Contents

1. About Test Drive

In this test drive which is of 15 mins duration, we are going see the capabilities of Splunk Enterprise. Splunk Enterprise Web Console comes with many built-in and add-on apps, we can use Search and Reporting app to generate reports and visualize the data in different formats based on the requirement. We are going to explore and analyses the user activities in the client virtual machine by using the /var/log, ~/.bash_history, /etc/passwd and Apache logs. In this Test drive, we are going install Splunk add-on for Apache webservers on Splunk instance and universal forwarder on client virtual machine (vm) that will forward the data from client machine to Splunk enterprise.

2. What is Splunk Enterprise

Splunk Enterprise is a software product that enables you to search, analyses, and visualize the machine-generated data gathered from the websites, applications, sensors, devices, and so on, that comprise your IT infrastructure or business. After you define the data source, Splunk Enterprise indexes the data stream and parses it into a series of individual events that you can view and search. You can use the search processing language or the interactive pivot feature to create reports and visualizations.

3. About universal forwarder

The universal forwarder collects data from a data source or another forwarder and sends it to a forwarder or a Splunk deployment. With a universal forwarder, you can send data to a Splunk Enterprise, Splunk Light, or Splunk Cloud. It also replaces the Splunk Enterprise light forwarder.
The universal forwarder is available as a separate installation package

3.1 What forwarders do

Forwarders get data from remote machines. They represent a more robust solution than raw network feeds, with their capabilities for the following actions:

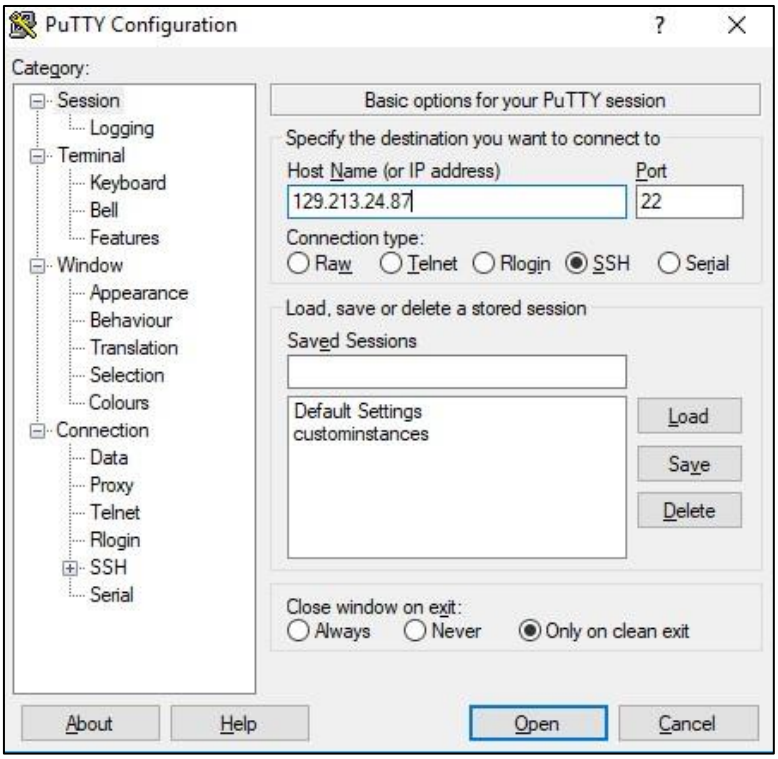
- Tagging of metadata (source, source type, and host)
- Configurable buffering
- Data compression Splunk Enterprise
- SSL security
- Use of any available network ports
- Running scripted inputs locally

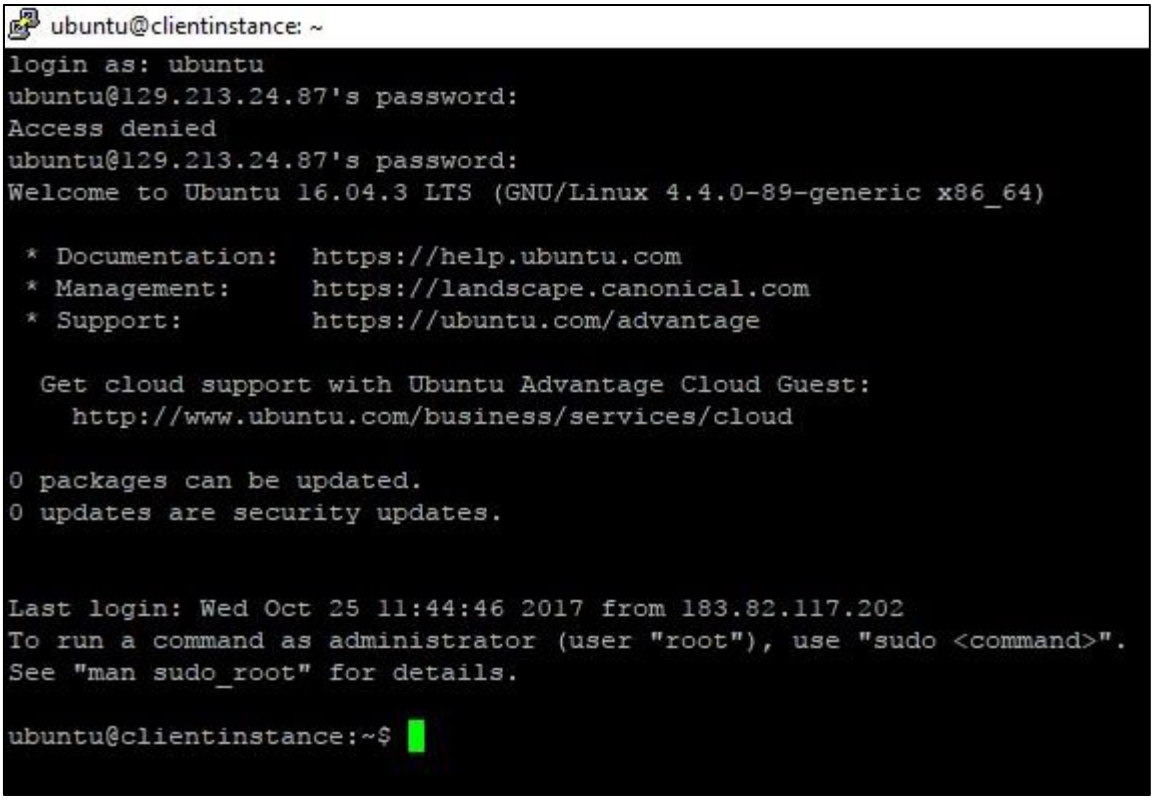
Forwarders usually do not index the data, but rather forward the data to a Splunk deployment that does the indexing and searching. A Splunk deployment can process data that comes from many forwarders. In most Splunk deployments, forwarders serve as the primary consumers of data. In a large Splunk deployment, you might have hundreds or even thousands of forwarders that consume data and forward for consolidation

4. Installing the universal forwarder on Linux

After test drive provisioning is complete, login credentials are provided in the test drive launch page as well as by e-mail. With the username, password, and client SSH URL provided, SSH into the Virtual machine from your terminal or SSH client.

1. Log into your SSH session using client SSH public IP, admin-username and admin-password provided in output section.





2. Download the latest Splunk package on the client VM by using the following command

wget -O splunkforwarder-7.0.0-c8a78efdd40f-Linux-x86_64.tgz 'https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_64&platform=linux&version=7.0.0&product=universalforwarder&filename=splunkforwarder-7.0.0-c8a78efdd40f-Linux-x86_64.tgz&wget=true'

3. Extract the files from zip folder **tar xvzf splunkforwarder-7.0.0-c8a78efdd40f-Linux-x86_64.tgz**

```
ubuntu@clientinstance:~$ tar xvzf splunkforwarder-7.0.0-c8a78efdd40f-Linux-x86_64.tgz
splunkforwarder/
splunkforwarder/etc/
splunkforwarder/etc/deployment-apps/
splunkforwarder/etc/deployment-apps/README
splunkforwarder/etc/apps/
splunkforwarder/etc/apps/splunk_httpinput/
splunkforwarder/etc/apps/splunk_httpinput/default/
splunkforwarder/etc/apps/splunk_httpinput/default/inputs.conf
splunkforwarder/etc/apps/search/
splunkforwarder/etc/apps/search/metadata/
splunkforwarder/etc/apps/search/metadata/default.meta
splunkforwarder/etc/apps/search/default/
splunkforwarder/etc/apps/search/default/app.conf
splunkforwarder/etc/apps/search/default/restmap.conf
splunkforwarder/etc/apps/search/default/props.conf
splunkforwarder/etc/apps/search/default/transforms.conf
splunkforwarder/etc/apps/SplunkUniversalForwarder/
splunkforwarder/etc/apps/SplunkUniversalForwarder/metadata/
splunkforwarder/etc/apps/SplunkUniversalForwarder/metadata/default.meta
splunkforwarder/etc/apps/SplunkUniversalForwarder/default/
splunkforwarder/etc/apps/SplunkUniversalForwarder/default/limits.conf
splunkforwarder/etc/apps/SplunkUniversalForwarder/default/README
splunkforwarder/etc/apps/SplunkUniversalForwarder/default/app.conf
splunkforwarder/etc/apps/SplunkUniversalForwarder/default/inputs.conf
splunkforwarder/etc/apps/SplunkUniversalForwarder/default/outputs.conf
splunkforwarder/etc/apps/SplunkUniversalForwarder/default/props.conf
splunkforwarder/etc/apps/SplunkUniversalForwarder/default/web.conf
splunkforwarder/etc/apps/SplunkUniversalForwarder/default/server.conf
```

