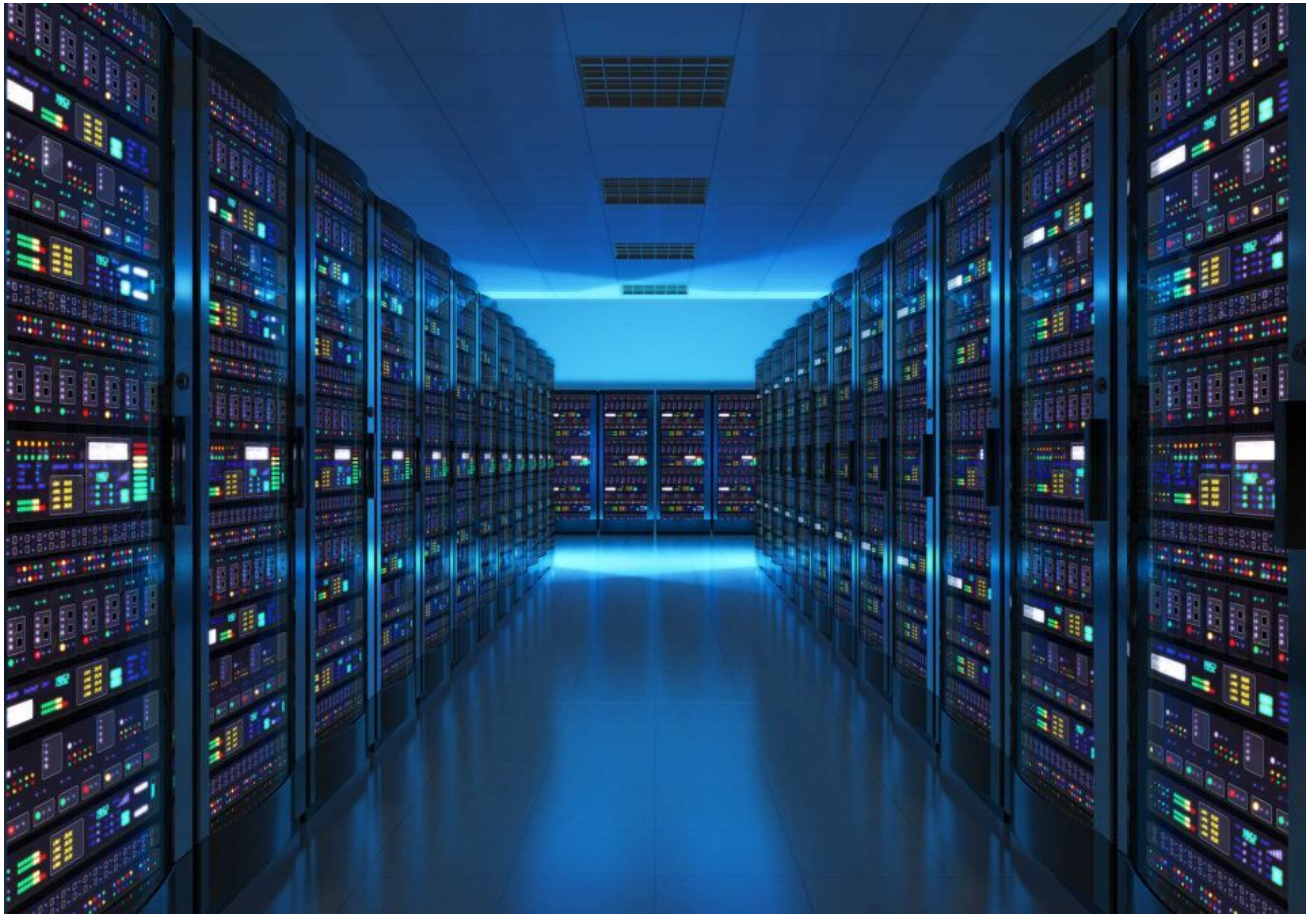
spline

Freie Universität Berlin

Serverarten & Serverdienste



spline

Freie Universität Berlin

SSH

Was ist SSH?:

