KPLABS Course

Splunk 2021 - Beginner to Architect

Domain 2

ISSUED BY
Zeal

REPRESENTATIVE
instructors@kplabs.in

Domain 2 - Getting started with Splunk

Module 1: Importing Data in Splunk

1.1 Import Data to Splunk

Before we start to build amazing dashboards, first we need to import some data to splunk.

Data Type	Description
HTTP Access Logs	Records data of requests processed by Web-Server.
Linux Authentication Logs	Authentication Success & Failure Related Messages.

1.2 Overview of Source Types

The source type is one of the default fields that the Splunk platform assigns to all incoming data.

It tells the platform what kind of data you have, so that it can format the data intelligently during indexing.

```
209.160.24.63 - - [18/Oct/2018:18:22:17] "GET /product.screen?productId=BS-AG-
G09&JSESSIONID=SD0SL6FF7ADFF4953 HTTP 1.1" 200 2550 "http://www.buttercupgames.com/product.screen?
productId=BS-AG-G09" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko)
Chrome/19.0.1084.46 Safari/536.5" 422
```

1.3 HTTP Access Logs

```
209.160.24.63 - - [18/Oct/2018:18:22:17] "GET /product.screen?productId=BS-AG-
G09&JSESSIONID=SD0SL6FF7ADFF4953 HTTP 1.1" 200 2550 "http://www.buttercupgames.com/product.screen?
productId=BS-AG-G09" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko)
Chrome/19.0.1084.46 Safari/536.5" 422
```

Extracted Information	Description
209.160.24.63	Client IP Address who made request.
[18/Oct/2018:18:22:17]	Timestamp of the Request
GET	HTTP Method
200	Response Success.
BS-AG-G09	Product ID

1.4 Setting Right Source Types

When we add some data to splunk, we have to set the right source type so that the data can be formatted.

Add this data. It is associated with source type of access_combined.

```
209.160.24.63 - - [18/Oct/2018:18:22:17] "GET /product.screen?productId=BS-AG-
G09&JSESSIONID=SD0SL6FF7ADFF4953 HTTP 1.1" 200 2550 "http://www.buttercupgames.com/product.screen?
productId=BS-AG-G09" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko)
Chrome/19.0.1084.46 Safari/536.5" 422
```

