MIRACLE
SOFTWARE SYSTEMS

Splunk Implementation in Apigee

A.AnuManasa
Apigee Developer
Miracle Software Systems, Inc.

www.miraclesoft.com

Introduction:

- Splunk is a enterprise software for searching, monitoring, and analyzing machine-generated big data, via a web-style interface.

- Splunk captures indexes and correlates real-time data in a searchable repository from which it can generate graphs, reports, alerts and dashboards.

Splunk Products:

- Splunk offers its software in two license types:
    - Splunk Enterprise
    - Splunk Cloud free version

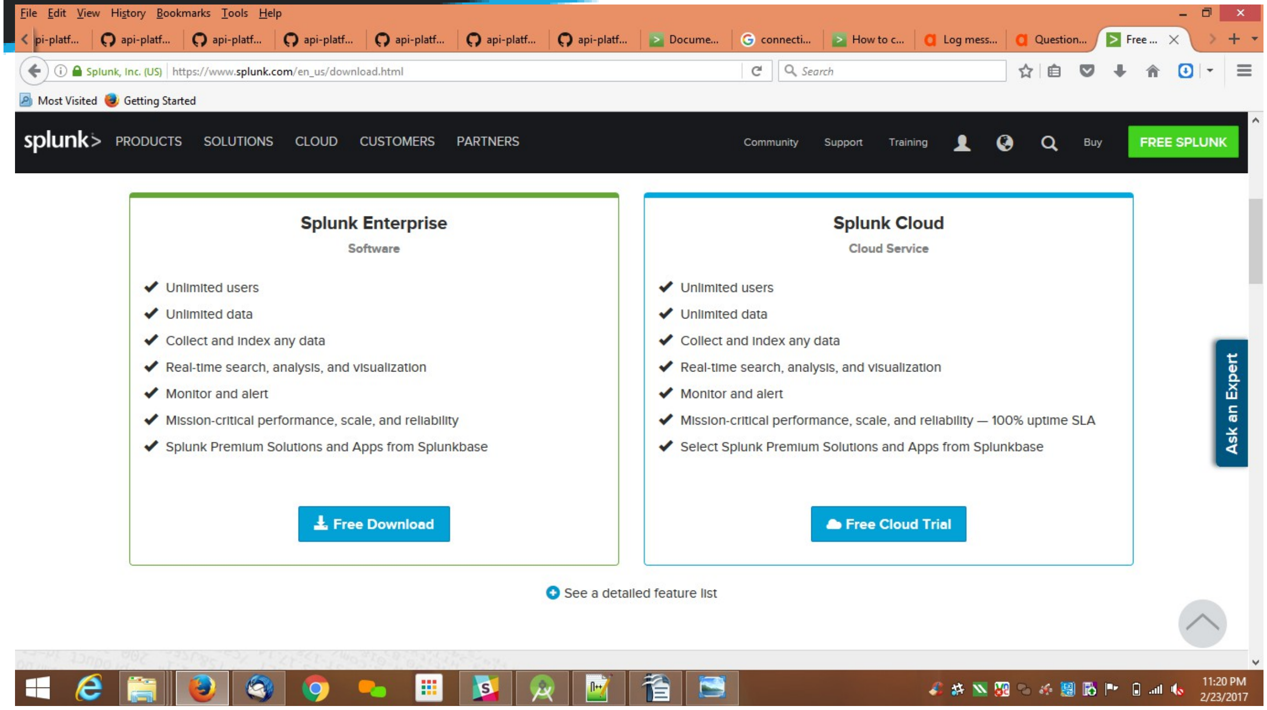
- Splunk Enterprise is expires in 60 days.

- Splunk Cloud is expires in 15 days.

Log on to Splunk:

- Go to the following URL and select Splunk cloud or Splunk Enterprise.

https://www.splunk.com/en_us/download.html


File Edit View History Bookmarks Tools Help
https://www.splunk.com/en_us/download.html
splunk> PRODUCTS SOLUTIONS CLOUD CUSTOMERS PARTNERS
Community Support Training Buy FREE SPLUNK
Ask an Expert
11:20 PM
2/23/2017

Splunk Enterprise
Software

- ✓ Unlimited users
- ✓ Unlimited data
- ✓ Collect and index any data
- ✓ Real-time search, analysis, and visualization
- ✓ Monitor and alert
- ✓ Mission-critical performance, scale, and reliability
- ✓ Splunk Premium Solutions and Apps from Splunkbase

