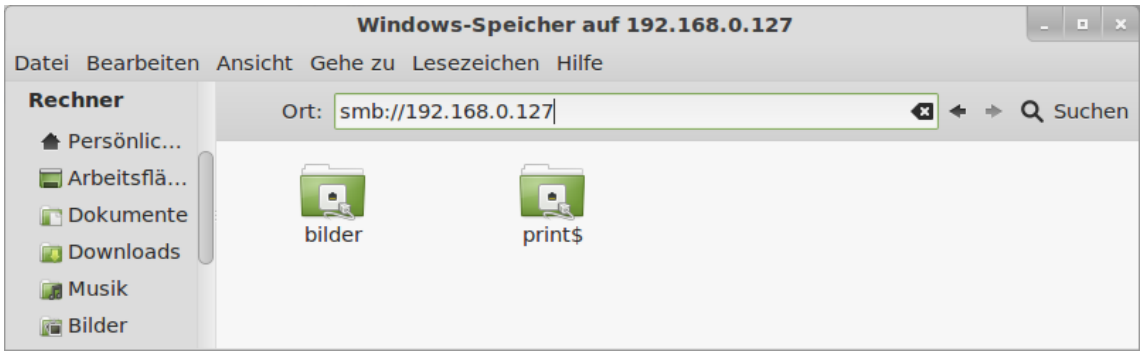
Windows-Kommandozeile:

```
net use Laufwerk: \\ip-Adresse\Freigabe
net use k: \\10.36.16.200\Austausch
```


Zugriff auf eine Samba-Freigabe unter Linux

Zugriff auf Freigaben über die Adresszeile im Datei-Browser

```
smb://ip-Adresse
smb://ip-Adresse/freigabe
smb://user@<ip-Adresse>
```



Zugriff auf eine Samba-Freigabe unter Linux (Kommandozeile)

Für die folgenden Zugriffe sind teilweise administrative Rechte am Client erforderlich.

```
mount //Server/Freigabe /Mountpoint –o Optionen
mount //10.1.1.10/Daten /media/Daten –o username=s1
```

Die Freigabe Daten wird nach /media/Daten gemountet. Die Authentifizierung am Server erfolgt als Benutzer s1

```
mount //10.1.1.10/Daten /media/Daten –o username=s1,
password=12345,uid=standard
```

Das Passwort kann in der Kommandozeile mit übergeben werden. Die Ergänzung uid=<lokaler user> ist sinnvoll, wenn der Systemadministrator root das Verzeichnis mountet, aber ein normaler Benutzer darauf zugreifen soll

```
umount /media/Daten
```
Aushängen einer Verbindung

Eintrag in /etc/fstab zum automatischen Mounten beim Neustart

Soll eine Serververbindung statisch gemountet werden, so bietet es sich an, die Verbindung in der Datei /etc/fstab festzulegen.

Eintrag in der Datei `/etc/fstab`:

```
//10.36.16.10/Austausch /mnt  cifs
username=s1,password=12345,uid=standard  0  0
```

`mount`	Alle Mountpoints werden angezeigt.
`mount -a`	Alle Laufwerke werden entsprechend der Einträge in der Datei /etc/fstab neu gemountet.
`umount`	Aushängen (un-mount) eines Dateisystems.

LABORÜBUNG 06 - ZUGRIFF AUF EINEN WEB-SERVER

Auf den Fileserver der Schule soll ein Web-Zugriff möglich sein. Schüler und Lehrer haben damit die Möglichkeit, im internen Netz der Schule Inhalte zu veröffentlichen.

Aufgaben

1. Installieren Sie den Webserver apache2. Greifen Sie von einem Browser darauf zu und zeigen Sie, dass der Webserver läuft.
2. Ändern Sie die Startseite des Webservers, so dass eine individuelle Seite der Schule angezeigt wird.
3. Richten Sie für jeden Schüler und Lehrer einen Bereich ein, damit diese eigene Inhalte über den schulinternen Webserver veröffentlichen können.

Hinweise

Installation des Apache2-Webservers

```
aptitude install apache2
```

Konfigurationsdateien

`/etc/apache/httpd.conf`	Konfigurationsdatei von Apache 1
`/etc/apache2/apache2.conf`	Hauptkonfigurationsdatei von Apache 2
`/etc/apache2/mods-available`	Verfügbare Module
`/etc/apache2/mods-enabled`	Module, die gestartet werden.
`/etc/apache2/sites-enabled`	Sites (virtuelle Hosts), die gestartet werden.

Starten und Stoppen des Webservers

`/etc/init.d/apache2 start`	Startet den Webserver
`/etc/init.d/apache2 stop`	Beendet den Webserver
`/etc/init.d/apache2 restart`	Beendet den Webserver und startet ihn neu.

Hinzufügen eines Moduls

Apache stellt über die Direktive userdir eine Möglichkeit bereit, ein bestimmtes Verzeichnis im Homeverzeichnis des jeweiligen Nutzers (z.B. public_html) automatisch auf die URL: http://hostname/~username zu veröffentlichen.

`a2enmod userdir`

Hinzufügen des Moduls userdir. Der Befehl legt im Verzeichnis `/etc/apache2/mods-enabled` zwei zusätzliche symbolische Links an, die in das Verzeichnis `mods-available` verweisen. Dadurch wird ein verfügbares Modul aktiviert.

`/etc/apache2/mods-enabled/userdir.conf`

In dieser Konfigurationsdatei, wird der Verzeichnispfad für die Webseiten der Benutzer festgelegt.

