Linux videot: <https://www.youtube.com/playlist?list=PLZw_fXxI6L50ovlxunMvWw-bEDc3TiBQp>

Contents

[TLDR 1](#_Toc48907919)

[Asenna OpenSSH-server: 1](#_Toc48907920)

[SSH käynnistyminen palvelimen käynnistyksen yhteydessä 1](#_Toc48907921)

[Root käyttäjä ei saa kirjautua 1](#_Toc48907922)

[Tietyn käyttäjän/ryhmän salliminen 1](#_Toc48907923)

[Kirjautumisaika (Login grace time) / kisoissa joskus nimellä timeout 2](#_Toc48907924)

[Portin muuttaminen 2](#_Toc48907925)

[Banneri ennen kirjautumista 3](#_Toc48907926)

[Banneri kirjautumisen jälkeen (MOTD) 3](#_Toc48907927)

[Avainparilla kirjautuminen 4](#_Toc48907928)

[Konfiguraation testaaminen 5](#_Toc48907929)

[Uudelleenkäynnistys 5](#_Toc48907930)

# TLDR

1. Asenna openssh-server paketti
2. Määritä ssh käynnistymään koneen yhteydessä komennolla systemctl enable ssh
3. Tee haluamasi asetukset /etc/ssh/sshd\_config tiedostoon
4. Testaa konfiguraatio sshd -t komennolla
5. Käynnistä palvelu uudestaan
6. Testaa ssh yhteyden ja asetusten toiminta ottamalla ssh yhteys työasemasta palvelimeen

Etäyhteydet ovat tärkeitä, jotta palvelimia voidaan hallita. On myös tärkeää, että tietohallinto pystyy ottamaan etäyhteyden käyttäjien tietokoneisiin. Etäyhteys Linux palvelimiin hoidetaan tyypillisesti salatun SSH yhteyden kautta.

Asentamalla OpenSSH-server paketin Debianiin voidaan ottaa käyttöön SSH-yhteydet. Tässä ohjeessa on erilaisia konfigurointeja joita siihen voi tehdä ja joita on tullut vastaan Taitaja-kisoissa.

# Asenna OpenSSH-server:

**apt install openssh-server**

Suurin osa konfiguroinneista tehdään muokkaamalla **/etc/ssh/sshd\_config** tiedostoa jollain tekstieditorilla.

SSH-yhteys muodostetaan näin:

**ssh käyttäjänimi@palvelimenip**

esim:

**ssh Mikko@192.168.0.69**

# SSH käynnistyminen palvelimen käynnistyksen yhteydessä

Ilman alla olevaa komentoa openSSH ei käynnisty tietokoneen uudelleenkäynnistyksen yhteydessä. Muista siis käyttää sitä! Lähes kaikki muut palvelut menevät päälle kun tietokone käynnistyy, mutta openSSH tulee tehdä tämä erikseen.

**systemctl enable ssh**

Muista myös testata tämän toiminta! Käynnistä koko palvelin uudestaan ja testaa SSH yhteys työasemalta. Voit myös käyttää **systemctl status ssh** komentoa.

# Root käyttäjä ei saa kirjautua

**PermitRootLogin yes**

PermitRootLogin kohdassa voi joskus oletuksena lukea muutakin kuin yes.

Vaihda tähän:

**PermitRootLogin no**

# Tietyn käyttäjän/ryhmän salliminen

sshd\_config voidaan määritellä tietyt käyttäjät ja ryhmät jotka saavat ottaa palvelimeen ssh yhteyden.

**AllowUsers käyttäjänimi**

Esim:

**AllowUsers maija**

Käyttäjälle voidaan myös määritellä mistä IP-osoitteesta hän voi kirjautua

**AllowUsers käyttäjänimi@osoite**

Esim:

**AllowUsers maija@172.22.1.3**

Myös ryhmiä voidaan sallia.

**AllowGroups ryhmännimi**

Esim:

**AllowGroups sshusers**

# Kirjautumisaika (Login grace time) / kisoissa joskus nimellä timeout

/etc/ssh/sshd\_config löytyy kohta:

**#LoginGraceTime 2m**

Tämä tekisi kirjautumisajasta 2 minuuttia.

Muuta siihen:

**LoginGraceTime 10**

Asettaisi kirjautumisajaksi 10 sekuntia. Muista ottaa risuaita pois edestä!

