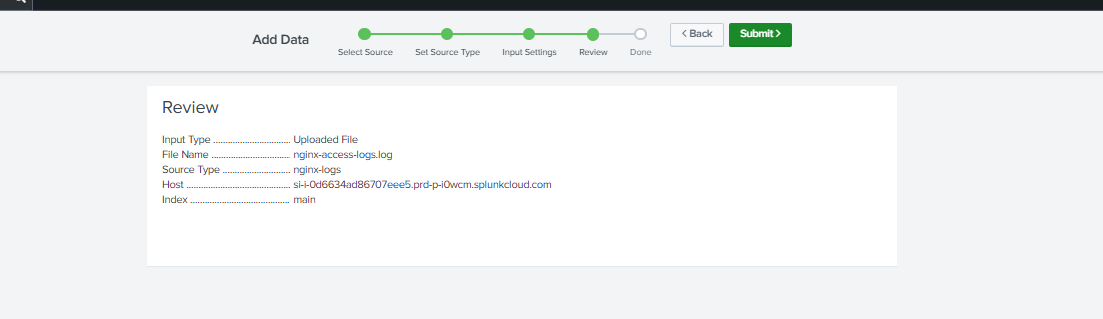
TASK: Create dashboard from nginx log file and implement the drill down feature.

SOLUTION:

1. Uploaded nginx log file  
      
   

Data:

192.168.1.10 - - [17/Sep/2025:10:15:30 +0000] "GET /home HTTP/1.1" 200 512

192.168.1.12 - - [17/Sep/2025:10:16:01 +0000] "POST /login HTTP/1.1" 401 256

192.168.1.15 - - [17/Sep/2025:10:17:12 +0000] "GET /dashboard HTTP/1.1" 500 128

192.168.1.18 - - [17/Sep/2025:10:18:30 +0000] "GET /contact HTTP/1.1" 200 1024

192.168.1.20 - - [17/Sep/2025:10:19:45 +0000] "POST /submit HTTP/1.1" 403 512

Show full details:

source="nginx-access-logs.log" host="si-i-0d6634ad86707eee5.prd-p-i0wcm.splunkcloud.com" index="main" sourcetype="nginx-logs"

| rex field=\_raw "^(?<client\_ip>\d+\.\d+\.\d+\.\d+) - - \[(?<timestamp>[^\]]+)\] \"(?<method>\w+) (?<uri>\S+) HTTP/1\.\d\" (?<status>\d{3}) (?<bytes>\d+)"

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

| head 20

-----------------------------------------------------------------------------------  
PANELS:

1. PANEL 1: Total Requests Per Hour

SPL:

source="nginx-access-logs.log" host="si-i-0d6634ad86707eee5.prd-p-i0wcm.splunkcloud.com" index="main" sourcetype="nginx-logs"

| timechart count span=1h

VISUALIZATION: timechart.

1. PANEL 2: Requests by HTTP Status Code  
   SPL:

source="nginx-access-logs.log" host="si-i-0d6634ad86707eee5.prd-p-i0wcm.splunkcloud.com" index="main" sourcetype="nginx-logs"

| rex field=\_raw "\"\s(?<status\_code>\d{3})\s"

| stats count by status\_code

| sort -count

VISUALIZATION: column chart.

1. PANEL 3: Top 10 Requested Endpoints

SPL:

source="nginx-access-logs.log" host="si-i-0d6634ad86707eee5.prd-p-i0wcm.splunkcloud.com" index="main" sourcetype="nginx-logs"

| rex field=\_raw "\"\w+\s(?<uri>/\S\*)\sHTTP"

| stats count by uri

| sort -count

| head 10

Visualization: column chart.

