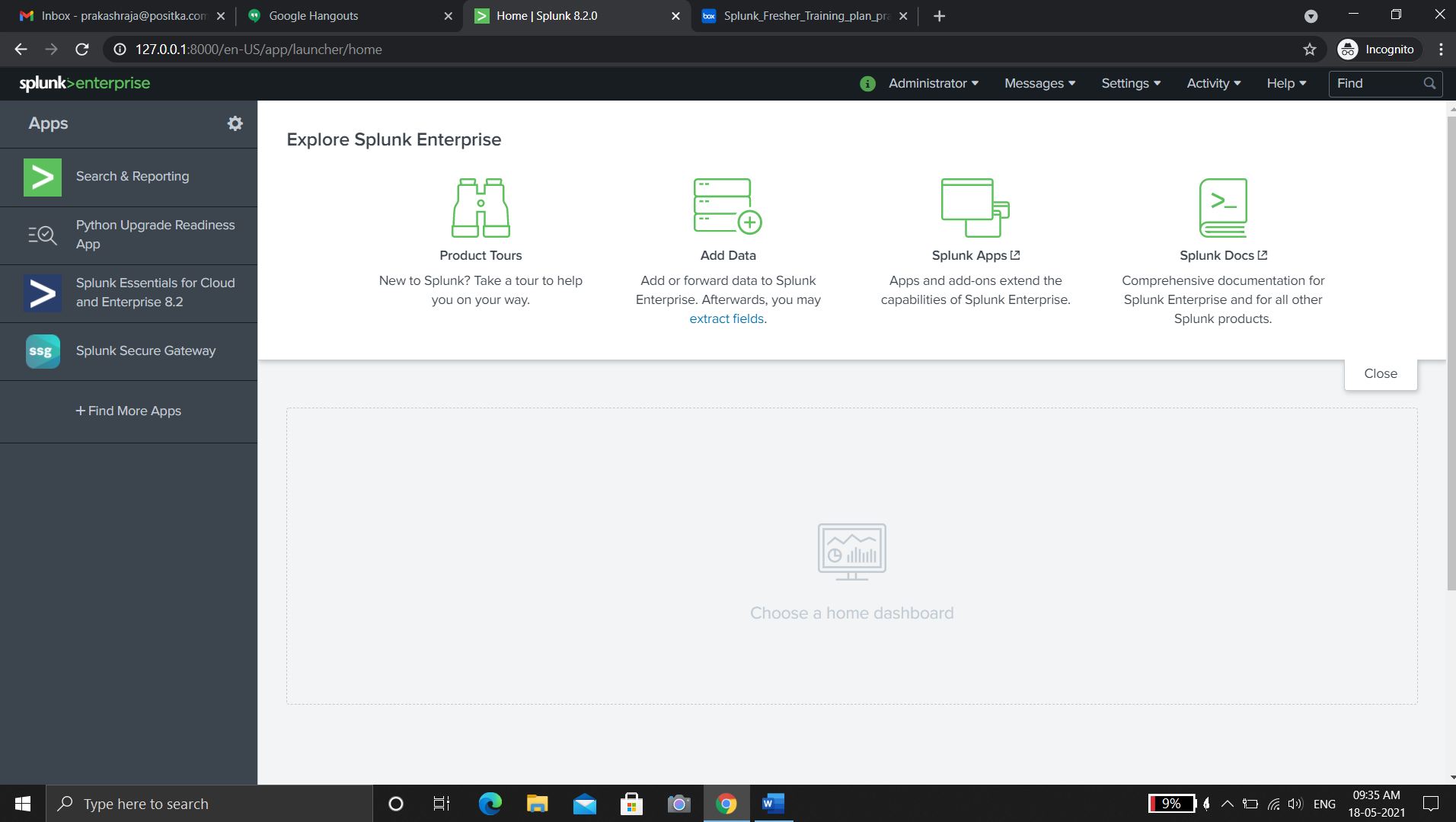
**WEEK 1**

**Splunk Installation on windows**

1. Download Splunk enterprise
2. Move on installation procedure



**Splunk installation on Linux**

1. To install Splunk

$ tar xvzf splunk.tgz -C /opt