Free Download

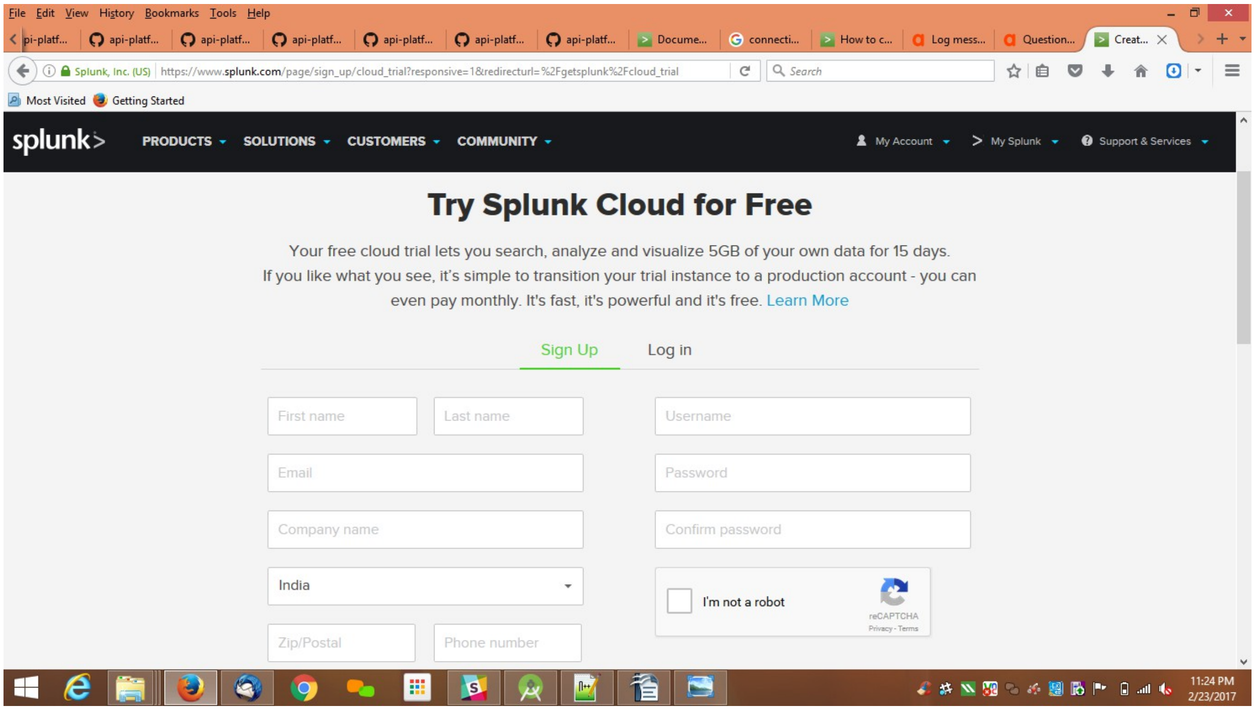
Splunk Cloud
Cloud Service

- ✓ Unlimited users
- ✓ Unlimited data
- ✓ Collect and index any data
- ✓ Real-time search, analysis, and visualization
- ✓ Monitor and alert
- ✓ Mission-critical performance, scale, and reliability — 100% uptime SLA
- ✓ Select Splunk Premium Solutions and Apps from Splunkbase

Free Cloud Trial

See a detailed feature list

- Select Splunk cloud and sign up with the user details.


File Edit View History Bookmarks Tools Help
https://www.splunk.com/page/sign_up/cloud_trial?responsive=1&redirecturl=%2Fgetsplunk%2Fcloud_trial
splunk> PRODUCTS SOLUTIONS CUSTOMERS COMMUNITY
My Account My Splunk Support & Services
11:24 PM
2/23/2017

Try Splunk Cloud for Free

Your free cloud trial lets you search, analyze and visualize 5GB of your own data for 15 days. If you like what you see, it's simple to transition your trial instance to a production account - you can even pay monthly. It's fast, it's powerful and it's free. Learn More

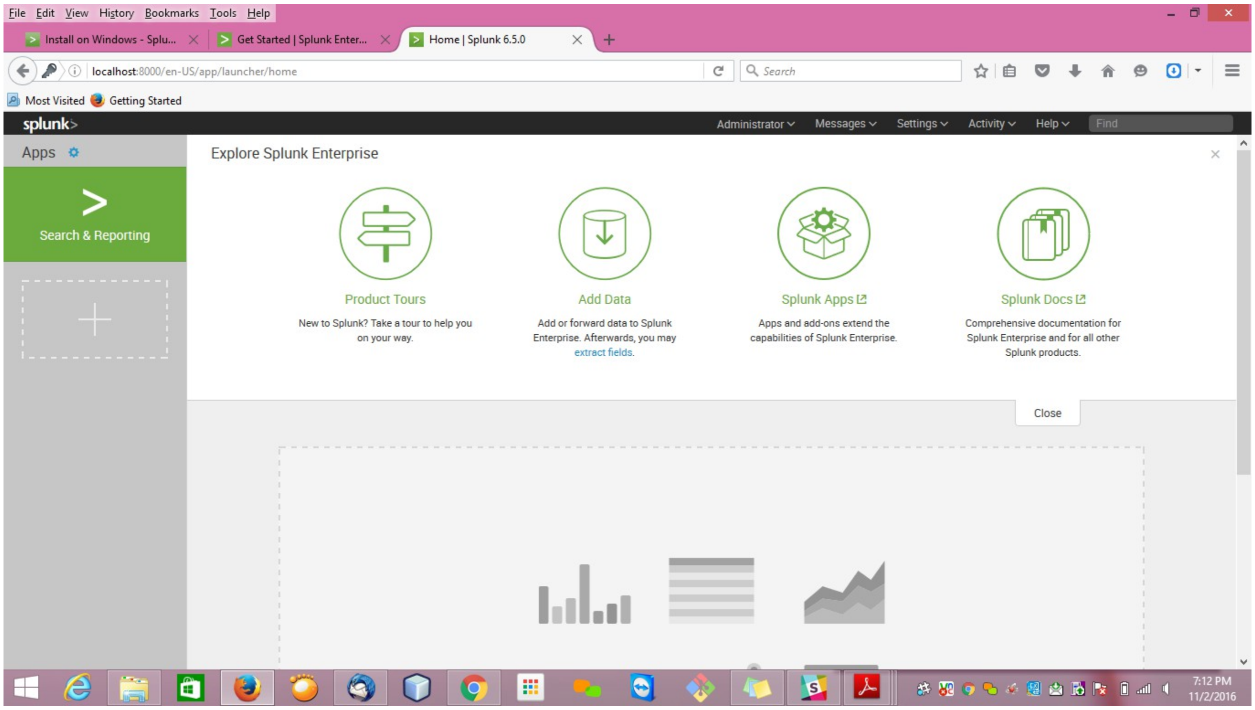
Sign Up Log in

First name	Last name
Email	
Company name	
India	
Zip/Postal	Phone number
Username	
Password	
Confirm password	

