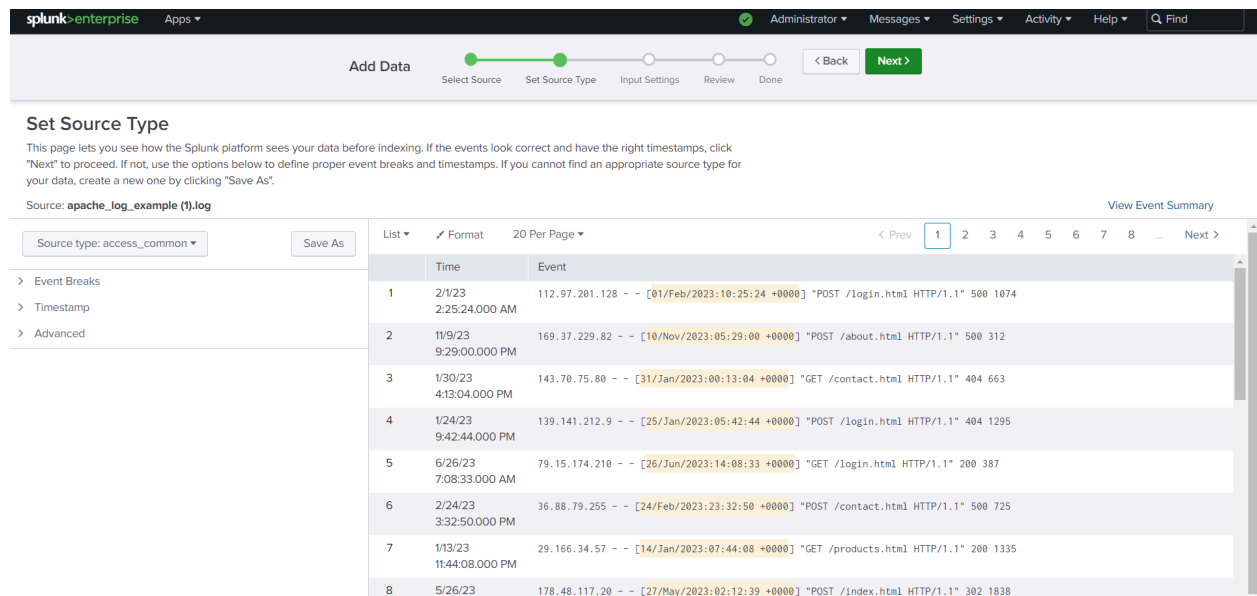


# Splunk Analysis Assignment: Apache Log Investigation

The dataset provided in the assignment is a simulated Apache log file containing 1000 entries. Each entry includes details such as the client's IP address, request date and time, the requested resource, HTTP response code, and the size of the response.

Adding the dataset in splunk and uploading it in the splunk.



**Set Source Type**

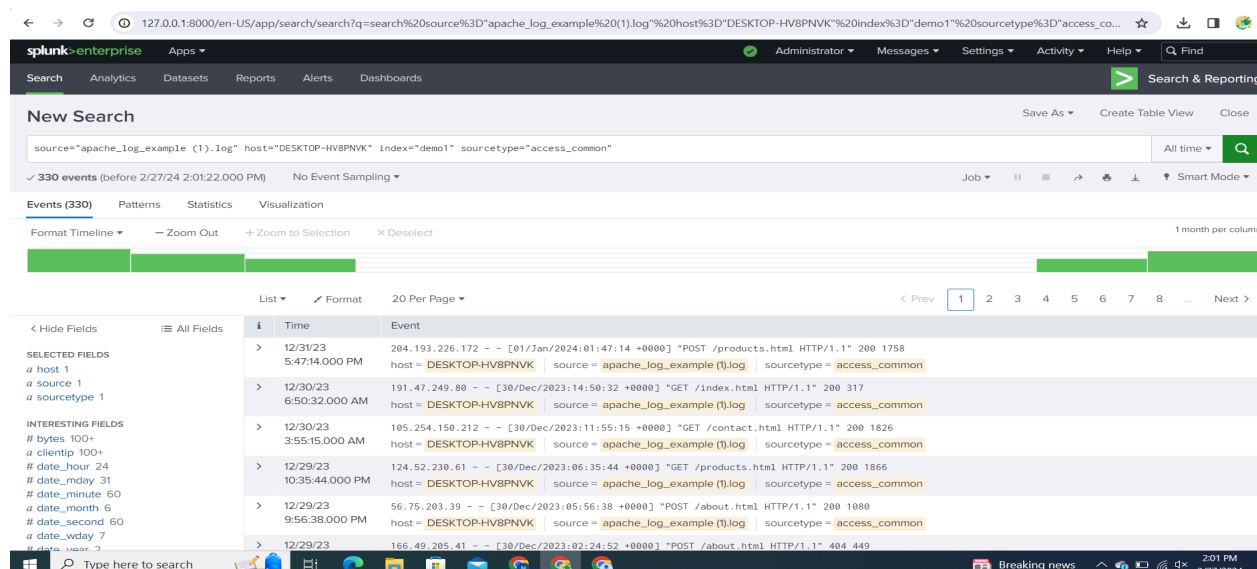
This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: `apache_log_example (1).log`

