

Lab Report — Using Basic Search in Splunk

Name: Dhruvish

Date: October 19, 2025

Platform: Splunk Cloud Trial

Objective

The purpose of this lab was to strengthen foundational **Search Processing Language (SPL)** skills within Splunk, focusing on keyword queries, Boolean logic, field/value filters, wildcards, time controls, and simple result shaping techniques like fields, table, dedup, and sort.

These are core competencies for log analysis, security monitoring, and SIEM (Security Information and Event Management) operations.

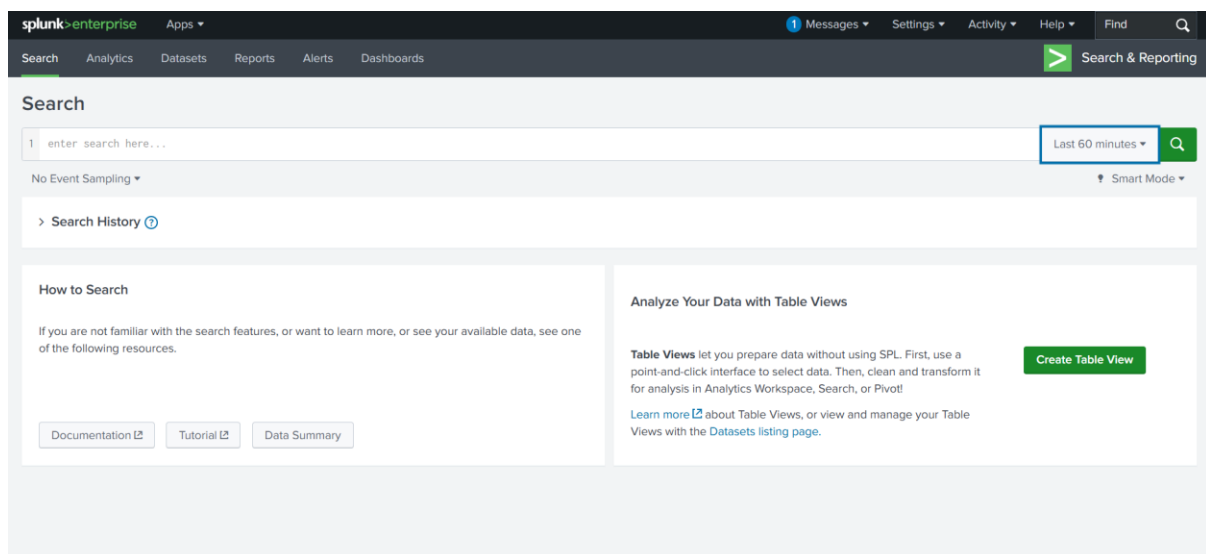
Tools Used

- **Splunk Cloud Trial** (or local Splunk Free installation)
- **Web Browser**

Procedure and Results

Step 1: Open Search & Set Time

- Logged into **Splunk Cloud Trial**.
- Navigated to **Apps ► Search & Reporting**.
- Time range set to **Last 60 minutes**.
- Ensured **Search Mode = Smart**.



Step 2: Keyword & Phrase Search

- **Command:**

index=_internal error

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query `index=_internal error`. The results show 7,508 events. A visualization at the top shows a bar chart of event counts over time. Below the chart, a table lists the events. The first event is a warning from the supervisor log, and the second is an error from the splunkd log.

i	Time	Event
>	10/19/25 1:54:18.000 PM	2025/10/19 13:54:18 [WARN] error registering data endpoints registration failed with status code: 403 host = LAPTOP-EU4VF6GR source = C:\Program Files\Splunk\var\log\splunk\supervisor.log sourcetype = supervisor-2
>	10/19/25 1:54:17.293 PM	10-19-2025 13:54:17.293 +0530 ERROR ExecProcessor [19184 ExecProcessor] - message from "C:\Program Files\Splunk\bin\Python3.9.exe" "C:\Program Files\Splunk\etc\apps\splunk_assist\bin\uiassets_modular_input.py" . host = LAPTOP-EU4VF6GR source = C:\Program Files\Splunk\var\log\splunk\splunkd.log sourcetype = splunkd
>	10/19/25 1:54:17.293 PM	10-19-2025 13:54:17.293 +0530 ERROR ExecProcessor [19184 ExecProcessor] - message from "C:\Program Files\Splunk\bin\Python3.9.exe" "C:\Program Files\Splunk\etc\apps\splunk_assist\bin\uiassets_modular_input.py" splunk.LicenseRestriction: [HTTP 402] Current license d oes not allow the requested action host = LAPTOP-EU4VF6GR source = C:\Program Files\Splunk\var\log\splunk\splunkd.log sourcetype = splunkd

Returned events containing the keyword “error.”