□ I'm not a robot

reCAPTCHA
Privacy - Terms

- Now Sign In to the Splunk Cloud then we get the dashboard as follows.



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.

Splunk Apps

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

Splunk Docs

Comprehensive documentation for Splunk Enterprise and for all other Splunk products.

- There are multiple ways of logging into Splunk. Below are described a few ways to log:

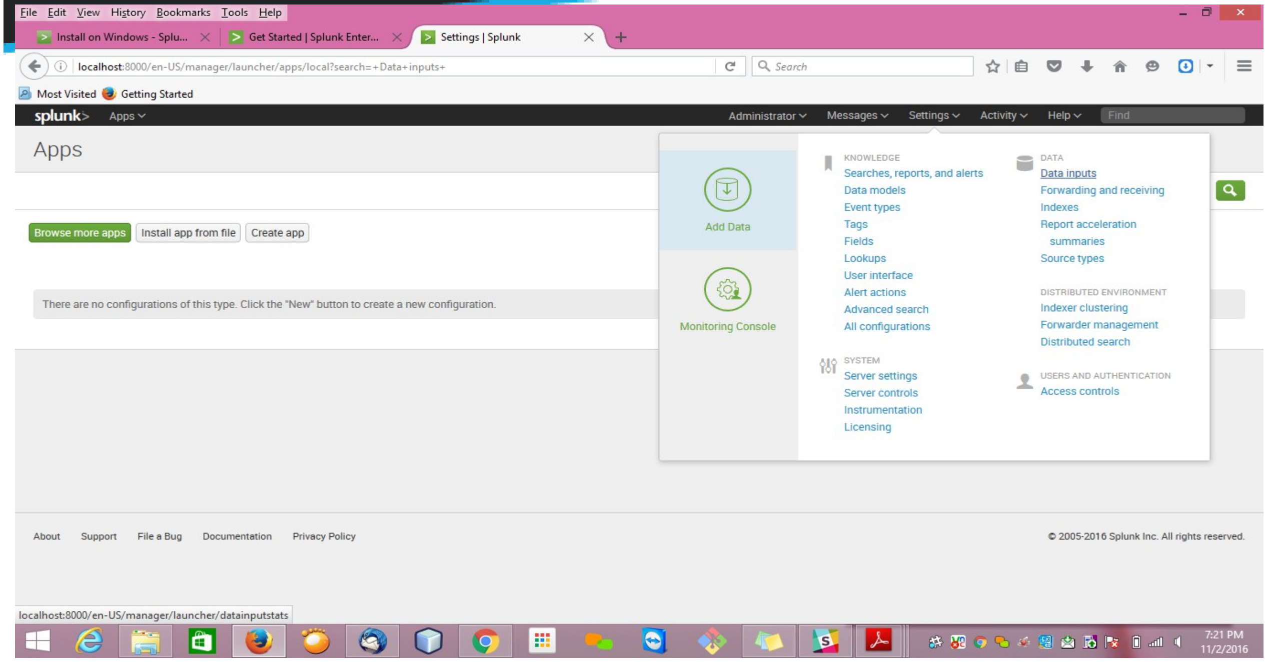
1. Log over HTTP
2. Log over TCP
3. Log via javascript

1. Log over HTTP:

- For creating HTTP Event collector in Splunk follow the below steps.

Step 1:

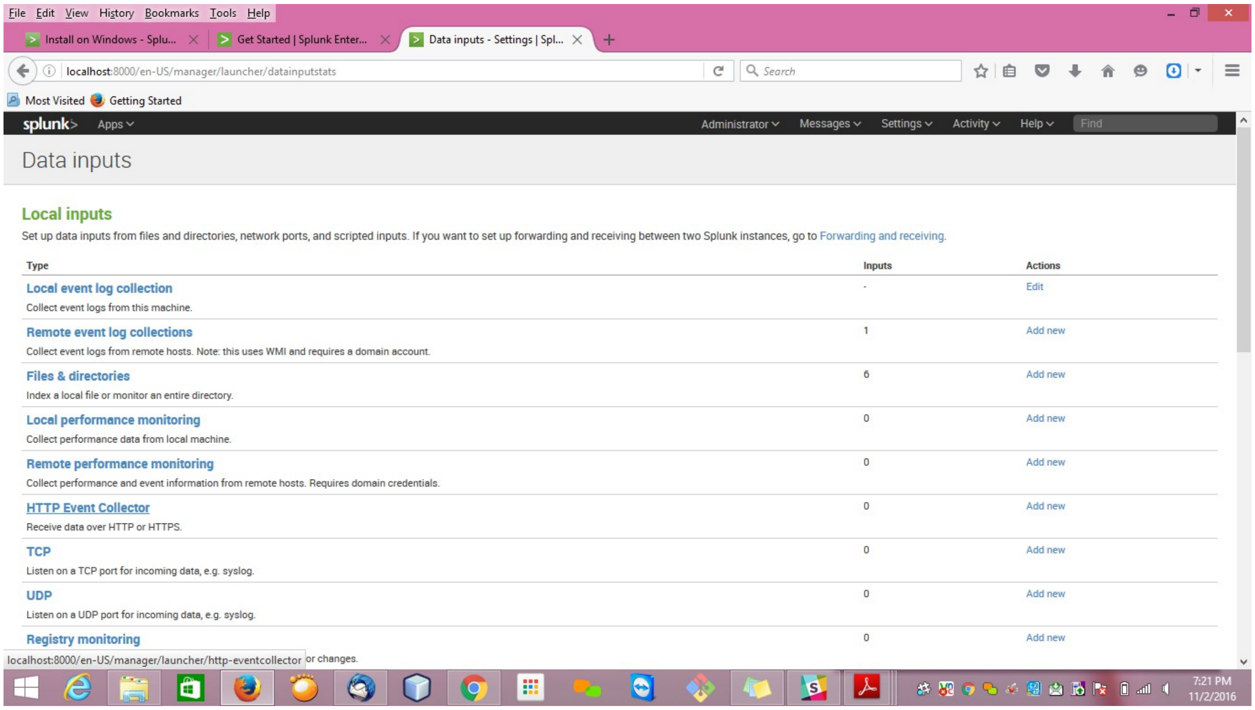
- Now go to the settings at top right corner in dashboard and Select Data Inputs in the Data tab.



There are no configurations of this type. Click the "New" button to create a new configuration.

Step 2:

- Now click on HTTP Event Collector.


File Edit View History Bookmarks Tools Help
Install on Windows - Splu...
Get Started | Splunk Enter...
Data inputs - Settings | Spl...
localhost:8000/en-US/manager/launcher/datainputstats
Search
Most Visited
Getting Started
splunk>
Apps
Administrator
Messages
Settings
Activity
Help
Find
localhost:8000/en-US/manager/launcher/http-eventcollector
7:21 PM
11/2/2016

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.

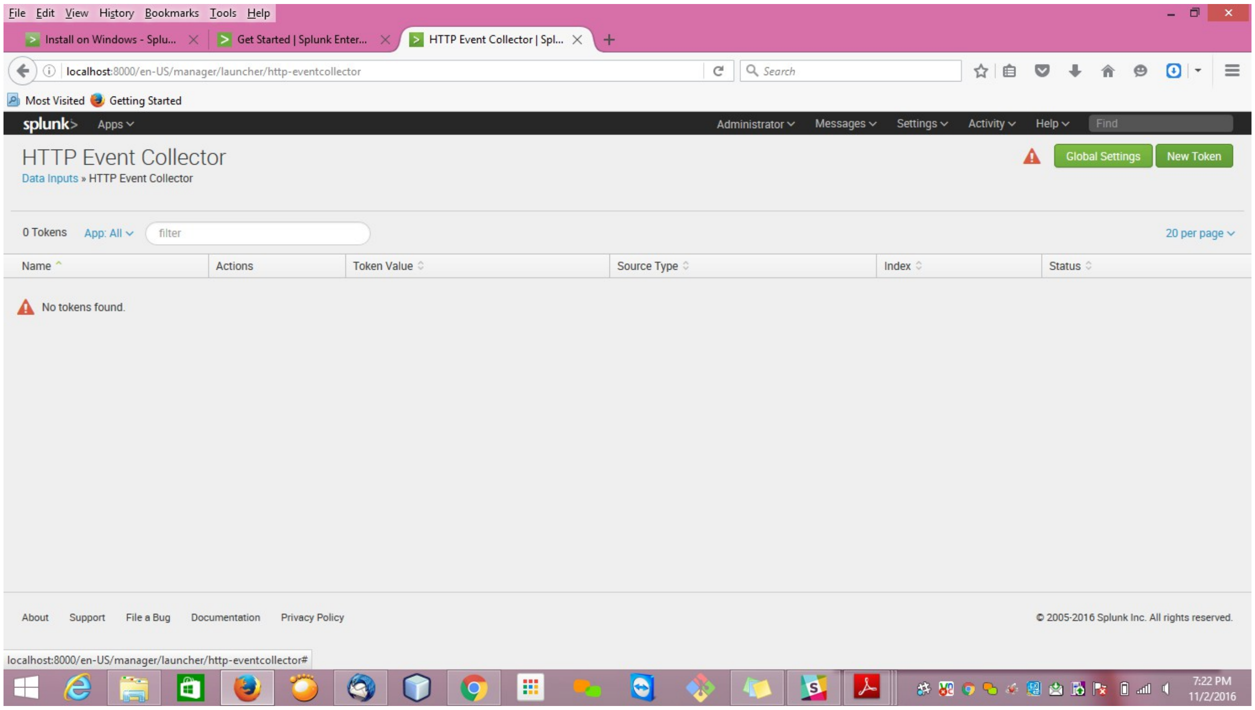
Type	Inputs	Actions
Local event log collection Collect event logs from this machine.	-	Edit
Remote event log collections Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.	1	Add new
Files & directories Index a local file or monitor an entire directory.	6	Add new
Local performance monitoring Collect performance data from local machine.	0	Add new
Remote performance monitoring Collect performance and event information from remote hosts. Requires domain credentials.	0	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
Registry monitoring or changes.	0	Add new

Step 3:

- Next Generate an HTTP Event Collector authentication token ("HEC token").

