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:

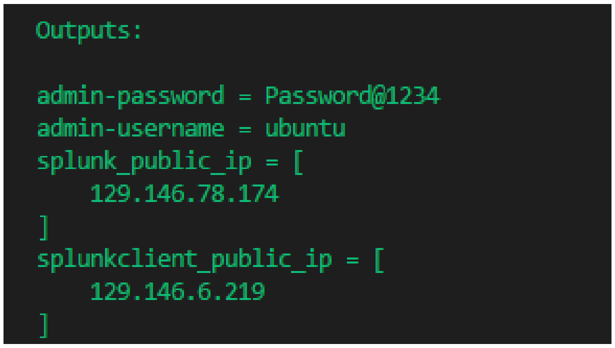
- Tagging of metadata (source, source type, and host)
- Configurable buffering
- Data compression Splunk Enterprise
- SSL security
- Use of any available network ports
- Running scripted inputs locally

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

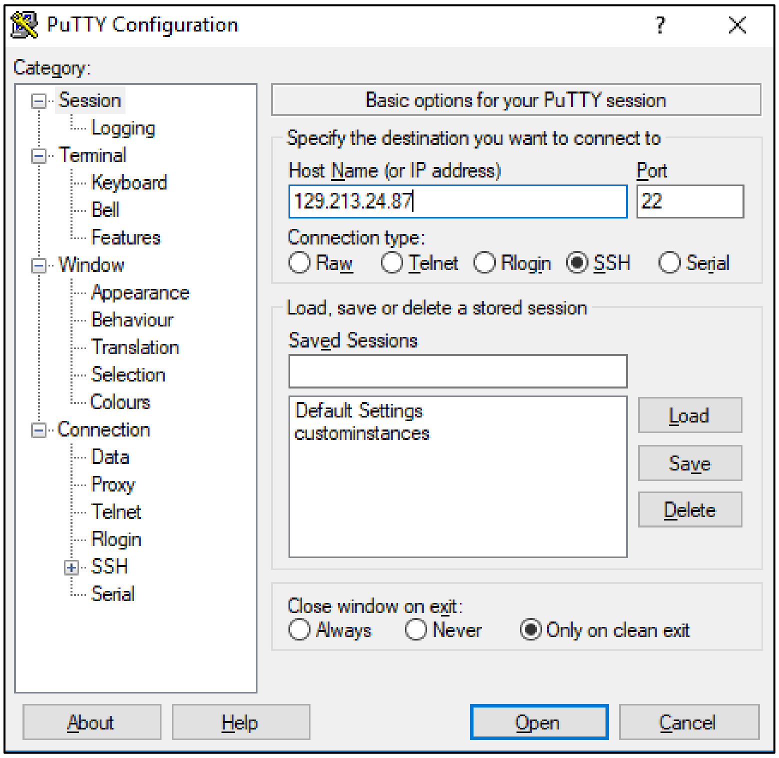
4. Installing the universal forwarder on Linux

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.



```
Outputs:

admin-password = Password@1234
admin-username = ubuntu
splunk_public_ip = [
    129.146.78.174
]
splunkclient_public_ip = [
    129.146.6.219
]
```



Specify the destination you want to connect to

Host Name (or IP address): 129.213.24.87

Port: 22

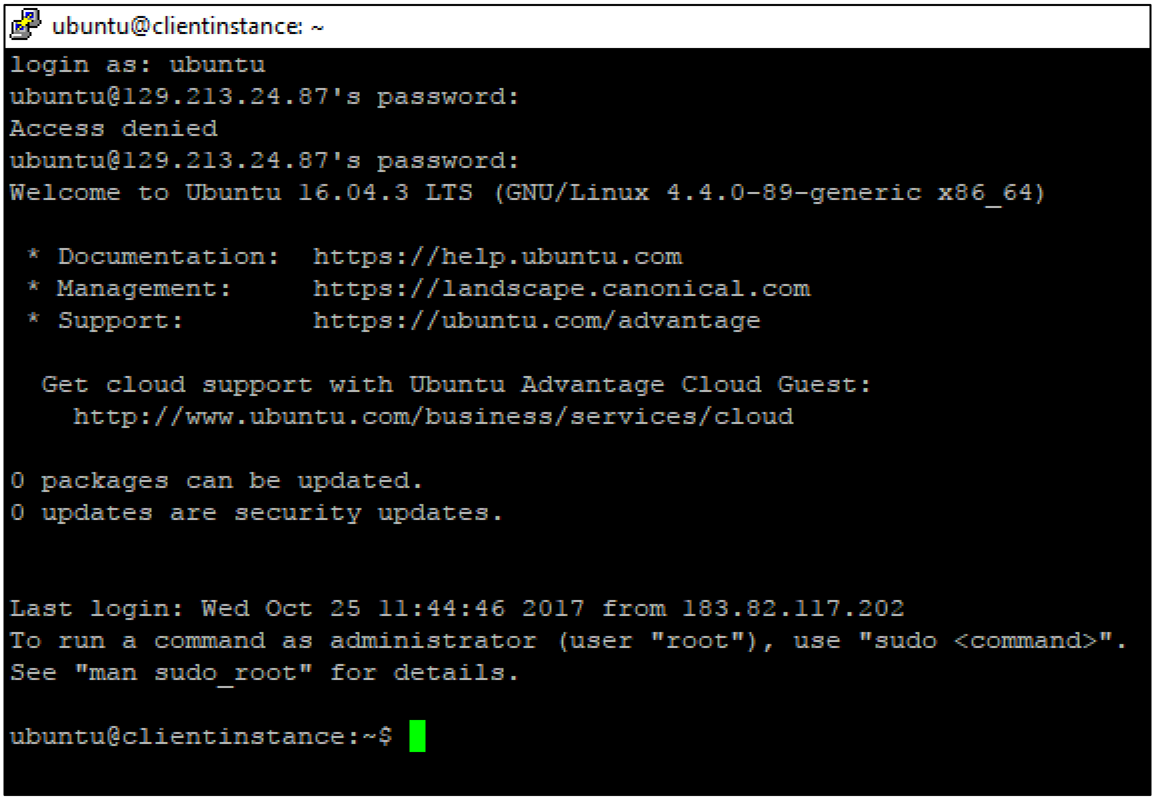
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions:

Default Settings
custominstances

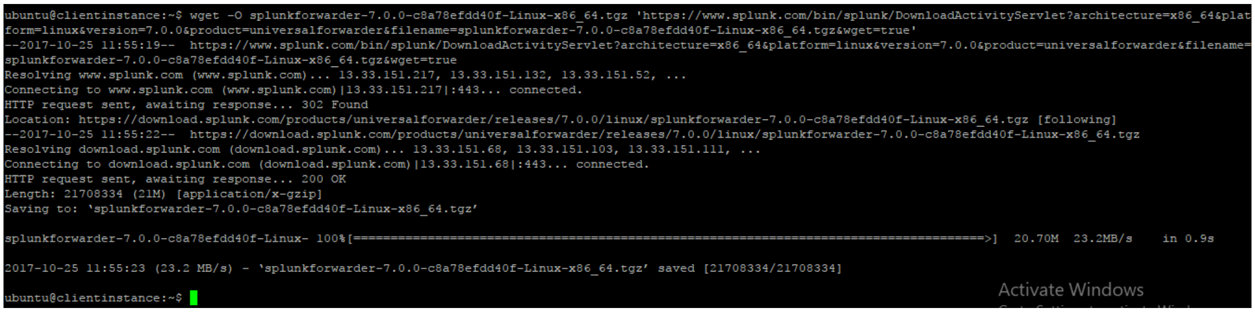
Close window on exit: ○ Always ○ Never ● Only on clean exit



```
login as: ubuntu
ubuntu@129.213.24.87's password:
Access denied
ubuntu@129.213.24.87's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-89-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  Get cloud support with Ubuntu Advantage Cloud Guest:
    http://www.ubuntu.com/business/services/cloud

0 packages can be updated.
0 updates are security updates.


Last login: Wed Oct 25 11:44:46 2017 from 183.82.117.202
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@clientinstance:~$
```

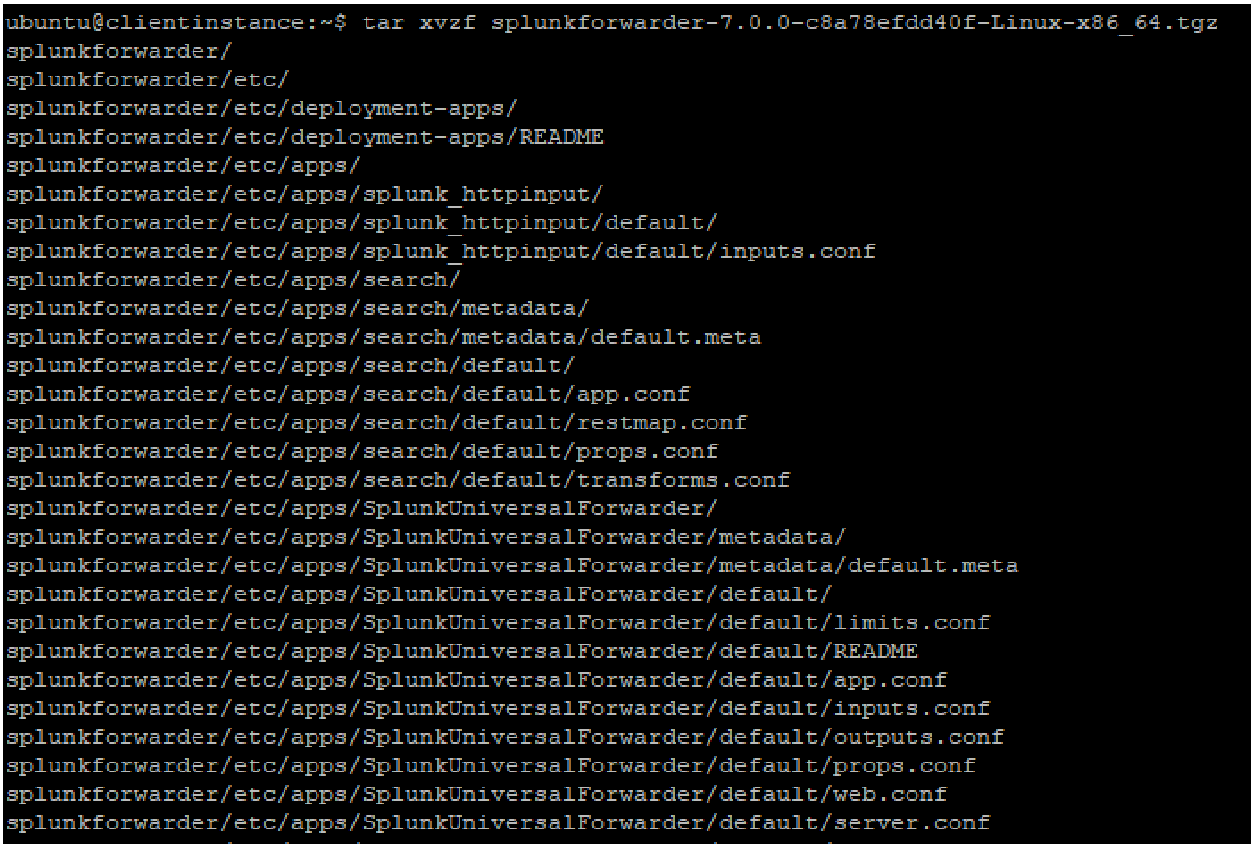
2. Download the latest Splunk package on the client VM by using the following command