4. Move the Splunk forwarder to *opt* location **sudo mv splunkforwarder /opt/**

```
splunkforwarder/share/splunk/3rdparty/Copyright-for-hive_1_2-1.2.1.txt
splunkforwarder/share/copyright.txt
ubuntu@clientinstance:~$ sudo mv splunkforwarder /opt/
ubuntu@clientinstance:~$
```

5. Navigate to the following location **cd /opt/splunkforwarder/bin**

```
ubuntu@clientinstance:~$ cd /opt/splunkforwarder/bin
ubuntu@clientinstance:/opt/splunkforwarder/bin$
```

6. To accept the license of splunk forwarder run the following command.

   ./splunk start --accept-license

```
ubuntu@clientinstance:/opt/splunkforwarder/bin$ ./splunk start --accept-license

This appears to be your first time running this version of Splunk.

Splunk> See your world.  Maybe wish you hadn't.

Checking prerequisites...
        Checking mgmt port [8089]: open
                Creating: /opt/splunkforwarder/var/lib/splunk
                Creating: /opt/splunkforwarder/var/run/splunk
                Creating: /opt/splunkforwarder/var/run/splunk/appserver/i18n
                Creating: /opt/splunkforwarder/var/run/splunk/appserver/modules/static/css
                Creating: /opt/splunkforwarder/var/run/splunk/upload
                Creating: /opt/splunkforwarder/var/spool/splunk
                Creating: /opt/splunkforwarder/var/spool/dirmoncache
                Creating: /opt/splunkforwarder/var/lib/splunk/authDb
                Creating: /opt/splunkforwarder/var/lib/splunk/hashDb
New certs have been generated in '/opt/splunkforwarder/etc/auth'.
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-7.0.0-c8a78efdd40f-linux-2.6-x86_64-mani
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done

ubuntu@clientinstance:/opt/splunkforwarder/bin$
```

7. Run the following command to enable boot-start. **sudo ./splunk enable boot-start**

```
ubuntu@clientinstance:/opt/splunkforwarder/bin$ sudo ./splunk enable boot-start
Init script installed at /etc/init.d/splunk.
Init script is configured to run at boot.
ubuntu@clientinstance:/opt/splunkforwarder/bin$
```

8. Configure Forwarder connection to Index Server

   ./splunk add forward-server <Splunk-IP>:9997

```
ubuntu@clientinstance:/opt/splunkforwarder/bin$ ./splunk add forward-server 129.213.16.37:9997
Splunk username: admin
Password:
Added forwarding to: 129.213.16.37:9997.
ubuntu@clientinstance:/opt/splunkforwarder/bin$
```

   In the above command where hostname.domain is the fully qualified address or IP of the index server (like splunkdnsjv6q3.subnet1.cloud.oracle.com, you can find this on the testdrive launch page named Splunk domain name and 9997 is the receiving port.

9. After executing the above command, it will ask for Splunk username and password are

   Usern ame: admin
   Password: changeme

10. Configure Forwarder connection to Index Server.

    /opt/splunkforwarder/bin/splunk list forward-server -auth admin:changeme

```
ubuntu@clientinstance:/opt/splunkforwarder/bin$ /opt/splunkforwarder/bin/splunk list forward-server -auth admin:changeme
Active forwards:
        129.213.16.37:9997
Configured but inactive forwards:
        None
ubuntu@clientinstance:/opt/splunkforwarder/bin$
```

11. Run the command that enables that data input. For example, to monitor the /var/log directory on the host with the universal forwarder installed, type in

    ./splunk add monitor /var/log

```
ubuntu@clientinstance:/opt/splunkforwarder/bin$ ./splunk add monitor /var/log
Added monitor of '/var/log'.
ubuntu@clientinstance:/opt/splunkforwarder/bin$
```

12. We can optionally add few more files for data input.

    ./splunk add monitor /etc/passwd

```
ubuntu@clientinstance:/opt/splunkforwarder/bin$ ./splunk add monitor /etc/passwd
Added monitor of '/etc/passwd'.
ubuntu@clientinstance:/opt/splunkforwarder/bin$
```

13. Some configuration changes might require that you restart the forwarder.

    ./splunk restart

```
ubuntu@clientinstance:/opt/splunkforwarder/bin$ ./splunk restart
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.

Stopping splunk helpers...

Done.

Splunk> See your world.  Maybe wish you hadn't.

Checking prerequisites...
        Checking mgmt port [8089]: open
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-7.0.0-c8a78efdd40f-linux-2.6-x86_64-mani
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done

ubuntu@clientinstance:/opt/splunkforwarder/bin$
```

Now you can see the logs information in Splunk Enterprise by connecting to the web interface

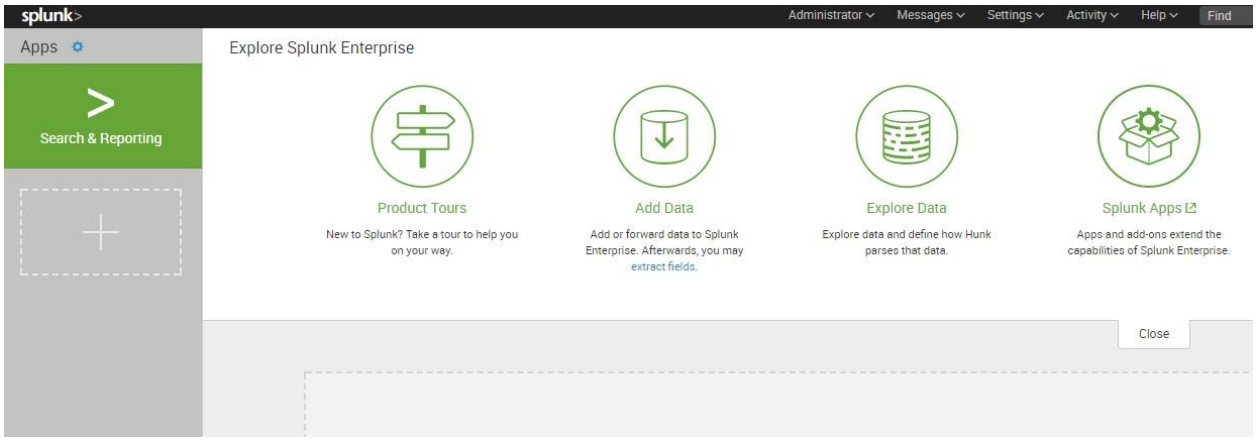
5. Login into Splunk Enterprise

1. Go to Splunk web console using Splunk Public_IP with port 8000.

Eg: Splunk_IP:8000

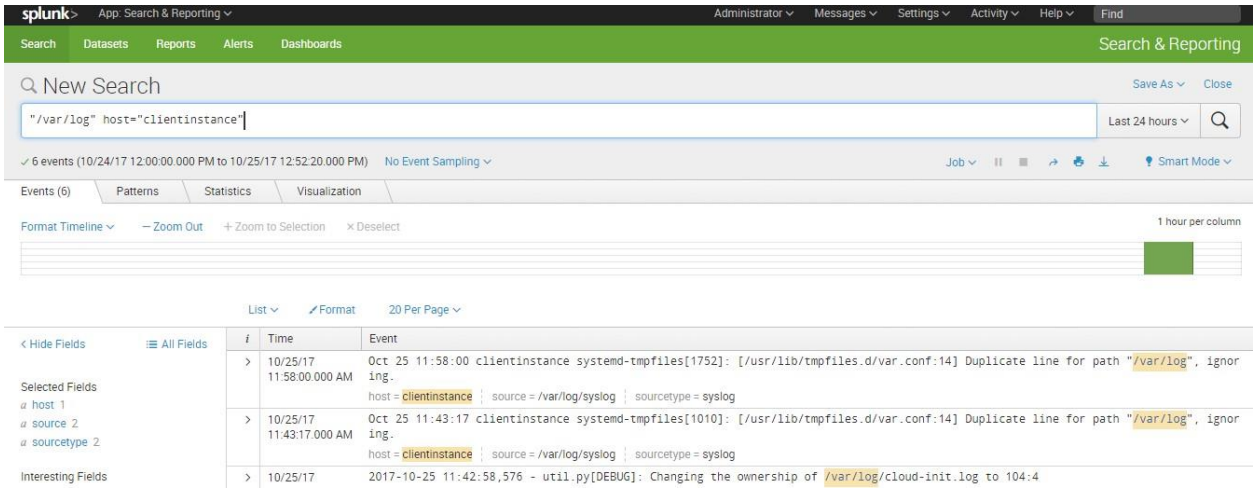
2. You can change your password.

