Nov 2024

Splunk4Rookies - AWS

Lab Guide

Overview

This lab guide contains the hands-on exercises for the Splunk4Rookies - AWS workshop. Before proceeding with these exercises, please ensure that you have a copy of the workshop slide deck, which will help to put into context the tasks you are carrying out.

Download the workshop slide deck: https://splk.it/S4R-AWS-Attendee

Prerequisites

In order to complete these exercises, you will need your own Splunk instance. Splunk's hands-on workshops are delivered via the Splunk Show portal and you will need a splunk.com account in order to access this.

If you don't already have a Splunk.com account, please create one here before proceeding with the rest of the workshop.

⚠️ Troubleshooting Connectivity

If you experience connectivity issues with accessing either your workshop environment or the event page, please try the following troubleshooting steps. If you still experience issues please reach out to the team running your workshop.

- **Use Google Chrome** (if you're not already)
- If the event page (i.e. *https://show.splunk.com/event/<eventID>*) didn't load when you clicked on the link, try **refreshing the page**
- **Disconnect from VPN** (if you're using one)
- **Clear your browser cache and restart your browser** (if using Google Chrome, go to: Settings > Privacy and security > Clear browsing data)
- **Try using private browsing mode** (e.g. Incognito in Google Chrome) to rule out any cache issues
- **Try using another computer** such as your personal computer - all you need is a web browser! Cloud platforms like AWS can often be blocked on corporate laptops.

Table of Contents

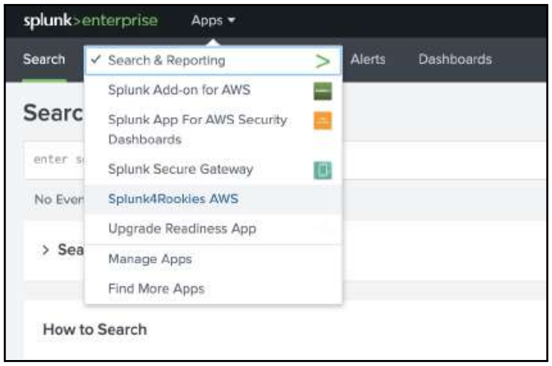
Exercise 1 – Explore AWS data in Splunk

Description

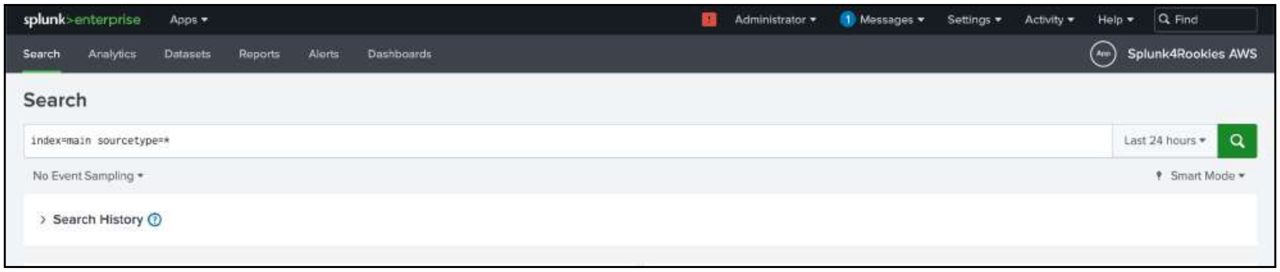
In this exercise you will begin to explore the data from AWS that is being ingested into Splunk and identify the common sourcetypes from the AWS data.

Steps

1. From the Splunk home page, click the **Apps** dropdown located in the top left corner and select "**Splunk4Rookies AWS**".

