Splunk Cloud enables you to store, search, **analyze**, and visualize the **machine-generated data** gathered from the websites, applications, sensors, devices, and so on. **Splunk Cloud** offers many of the features of **Splunk Enterprise** as a cloud service. You can use Splunk Cloud alone or with Splunk Enterprise on-premises software as a hybrid solution.

We used just **Splunk Forwarder** (A simplified version of Splunk Enterprise but its own download and installation) which is found on the EC2 instance and **Splunk Cloud (WebService provided by Splunk)**

We are using a **TRIAL** version of Splunk Cloud which will be **EXPIRED**. Sign up for a new Splunk Cloud account here: https://www.splunk.com/ and on the right side you will click "Free Splunk" and then make sure to select "Cloud Trial" at the bottom.

To send data to Splunk Cloud, you run **forwarders** on machines that have access to the source data. **Splunk Cloud** software ingests the forwarded data and **indexes** it, transforming it into searchable knowledge in the form of **events**. After **event processing** is complete, you can associate events with **knowledge objects** to enhance their usefulness. For example, you can use the search processing language or the interactive pivot feature to **create reports** and **visualizations**.

*** You will need to change configurations for the Universal Forwarder in order to point to the correct Splunk Cloud***

Please follow this guide to set up the Splunk Plugin for Jenkins in order to setup the configuration:

https://wiki.jenkins.io/display/JENKINS/Splunk+Plugin+for+Jenkins

http://docs.splunk.com/Documentation/SplunkCloud/7.0.3/User/ForwardDataToSplunkCloudFromWindows

Forward data to Splunk Cloud from Microsoft Windows

To get data into Splunk Cloud, log into your Splunk Cloud deployment and do the following:

1. Download the Splunk Universal Forwarder for Windows.
2. Install the Splunk Universal Forwarder for Windows.
    1. Uncheck the box as soon as the box pops up
3. Download and install the universal forwarder credentials.

1. Can be found on your Splunk Cloud dashboard
2. Click universal forwarder
3. Download Universal Forwarder Credentials

4. Configure data inputs, which specify the data to be collected and forwarded.
    1. Open-up command line as administrator
    2.

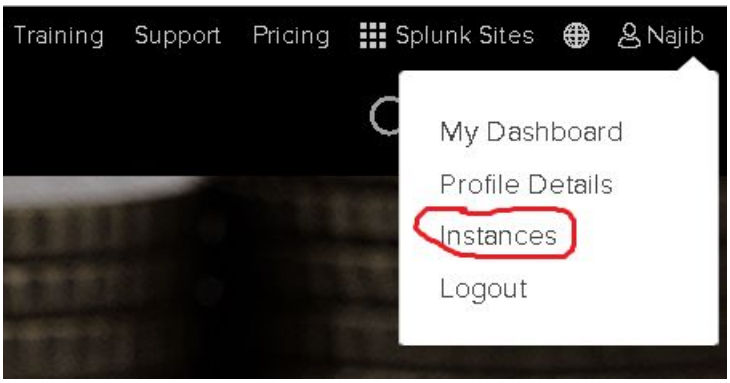
C:\>set SPLUNK_HOME="C:\Program Files\Splunk"

C:\>%SPLUNK_HOME%\bin\splunk install app "\Users\WhateverYourNameIs"\Downloads\splunkclouduf.spl -auth admin:changeme

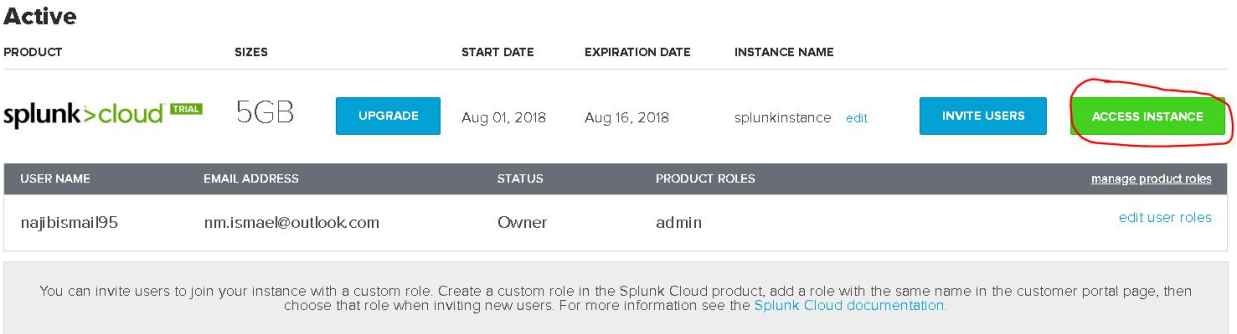
When restarting the Splunk instance, after setting up the forwarder credentials; there is a command to restart it but you need to cd into the Splunk folder in your program files, after that you need to specify your environment variables then cd into the bin and then run the command. Example below

