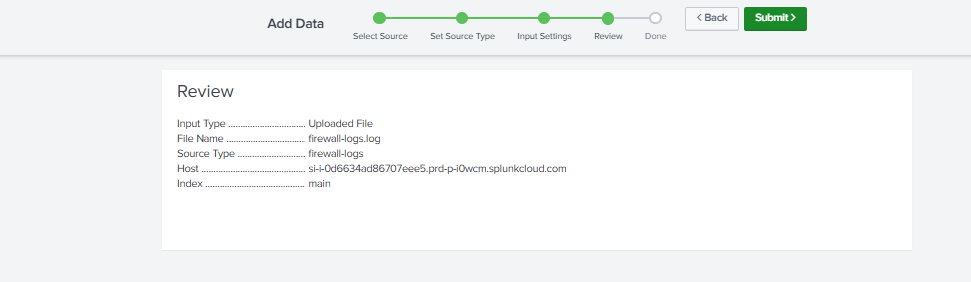
TASK: create a dashboard from log files also implement the drill down feature.

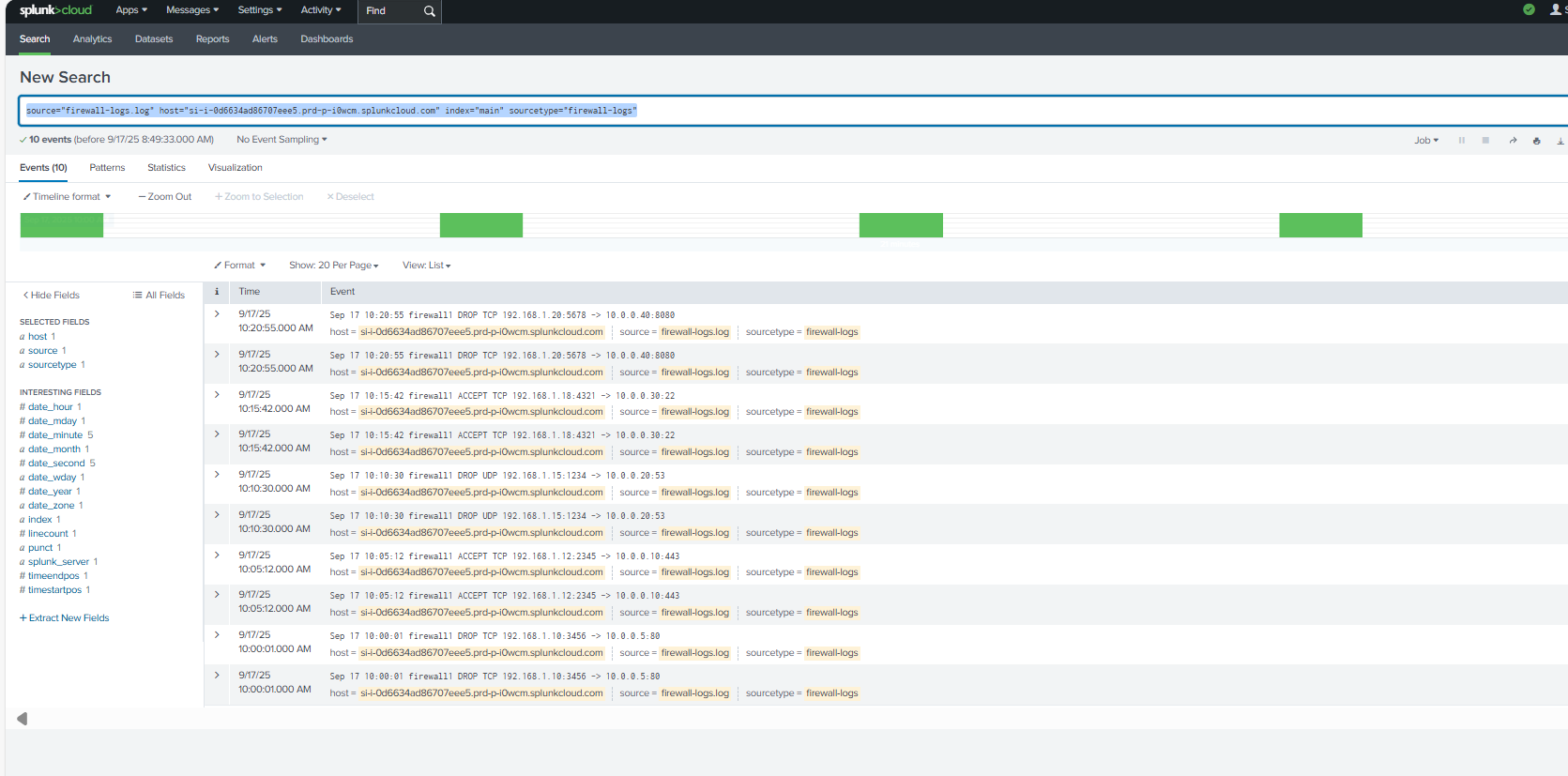
STEPS:

1. Uploaded the log file into the splunk:



1. Base search querry given by splunk:

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



1. Firewall logs:

Sep 17 10:00:01 firewall1 DROP TCP 192.168.1.10:3456 -> 10.0.0.5:80

Sep 17 10:05:12 firewall1 ACCEPT TCP 192.168.1.12:2345 -> 10.0.0.10:443

Sep 17 10:10:30 firewall1 DROP UDP 192.168.1.15:1234 -> 10.0.0.20:53

Sep 17 10:15:42 firewall1 ACCEPT TCP 192.168.1.18:4321 -> 10.0.0.30:22

Sep 17 10:20:55 firewall1 DROP TCP 192.168.1.20:5678 -> 10.0.0.40:8080

PANELS:

1. PANEL 1: Protocol-wise Action Count  
   description: This panel shows the number of firewall events broken down by protocol (TCP/UDP) and action (DROP/ACCEPT).

Spl querry:

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

| rex field=\_raw "^(?<timestamp>\w+\s+\d+\s+\d+:\d+:\d+)\s+\S+\s+(?<action>DROP|ACCEPT)\s+(?<protocol>\S+)"

| stats count by protocol, action

Visualization: bar chart

1. PANEL 2: Most Targeted Destination Ports  
   description: This panel provides a **destination port analysis**, helping you understand which services or ports your firewall sees most traffic for, and highlights potential attack or usage patterns.

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

| rex field=\_raw "->\s+(?:\d+\.\d+\.\d+\.\d+):(?<dest\_port>\d+)"

| stats count by dest\_port

| sort - count

| head 10

Visualization: column chart

1. PANEL 3: Detailed Firewall Logs

description: This panel is a **detailed firewall logs table** showing all individual traffic events.

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

| rex field=\_raw "^(?<timestamp>\w+\s+\d+\s+\d+:\d+:\d+)\s+(?<host>\S+)\s+(?<action>DROP|ACCEPT)\s+(?<protocol>\S+)\s+(?<src\_ip>\d+\.\d+\.\d+\.\d+):(?<src\_port>\d+)\s+->\s+(?<dest\_ip>\d+\.\d+\.\d+\.\d+):(?<dest\_port>\d+)"

| table timestamp, host, action, protocol, src\_ip, src\_port, dest\_ip, dest\_port

| sort – timestamp

Visualization: table

1. PANEL 4: Firewall Actions Count

description: This panel is a **summary of firewall actions**, showing the total number of **DROP** and **ACCEPT** events.

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

| rex field=\_raw "^(?<timestamp>\w+\s+\d+\s+\d+:\d+:\d+)\s+(?<host>\S+)\s+(?<action>DROP|ACCEPT)"

| stats count by action

Visualization: column chart

1. PANEL 5: DETAILED VIEW OF FIREWALL ACTIONS

description: drill down feature implemented and this panel shows the detailed view of drop and accept actions

SPL querry:

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

| rex field=\_raw "^(?<timestamp>\w+\s+\d+\s+\d+:\d+:\d+)\s+(?<host>\S+)\s+(?<action>DROP|ACCEPT)\s+(?<protocol>\S+)\s+(?<src\_ip>\d+\.\d+\.\d+\.\d+):(?<src\_port>\d+)\s+->\s+(?<dest\_ip>\d+\.\d+\.\d+\.\d+):(?<dest\_port>\d+)"

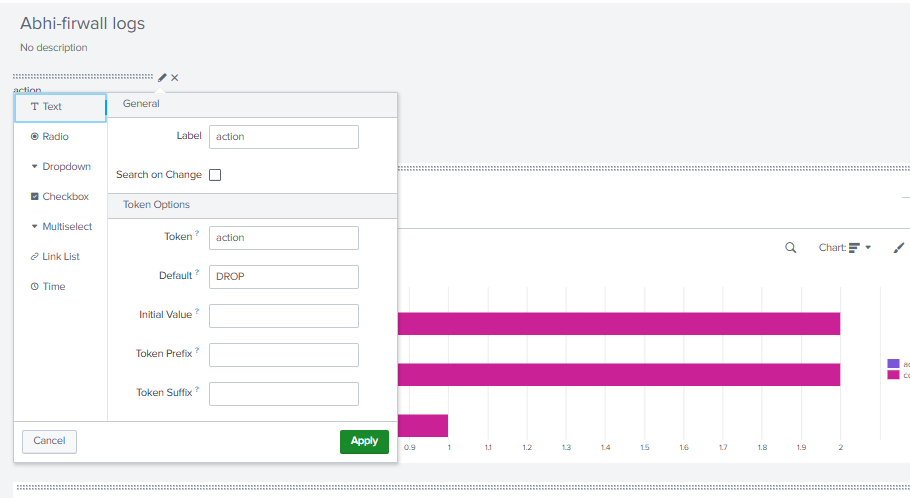
| where action="$selected\_action$"