1. To run splunk

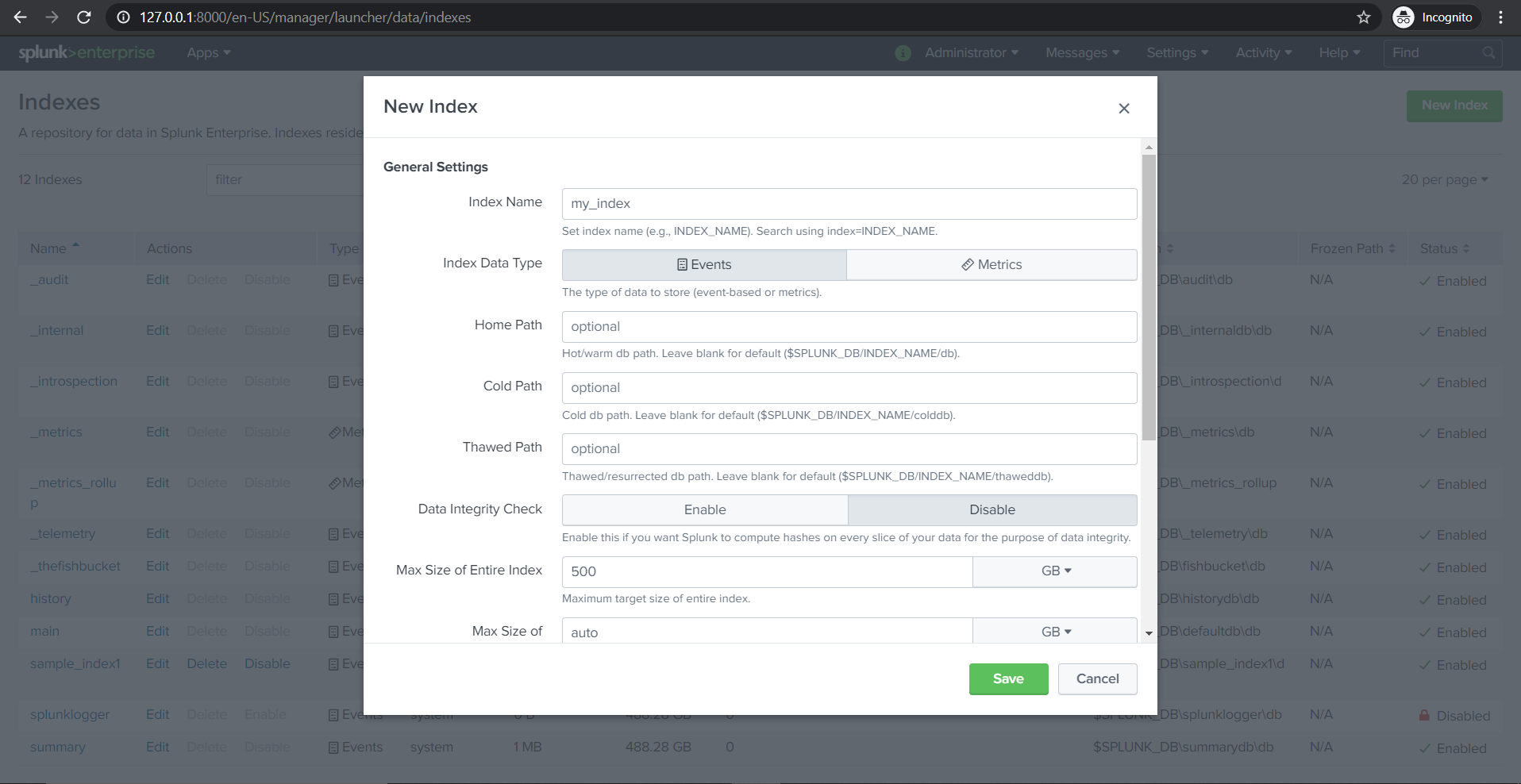
$ ./splunk start –accept-license

1. To enable boot start splunk

$ sudo ./splunk enable boot-start

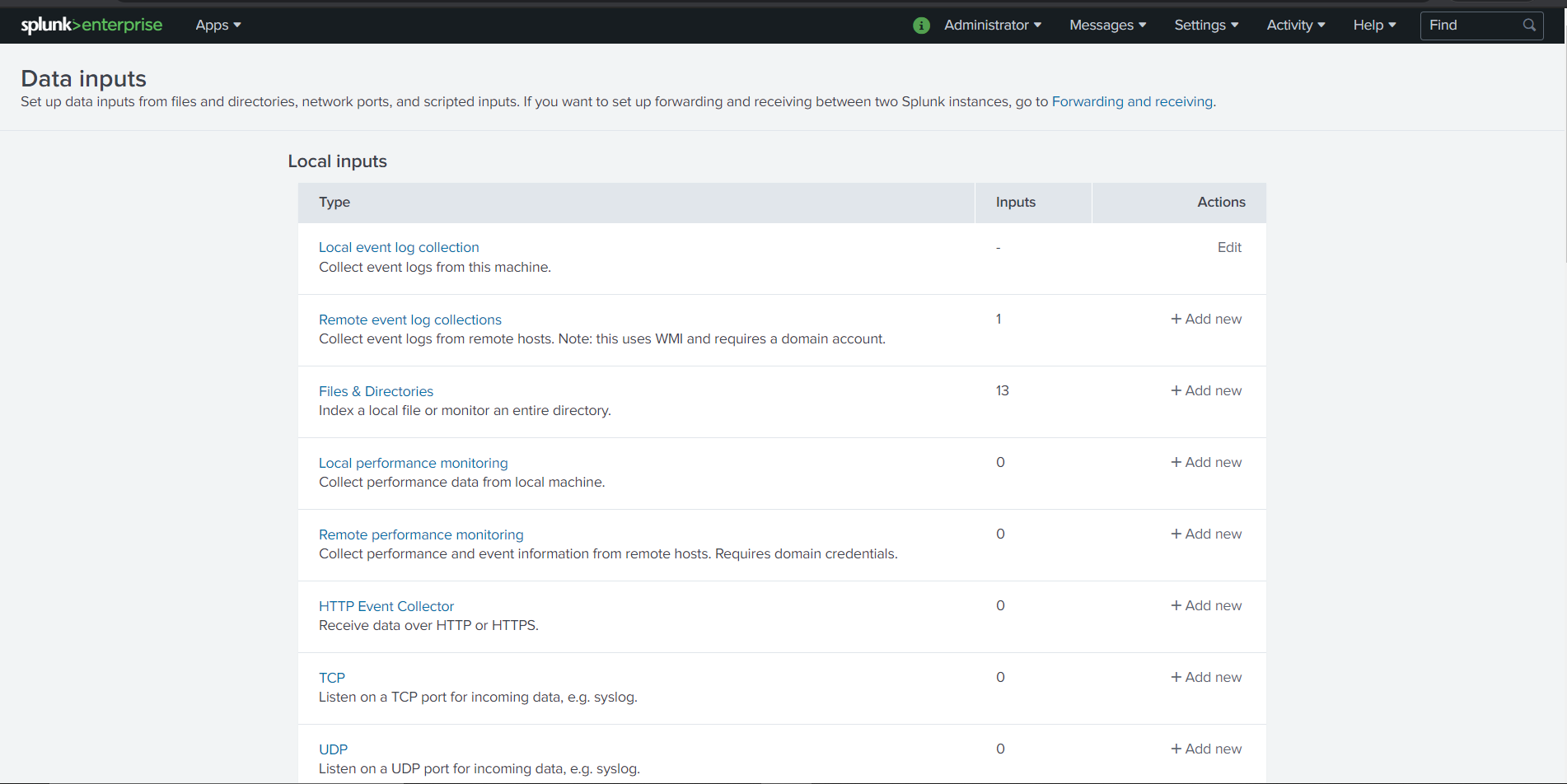
**To create a new index**

1. Settings -> data(indexes)
