2. Dashboard Cookbook - Time Series

2023-07-07 10:54:01 AM to 2023-07-07 11:54:01 AM

errorCode * timeslice 15m

Welcome to the dashboards demo for dashboards!

This is one of a series of demonstration dashboards see:

1. Basics
2. Time Series
3. Advanced Analytics
4. Advanced Technigues

Checkout these micro learning videos:

- Create a Dashboard - Create a Simple Dashboard - Customize a Dashboard - Share a Dashboard Inside Your Organization

This is a set of dashboards that demonstrate how to write and format search output, and match that to various panel types.

Tip: Be A Legend

There are many possible options for the chart legend as shown in these panels:

- side
- bottom
- none
- displayed as a table

Tip: Chart Units

Improve the readability of charts by setting the correct units type for the axis such as bytes, MB, ms etc.

Tip: Time Ranges Per Panel

The time range of a panel can 'inherit' that global setting for the dashboard. You can also set a separate time range in the individual panels that don't change with the range for the whole dashboard.

Tip: Take an override

For metrics time series panels it's common to use an override to alias a time series name such as alais series #A with value

```
{{_collector}} - {{_devname}}
```

This makes charts more readable with nice concise series names.

Time Series Charting: Logs Need Timeslicing

Charting over time is important to get context on the issue at hand, gain insights about trends over time, and to determine if current state is normal or exceptional.

For log search use **timeslice** operator to create time buckets suitable for bar, line or area time series graphs. Timeslice buckets the events into time bands such as 5m, 1h or a fixed number of buckets.

There are THREE common types of time series searches and panels:

1. single series over time, or more than one aggregate for same timeslice

```
| timeslice by 5m | count _timeslice
or
| timeslice by 5m | count_distinct(errorcode) as codes, count _timeslice
or
| pct(size,10,50,95,99) by _timeslice
```

2. dynamic series over time. Use ***transpose** to chart for multiple series per timeslice. You will get one series for each value of a column.

```
| timeslice by 5m | count _timeslice, errorCode | transpose row _timeslice column errorCode
```

3. Time compare to compare current value with previous periods. This can be one or more periods or an aggregate

```
| timeslice by 5m | count _timeslice | compare with timeshift 7d
or
| compare with timeshift 7d 3
or
| compare with timeshift 7d 3 avg
```

Time Series Charting Metrics

Metrics data is also time series data so there is no need to 'timeslice' it. You also don't have to aggregate metrics to make a time series chart although it might be useful to do so.

You may need to define the quantize value though if you want specific time blocks.

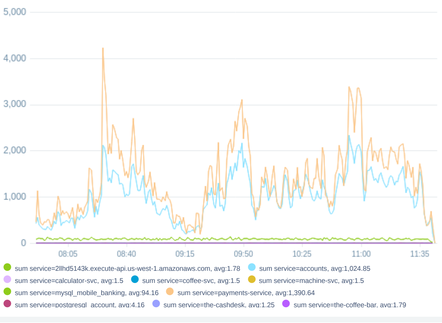
```
metric=service_requests _contentType=metricfromtrace
| quantize 1m using sum
| sum by service
```

When charting metric data the final format is much more dependant on the settings each panel for layout and format compared to logs.

For example many panel types have a 'statistic' option to choose say a average, latest, max etc for raw metric data.

