ssh für Windows - Linux - Kombinierer

auf den Forentagen in Mannheim September 2019

Thorsten Maxeiner - Maxeiner-computing

whoami

```
{
    {
        “Name” : “Thorsten Maxeiner”,
        “Job” : “Maxeiner-computing”,
        “Develop” :
        [
            “Delphi” : “V1 ...”,
            “Kylix” : “V1 ...”,
            “Python” : “V2.4 ...”
        ]
        “OS” :
        [
            “Windows” : “1992”,
            “Linux” : “2003”
        ]
    }
```

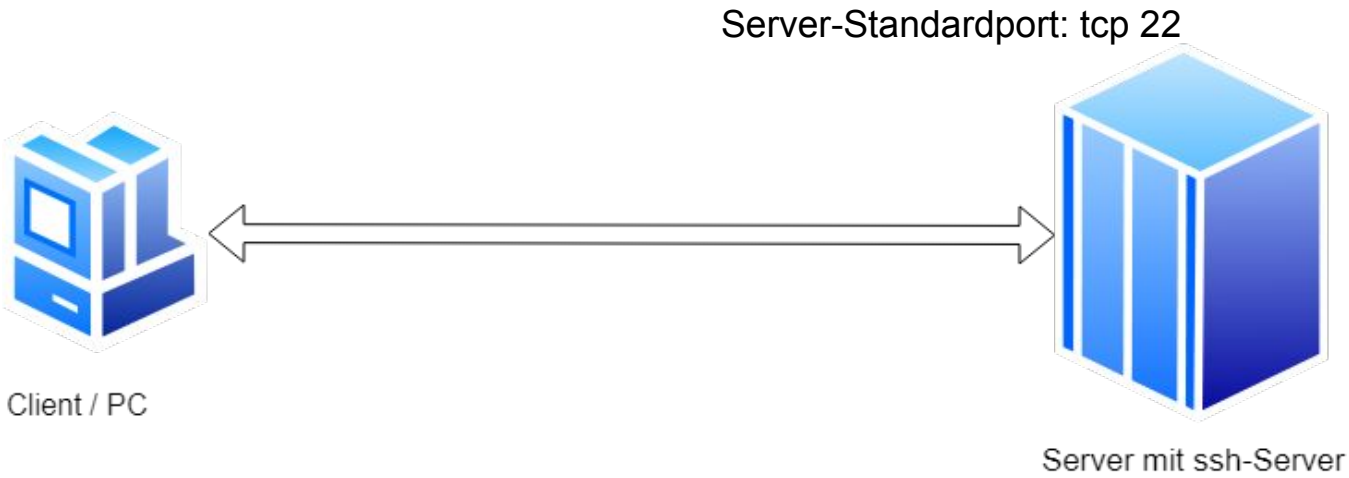
Was ist ssh / warum ssh

ssh = Protokoll zum gesicherten Zugriff auf Server, PCs, Embedded-Systeme,...

Verschlüsselung **Authentifizierung**

- Viele Betriebssysteme
- Geringe Bandbreite
- Nützliche Zusatzfunktionen

Aufbau



Demo

Clients

Putty : https://www.putty.org

Termius : https://termius.com

MobaXTerm : https://mobaxterm.mobatek.net

windows powershell mit openssh : in Windows 10 bereits drin

Anpassung in Serverconfig

Sicherheitsanpassungen am Server:

- Port 22 auf anderen Port legen

Diesen Schritt immer als als erstes machen!

Anpassung in Serverconfig

Port auf anderen Port legen:

sudo nano **/etc/ssh/sshd_config**

dort: Zeile **Port 22** ändern in z.B. **Port 12322**

Demo

Dateien im Ablauf einer Verbindung

Verzeichnis .ssh im Homedir :		Beinhaltet alles für die Clientverbindungen Linux: /home/<user>/.ssh/ Windows: c:\Users\<user>\.ssh\
known_host	:	Liste der bekannten Host-Kennungen
authorized_keys	:	Liste der öffentlichen Schlüssel
id_rsa	:	Standardname des eigenen privaten ssh-Keys
id_rsa.pub	:	eigener öffentlicher Schlüssel
config	:	Einstellungspakete für einzelne Hosts