2. Click new index
3. Set parameters for index
4. Click save.



**Getting data on windows and linux**

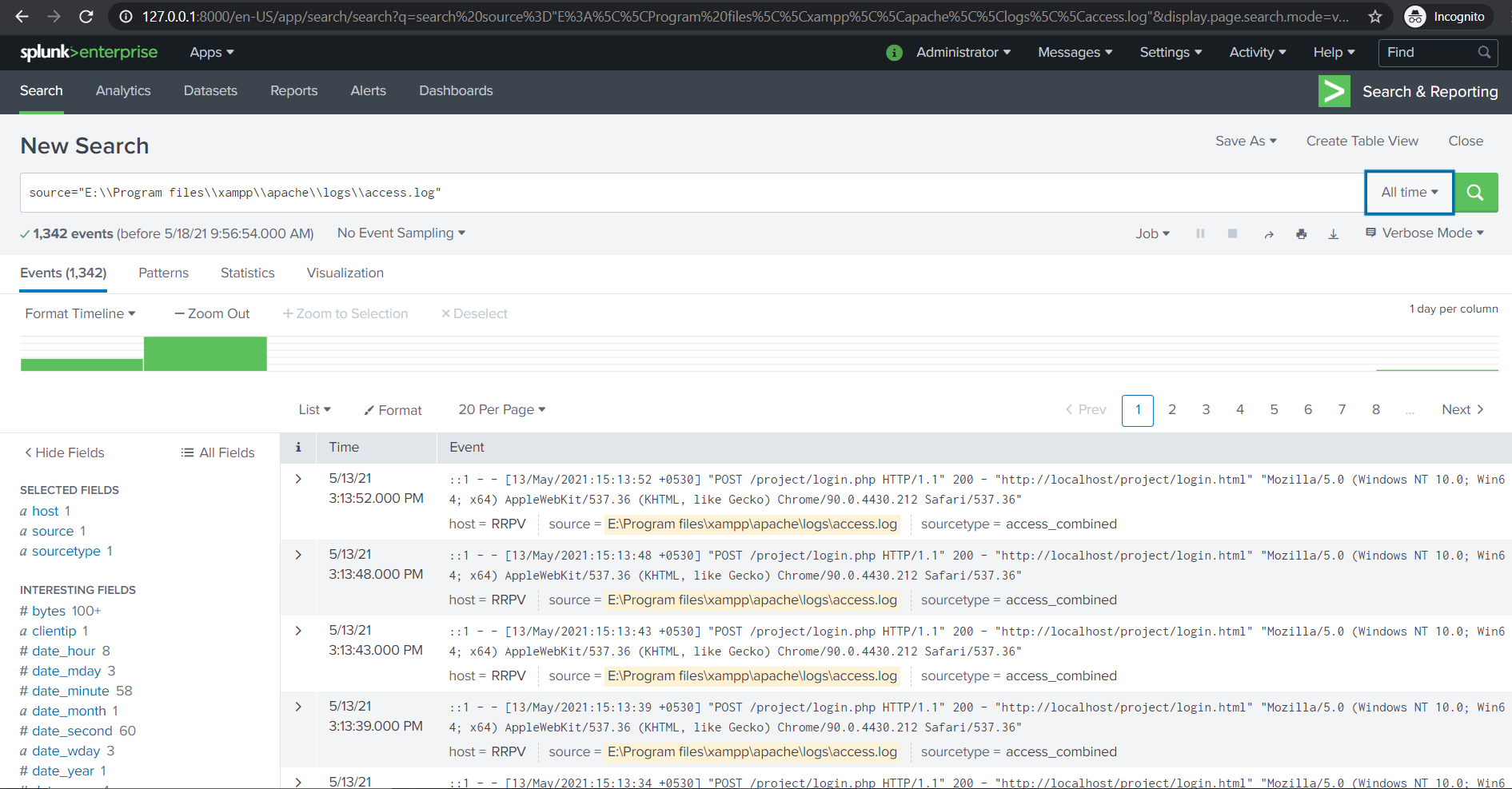
1. Login splunk (127.0.01:8000)
2. Settings -> data(data inputs)



