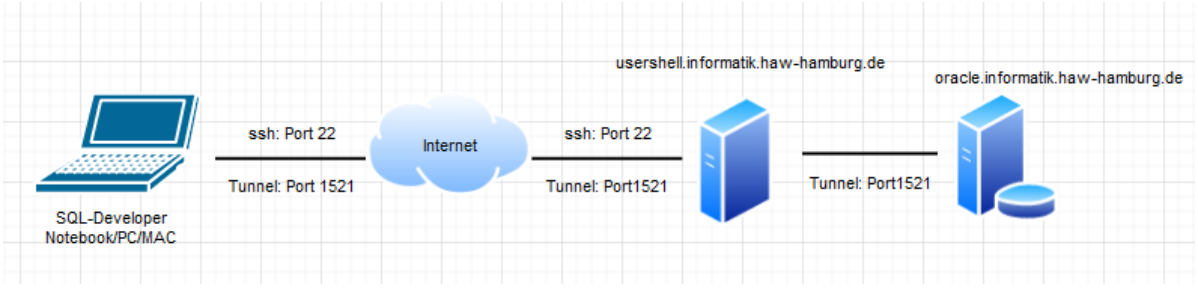
Zugriff auf die Datenbank außerhalb des HAW-Labornetzwerkes über einen SSH-Tunnel:

Der externe Zugriff auf die Oracle-DB kann nur mit einen ‚SSH-Tunnel' über den SSH-Server ‚usershell.informatik.haw-hamburg.de' erfolgen:



1. Einmalige Private-/Public-Key Einrichtung im Pool AI-Labor

Der Login auf usershell.informatik.haw-hamburg.de kann von außerhalb des AI-Labors nur über die sogenannte Private-/Public-Key Methode erfolgen. Für das Einrichten eines Private-/Public-Keys ist es notwendig, sich im Pool des AI-Labors einzuloggen und initial einen Private-/Public-Key zu installieren.

Für diese Einrichtung ist ein Pool-PC neu in den Linux-Mode zu booten. Dazu benötigen Sie einen Account in der Informatik, dieser Account beginnt immer mit ‚inf<W-Kennung>' (z.B. infwab101).
Sie haben die Möglichkeit die Einrichtung über die grafische Oberfläche (intuitiver) oder über den Linux-Konsolenmode durchzuführen. Diese Anleitung beschreibt den aufwendigeren Konsolenmode.
Wechseln Sie mit Ctrl-Alt-F2 in den Konsolenmode, über CTRL-Alt-F7 kommen Sie wieder zurück in den grafischen Mode.

Für die Generierung eines Private-/Public-Keypaars geben Sie in der Konsole oder einem einem Terminal folgendes ein:

Falls der Ordner .ssh noch nicht in Ihrem Homeordner existiert, diesen bitte anlegen mit:
Auflisten: ls -ld .ssh
Ordner anlegen: mkdir -p .ssh
Zugrifssrechte einschränken: chmod 700 .ssh
Verzeichnis wechseln: cd .ssh

Generierung eines Private-/Public-Keypaars : ssh-keygen -t rsa -b 4096
Enter file in which to save the key: oracleTunnelPPK
*Enter passphrase (empty for no passphrase): ********
*Enter same passphrase again: *******
Your identification has been saved in oracleTunnelPPK
Your public key has been saved in oracleTunnelPPK.pub

Public-Key bekanntgeben: cat oracleTunnelPPK.*pub* >> authorized_keys
Zugriffssrechte einschränken: chmod 600 authorized_keys

Im Konsolenmode müssen Sie im Gegensatz zum UI-Mode das Device vom USB-Stick herrausfinden: `lsblk`
USB-Stick mounten (z.B. sdc1): `udisksctl mount -b /dev/sdc1`
USB-Stick Verzeichnis angezeigen; `ls -l /media/<user>/stick`

verschieben Sie Ihren Private- und Public-Key auf den USB Stick und sichern Sie diesen anschliessend an einen Ort:
`mv oracleTunnelPPK /media/<user>/stick`
`mv oracleTunnelPPK.pub /media/<user>/stick`
USB-Sick wieder entfernen/lösen: `udisksctl unmount -b /dev/sdc1`

Die Installation des Public-Keys in Ihrem Home-Directory ist dann abgeschlossen.

Den Private-Key `oracleTunnelPPK` mit der dazu gehörenden Passphrase benötigen Sie, um im SQL-Developer einen Verbindungsaufbau mit Tunnel durchzuführen.

2. SSH-Verbindung mit Tunnel für Port 1521 für Oracle-DB einrichten:

Variante Tunnel mit ssh:

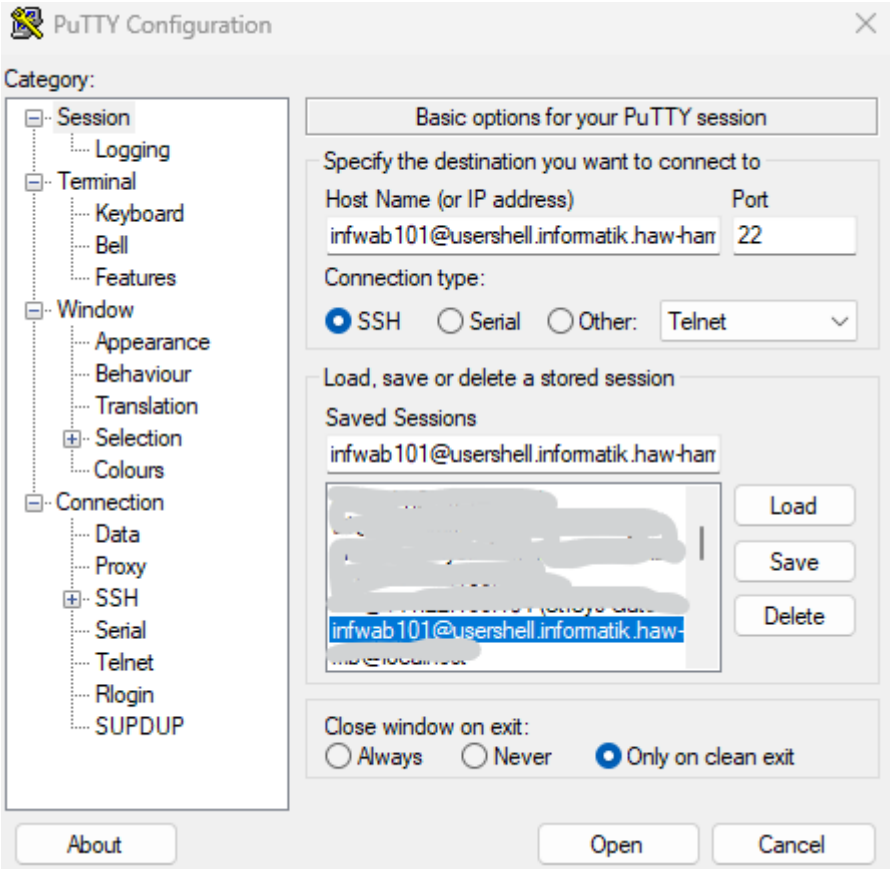
Agent starten: ssh-agent > ~/.ssh/my_agent_info
Agent-Daten laden: . ~/.ssh/my_agent_info
Private-Key in Agent laden: ssh-add ~/.ssh/oracleTunnelPPK
Tunnel starten: ssh -L 1521:oracle.informatik.haw-hamburg.de:1521 <infAccount>@usershell.informatik.haw-hamburg.de

Variante Tunnel mit Putty in der Command-Line:

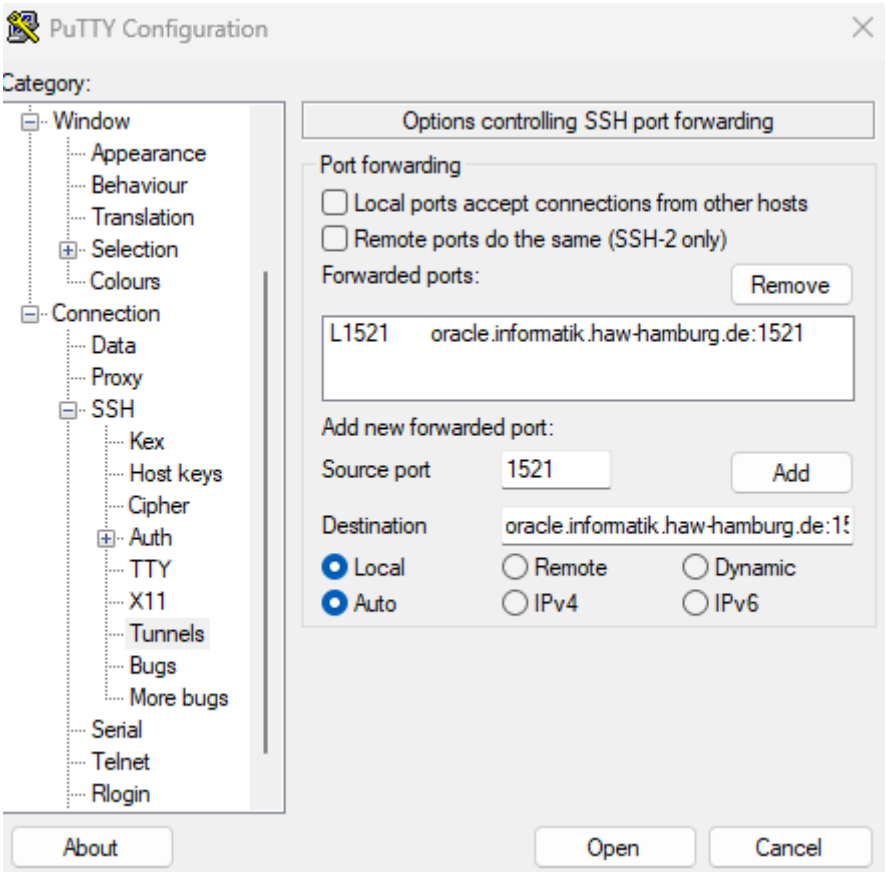
Pageant starten und Private-Key laden
Putty: putty.exe -L 1521:oracle.informatik.haw-hamburg.de:1521 -ssh <infAccount>@usershell.informatik.haw-hamburg.de

Variante Tunnel mit Putty im GUI Mode:

→ Host Name mit Username: inf<W-Kennung>@usershell.informatik.haw-hamburg.de



→ unter Connection → SSH → Tunnels:
Source Port: 1521
Destination: oracle.informatik.haw-hamburg.de:1521
→ mit Add den Tunnel hinzufügen



→ unter Session → Save diese Konfiguration speichern:
inf<W-Kennung>@usershell.informatik.haw-hamburg.de
→ mit Open die SSH-Verbindung mit dem Tunnel unter Eingabe der Passphrase starten

3. Der Java JDBC-Connect-String lautet dann:

```
"jdbc:oracle:thin:@localhost:1521/inf.informatik.haw-hamburg.de"
```