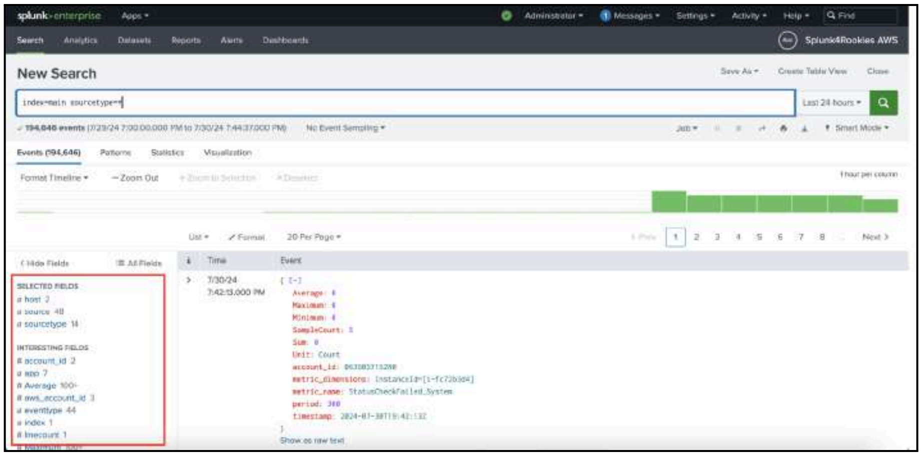


2. From the Splunk Search page begin to explore some of the different AWS data sources that have been ingested into Splunk. In the search bar, type `index="main" sourcetype=*` and set the time picker for **Last 24 Hours**. Run the search by pressing enter or clicking the search button.



```
index=main sourcetype=*
```

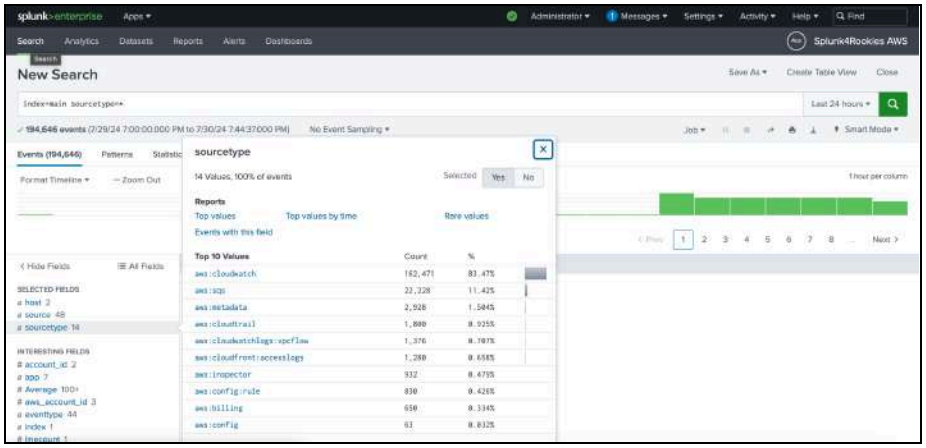
3. Explore the **Selected Fields** & **Interesting Fields** located on the left side of the screen.



```
index=main sourcetype=*
```

```
{ [-]
   Average: 0
   Maximum: 0
   Minimum: 0
   SampleCount: 1
   Sum: 0
   Unit: Count
   account_id: 063083713280
   metric_dimensions: InstanceId=[i-fc72b3d4]
   metric_name: StatusCheckFailed_System
   period: 300
   timestamp: 2024-07-30T19:42:13Z
}
```

4. Click on **sourcetype** and review the different AWS services that are sending data into Splunk.



```
index=main sourcetype=*
```

194,646 events (7/29/24 7:00:00.000 PM to 7/30/24 7:44:37.000 PM)

sourcetype

14 Values, 100% of events

Top 10 Values	Count	%
aws:cloudwatch	162,471	83.47%
aws:sqs	22,228	11.42%
aws:metadata	2,928	1.504%
aws:cloudtrail	1,800	0.925%
aws:cloudwatchlogs:vpcflow	1,376	0.707%
aws:cloudfront:accesslogs	1,280	0.658%
aws:inspector	932	0.479%
aws:config:rule	830	0.426%
aws:billing	650	0.334%
aws:config	63	0.032%

5. Click on **aws:sqs** to add it to the search bar. Notice the search automatically runs. Explore the events for the **aws:sqs** sourcetype. After exploring return to the original search `index="main" sourcetype=*`

6. Explore other interesting AWS sourcetypes in Splunk and look at the individual events for those sourcetypes.

Exercise 2 – Identify global traffic using AWS VPC Flow Logs

Description

In this exercise you will be exploring the AWS VPC Flow Logs to investigate location access and identify potential security risks.