1. PANEL 4: Top 10 Client IPs

SPL:

source="nginx-access-logs.log" host="si-i-0d6634ad86707eee5.prd-p-i0wcm.splunkcloud.com" index="main" sourcetype="nginx-logs"

| rex field=\_raw "^(?<client\_ip>\d+\.\d+\.\d+\.\d+)"

| stats count by client\_ip

| sort -count

| head 10

VISUALIZATION: column chart

1. PANEL 5: Client & Server Errors Over Time

SPL:

source="nginx-access-logs.log" host="si-i-0d6634ad86707eee5.prd-p-i0wcm.splunkcloud.com" index="main" sourcetype="nginx-logs"

| rex field=\_raw "\"\s(?<status\_code>\d{3})\s"

| search status\_code>=400

| timechart count by status\_code span=1h

VISUALIZATION: area chart

1. PANEL 6: Requests by HTTP Method

SPL:  
source="nginx-access-logs.log" host="si-i-0d6634ad86707eee5.prd-p-i0wcm.splunkcloud.com" index="main" sourcetype="nginx-logs"

| rex field=\_raw "\"(?<method>\w+)\s"

| stats count by method

VISUALIZATION: pie chart

1. PANEL 7: detailed data of requests.

SPL:

source="nginx-access-logs.log" host="si-i-0d6634ad86707eee5.prd-p-i0wcm.splunkcloud.com" index="main" sourcetype="nginx-logs"

| rex field=\_raw "^(?<client\_ip>\d+\.\d+\.\d+\.\d+)"

| rex field=\_raw "\[(?<timestamp>[^\]]+)\]"

| rex field=\_raw "\"(?<method>GET|POST)\s(?<uri>/\S\*)\sHTTP"

| rex field=\_raw "\"\s(?<status\_code>\d{3})\s(?<bytes>\d+)"

| where method="$selected\_method$"

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

| sort - timestamp

VISUALIZATION: table

DRILLDOWN feature showing table

Configured with token: selected\_method

ADDED TITLE HEADINGS:  
  
1. Nginx Traffic And Performance Dashboard

<row>

<panel>

<html>

<h1 style="text-align: center; color: black; background-color:#94D2EC; padding: 15px; font-size: 30px;">Nginx Traffic And Performance Dashboard</h1>