   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'



```
ubuntu@clientinstance:~$ wget -O splunkforwarder-7.0.0-c8a78efdd40f-Linux-x86_64.tgz 'https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_64&plat
form=linux&version=7.0.0&product=universalforwarder&filename=splunkforwarder-7.0.0-c8a78efdd40f-Linux-x86_64.tgz&wget=true'
--2017-10-25 11:55:19--  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
Resolving www.splunk.com (www.splunk.com)... 13.33.151.217, 13.33.151.132, 13.33.151.52, ...
Connecting to www.splunk.com (www.splunk.com)|13.33.151.217|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://download.splunk.com/products/universalforwarder/releases/7.0.0/linux/splunkforwarder-7.0.0-c8a78efdd40f-Linux-x86_64.tgz [following]
--2017-10-25 11:55:22--  https://download.splunk.com/products/universalforwarder/releases/7.0.0/linux/splunkforwarder-7.0.0-c8a78efdd40f-Linux-x86_64.tgz
Resolving download.splunk.com (download.splunk.com)... 13.33.151.68, 13.33.151.103, 13.33.151.111, ...
Connecting to download.splunk.com (download.splunk.com)|13.33.151.68|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 21708334 (21M) [application/x-gzip]
Saving to: 'splunkforwarder-7.0.0-c8a78efdd40f-Linux-x86_64.tgz'

splunkforwarder-7.0.0-c8a78efdd40f-Linux- 100%[=====================================================================================>]  20.70M  23.2MB/s    in 0.9s

2017-10-25 11:55:23 (23.2 MB/s) - 'splunkforwarder-7.0.0-c8a78efdd40f-Linux-x86_64.tgz' saved [21708334/21708334]

ubuntu@clientinstance:~$
```

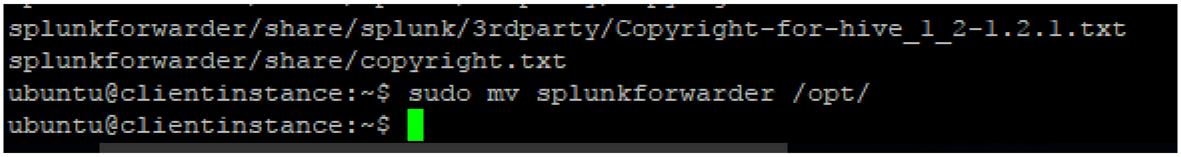
3. Extract the files from zip folder
   tar xvzf splunkforwarder-7.0.0-c8a78efdd40f-Linux-x86_64.tgz



```
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

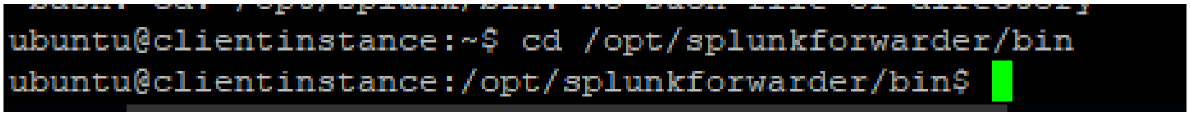
   sudo mv splunkforwarder /opt/



```
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

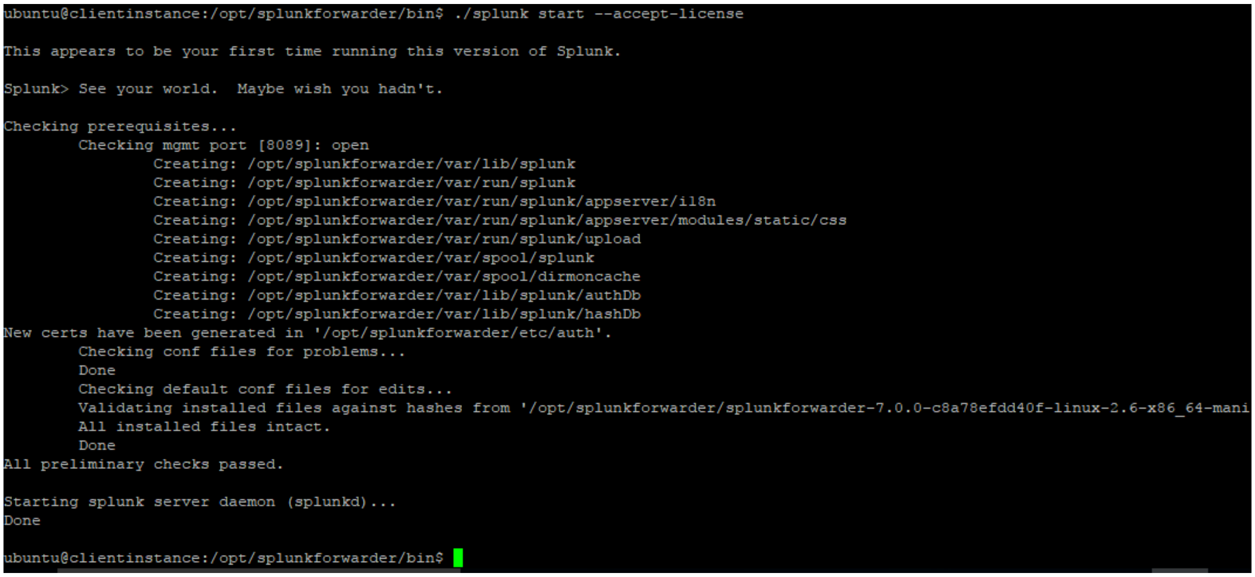
   cd /opt/splunkforwarder/bin



```
bash: cd: /opt/splunk/bin: No such file or directory
ubuntu@clientinstance:~$ cd /opt/splunkforwarder/bin
ubuntu@clientinstance:/opt/splunkforwarder/bin$
```

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

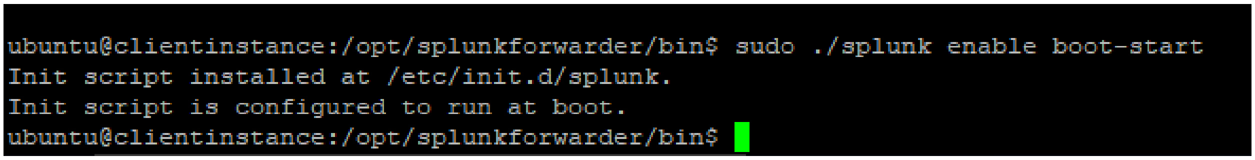
   ./splunk start --accept-license



```
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.

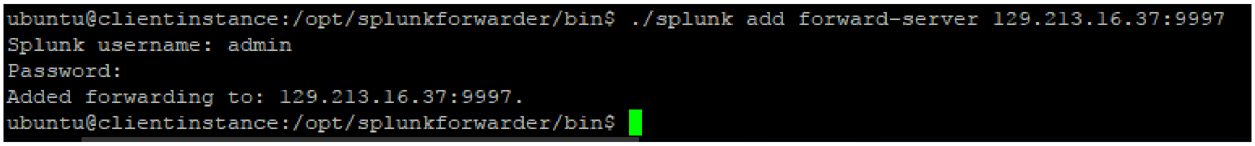
   sudo ./splunk enable boot-start



```
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-fqdn>: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 test-drive launch page named Splunk domain name and 9997 is the receiving port.

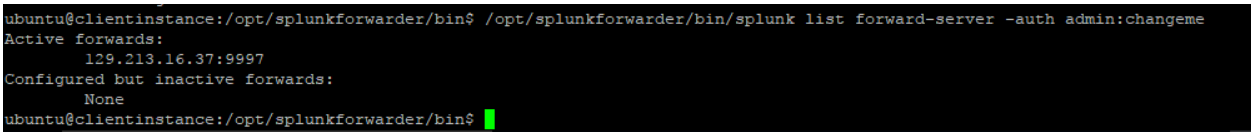
9. After executing the above command, it will ask for Splunk username and password are

   Usern ame: admin

Password: changeme

10. Configure Forwarder connection to Index Server.

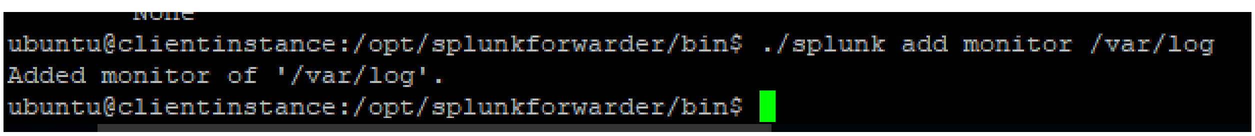
    /opt/splunkforwarder/bin/splunk list forward-server -auth admin:changeme



```
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

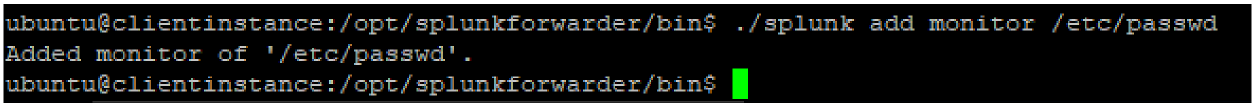
    ./splunk add monitor /var/log



```
        None
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.

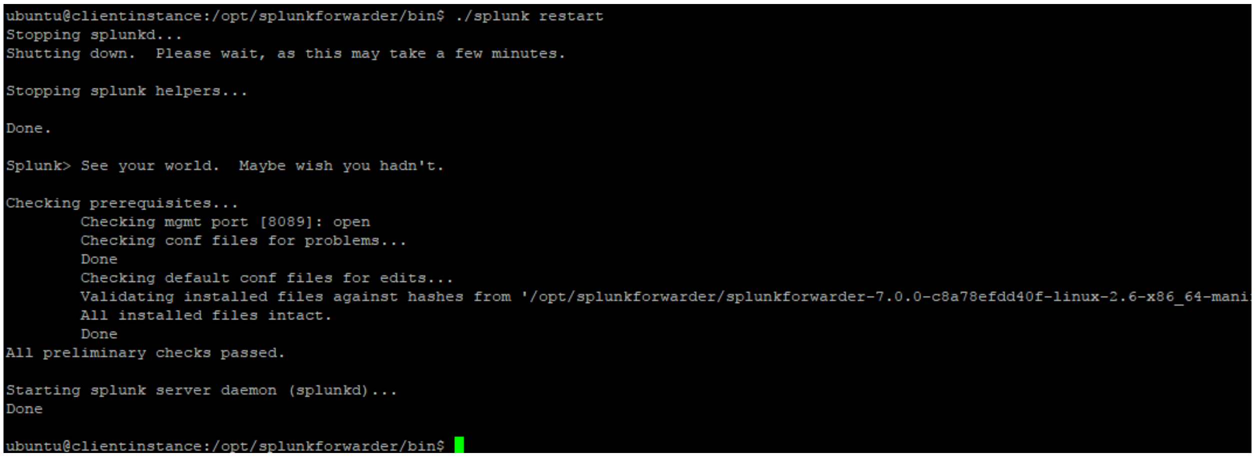
    ./splunk add monitor /etc/passwd



```
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

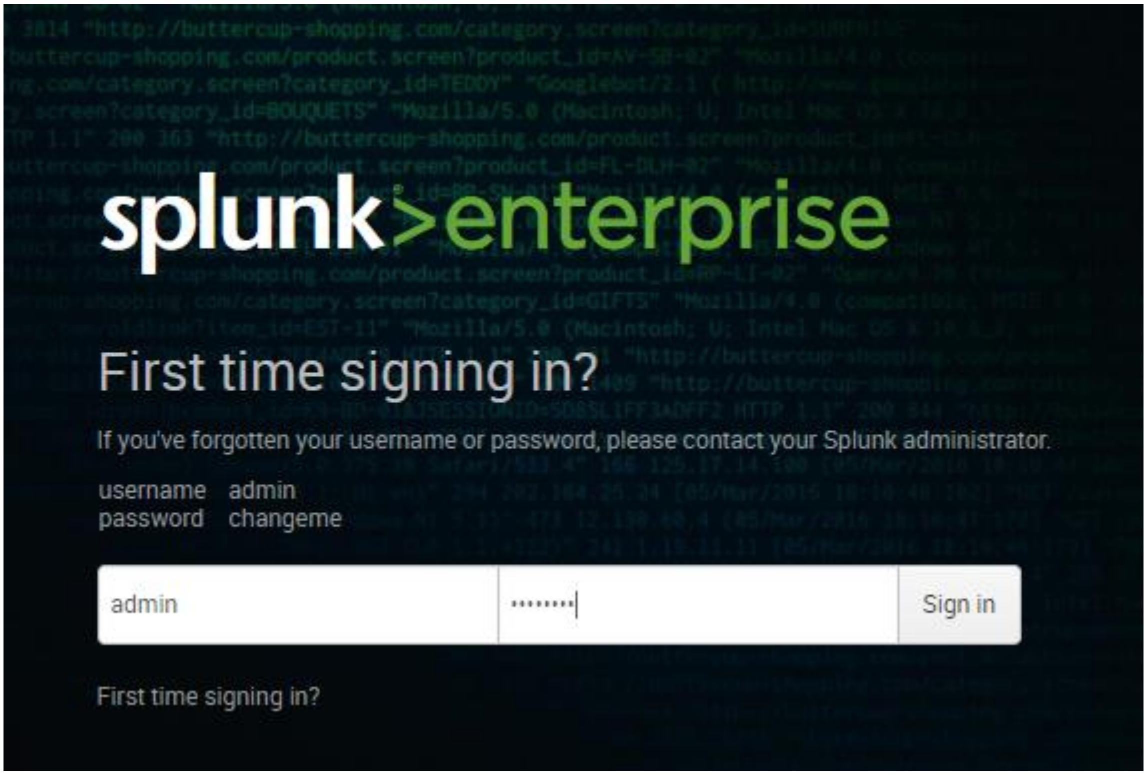


```
ubuntu@clientinstance:/opt/splunkforwarder/bin$ ./splunk restart
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.