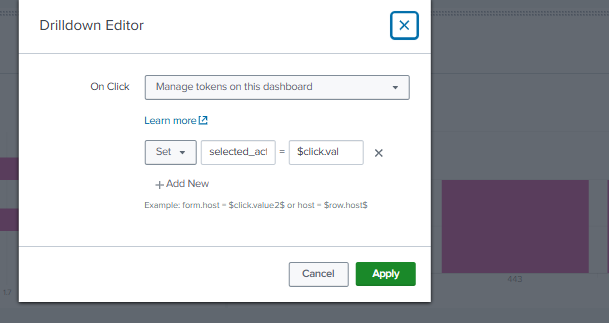
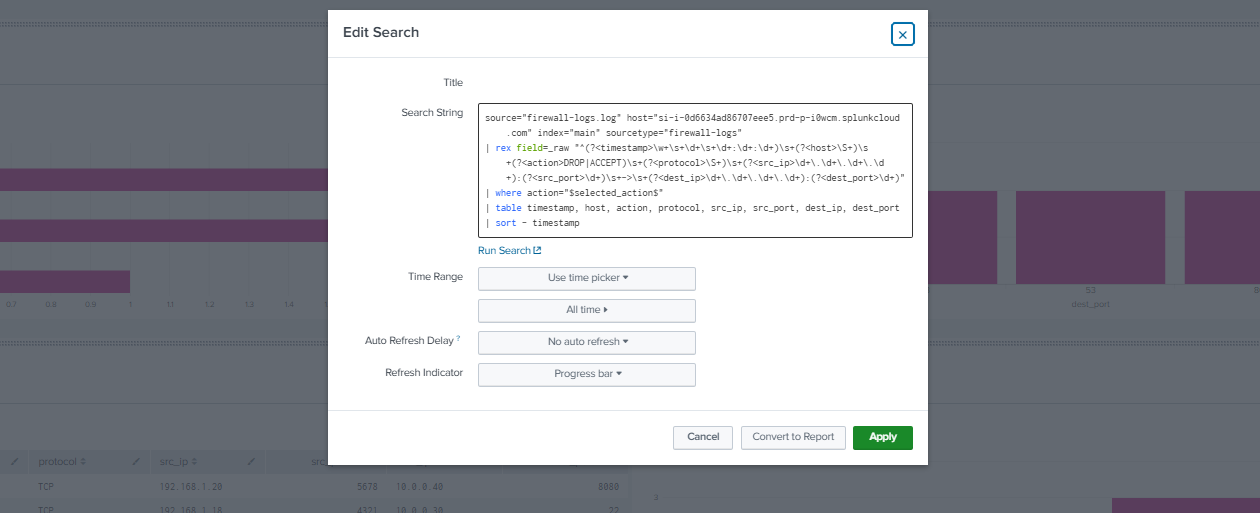
| table timestamp, host, action, protocol, src\_ip, src\_port, dest\_ip, dest\_port

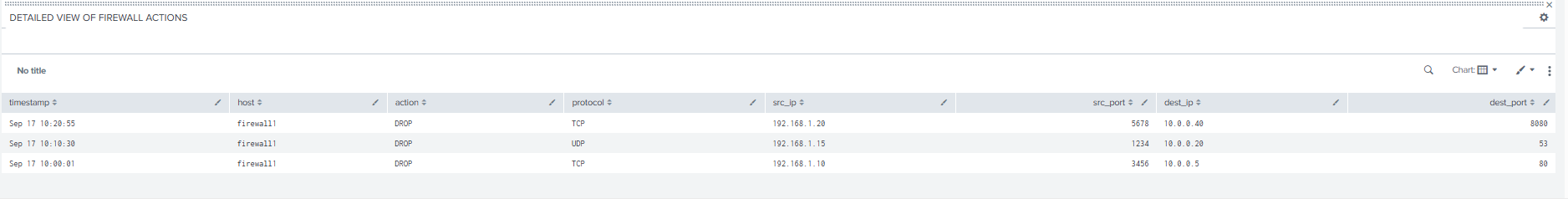
| sort - timestamp

Visualization: table  
  
DRILLDOWN:

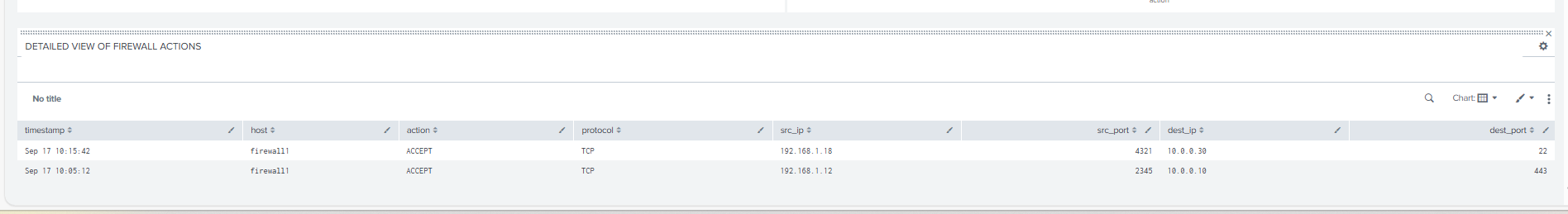
1. Created a markdown text .Set Default as Drop (whenever you open the dashboard you can see the drop actions details in the panel)



1. Created token in the 4th panel:  
   token: selected\_action  
   
2. Hardcoded the panel spl querry and saved it as panel Once …and edited that querry with token.(panel 5)  
   
3. When I click on DROP in panel 3 .. I will get the detailed results in panel 4



1. When I click ACCEPT on panel 3.. I will get detailed results in panel 4.



ADDING TITLES BY EDITING HTML FILE

1. Network Security Firewall Dashboard:

<row>

<panel>

<html>

<h1 style="text-align: center; color: black; background-color:#94D2EC; padding: 15px; font-size: 30px;">Network Security Firewall Dashboard</h1>

</html>

</panel>

</row>

1. DRILL DOWN FEATURE OF FIREWALL ACTIONS:

<row>

<panel>

<html>

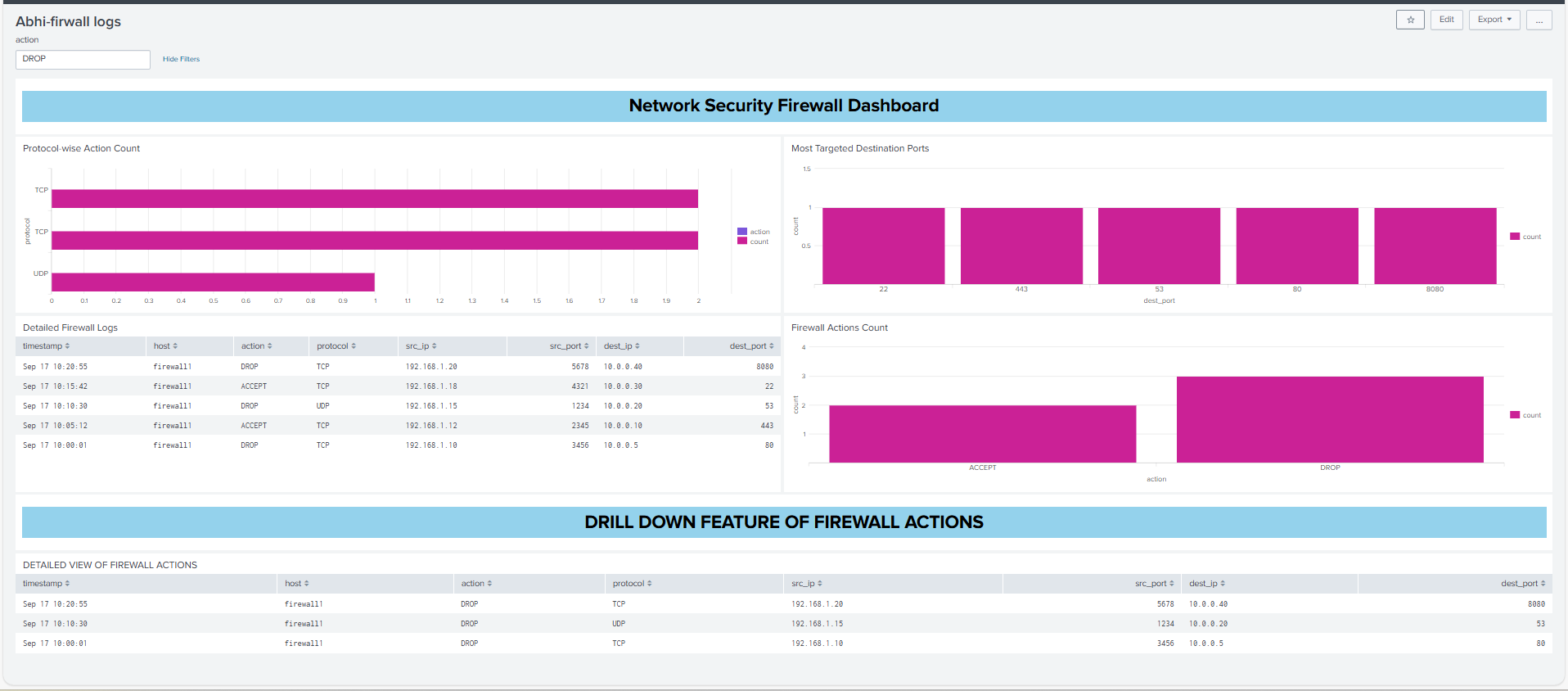
<h1 style="text-align: center; color: black; background-color:#94D2EC; padding: 15px; font-size: 30px;">DRILL DOWN FEATURE OF FIREWALL ACTIONS</h1>

