

## Problem Statement:

Create an automation to enable SSH based remote access on 5 different Ubuntu 18.04 servers for a user. Once the automation is run, it should expect username as a command line argument and enable the access for that username. Make necessary assumptions on your own

Now there are two parts of the problem. Let's break it one by one.

### Enabling SSH :-

“SSH is typically used to log into a remote machine and execute commands, but it also supports tunneling, forwarding TCP ports and X11 connections; it can transfer files using the associated SSH file transfer (SFTP) or secure copy (SCP) protocols. SSH uses the client-server model “. Thus in simple words, one could talk to another system, while working on one system, via SSH.

We want SSH to be enabled automatically while we start the system. This can be done in multiple ways. Some ways re :

- In the linux command line window, go to the cron tab.  
`sudo nano crontab` or `crontab -e`.  
in that, write the command to start the ssh and save it.  
`@ systemctl start sshd.service`
- Create an RSA Authentication. “RSA (Rivest–Shamir–Adleman) is one of the first public-key cryptosystems and is widely used for secure data transmission”. (Recommended)
- Write a simple script to enable SSH. Save the script in the systemd folder, so that it runs with top priority when the system starts.

### Enabling the Access :-

- If you chose the second option to enable the SSH, then add the contents of the public key file into `~/.ssh/authorized_keys` on the remote site (the file should be mode 600).  
If you are a developer and you want to access debian.org systems with such a key, it's possible to have the developer database propagate your key to all of the debian.org machines.

OpenSSH offers RSA and DSA authentication to remote systems without supplying a password. “keychain” is a special bash script designed to make key-based authentication incredibly convenient and flexible.

To install keychain in Ubuntu/Debian :

```
$ sudo apt-get update
```

```
$ sudo apt-get install keychain
```

Thus granting the user access without a password can be done by private – public key techniques. RSA and DSA are such examples. One could also create a web page for this as well. it asks for login, then allows logged in user to upload the public key. On submit, the key is uploaded from the frontend to backend. Backend code has access to the servers. Backend uploads the public key to servers, and signals the frontend.

References :

<https://www.debian.org/>

<https://www.ibm.com/support/knowledgecenter/>

<https://www.cyberciti.biz/faq/>