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, you can find web url in testdrive launch page named Splunk Web url



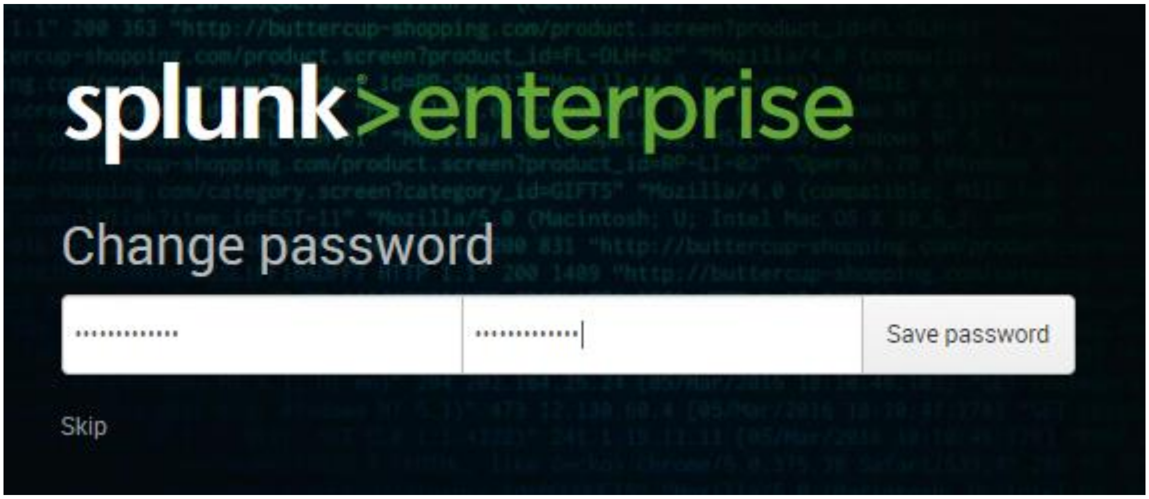
First time signing in?

If you've forgotten your username or password, please contact your Splunk administrator.

username admin
password changeme

admin ••••••••

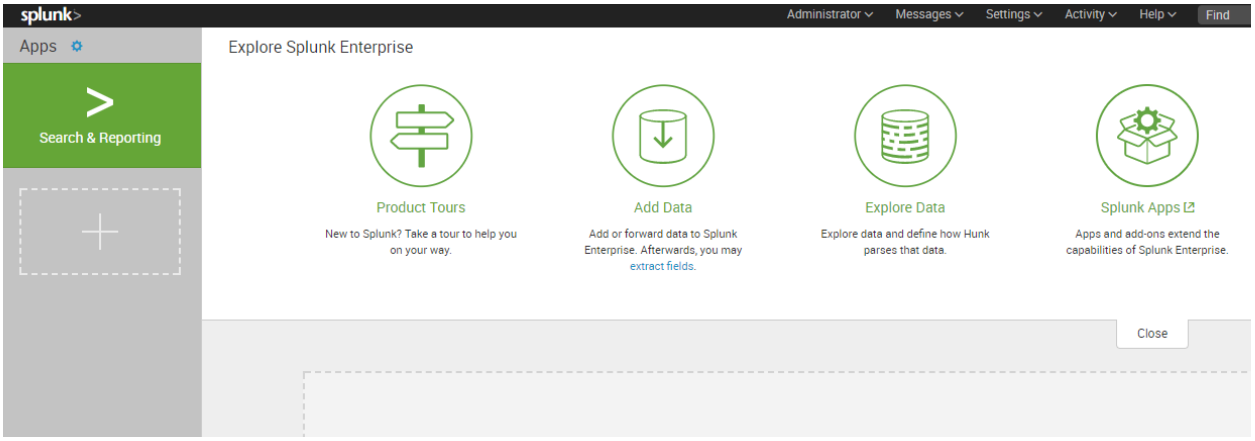
2. You can change your password.



Change password

•••••••••••••• ••••••••••••••

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



Explore Splunk Enterprise

Product Tours
New to Splunk? Take a tour to help you on your way.

Add Data
Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

Explore Data
Explore data and define how Hunk parses that data.

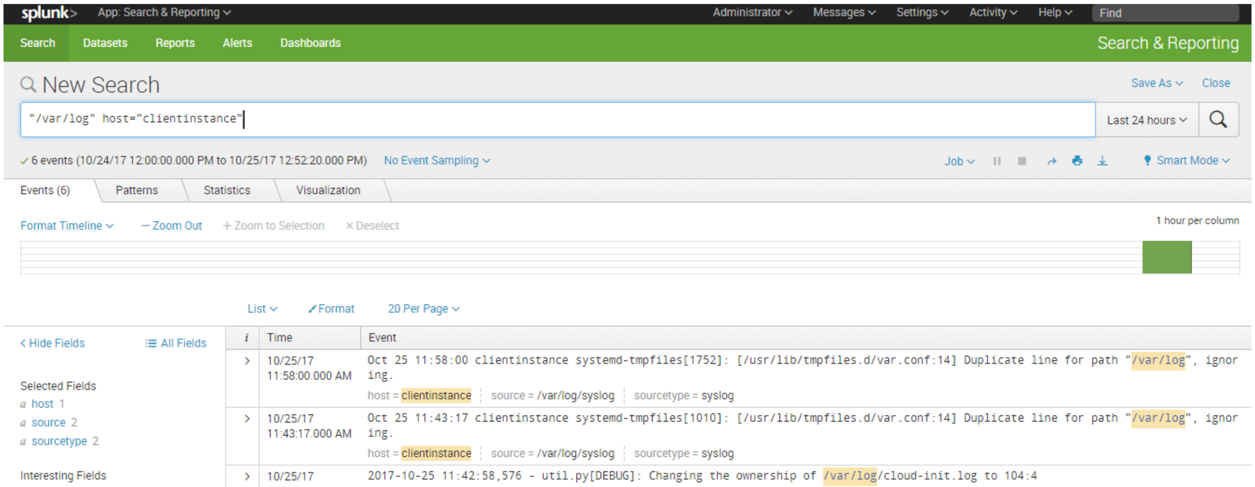
Splunk Apps
Apps and add-ons extend the capabilities of Splunk Enterprise.

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.



```
"/var/log" host="clientinstance"
```

✓ 6 events (10/24/17 12:00:00.000 PM to 10/25/17 12:52:20.000 PM)

i	Time	Event
>	10/25/17 11:58:00.000 AM	Oct 25 11:58:00 clientinstance systemd-tmpfiles[1752]: [/usr/lib/tmpfiles.d/var.conf:14] Duplicate line for path "/var/log", ignoring. host = clientinstance ¦ source = /var/log/syslog ¦ sourcetype = syslog
>	10/25/17 11:43:17.000 AM	Oct 25 11:43:17 clientinstance systemd-tmpfiles[1010]: [/usr/lib/tmpfiles.d/var.conf:14] Duplicate line for path "/var/log", ignoring. host = clientinstance ¦ source = /var/log/syslog ¦ sourcetype = syslog
>	10/25/17	2017-10-25 11:42:58,576 - util.py[DEBUG]: Changing the ownership of /var/log/cloud-init.log to 104:4

7. User Activity Analysis

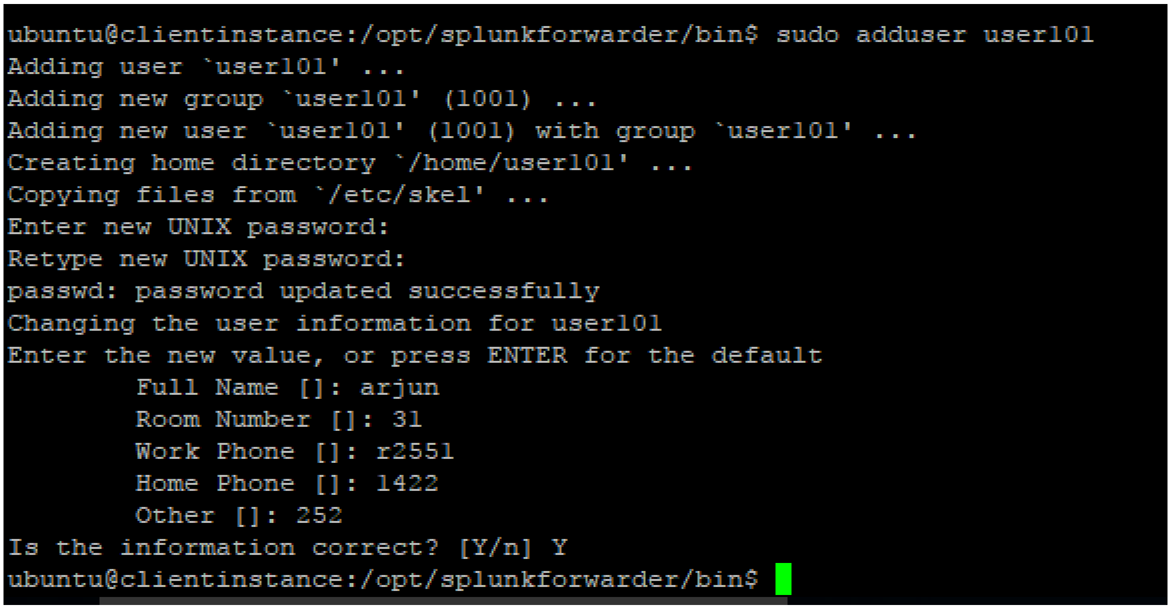
1. Connect to the clientvm as mentioned above (SSH into the VM as shown in step 1 of how to Install Universal Forwarder on Linux).

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.