Jos et ehdi kirjautua 10 sekunnin aikana ruutu jää ikään kuin jumiin ja jos painat enteriä tulee tälläinen:



# Portin muuttaminen

/etc/ssh/sshd\_config löytyy kohta:

**#port 22** eli se on kommentti.

Ota risuaita pois ja määritä mitä porttia haluat käyttää.

Esim:

**port 2222**

tai

**port 2000**

Kun olet vaihtanut portin ja haluat testata ssh yhteyttä sinun tulee muuttaa komentoa hiukan:

**ssh käyttäjänimi@iposoite –p portinnumero**

esim:

**ssh root@172.22.1.69 –p 2222**

Jos et lisää –p ja portin numero kohtaa yrittää ssh edelleen ottaa yhteyttä porttiin 22 koska oletus

Ota huomioon että jos muutat porttia ja tehtävässä vaaditaan palomuurin käyttämistä, joudut luultavasti tekemään myös palomuuriin (iptables) muutoksia.

# Banneri ennen kirjautumista

Jos haluat että banneri tulee ennen kirjautumista (login) tee näin.

**nano /etc/ssh/sshd\_config**

Muokkaa kohtaa:

**#Banner none**

Ja tee siitä:

**Banner /etc/banner**

Voit määritellä itse mistä polusta banneri haetaan mutta tässä esimerkissä on käytetty polkua /etc/banner

Seuraavaksi muokkaa /etc/banner tiedostoa haluamaksesi. Esim:

**nano /etc/banner**



Kun käyttäjä yrittää kirjautua tulee tämä teksti ennen kirjautumista:



# Banneri kirjautumisen jälkeen (MOTD)

Kun käyttäjä kirjautuu sshn kautta palvelimelle hän saa tervetuloa viestin:



Tätä voidaan muuttaa seuraavasti /etc/ssh/sshd\_config :

**PrintMotd no**

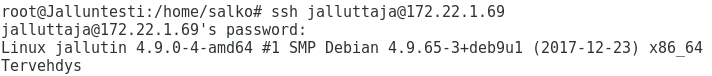
Muuta tähän

**PrintMotd yes**

Seuraavaksi muokkaa tiedostoa /etc/motd

**nano /etc/motd**

ja lisää siihen viestisi esim: Tervehdys.



# Avainparilla kirjautuminen

Alkuun varmista että palvelimen /etc/ssh/sshd\_config tiedostossa on sallittu rootin kirjautuminen:

**PermitRootLogin yes**

Jos tässä kohdassa lukee no, emme voi kopioida avainparia palvelimelle.

Seuraavaksi kirjaudu linux työasemalla ja luo avainpari.

**ssh-keygen –t rsa**

Tämä luo avaimen ja näyttää suurinpiirtein tältä:



Passphrasea emme tarvitse joten voit painaa vain Enteriä jokaisessa kohdassa.

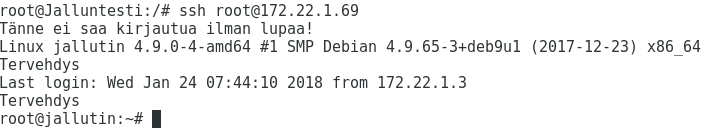
Seuraavaksi avain tulee kopioida palvelimelle.

**ssh-copy-id käyttäjä@sshpalvelin**

Esim:

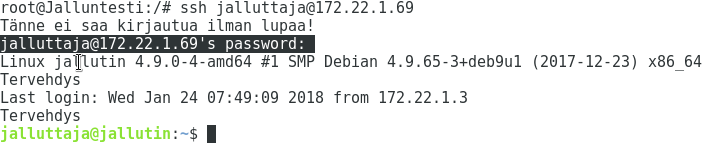
**ssh-copy-id root@172.22.1.69**

Tämä loisi rootille avainparin palvelimelle 172.22.1.69. Kun tämä käyttäjä kirjautuu palvelimelle ssh yhteyden kautta ei häneltä kysytä salasanaa. Kirjautuminen näyttää siis tältä:



Jos tämä ei toimi, varmista että /etc/ssh/sshd\_config **PermitRootLogin yes** on asetettu.

Jos taas joku muu käyttäjä kirjautuu häneltä kysytään edelleen salasanaa:



# Konfiguraation testaaminen

Alla olevalla komennolla saat testattua konfiguraation. Jos siinä on virheitä niistä ilmoitetaan.

**sshd -t**

# Uudelleenkäynnistys

Kun olet tehnyt kaikki muutokset käynnistä ssh uudestaan.

**systemctl restart ssh**

Onko kaikki kunnossa näet:

**systemctl status ssh**