Benutzerauthentifizierung

Apache erlaubt es, in einem Verzeichnis eine Zugriffsdatei (.htaccess) anzulegen. In dieser Zugriffsdatei sind die Bedingungen festgelegt, unter denen ein Benutzer auf dieses Verzeichnis zugreifen kann. Damit die Benutzerauthentifizierung mit .htaccess greift, muss im jeweiligen Abschnitt die Direktive „AllowOverride None“ auf „AllowOverride AuthConfig“ oder „AllowOverride All“ gesetzt werden.

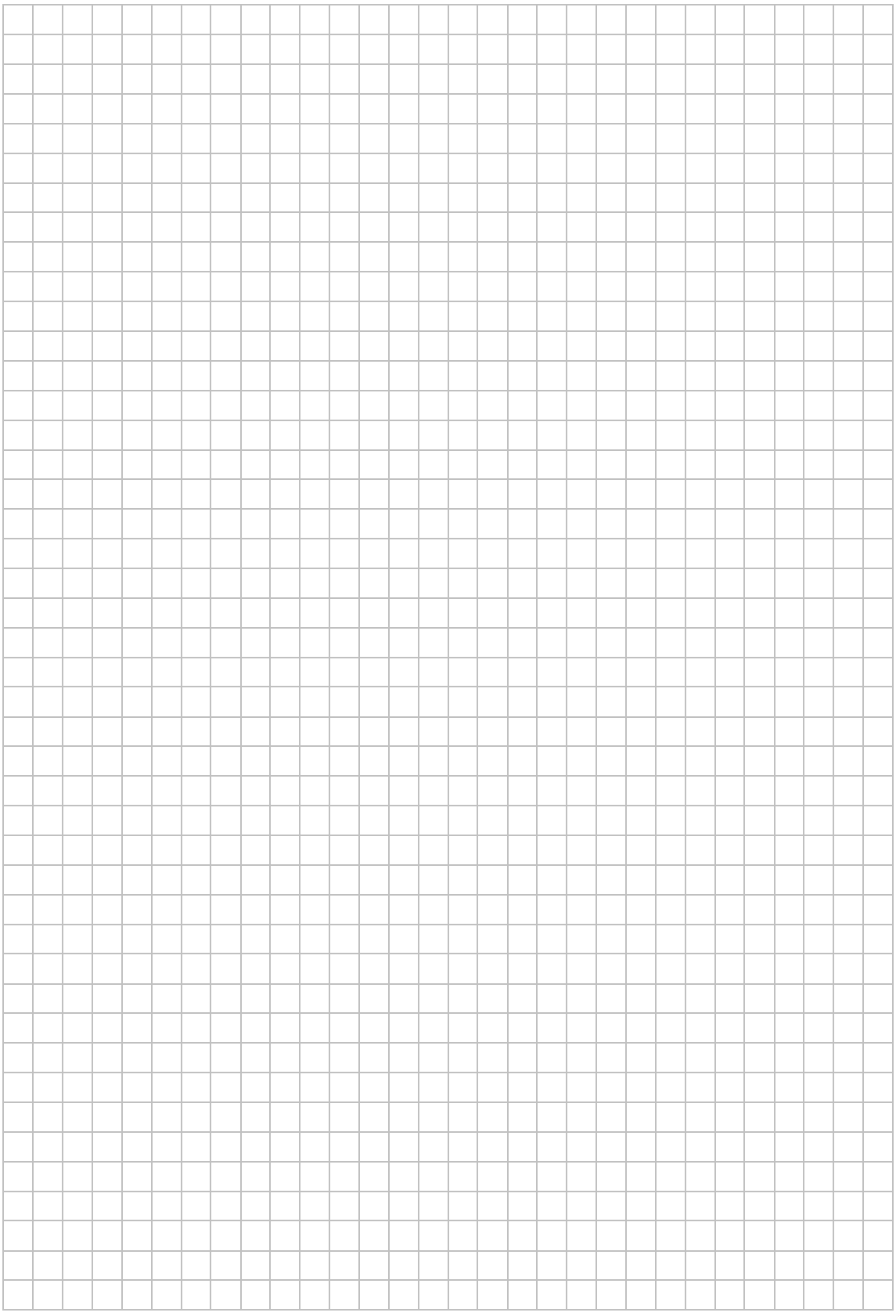
```
/etc/apache2/sites-available/default

<Directory /var/www/>
     AllowOverride All
     ...
</Directory>
```

Beispiel für eine .htaccess-Datei:

```
AuthType Basic
AuthName "SCHULNETZ-Skripte"
AuthUserFile /var/.htpasswd
require user schulnetz
```

`AuthType Basic`	Standard-Benutzerauthentifizierung
`AuthName "SCHULNETZ-Skripte"`	Beschreibung, die im Anmeldebildschirm erscheint.
`AuthUserFile`	Pfad zur Passwortdatei; Die Passwortdatei sollte außerhalb des Webbereichs liegen.
`require user l1 l2`	Benutzer l1 und l2 sind anmeldeberechtigt.
`require valid-user`	Alle Benutzer in der Passwortdatei sind anmeldeberechtigt.
`htpasswd`	Programm zum Verwalten von Passwort-Dateien.
`htpasswd –c .htpasswd l1`	Legt eine neue Passwort-Datei .htpasswd und den Benutzer l1 an.
`htpasswd .htpasswd l2`	Legt den Benutzer l2 in der Passwort-Datei .htpasswd an.