HEC tokens are sent in the headers of incoming data packets to authenticate them with Splunk Enterprise or Splunk Cloud.

- Now Create a token by selecting New Token at top right corner.


File Edit View History Bookmarks Tools Help
Install on Windows - Splu...
Get Started | Splunk Enter...
HTTP Event Collector | Spl...
localhost:8000/en-US/manager/launcher/http-eventcollector
Search
Most Visited
Getting Started
splunk>
Apps
Administrator
Messages
Settings
Activity
Help
Find
Global Settings
New Token
App: All
filter
20 per page
About
Support
File a Bug
Documentation
Privacy Policy
© 2005-2016 Splunk Inc. All rights reserved.
localhost:8000/en-US/manager/launcher/http-eventcollector#
7:22 PM
11/2/2016

HTTP Event Collector

Data Inputs » HTTP Event Collector

0 Tokens

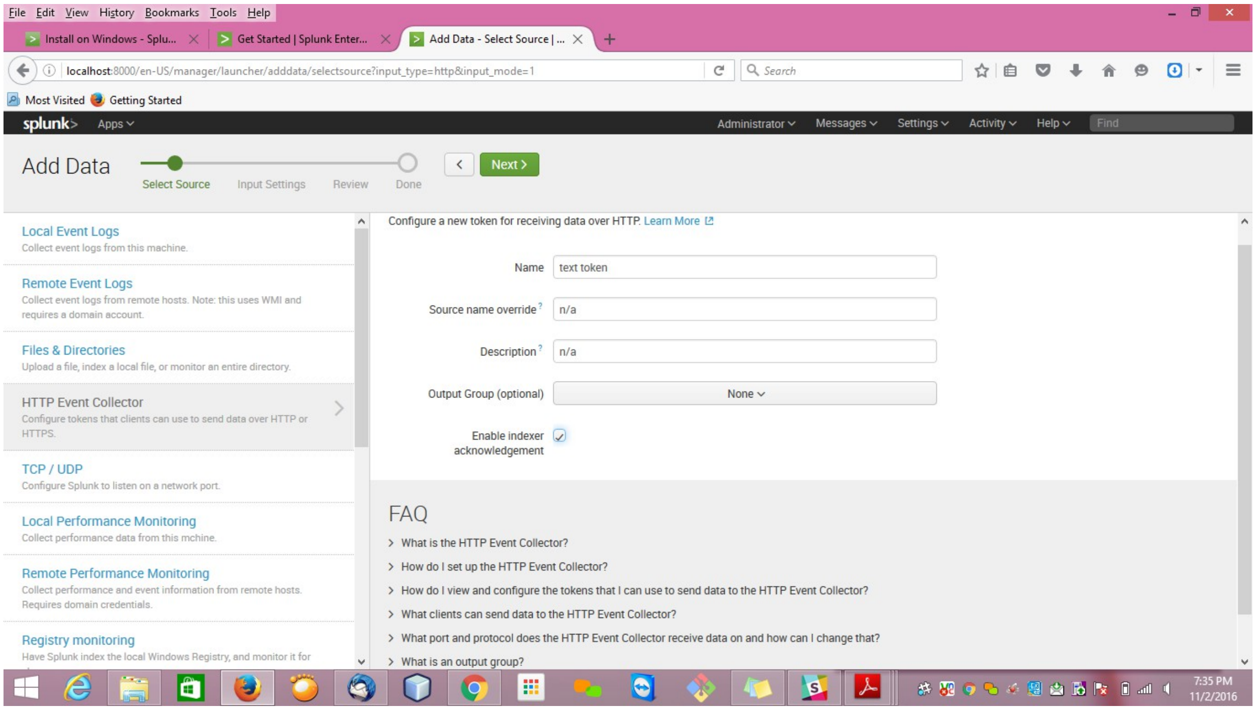
Name	Actions	Token Value	Source Type	Index	Status

No tokens found.

Step 4:

- Now Select Source screen of the Add Data workflow appears.

- This is where you name the HEC input, and optionally specify a description, a source field name to assign to all event data accepted with this input's token, and an output group (a named group of Splunk indexers) also enable indexer acknowledgment.


File Edit View History Bookmarks Tools Help
Install on Windows - Splu...
Get Started | Splunk Enter...
Add Data - Select Source | ...
localhost:8000/en-US/manager/launcher/adddata/selectsource?input_type=http&input_mode=1
Search
Most Visited
Getting Started
splunk>
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Input Settings
Review
Done
Next >
7:35 PM
11/2/2016

Local Event Logs
Collect event logs from this machine.

Remote Event Logs
Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.

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.

Local Performance Monitoring
Collect performance data from this mchine.

Remote Performance Monitoring
Collect performance and event information from remote hosts. Requires domain credentials.

