# Serverdienste:

Wichtig sind bei allen Serverdiensten die Dateien /etc/hosts.allow und /etc/hosts.deny in denen jeweils steht welche Dienste für wen erlaubt oder veweigert werden (zuerst wird allow ausgewertet dann deny)

z.B. in hosts.deny ALL:ALL … d.h. es wird grundsätzlich alles verboten und dann in der allow die Dienste einzeln einschalten z.B. smbd:ALL oder smbd:192.168..

Zusätzlich gelten Firewall-Regeln mit iptables womit man Zugriffe auf und von IP-Adressbereichen und Ports sehr detaillier einstellen kann.

## nfs:

Geht nur zwischen Linux Clients, sehr schnell (wesentlich performanter als samba), Rechtevergabe sehr eingeschränkt (geht nur über die USERID) und lässt sich auf IP Adressen beschränken -> deshalb nur in zentral verwalteten Umgebungen, wo der user nicht root ist (usermod nicht verwendbar) und der Admin auch die Netzwerkadressen vergibt.

eingestellt wird alles in /etc/exports (welche user (UID) bzw. welche Netzwerkbereiche dürfen zugreifen)

## ftp:

Unter Windows: im IIS (Programme - Windowsfeatures, Hackel setzen) – einfache Freigabemöglichkeiten

Unter Linux: am einfachsten vsftp (very simple ftp) oder ftppro – über ein einziges conf konfigurierbar (Gastzugriff, chain … in Unterordner gefangen halten)

Vorteil: sftp – sicherer Dienst, gutes, zuverlässiges Protokoll (im Gegensatz zu http)

## Samba:

(siehe auch Frage 5)

Täuscht Windows Freigaben vor (-> Bei Windows ist nichts zu tun außer Freigaben zu machen, Berechtigungen (jeder alles) und Sicherheit (konkret für Benutzer einschränken) setzen)

Unter Linux: sudo apt-get install samba-server und dann /etc/samba/smb.conf bearbeiten

Security = user … jeden Benutzer mit smbpasswd –a anlegen

= domain … holt sich Infos vom ActiveDirectory

So schaut der Eintrag in der /etc/samba/smb.conf für joomla Seiten aus, die in der Schule vom Benutzer schueler bearbeitet werden können (deshalb hat die Gruppe www-data auch Schreibrechte)

*[webprojects]* ...Section header line

*comment = Informatik Web Projekt Server*

*path = /var/www* ...Verzeichnis auf das Zugriff gewährt wird

*guest ok = no* ...Es wird ein Passwort benötigt

*available = yes* ...Service ist verfügbar

*browseable = yes* ...Share ersichtlich in Liste der verfügbaren Shares

*writeable = yes* ...Schreiben erlaubt (Gegenteil von read only)

*create mask = 0775* ...Bei Erstellen einer Datei hat user rwx (7), group rwx (7) und other rx Rechte (5)

*force create mode = 0775* ...Neue Dateien gezwungen rwx für user, rwx für group und rx für other zu haben

*force directory mode = 0775* ...Neue Ordner gezwungen rwx für user, rwx für group und rx für other zu haben

*directory mask = 0775* ...Wenn ein Ordner erstellt wird hat user rwx, group rwx und other rx

*force user = schueler* ...Nachdem eine Verbindung hergestellt wurde, werden alle Operationen als schueler durchgeführt

*force group = www-data* ...Alle user werden der group "www-data" zugeordnet

allgemein unter Linux Zugriffsrechte festlegen z.B. ALL:ALL oder smbd:ALL

hosts.allow und hosts.deny

**Clients:**

nfs:

ist in Linux bei der Standardinstallation dabei

Verwenden mit mount: entferntes Verzeichnis als lokales darstellen  
sudo mount Server:Freigabe lokalerPfad

oder mit scp (secure copy)

Samba:

mount -t cifs [//gandalf.htl-villach.at/Public](file:///\\gandalf.htl-villach.at\Public) /mnt/gandalfp -o user=nnnnnnnv

wobei /mnt/gandalfp bereits bestehen muss (also evtl. vorher mit mkdir erzeugen)

im Browser (conqueror) mit smb://

ftp oder besser sftp:

Clients sind überall von Haus aus dabei

ftp> get put dir ….

literal und umschalten zwischen activ und passiv mode

oder im Browser mit ftp://

oder ftp-Clients wie Filezilla

Gute sichere und schnelle Möglichkeit zum Kopieren zwischen Linux Rechnern ist scp (Secure Copy)

allerdings muss open-ssh installiert sein, weil der Transport über ssh erfolgt

Befehlssyntax ist

scp Quelle Ziel

oder noch genauer

scp username@server:/quellpfad/quelldatei username@zielserver:/zielpfad/