Notizen



LABORÜBUNG 07 - LOKALE DATENSICHERUNG

Die Anwenderdateien sollen am Server lokal in einer anderen Partition oder auf einem anderen Datenträger regelmäßig gesichert werden. Dabei sollen nur die Daten gesichert werden, die seit der letzten Sicherung neu angelegt oder verändert worden sind.

Das Verzeichnisse /home /root und /etc am Server sollen regelmäßig nach /backup gesichert werden.

Aufgaben

1. Legen Sie das Verzeichnis backup an und sichern Sie die Homeverzeichnisse der Benutzer mit rsync.
2. Testen Sie das Wiederherstellen der Daten.
3. Erstellen Sie ein Skript, um die Verzeichnisse /home /root und /etc zu sichern. Automatisieren Sie die Datensicherung, so dass diese automatisch einmal am Tag (in der Testphase alle 2 Minuten) ausgeführt wird.
4. Ergänzen Sie das Skript so, dass Backupverzeichnisse, die älter als 2 Wochen sind (in der Testphase 10 Minuten), automatisch gelöscht werden.

Notizen

Hinweise

Lokales Sichern mit rsync

```
rsync [Optionen] <Quelle> <Ziel>
```

`rsync -a <Quelle> <Ziel>` Sichert Unterverzeichnisse, Dateirechte, Eigentümer, etc. (Archiv-Modus).

`rsync -av <Quelle> <Ziel>` Zeigt den Fortschritt der Sicherung an (verbose).

`rsync -av /home /backup` Sichert das Verzeichnis /home nach /backup

`rsync -av /home/ /backup` Sichert den Inhalt des Verzeichnisses /home nach /backup

`rsync -av --delete /home /backup` Sichert das Verzeichnis /home nach /backup und löscht dabei im Zielverzeichnis Dateien, die im Quellverzeichnis nicht mehr existieren (Synchronisation).

```
rsync -av --delete --backup --backup-dir="/backup/del-1"
/home /backup
```

Kopiert die Dateien, die durch die Synchronisation überschrieben oder gelöscht werden in das angegebene Backupverzeichnis.

Löschen von alten Backupverzeichnissen

```
find /backup -maxdepth 1 -name "del-*" -mtime +14 -print
find /backup -maxdepth 1 -name "del-*" -mmin +10 -print
```

Zeigt alle Verzeichnisse an, die sich im Verzeichnis /backup befinden, mit "del-" beginnen und älter als 14 Tage (10 Minuten) sind.

```
find /backup -maxdepth 1 -name "del-*" -mtime +14 -exec rm
-r {} \;
```

Löscht alle gefundenen Verzeichnisse.

Automatisiertes Starten von Skripten (/etc/crontab)

Die Datei /etc/crontab wird vom System überwacht und es wird jede Minute überprüft, ob ein Eintrag in dieser Datei ist, der abgearbeitet werden muss.

```
15  2 * * * root /root/skripte/backup.sh
```

Das Skript wird täglich um 2.15 Uhr als Benutzer root gestartet.

```
*/2 * * * * root /root/skripte/backup.sh
```

Das Skript wird alle 2 Minuten gestartet.