Registry monitoring
Have Splunk index the local Windows Registry, and monitor it for

Configure a new token for receiving data over HTTP. Learn More

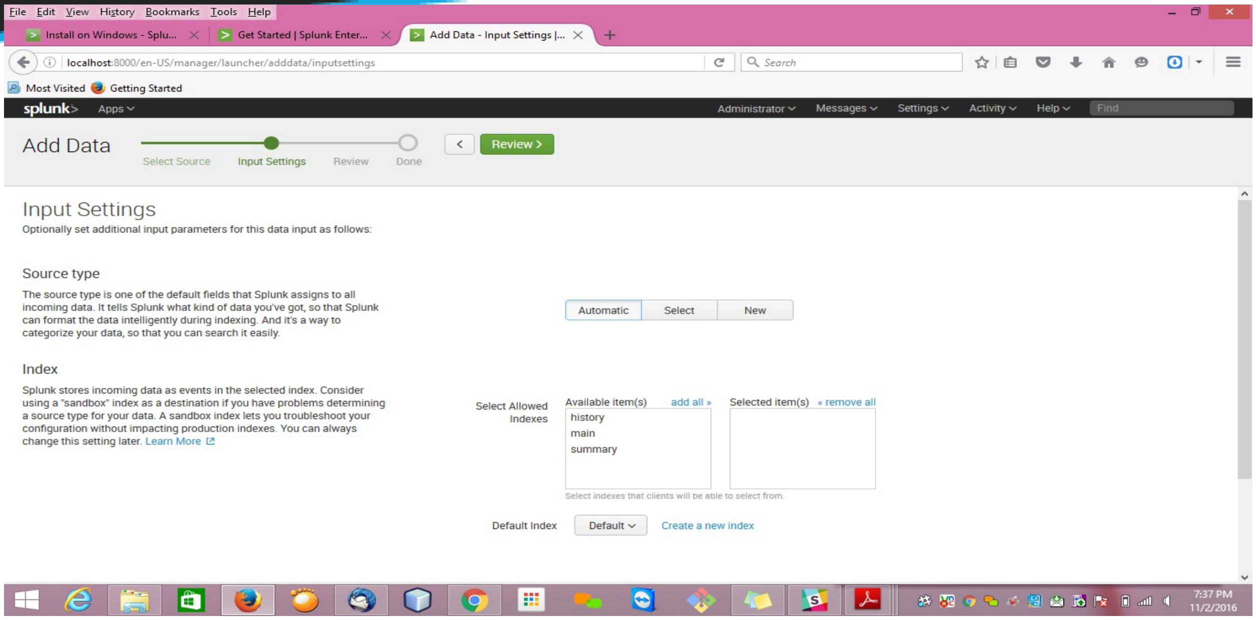
Name	text token
Source name override ?	n/a
Description ?	n/a
Output Group (optional)	None
Enable indexer acknowledgement	☑

FAQ

- What is the HTTP Event Collector?
- How do I set up the HTTP Event Collector?
- How do I view and configure the tokens that I can use to send data to the HTTP Event Collector?
- What clients can send data to the HTTP Event Collector?
- What port and protocol does the HTTP Event Collector receive data on and how can I change that?
- What is an output group?

Step 5:

- Next Input Settings screen appears. On this screen, determine how to assign a sourcetype field value to incoming data (either automatically, by specifying an existing one, or by creating a new one) and what indexes are allowed to index the data accepted with this input's token.


File Edit View History Bookmarks Tools Help
Install on Windows - Splu...
Get Started | Splunk Enter...
Add Data - Input Settings |...
localhost:8000/en-US/manager/launcher/adddata/inputsettings
Search
Most Visited
Getting Started
splunk>
Apps
Administrator
Messages
Settings
Activity
Help
Find
Select Source
Input Settings
Review
Done
<
Review >
7:37 PM
11/2/2016

Add Data

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.

Automatic | Select | New

Index

Splunk stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More

Select Allowed Indexes

Available item(s) add all »
- history
- main
- summary

Selected item(s) « remove all

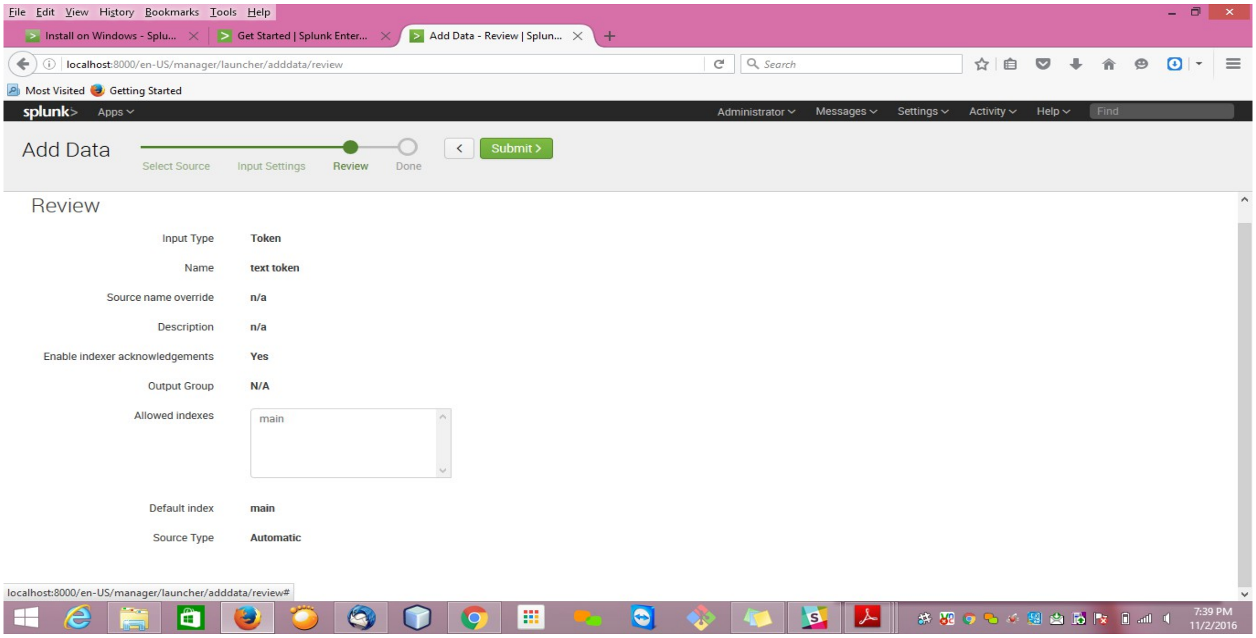
Select indexes that clients will be able to select from.