C:\Program Files\Splunk>%SPLUNK_HOME%\bin\splunk restart

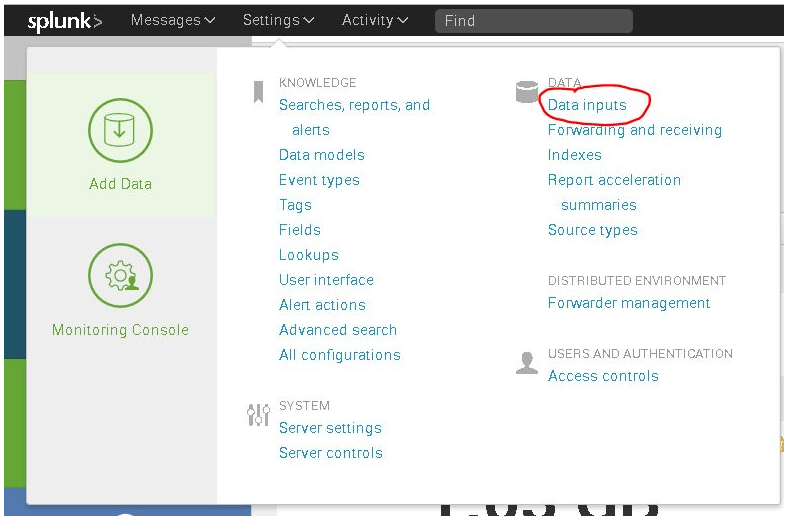
1) In order to get a new Splunk Cloud hooked up to our Forwarder, sign up for an account on Splunk.com and make sure to choose Cloud
2) Once you have a Cloud Account, you will go to your instances



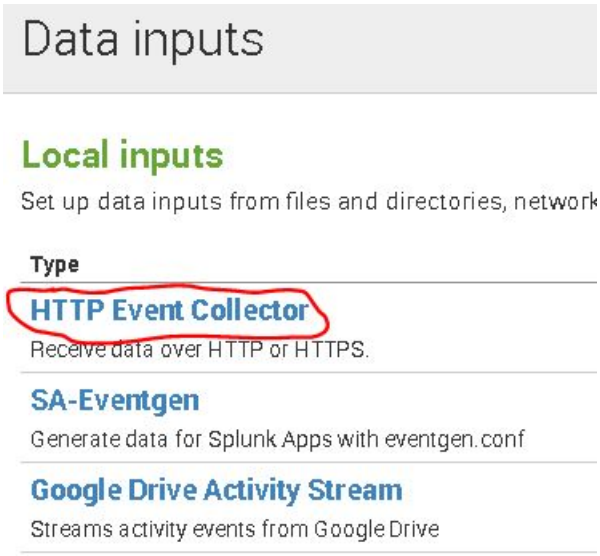
3) You will Access Instance



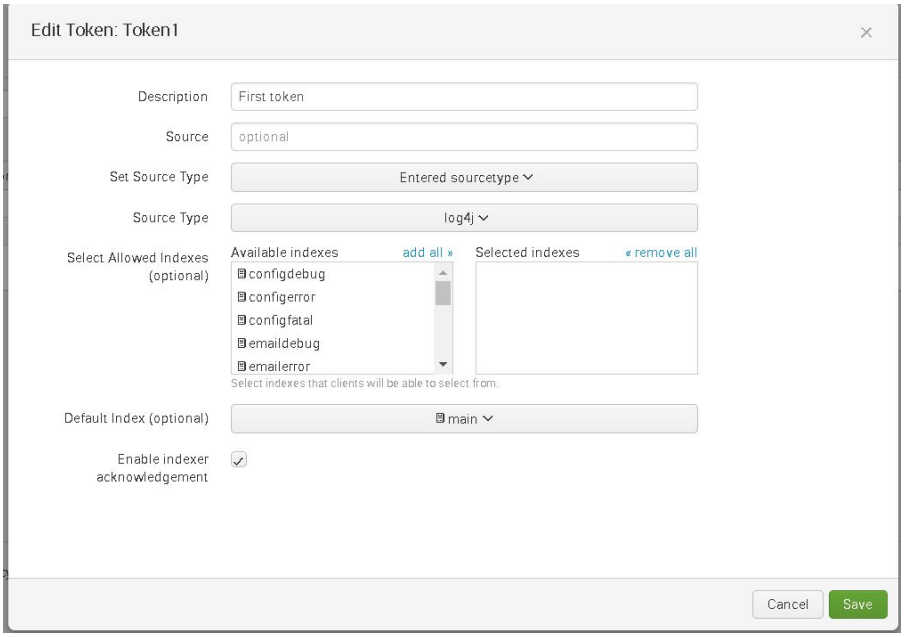
4) Go to Data Inputs



5) Go to HTTP Event Collector



6) Make a new token which acts as our unique ID in a way between the Forwarder and Cloud



5

7) This is what the configuration looks like on Jenkins