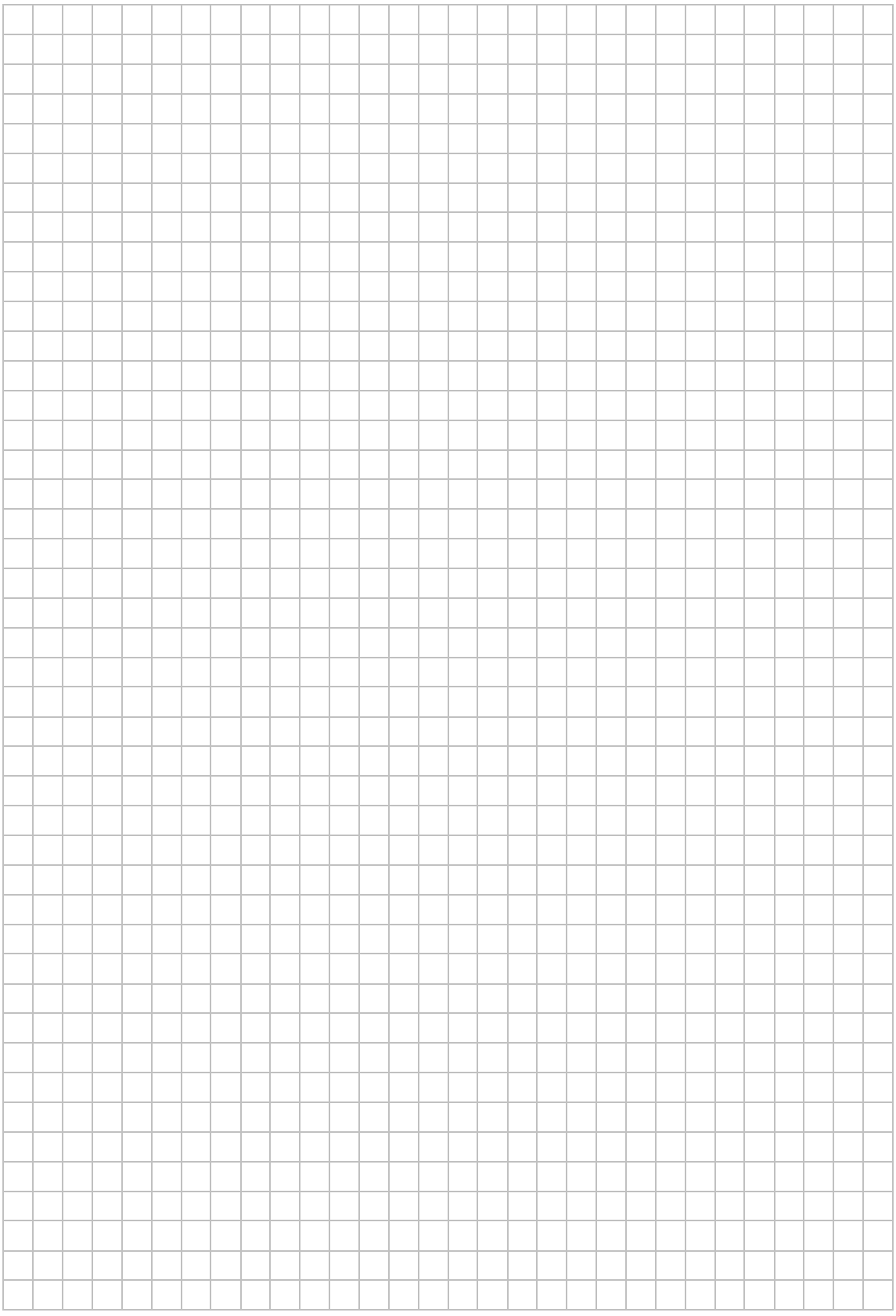
Beispielskript zur Datensicherung

In diesem Beispiel werden die Verzeichnisse */home*, */root* und */etc* nach */backup* gesichert. Im Verzeichnis */backup* wird ein Unterverzeichnis *deleted* angelegt, in dem zwischenzeitlich überschriebene oder gelöschte Versionen der Daten zu finden sind.

Listing von /root/skripte/backup.sh

```
#!/bin/bash
# Beispielskript zur Datensicherung (lokal)
#
# Es wird ein Verzeichnis angelegt, in das die geloeschten
# oder ueberschriebenen Dateien kopiert werden.
DATE=$(date +'%Y%m%d-%H%M')
DELDIR="/backup/deleted/deleted-$DATE"
mkdir -p $DELDIR
#
# Es wird eine Logdatei festgelegt, in der man spaeter den Erfolg
# oder Misserfolg der Datensicherung nachlesen kann.
LogDatei="/root/skripte/backup.log"
#
# Beginn und Ende der Datensicherung werden protokolliert.
echo "Start: " $(date +'%Y-%b-%d-%H:%M,%S') >> $LogDatei
#
rsync -a --delete --backup --backup-dir=$DELDIR /home /backup >> $LogDatei
2>&1
rsync -a --delete --backup --backup-dir=$DELDIR /root /backup >> $LogDatei
2>&1
rsync -a --delete --backup --backup-dir=$DELDIR /etc  /backup >> $LogDatei
2>&1
#
# Dateien, die vor mehr als 2 Wochen geloescht wurden, werden auch in
# der Datensicherung endgueltig geloescht.
find /backup/deleted -maxdepth 1 -name "deleted-*" -mtime +14 -exec rm -r
{} \;
#
echo "Ende:  " $(date +'%Y-%b-%d-%H:%M,%S') >> $LogDatei
echo "-----------------------------------" >> $LogDatei
```


Notizen



LABORÜBUNG 08 - DATENSICHERUNG IM NETZ

Die Anwenderdateien am Server sollen auf einem anderen Computer (Backup-Server) über das Netz gesichert werden. Dabei sollen nur die Daten gesichert werden, die seit der letzten Sicherung neu angelegt oder verändert worden sind.

Als Übungsszenario soll das Verzeichnis /home des Servers auf den Arbeitsplatzcomputer im Verzeichnis /backup-server gesichert werden.

Aufgaben

1. Legen Sie an Ihrem Arbeitsplatzcomputer das Verzeichnis /backup-server an und sichern Sie das Verzeichnis /home des Servers.
2. Testen Sie das Wiederherstellen der Daten.
3. Erstellen Sie ein Skript, um die Datensicherung „auf Knopfdruck“ durchführen zu können.
4. Sorgen Sie dafür, dass das Skript ohne manuelle Benutzereingabe läuft und automatisieren Sie die Datensicherung.

Notizen

Hinweise

Sichern mit rsync über das Netz

Mit rsync kann man eine Datensicherung zwischen zwei Linux-PC auch über das Netz durchführen. Die Verbindung der PC erfolgt verschlüsselt über das ssh-Protokoll. Der entfernte PC wird über <Benutzername>@<Rechnername>:<Verzeichnis> oder <Benutzername>@<IP-Adresse>:<Verzeichnis> angesprochen.

```
rsync [Optionen] <Quelle> <Ziel>
```

```
rsync -av root@10.1.1.100:/home /backup-server
```

Sichert das Verzeichnis /home des PC 10.1.1.100 im lokalen Verzeichnis /backup-server.

Beispielskript zur Datensicherung

Listing von /root/skripte/backup-server.sh

```
#!/bin/bash
# Beispielskript zur Datensicherung ueber das Netz
# Backup der Homeverzeichnisse des Servers 10.1.1.100
#
rsync -a --delete root@10.1.1.100:/home /backup-server
```

SSH-Zugriff ohne Passwort

Wenn am Server der öffentliche Schlüssel des Clients als autorisiert eingetragen ist, kann der Client ohne Eingabe eines Passwortes auf den Server zugreifen.