</html>

</panel>

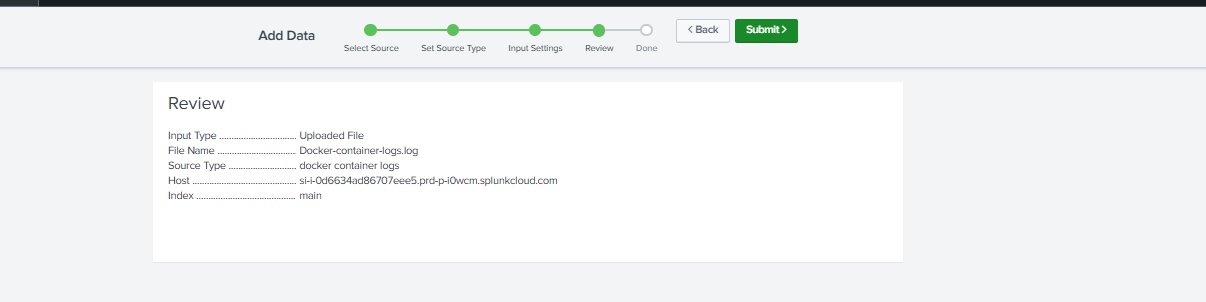
</row>

DASHBOARD:



TASK: add up docker container logs data and create panels.

1. Uploaded the data:



1. Docker-container-logs.log:

2025-09-17T10:00:01.123Z container1 INFO Container started successfully

2025-09-17T10:05:45.456Z container1 WARN Memory usage high: 85%

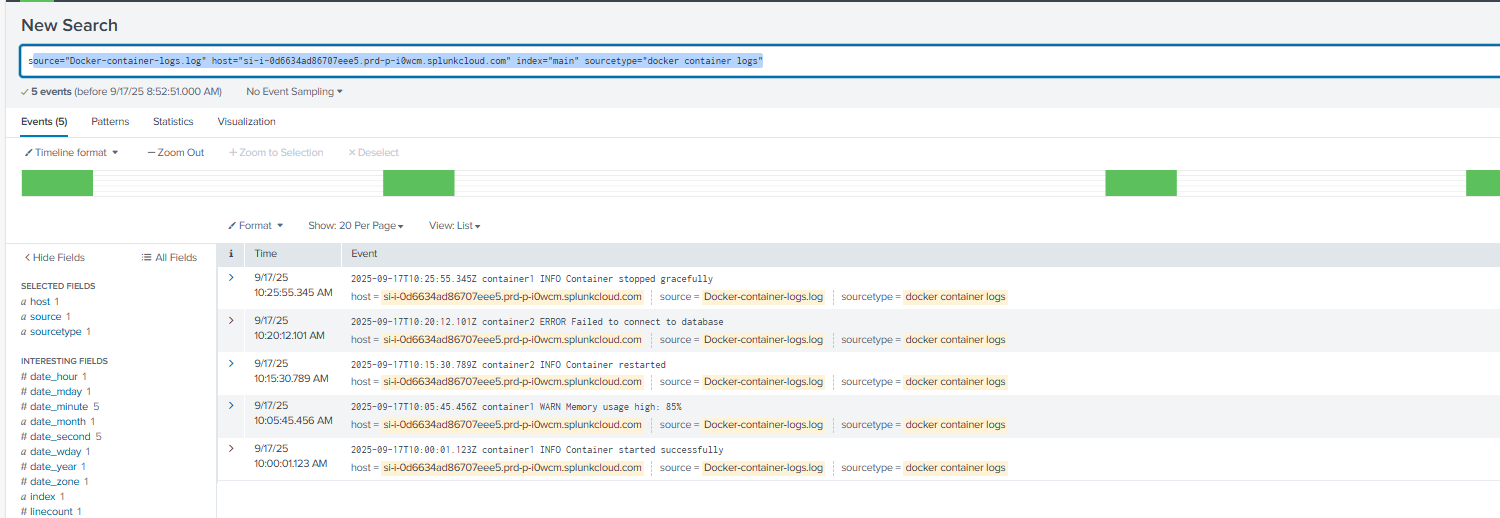
2025-09-17T10:15:30.789Z container2 INFO Container restarted