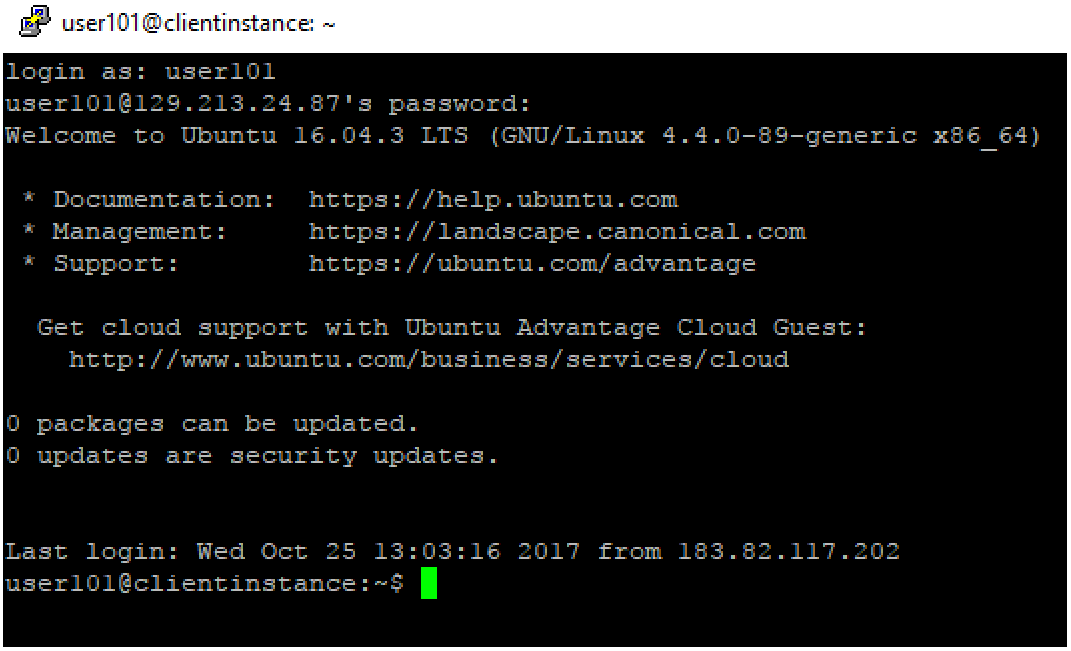
4. Repeat the above procedure for user102 and user 103 as shown in the below screenshot



```
ubuntu@clientinstance:/opt/splunkforwarder/bin$ sudo adduser user101
Adding user `user101' ...
Adding new group `user101' (1001) ...
Adding new user `user101' (1001) with group `user101' ...
Creating home directory `/home/user101' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for user101
Enter the new value, or press ENTER for the default
        Full Name []: arjun
        Room Number []: 31
        Work Phone []: r2551
        Home Phone []: 1422
        Other []: 252
Is the information correct? [Y/n] Y
ubuntu@clientinstance:/opt/splunkforwarder/bin$
```

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.



user101@clientinstance: ~

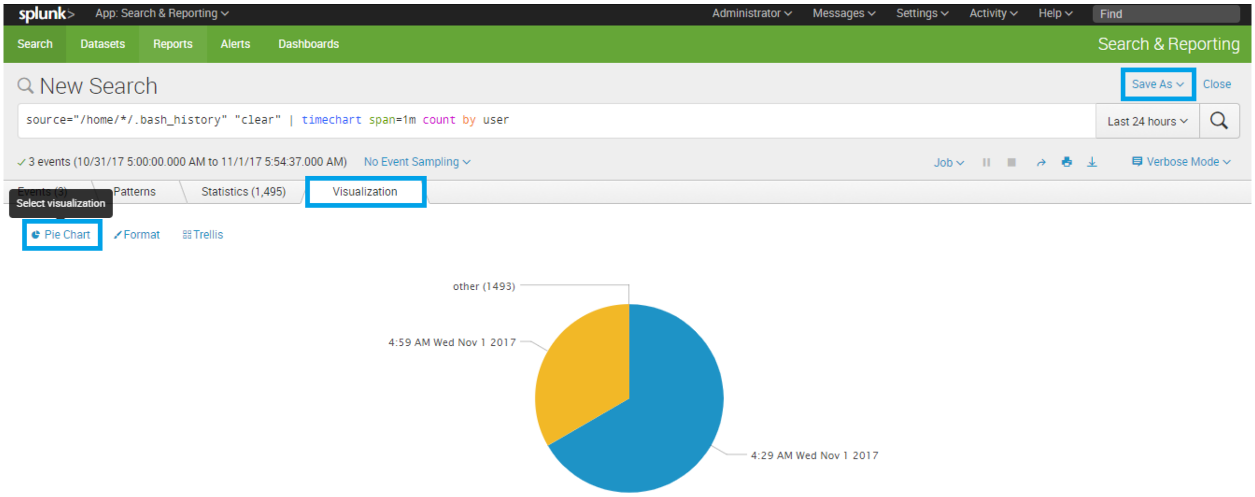
```
login as: user101
user101@129.213.24.87's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-89-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  Get cloud support with Ubuntu Advantage Cloud Guest:
    http://www.ubuntu.com/business/services/cloud

0 packages can be updated.
0 updates are security updates.


Last login: Wed Oct 25 13:03:16 2017 from 183.82.117.202
user101@clientinstance:~$
```

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

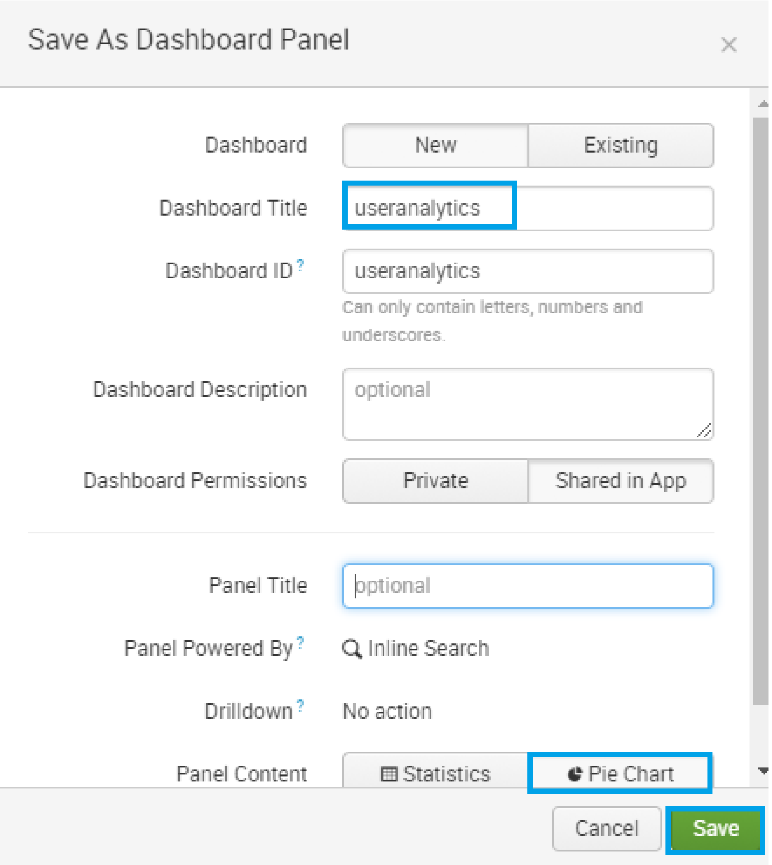
4. We will get the following screenshot



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

✓ 3 events (10/31/17 5:00:00.000 AM to 11/1/17 5:54:37.000 AM) No Event Sampling

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**



Dashboard: New | Existing

Dashboard Title: useranalytics

Dashboard ID ?: useranalytics

Can only contain letters, numbers and underscores.

Dashboard Description: optional

Dashboard Permissions: Private | Shared in App

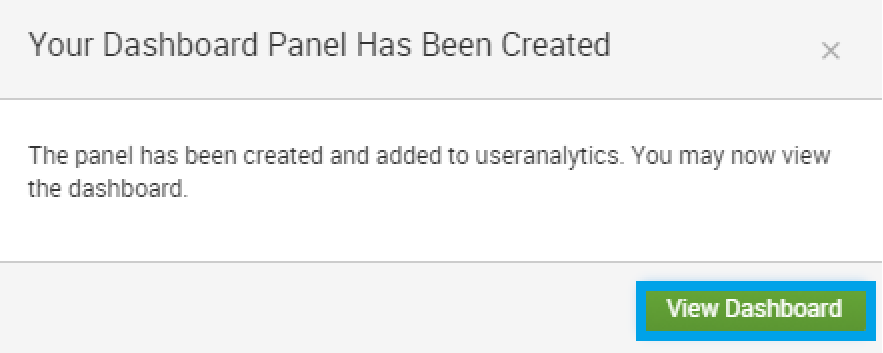
Panel Title: optional

Panel Powered By ?: Inline Search

Drilldown ?: No action

Panel Content: Statistics | Pie Chart

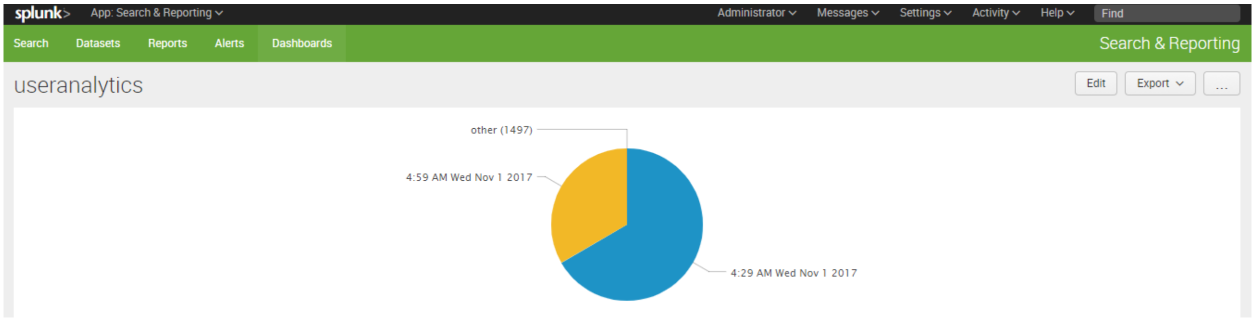
6. Click on **View Dashboard**



Your Dashboard Panel Has Been Created

The panel has been created and added to useranalytics. You may now view the dashboard.