</html>

</panel>

</row>  
  
2. DRILL DOWN FEATURE FOR HTTP METHODS  
  
<row>

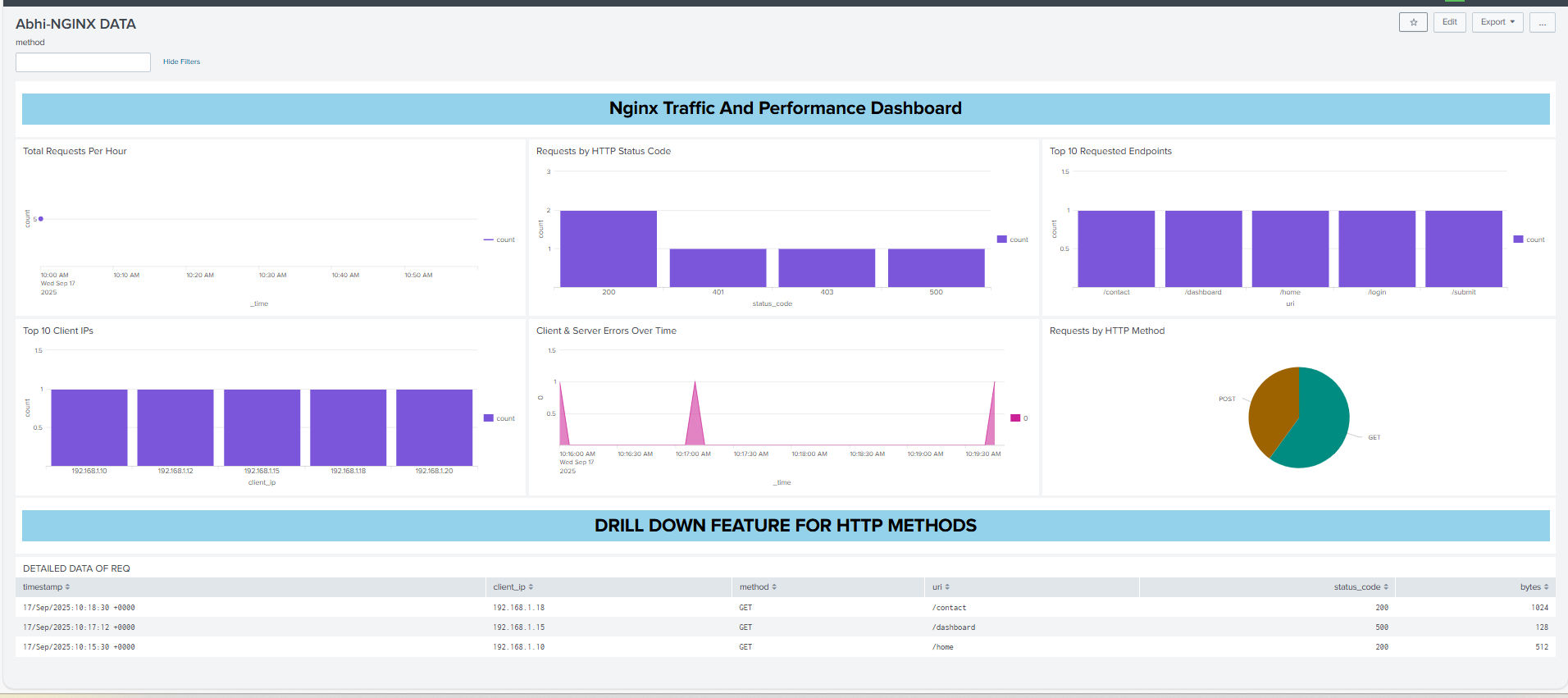
<panel>

<html>

<h1 style="text-align: center; color: black; background-color:#94D2EC; padding: 15px; font-size: 30px;">DRILL DOWN FEATURE FOR HTTP METHODS</h1>

</html>

</panel>

DASHBOARD:  


DRILLDOWN:

1. Going to edit this query for drill down:  
    Now i have hardcoded the query here:

source="nginx-access-logs.log" host="si-i-0d6634ad86707eee5.prd-p-i0wcm.splunkcloud.com" index="main" sourcetype="nginx-logs"

| rex field=\_raw "\"(?<method>POST)\s(?<uri>/\S\*)\sHTTP"

| rex field=\_raw "^(?<client\_ip>\d+\.\d+\.\d+\.\d+)"

| rex field=\_raw "\[(?<timestamp>[^\]]+)\]"

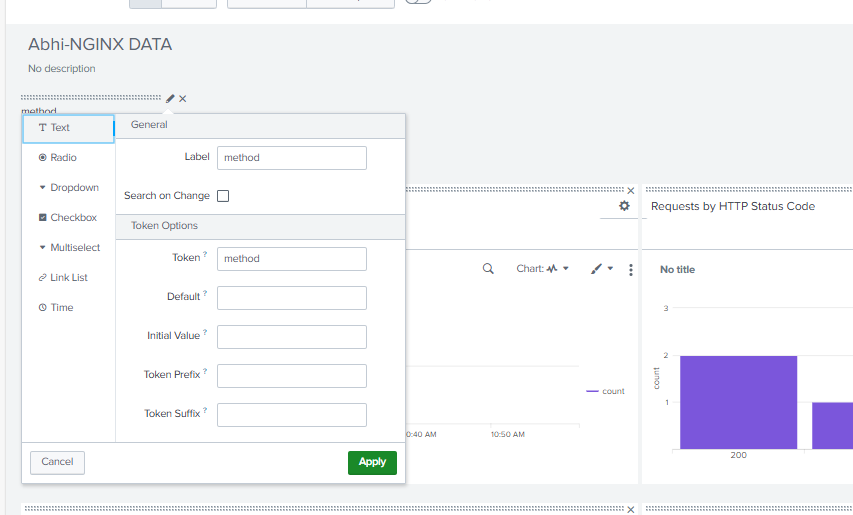
| rex field=\_raw "\"\s(?<status\_code>\d{3})\s(?<bytes>\d+)"

