Contents

[**SSH: Secure Shell** 1](#_Toc495445185)

[ Syntax 1](#_Toc495445186)

[ To check remotely login user 1](#_Toc495445187)

[ What if public key is changed? 1](#_Toc495445188)

[**SSH Passwordless Login/SSH key based login** 2](#_Toc495445189)

[ How passwordless authentication works? 2](#_Toc495445190)

[ **Steps to configure passwordless login (On client machine)** 2](#_Toc495445191)

[ **Key and their permissions** 2](#_Toc495445192)

[ **Different files**: 3](#_Toc495445193)

[**Notes** 3](#_Toc495445194)

[**Special cases (make changes at server machine)** 3](#_Toc495445195)

[ Disable root login 3](#_Toc495445196)

[ Only key based authentication/no password permitted 3](#_Toc495445197)

# 

# **SSH: Secure Shell**

* ssh protocol is used to remotely login to other machines.
* It uses port no: 22
* Suppose server machine: vaibhav

Client machine: vclient1

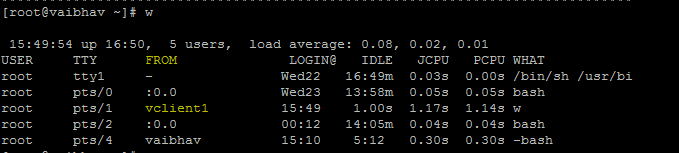
* Here, client machine tries to connect server machine so ssh command is run on client machine.
* Syntax: ssh username@hostname/IP

Here, username is optional. If no username is specified, the user invoking ssh is used.

For an example, if invoking user is root then it will remotely login to root user if no username is specified.

* To check remotely login user,

Command: w **OR** w -f



Here, how ssh works,

* When client attempts to connect to server through ssh, it uses public key.
* Before remote login, server sends copy of public key to the client and this public key is stored at client machine under ~/.ssh/known\_hosts.
* Every time, client connects to server, it gets same public key from server. Here, client verifies public key sent by client with key under ~/.ssh/known\_hosts.
* Prompt will be appeared for password of remote server and If key matches then connection is established.

### What if public key is changed?

* Due to some reasons like hardware failure, server rebuild, etc, public key is changed. In such a case, connection is not established.
* To solve that, clear contents of known\_hosts file and attempts to login through ssh again, server will send modified copy of public key.
* Steps: @ client machine

vi ~/.ssh/known\_hosts

Press dd

:wq

* Also host keys are stored @ server under /etc/ssh/\*key\*

**SSH Passwordless Login/SSH key based login**:

* When client machine wants to connect to the server machine via ssh, password must be entered each time. To avoid entering password at each login time, passwordless authentication is used.

### How passwordless authentication works?

* Here, SSH key pairs are used. This pair consists of private key and public key.
* Private Key can be protected by passphrase and kept at client machine only.
* Public key is copied to server machine. Public key does not need to be secret.
* Here, keys are such that public key can issue a challenge that can only be answered by private key only.

### **Steps to configure passwordless login (On client machine)**

* To generate RSA (algorithm to generate keys) key,

Command: ssh-keygen -t rsa

Here, ssh-keygen is used to generate key par, -t indicates type of key. Here, rsa key pair will be generated here.

* Keys will be stored under ssh folder of current user’s home directory.

Public Key: .ssh/ id\_rsa.pub

Private Key: .ssh/id\_rsa

* To copy public key to server machine,

Command: ssh-copy-id <filename> <username>@<Server’s hostname/IP>

Example: ssh-copy-id -i ~/.ssh/id.rsa.pub root@vaibhav

Here, ssh-copy-d command sends public key by default.

So, ssh-copy-id root@vaibhav also works.

* To access through passwordless,

Command: ssh username@<IP/hostname>

Example: ssh root@192.168.5.2 **OR** ssh root@vaibhav

* **Key and their permissions**:

|  |  |  |  |
| --- | --- | --- | --- |
| Key/files | location | files | Permissions |
| Private key | at client machine only | ~/.ssh/id\_rsa | 600 |
| Public key | at both client machine and server machine | ~/.ssh/id\_rsa.pub | 644 |
| at server machine only  in place of public key id\_rsa.pub | .ssh/ authorized\_keys | 600 |
| .ssh directory | at both client machine and server machine | ~/.ssh | 700 |

### **Different files**:

|  |  |
| --- | --- |
| /etc/ssh/sshd\_config | ssh configuration file |
| ~/.ssh/known\_hosts | at client machine It contains fingerprint of host It is not either public or private key |
| ~/.ssh/authorized\_keys | holds list of authorized public keys for servers |
| ~/.ssh/id\_rsa.pub | public key of single host/server machine |

**Notes**:

* ssh configuration file: /etc/ssh/sshd\_config
* Start/stop/restart ssh service,

service sshd start/stop/restart/status

chkconfig sshd on/off

* For every user, key pair is different.

For an example, if pair is generated for root user passwordless login, same pair cannot work for other user like testuser.

For other user like testuser, another key pair must be generated.

**Special cases (make changes at server machine)**:

* Disable root login,

At server machine,

vi /etc/ssh/sshd\_config

PermitRootLogin no

* Only key based authentication/no password permitted,

vi /etc/ssh/sshd\_config

PasswordAuthentication no