`ssh-keygen`	Erzeugen eines Schlüsselpaares am Client
`~/.ssh/id_rsa`	Privater Schlüssel des Client
`~/.ssh/id_rsa.pub`	Öffentlicher Schlüssel des Client

```
cat id_rsa.pub >> ~/.ssh/authorized_keys
```

Eintragen des öffentlichen Client-Schlüssel als autorisierter Client am Server.

LABORÜBUNG 09 - PASSWORT-RECOVERY

An einem Linux-Server ist das root-Passwort nicht mehr bekannt.

Aufgaben

1. Starten Sie den Rechner mit einer Root-Shell oder einem Live-System und löschen Sie das vorhandene root-Passwort. Vergeben Sie nach einem Neustart ein neues root-Passwort.
2. Überprüfen Sie, ob das Passwort-Recovery erfolgreich war.

Password-Recovery mit einer Root-Shell

Der Startvorgang unter Linux erfolgt mit Hilfe eines Bootloaders (Lilo oder Grub). Ist dieser Bootloader nicht durch ein Passwort abgesichert (was selten gemacht wird), lässt sich dem Bootloader ein zusätzlicher Parameter übergeben, damit ein Minimalsystem bootet und eine Shell für den Benutzer root zur Verfügung steht.

Grub editieren

Während der Bootloader Grub angezeigt wird, muss die Taste „e“ gedrückt werden, um in den Editiermodus zu kommen. In der Kernel-Boot-Zeile wird der Eintrag init=/bin/bash hinzugefügt. Dieser Eintrag ist temporär.

`kernel /vmlinuz-2.618-3-686 root=/dev/sda2 ro init=/bin/bash`	
`b`	Startet den Bootvorgang

Neues Passwort vergeben

`mount -o remount,rw /`	Damit das Passwort gespeichert werden kann, muss die /-Partition beschreibbar sein.
`mount /usr`	Das Programm passwd liegt unter /usr/bin. Gegebenenfalls muss dieses Verzeichnis erst gemountet werden.
`passwd`	Passwort eingeben
`sync`	Schreibt die Änderung vom Arbeitsspeicher auf die Festplatte.
`mount -o remount,ro /`	Sicherheitshalber kann vor dem Neustart die /-Partition wieder in den reinen Read-Only-Modus versetzt werden.

Passwort-Recovery mit einem Live-System

Nach dem Booten eines Computers mit einem Linux-Live-System (z.B. Installations-CD) kann das root-Passwort des ursprünglichen Systems gelöscht oder neu gesetzt werden. Je nach Version des Live-Systems muss die Partition, in der die /etc/shadow liegt noch gemountet werden. Die Partition muss beschreibbar sein.

Mounten der root-Partition

`fdisk -l`	Anzeige der Partitionierungsdaten, um herauszufinden, in welcher Partition das Wurzelverzeichnis liegt.
`mount /dev/hda1 /mnt`	Mounten der Partition /dev/hda1 nach /mnt

Bearbeiten der Passwort-Datei und manuelles Löschen des Passwortes

In der Passwortdatei /etc/shadow findet man die verschlüsselten Passwörter der Benutzer. Wenn das Passwort gelöscht wird, erfolgt der Zugriff ohne Authentifizierung.

`vi /mnt/etc/shadow` Bearbeiten der Passwortdatei

```
root:$1$G1iCdhXU$JZjZSXWV2kznKIzCUqKBu.:13696:0:99999:7:::
root::13696:0:99999:7:::
```

Nach dem Neustart, kann für root ein neues Passwort vergeben werden.

Leere Passwörter

Einige Distributionen akzeptieren keine Anmeldung von root mit einem leeren Passwort. In diesem Fall kopiert man den verschlüsselten String eines bekannten Passwortes oder generiert ein verschlüsseltes leeres Passwort.

`mkpasswd 12345`	Erzeugt ein (mit crypt) verschlüsseltes Passwort
`mkpasswd ''`	Erzeugt ein verschlüsseltes leeres Passwort
`mkpasswd -S 'U6' ''`	Erzeugt ein verschlüsseltes leeres Passwort mit dem Salt U6 (U6aMy0wojaho).

Alternative: Ändern des Passwortes mit einer chroot-Umgebung

Nachdem der PC von einem Linux-Live-System gestartet wurde, lässt sich mit dem chroot-Befehl eine neue root-Umgebung festlegen, in der natürlich auch das gesamte Linux-System vorhanden sein muss.

`chroot /mnt`	Das Verzeichnis /mnt wird als neue Wurzel des Verzeichnisbaums festgelegt.
`mount /usr`	Das Programm passwd liegt unter /usr/bin. Gegebenenfalls muss dieses Verzeichnis erst gemountet werden.
`passwd`	Passwort eingeben
`sync`	Schreibt die Änderung vom Arbeitsspeicher auf die Festplatte.
`exit`	Beenden der chroot-Umgebung.