Source type: `access_common` Save As

| Time                       | Event  |
|----------------------------|--|
| 2/1/23<br>2:25:24.000 AM   | 112.97.201.128 - - [01/Feb/2023:10:25:24 +0000] "POST /login.html HTTP/1.1" 500 1074 |
| 11/9/23<br>9:29:00.000 PM  | 169.37.229.82 - - [10/Nov/2023:05:29:00 +0000] "POST /about.html HTTP/1.1" 500 312   |
| 1/30/23<br>4:13:04.000 PM  | 143.70.75.80 - - [31/Jan/2023:00:13:04 +0000] "GET /contact.html HTTP/1.1" 404 663   |
| 1/24/23<br>9:42:44.000 PM  | 139.141.212.9 - - [25/Jan/2023:05:42:44 +0000] "POST /login.html HTTP/1.1" 404 1295  |
| 6/26/23<br>7:08:33.000 AM  | 79.15.174.210 - - [26/Jun/2023:14:08:33 +0000] "GET /login.html HTTP/1.1" 200 387    |
| 2/24/23<br>3:32:50.000 PM  | 36.88.79.255 - - [24/Feb/2023:23:32:50 +0000] "POST /contact.html HTTP/1.1" 500 725  |
| 1/13/23<br>11:44:08.000 PM | 29.166.34.57 - - [14/Jan/2023:07:44:08 +0000] "GET /products.html HTTP/1.1" 200 1335 |
| 5/26/23                    | 178.48.117.20 - - [27/May/2023:02:12:39 +0000] "POST /index.html HTTP/1.1" 302 1838  |

Results of scan and report are events and its shows the logs with event id and timestamp. All total 1000 events



**New Search**

source="apache\_log\_example (1).log" host="DESKTOP-HV8PNVK" index="demo1" sourcetype="access\_common"

330 events (before 2/27/24 2:01:22.000 PM) No Event Sampling

| Time                        | Event   |
|-----------------------------|---|
| 12/31/23<br>5:47:14.000 PM  | 204.193.226.172 - - [01/Jan/2024:01:47:14 +0000] "POST /products.html HTTP/1.1" 200 1758<br>host = DESKTOP-HV8PNVK   source = apache_log_example (1).log   sourcetype = access_common |
| 12/30/23<br>6:50:32.000 AM  | 191.47.249.80 - - [30/Dec/2023:14:50:32 +0000] "GET /index.html HTTP/1.1" 200 317<br>host = DESKTOP-HV8PNVK   source = apache_log_example (1).log   sourcetype = access_common        |
| 12/30/23<br>3:55:15.000 AM  | 105.254.158.212 - - [30/Dec/2023:11:55:15 +0000] "GET /contact.html HTTP/1.1" 200 1826<br>host = DESKTOP-HV8PNVK   source = apache_log_example (1).log   sourcetype = access_common   |
| 12/29/23<br>10:35:44.000 PM | 124.52.230.61 - - [30/Dec/2023:06:35:44 +0000] "GET /products.html HTTP/1.1" 200 1866<br>host = DESKTOP-HV8PNVK   source = apache_log_example (1).log   sourcetype = access_common    |
| 12/29/23<br>9:56:38.000 PM  | 56.75.203.39 - - [30/Dec/2023:05:56:38 +0000] "POST /about.html HTTP/1.1" 200 1080<br>host = DESKTOP-HV8PNVK   source = apache_log_example (1).log   sourcetype = access_common       |
| 12/29/23                    | 166.49.285.41 - - [30/Dec/2023:02:24:52 +0000] "POST /about.html HTTP/1.1" 404 449  |

- How many requests were made?

source="apache\_log\_example (1).log" host="DESKTOP-HV8PNVK" index="demo1" sourcetype="access\_common" | stats count