7. You can view the dashboard as below screen

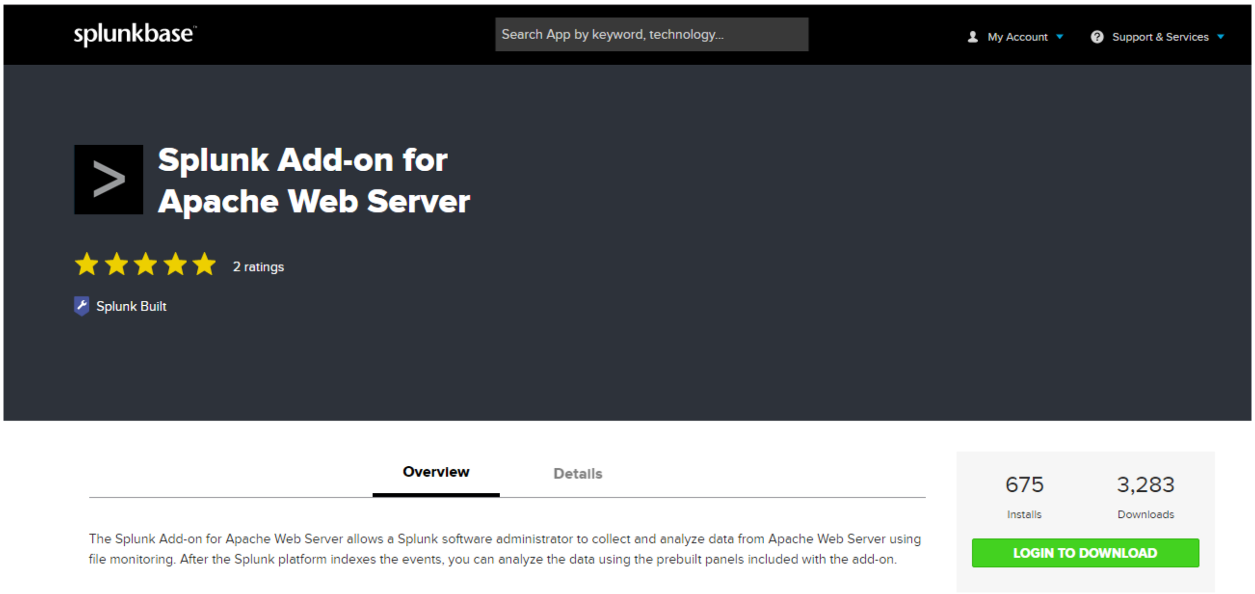


8. Installation of Splunk Add-on for Apache Web Server on Splunk.

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/

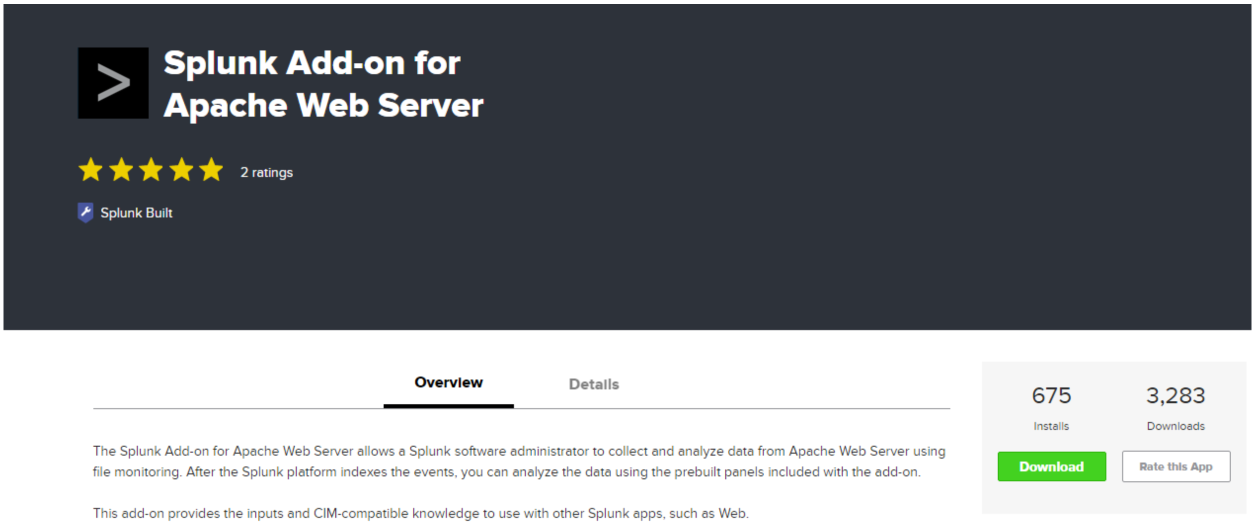
2. Click on Login to download the you will be prompted to login page, login with your Splunk account credentials.



Splunk Add-on for Apache Web Server

The Splunk Add-on for Apache Web Server allows a Splunk software administrator to collect and analyze data from Apache Web Server using file monitoring. After the Splunk platform indexes the events, you can analyze the data using the prebuilt panels included with the add-on.

3. Click on download.

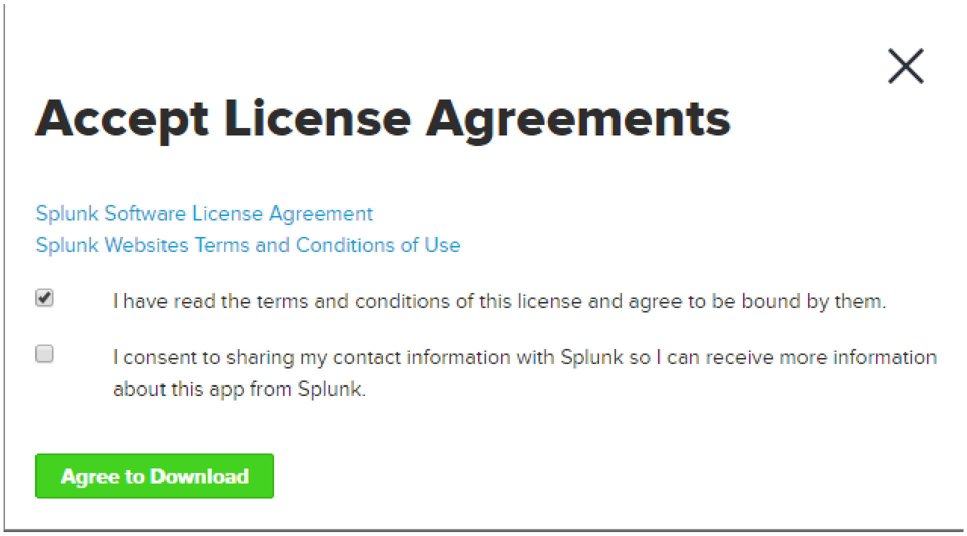


Splunk Add-on for Apache Web Server

The Splunk Add-on for Apache Web Server allows a Splunk software administrator to collect and analyze data from Apache Web Server using file monitoring. After the Splunk platform indexes the events, you can analyze the data using the prebuilt panels included with the add-on.

This add-on provides the inputs and CIM-compatible knowledge to use with other Splunk apps, such as Web.

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



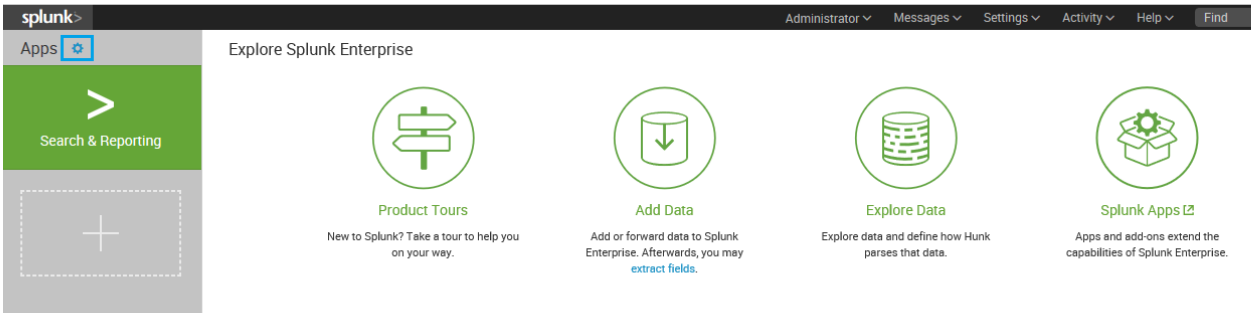
Accept License Agreements

Splunk Software License Agreement
Splunk Websites Terms and Conditions of Use

☑ I have read the terms and conditions of this license and agree to be bound by them.

□ I consent to sharing my contact information with Splunk so I can receive more information about this app from Splunk.

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



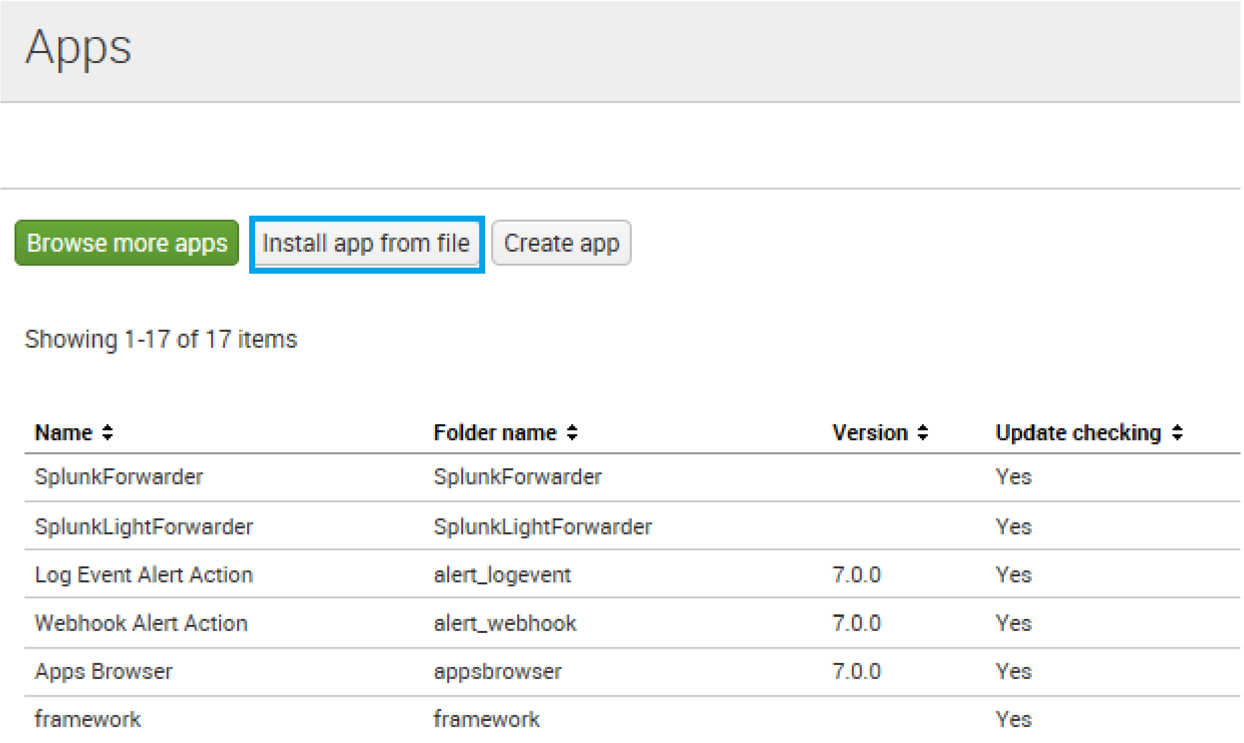
New to Splunk? Take a tour to help you on your way.

Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

Explore data and define how Hunk parses that data.

Apps and add-ons extend the capabilities of Splunk Enterprise.

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

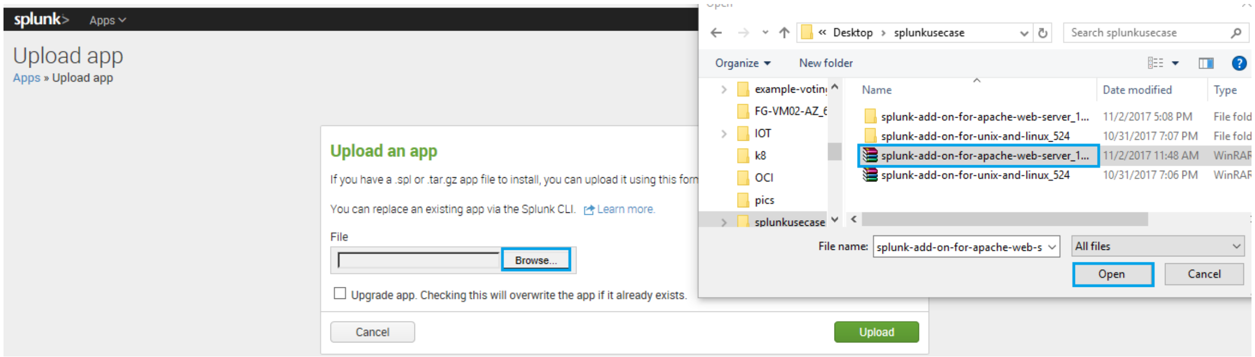


Apps

Showing 1-17 of 17 items

Name	Folder name	Version	Update checking
SplunkForwarder	SplunkForwarder		Yes
SplunkLightForwarder	SplunkLightForwarder		Yes
Log Event Alert Action	alert_logevent	7.0.0	Yes
Webhook Alert Action	alert_webhook	7.0.0	Yes
Apps Browser	appsbrowser	7.0.0	Yes
framework	framework		Yes

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



Upload app

Apps » Upload app

Upload an app

If you have a .spl or .tar.gz app file to install, you can upload it using this forn

You can replace an existing app via the Splunk CLI. Learn more.

