Rex tutorial for java : https://www.geeksforgeeks.org/write-regular-expressions/

Splunk - > Rex

Normal query | rex field=<field Name> “… ( ?<field name> …)…. Post pattern



Pre pattern extract pattern



Eg. Hi , Abhaya is a good boy !

If want to extract “Abhaya” from the line then : all the string or whatever before “Abhay” in line is pre-Pattern . And whatever comes after ‘Abhay” is post-pattern .

Example:

Index=”i18v-pr” “namespace\_name”:”i18v-prod-apollo” “Kubernetes.labels.ApolloService”:”\*intermittence\*” | rex field=log “.?\]\s+(?<log>.\*)”



Note: <log> this diamond symbol will throw error so we need to use - > &lt;log&gt; in place of diamond

Index=”i18v-pr” “namespace\_name”:”i18v-prod-apollo” “Kubernetes.labels.ApolloService”:”\*intermittence\*” | rex field=log “.?\]\s+(?&lt;log&gt;.\*)”



Here : log - > is existing field in splunk

Log - > inside the<log> is the variable which put all the values in .