3. After logging in, you will be prompted to dashboard page.



4. Click on the search & reporting tile on the left panel, it will take us to the search and reporting page.
5. Type the following in the search box and click on the search icon

   "/var/log" host=clientvm
6. We will be presented with events related to /var/log as shown below.



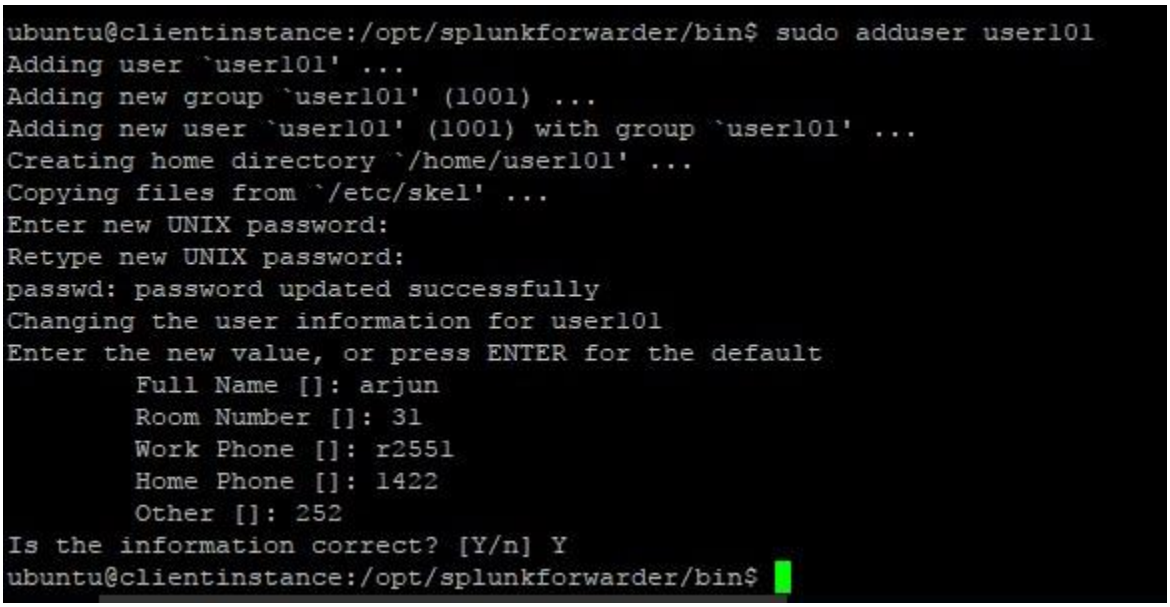
7. User Activity Analysis

1. Connect to the clientvm as mentioned above (SSH into the VM as shown in step 1 of how to Install Universal Forwarder on Linux).
2. Execute the following commands in the clientvm

sudo adduser user101

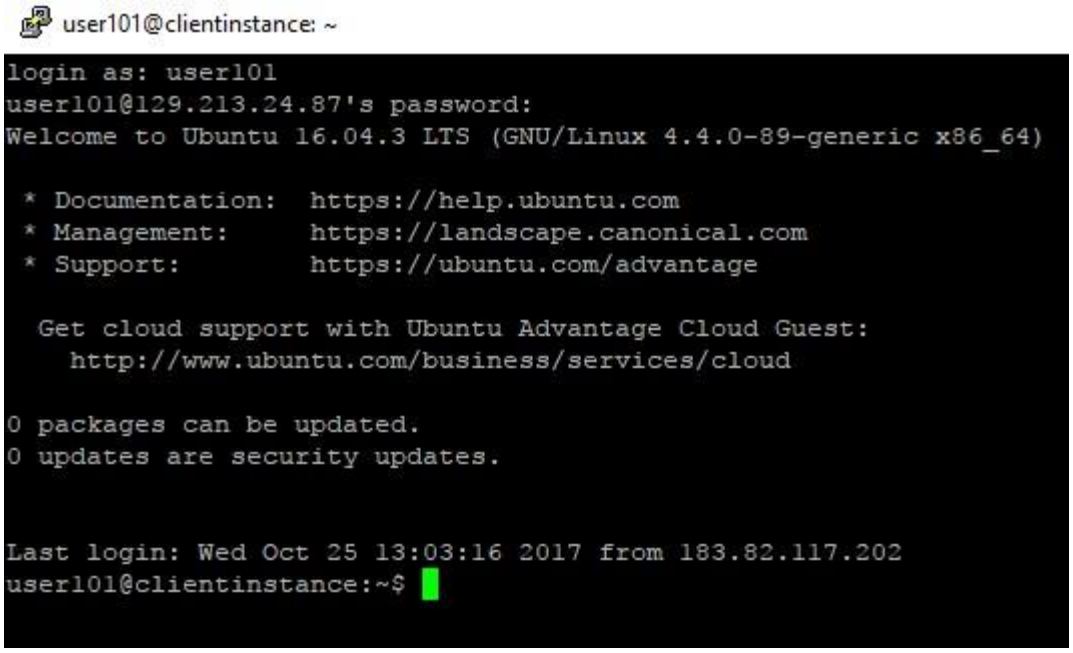
3. You will be prompted for the new password, enter the new password for the newly created user and hit enter. Then we will be prompted to Re Type the new password.