- **Phrase Search:**

index=_internal "rest handler"

Used quotes for exact phrase matching. Confirmed that searches are **case-insensitive** by default.

Step 3: Boolean Logic

Practiced combining logical operators to refine searches.

- **Errors or warnings:**

index=_internal (error OR warn)

The screenshot shows the Splunk Enterprise search interface with the query `index=_internal (error OR warn)`. The results show 7,948 events. A visualization at the top shows a bar chart of event counts over time. Below the chart, a table lists the events. The first event is an error from the splunkd log, and the second is a warning from the supervisor log.

i	Time	Event
>	10/19/25 1:56:33.001 PM	10-19-2025 13:56:33.001 +0530 ERROR ExecProcessor [19184 ExecProcessor] - message from "C:\Program Files\Splunk\bin\Python3.9.exe" "C:\Program Files\Splunk\etc\apps\splunk_assist\bin\uiassets_modular_input.py" . host = LAPTOP-EU4VF6GR source = C:\Program Files\Splunk\var\log\splunk\splunkd.log sourcetype = splunkd
>	10/19/25 1:56:33.001 PM	10-19-2025 13:56:33.001 +0530 ERROR ExecProcessor [19184 ExecProcessor] - message from "C:\Program Files\Splunk\bin\Python3.9.exe" "C:\Program Files\Splunk\etc\apps\splunk_assist\bin\uiassets_modular_input.py" splunk.LicenseRestriction: [HTTP 402] Current license d oes not allow the requested action host = LAPTOP-EU4VF6GR source = C:\Program Files\Splunk\var\log\splunk\splunkd.log sourcetype = splunkd
>	10/19/25 1:56:33.001 PM	10-19-2025 13:56:33.001 +0530 ERROR ExecProcessor [19184 ExecProcessor] - message from "C:\Program Files\Splunk\bin\Python3.9.exe" "C:\Program Files\Splunk\etc\apps\splunk_assist\bin\uiassets_modular_input.py" raise splunk.LicenseRestriction

- Errors but not UI-related:

index=_internal error NOT ui

- Grouped logic example:

index=_internal (error OR fail) (http OR tcp)

Step 4: Field/Value Filters

Used field filters for more precise searches.

- By sourcetype:

index=_internal sourcetype=splunkd

New Search

1 index=_internal sourcetype=splunkd

✓ 24,775 events (10/19/25 12:58:00.000 PM to 10/19/25 1:58:48.000 PM) No Event Sampling

Events (24,775) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

1 minute per column

List Format 20 Per Page

i	Time	Event
>	10/19/25 1:58:47.799 PM	10-19-2025 13:58:47.799 +0530 ERROR ExecProcessor [19184 ExecProcessor] - message from "C:\Program Files\Splunk\bin\Python3.9.exe" "C:\Program Files\Splunk\etc\apps\splunk_assist\bin\supervisor_modular_input.py" . host = LAPTOP-EU4VF6GR source = C:\Program Files\Splunk\var\log\splunk\splunkd.log sourcetype = splunkd
>	10/19/25 1:58:47.799 PM	10-19-2025 13:58:47.799 +0530 ERROR ExecProcessor [19184 ExecProcessor] - message from "C:\Program Files\Splunk\bin\Python3.9.exe" "C:\Program Files\Splunk\etc\apps\splunk_assist\bin\supervisor_modular_input.py" splunk.LicenseRestriction: [HTTP 402] Current license does not allow the requested action host = LAPTOP-EU4VF6GR source = C:\Program Files\Splunk\var\log\splunk\splunkd.log sourcetype = splunkd
>	10/19/25 1:58:47.799 PM	10-19-2025 13:58:47.799 +0530 ERROR ExecProcessor [19184 ExecProcessor] - message from "C:\Program Files\Splunk\bin\Python3.9.exe" "C:\Program Files\Splunk\etc\apps\splunk_assist\bin\supervisor_modular_input.py" raise splunk.LicenseRestriction

- By source path (wildcard):

index=_internal source="*metrics.log"

New Search

1 index=_internal source="*metrics.log"

