Note:

- Fresh Installation

Steps:

- download the ova (e.g., FortiSIEM-VA-7.1.6.1663.ova) and open in VMWare workstation
- normal settings
  - OS - 25GB
  - OPT - 100GB
  - CMDB - 60GB
  - SVN - 60GB
  - Local database - depending on required retention period
    - `Local database = (RF X EPS X Event Size X Online Retention X 24 X 60 X 60)/(Compression Ration X 1024 X 1024 X 1024)`
      - RF - Retention Factor
- FortiSIEM will use `Rocky Linux`
  - localhost login - root
  - password - ProspectHills
- go to `configFSM.sh` script and run it

```
find / -name "configFSM.sh"
```

- we get 4 options to configure (`FortiSIEM Manger` is optional, its for huge setup)
- just select `Supervisor` its an all-in-one solution > `install_without_fips`
- setup the IPv4 address, Gateway and DNS1 and DNS2
- configure the hostname (i.e., `FQDN`)
- for checking network connectivity, enter the host (default:- google.com)
- run configuration command (i.e., python script)
- after installation, login
- ping the gateway to check the connectivity

- ping google to check the internet connectivity
- to activate the license visit the FortiCloud(`support.fortinent.com`) and enter product serial number. (basically you will get email from the fortinet)
  - choose non-government user
- if you already registered, got to FortiCloud > Product > Product List, then change the hardware id (you can find harware ID in FortiSIEM). Then download the new license. then upload it in FortiSIEM (e.g., https://IP/phoenix/licenseUpload.html)
- Choose Enterprise as license type if you are not using multi tenant.
- now you can login
- during installation, you need to choose DB, choose `clickhouse` (best option), `storage tier` can be 1 (if replication factor is 1), then you need to mount the hard disk
  - for this create a new host in `PuTTY Configuration`. give host name (or IP address), port and save session then save and open. then login as `root`
    - to get the list of all the partition: `lsblk` - note down the `sde`
  - Disk path should be: `/dev/sde` and then press `test` then you will be redirected to page 2 and here you need to provide the admin password.
- next login and access the UI
- to verify the services, we should see all the services up and running in `PuTTY`, use `phstatus` command

Note:

- PuTTY is **a free terminal emulator Windows users can use to connect to a website via SSH**. This allows you to run UNIX commands on your server, which is not available when connecting using an FTP client.