1. Select input type

Example: Local event log, files and directories, local or remote performance monitoring, http event collector, tcp, udp, etc.,

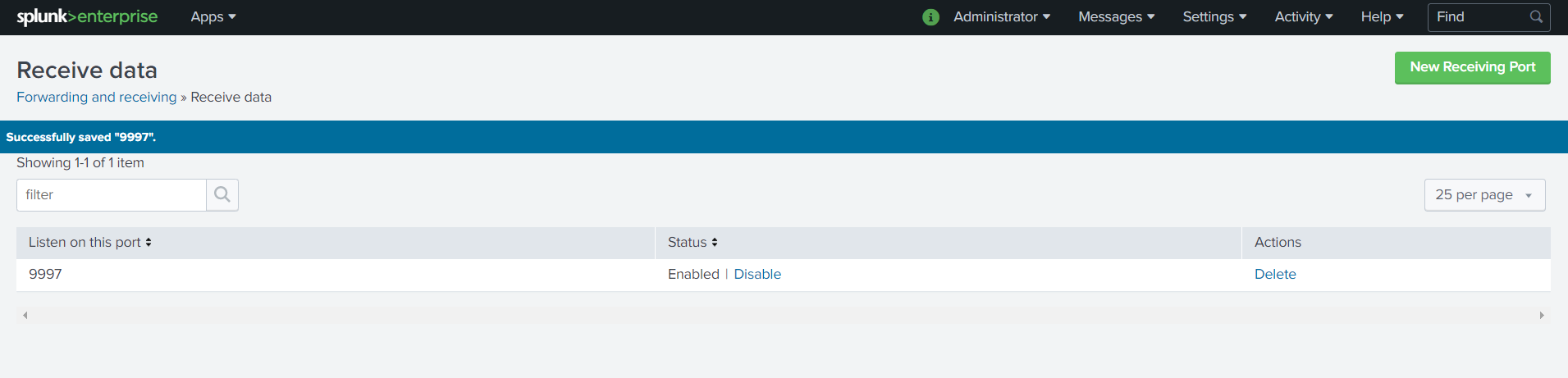
1. Select input type Click add new
2. Set the input parameters
3. Review data input parameters
4. Click submit



**To get data using universal forworders**

**On splunk**

1. Settings -> forwarding and receiving
2. On receiving data, click add new(configure receiving)
3. Setup listening port (9997 tcp)
4. Click save