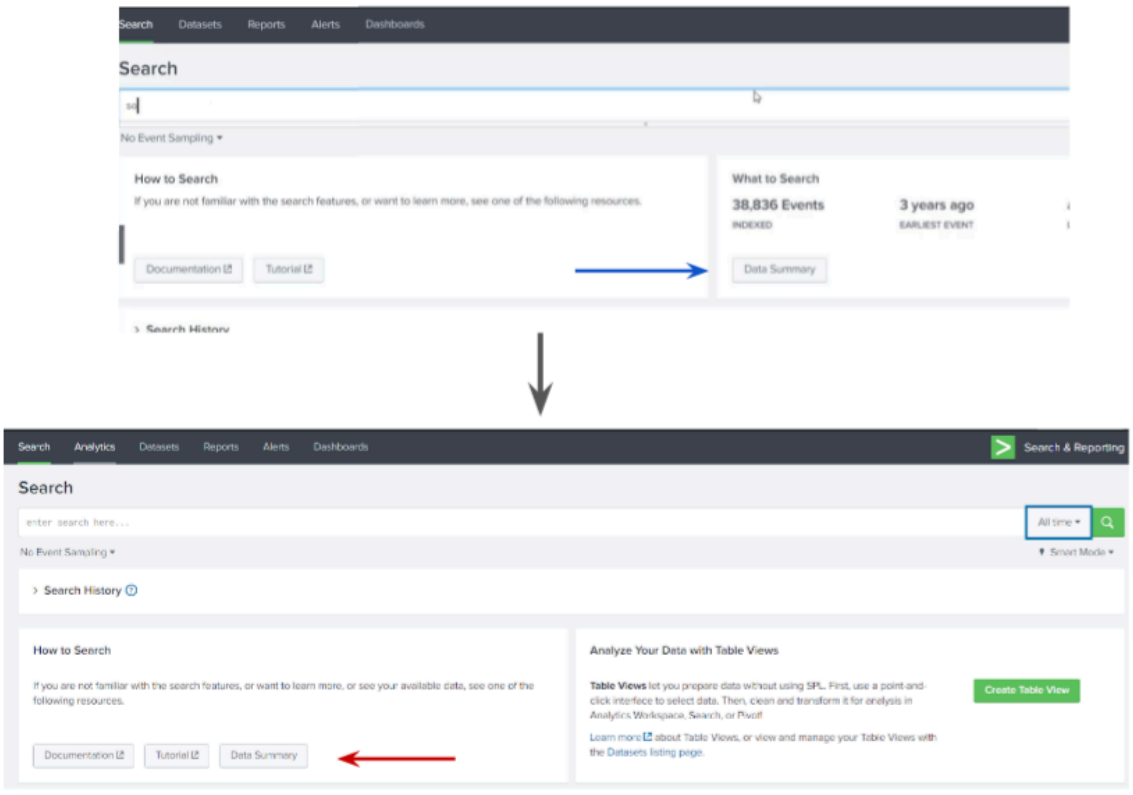
1.5 Important Note

Most of the common types of data are easily parsed by Splunk considering right source type are associated with it.

Additional Splunk Add Ons are available in marketplaces that can also parse the data for a specific source type.

For custom data, you can create your own parser that can parse the data.

1.6 Minor Changes Across Versions



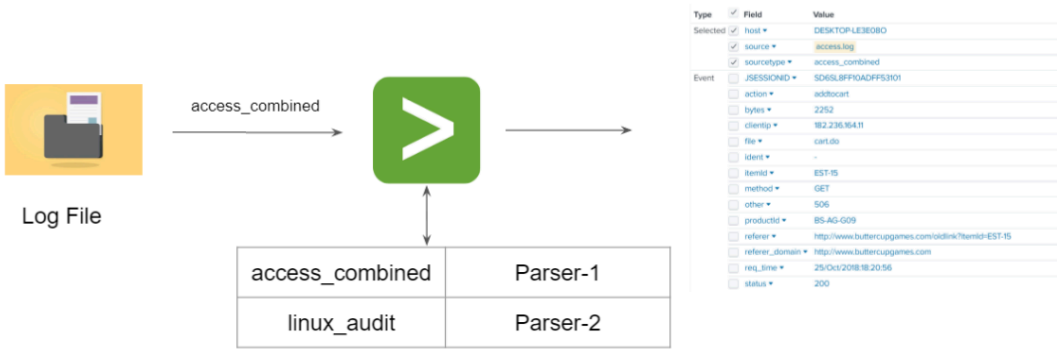
.

Module 2: Parsing Authentication Logs

2.1 Revising Log Parsing

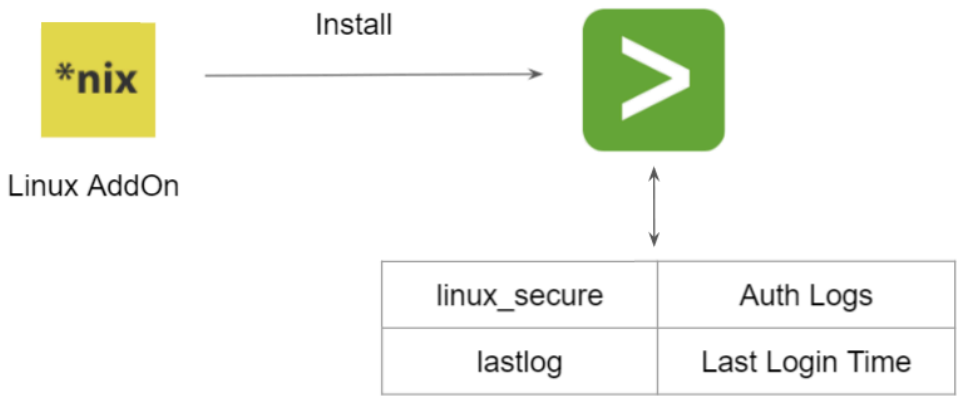
Whenever we upload the log file, it is important to set the right source type associated with it.

This allows Splunk to parse the log accordingly.



2.2 Parsing Linux Authentication Logs

For the logs that are not parsed by splunk, you can install various AddOns from Splunk marketplace that can do the parsing for us.



Module 3: Security Use-Case - Finding Attack Vectors

3.1 Current Scenario

At this stage, we have the Linux Authentication logs available in Splunk and are parsed.

The important part is what you do with these log files.