Schlüssel

- Datei mit Zeichenfolge, erzeugt mit ssh-keygen oder puttygen
- Kann mit oder ohne Passwort erzeugt werden
- Vorteil: Quasi 2-Faktor-Authentifizierung
- Vorteil: bei Erzeugung ohne Passwortabfrage automatische Prozesse möglich
- Am Server kann Anmeldung ohne Schlüssel verboten werden

Einfach:
- ssh-keygen starten (Default: RSA 2048 bit)
- Dateiname eingeben
- 2x Enter drücken

Demo: Schlüssel erzeugen

Demo

Anwendung: Datenübertragung

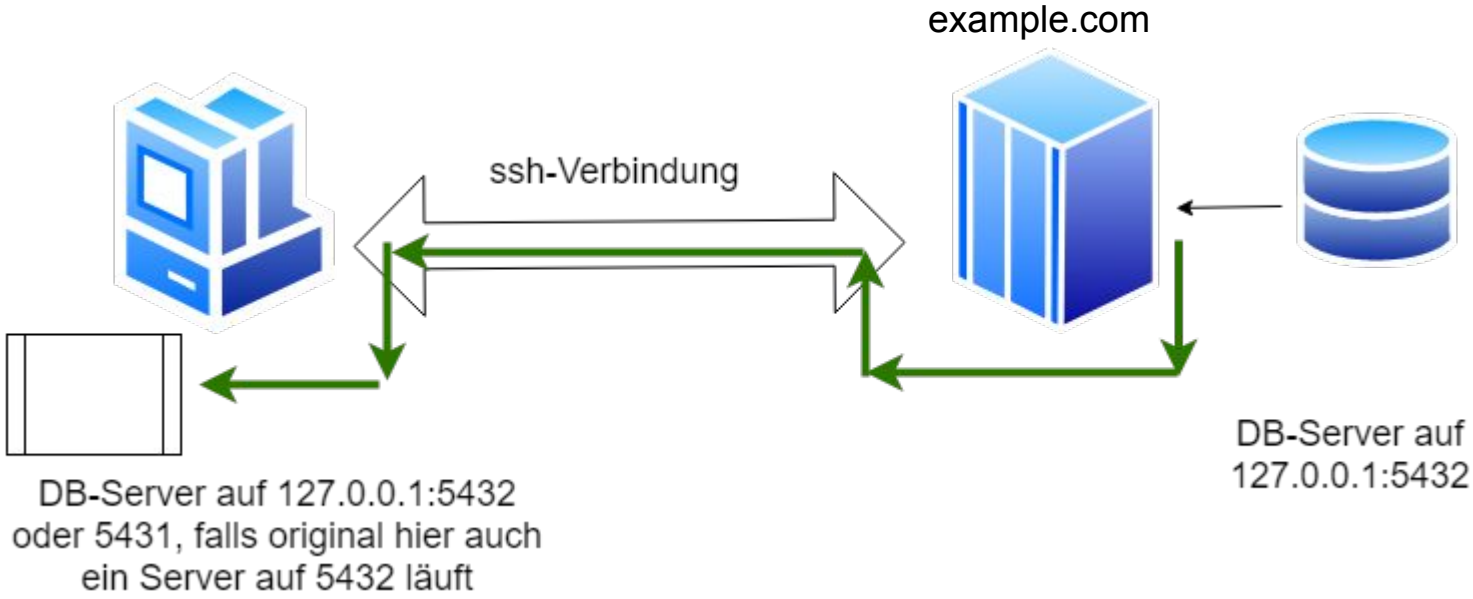
sftp über ssh

Quasi alle FTP-Programme können auch über ssh arbeiten

Vorteil: kein FTP-Server notwendig!

Demo mit WinSCP und Speedcommander

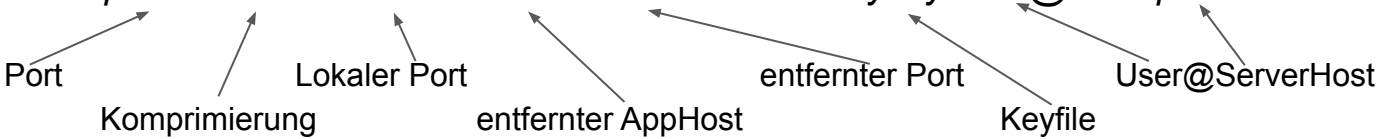
Anwendung: Tunnelbau



Auf der Konsole: einfacher intuitiver Befehl...

