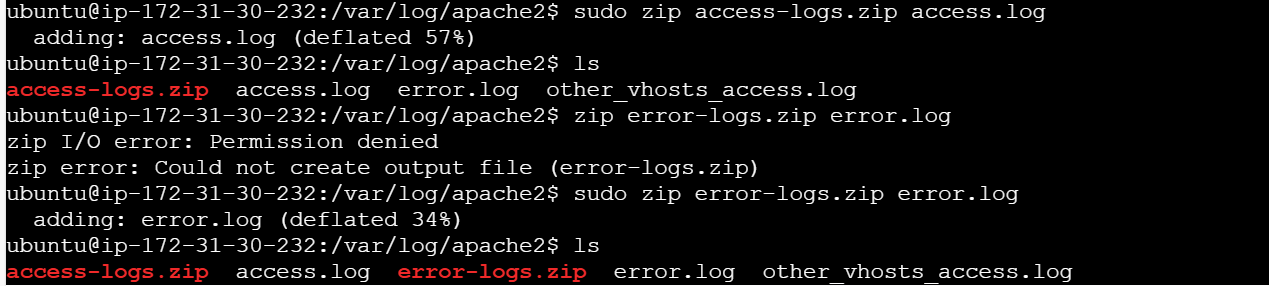
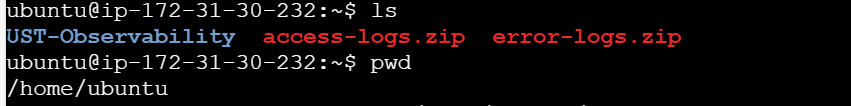
TASK:

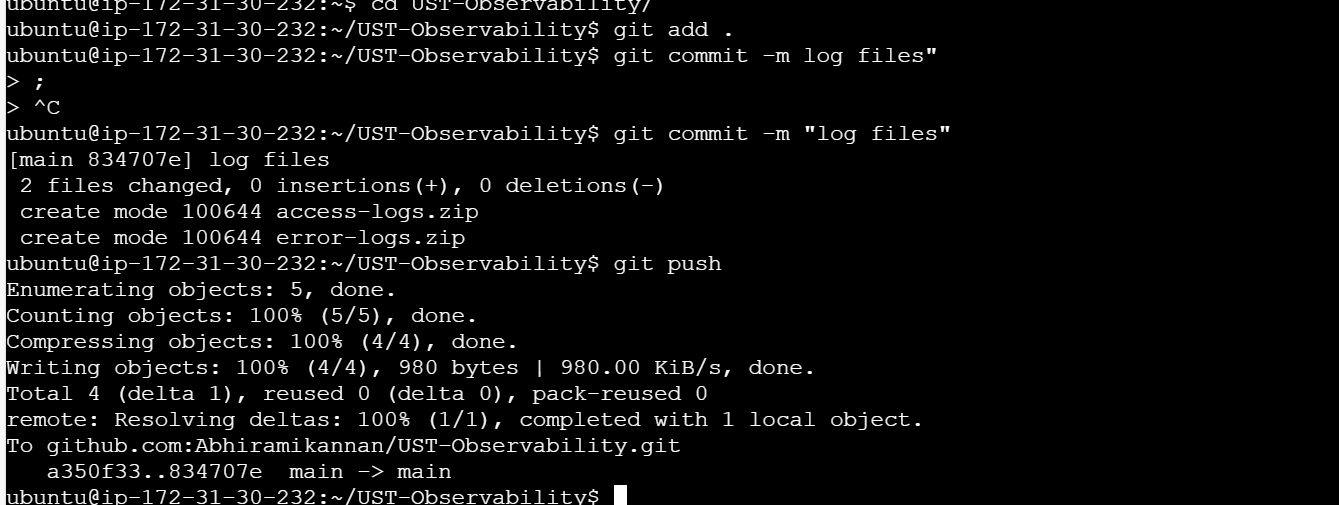
1. Download apache log files from internet
2. Create dashboard in splunk from the log file.
3. The dashboard contains 2xx,4xx,5xx panels.