3.2 Use-Case: Find Attack Vectors

Compliance auditor has requested you to find certain attack vectors related to SSH Logins.

Following are the requirements set by the auditor:

Sr No	Requirement
1	Find the total number of SSH failed login attempts.
2	Find how many failed logins from every IPs.
3	Find List of Countries from which the failed login attempts were made.
4	Create a visualization of countries in world map based on failed logins.

3.3 SPL Command - stats

Calculates aggregate statistics, such as average, count, and sum, over the results set.

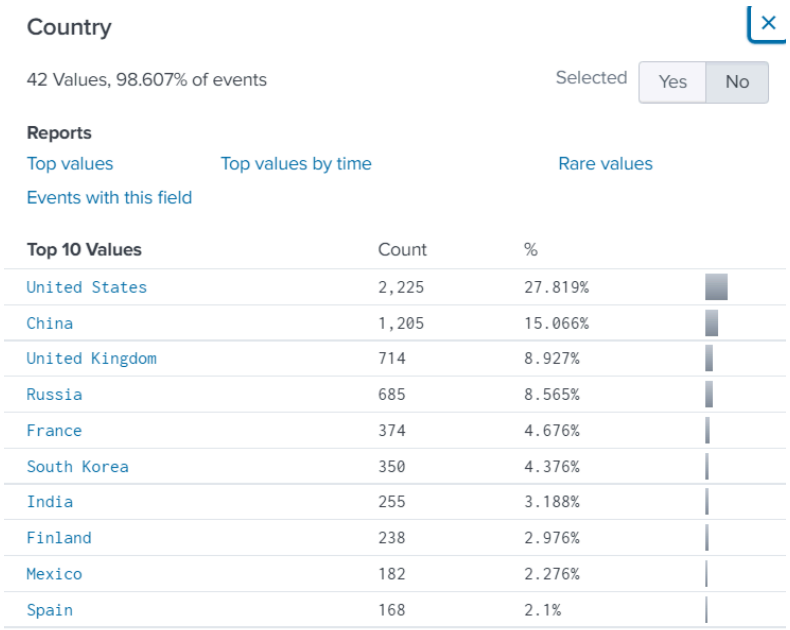
We have following data: List of IP Address, Failed Attempts

Count number of failed attempts from every IP addresses.

host	GET
www1	8413
www2	4654

3.4 SPL Command - iplocation

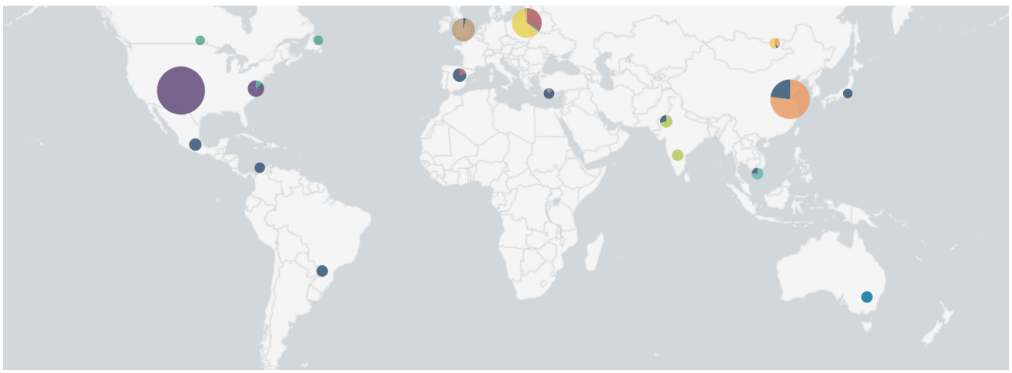
Extracts location information from IP addresses by using 3rd-party databases. This command supports IPv4 and IPv6.



3.5 SPL Command - geostats

geostats command is used to generate statistics to display geographic data and summarize the data on maps.

The command generates statistics which are clustered into geographical bins to be rendered on a world map.