Default Index: Default

Create a new index

Step 6:

- On the Input Settings page, leave the Source type as Automatic, and then choose at least one index that is not used for production, or real-world, purposes. Then, click Review. The Review page appears as below.


File Edit View History Bookmarks Tools Help
Install on Windows - Splu...
Get Started | Splunk Enter...
Add Data - Review | Splun...
localhost:8000/en-US/manager/launcher/adddata/review
Search
Most Visited
Getting Started
splunk>
Apps
Administrator
Messages
Settings
Activity
Help
Find
Select Source
Input Settings
Review
Done
<
Submit >
localhost:8000/en-US/manager/launcher/adddata/review#
7:39 PM
11/2/2016

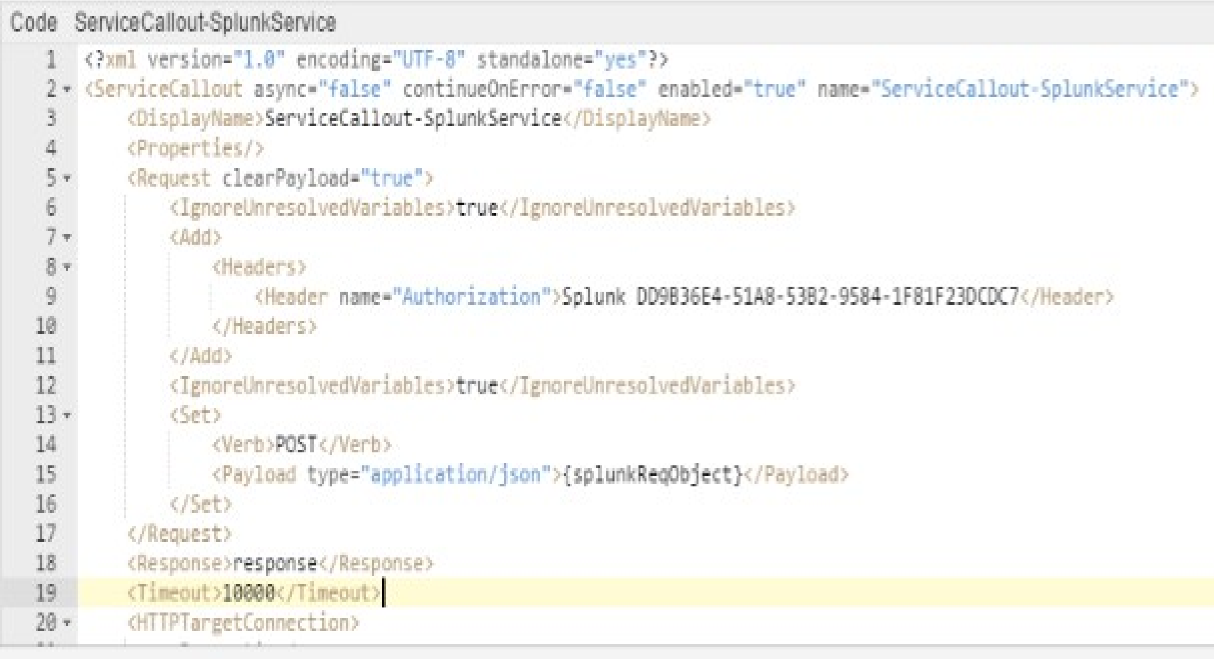
Add Data

Review

Input Type	Token
Name	text token
Source name override	n/a
Description	n/a
Enable indexer acknowledgements	Yes
Output Group	N/A
Allowed indexes	main
Default index	main
Source Type	Automatic

Step 7:

- Now SignIn into the Apigee and create an API proxy and configured with the HTTP Event Collector token.
- For that we used Service Callout Poicy in Apigee and configured with the HTTP Token as shown in below figure.