SOLUTION:

1. Created a aws instance and executed the commands :
   1. Sudo apt update
   2. Sudo apt install apache2
   3. Sudo systemctl status apache2
   4. Cd /var/logs/apache2/access.logs
   5. Cd /var/logs/apache2/error.logs
   6. These 2 files can be copied to my system by pushing into github after zipping the logs.
      1. sudo zip access-logs.zip access.log
      2. sudo zip error-logs.zip error.log



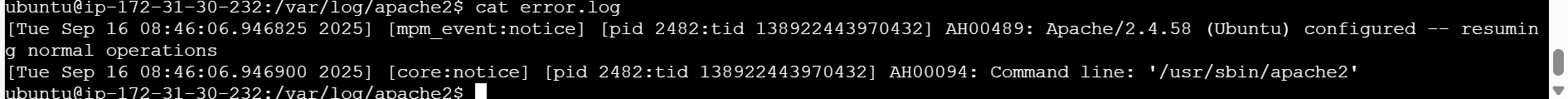




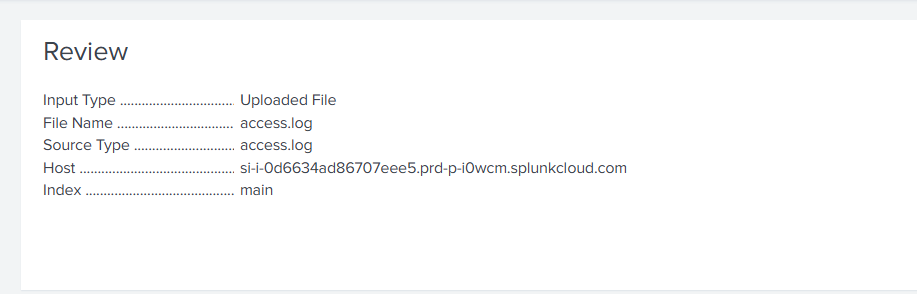
Cat access.log:



Cat error.log



1. Uploaded the access.log file into splunk



1. 2xx panel:

index=main sourcetype="access.log" | rex "^[^ ]+ [^ ]+ [^ ]+ \[.+\] \"[^\"]+\" (?<status>\d{3})" | search status>=200 status<300 | stats count

1. 4xx panel:

index=main sourcetype="access.log" | rex "^[^ ]+ [^ ]+ [^ ]+ \[.+\] \"[^\"]+\" (?<status>\d{3})" | search status>=400 status<500 | stats count

1. 5xx panel:

index=main sourcetype="access.log" | rex "^[^ ]+ [^ ]+ [^ ]+ \[.+\] \"[^\"]+\" (?<status>\d{3})" | search status>=500 status<600 | stats count

1. Heading: Edited the source code:

<row>

<panel>

<html>

<h1 style="text-align: center; color: black; background-color:#94D2EC; padding: 15px; font-size: 30px;">Apache Access Log Status Overview</h1>

</html>

</panel>

</row>

<row>

1. Heading: Details of Status codes:

<row>

<panel>

<html>

<h1 style="text-align: center; color: black; background-color:#94D2EC; padding: 15px; font-size: 30px;">DETAILS OF STATUS CODES</h1>

</html>

</panel>

</row>

1. Details of status code:

index=main sourcetype="access.log"

| rex "^(?<client\_ip>[^ ]+) [^ ]+ [^ ]+ \[(?<timestamp>[^\]]+)\] \"(?<method>[^\"]+)\" (?<status>\d{3}) (?<bytes>\d+)"

| eval status = tonumber(status)

| where status = status

| table client\_ip, timestamp, method, status, bytes

1. piechart:

index=main sourcetype="access.log"

| rex "^(?<client\_ip>[^ ]+) [^ ]+ [^ ]+ \[(?<timestamp>[^\]]+)\] \"(?<method>[^\"]+)\" (?<status>\d{3}) (?<bytes>\d+)"