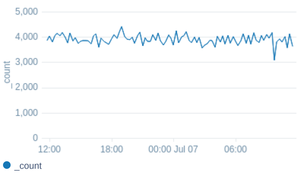
Distributed Tracing Requests By Service

2023-07-07 7:45:08 AM to 2023-07-07 11:45:08 AM

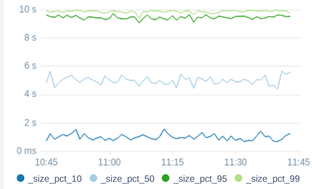


Time Series Single: count by _timeslice

2023-07-06 11:45:08 AM to 2023-07-07 11:45:08 AM

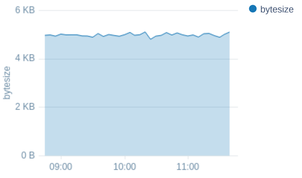


Time Percentiles with pct() operator, ms Unit y axis

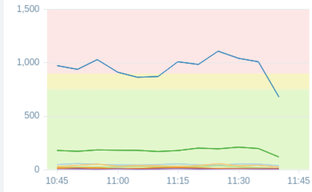


Time Series Single Area, bytes units, Legend: right

2023-07-07 8:45:08 AM to 2023-07-07 11:45:08 AM

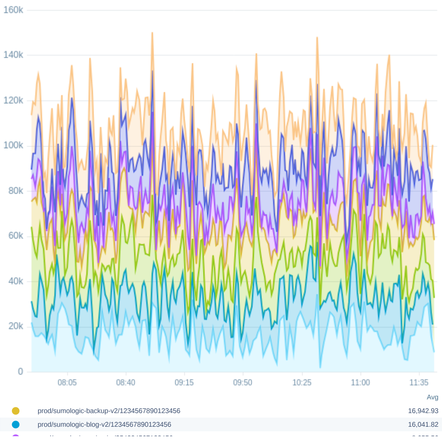


Timeseries For Multi Series (Transpose) , Thresholds Tab S…

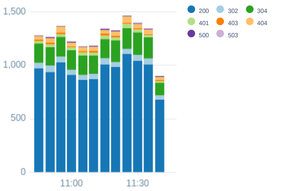


Metrics: Requests Served by ALB With Stats Table

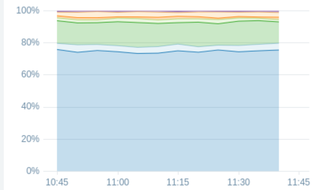
2023-07-07 7:45:08 AM to 2023-07-07 11:45:08 AM



Timeseries multiple stacked with transpose Legend: Table ri…



time series Transpose with Stacked Percent Area

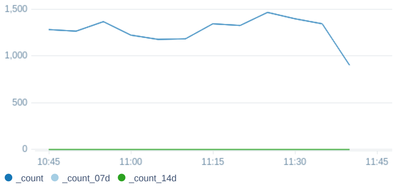


Time Compare

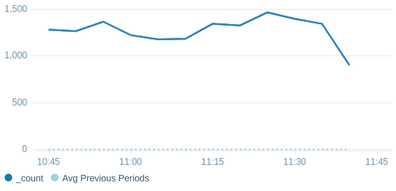
For a series over time we can add time compare to one or more previous periods. "this time last week", or this can be an average "average for this time for last 3 weeks"

```
_sourceCategory = Labs/Apache/Access
| timeslice by 5m
|count by _timeslice
 | compare with timeshift 7d 2
```

Time Compare



Time Compare (Avg)



Smooth Operator (Trend)

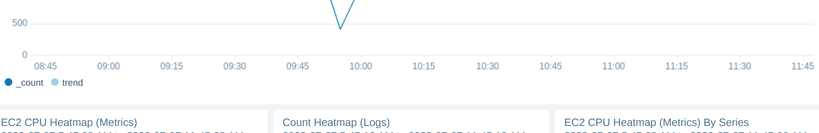
You may recall Sade from the late 20th century? If so you will love how you can add a trendline with the 'smooth operator'.

```
_sourceCategory = Labs/Apache/Access
| timeslice by 5m
|count by _timeslice  | sort _timeslice asc
 |smooth _count as trend
```

Did you know you can put markdown links in these panels?

Adding Trend: The 'smooth operator'

2023-07-07 8:45:08 AM to 2023-07-07 11:45:08 AM



Heat Maps

A heat map visualizes the count of data points returned by a metric ranges over time intervals of a specified duration. This feature is m non-aggregate results.

In a heat map, data points are aggregated by value on the y-axis, a Sumo Logic automatically calculates values for these settings, bas explicitly configure the desired value and time ranges, by clicking t section of the Chart View UI and entering new values.

metrics query:

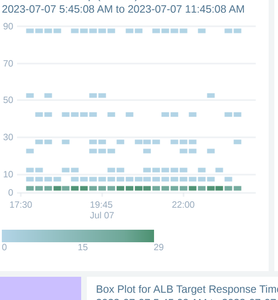
```
 instanceid =* namespace=aws/ec2
 metric=CPUUtilization Statistic=average
 | avg by instanceid
```

logs example (must timeslice ... transpose)

```
 exception | timeslice 15m
 | count by _timeslice,host | transpose row _
```

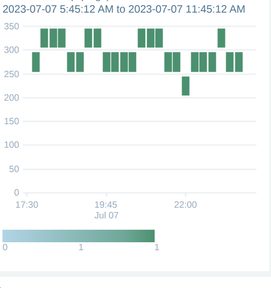
EC2 CPU Heatmap (Metrics)

2023-07-07 5:45:08 AM to 2023-07-07 11:45:08 AM



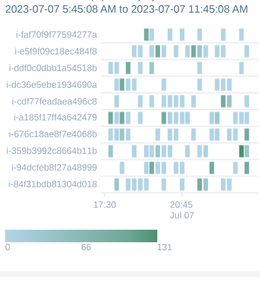
Count Heatmap (Logs)

2023-07-07 5:45:12 AM to 2023-07-07 11:45:12 AM



EC2 CPU Heatmap (Metrics) By Series

2023-07-07 5:45:08 AM to 2023-07-07 11:45:08 AM



Box Plots

Time series box plots are a great way to show statistical spread over time say for build tim

```
 _sourceCategory=*alb*
 | parse "* * * * * * * * * * * \"*\" \"*\" * * * \"*\"" as
 | timeslice
 | min(TargetProcessingTime), max(TargetProcessingTime),pct(T
```

Box Plot for ALB Target Response Time

2023-07-07 5:45:09 AM to 2023-07-07 11:45:09 AM