Steps

1. From the Splunk search bar search for events from the Cloudwatch VPC Flow Logs sourcetype and click search

   Example SPL query:

   ```
   index=main sourcetype="aws:cloudwatchlogs:vpcflow"
   ```

2. Now that you have explored the data from the VPC Flow Logs it's time to add additional fields to add to the context. From the Splunk search bar add the `iplocation` command to extract information based on the `srp_ip` field.

   Example SPL query:

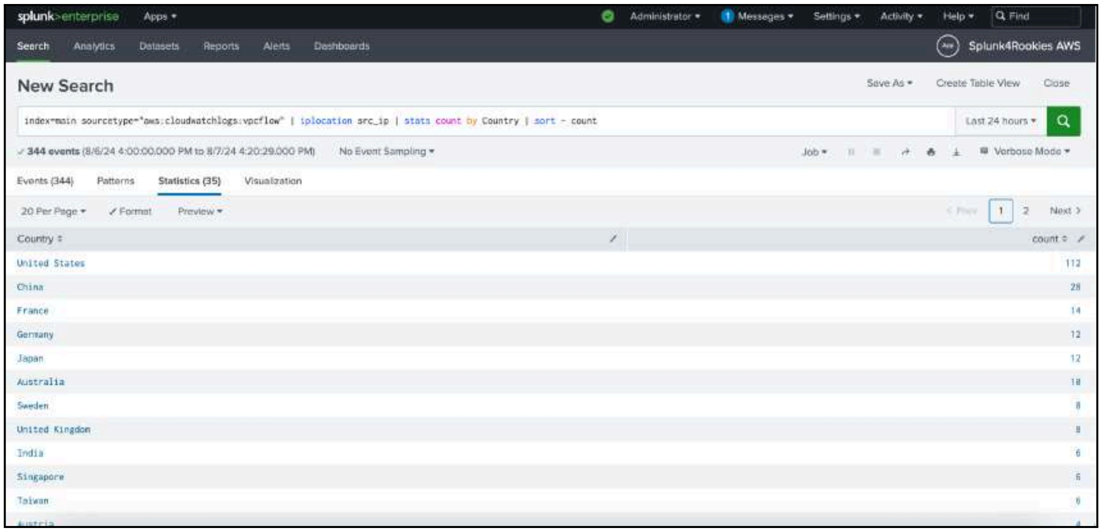
```
index=main sourcetype="aws:cloudwatchlogs:vpcflow"
| iplocation src_ip
```

Note: ***iplocation*** is a Splunk command that extracts location information from IP addresses by using 3rd-party databases.

3. Notice the additional fields of Country, City, lat, & lon now appear in the Interesting Fields. Using the newly added Country field, count the number of events and then sort the count of events.

   Example SPL query:

```
index=main sourcetype="aws:cloudwatchlogs:vpcflow"
| iplocation src_ip
| stats count by Country
| sort - count
```



```
index=main sourcetype="aws:cloudwatchlogs:vpcflow" | iplocation src_ip | stats count by Country | sort - count
```

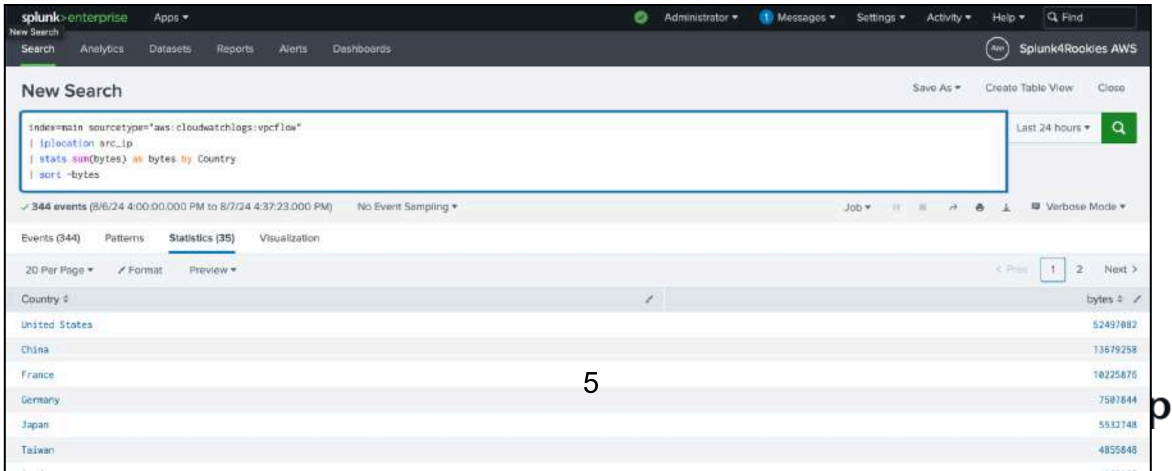
✓ 344 events (8/6/24 4:00:00.000 PM to 8/7/24 4:20:29.000 PM)