File

□ Upgrade app. Checking this will overwrite the app if it already exists.

« Desktop › splunkusecase

Search splunkusecase

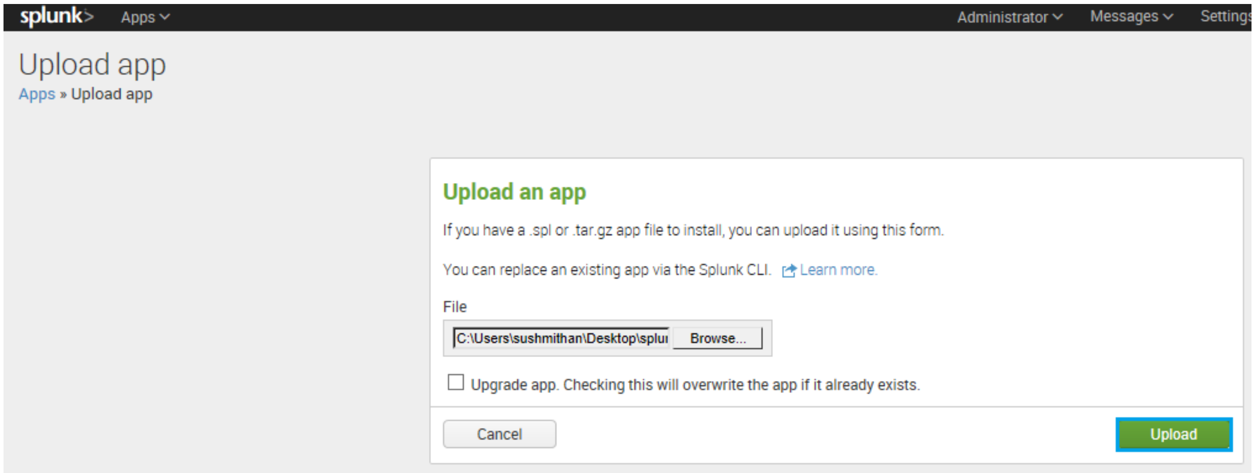
example-votin
FG-VM02-AZ_6
IOT
k8
OCI
pics
splunkusecase

Name	Date modified	Type
splunk-add-on-for-apache-web-server_1...	11/2/2017 5:08 PM	File fold
splunk-add-on-for-unix-and-linux_524	10/31/2017 7:07 PM	File fold
splunk-add-on-for-apache-web-server_1...	11/2/2017 11:48 AM	WinRAR
splunk-add-on-for-unix-and-linux_524	10/31/2017 7:06 PM	WinRAR

File name: splunk-add-on-for-apache-web-s

All files

8. Click on **Upload**



Upload app

Apps » Upload app

Upload an app

If you have a .spl or .tar.gz app file to install, you can upload it using this form.

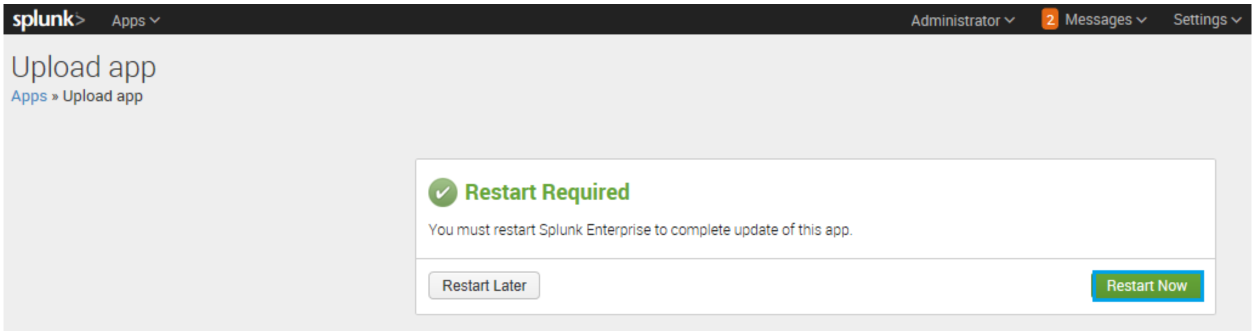
You can replace an existing app via the Splunk CLI. Learn more.

File

C:\Users\sushmithan\Desktop\splu

□ Upgrade app. Checking this will overwrite the app if it already exists.

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



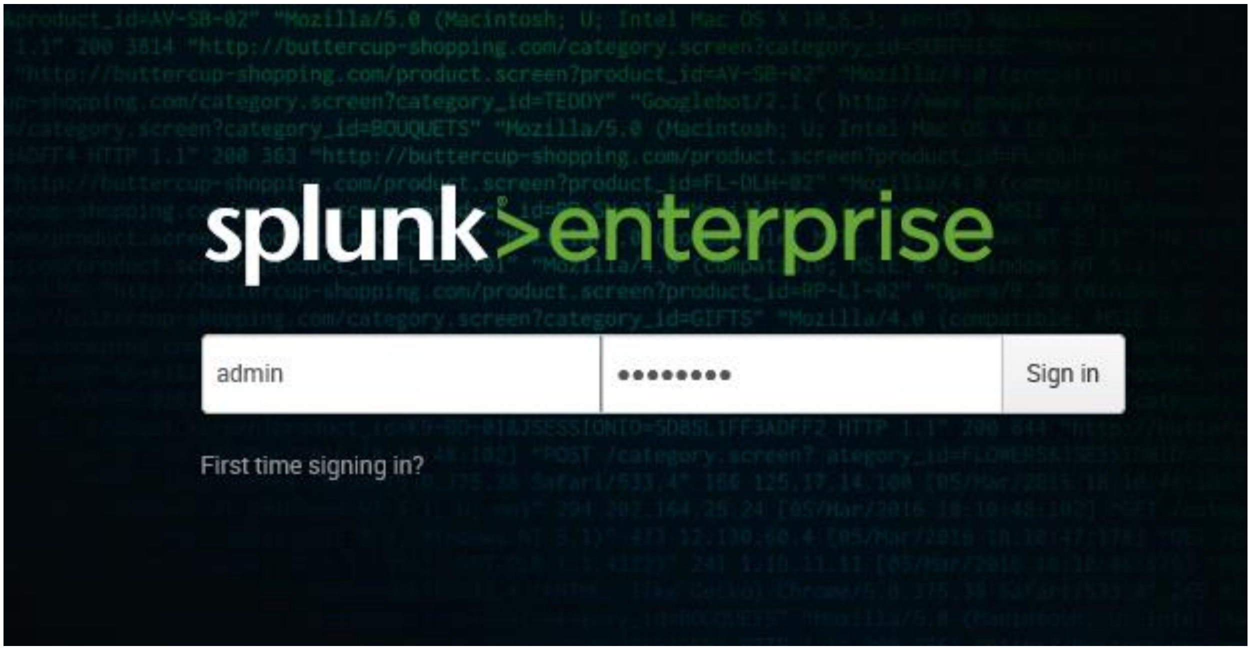
Upload app

Apps » Upload app

Restart Required

You must restart Splunk Enterprise to complete update of this app.

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

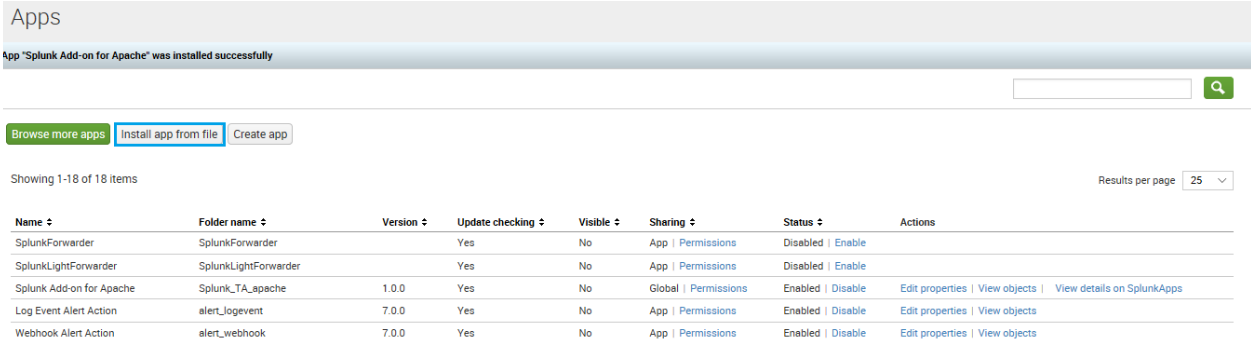


admin

••••••••

First time signing in?

11. Click on Install app from file



Apps

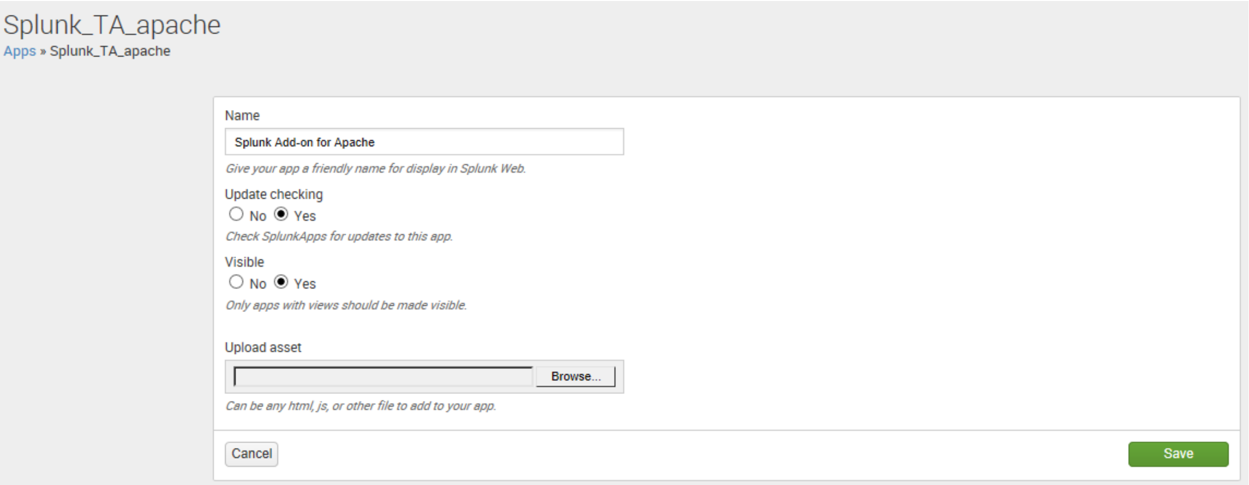
App "Splunk Add-on for Apache" was installed successfully

Showing 1-18 of 18 items

Results per page 25

Name ⇕	Folder name ⇕	Version ⇕	Update checking ⇕	Visible ⇕	Sharing ⇕	Status ⇕	Actions
SplunkForwarder	SplunkForwarder		Yes	No	App | Permissions	Disabled | Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App | Permissions	Disabled | Enable	
Splunk Add-on for Apache	Splunk_TA_apache	1.0.0	Yes	No	Global | Permissions	Enabled | Disable	Edit properties | View objects | View details on SplunkApps
Log Event Alert Action	alert_logevent	7.0.0	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
Webhook Alert Action	alert_webhook	7.0.0	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects

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



Splunk_TA_apache

Apps » Splunk_TA_apache

Name

Splunk Add-on for Apache

Give your app a friendly name for display in Splunk Web.

Update checking

○ No ● Yes

Check SplunkApps for updates to this app.

