Installation

Install ubuntu

In VMBox: netwerkadapter 1 – host-only (ubuntu krijgt een ip adres 192.168.56.101)

PC krijgt 192.168.56.1 op host-only netwerk

Netwerkadapter 2 – bridged, voor internet connectie

Op windows: firewall voor host-only netwerk uitschakelen

Users

Useradd -m admin (admin user aanmaken met home directory)

Passwd admin (password instellen)

Usermod -aG sudo admin (admin user toevoegen aan de sudo groep)

SSH

Sudo apt-get install openssh-server (installeer ssh server)

Sudo service ssh status (status ssh controleren)

On client

Mkdir ~/.ssh (maak een map aan voor rsa keys)

Chmod 700 ~/.ssh (rechten van de map aanpassen: eigenaar kan read, write en execute doen)

Ssh-keygen -t rsa -b 4096 (key genereren. Deze is default 2048 bits lang, 4096 bits is veel veiliger)

ssh-copy-id [admin@192.168.56.101](mailto:admin@192.168.56.101) (kopieer public key naar de server)

On server

Sudo nano /etc/ssh/sshd\_config (ssh config bestand openen)

#PasswordAuthentication yes -> PasswordAuthentication no

Sudo service ssh restart (ssh server restarten)

With public key authentication, the authenticating entity has a public key and a private key. Each key is a large number with special mathematical properties. The private key is kept on the computer you log in from, while the public key is stored on the **.ssh/authorized\_keys** file on all the computers you want to log in to. When you log in to a computer, the SSH server uses the public key to "lock" messages in a way that can only be "unlocked" by your private key - this means that even the most resourceful attacker can't snoop on, or interfere with, your session. As an extra security measure, most SSH programs store the private key in a passphrase-protected format, so that if your computer is stolen or broken in to, you should have enough time to disable your old public key before they break the passphrase and start using your key

Different SSH programs generate public keys in different ways, but they all generate public keys in a similar format:

<ssh-rsa or ssh-dss> <really long string of nonsense> <username>@<host>

RSA is the only recommended choice for new keys, so this guide uses "RSA key" and "SSH key" interchangeably.

Key-based authentication uses two keys, one "public" key that anyone is allowed to see, and another "private" key that only the owner is allowed to see. To securely communicate using key-based authentication, one needs to create a key pair, securely store the private key on the computer one wants to log in from, and store the public key on the computer one wants to log in to.

Password authentication

The main problem with public key authentication is that you need a secure way of getting the public key onto a computer before you can log in with it. If you will only ever use an SSH key to log in to your own computer from a few other computers (such as logging in to your PC from your laptop), you should copy your SSH keys over on a memory stick, and [disable password authentication](https://help.ubuntu.com/community/SSH/OpenSSH/Configuring#disable-password-authentication) altogether. If you would like to log in from other computers from time to time (such as a friend's PC), make sure you have a [strong password](https://help.ubuntu.com/community/StrongPasswords).

WebServer

Prepare for MEAN stack

Sudo apt-get install git (git installeren)

Apt-get install mongodb (installeer MongoDB)

Apt-get install nodejs npm (installeer node en npm)

Npm install -g gulp bower (installeer globaal gulp en bower)

Npm install -g mean-cli (MEAN cli installeren)

Mean init webapp (MEAN app maken)

Apt-get install nginx (nginx webserver downloaden)

Nginx installeren

Map aanmaken in /var/www/labo1

/ect/nginx/sites-available/default aanpassen:

root /var/www/labo1;

Git repo pullen voor updates