4. Repeat the above procedure for user102 and user 103 as shown in the below screenshot



8. SSH into the clientvm using the above users (user101, user102 and user103) and passwords.

9. Connect to the clientvm and execute the following commands as shown in the screenshot.

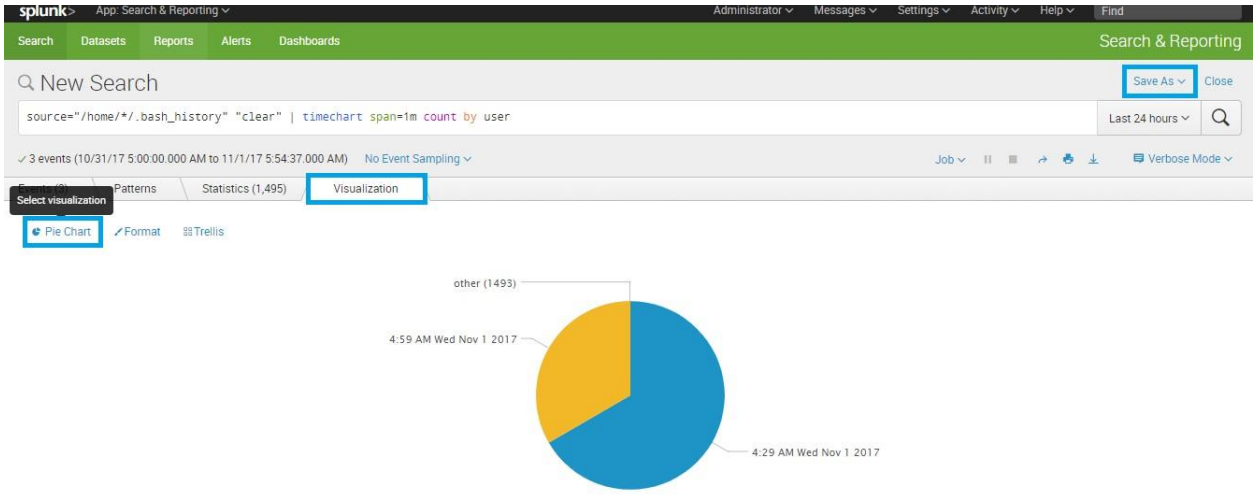


8. Generating Reports and showing them in Dashboard

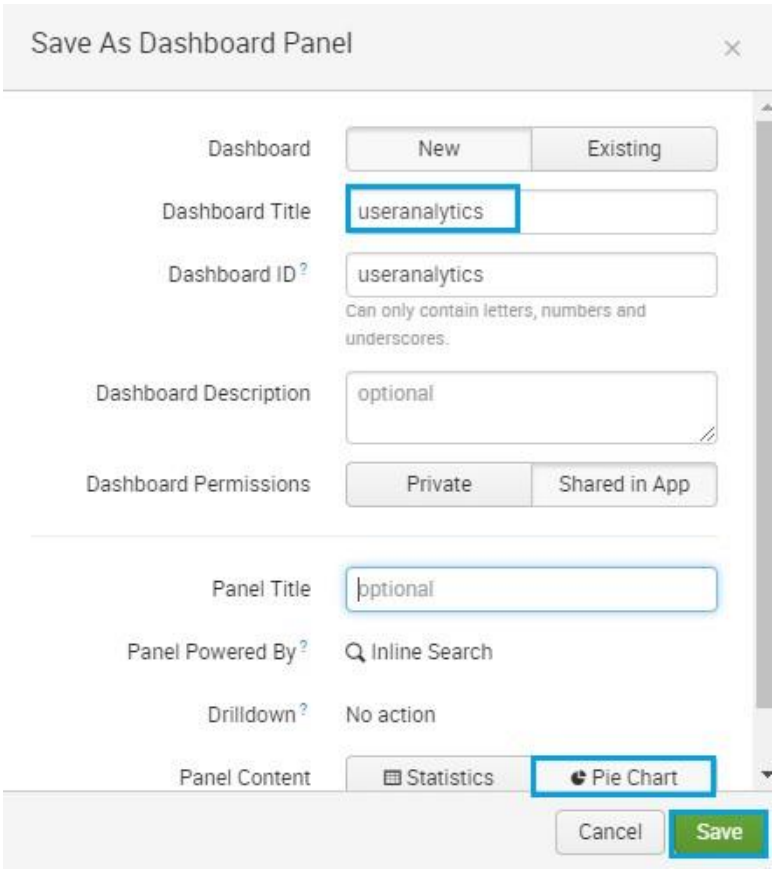
1. Now go to the Splunk web console as mentioned above in the section titled “Login into Splunk Enterprise”.
2. Click on the search and reporting tile which we can find on the left navigation.
3. Enter the following search command in the search box and hit the search icon. It will generate the events to find out how many times the user used "clear" command (we can replace clear by any other command to find its usage frequency)

   source="/home/*/.bash_history" "clear" | timechart span=1m count by user

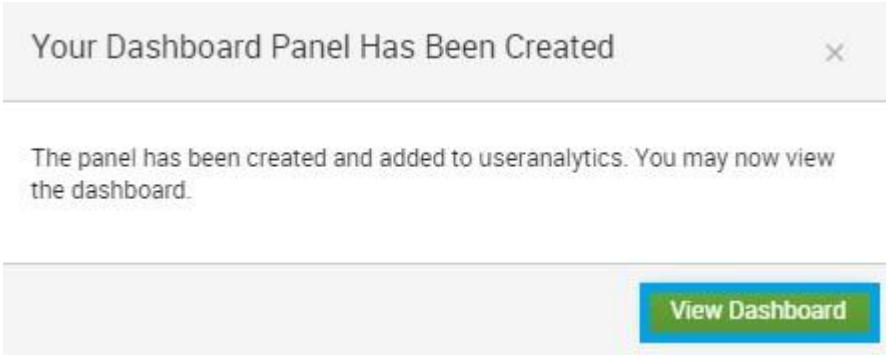
4. We will get the following screenshot



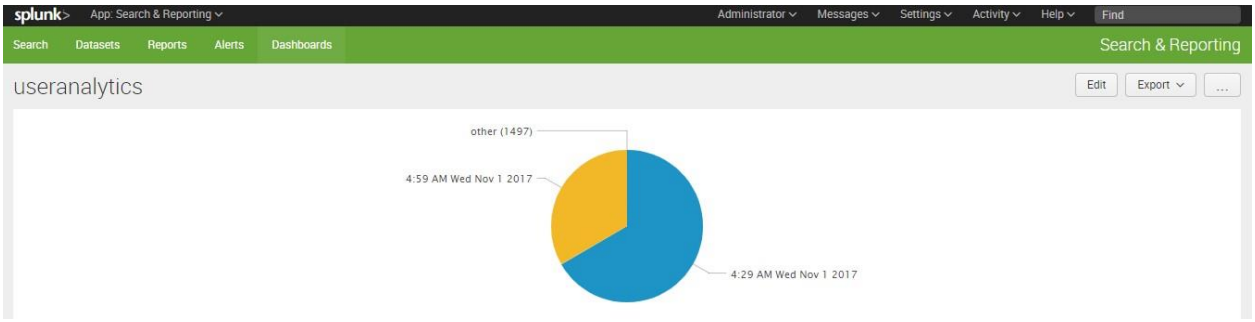
5. Click on **Save As** then select **Dashboard Panel** give any name in Title and select panel content as Pie Chart and click on **Save**



6. Click on **View Dashboard**



7. You can view the dashboard as below screen

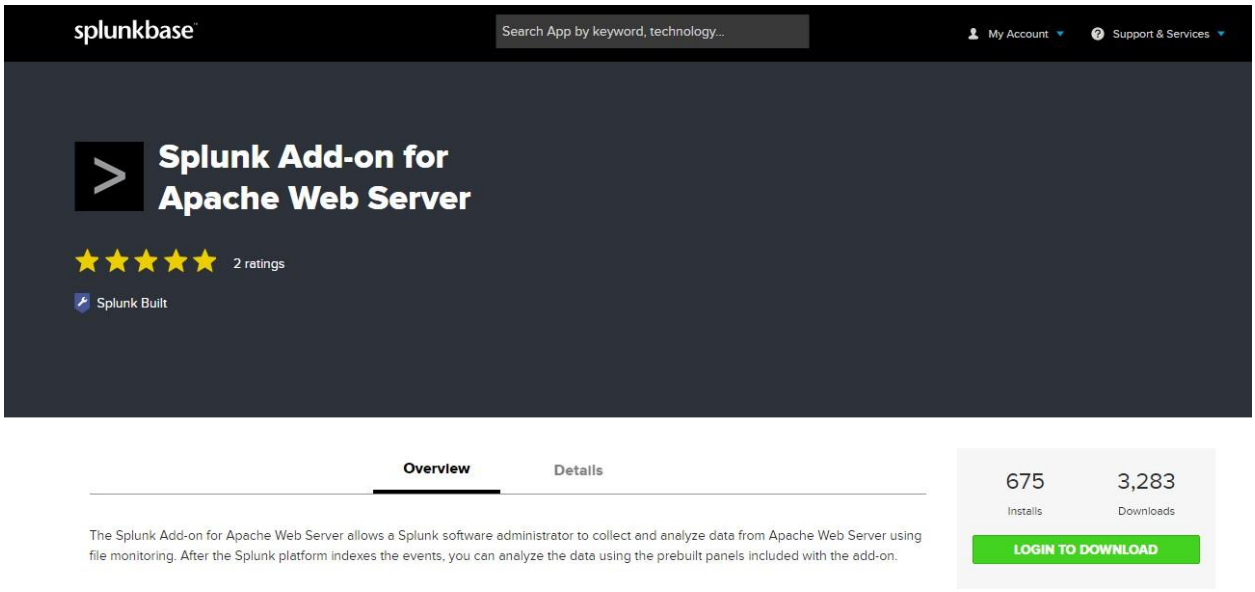


8. Installation of Splunk Add-on for Apache Web Server on Splunk.

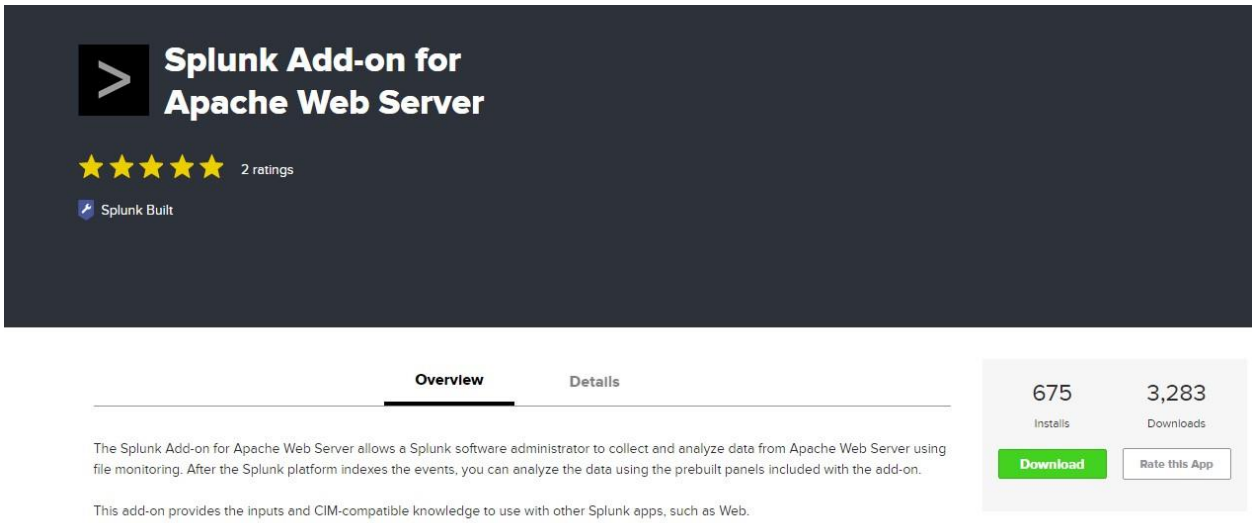
1. Download the Splunk Add-on for Apache web Server from below link. To download the Add-on, you need to create Splunk account.

