Serviços - Aula 1.1 - Ubuntu setup

Entrar na máquina (primeira vez) —
Selecionar lenode criado copiar comando de "SSH Access"
ssh <user>@<ip>

Update software —
`apt-get update && apt-get upgrade`
A primeira coisa a fazer com uma nova máquina

Set hostname —
`hostnamectl set-hostname django-server`
hostname para verificar que o hostname foi alterado

Adicionar host ao ficheiro hosts — nano etc/hosts
`adicionar linha <ip> <hostname atribuido>`
Será revelado mais tarde o propósito.

Adicionar utilizador limitado —
`adduser stefanp-admin`
Boa prática pois o utilizador root pode fazer o que quiser com a máquina. Ao utilizar uma rede pública um hacker poder obter as credenciais da vossa máquina e destruir todo o nosso trabalho. Usar Nord VPN. Passar password

Adicionar utilizador grupo dos superusers —
`adduser stefanp-admin sudo`
Necessários para que o novo utilizador possa executar comandos como superuser e para evitar que se façam estragos na máquina.

Entrar na máquina (com utilizador limitado) —
Selecionar lenode criado copiar comando de "SSH Access"
ssh stefanp-admin@<ip>

Porquê fazer isto tudo? Instalação mais perto do mundo real, necessário tomar precauções: ativar autenticação por chave ssh, firewall.

Fazer autenticação por chave estrangeira —
`mkdir -p ~/.ssh`
Mais seguro e conveniente. A partir de uma palavra chave dada é gerado um hash, a partir do qual não é possível em tempo útil obter a password usando uma abordagem de força bruta. Não é necessário por a password

cada vez que se faz login na máquina. Ótimo quando se pretende correr scripts remotos comunicando com o servidor.
`ls -la`
Verificar se diretoria foi criada.

Criar chave ssh na máquina cliente —
`ssh-keygen -b 4096`

Enviar chave pública para o servidor —
`scp ~/.ssh/id_rsa.pub stefanp-admin@176.58.105.101:~/.ssh/authorized_keys`

`scp <ficheiro> <user>@<ip>:<localização do destino>`

Definir permissões no ficheiro da chave pública —
```
chmod <owner><group><everyone> <nome do ficheiro da chave pública>
chmod 700 ~/.ssh/
chmod 600 ~/.ssh/*
```

```
rwx
421

7 = 4 + 2 + 1 = read, write and execute
6 = 4 + 2 = read and write
5 = 4 + 1 = read and execute
```

Necessário de forma a garantir que apenas o utilizador pode alterar a chave ssh, e apenas esse utilizador possa usar a chave para se autenticar.

Desabilitar autenticação com root e autenticação com password —
`sudo nano /etc/ssh/sshd_config`

```
==================sshd_config====================
PermitRootLogin no
PasswordAutehtication no
```

Aplicar alterações no sshd_config
`sudo service sshd restart`

Ativar firewall —
- Instalar ufw (uncomplicated firewall)

`sudo apt install ufw`
- Permitir ligações de saída

`sudo ufw default allow outgoing`

- Negar ligações de entrada

```
sudo ufw default deny incoming
```

- Cuidado em fazer próximos comandos caso contrário fica-se fechado fora da máquina
- Permitir ligações ssh

```
sudo ufw allow ssh
```

- Permitir ligações ao porto 8000 onde o servidor de desenvolvimento corre.

```
sudo ufw allow 8000
```

- Ativar firewall

```
sudo ufw enable
```

- Ver regras do ufw

```
sudo ufw status
```

Porta 22 é a ssh