2025-09-17T10:20:12.101Z container2 ERROR Failed to connect to database

2025-09-17T10:25:55.345Z container1 INFO Container stopped gracefully

1. Base search querry:

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



PANELS:

1. Panel 6: logs by level

SPL:

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

| rex field=\_raw "^(?<timestamp>\S+)\s+(?<container>\S+)\s+(?<level>INFO|WARN|ERROR)\s+(?<message>.+)"

| stats count by container, level

Visulaization: table

1. Panel 7: Logs Over Time

Spl:

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

| rex field=\_raw "^(?<timestamp>\S+)\s+(?<container>\S+)\s+(?<level>INFO|WARN|ERROR)"

| timechart count by level span=1h

Visualization: line chart

1. Panel 8 : Containers with Most ERROR Logs

Spl:

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

| rex field=\_raw "^(?<timestamp>\S+)\s+(?<container>\S+)\s+(?<level>INFO|WARN|ERROR)"

| where level="ERROR"

| stats count by container

| sort – count

Visualization: column chart

1. PANEL 9: Detailed view of the Container

SPL:

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

| rex field=\_raw "^(?<timestamp>\S+)\s+(?<container>\S+)\s+(?<level>INFO|WARN|ERROR)\s+(?<message>.+)"

| where level="ERROR" AND container="$selected\_container$"

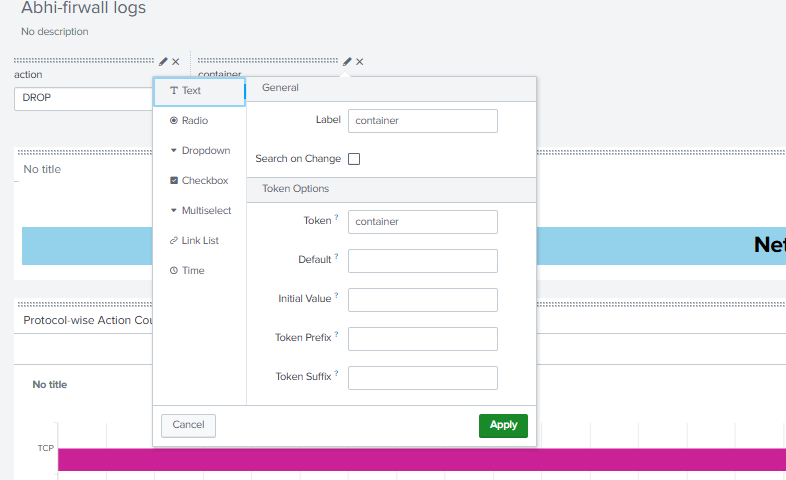
| table timestamp, container, level, message