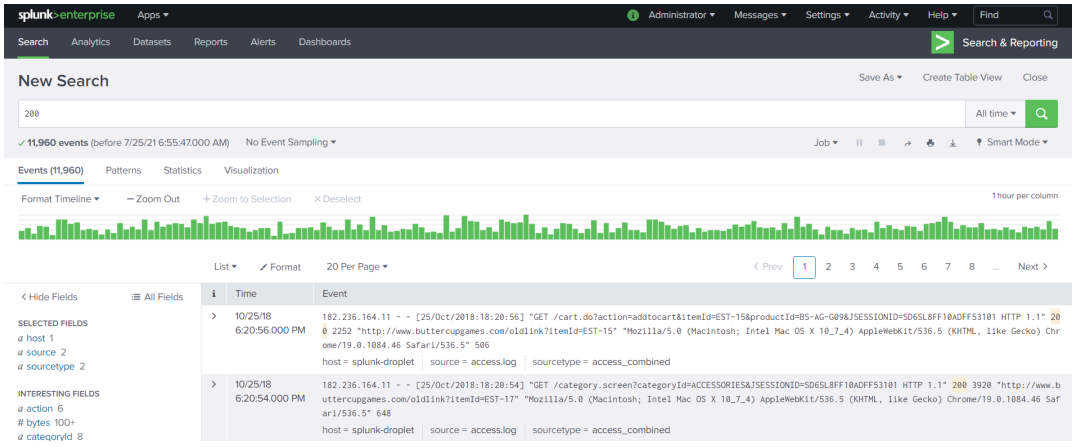
3.6 Search Filters for Use-Case

Requirement	Final Command
Total number of SSH failed login attempts.	source="secure.log" action=failure
Find how many failed logins from every IPs.	source="secure.log" action=failure | stats count by src
Find List of Countries from which the failed login attempts were made.	source="secure.log" action=failure | iplocation src
Create a visualization of countries in world map based on failed logins.	source="secure.log" action=failure | iplocation src | geostats count by Country

Module 3: Basics of Search

4.1 Basics of Search

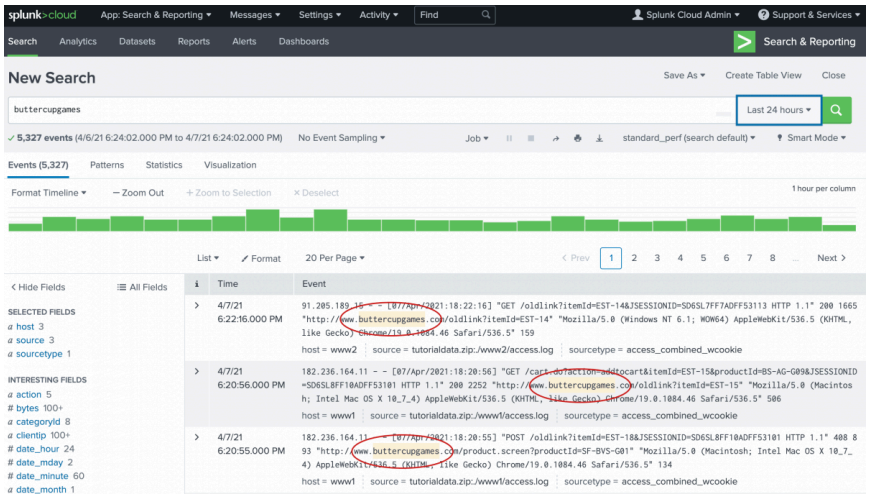
One of the easiest ways to search for a specific data is to type in the search string.



4.2 Time Range Picker

Restricting, or filtering, your search criteria using a time range is the easiest and most effective way to optimize your searches.

You can use time ranges to troubleshoot an issue, if you know the approximate timeframe when the issue occurred.



4.3 Boolean Expressions

The Splunk search processing language (SPL) supports the Boolean operators: AND, OR, and NOT.

Use-Case	SPL
Search for all failed login attempts for user root	root AND failed
Search for failed logins for all user except root	failed NOT root
Search failed logins for user admin OR root	failed admin OR root

The AND operator is always implied between terms, that is: web error is the same as web AND error. So unless you want to include it for clarity reasons, you should not need to specify the AND operator.