- **SSH (Secure Shell)** - Netzwerkprotokoll und Programm
- Stellt eine verschlüsselte Netzwerkverbindung auf sichere Art und Weise mit einem entfernten Gerät
- Wird erwendet, um lokal auf eine entfernte Kommandozeile zuzugreifen
- Wird zum Beispiel zur Fernwartung eines entfernten Servers verwendet
- Benutzt TCP-Protokoll
- Standart-Port: 22

spline

Freie Universität Berlin

SSH

Wie benutzt man SSH?:

- Um eine SSH-Verbindug herzustellen muss auf dem Server/Rechner, zu dem man sich verbinden will, ein SSH-Server laufen
- **Syntax: *ssh <benutzername>@<domain>***
- Um den SSH-Server zu starten muss man das Paker **ssh** oder **openssh** installieren und den Service enablen:

  systemctl enable ssh

  systemctl start ssh
- Beispiel: ***ssh gordon@fob.spline.de***

spline

Freie Universität Berlin

SSH

Konfiguration von SSH:

- Bei einer Standartkonfiguration kann man nur als auf dem Server existierender Benutzer zugreifen
- Die Konfigurationsdatei liegt unter ***/etc/ssh/sshd_config***
- Bei vielen Server ist es sinnvoll sich sofort als ***root*** einzuloggen
- Da muss man die Zeile ***PermitRootLogin <parameter>*** auskommentieren
- Es ist gefährlich sich mit Passwort einzuloggen, vor allem wenn man sich als ***root*** einloggt. In diesem Falle kann man SSH-Keys benutzen

spline_

Freie Universität Berlin

SSH

SSH-Keys:

- Es ist sinnvoll ein Schlüsselpaar für SSH zu erstellen
- Syntax: ***ssh-keygen***
- Dies wird ein ***privaten*** und einen ***öffentlichen*** Schlüssel erstellen: Standard-Namen: ***id_rsa*** und ***id_rsa.pub***
- Option ***-t*** legt die Verschlüsselungmethode fest. Zum Beispiel ***rsa***
- Option ***-b*** legt die Bitlänge fest. Zum Beispiel ***4096***
- Option ***-C*** steht für Kommentar
- Beipsiel: ***ssh-keygen -t rsa -b 4096 -C "email@example.com"***

spline_

Freie Universität Berlin

SSH

Benutzen von SSH-Keys:

- Die Schlüssel werden im ***~/.ssh*** erstellt
- Um die Schlüsselauthentifizierung zu ermöglichen muss man den öffentlichen Schlüssel auf den Server hochladen
- Den Inhalt schreibt man in die Datei ***/root/.ssh/autorized_keys***
- In der Konfiguration Ist folgendes einzugeben oder auskommentieren und anpassen:
  PermitRootLogin without-password
  AuthorizedKeysFile .ssh/authorized_keys
  PubkeyAuthentication yes
  PasswordAuthentication no
- Dann kann man den SSH-Service neustarten und verbinden:
  ssh <benutzer>@<domain> -i <Pfad zu dem privaten Schlüssel>

spline_

Freie Universität Berlin

SSH

Konfiguration von SSH-Client:

- Die Konfiguration von dem Client iegt in ***~/.ssh***
- Was ziemlich sinnvoll ist – eine ***config*** Datei anzulegen
- Ermöglicht Parameter für einzelne Hosts vorzudefinieren
- Beispiel:
  Host <Name>
  HostName <Domain oder IP>
  User <Benutzer>
  Port <Port>
  IdentityFile <Pfad zu dem privaten Schlüssel>
  ProxyCommand ssh -W %h:22 <benutzer>@domain>

spline

Freie Universität Berlin

Apache

Apache-Server:

- ***Apache*** ist einer der populärsten Webserver
- Das Paket heißt ***apache2***
- Starten: ***systemctl enable apache2 && systemctl start apache2***
- Die Konfiguration liegt in ***/etc/apache2.conf***
- Die index.html liegt standartmäßig in ***/var/www/html/index.html***
- Standart-Port ist 80 (kann man in ***/etc/apache2/ports.conf*** ändern)
- Für https ist der Standart-Port 443 (braucht SSL-Zertifikat)