✓ 14,548 events (10/19/25 12:59:00.000 PM to 10/19/25 1:59:20.000 PM) No Event Sampling

Events (14,548) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

1 minute per column

List Format 20 Per Page

i	Time	Event
>	10/19/25 1:58:54.679 PM	10-19-2025 13:58:54.679 +0530 INFO Metrics - group=thruput, name=thruput, instantaneous_kbps="6.054", instantaneous_eps="21.071", average_kbps="3.434", total_k_processed="530771.000", kb="181.571", ev=632 host = LAPTOP-EU4VF6GR source = C:\Program Files\Splunk\var\log\splunk\metrics.log sourcetype = splunkd
>	10/19/25 1:58:54.679 PM	10-19-2025 13:58:54.679 +0530 INFO Metrics - group=thruput, name=index_thruput, instantaneous_kbps="6.050", instantaneous_eps="19.404", average_kbps="3.433", total_k_processed="530692.000", kb="181.448", ev=582 host = LAPTOP-EU4VF6GR source = C:\Program Files\Splunk\var\log\splunk\metrics.log sourcetype = splunkd
>	10/19/25 1:58:54.679 PM	10-19-2025 13:58:54.679 +0530 INFO Metrics - group=queue, name=typingqueue, max_size_kb=500, current_size_kb=0, current_size=0, largest_t_size=166, smallest_size=0 host = LAPTOP-EU4VF6GR source = C:\Program Files\Splunk\var\log\splunk\metrics.log sourcetype = splunkd

- Combined with Boolean logic:

`index=_internal sourcetype=splunkd (error OR warn)`

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query `index=_internal sourcetype=splunkd (error OR warn)`. Below the search bar, it indicates 8,189 events found for the time range 10/19/25 12:59:00.000 PM to 10/19/25 1:59:58.000 PM. The interface includes a visualization section with a bar chart and a table of events. The table shows three events, all with a severity of ERROR, occurring at 10/19/25 1:59:47.728 PM. The events are related to a message from a Python script and a license restriction error.

i	Time	Event
>	10/19/25 1:59:47.728 PM	10-19-2025 13:59:47.728 +0530 ERROR ExecProcessor [19184 ExecProcessor] - message from "C:\Program Files\Splunk\bin\Python3.9.exe" "C:\Program Files\Splunk\etc\apps\splunk_assist\bin\uiassets_modular_input.py" . host = LAPTOP-EU4VF6GR source = C:\Program Files\Splunk\var\log\splunk\splunkd.log sourcetype = splunkd
>	10/19/25 1:59:47.728 PM	10-19-2025 13:59:47.728 +0530 ERROR ExecProcessor [19184 ExecProcessor] - message from "C:\Program Files\Splunk\bin\Python3.9.exe" "C:\Program Files\Splunk\etc\apps\splunk_assist\bin\uiassets_modular_input.py" splunk.LicenseRestriction: [HTTP 402] Current license does not allow the requested action host = LAPTOP-EU4VF6GR source = C:\Program Files\Splunk\var\log\splunk\splunkd.log sourcetype = splunkd
>	10/19/25 1:59:47.728 PM	10-19-2025 13:59:47.728 +0530 ERROR ExecProcessor [19184 ExecProcessor] - message from "C:\Program Files\Splunk\bin\Python3.9.exe" "C:\Program Files\Splunk\etc\apps\splunk_assist\bin\uiassets_modular_input.py" raise splunk.LicenseRestriction

Step 5: Wildcards & Quoting

Demonstrated wildcard and quoting techniques.

- Wildcard example:
`source="*scheduler.log"`
- Quoted value example:
`sourcetype="splunkd_ui_access"`

Step 6: Time Control in SPL

Controlled search time windows directly in SPL.