4.4 Search Modes

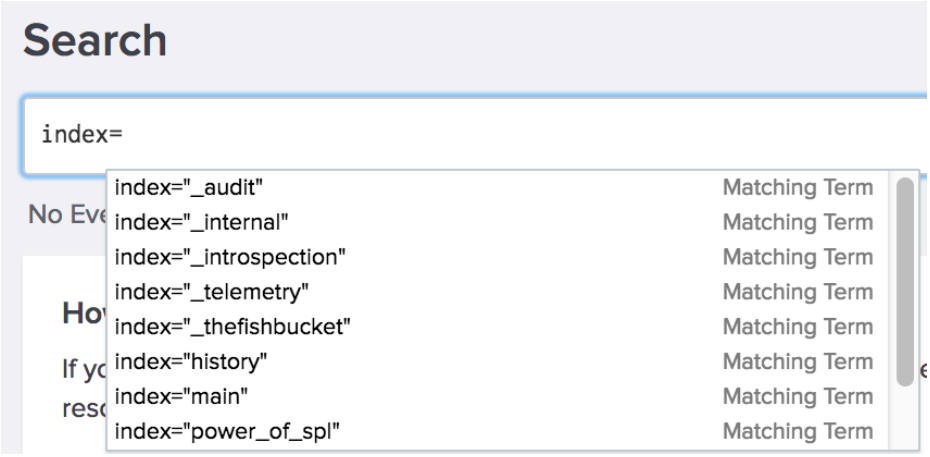
You can use the Search Mode selector to provide a search experience that fits your needs.

Search Modes	Description
Fast Mode	Field discovery is disabled for this mode for better performance.
Verbose Mode	Returns all of the field and event data it possibly can, even if it means the search takes longer to complete.
Smart Mode	Toggles behaviour based on the type of search

Module 5: Splunk Search Assistant

5.1 Overview of Splunk Search Assistant

When you begin typing certain letters or terms into the search bar, the search assistant will begin to show you terms and searches that match what you are typing.



5.2 Search Assistant Modes

Splunk Search Assistant has three modes:

- Full
- Compact
- None

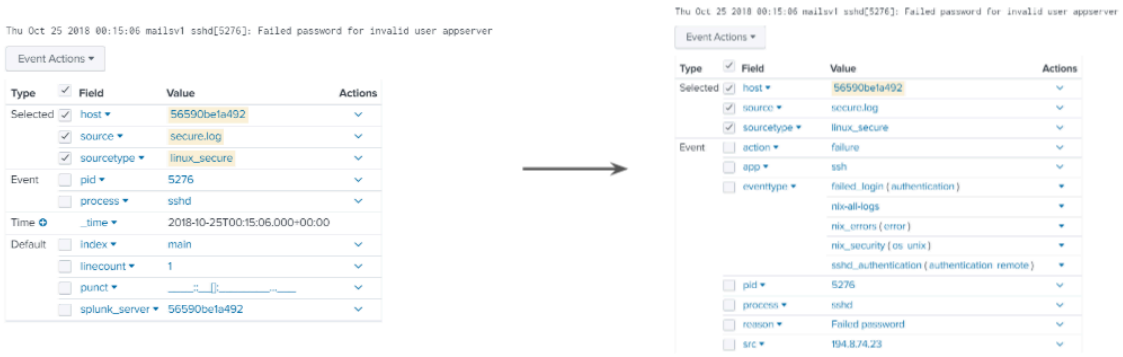
By default, the compact mode is selected but can be changed from Account Settings.

Module 6: Understanding Add-Ons and Apps

6.1 Use-Case: Linux Authentication Logs

In our previous section, where we had uploaded the Linux authentication logs, we observed that the logs were not parsed by default.

However, after installing the Linux Add-On, the log was automatically parsed.



