SSH

Open-SSH or SSH:

- Secure Shell or SSH helps in accessing the servers remotely.
- It has a server componnet whch runs in the backgoround and a clinet component which helps in connecting to a server.
- The default port is 22 and can be changed to a different port.
- Logs will be stored in "/var/log/auth.log"
- sshd is server deamon, for the systems with init system as systemd.
  `systemctl status sshd.service` (to verify the ssh deamon)
- Root login will be suppressed by default.
- System level config available at "/etc/ssh/sshd_config"

Connecting to a remote sever via ssh:

- ssh client allows to connect to a remote by connecting to ssh server running in the remote machine.
- Syntax
  `ssh -v user@ipadd` -- with default port number 22
  `ssh -v -p [port number] user@ipadd`
  v - verbose, give more details on what's going on
  p - port number, default value is 22
- to verify the status use the below for systemd
  `systemctl status sshd.service`

Configuring an ssh client:

- A ".ssh" folder can be created in users home directory to store user level configurations.
- A config file will have the syntax below
  `Host "the name remote server to be identified with"`
  `Hostname "ipaddress or dns"`
  `Port "portnumber"`
  `User "username"`
  `IdentityFile "the file path having to ssh private key"`

Public and Private key authentication:

- The default authentication mode is by providing the user credentials.

- Public Private key authentication is more secure.
- Password authentication can be disabled to be more secureds.
- ssh-keygen is a binary comes along with ssh installation, allows to generate a public private key pair.
- Syntax

  ```
  ssh-keygen -t type -C comment
  ```

  t - type (rsa or ed25519 or other)
- Osnce a key pair genrated .pub file consists of a public key can be add to the sites that supports ssh authentication.
- The public key can either be copied to the path asked in the websites or paste the key in authorized_keys file in .ssh directory of a remote server that to be connected to.
- Key can alos be copied to a remote servers authorized_keys file using below syntax

  ```
  ssh-copy-id -i "key path on server" username@servername
  ```

- Below syntax using a keyfile path that can be specified to connect a remote server

  ```
  ssh -i keyfile servertoconnect
  ```

- A passphrase is helps in identifiying malicious connections.
- SHH agent maintains the cache of the keys which helps in not typing the passphrase. It can be started by

  ```
  eval "$(ssh-agent)"
  ```

- Key can be added to cache by using `ssh-add key`

Troubleshooting ssh:

- systems with systemd as init system troubleshooting can be done by observing for issues in the journal.

  ```
  journalctl -fu ssh/sshd
  ```

  f - follow

  u - unit
- Logs can also be found in /var/log/auth.log

Resources online

- [LearnLinuxTv - Open SSH Guide]
- [LearnLinuxTv - Open SSH Playlist]