Country	count
United States	112
China	28
France	14
Germany	12
Japan	12
Australia	10
Sweden	8
United Kingdom	8
India	6
Singapore	6
Taiwan	6
Austria	4

4. Next we are going to include the sum of traffic flow by country represented in bytes using the stats command and display that in order of most traffic to least amount of traffic.

   Example SPL query:

```
index=main sourcetype="aws:cloudwatchlogs:vpcflow"
| iplocation src_ip
| stats sum(bytes) as bytes by Country
| sort -bytes
```



```
index=main sourcetype="aws:cloudwatchlogs:vpcflow"
| iplocation src_ip
| stats sum(bytes) as bytes by Country
| sort -bytes
```

✓ 344 events (8/6/24 4:00:00.000 PM to 8/7/24 4:37:23.000 PM)

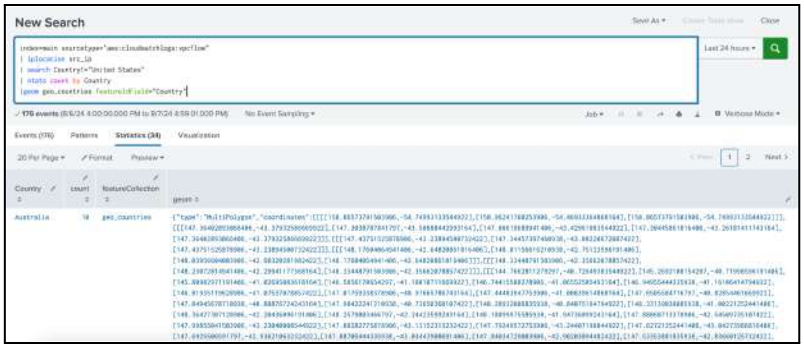
Country	bytes
United States	52497082
China	13679258
France	10225876
Germany	7507844
Japan	5532748
Taiwan	4855848

5. Looking at the data, notice that the United States has the highest amount of traffic. Let's remove the United States from the search and use the `geom` command to create a heatmap.

   Example SPL:

```
index=main sourcetype="aws:cloudwatchlogs:vpcflow"
| iplocation src_ip
| search Country!="United States"
| stats count by Country
| geom geo_countries featureIdField="Country"
```

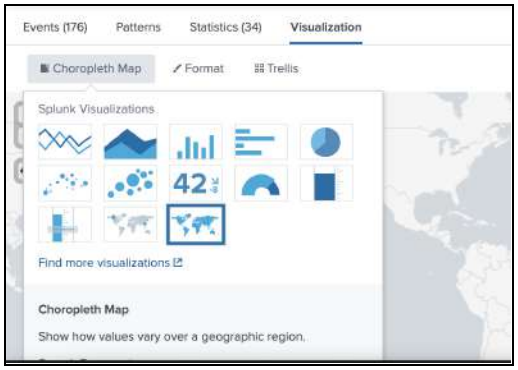
   Notice the United States is no longer listed. Let's turn this data into a heat map by clicking on the visualization tab and selecting **Choropleth Map.**



```
index=main sourcetype="aws:cloudwatchlogs:vpcflow"
| iplocation src_ip
| search Country!="United States"
| stats count by Country
|geom geo_countries featureIdField="Country"
```

