1. Splunk 是机器数据的引擎。使用 Splunk 可收集、索引和利用所有应用程序、服务器和设备生成的快速移动型计算机数据。Splunk利用内在的机器学习方法，对收集到的数据自动进行整合，制表。

2. SplunkBase是Splunk的社区，里面有社区人士专门为某些特别的应用例如AWS, VMWARE等任务写的Add-on包。

3. Splunk主要有3个组件。Indexer, Search Head, Forwarder.

Indexer(索引器)： 用于将unstructed的数据变为structured. 建立好文件夹保存到Splunk数据库中。并且执行具体的搜索工作。

Search Head（搜索头）: 使得可以使用 Splunk搜索语法去搜索数据，并且整合返回搜索结果。提供各种的结果图标。

Forwarder(转发器): 是Splunk Enterprise的实力， 安装在服务器上，将搜集的数据发送到Indexer中。

Note: 这三个基本组建可以部署在单个机器上，也可以部署在分布式的结构上。

4. Splunk的三种角色:

Admin: 管理员可以安装apps, 创建 knowledge objects.

Power: 可以创建knowledge objects， 分享knowledge objects, 以及完成实时搜索

User: 只能看自己或者被分享的knowledge objects.

5.