Ubuntu server first steps

Client: Generate keys

This command generate a two files with private and public keys. The public-key file will end with `.pub` extention, a private key file has no extention

```
ssh-keygen
```

Public key you may share with everyone, but private key must be keep in secret.

Client: Share key (publish)

You need to share you public key with target machine (server).

Best way for Ubuntu is add public key to github ssh keys, then it will be avaidable at `github.com/<username>.keys`

Server: Install Ubuntu-server

Becouse you install a server version, the common way to interact is remote control (.ssh), but you need to create base authorization method via physical terminal. The public key made for this purpose, but type public key by hands is takes too long, so we were publish our public key with entire ethernet at `github.com/<username>.keys`

While install, select **import identity** and enter GitHub user name. Ubuntu will automaticaly read public key and save it.

It's strongly recommended use only ssh-keys and disable password authentification.

Connect

For connect from client use this command to connect:

```
ssh -i ~/.ssh/some_server_name username@my.domain.com -p 22
```

where `-i` is identity path (private key path), where `~` - is home client user directory.

where `-p` is target port (default: 22)

where `username` - remote username (you enter while install)

where `my.domain.com` - ip of target machine or domain name

First connection from clinet to server must be as created user (not root).

If connection sucseeded and keys are valid, system ask you to add connection to `known_hosts`, type yes.

> In case of server system reinstall old clients may see message, thats says that identity is changed. This problem rised becouse server keys stored on clinet machine is old. For fix this, in Windows, go to `userfolder/.ssh` and edit `known_hosts` . Delete lines associated with server. And try to connect again.

Root login

After install public key will be stored in `~/.ssh/authorized_keys`

where `~` is user directory: `/home/username`.

For activate root, type this and enter password.

```
sudo su
```

Now you are login as root user and can go to `/root/.ssh`, this folder is already has authorized_keys file, but file is empty. This means that nobody can use ssh for login as root. For fix this you need to copy public key from user authorized_keys to root authorized_keys.

You may use this: (*cat* is print file content, >> is redirect output to new file line).

```
cat /home/<username>/.ssh/authorized_keys >> /root/.ssh/authorized_keys
```

Now you can connet via ssh as root.

Setup after install and connect

Extend disk space

This step may be already done while install, but if not do this:

```
vgdisplay
lvextend -l +100%FREE /dev/mapper/ubuntu--vg-ubuntu--lv
resize2fs /dev/mapper/ubuntu--vg-ubuntu--lv
df -h
```

For laptops:

Disable machine sleep if laptop lid is closed and `reboot` for apply changes:

```
sudo sh -c 'echo "HandleLidSwitch=lock" >> /etc/systemd/logind.conf' && reboot
```

Change hostname

Check information about host:

```
hostnamectl
```

Change hostname:

```
sudo hostname new_hostname
```

Create users

```
useradd -m -s /bin/bash username
```

Cut maximum journal disk size

```
sudo journalctl --vacuum-size=100M
```

Nvidia

```
sudo apt-get purge nvidia-headless-no-dkms-535-server # Or your version
sudo apt-get install nvidia-driver-535 # Or your version
sudo reboot
nvidia-smi # Validate
```

Revision #10
Created 21 January 2024 13:56:48 by annndruha
Updated 12 December 2024 18:18:22 by annndruha