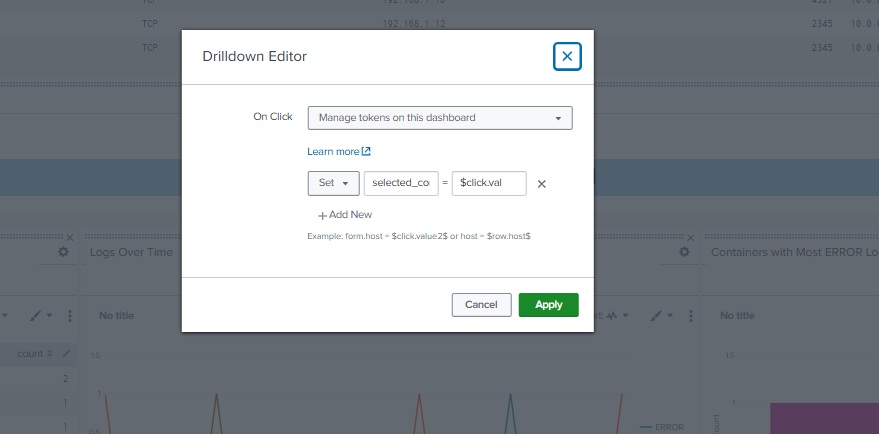
| sort – timestamp

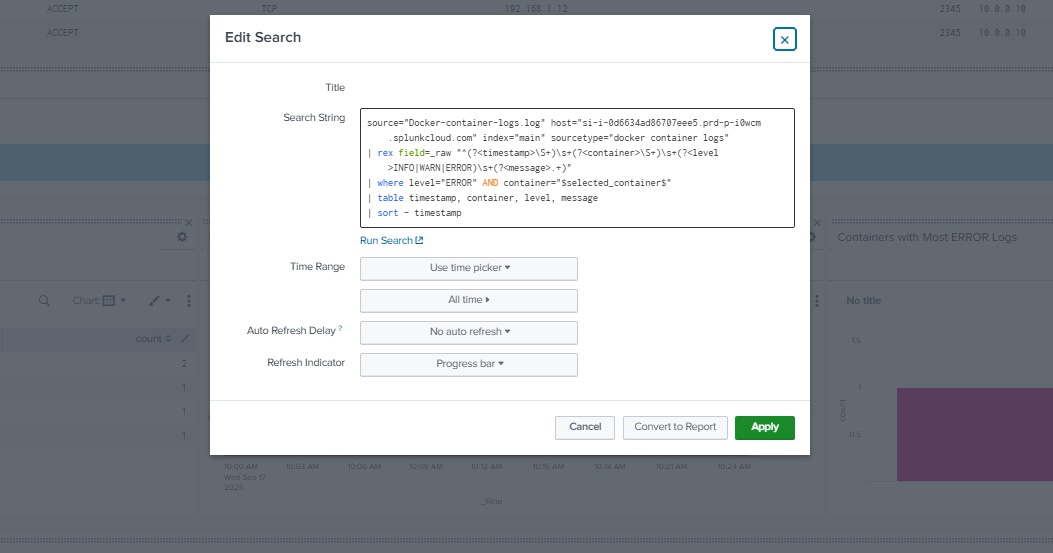
Visualization: table

DRILL DOWN:

1. Created the markdown text input



1. Edited the panel 8 to add drill down token.  
   
2. Edited panel 9 hardcoded querry with token passing.



TITLES ADDED:

1. Docker Container Monitoring Dashboard

<row>

<panel>

<html>

<h1 style="text-align: center; color: black; background-color:#94D2EC; padding: 15px; font-size: 30px;">Docker Container Monitoring Dashboard</h1>

</html>

</panel>

</row>

1. Drill down:

<row>

<panel>

<html>

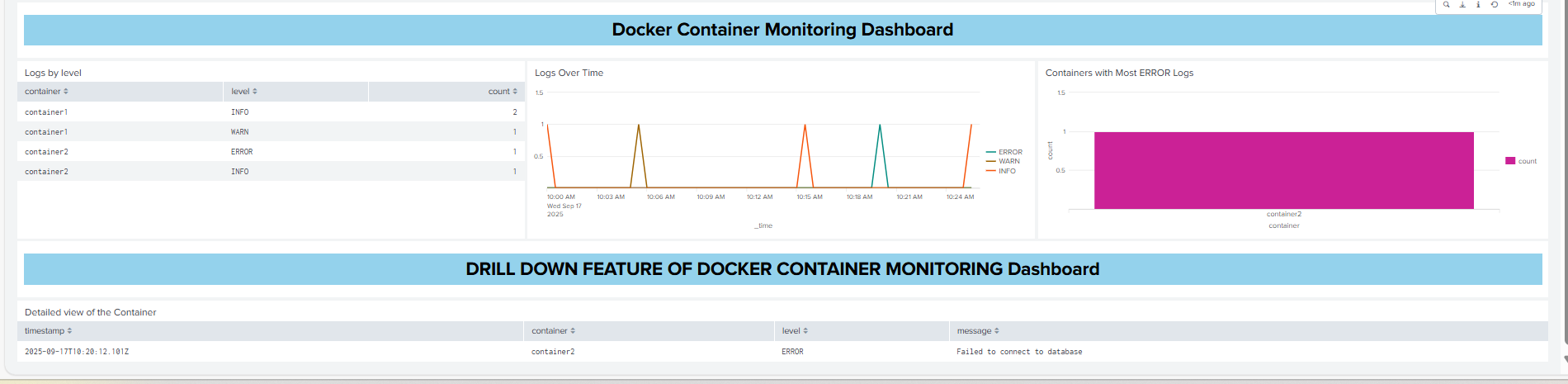
<h1 style="text-align: center; color: black; background-color:#94D2EC; padding: 15px; font-size: 30px;">DRILL DOWN FEATURE OF DOCKER CONTAINER MONITORING Dashboard</h1>

