



KPLABS Course

Splunk 2021 - Beginner to Architect

Domain 5

ISSUED BY

Zeal

REPRESENTATIVE

instructors@kplabs.in



Domain 5 - Post Installation Activities

Module 1: Understanding Regular Expressions

1.1 Basics of Regular Expressions

Regular Expressions (regex) is a sequence of characters that defines a search pattern.

“There is a Rainbow which arises on the south shore of Mumbai”

Rainbow - Literal Character

Meta Character is a character or sequence of character that has a special meaning that provides information about the other characters

1.2 Meta Characters

\d - Any digit from 0-9

\w - Any word (A-Z, a-z, 0-9]

\s - whitespace

. - Any character.

[] - Matches characters in brackets.

[^] - Matches characters not in brackets.

Module 2: Parsing Web Server Logs & Named Group Expression

2.1 Getting the basics straight

There are two ways to have data parsed in Splunk:

1. Create an addon and write a custom regex
2. Use Add-Ons from the marketplace which has a built-in regex for specific log.

Sample Log Data:

```
93.180.71.3 - - [17/May/2015:08:05:27 +0000] "GET /downloads/product_1 HTTP/1.1" 304 0 "-"  
"Debian APT-HTTP/1.3 (0.8.16~exp12ubuntu10.21)"
```

2.2 Named Capturing Group

Named Capturing group makes understanding the parsed data in a much more easier manner.

It is used extensively in various Splunk Add-Ons available in the marketplace.

Sample Syntax:

(?<name>regex)

Module 3: Importance of Source Types

In Splunk, field extractions and regex are generally defined at the source types level.

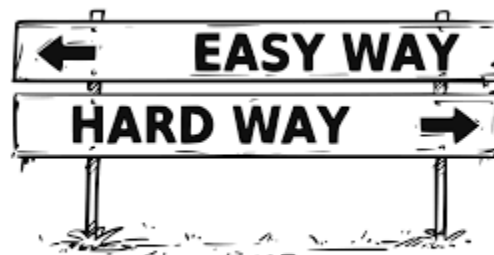
They can be defined in props.conf as well as transforms.conf

If the source type of your log is incorrect then it will not get parsed properly.

Splunk comes with some built-in source types and it's associated regex for common logs.

Module 4: Interactive Field Extractor (IFX)

Interactive Field Extractor allows us to teach Splunk on how to extract fields from your data without writing regex.



Module 5: props.conf and transforms.conf

5.1 Creating Custom Source Types

Splunk comes with default source types and field extractions for common log files.

However, we can create our own custom source type as well.

Every source type has some associated configuration settings.

These configuration parameters and source type details are stored in props and transforms.

5.2 Props and Transforms

In props.conf, we define that event with source type XXXX has the extraction of YYYY applied to it during the search time.

transforms.conf contains the actual extractions.

Module 6: Splunk Event Types

6.1 Understanding EventTypes

EventTypes are categorization systems to help you make sense of your data.

`sourcetype=access_combined status=200 action=purchase`



If you save the above as an eventtype `success_purchase`, any event that gets returned by the search gets associated eventtype

6.2 Limitation of EventTypes

We cannot have event type based on search which has the following aspects:

- i) Includes pipe operator after a simple search.
- ii) Includes a sub-search.

Module 7: Tags

Tags enable you to assign names to specific field and value combinations, including event type, host, source, or source type.

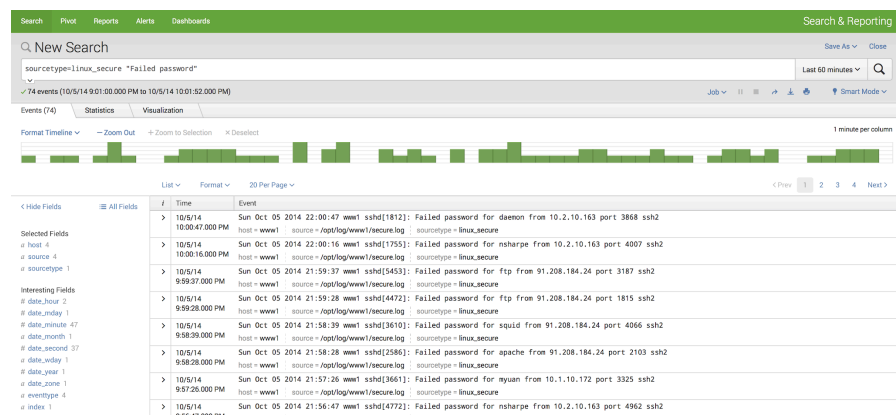
Example Use Case:

Your Network Logs have IP addresses belonging to three subnets.