   https://splunkbase.splunk.com/app/3186/

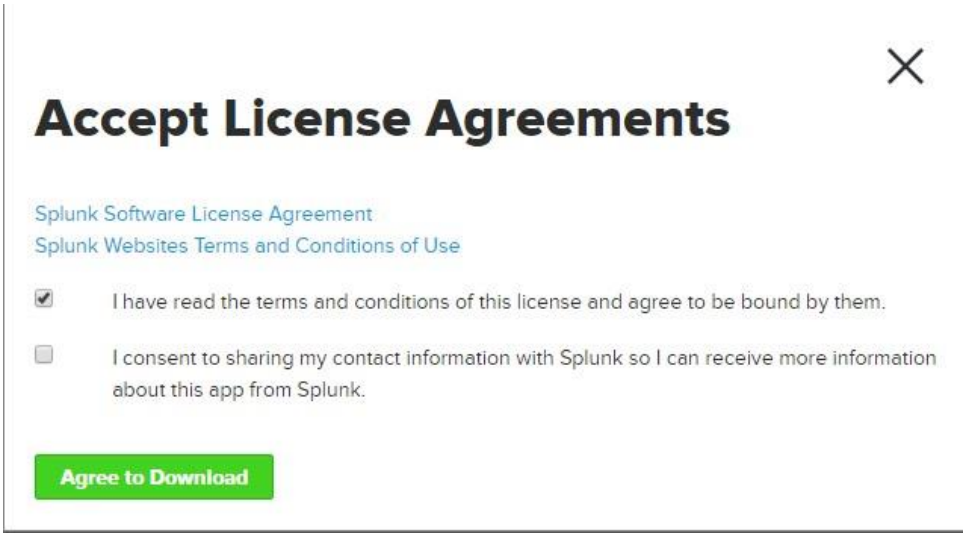
2. Click on Login to download the you will be prompted to login page, login with your Splunk account credentials.



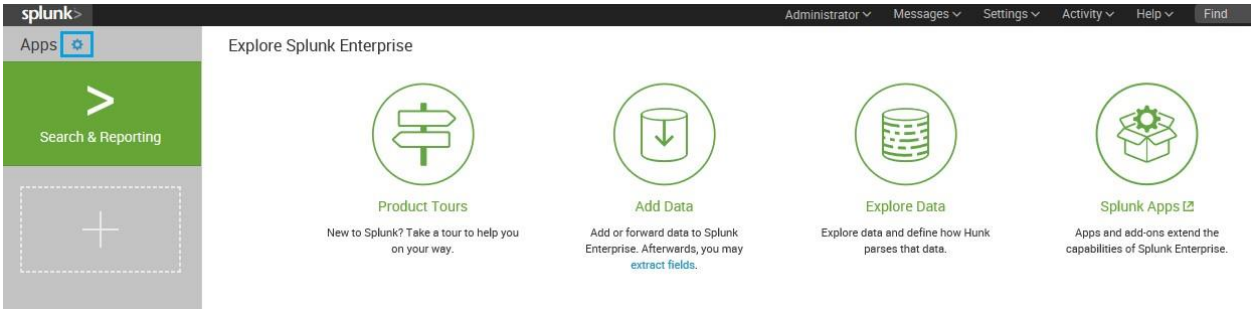
3. Click on download.



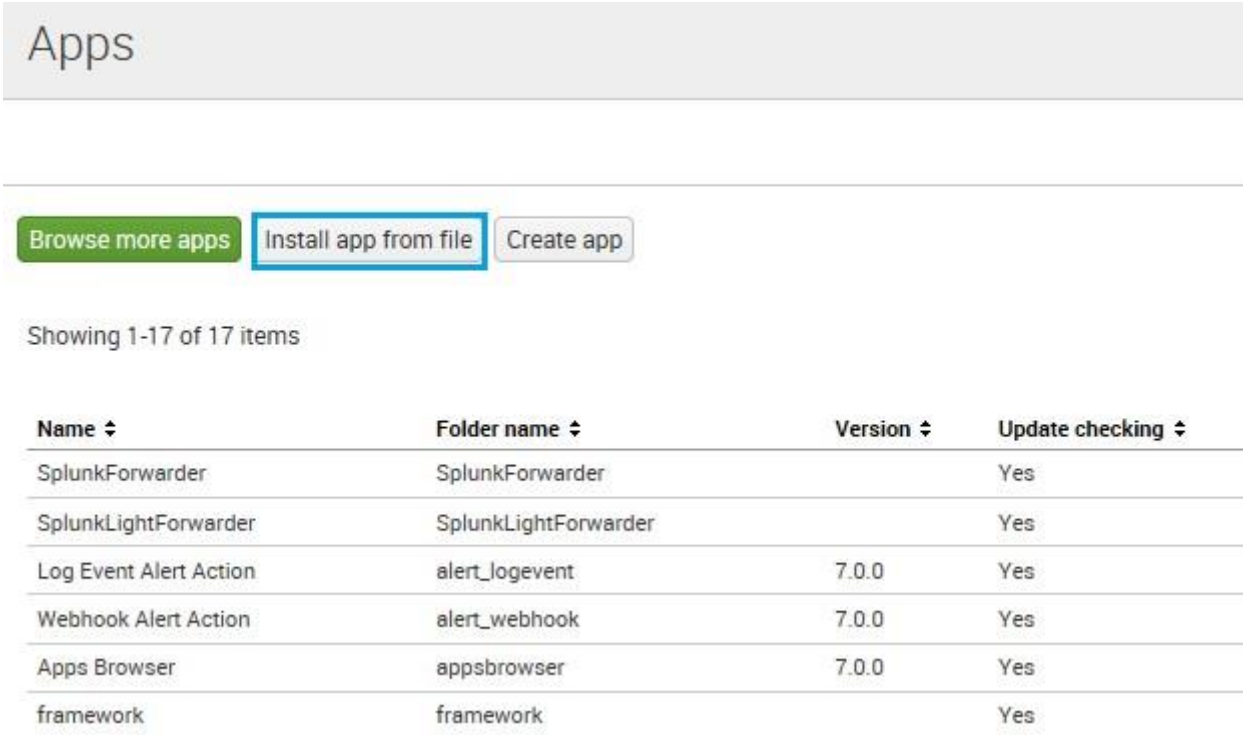
4. Accept the license agreements as shown below and click ok.



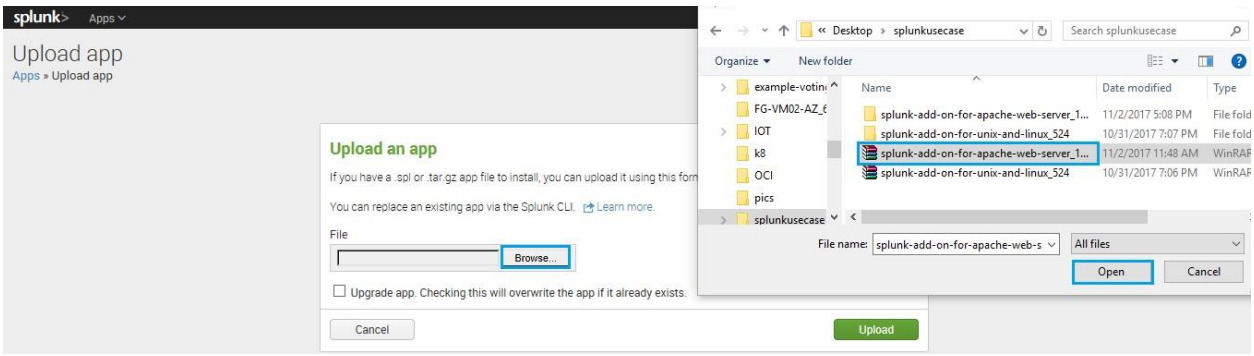
5. In Splunk Web UI, click on settings icon beside Apps as shown in below screen



