SSH [SECURE SHELL]

* Main configuration file = **/etc/ssh/sshd\_config**.
* Port **= 22**.
* Daemon = **sshd**.
* To connect using ssh, you have to generate pub key and copy it to client machine.
* To copy ssh pub key to another pc = **ssh-copy-id -i /root/.ssh/id\_rsa.pub user@client ip**.
* To login with hostname, add an entry in **/etc/hosts** file with **client hostname and ip**.

**SCP**

* It is used to copy the files between ssh connections securely with encryption.
* **scp source-file clientip:/dest-location** = To copy a file from one machine to another.
* **scp –r /source-file clientip:/dest-location** = To copy a dir recursively (sub-dir) to another machine.
* **scp sourceip:/source-file dest-location =** To copy file being in destination location.
* **scp –r sourceip:/source-dir /dest-location** = To copy dir being in destination location.

**RSYNC**

* It is used for backing up/mirroring the data between two machines to keep them in **“SYNC”.**
* The main advantage is, it just copies the files which are not in destination, rather than copying entire dir.
* If rsync is combined with ssh, it will be great to sync data securely.
* **rsync –rv –e ssh source-dir dest-ip:/dest-location** = To sync files between two machines with rsync and ssh.
* **rsync –avz –e ssh source-dir dest-ip:/dest-location** = To compress the data and send it to other machine with ssh.
* **rsync –rv source-dir dest-ip:/dest-location** = To sync 2 machines without ssh.
* **rsync –avz source dest-ip:/destination** = To compress and sync data without ssh.