✓ 1,000 events (before 2/27/24 2:05:13.000 PM) No Event Sampling ▼

Events Patterns **Statistics (1)** Visualization

20 Per Page ▼ Format Preview ▼

count ↕

1000

- count = 1000
- View events
- Other events
- Exclude from results
- New search

source="apache\_log\_example (1).log" host="DESKTOP-HV8PNVK" index="demo1" sourcetype="access\_common" | stats count

✓ 1,000 events (before 2/27/24 2:09:09.000 PM) No Event Sampling ▼ Job ▾ || ▮ → ↻

**Events (1,000)** Patterns Statistics (1) Visualization

Format Timeline ▼ - Zoom Out + Zoom to Selection × Deselect

List ▼ Format 20 Per Page ▼ < Prev 1 2 3 4 5 6

| < Hide Fields  | ≡ All Fields | i | Time                        | Event   |
|--|--------------|---|-----------------------------|---|
| <b>SELECTED FIELDS</b><br>a host 1<br>a source 1<br>a sourcetype 1<br><br><b>INTERESTING FIELDS</b><br># bytes 100+<br>a clientip 100+<br># date_hour 24<br># date_mday 31<br># date_minute 60<br>a date_month 12<br># date_second 60<br>a date_wday 7<br># date_year 2<br># date_zone 1<br>a file 5<br>a ident 1<br>a index 1 |              | > | 12/31/23<br>5:47:14.000 PM  | 204.193.226.172 - - [01/Jan/2024:01:47:14 +0000] "POST /products.html HTTP/1.1" 200 1758<br>host = DESKTOP-HV8PNVK source = apache_log_example (1).log sourcetype = access_common |
|  |              | > | 12/30/23<br>6:50:32.000 AM  | 191.47.249.80 - - [30/Dec/2023:14:50:32 +0000] "GET /index.html HTTP/1.1" 200 317<br>host = DESKTOP-HV8PNVK source = apache_log_example (1).log sourcetype = access_common        |
|  |              | > | 12/30/23<br>3:55:15.000 AM  | 105.254.150.212 - - [30/Dec/2023:11:55:15 +0000] "GET /contact.html HTTP/1.1" 200 1826<br>host = DESKTOP-HV8PNVK source = apache_log_example (1).log sourcetype = access_common   |
|  |              | > | 12/29/23<br>10:35:44.000 PM | 124.52.230.61 - - [30/Dec/2023:06:35:44 +0000] "GET /products.html HTTP/1.1" 200 1866<br>host = DESKTOP-HV8PNVK source = apache_log_example (1).log sourcetype = access_common    |
|  |              | > | 12/29/23<br>9:56:38.000 PM  | 56.75.203.39 - - [30/Dec/2023:05:56:38 +0000] "POST /about.html HTTP/1.1" 200 1080<br>host = DESKTOP-HV8PNVK source = apache_log_example (1).log sourcetype = access_common       |
|  |              | > | 12/29/23<br>6:24:52.000 PM  | 166.49.205.41 - - [30/Dec/2023:02:24:52 +0000] "POST /about.html HTTP/1.1" 404 449<br>host = DESKTOP-HV8PNVK source = apache_log_example (1).log sourcetype = access_common       |
|  |              | > | 12/29/23<br>9:06:32.000 AM  | 106.246.37.102 - - [29/Dec/2023:17:06:32 +0000] "GET /products.html HTTP/1.1" 404 830<br>host = DESKTOP-HV8PNVK source = apache_log_example (1).log sourcetype = access_common    |

- What are the top requested URLs?

9:06:32.000 AM host = DESKTOP-HV8PNVK source = apache\_log\_example (1).log sourcetype = access\_common

**uri**

5 Values, 100% of events Selected Yes No

**Reports**

Top values Top values by time Rare values

Events with this field

| Values         | Count | %     |
|----------------|-------|-------|
| /about.html    | 221   | 22.1% |
| /login.html    | 210   | 21%   |
| /products.html | 207   | 20.7% |
| /index.html    | 199   | 19.9% |
| /contact.html  | 163   | 16.3% |

> 12/27/23 149.105.33.158 - - [28/Dec/2023:01:24:21 +0000] "GET /contact.html HTTP/1.1" 302 1030 sourcetype = access\_common

- What are the most common response codes?

```

11 HTTP/1.1" 404 1300
... sourcetype = access_common

...ml HTTP/1.1" 200 633
... sourcetype = access_common

11 HTTP/1.1" 302 392
... sourcetype = access_common

11 HTTP/1.1" 200 643
... sourcetype = access_common

11 HTTP/1.1" 302 1624
... sourcetype = access_common

...tml HTTP/1.1" 500 1030
... sourcetype = access_common

...html HTTP/1.1" 302 713
... sourcetype = access_common

...ml HTTP/1.1" 500 312
... sourcetype = access_common

...html HTTP/1.1" 404 832
... sourcetype = access_common

...ml HTTP/1.1" 404 1843
... sourcetype = access_common

...html HTTP/1.1" 404 259
...