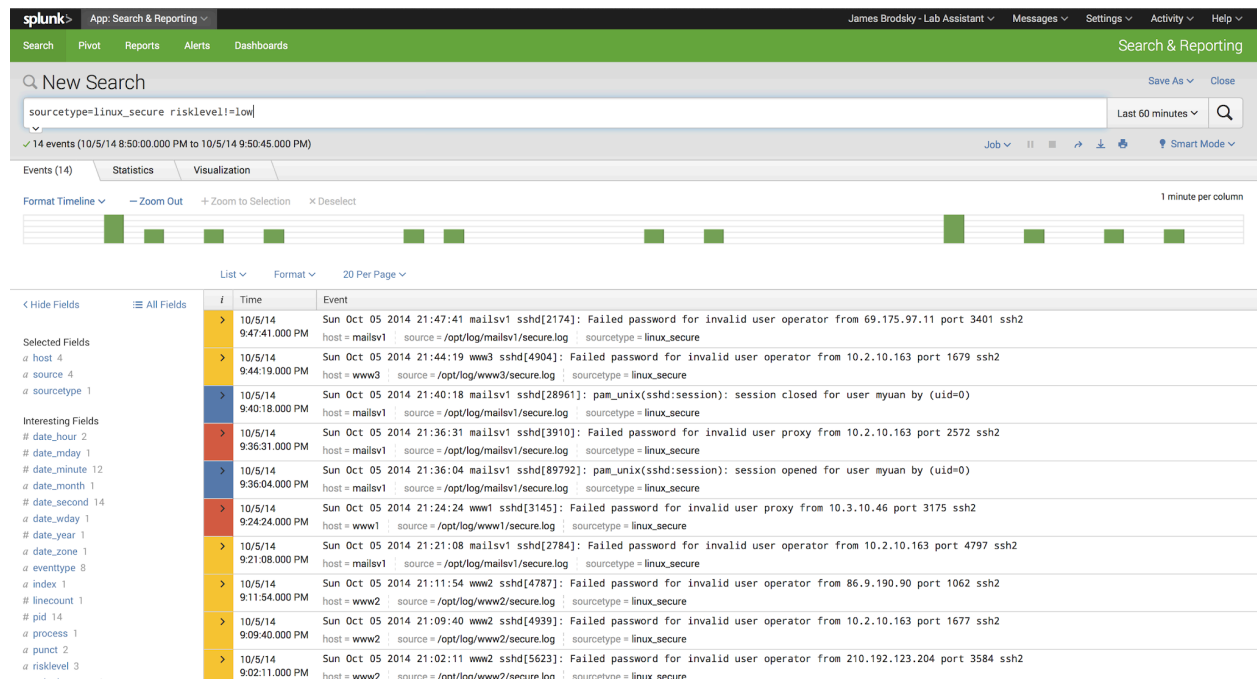
- 192.168.10.0/24 Tag: Singapore region VPC
- 10.77.0.0/16 Tag: Tag: Mumbai region VPC
- 10.66.0.0/16 Tag: Tag: Oregon region VPC

Module 8: Splunk Events Types Priority and Coloring Scheme

Typically event type field gets attached to the matching events when wildcard search is used.



However, with colored events, we can easily identify events by the associated color to indicate the overall severity.



Module 9: Splunk Lookups

Lookups enhance the power of Splunk by enabling correlation of search results with 3rd party data like databases, directories, CSV files, and others.

It allows us to co-relate external information with the search results.

Let's understand with an example:

Event in Splunk might contain customerID field.

We want to get more information like customerName, customerNumber which are stored externally in files.

Module 10: Splunk Alerts

Alerts are used to monitor and respond to a particular event.

Alerts not necessarily mean to send an email on a specific action, it can do much more better things like event-driven action.

Throttling of alerts is also an important factor during an outage.