</html>

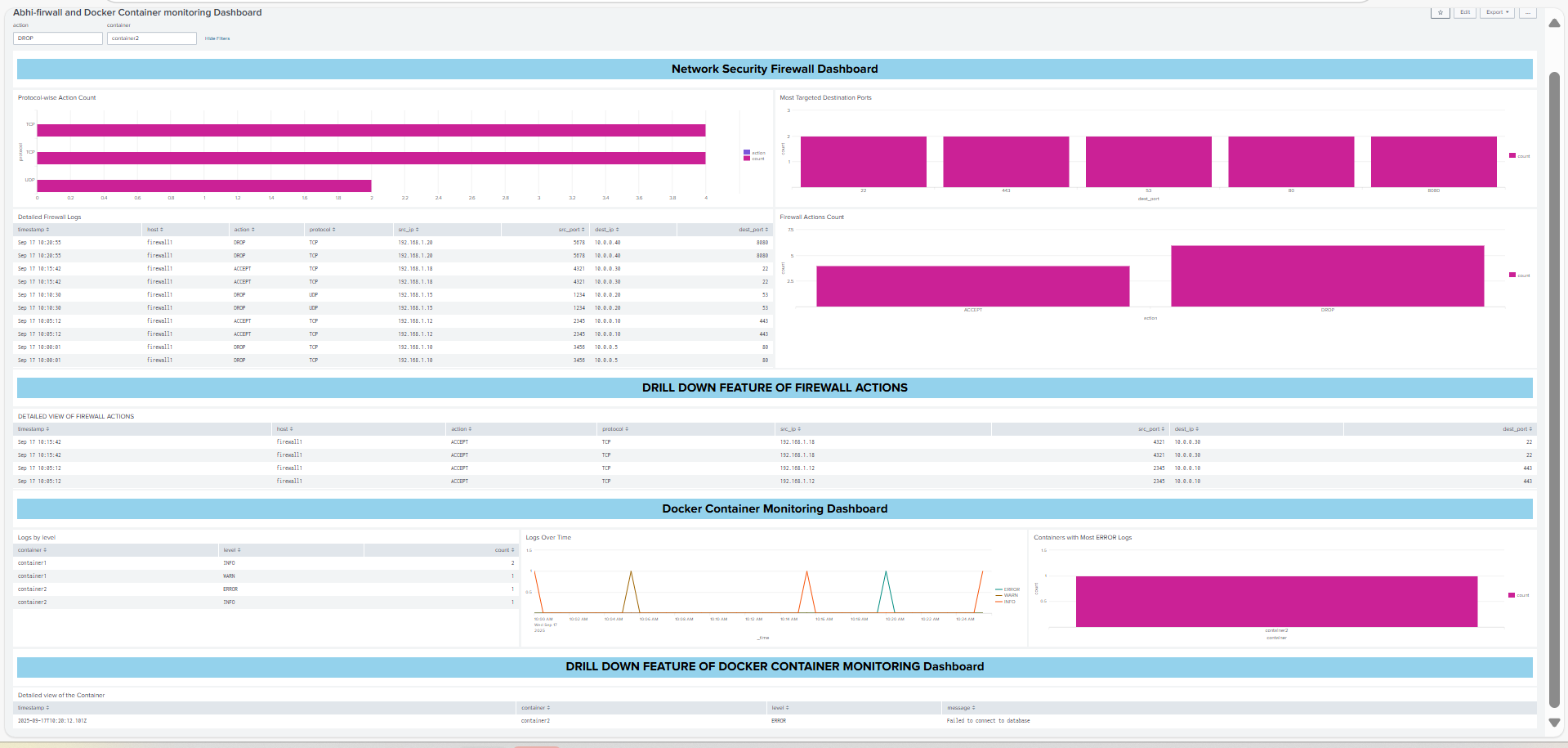
</panel>

</row>

DASHBOARD:



WHOLE DASHBOARD:



Json:

[UST-Observability/Json\_backup\_files/5\_Splunk\_firewall\_and\_docker\_monitoring\_dashboard.json at main · Abhiramikannan/UST-Observability](https://github.com/Abhiramikannan/UST-Observability/blob/main/Json_backup_files/5_Splunk_firewall_and_docker_monitoring_dashboard.json)