**On forwarding device or machine(windows)**

1. Download universal forwarder
2. Install and set host name: port of Splunk server

**On forwarding device (Linux)**

1. Download universal forwarder
2. Install it

$ tar xvzf splunkforwarder.tgz -C /opt

1. Navigate to bin directory

$ cd /opt/splunkforwarder/bin

1. To start

$ ./splunk start –accept-license

1. Enter username and password
2. To enable boot start

$ sudo ./splunk enable boot-start

1. To add splunk receiving server

$ sudo ./splunk add forward-server hostname:portreceiving

1. To add directory of logs

$ sudo ./splunk add monitor filepath

**To search events and logs**

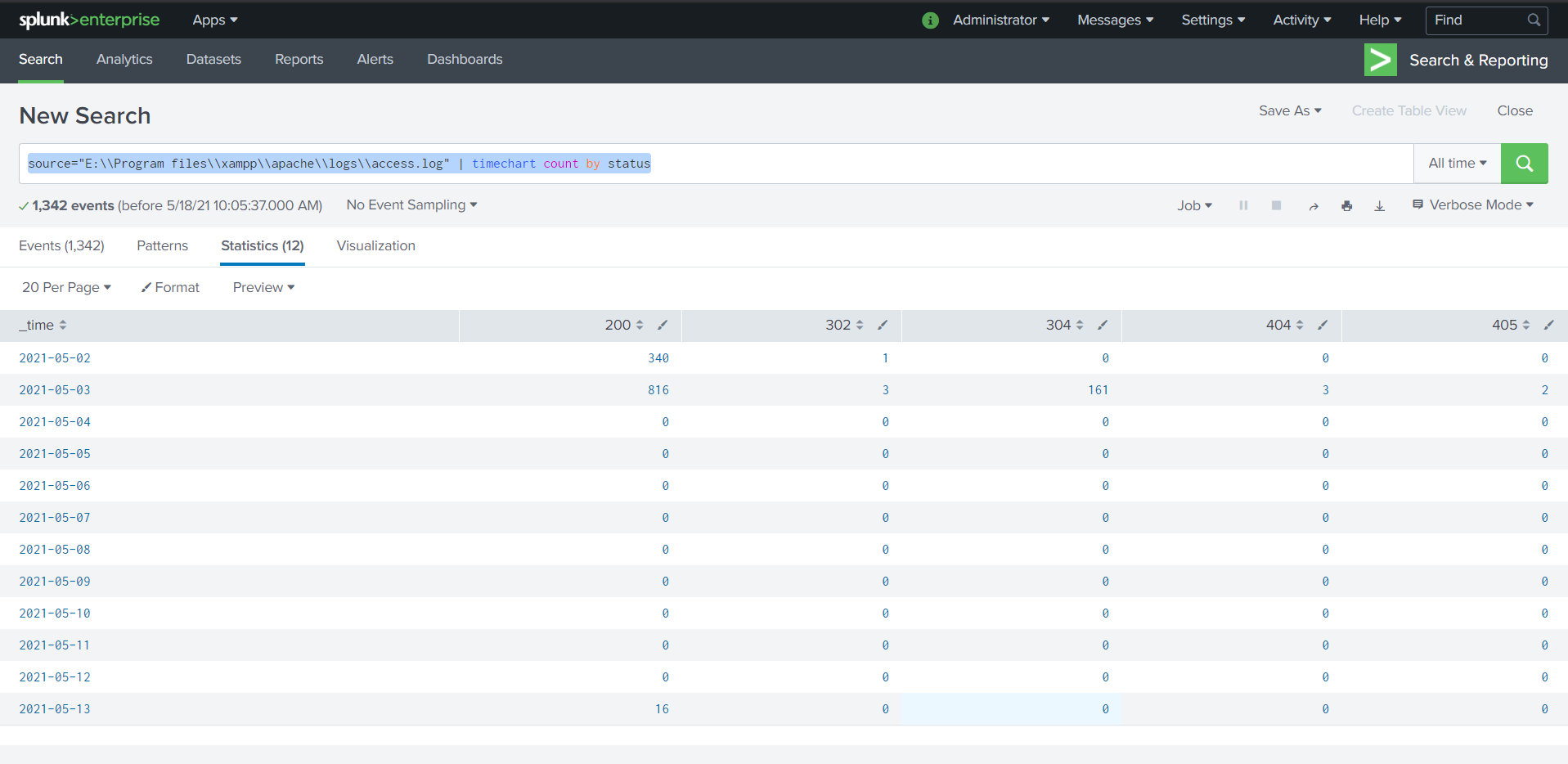
1. Apps -> Search and reporting
2. Enter search values on search bar