Anwendung: Tunnelbau

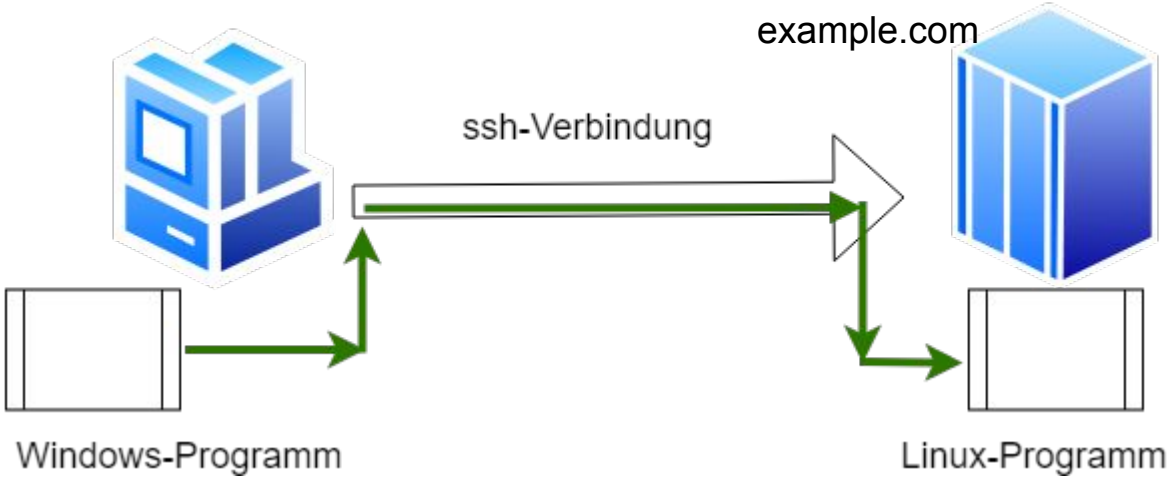
Kommando: *ssh -p 12322 -C -L 5431:127.0.0.1:5432 -i ~/.ssh/mykey user@example.com*



Demo

Anwendung: Befehlsausführung

Windows steuert einen Linux-Server fern



Anwendung: Befehlsausführung

Anwendungen:

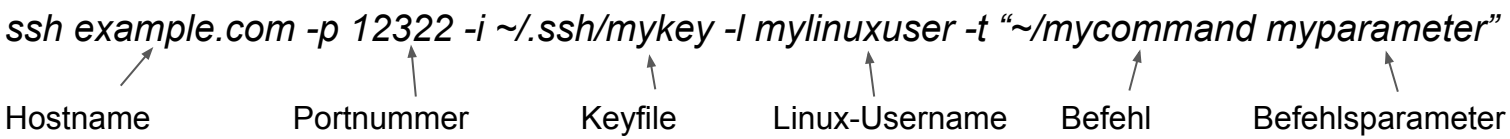
- Eventgesteuerte Backups
- Rechner-Shutdown
- Parameter für Configdateien schreiben
- …

Vorteile:

- Verschlüsselte Kommunikation ohne Aufwand
- Authentifizierung ohne Aufwand

Anwendung: Befehlsausführung

Ausführung auf Kommandozeile unter Windows oder Linux:



Nutzung Delphi-Like:

TSSHCommand: Wrapper für Windows-eigenes ssh als Record

https://github.com/tmaxeiner/TSSHCommand

Demo

Weitere Anwendungen (ohne Empfehlung!)

- VPN-Ersatz: über einen VPN-Eingang ins eigene Netz durch Tunnel auf Anwendungen zugreifen

- X1-Forwarding: Grafische Oberfläche eines Linux-Systems über einen X-Server auf einem Windows-PC nutzen

- Remote-Service: z.B. vom Client zum eigenen Server einen Tunnel für DB-Wartung, geht auch in eingeschränkten Firmen-Netzwerken, wenn eigener ssh-Server auf Port 80 liegt :-)

Hier gilt aber: nicht alles was geht muss man auch machen!!!

Ende :-)

Fragen?