



Charting Averages, LogReduce(R), LogCompare, and Outliers

Calculating Changes and Moving Averages

diff

smooth

LogCompare and LogReduce

LogReduce

Surrounding message

LogCompare

deltaPercentage

isNew

Outlier

Calculating Changes and Moving Averages

diff

- ex) Calculate **difference in number** of requests over the last 15 minutes:

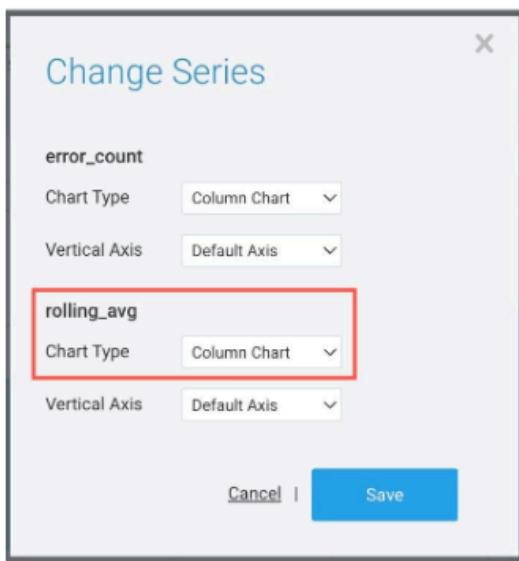
```
_sourceCategory=Labs/Apache/Access
| timeslice 1m
| count by _timeslice
| sort by _timeslice asc
| diff _count
```

smooth

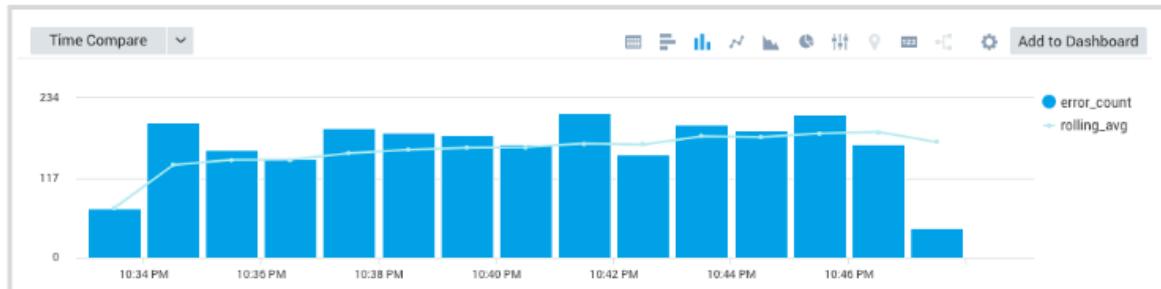
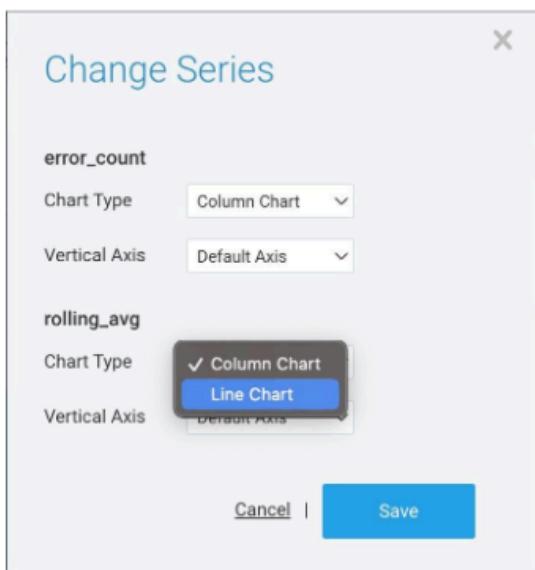
- Calculate moving **average** of 404 occurrences over the last 15 minutes

```
_sourceCategory=Labs/Apache/Access and status_code=404
| timeslice 1m
| count as error_count by _timeslice
| sort by _timeslice asc
| smooth error_count as rolling_avg
```

In the **Change Series** pop up, click **Chart Type** drop-down arrow for **rolling_avg**.



Select **Line Chart** from the drop down list, and then click **Save**.



LogCompare and LogReduce

LogReduce

- Allows you to distill unique messages from the noise by identifying **recurring Signatures** in the data

Surrounding message

3. Now, click on the Host to view [surrounding messages](#). You will be able to look at surrounding messages for 1, 5 or 10 minutes +/- . This troubleshooting capability may additional help you to identify why something has happened.

#	Time	Message
1	07/24/2017 08:42:27.000 -0700	Jul 24 15:42:27 VIRUS OUTBOUND bad file attachment [Classification: A [Priority: 2] {TCP} 36.218.252.27:93038 -> 10.182.141.33:74396 Host: 54.224.66.85 ▾ Name: Http Input ▾ Category: Labs/security/snort ▾

[+/- 1 Minute](#) [+/- 5 Minutes](#) [+/- 10 Minutes](#)

LogCompare

- Allows you to compare log activity from two different time period
 - Insight on how your current time compares to a baseline

```
_sourceCategory=Labs/Apache/Access and status_code=404  
| logcompare timeshift -24h
```

deltaPercentage

- To view only those results where Delta Percentage is more than 25%

```
_sourceCategory=Labs/Apache/Access and status_code=404  
| logcompare timeshift -24h  
| where abs(_deltaPercentage) > 25
```

isNew

- To view results where there is a new Signature in the current time period

```
_sourceCategory=Labs/Apache/Access and status_code=404  
| logcompare timeshift -24h  
| where (_isNew)
```

Outlier

- Allows you to identify events **outside of a threshold**.

```
_sourceCategory=Labs/Apache/Access status_code=404  
| timeslice 1m  
| count(status_code) as error_count by _timeslice  
| outlier error_count window=10, consecutive=1, threshold=3, direction=+-
```