LOGS

WHAT IS A LOG?

logs are records of events or activities.

EXAMPLES

Diary: A personal log of daily events and thoughts.

Server Logs: Records of events and interactions on a computer server.

Time Entry Logs: Record of when you logged in and out.

Security Camera Logs: Records when and how an activity happen

COMPUTER LOGS

System Logs: Record system events, errors, and warnings.

Application Logs: Capture events related to specific applications.

Security Logs: Track security-related events and authentication attempts.

Audit Logs: Document changes to a system's configuration or important data.

IMPORTANCE

Logs are crucial for troubleshooting issues, identifying security breaches, and analyzing system performance.

SPLUNK

WHAT IS SPLUNK?

Splunk is a **SIEM** (Security Information and Event Management) tool.

It’s a platform for **searching**, **monitoring**, and **analyzing** machine-generated data.

KEY FEATURES

* Real-time monitoring
* Log and event data analysis
* Customizable dashboards

COMMON USE CASES

IT Operations

Monitor system performance, troubleshoot issues.

Security

Detect and respond to security threats.

Business Analytics

Gain insights from data for informed decision-making.

SPLUNK COMPONENTS

1. Forwarders

Collect and forward data to the Splunk indexer.

2. Indexer

Stores and indexes the incoming data.

3. Search Head

Interface for searching and visualizing data.

4. Deployment Server

Manages configurations across multiple Splunk instances.

SPLUNK QUERY LANGUAGE

spl Copy code

```
index=web_logs status=500 | stats count by host
```

SPLUNK DATA ARCHITECTURE

The data is in **Key – Value** pairs

DATA INGESTION

* Data is ingested into Splunk from multiple sources

* Each source has a forwarder pointing to the Splunk instance

ACCESS TO SPLUNK

- Allow access to port 8000 in security group
- Allow All-TCP traffic from Anywhere
- http://public_ip:8000

LOGIN TO SPLUNK

Username: admin

Password: **SPLUNK-**instanceID

DEMO

Create a SPLUNK Instance on AWS

SPLUNK FREE TRAINING

https://www.splunk.com/en_us/training/free-courses/overview.html

https://www.youtube.com/playlist?list=PL7zWAA-DF0k_sxswRiB7_GUTyI0FoV7lc

SEARCH SPLUNK IN COMMUNITY AMI

splunk_AMI_9.0.5_2023-06-02_17-33-59-7b65de6c-5006-4ca2-bd75-fdba95ae5d9d

INGEST DATA

https://github.com/tjjoshua/splunk_logs/blob/main/filebeat/module/mysql/slowlog/test/mysql-debian-5.7.17.log

https://www.kaggle.com/datasets

SPLUNK SEARCHES

SEARCH USING FIELD-VALUE PAIRS

When you are looking for a specific value in a field, identify the field in your search using a field-value pair.

Example

Search port=53002

SEARCHING FOR MULTIPLE KEYWORDS

When you specify multiple terms to search for, there is an implied **AND** operator between each term.

Example:

Search root Message="Successful Login“

Search root AND Message="Successful Login"

SEARCHING WITH BOOLEAN OPERATORS

- Search admin OR Message="Successful Login“
- NOT Port=34660
- Port=34660 Message!="Successful Login«
- Port>34660
- Port>34660 Time<"21:23:43“
- Port IN (34660 40000)

USING WILDCARDS

- Search Time="21*"

CREATING TABLES


```
* Message="Failed Login"   IPAddress="1.116.*.*“

| table Message IPAddress
```

LIMITING RESULTS


```
* Message="Failed Login"   IPAddress="1.116.*.*“
| table Message IPAddress
| top limit=20 IPAddress
```

CREATING DASHBOARDS

Use the visualization tab

SPLUNK SEARCH FIELDS

Example:

```
Index=web   sourcetype=network   product=*
| fields product IP
| table product IP User
| dedup product
```

EXAMPLE

NOTE: Press shift + Enter to insert a pipe symbol on a new line

```
* source="ssh_login_attempts.csv" Message="Failed Login" IPAddress="1.*"
| table Messsage IPAddress
| top limit=10 IPAddress
```

SAVE RESULTS

After running your search:

<u>Go to:</u>

- Save AS
- Reports

SCHEDULE QUERY TO RUN

- Click **edit**
- **Edit Schedule**

DELETING DATA FROM SPLUNK

To delete data from Splunk:

1- Goto setting and modify admin permissions (Add “can-delete” role”)

2- run this command

* source=“name of the source you want to delete" | delete

EXERCISE

1 – How many successful login attempts exist from this IP 49.234.24.246

2 - How many failed login attempts exist from this IP 49.234.24.246

3 – How many events happened in 2012

4 – How many events happened in Ports greater than 59126

5 – Find all login attempts from payara