Visible

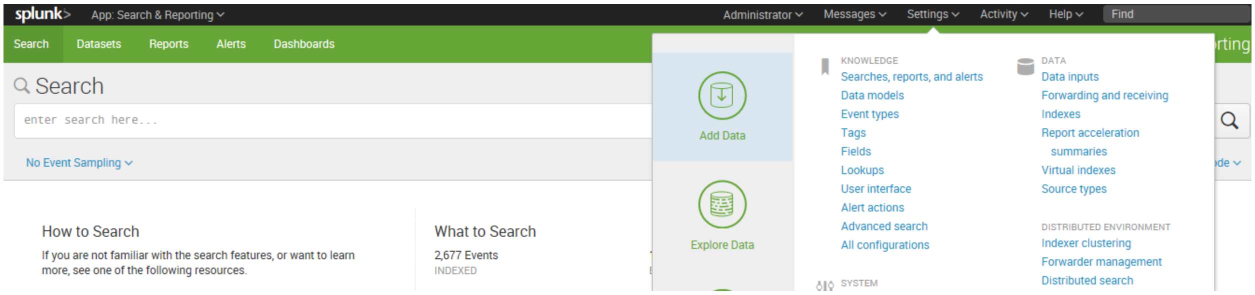
○ No ● Yes

Only apps with views should be made visible.

Upload asset

Can be any html, js, or other file to add to your app.

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



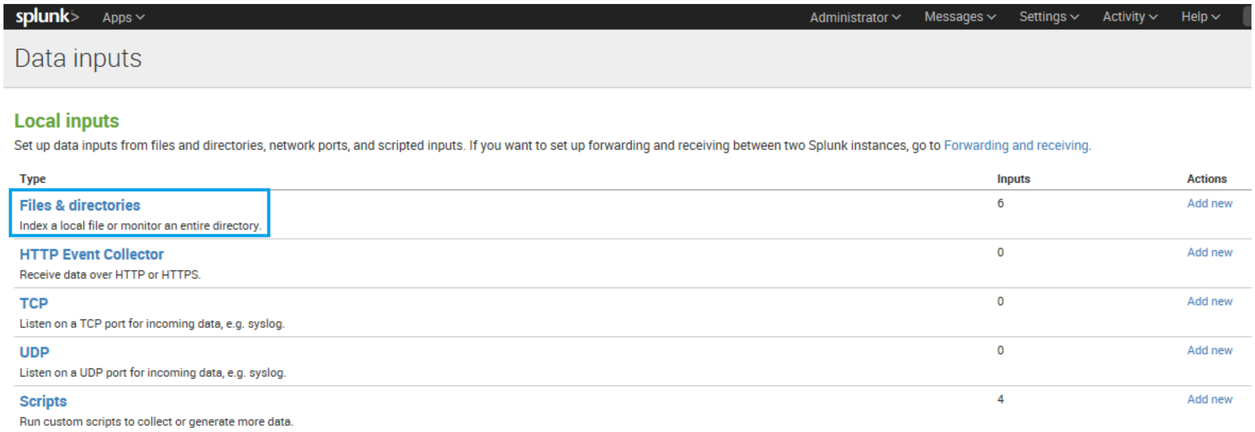
How to Search

If you are not familiar with the search features, or want to learn more, see one of the following resources.

What to Search

2,677 Events
INDEXED

14. Select **File & directories**



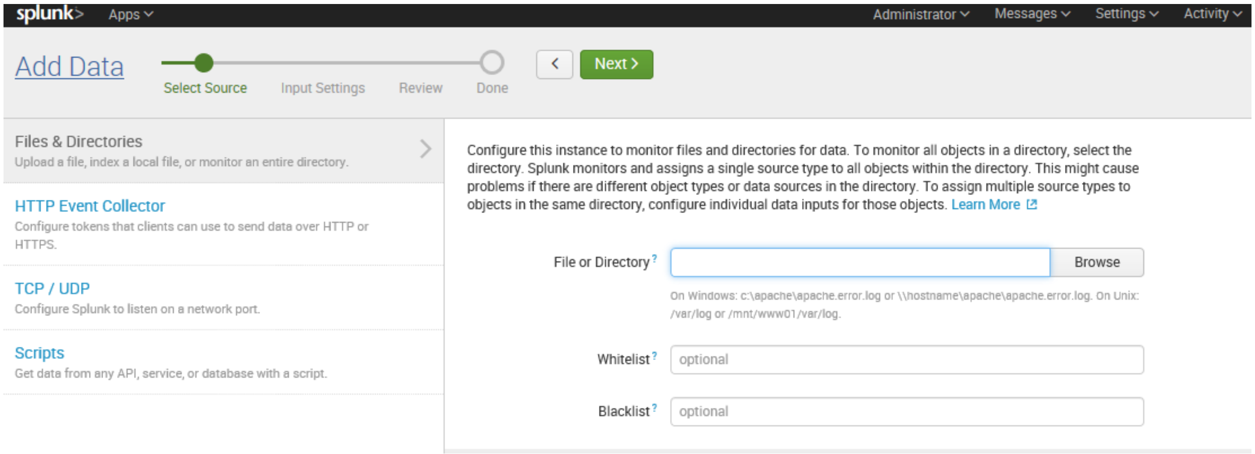
Data inputs

Local inputs

Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to Forwarding and receiving.

Type	Inputs	Actions
Files & directories Index a local file or monitor an entire directory.	6	Add new
HTTP Event Collector Receive data over HTTP or HTTPS.	0	Add new
TCP Listen on a TCP port for incoming data, e.g. syslog.	0	Add new
UDP Listen on a UDP port for incoming data, e.g. syslog.	0	Add new
Scripts Run custom scripts to collect or generate more data.	4	Add new

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



Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure Splunk to listen on a network port.

Scripts
Get data from any API, service, or database with a script.

Configure this instance to monitor files and directories for data. To monitor all objects in a directory, select the directory. Splunk monitors and assigns a single source type to all objects within the directory. This might cause problems if there are different object types or data sources in the directory. To assign multiple source types to objects in the same directory, configure individual data inputs for those objects. Learn More

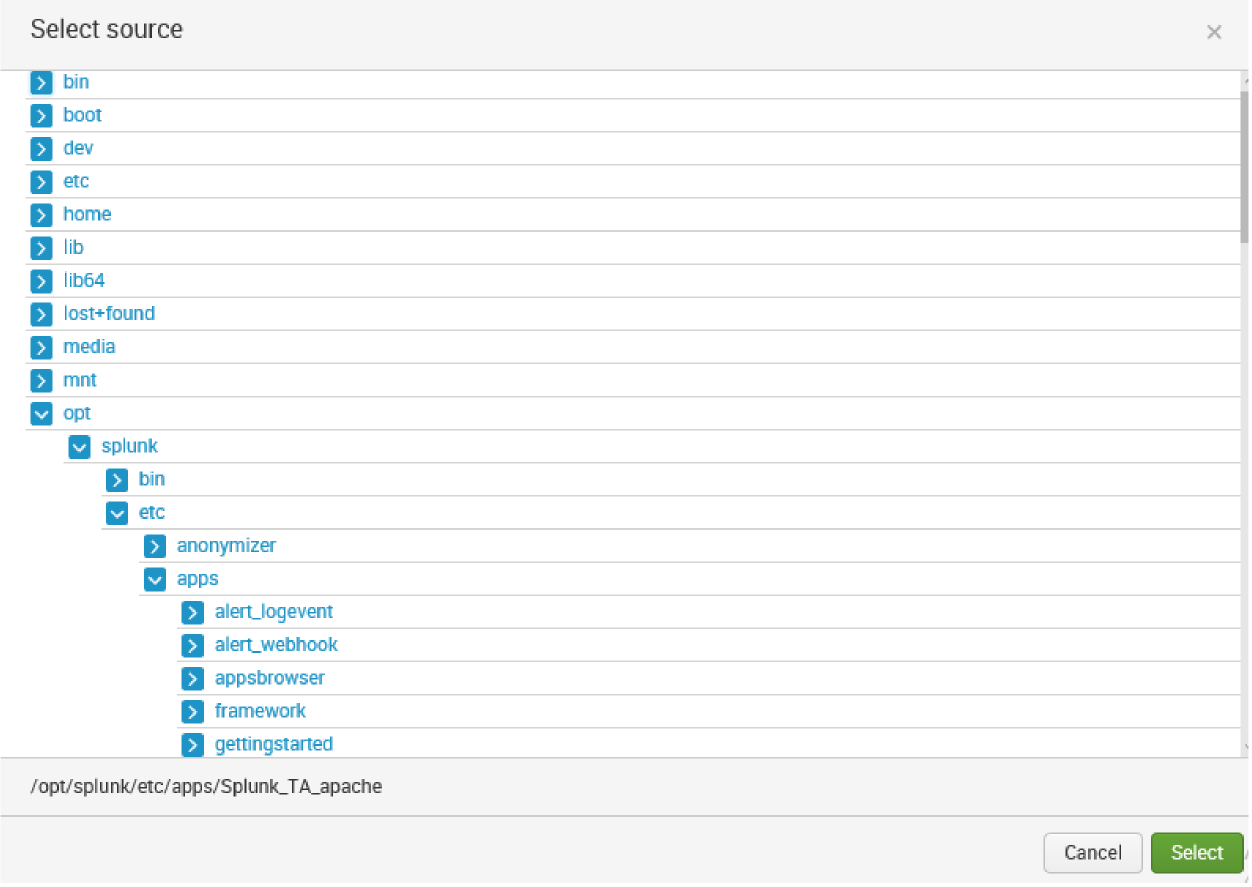
File or Directory ?

On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.

Whitelist ? optional

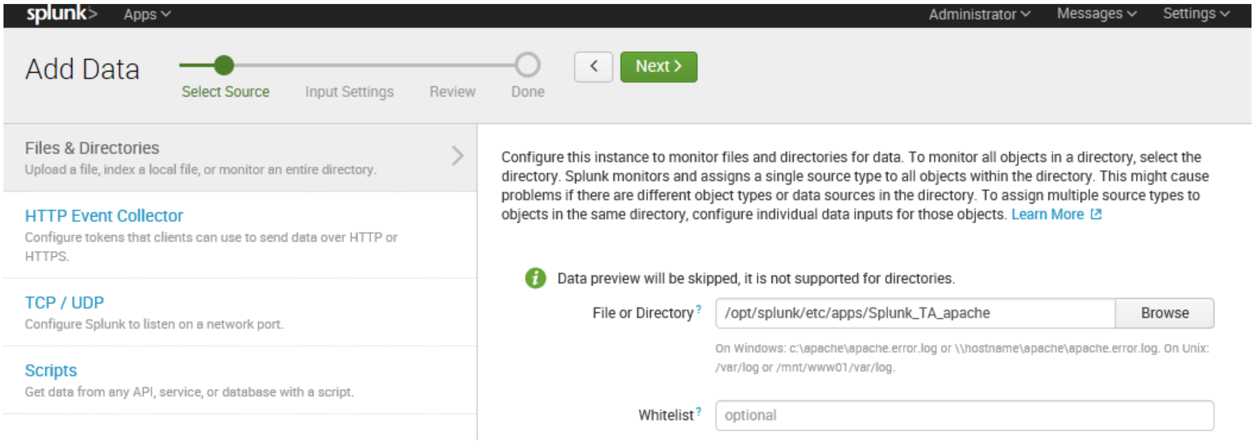
Blacklist ? optional

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



/opt/splunk/etc/apps/Splunk_TA_apache

17. Click on **Next**


splunk>
Apps
Administrator
Messages
Settings
Add Data
Select Source
Input Settings
Review
Done
<
Next >
Files & Directories
Upload a file, index a local file, or monitor an entire directory.
HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.
TCP / UDP
Configure Splunk to listen on a network port.
Scripts
Get data from any API, service, or database with a script.
Browse

Configure this instance to monitor files and directories for data. To monitor all objects in a directory, select the directory. Splunk monitors and assigns a single source type to all objects within the directory. This might cause problems if there are different object types or data sources in the directory. To assign multiple source types to objects in the same directory, configure individual data inputs for those objects. Learn More