- Last 2 hours (rounded):
`index=_internal earliest=-2h@h latest=@h`

splunk>enterprise Apps ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find 🔍

Search Analytics Datasets Reports Alerts Dashboards **Search & Reporting**

New Search

1 `index=_internal earliest=-2h latest=@h` Last 60 minutes 🔍

✓ 19,580 events (10/19/25 11:30:00.000 AM to 10/19/25 1:30:00.000 PM) No Event Sampling ▾

Events (19,580) Patterns Statistics Visualization

Format Timeline ▾ Zoom Out + Zoom to Selection × Deselect 1 minute per column

List ▾ Format 20 Per Page ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

Time	Event
10/19/25 1:29:59.209 PM	10-19-2025 13:29:59.209 +0530 INFO TailReader [15488 tailreader0] - Batch input finished reading file='C:\Program Files\Splunk\var\spool\splunk\tracker.log' host = LAPTOP-EU4VF6GR source = C:\Program Files\Splunk\var\log\splunk\splunkd.log sourcetype = splunkd
10/19/25 1:29:56.213 PM	10-19-2025 13:29:56.213 +0530 INFO RegisterPackageHandler [16388 TcpChannelThread] - DISPATCH::REGISTER_PACKAGE_ENDPOINTS method=POST host = LAPTOP-EU4VF6GR source = C:\Program Files\Splunk\var\log\splunk\splunkd.log sourcetype = splunkd
10/19/25 1:29:56.213 PM	127.0.0.1 - splunk-system-user [19/Oct/2025:13:29:56.213 +0530] "POST /services/register-package-endpoints/output_mode=json HTTP/1.1" 403 50 "-" "Go-http-client/1.1" - - - 1ms host = LAPTOP-EU4VF6GR source = C:\Program Files\Splunk\var\log\splunk\splunkd_access.log sourcetype = splunkd_access

SELECTED FIELDS
a host 1
a source 15
a sourcetype 10

INTERESTING FIELDS
a component 11
date_hour 5
date_mday 1
date_minute 49

- Yesterday only:

`index=_internal earliest=@d-1d latest=@d`

splunk>enterprise Apps ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find 🔍

Search Analytics Datasets Reports Alerts Dashboards **Search & Reporting**

New Search

1 `index=_internal earliest=@d-1d latest=@d` Last 60 minutes 🔍

79,287 of 79,287 events matched No Event Sampling ▾

Events (79,287) Patterns Statistics Visualization

Format Timeline ▾ Zoom Out + Zoom to Selection × Deselect 1 hour per column

List ▾ Format 20 Per Page ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

Time	Event
10/18/25 11:59:55.379 PM	10-18-2025 23:59:55.379 +0530 INFO TailReader [15488 tailreader0] - Batch input finished reading file='C:\Program Files\Splunk\var\spool\splunk\tracker.log' host = LAPTOP-EU4VF6GR source = C:\Program Files\Splunk\var\log\splunk\splunkd.log sourcetype = splunkd
10/18/25 11:59:53.045 PM	127.0.0.1 - splunk-system-user [18/Oct/2025:23:59:53.045 +0530] "GET //services/cluster/config/output_mode=json HTTP/1.0" 402 128 "-" "Python-httplib2/0.20.4 (gzip)" - - - 0ms host = LAPTOP-EU4VF6GR source = C:\Program Files\Splunk\var\log\splunk\splunkd_access.log sourcetype = splunkd_access
10/18/25 11:59:53.012 PM	127.0.0.1 - splunk-system-user [18/Oct/2025:23:59:53.012 +0530] "GET //services/server/roles?output_mode=json HTTP/1.0" 200 798 "-" "Python-httplib2/0.20.4 (gzip)" - - - 0ms host = LAPTOP-EU4VF6GR source = C:\Program Files\Splunk\var\log\splunk\splunkd_access.log sourcetype = splunkd_access

SELECTED FIELDS
a host 1
a source 17
a sourcetype 11

INTERESTING FIELDS
a component 12
date_hour 13
date_mday 1
date_minute 60

Step 7: Shape the Results

Used result-shaping commands to make data easier to read.

- Select specific fields:

`index=_internal sourcetype=splunkd error | fields _time host source sourcetype`

- Create a table view:

`index=_internal sourcetype=splunkd warn | table _time host source log_level`

[illegible]

Reflection

- **Keyword search felt too broad** during initial queries (index=_internal error) because it matched every log with the word “error.” Using **field filters** (e.g., sourcetype=splunkd) drastically improved relevance.
- **Rule of thumb:** Use table for summaries or structured reporting; stay in **raw view** during early troubleshooting.
- **Most reusable search:**
 - index=_internal sourcetype=splunkd (error OR warn)

This query is ideal for **SOC health monitoring** and can be reused for automated alerts.

Summary

This lab demonstrated how to efficiently query and interpret logs using Splunk’s SPL. Skills practiced — Boolean logic, field filtering, wildcards, time range control, and result shaping — are foundational to **SIEM analysis** and real-world **incident response** workflows.