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

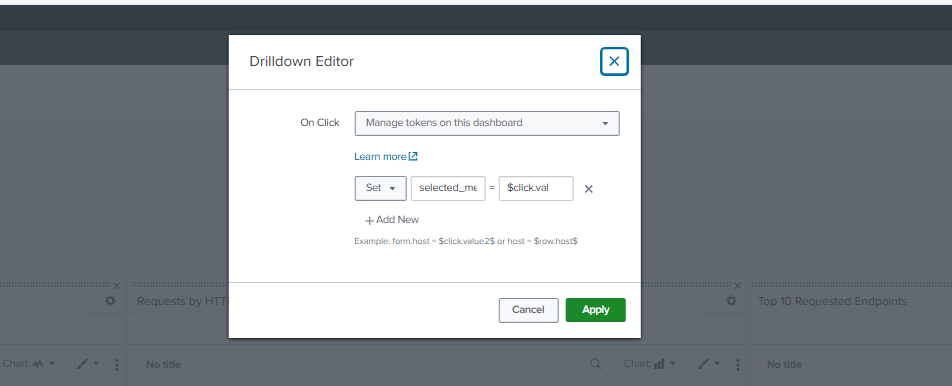
| sort - timestamp  
  
  
Saved this as a panel. Now i need to Implement the drill down feature in this panel when i click on the pie chart panel.(panel6: Requests by HTTP Method). Give input as method.

Screenshots:

Input added:



1. Token: selected\_method  
    Here in the pie chart panel i have clicked the edit drill down and added token and value.

Screenshot:  


1. After token:

source="nginx-access-logs.log" host="si-i-0d6634ad86707eee5.prd-p-i0wcm.splunkcloud.com" index="main" sourcetype="nginx-logs"

| rex field=\_raw "^(?<client\_ip>\d+\.\d+\.\d+\.\d+)"

| rex field=\_raw "\[(?<timestamp>[^\]]+)\]"

| rex field=\_raw "\"(?<method>GET|POST)\s(?<uri>/\S\*)\sHTTP"

| rex field=\_raw "\"\s(?<status\_code>\d{3})\s(?<bytes>\d+)"

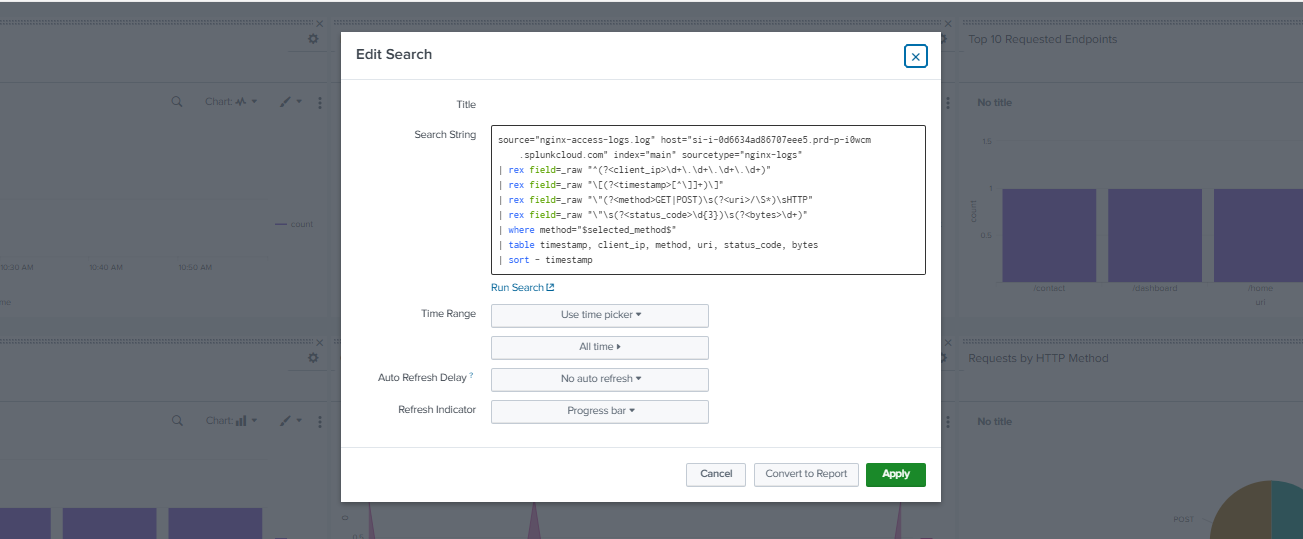
| where method="$selected\_method$"