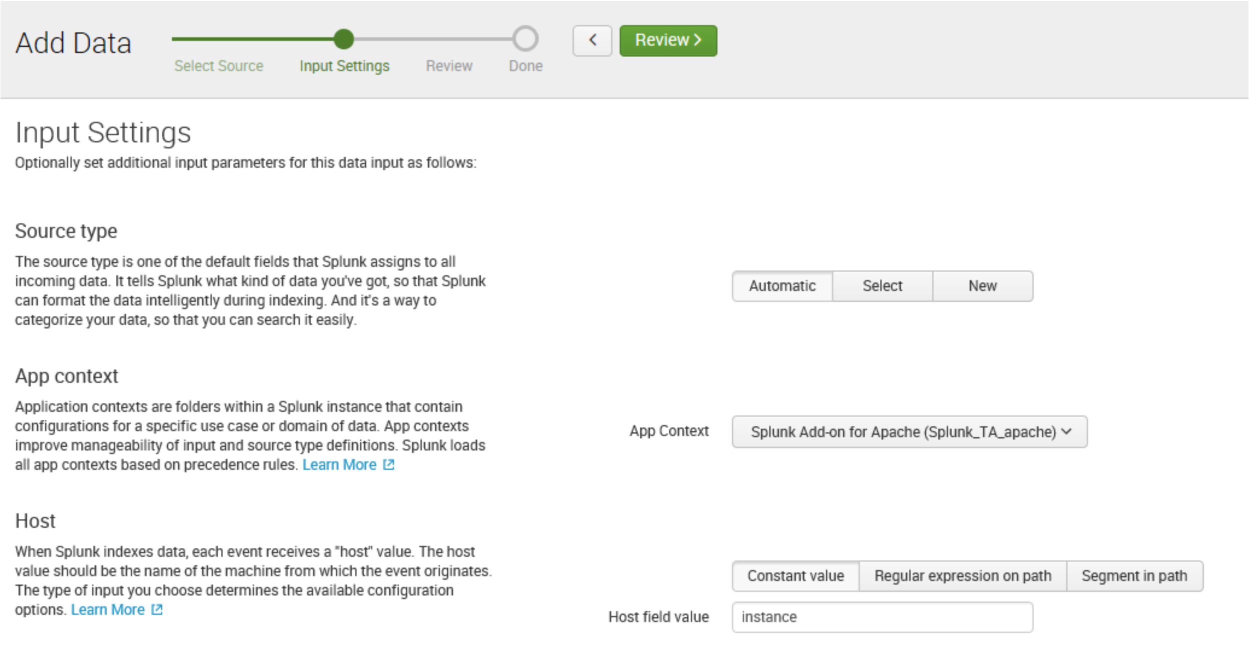
Data preview will be skipped, it is not supported for directories.

File or Directory ? /opt/splunk/etc/apps/Splunk_TA_apache

On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.

Whitelist ? optional

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



Input Settings

Optionally set additional input parameters for this data input as follows:

Source type

The source type is one of the default fields that Splunk assigns to all incoming data. It tells Splunk what kind of data you've got, so that Splunk can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

App context

Application contexts are folders within a Splunk instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. Splunk loads all app contexts based on precedence rules. Learn More

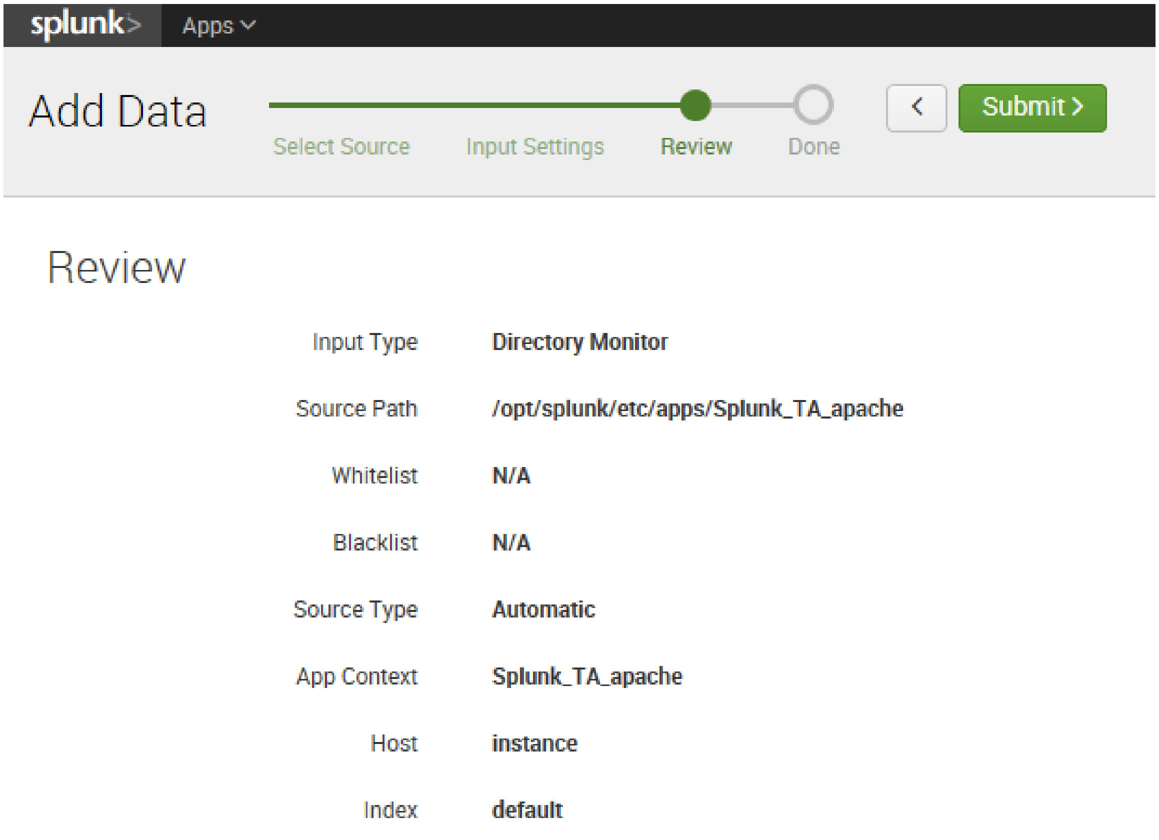
App Context: Splunk Add-on for Apache (Splunk_TA_apache)

Host

When Splunk indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More

Host field value: instance

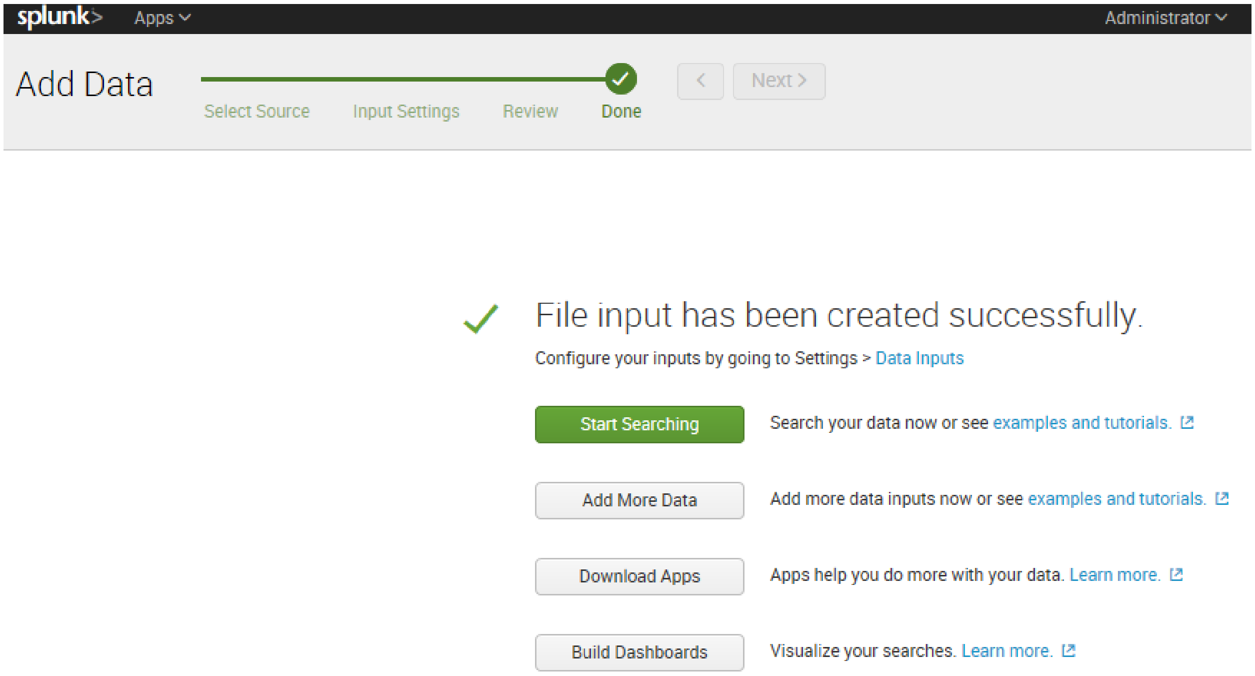
19. After reviewing click on **Submit.**



Review

Input Type	Directory Monitor
Source Path	/opt/splunk/etc/apps/Splunk_TA_apache
Whitelist	N/A
Blacklist	N/A
Source Type	Automatic
App Context	Splunk_TA_apache
Host	instance
Index	default

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



File input has been created successfully.

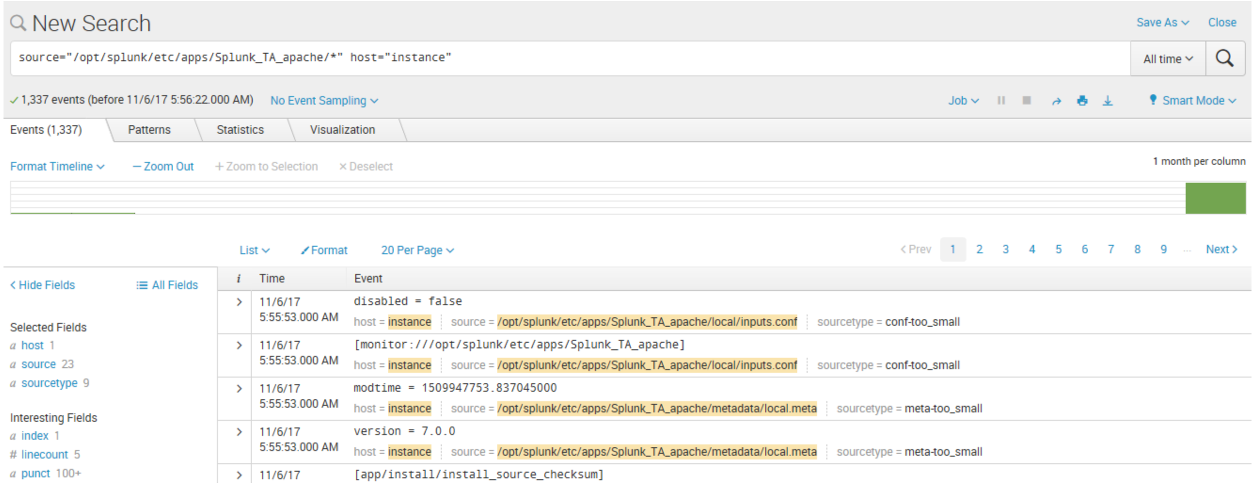
Configure your inputs by going to Settings > Data Inputs

Search your data now or see examples and tutorials.

Add more data inputs now or see examples and tutorials.

Apps help you do more with your data. Learn more.

Visualize your searches. Learn more.



```
source="/opt/splunk/etc/apps/Splunk_TA_apache/*" host="instance"
```

✓ 1,337 events (before 11/6/17 5:56:22.000 AM)

Selected Fields
- a host 1
- a source 23
- a sourcetype 9

Interesting Fields
- a index 1
- # linecount 5
- a punct 100+

i	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]