

- ① ~~System~~
- ② ~~upgrade plan~~
- ③ ~~Setting~~
- ④ ~~Monitoring Console~~

② Upgrade Plan

- ① Pre-implementation.
- ② During Implementation.
- ③ Post Implementation.



① Dependencies \rightarrow App & Add-on.

\downarrow
Sunk, DRconnect

② Backup (local folders) \rightarrow Config, User specific.

③ Backup (XML files) \rightarrow Dashboard

④ Backup / Screenshot \rightarrow Dashboard.

During Implementation

Post Implementation

Verification

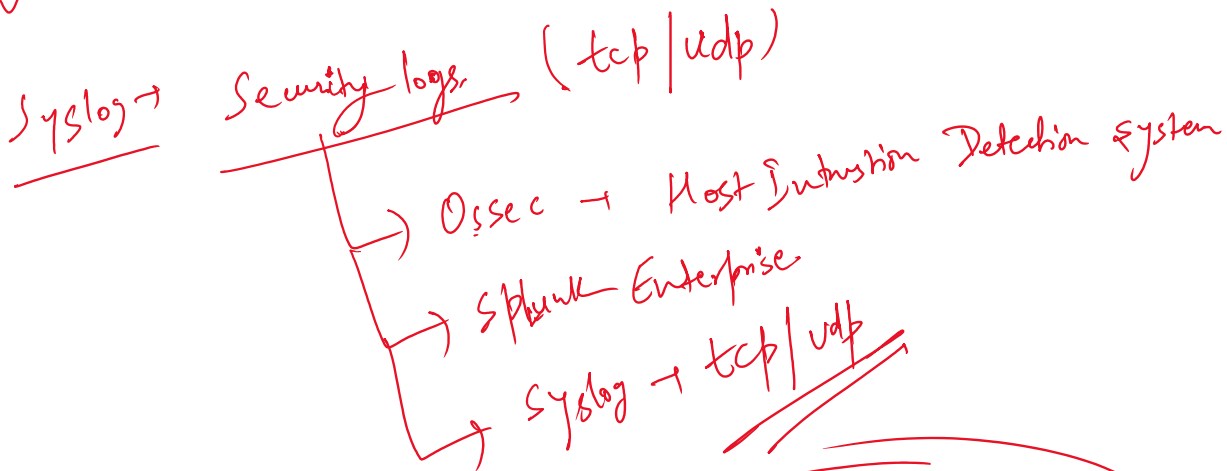
① Data Ingestion

- ① Management Instance - CM, Deployer & DS
- ② Forwarder
- ③ Search Head
- ④ Indexer

\rightarrow Splunk Recommendation

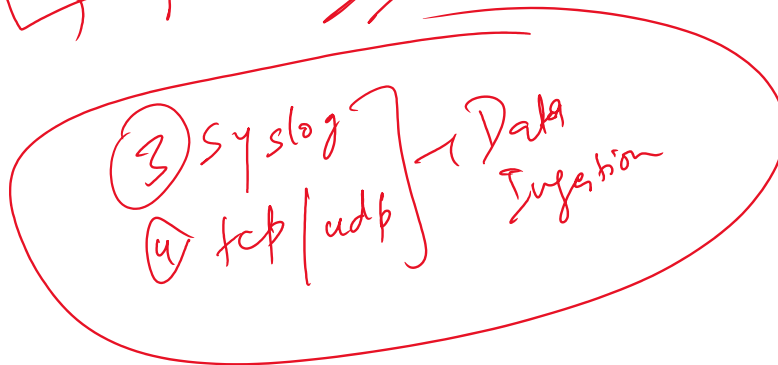
... with ports (tcp/udp)

✓



① Ossec

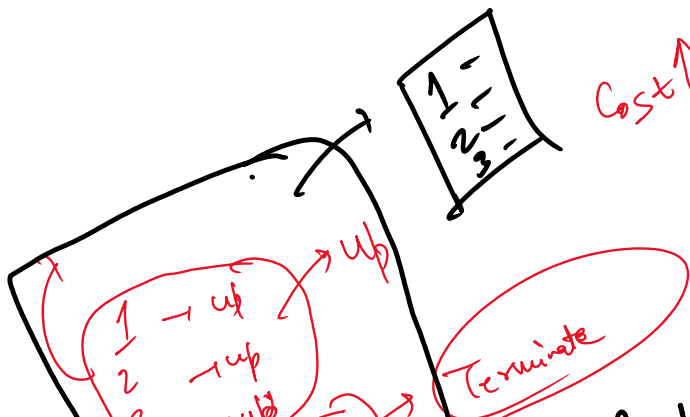
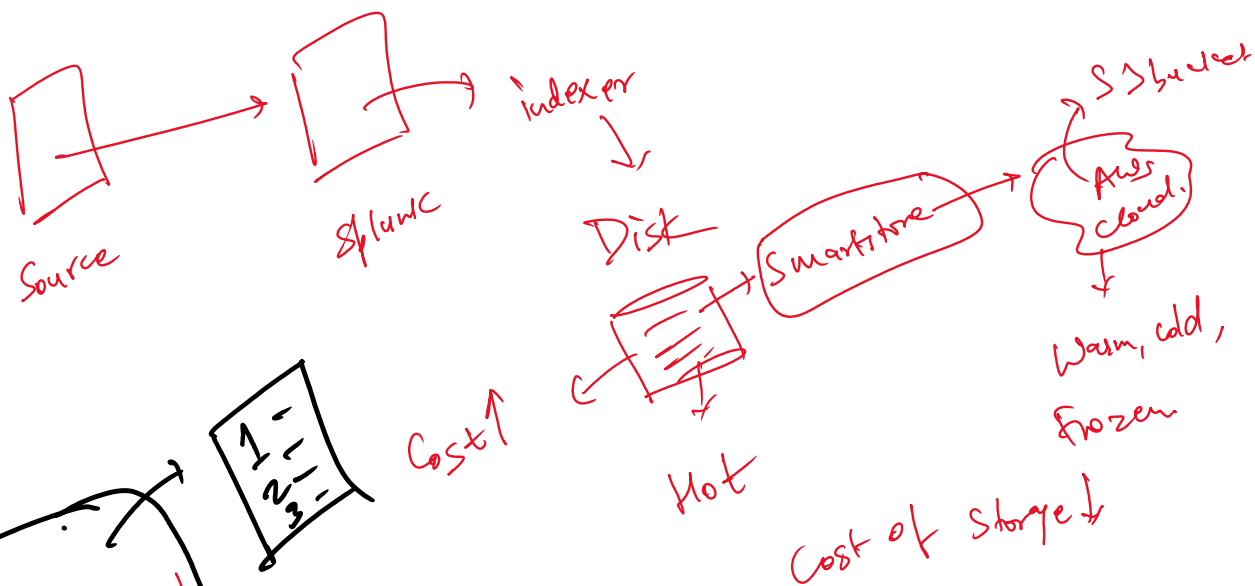
② Splunk



<syslog>

</syslog>

```
<syslog_output>
<server>127.0.0.1</server>
<port>514</port>
<format>default</format>
</syslog_output>
```



forwards