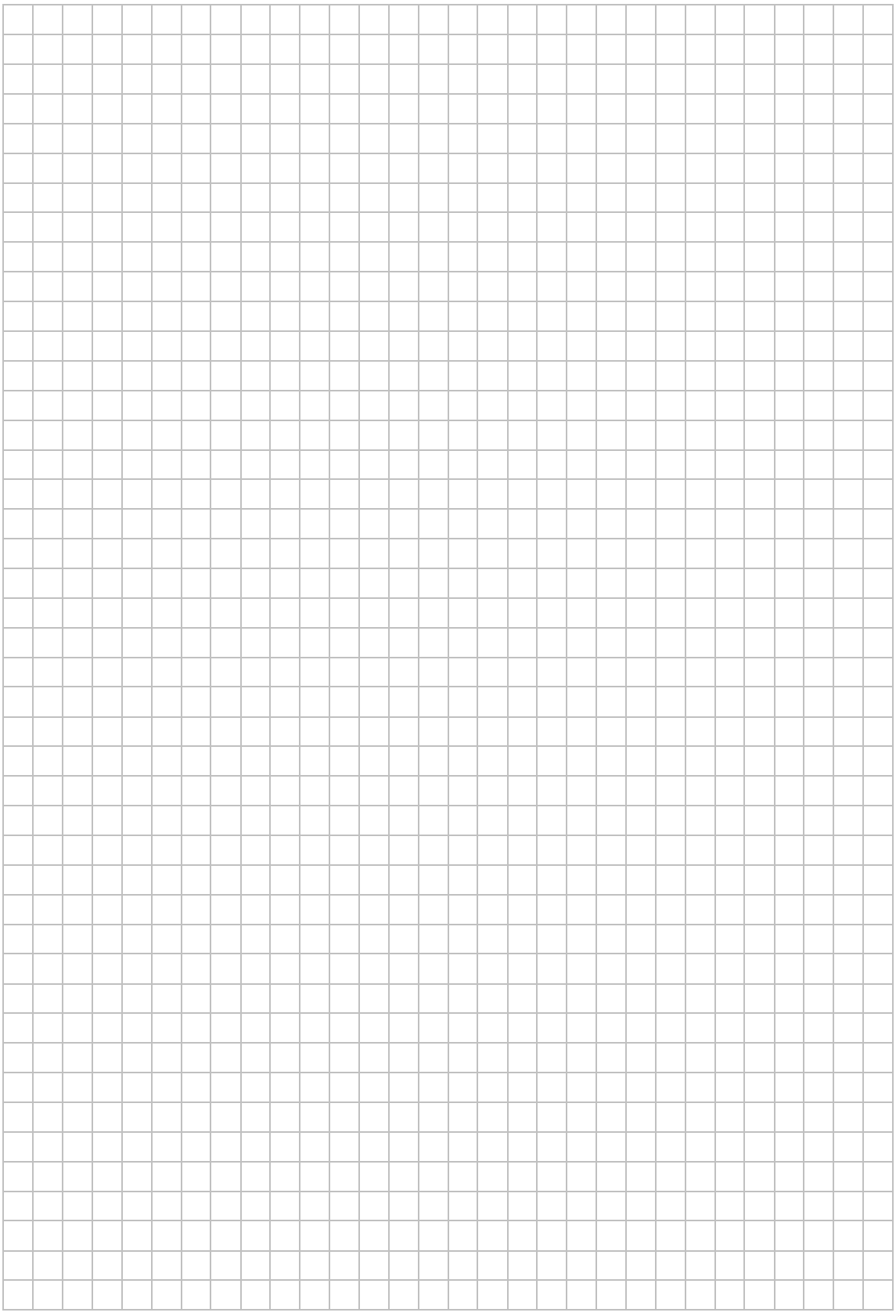
Der Wechsel in die chroot-Umgebung funktioniert nur, bei etwa gleichartigen Systemen, d. h., die Live-Umgebung sollte etwa die gleiche Architektur (vor allem 32bit, 64 bit) haben, wie das installierte System.

LABORÜBUNG 10 - SYSTEMÜBERWACHUNG

Aufgaben

1. Ermitteln Sie folgende Daten für Ihren Computer:
   - Wie lange läuft Ihr Computer bereits?
   - Welche Benutzer haben sich in der letzten Zeit am System angemeldet?
   - Welche Benutzer sind gerade am System angemeldet?
2. Ermitteln Sie, wie groß der belegte Speicherplatz und der noch freie Speicherplatz auf den einzelnen Partitionen der Festplatte sind.
3. Ermitteln Sie, wie viel Festplatten-Speicherplatz die einzelnen Ordner im Wurzelverzeichnis (/bin, /boot, /etc, …) benötigen. Welche Ordner benötigen am meisten Platz? In welchen Ordnern erwarten Sie im Laufe der Zeit den größten Zuwachs?
4. Starten Sie ein größeres Programm und beobachten Sie dabei die CPU- und Arbeitsspeicher-Auslastung Ihres Computers.
5. Schließen Sie einen USB-Stick an den PC an und beobachten Sie dabei Kernel- und Systemmeldungen.

Notizen



Hinweise

Logdateien zur Speicherung verhaltensrelevanter Ereignisse

```
/var/log/messages
/var/log/auth.log
/var/log/kern.log
```

Ausgabe von Logdateien

`less /var/log/messages`	Zeigt die Logdatei mit dem Programm less an.
`tail /var/log/messages`	Zeigt die letzten 10 Zeilen der Logdatei an.
`tail –f /var/log/messages`	Zeigt die letzten 10 Zeilen der Logdatei an und hält die Logdatei geöffnet.
`dmesg`	Zeigt die Systemmeldungen beim letzten Neustart an.

Überwachung der Verbindungen

`last`	Verbindungszeiten der Systembenutzer
`lastlog`	Letzter Anmeldezeitpunkt der eingerichteten Benutzer.
`who`	Zeigt an, wer gerade angemeldet ist.
`w`	Zeigt an, wer gerade angemeldet ist und welches Programm zuletzt gestartet wurde.

