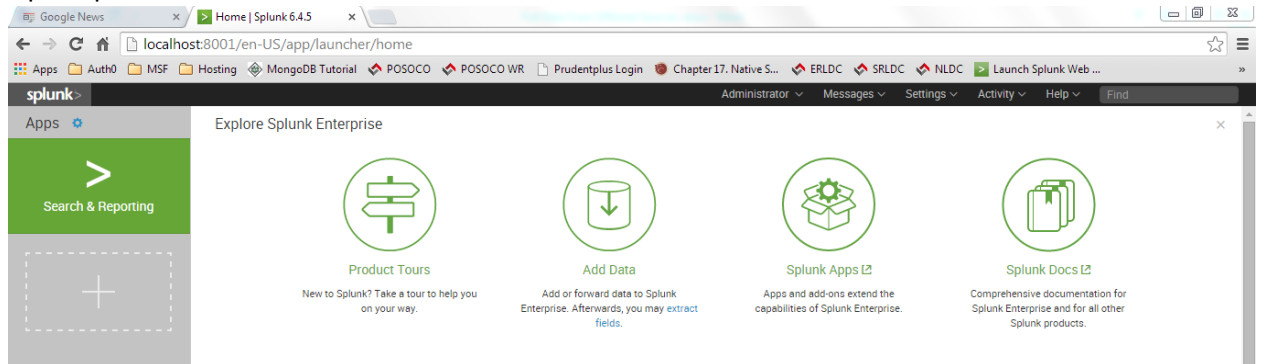
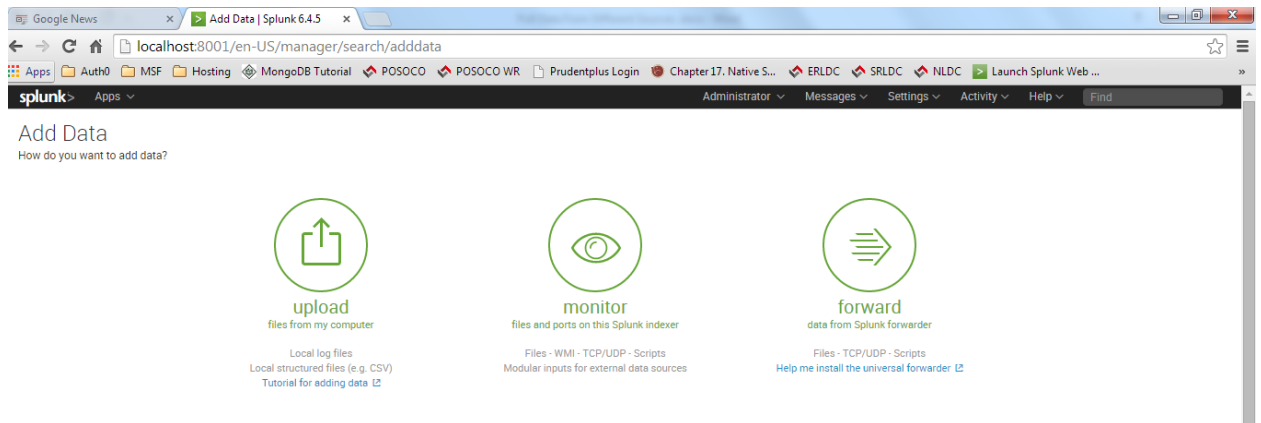


Pull Data from Windows Event Log

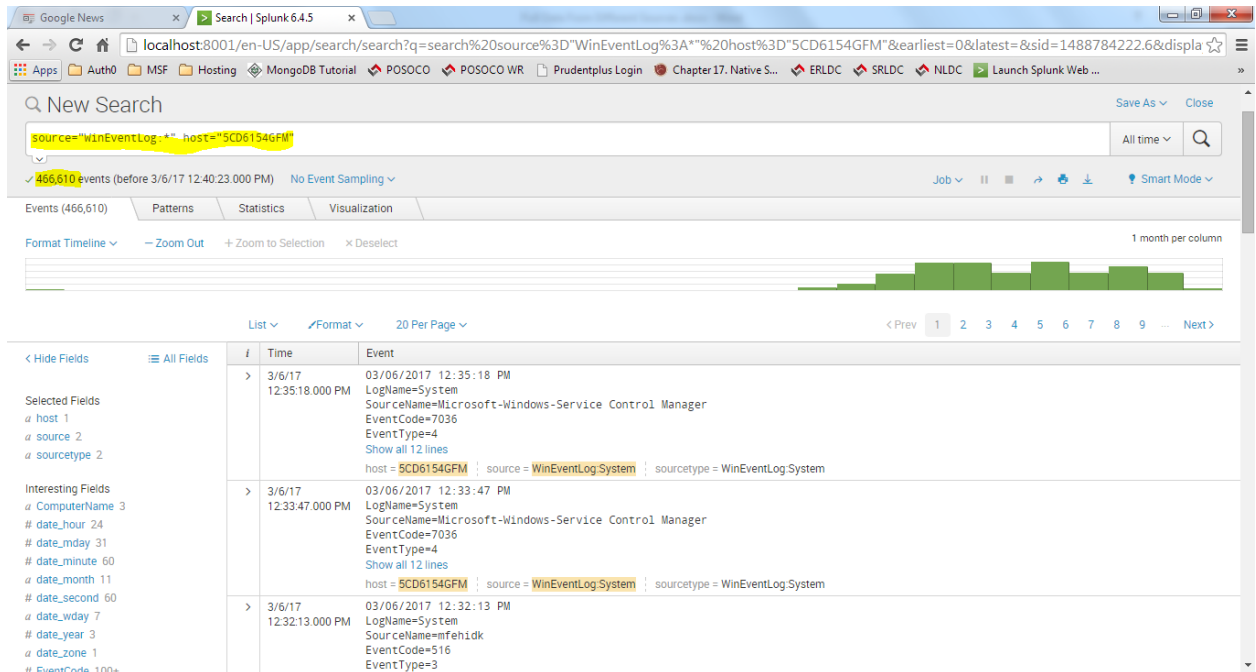
1. Open Splunk Home and Click on Add Data



2. Click on Monitor



3. Click on **Local Event Logs**, select appropriate event logs like **Application** and **System**. Click Next.
4. In the next tab chose/create an **index** if required and click **Review**.
5. Click **Submit** and then click **Start Searching**. It will display all the event logs from System.



Pull Data from Database Log Table

1. We can use scripts to pull data from Database Tables.
2. We can use shell scripts, python scripts, Windows batch files, PowerShell, or any other utility that can format and stream the data that we want to index.
3. An example is given in the below link.

<https://docs.splunk.com/Documentation/Splunk/8.0.0/AdvancedDev/ScriptExample>