✓ 176 events (8/6/24 4:00:00.000 PM to 8/7/24 4:59:01.000 PM)   No Event Sampling ▾

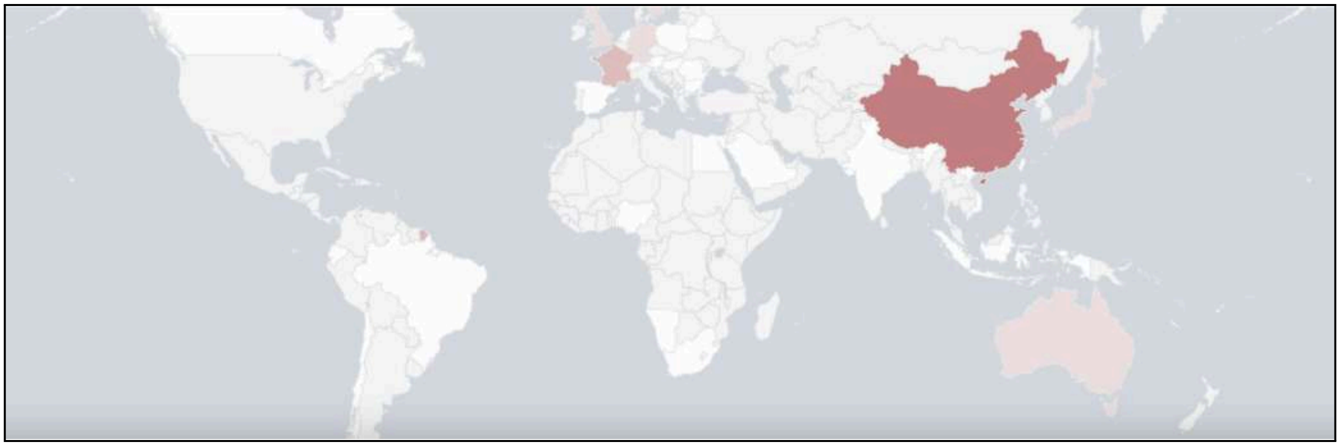
Country	count	featureCollection	geom
Australia	10	geo_countries	{"type":"MultiPolygon","coordinates":[illegible]



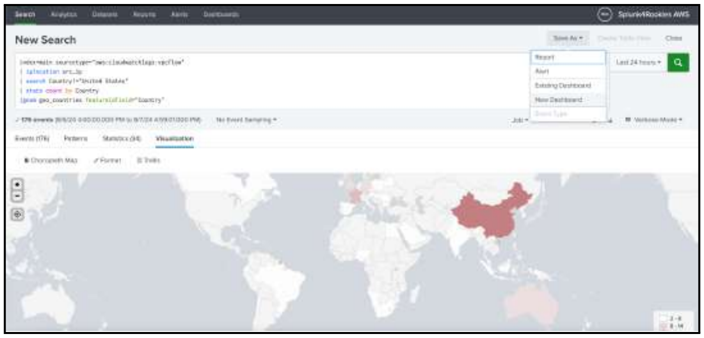
Choropleth Map

Show how values vary over a geographic region.

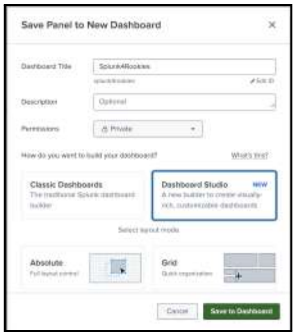
Your heatmap should looks similar to this:



6. Add your visualization to a new dashboard by clicking “Save As” and select **New Dashboard.** Name your Dashboard “Splunk4Rookies” and select the **Dashboard Studio** & **Absolute** options. Click **Save to Dashboard.**



```
index=main sourcetype="aws:cloudwatchlogs:vpcflow"
| iplocation src_ip
| search Country!="United States"
| stats count by Country
|geom geo_countries featureIdField="Country"
```