Speicherbelegung

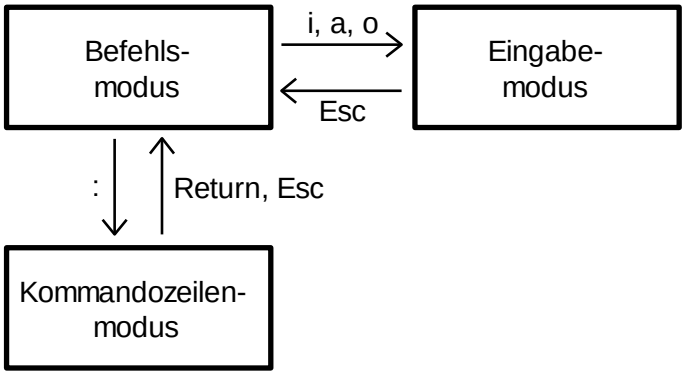
`df`	Zeigt den Speicherplatz der verwendeten Partitionen an.
`df -h`	Ausgabe von `df` in einer besser lesbaren Form (human readable).
`du`	Zeigt an, wie viel Festplatten-Speicherplatz einzelne Dateien oder Verzeichnisse benötigen.
`du -h`	Ausgabe des benötigten Speicherplatzes in einer besser lesbaren Form.
`du -hs /var`	Ermittelt den gesamten Speicherplatz im Verzeichnis /var (incl. aller Unterverzeichnisse).
`du -hs`	Ermittelt den Speicherplatz des aktuellen Verzeichnisses.
`du -hs *`	Ermittelt den Speicherplatz aller Dateien und Unterverzeichnisse.

Ermittlung laufender Prozesse

`top`	Programm zur Beobachtung der Prozesse und Computerauslastung.
`ps`	Anzeige von Prozessen
`ps auxw`	Ausführliche Anzeige aller laufenden Prozesse.
`ps auxw | grep gnome`	Die Prozessliste wird nach der Zeichenkette „gnome“ durchsucht.

DER EDITOR VI

Der Editor vi ist der Standard-Editor unter Linux. Wichtig ist er vor allem deshalb, weil er auf jedem Linux-System verfügbar ist. Üblicherweise wird heute eine erweiterte Version des vi (vim) benutzt.



Modi des Editors

Der Texteditor vi unterscheidet drei Modi:

Befehlsmodus: (command mode) Alle Zeichen werden als Befehle interpretiert.

Eingabemodus: (insert mode) In diesem Modus kann Text eingegeben werden.

Kommandozeilenmodus: (last-line mode) Zum Speichern, Beenden oder zum Aufruf komplexer Funktionen (z. B. Suchen, Ersetzen)

Nach dem Start des Editors befindet man sich im Befehlsmodus.

`i`	Wechsel in den Eingabemodus
`:`	Wechsel in den Kommandozeilenmodus
`Esc`	Wechsel in den Befehlsmodus

Einige elementare Befehle

`vi Dateiname`	Start des Editors vi
`dd`	Löschen einer Zeile
`u`	Macht den letzten Befehl rückgängig.
`:wq`	Speichern und Beenden
`:q!`	Beenden ohne zu speichern
`:set number`	Zeilennummerierung
`:syntax on`	Syntax-Highlighting
`vimtutor`	Interaktives Lernprogramm für den Editor vi

DER ZEILENEDITOR SED

Ersetzen von Zeichenketten in Dateien

Ersetzen von Zeichenketten in allen Dateien mit der Endung html im aktuellen Verzeichnis:

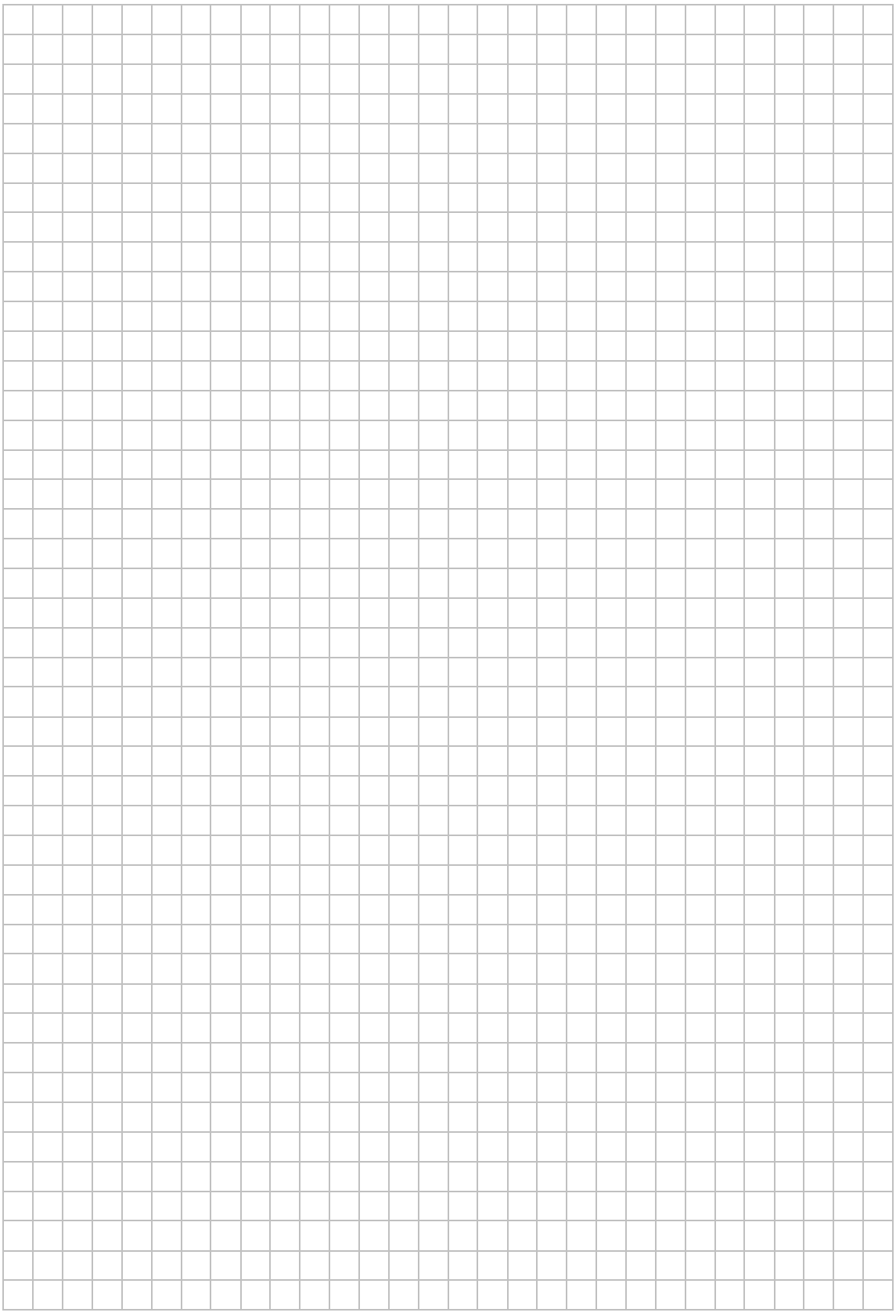
```
sed -i -e '~s|alt|neu|g' *.html
sed -i -e '~s/alt/neu/g' *.html

perl -pi -e '~s|alt|neu|g' *.html

find . -iname "*.html" -depth 1 -exec sed -i "" -e
"s/alt/neu/g" {} \;
```