```

Mostly the replies are 404,200,302, 500

index="demo1" | stats dc(client\_ip)

✓ 1,000 events (before 2/27/24 2:24:29.000 PM)

No Event Sampling ▼

Events (1,000)

Patterns

Statistics (1)

Visualization

20 Per Page ▼

✍ Format

Preview ▼

dc(client\_ip) ⇅

0

The splunk auto advance search queries.

Time analysis -

New Search

index="demo1" | timechart span=1h count

✓ 1,000 events (before 2/27/24 2:25:59.000 PM)

No Event Sampling ▼

Events (1,000)

Patterns

Statistics (8,732)

Visualization

20 Per Page ▼

✍ Format

Preview ▼

\_time ⇅

2023-01-01 22:00

2023-01-01 23:00

2023-01-02 00:00

2023-01-02 01:00

2023-01-02 02:00

2023-01-02 03:00

2023-01-02 04:00

2023-01-02 05:00

2023-01-02 06:00

2023-01-02 07:00

2023-01-02 08:00

2023-01-02 09:00

2023-01-02 10:00

2023-01-02 11:00

Events (1,000)

Patterns

Statistics

Visualization

Smaller

Larger

9 patterns based on a sample of 1,000 events

⚠️

 Less than 5,000 events may produce poor patterns. Try a search in a larger time range or with fewer constraints.

13.6% <timestamp>INFO Service started successfully

11.5% <timestamp>INFO User login successful

11.5% <timestamp>WARN Disk usage exceeds 80%

11.1% <timestamp>ERROR Backup failed due to insufficient disk space

10.9% <timestamp>ERROR User login failed

10.8% <timestamp>ERROR Service failed to start

10.8% <timestamp>WARN User login attempt failed

10.3% <timestamp>WARN Service response time is slow

9.5% <timestamp>INFO Scheduled backup completed

If we create a table view we can get all the logs in a table format where you can clearly read the event.

Search Analytics Datasets Reports Alerts Dashboards

Search & Reporting

Create Table View

Cancel

\*

Q

Select existing fields

Filter existing fields

+ Add a missing existing field

☐ all fields

☒ @ \_time

☒ > \_raw

☐ # date\_hour

☐ # date\_mday

☐ # date\_minute

☐ # date\_month

☐ # date\_second

☐ # date\_wday

☐ # date\_year

☐ # date\_zone

☒ # host

☐ # index

☐ # linecount

☐ # punct

✓ Previewing 50 events (1/1/23 12:00:17:000 AM to 2/27/24 2:29:53.000 PM) Sample: Latest

| a source                    | a sourcetype | > _raw   |
|-----------------------------|--------------|--|
| system_log_example_1000.txt | demo         | 2023-01-01 23:59:42 ERROR Backup failed due to insufficient disk space |
| system_log_example_1000.txt | demo         | 2023-01-01 23:58:34 ERROR Backup failed due to insufficient disk space |
| system_log_example_1000.txt | demo         | 2023-01-01 23:58:08 WARN User login attempt failed                     |
| system_log_example_1000.txt | demo         | 2023-01-01 23:57:48 WARN Service response time is slow                 |
| system_log_example_1000.txt | demo         | 2023-01-01 23:57:47 INFO Service started successfully                  |
| system_log_example_1000.txt | demo         | 2023-01-01 23:56:49 ERROR Backup failed due to insufficient disk space |
| system_log_example_1000.txt | demo         | 2023-01-01 23:56:04 WARN User login attempt failed                     |
| system_log_example_1000.txt | demo         | 2023-01-01 23:55:43 ERROR Service failed to start                      |
| system_log_example_1000.txt | demo         | 2023-01-01 23:54:18 WARN User login attempt failed                     |
| system_log_example_1000.txt | demo         | 2023-01-01 23:52:02 WARN Disk usage exceeds 80%                        |
| system_log_example_1000.txt | demo         | 2023-01-01 23:50:27 WARN User login attempt failed                     |
| system_log_example_1000.txt | demo         | 2023-01-01 23:45:46 INFO User login successful                         |
| system_log_example_1000.txt | demo         | 2023-01-01 23:41:42 WARN Disk usage exceeds 80%                        |