

## Yleinen ohjeistus Taitaja-tehtävään

### Yleiset ohjeet:

- Jollei muuten ohjeisteta, käytä aina salasananä "Qwerty7". Tämä salasana on myös käyttäjän salasana valmiiksi asennetuissa palvelimissa, ellei muuta mainita.
- Palvelimien nimet tulee olla määritettynä tehtävän mukaisesti.
- Linux palvelimet asennetaan oletuksena ilman graafista tilaa ja Windows graafisella ellei toisin mainita.
- Asennettävien palveluiden ja palvelimien kielenä tulee olla englanti, ellei toisin mainita. Tämä voi vaikuttaa pisteytykseen.
- Jos tehtävässä ei sanota tarkkaan miten pitää toteuttaa, toteuta haluamallasi tavalla siten että se vastaa tehtävässä annettuja ohjeita. Toiminallisuutta testataan.
- Korvaa tehtävässä löytyvät "X" – kirjaimet kilpailijanumerollasi.

Esim. <http://taitajaX.local> => <http://taitaja9.local>

Hyödynnä edellisenpäivän tehtävässä rakennettua verkkoa. DNS palvelimena toimii edellisenpäivänä konfiguroidut DNS palvelimet. VMWare palvelimella on viimeinen IP-osoite palvelinsalin verkosta. Käyttäjätunnus on root.

**HUOM! Lue tehtävä läpi kokonaisuudessaan ennen kuin aloitat sen tekemisen. Muistinpanojen tekeminen tehtäväpaperiin on sallittua. Palvelimet tullaan uudelleenkäynnistämään tehtävän päätteeksi joten varmista että kaikki toimivat myös silloin.**

Firma OY:ssä on siirrytty fyysisistä palvelimista pilvipalvelimiin. Siirto on vielä pahasti kesken ja sinut on kutsuttu lisätueksi että saadaan kaikki firman namiskat pilvipalveluun. Pilvipalvelu on toteutettu VMware ohjelmalla ja IT-infrasta olitkin saanut jo työkoneen jossa valmiiksi asennettu tai sitten C:n juureen tuotu vaaditut ohjelmat joita ei ehditty vielä asentamaan. Toimitusjohtaja ja IT-asiantuntija ovat valmiiksi suunnitelleet siirron ja miten palvelimet konfiguroidaan pilvipalvelussa.

## LNX1

Sinulle on asennettu valmiiksi Debian 8.3 käyttöjärjestelmällä varustettu webpalvelimeksi.

Sinulle on annettu seuraavat määrittymiset konfiguroitavaksi:

Palvelinkonfiguraatiota

- Käytä DNS:nä DC1 ja DC2 palvelimia.
- Konfiguroi aikavyöhyke suomen aikaan.

Apache2:

- WWW-sivun hakemisto tulee olla /opt/www/ alla.
- Hakemiston omistajana tulee olla Apachen käyttäjä ja ryhmä. Tällä käyttäjällä ja ryhmällä tulee olla kaikki oikeudet tähän hakemistoon, muilla vain lukuoikeus.
- Varmuuskopioi kerran tunnissa www hakemiston sisältö /opt/backup hakemiston alle ZIPinä, jonka nimi on vuosi/kuukausi/päivä-tunti.zip.
- Luo hakemistoon verkkosivu jossa lukee "Taitaja 2016"
- Ota käyttöön SSL tälle sivulle. Luo tätä varten sertifikaatti joka on validi domain nimen kanssa, firma.com. Asenna sertifikaatti työasemalle ja testaa ettei tule varoituksia kun yhdistät sivulle suojattuna sivulle, <https://firma.com>. Konfiguroi automaattinen uudelleenohjaus https sivulle. TIPS: easyrsa.
- Luo virtuaalipalvelin intra.firma.com jonne pääsy on sallittua vain Firma Oy:n julkisesta osoitteesta.

MySQL

- Asenna MySQL
- Konfiguroi MySQL root salasanaksi Qwerty7
- Luo tietokanta Taitaja

Palomuuuri

- Salli palomuurista portit 80 ja 443.
- Estä SMTP portti sisälle päin
- Estä SSH portti sisälle päin, salli Firma Oy:n verkosta palvelimelle
- Salli ICMP protokola
- Varmista että palomuuuri toimii uudelleenkäynnistyksen jälkeen edellä mainittujen asetusten mukaisesti.

SMTP

- Konfiguroi sähköpostipalvelu lähettämään postit tuomariverkon palvelimelle.

SSH

- Salli root käyttäjän kirjautuminen avainparilla. Luo avainparit ja asenna tämä Puttyyn Windows 8.1 työasemalle.
- Konfiguroi SFTP rootiksi /opt/
- Salli "sftpuser" käyttäjän yhdistämisen tälle hakemistolle ja lukemaan / kirjoittamaan.
- Määritä /opt/www hakemistoon luku ja suoritusoikeudet kaikille, omistajalle kaikki ja ryhmälle suoritus, luku ja kirjoitusoikeudet.

#### Käyttäjät

- Luo käyttäjä "pomo" ja lisää käyttäjä "sudo" ryhmään.
- Luo käyttäjä "sftpuser" ja lisää "sftpushers" sekä "www-data" ryhmään. Älä salli sftp käyttäjän kirjautumisen muulla kuin sftp:llä. Käyttäjän ei tulisi päästä kirjautumaan terminaalista. Käyttäjä on verkkosivujen päivittämistä varten.

## Monitorointi

Konfiguroi monitorointi Firma Oy:n reitittimeen seuraavanlaiseksi:

- Konfiguroi Mikrotik tarkistamaan että palvelimet vastaavat pingiin 5min välein. Jos tila vaihtuu (ping vastaa ja ei vastaa eli laite on pudonnut verkosta) lähettää sähköpostia tuomariverkon postipalvelimelle (100.100.100.100). Lähetysosoite pitää olla mikko@firma.com
- Näet sähköpostin webmailissa <http://100.100.100.100>. Käyttäjätunnuksen ja salasana on annettu erillisenä paperilla.

## Dokumentaatio

Tee dokumentaatio jossa käy selväksi:

- IP-osoitteet
- Verkkokuvassa kaikki verkkolaitteet ja niiden kytkennät
- Tärkeimmät palvelut (kuten Active Directory Domain Services)
- Käyttäjätunnuksat ja salasanat