Dashboard Title: Splunk4Rookies

Description: Optional

Permissions: Private

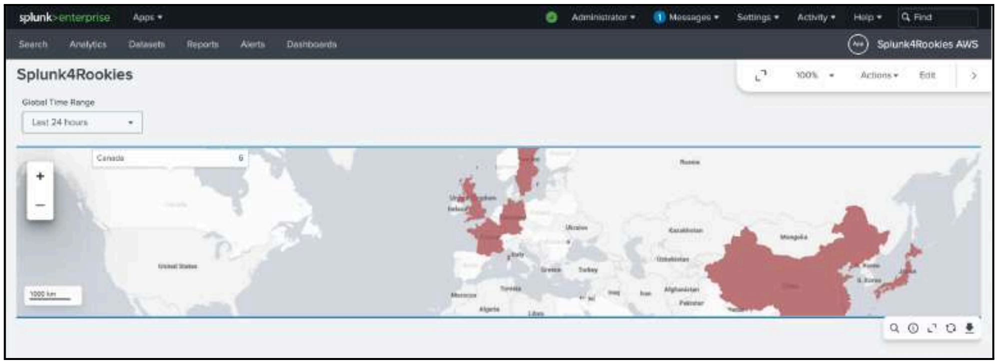
How do you want to build your dashboard?

Classic Dashboards — The traditional Splunk dashboard builder

Dashboard Studio NEW — A new builder to create visually-rich, customizable dashboards

Absolute — Full layout control

Grid — Quick organization



Exercise 3 – Monitor CPU Performance using AWS CloudWatch Logs

Description

In this exercise you will monitor CPU performance across all the EC2 instances using AWS Cloudwatch logs.

Steps

1. From the Splunk search bar search for events from the Cloudwatch sourcetype and click search.

   Example SPL query:

   ```
   index=main sourcetype="aws:cloudwatch"
   ```

2. To look at CPU performance, start by narrowing your search to include events where the `eventtype` equals `aws_cloudwatch_ec2_perf_cpu`

   Sample SPL query:

   ```
   index=main sourcetype="aws:cloudwatch" eventtype=aws_cloudwatch_ec2_perf_cpu
   ```

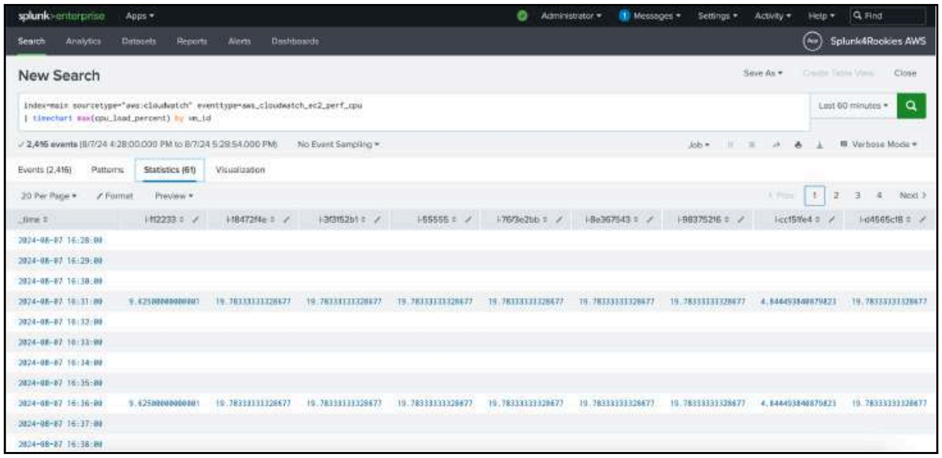
   Now Splunk is only showing events that include EC2 CPU performance.

3. To monitor CPU performance over time, use the `Timechart` Splunk command to track the `max` CPU performance by each `vm_id.` Set the time picker to 60 minutes.

   Sample SPL query:

   ```
   index=main sourcetype="aws:cloudwatch" eventtype=aws_cloudwatch_ec2_perf_cpu
   | timechart max(cpu_load_percent) by vm_id
   ```

Note: A timechart is a statistical aggregation applied to a field to produce a chart, with time used as the X-axis. You can specify a split-by field, where each distinct value of the split-by field becomes a series in the chart.