| stats count by status

1. Title for piechart:

<row>

<panel>

<html>

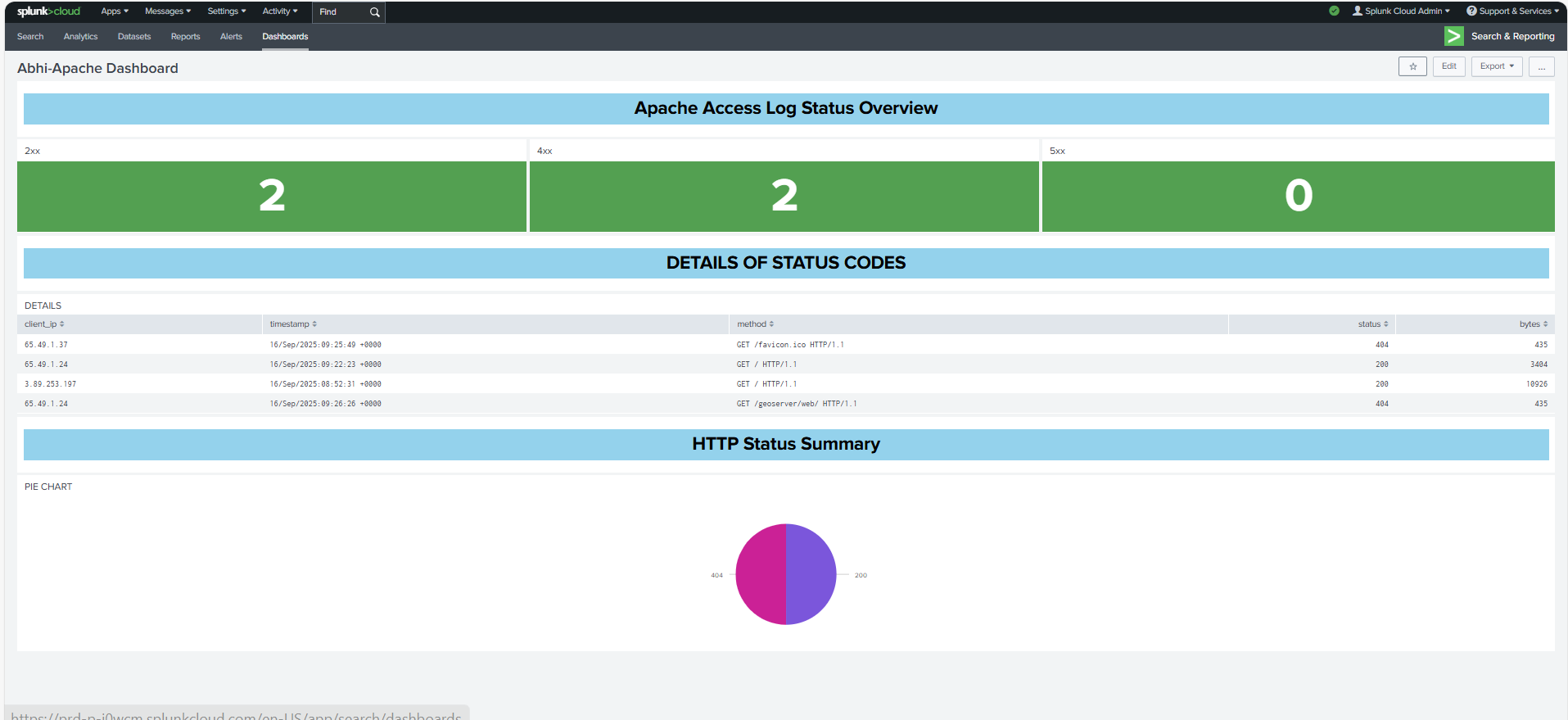
<h1 style="text-align: center; color: black; background-color:#94D2EC; padding: 15px; font-size: 30px;">HTTP Status Summary</h1>

</html>

</panel>

</row>

1. Dashboard:



1. Backup: [UST-Observability/Json\_backup\_files/3\_splunk\_apache2\_logs\_dashboard3.json at main · Abhiramikannan/UST-Observability](https://github.com/Abhiramikannan/UST-Observability/blob/main/Json_backup_files/3_splunk_apache2_logs_dashboard3.json)