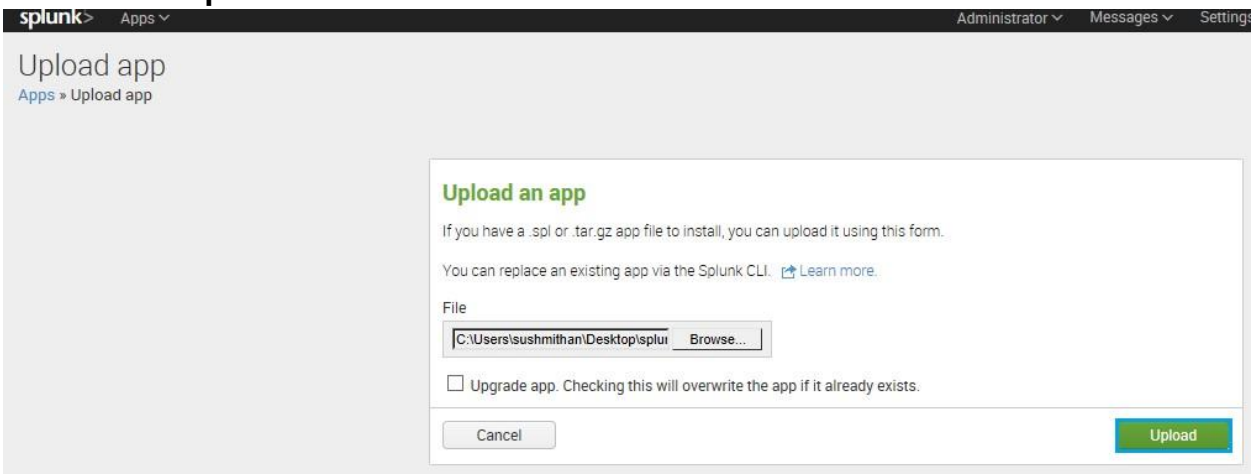
6. Click on **Install app from file**



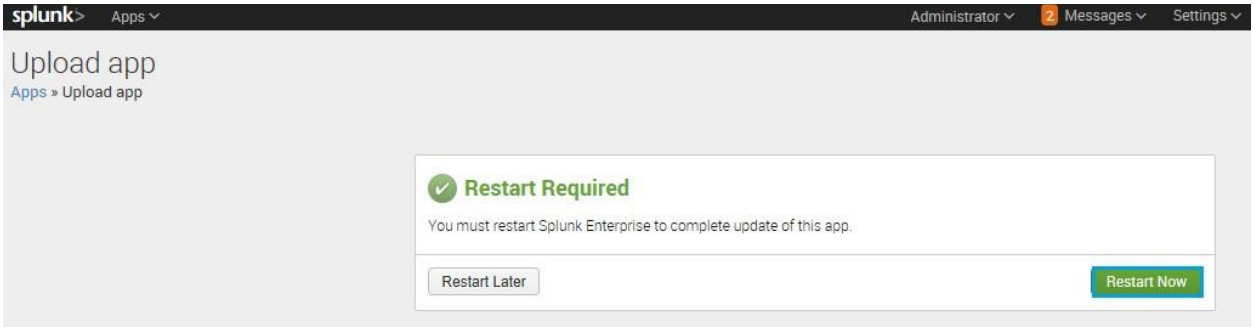
7. Click on Browse and select the downloaded Apache add-on RAR file and hit open.



8. Click on **Upload**

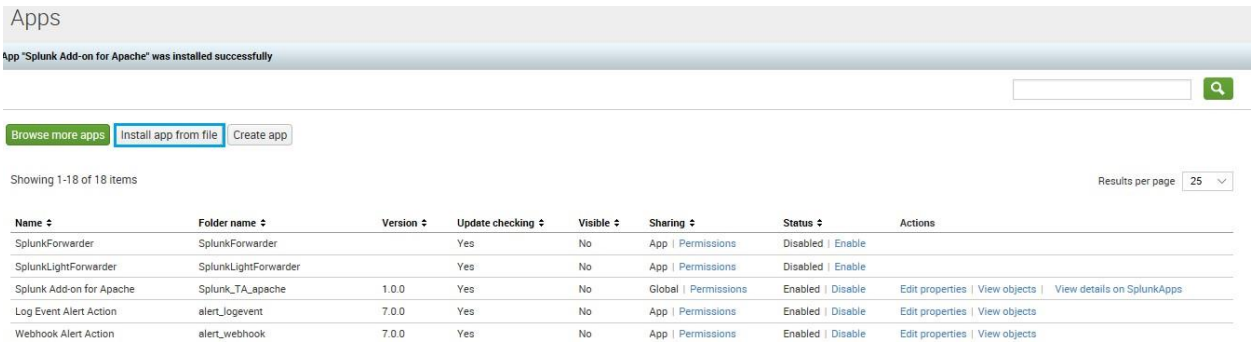


9. Once you uploaded the installation file, it will ask to restart, click on **Restart Now**



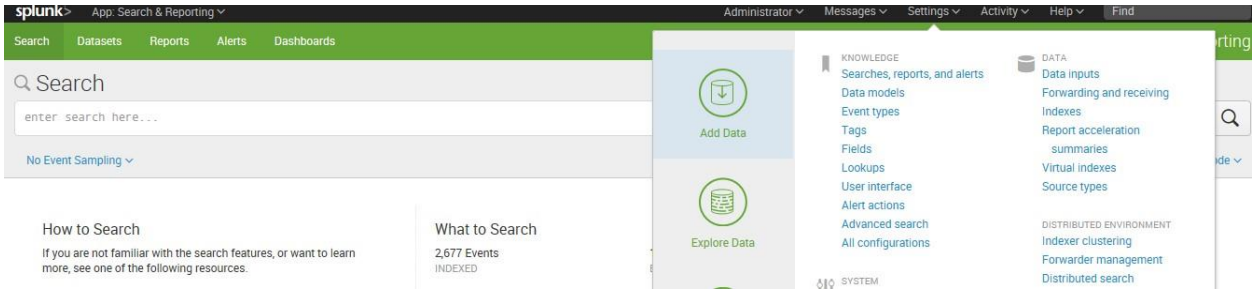
10. After restarting, it will automatically open Splunk web GUI to login again.

11. Click on Install app from file

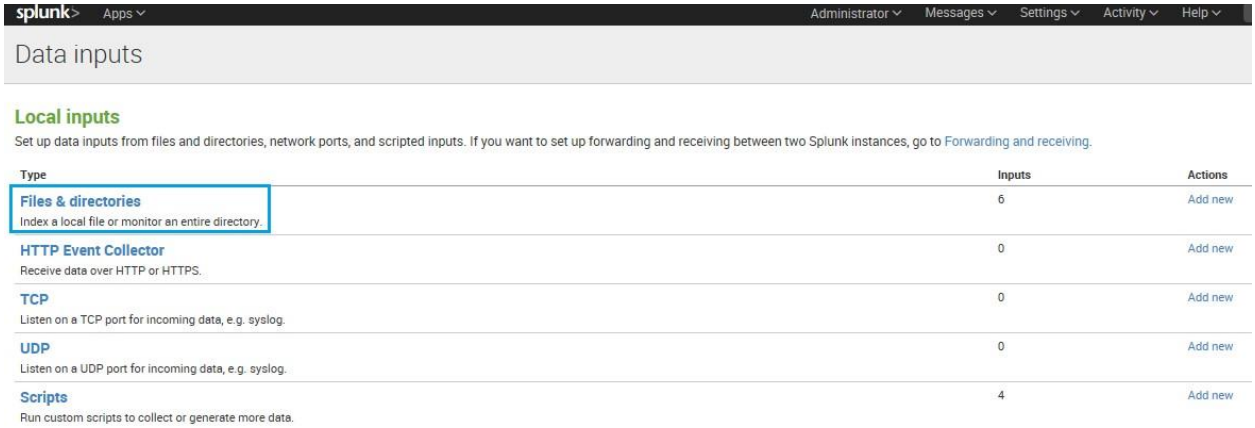


12. If you want to see your installation on dashboard click yes under visible and save the file

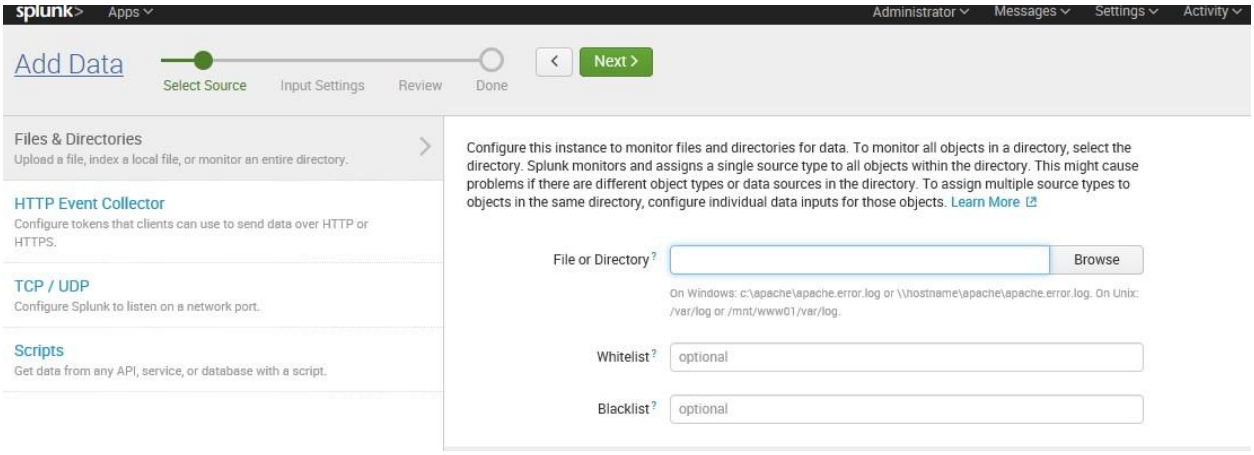
13. Navigate to **settings > Data inputs**