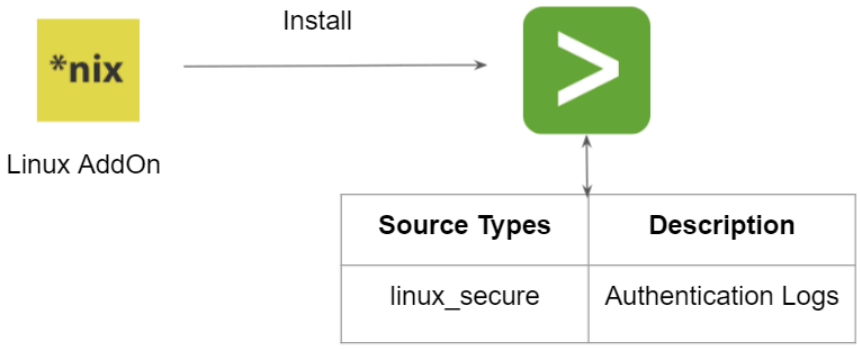
Before AddOn

After AddOn

6.2 Overview of Splunk Add-ons

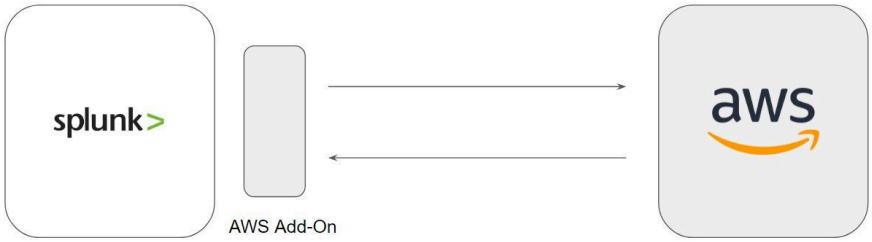
Add-ons extend the functionality of the Splunk platform and provide required field extractions, lookups, saved searches, and others.

For the logs that Splunk does not parse by default, you can install various AddOns from the Splunk marketplace to do the parsing for us.



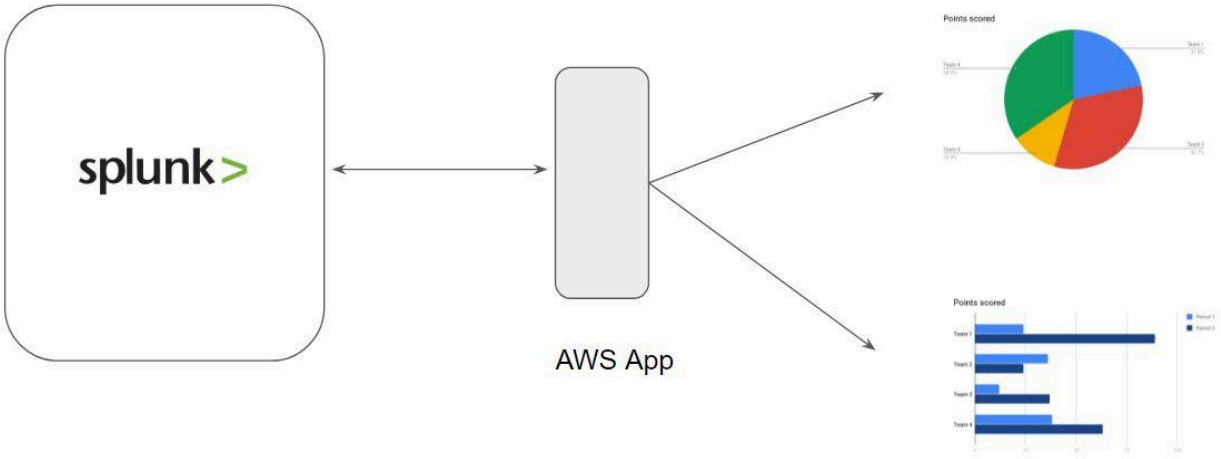
6.3 Splunk Add-on For Data Input

Add-ons can also be used to extract data from a specific destination.



6.4 Overview of Splunk Apps

Apps deliver user experience that makes data immediately useful typically with pre-built dashboards that makes data easy to analyze.



6.5 Apps and Addon Support

There are three types of support criteria that you will generally see in splunkbase:

- Splunk Supported
- Developer Supported
- Community Supported

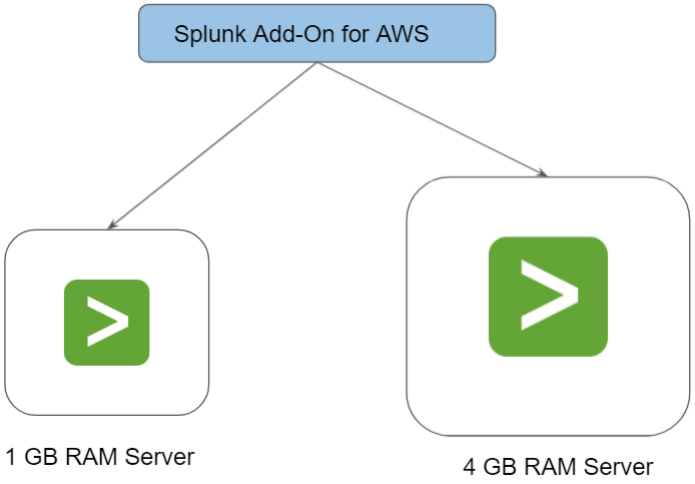
By default, the Splunk platform includes one basic app that allows us to work with our data; the Search and Reporting app.