New Search

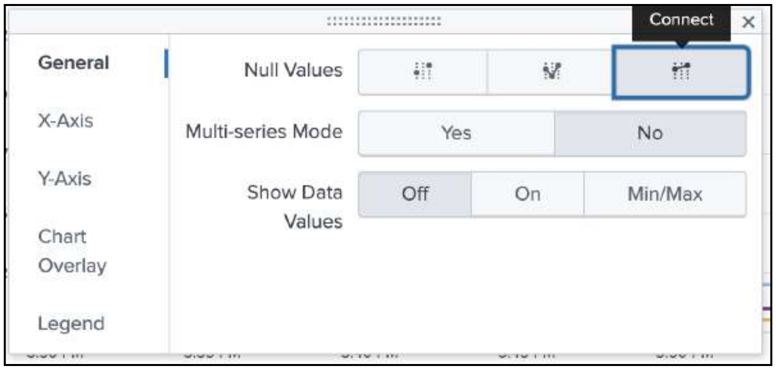
```
index=main sourcetype="aws:cloudwatch" eventtype=aws_cloudwatch_ec2_perf_cpu
| timechart max(cpu_load_percent) by vm_id
```

Last 60 minutes ▾

✓ 2,416 events (8/7/24 4:28:00.000 PM to 8/7/24 5:28:54.000 PM) No Event Sampling ▾

_time	i-f12233	i-18472f4e	i-3f3f52b1	i-55555	i-76f3e2bb	i-8e367543	i-98375216	i-cc15ffe4	i-d4565cf8
2024-08-07 16:28:00									
2024-08-07 16:29:00									
2024-08-07 16:30:00									
2024-08-07 16:31:00	9.62500000000001	19.78333333328677	19.78333333328677	19.78333333328677	19.78333333328677	19.78333333328677	19.78333333328677	4.844493840879823	19.78333333328677
2024-08-07 16:32:00									
2024-08-07 16:33:00									
2024-08-07 16:34:00									
2024-08-07 16:35:00									
2024-08-07 16:36:00	9.62500000000001	19.78333333328677	19.78333333328677	19.78333333328677	19.78333333328677	19.78333333328677	19.78333333328677	4.844493840879823	19.78333333328677
2024-08-07 16:37:00									
2024-08-07 16:38:00									

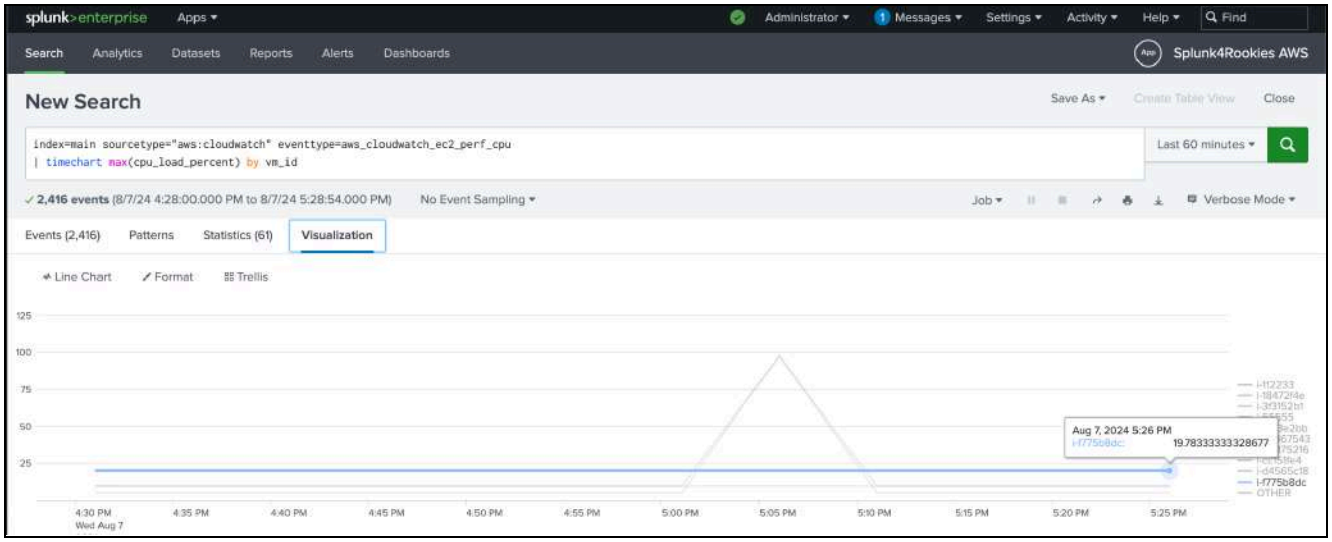
4. Create a line graph visualization that shows the CPU performance utilization for the last 60 minutes. Once you have created the line chart change the format to connect the lines