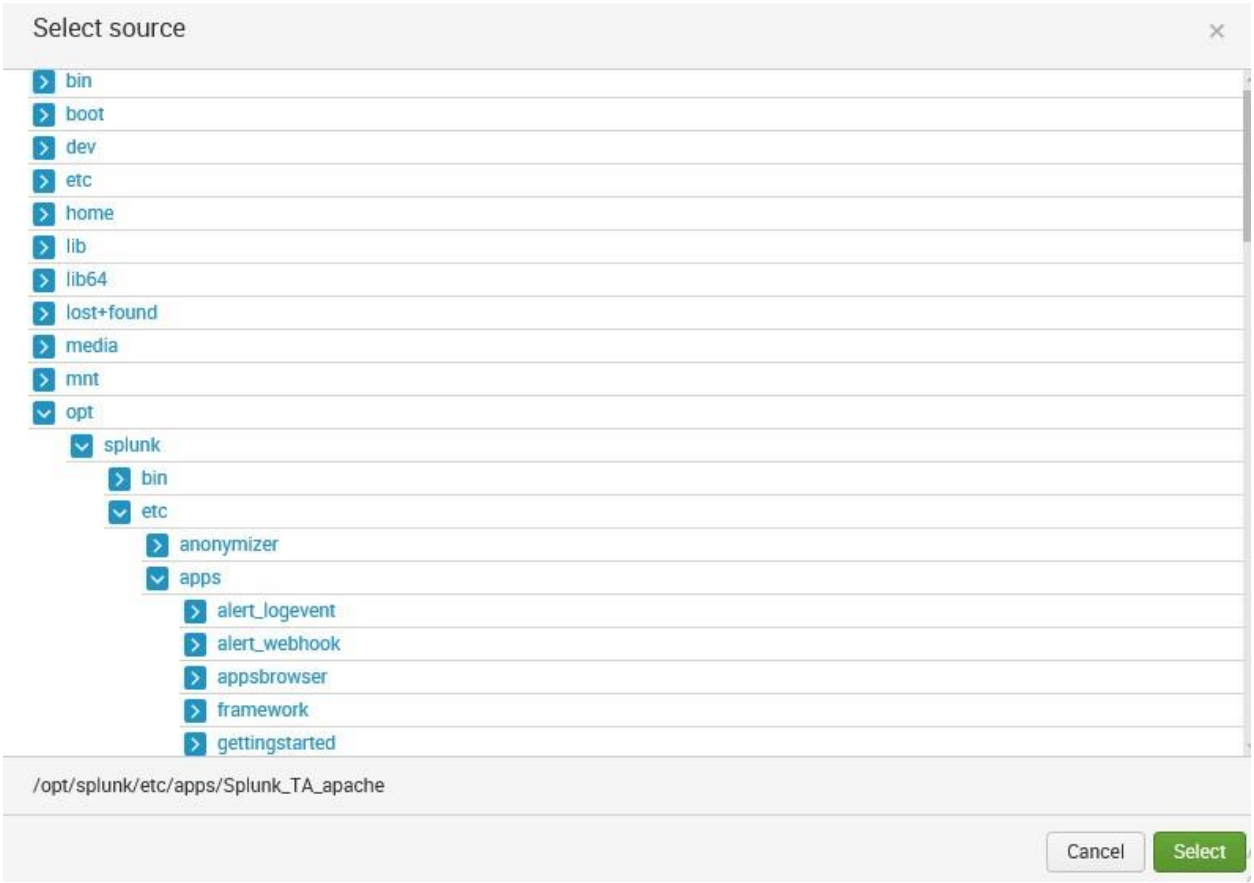
14. Select **File & directories**



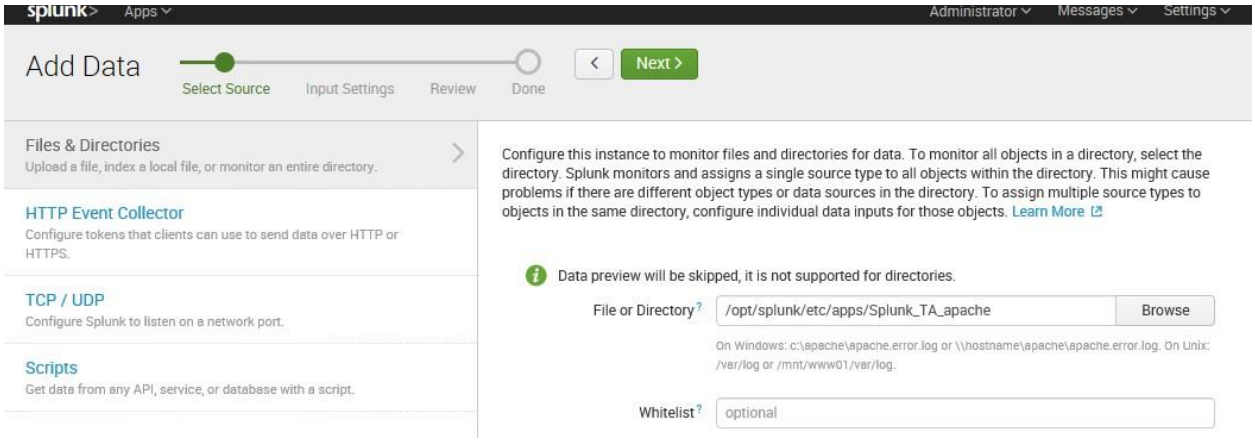
15. Click on **Browse** to select the path of file



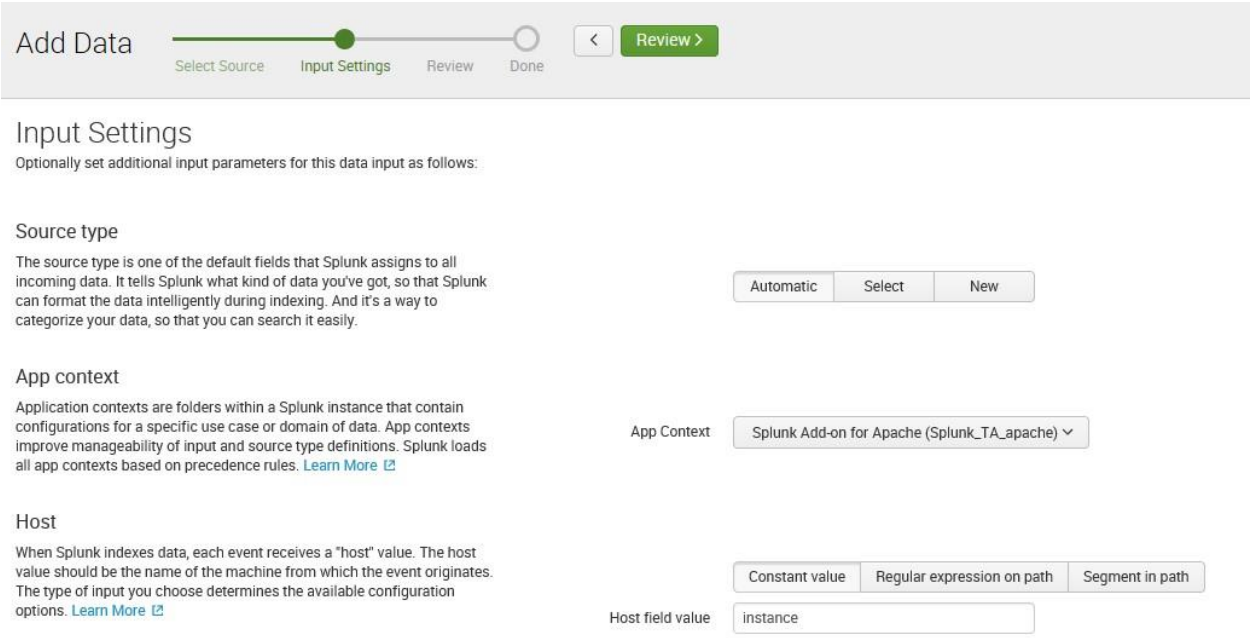
16. Select the path as **/opt/splunk/etc/apps/Splunk_TA_apache** and click on **select.**