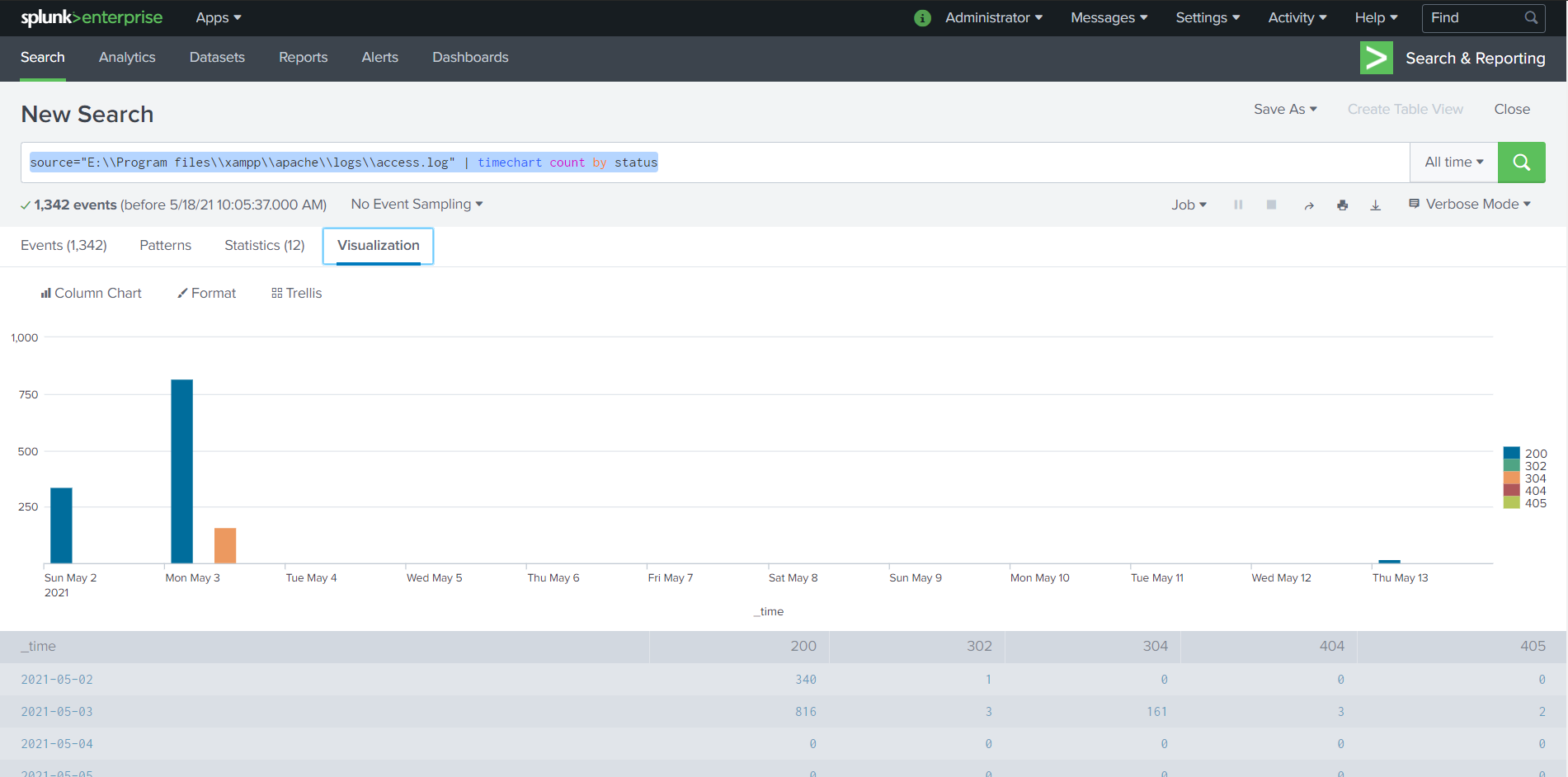
Example: source="E:\\Program files\\xampp\\apache\\logs\\access.log" | timechart count by status

1. Select timeframe

Example: all time, last 30 seconds, last 1 day, etc.