6.6 Important Note - Hardware Considerations

Some of the Splunk Add-ons and Apps are resource heavy.

Running them in instance with lower hardware will lead to Splunk/Server going down or becoming unresponsive.

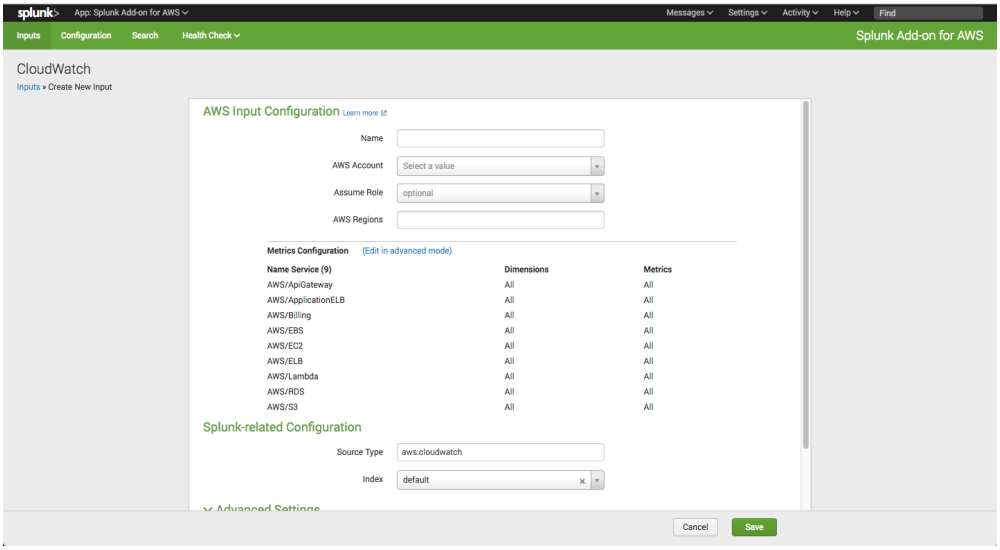
6.7 Demo - Different Hardware for Add-On



Module 7: Installing Splunk Add-On for AWS

7.1 Splunk Add-On For AWS

The Splunk Add-on for Amazon Web Services allows a Splunk software administrator to collect AWS related data and logs.



7.2 Checks while Installing Add-Ons in Splunk

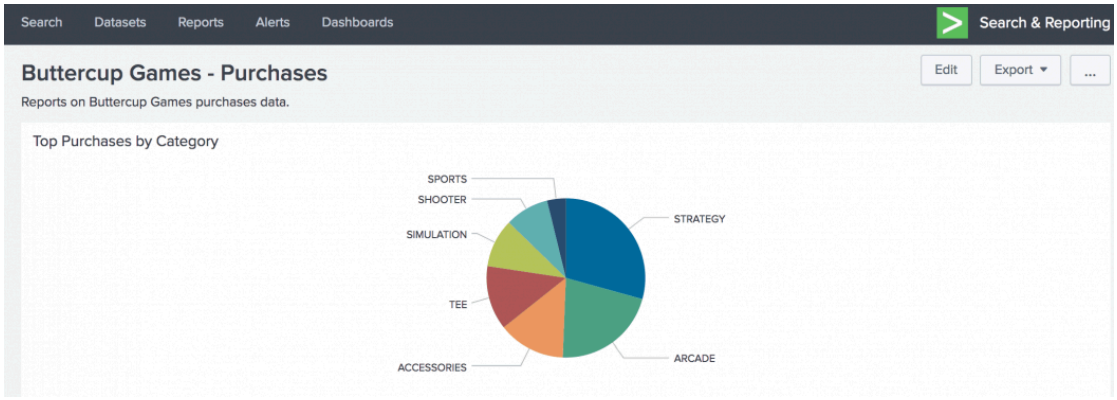
There are certain important checks to make before installing a Splunk Add-On.

1. Add-On must support your Splunk version.
2. Hardware requirements for the Add-On.
3. Support Type

Module 8: Dashboards and Panels

Splunk Dashboards are views that consist of panels.

Panel can contain search boxes, text boxes, charts, tables, etc.



Join Our Discord Community

We invite you to join our Discord community, where you can interact with our support team for any course-based technical queries and connect with other students who are doing the same course.

Joining URL:

http://kplabs.in/chat