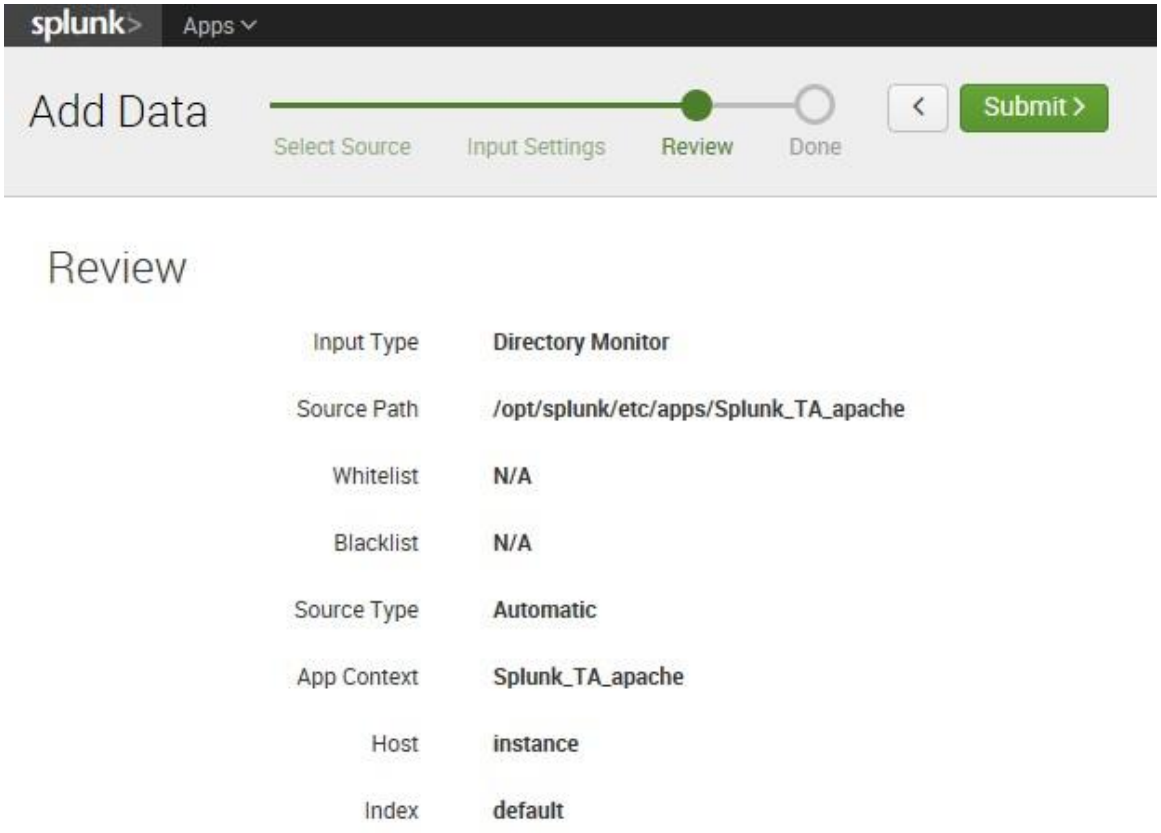
17. Click on **Next**



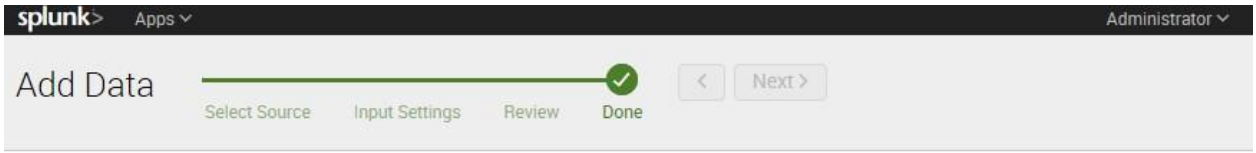
18. Under App context select **Splunk_TA_apache** and click on **Review.**

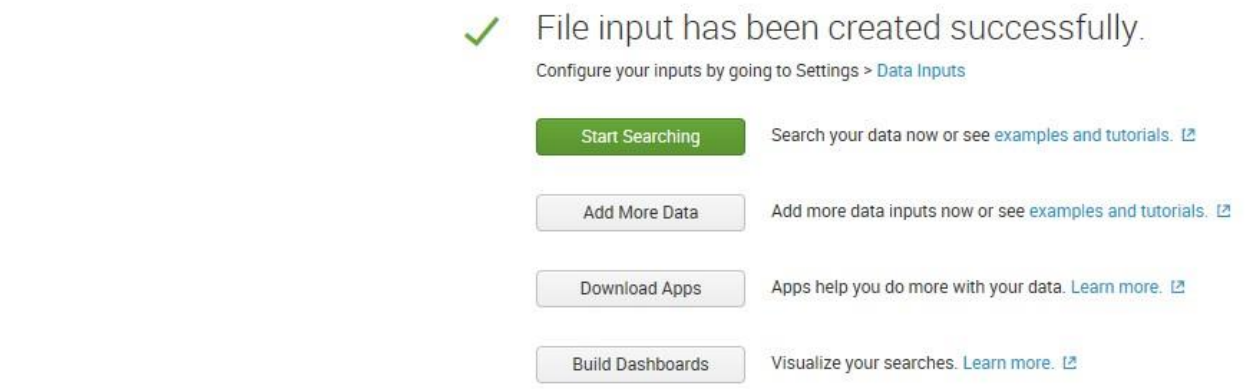


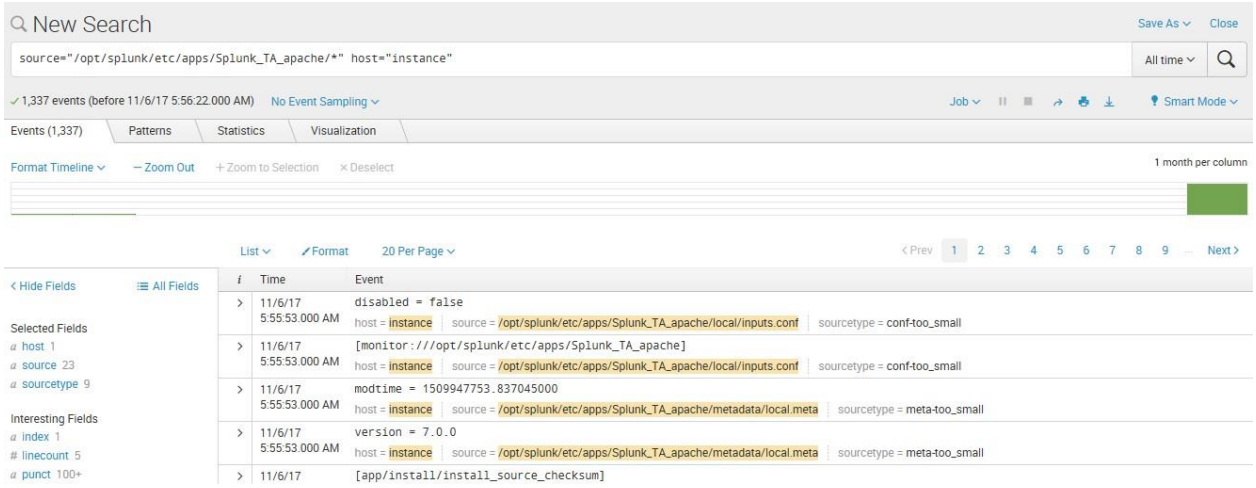
19. After reviewing click on **Submit.**



20. You can start searching your apache logs from here.


splunk>
Apps
Administrator
Add Data
Select Source
Input Settings
Review
Done
Next


File input has been created successfully.
Configure your inputs by going to Settings > Data Inputs
Start Searching
Search your data now or see examples and tutorials.
Add More Data
Add more data inputs now or see examples and tutorials.
Download Apps
Apps help you do more with your data. Learn more.
Build Dashboards
Visualize your searches. Learn more.


New Search
Save As
Close
source="/opt/splunk/etc/apps/Splunk_TA_apache/*" host="instance"
All time
1,337 events (before 11/6/17 5:56:22.000 AM)
No Event Sampling
Job
Smart Mode
Events (1,337)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 month per column
List
Format
20 Per Page
Prev
1
2
3
4
5
6
7
8
9
Next
Hide Fields
All Fields
Selected Fields
host 1
source 23
sourcetype 9
Interesting Fields
index 1
linecount 5
punct 100+
Time
Event
11/6/17 5:55:53.000 AM
disabled = false
host = instance
source = /opt/splunk/etc/apps/Splunk_TA_apache/local/inputs.conf
sourcetype = conf-too_small
11/6/17 5:55:53.000 AM
[monitor:///opt/splunk/etc/apps/Splunk_TA_apache]
host = instance
source = /opt/splunk/etc/apps/Splunk_TA_apache/local/inputs.conf
sourcetype = conf-too_small
11/6/17 5:55:53.000 AM
modtime = 1509947753.837045000
host = instance
source = /opt/splunk/etc/apps/Splunk_TA_apache/metadata/local.meta
sourcetype = meta-too_small
11/6/17 5:55:53.000 AM
version = 7.0.0
host = instance
source = /opt/splunk/etc/apps/Splunk_TA_apache/metadata/local.meta
sourcetype = meta-too_small
11/6/17
[app/install/install_source_checksum]