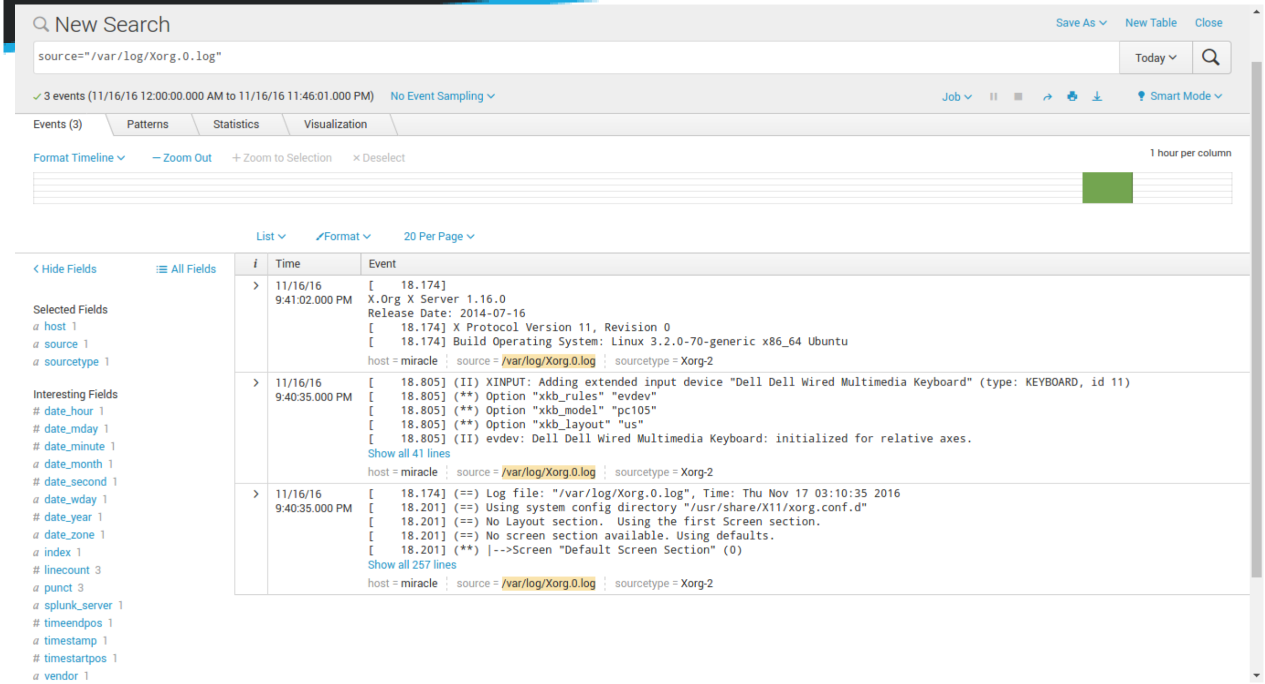


Code ServiceCallout-SplunkService

```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ServiceCallout async="false" continueOnError="false" enabled="true" name="ServiceCallout-SplunkService">
    <DisplayName>ServiceCallout-SplunkService</DisplayName>
    <Properties/>
    <Request clearPayload="true">
        <IgnoreUnresolvedVariables>true</IgnoreUnresolvedVariables>
        <Add>
            <Headers>
                <Header name="Authorization">Splunk DD9B36E4-51A8-53B2-9584-1F81F23DCDC7</Header>
            </Headers>
        </Add>
        <IgnoreUnresolvedVariables>true</IgnoreUnresolvedVariables>
        <Set>
            <Verb>POST</Verb>
            <Payload type="application/json">{splunkReqObject}</Payload>
        </Set>
    </Request>
    <Response>response</Response>
    <Timeout>10000</Timeout>
    <HTTPTargetConnection>
```

Step 8:

- Now we can observe the Apigee logs in Splunk whenever we are trying to access the proxy.
- Following is the sample output for the logs.



```
source="/var/log/Xorg.0.log"
```

✓ 3 events (11/16/16 12:00:00.000 AM to 11/16/16 11:46:01.000 PM)

Selected Fields
a host 1
a source 1
a sourcetype 1

Interesting Fields
# date_hour 1
# date_mday 1
# date_minute 1
a date_month 1
# date_second 1
a date_wday 1
# date_year 1
a date_zone 1
a index 1
# linecount 3
a punct 3
a splunk_server 1
# timeendpos 1
a timestamp 1
# timestartpos 1
a vendor 1

11/16/16
9:41:02.000 PM

```
[     18.174]
X.Org X Server 1.16.0
Release Date: 2014-07-16
[     18.174] X Protocol Version 11, Revision 0
[     18.174] Build Operating System: Linux 3.2.0-70-generic x86_64 Ubuntu
```

host = miracle | source = /var/log/Xorg.0.log | sourcetype = Xorg-2

11/16/16
9:40:35.000 PM

```
[     18.805] (II) XINPUT: Adding extended input device "Dell Dell Wired Multimedia Keyboard" (type: KEYBOARD, id 11)
[     18.805] (**) Option "xkb_rules" "evdev"
[     18.805] (**) Option "xkb_model" "pc105"
[     18.805] (**) Option "xkb_layout" "us"
[     18.805] (II) evdev: Dell Dell Wired Multimedia Keyboard: initialized for relative axes.
```

Show all 41 lines

host = miracle | source = /var/log/Xorg.0.log | sourcetype = Xorg-2

11/16/16
9:40:35.000 PM

```
[     18.174] (==) Log file: "/var/log/Xorg.0.log", Time: Thu Nov 17 03:10:35 2016
[     18.201] (==) Using system config directory "/usr/share/X11/xorg.conf.d"
[     18.201] (==) No Layout section.  Using the first Screen section.
[     18.201] (==) No screen section available. Using defaults.
[     18.201] (**) |-->Screen "Default Screen Section" (0)
```

Show all 257 lines

host = miracle | source = /var/log/Xorg.0.log | sourcetype = Xorg-2