Null Values

Multi-series Mode: Yes | No

Show Data Values: Off | On | Min/Max



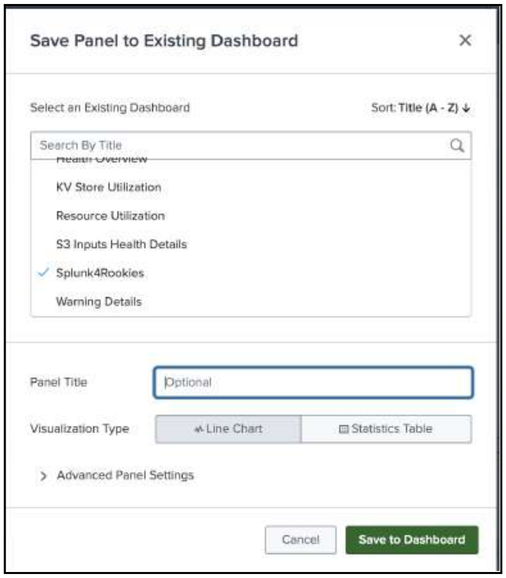
New Search

```
index=main sourcetype="aws:cloudwatch" eventtype=aws_cloudwatch_ec2_perf_cpu
| timechart max(cpu_load_percent) by vm_id
```

✓ 2,416 events (8/7/24 4:28:00.000 PM to 8/7/24 5:28:54.000 PM) No Event Sampling ▾

Aug 7, 2024 5:26 PM
i-f775b8dc 19.78333333328677

5. Save the visualization to your Splunk4Rookies dashboard.



Save Panel to Existing Dashboard ×

Select an Existing Dashboard Sort: Title (A - Z) ↓

Search By Title

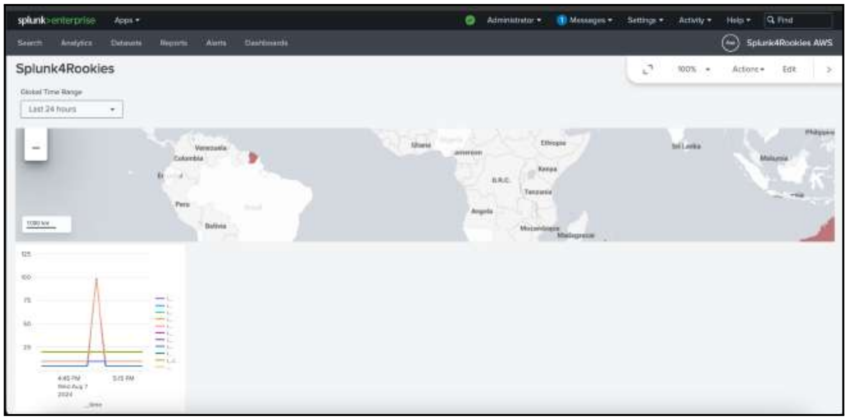
- Health Overview
- KV Store Utilization
- Resource Utilization
- S3 Inputs Health Details
- ✓ Splunk4Rookies
- Warning Details

Panel Title: Optional

Visualization Type: Line Chart | Statistics Table

› Advanced Panel Settings

Cancel | Save to Dashboard



splunk>enterprise
Apps ▾
Administrator ▾
Messages ▾
Settings ▾
Activity ▾
Help ▾
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Splunk4Rookies AWS
Splunk4Rookies
Global Time Range
Last 24 hours
100%
Actions ▾
Edit
Venezuela
Colombia
Peru
Bolivia
Ghana
Ethiopia
Kenya
Tanzania
Angola
Mozambique
Madagascar
Sri Lanka
Malaysia
Philippines
125
100
75
50
25
4:45 PM
Wed Aug 7
2024
5:15 PM