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

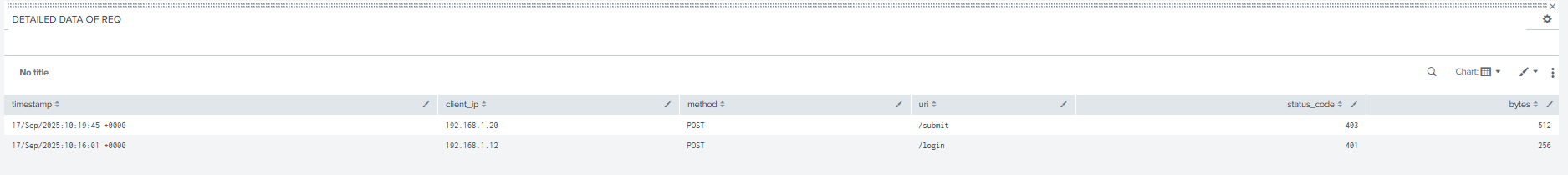
| sort - timestamp

After adding the token i should edit the spl query in the panel where i hardcoded the fields .. with the token.. Then only i can see the drill down feature in that panel .

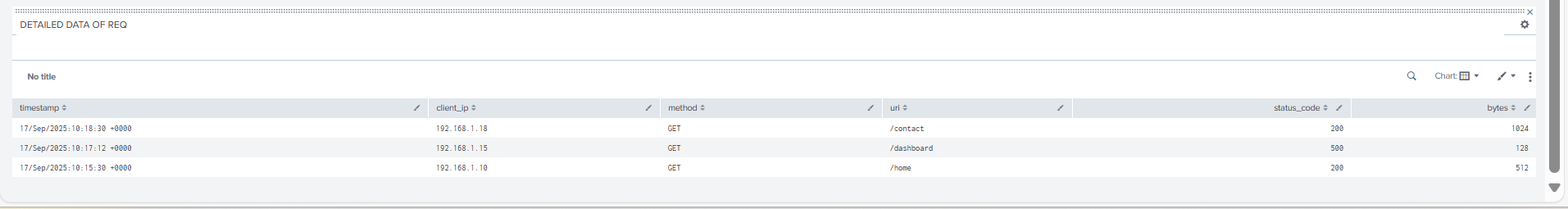
So when i am clicking the pie chart panel (GET) -> shows details of get req in the last panel where i applied drilldown  
Same with POST-> it shows detailed view of post  
  
Screenshots:



When i click on POST:



When i click on GET:

  
 Json: [UST-Observability/Json\_backup\_files/4\_Splunk\_nginx\_monitoring\_dashboard.json at main · Abhiramikannan/UST-Observability](https://github.com/Abhiramikannan/UST-Observability/blob/main/Json_backup_files/4_Splunk_nginx_monitoring_dashboard.json)