Umbenennen und Kopieren von Dateien

Alle Dateiname mit der Zeichenkette html werden in htm umgewandelt.

```
rename 's/html/htm/g' *

Alle Dateien mit Bezeichnung *_123.html nach *.234.html kopieren.

mkdir temp
cp *_123.html temp
cd temp
rename 's/123/234/' *
mv * ..
rmdir temp
```


Notizen



LINUX-VERZEICHNISSTRUKTUR

In einem Linux-System werden Dateien in einem Verzeichnisbaum abgelegt, das mit dem Wurzelverzeichnis / beginnt. Im Gegensatz zu Windows werden einzelne Partitionen direkt in diesen Verzeichnisbaum eingehängt (gemountet).

/	Wurzelverzeichnis
/bin	Hier befinden sich wichtige Programme für Anwender, die unmittelbar nach dem Start des Systems zur Verfügung stehen müssen, z. B. die Shells.
/boot	Hier befinden sich die zum Hochfahren des Systems unbedingt erforderlichen Dateien. In der Hauptsache ist das der Kernel, im Normalfall eine Datei mit dem Namen vmlinuz.
/dev	Dieses Verzeichnis enthält Spezialdateien, sogenannte Gerätedateien, die eine Schnittstelle zur Hardware darstellen. Hier finden sich z. B. Einträge für alle Festplatten und ihre Partitionen: (/dev/hda, /dev/hda1, ...)
/etc	Hier sind viele der Konfigurationsdateien untergebracht, welche die Einstellungen verschiedener Programme oder auch grundlegende Systeminformationen enthalten.
/home	In diesem Verzeichnis liegen die Home-Verzeichnisse der Benutzer des Systems.
/lib	Hier befinden sich die wichtigsten Funktionsbibliotheken des Systems.
/proc	Dies ist eigentlich kein normales Verzeichnis, sondern stellt eine Schnittstelle zum Kernel dar. Jedes laufende Programm (d. h. jeder Prozess) wird hier in einem Unterverzeichnis geführt, dessen Dateien viele Informationen z. B. über den aktuellen Programmstatus enthalten. Zudem gibt es eine umfangreiche Verzeichnisstruktur mit Daten über den Kernel und die Hardware des Systems.
/root	Dies ist das Home-Verzeichnis des Systemverwalters *root*. Es liegt traditionell auf der Systempartition im Wurzelverzeichnis, damit *root* auch dann auf seine Dateien (beispielsweise Diagnoseprogramme) zugreifen kann, wenn durch einen Fehler der Zugriff auf andere Partitionen nicht mehr möglich ist.
/sbin	Ähnlich wie */bin* enthält auch */sbin* wichtige Programme. Diese sind jedoch hauptsächlich für den Systemverwalter gedacht, da sie Funktionen erfüllen, auf die ein normaler Benutzer keinen Zugriff hat.
/tmp	Dieses Verzeichnis kann von jedem Benutzer und jedem Programm als temporäre Ablage für Dateien verwendet werden. Bei einigen Distributionen wird das /tmp-Verzeichnis bei einem Neustart automatisch gelöscht.
/usr	(unix system resources) Die umfangreichste Verzeichnisstruktur des Systems umfasst den größten Teil der installierten Software.

`/opt` (optional) Verzeichnis, in dem optionale Programme, die nicht dem Paketmanagement unterliegen, installiert werden können.

`/var` Unter diesem Verzeichnis werden hauptsächlich variable, sich ständig ändernde Dateien gespeichert. z. B. spool-Verzeichnisse der Drucker.