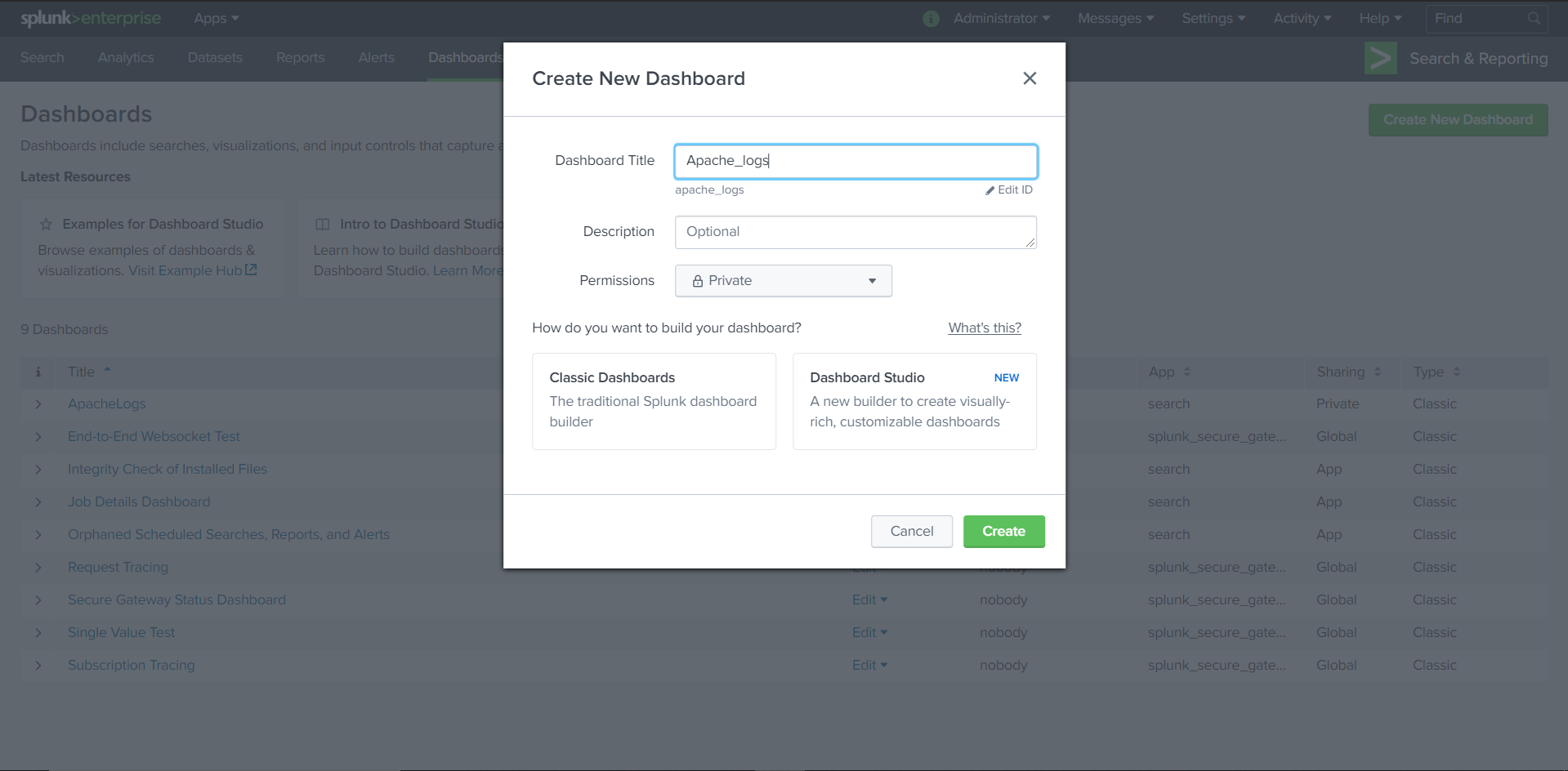
1. Click search



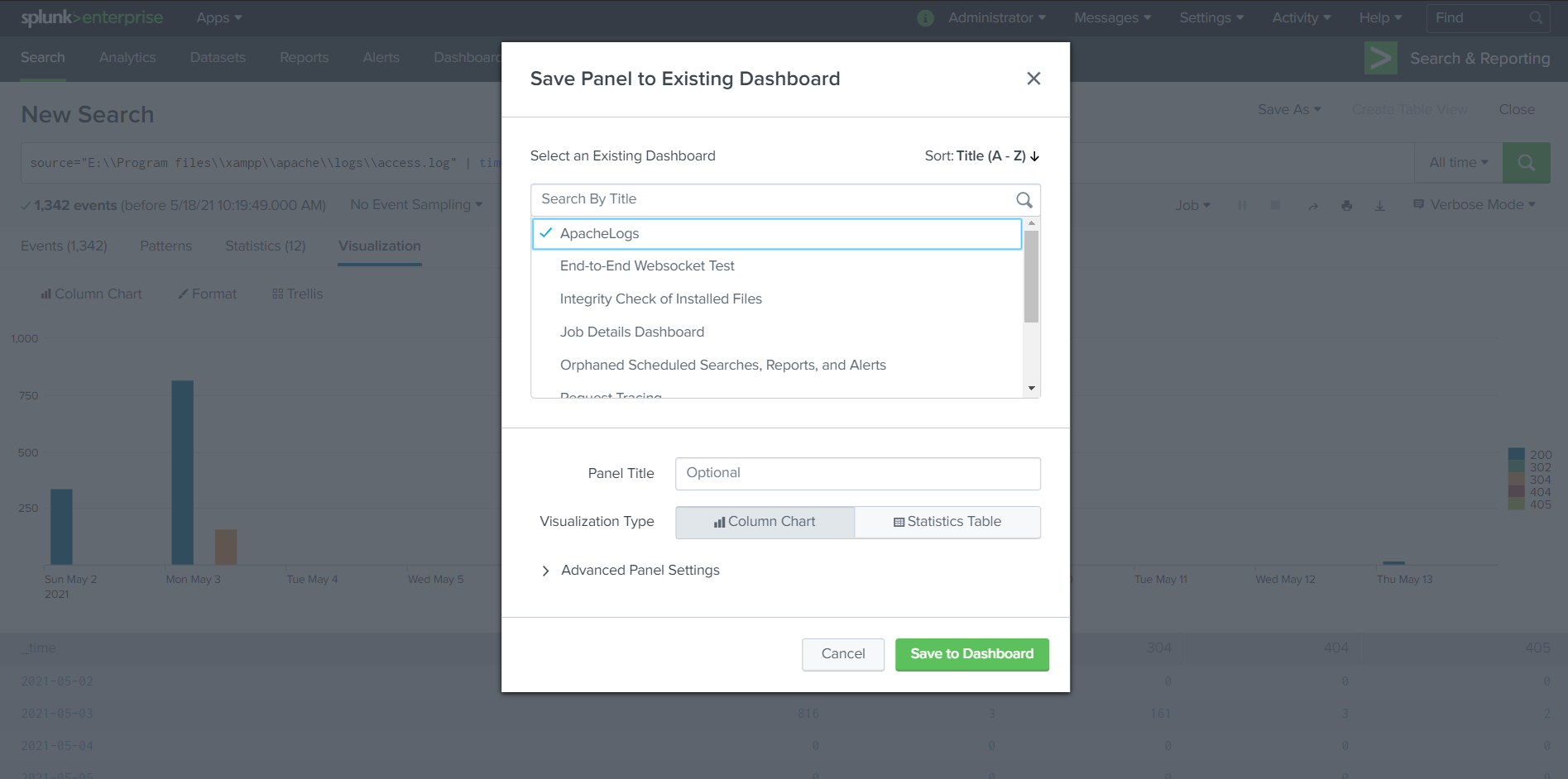


**To create a dashboard**

1. Apps(Search and reporting)
2. click dashboard -> New dashboard
3. Enter dashboard parameters
4. Click create



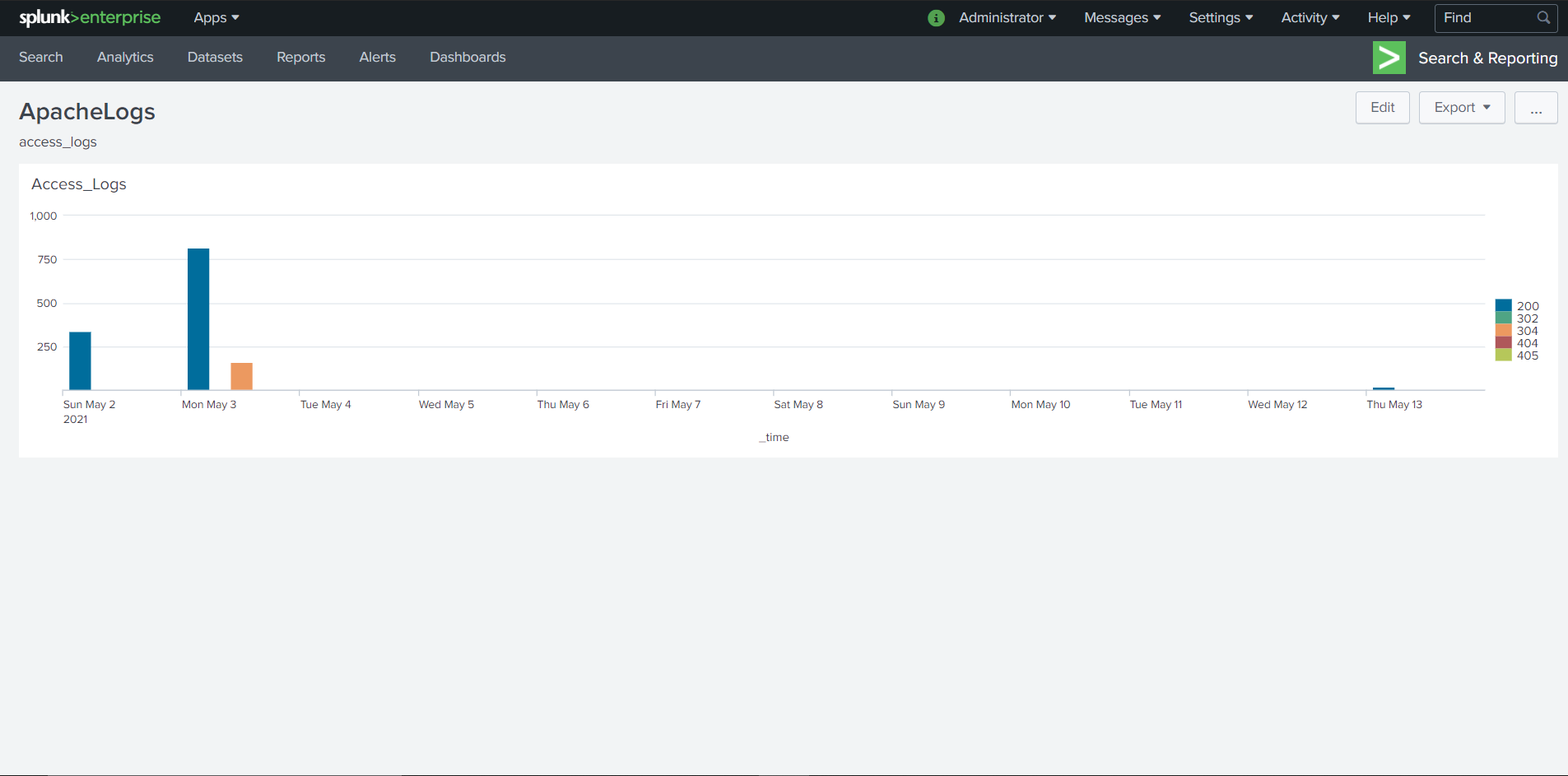
1. Search the logs and event want to add on dashboard
2. Click visualization
3. Save as -> Existing dashboard
4. Enter dashboard parameters



1. Click save to dashboard

**To go to dashboard**

1. Apps(Search and reporting)
2. Click dashboards
3. Select the dashboard you want to view



**Alert creation using Splunk**

1. Search the alert parameters
2. Go to visualization (Set visualization)
3. Save as -> Alert
4. Set the alert parameters and alert method
5. Click save

