

SSH key Generation on Ubuntu

Secure Shell (SSH) is a network protocol for creating a secure connection between a client and a server. With SSH, you can run commands on remote machines, create tunnels, forward ports, and more.

Creating SSH keys on Ubuntu

The chances are that you already have an SSH key pair on your Ubuntu client machine. The old one will be overwritten if you generate a new key pair. To check whether the key files exist, run the following `ls` command:

```
ls -l ~/.ssh/id_*.pub
```

If the command returns something like `No such file or directory`, or `no matches found`, the user does not have SSH keys, and you can proceed with the next step and generate an SSH key pair.

To generate a new 4096 bits SSH key pair with your email address as a comment, run:

```
ssh-keygen -t rsa -b 4096 -C "your_email@domain.com"
```

this will ask passphrase key, leave it and press enter, and press again until the whole interaction looks like this:

Open image-20220530-090236.png

To verify your new SSH key pair is generated, type:

```
ls ~/.ssh/id_*
```

```
/home/yourusername/.ssh/id_rsa /home/yourusername/.ssh/id_rsa.pub
```

That's it. You've successfully generated an SSH key pair on your Ubuntu client machine.

now follow the following steps:

```
cd ~/.ssh
```

```
cat id_rsa.pub
```

you will get your pub key in your terminal. Just copy the pub_key and save it into a text file

now it's time to get your hash key. write the following command in your terminal:

```
sudo cat /etc/shadow
```

Each line of the /etc/shadow file contains nine comma-separated fields:

```
[--]: [----]: [---]: - [---]: ----
```

```
|      |      |  |  |  |||+-----> 9. Unused
```

```
|      |      |  |  |  ||+-----> 8. Expiration date
```

```
|      |      |  |  |  |+-----> 7. Inactivity period
```

```
|      |      |  |  |  +-----> 6. Warning period
```

```
|      |      |  |  +-----> 5. Maximum password  
age
```

```
|      |      |  +-----> 4. Minimum password  
age
```

```
|      |      +-----> 3. Last password  
change
```

```
|      +-----> 2. Encrypted Password
```

+-----> 1. Username

Best Wishes.