

Become a

Sumo Metrics Analyst

Metrics Mastery Certification



Become a Sumo Metrics Certified Analyst

1. Learn how to use a unified Logs and Metrics solution
2. Learn about Metrics and their properties
3. Learn how to collect Metrics data
4. Develop a toolset for basic and advanced Metrics analytics
5. Apply knowledge through Labs to solve common use cases

Course Agenda

- 10 min. ● Course Logistics
- 20 min. ● Reviewing the Basics: Demo and Data Flow
- 10 min. ● Collecting Metrics
- 10 min. ● Analyzing Metrics
- 40 min. ● Use Cases
- 20 min. ● Monitoring Metrics
- 10 min. ● Summary and Next Steps
- 60 min. ● Examination

Logistics

How do I get access to the training?

sumo logic



Tutorial: Hands-on Exercises

Training Environment:

Go to: service.sumologic.com

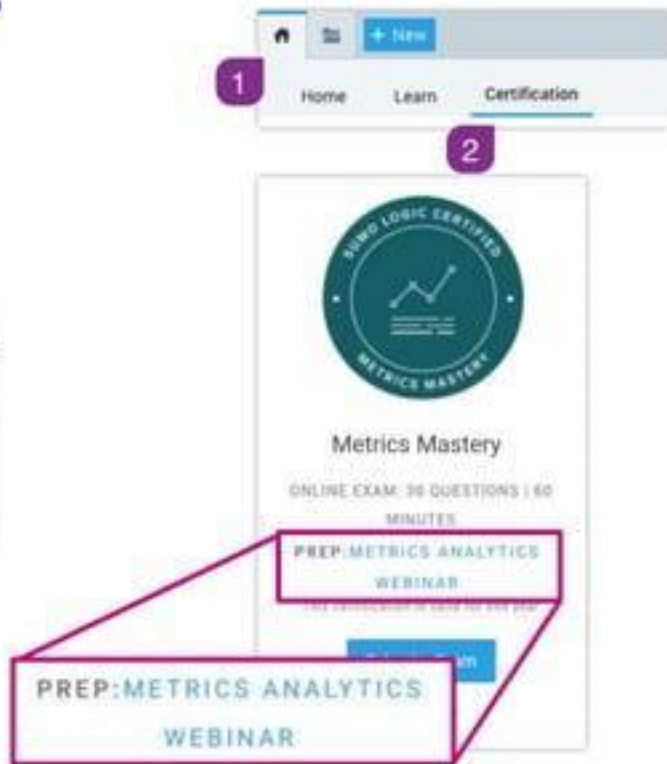
username: training+user###@sumologic.com

password: Sum0Labs!

will be a
number between
001 and 600

Hands-on Labs:

- Follow along using the labs found under **Home > Certifications**



Reviewing the Basics

Demo & Dataflow

sumo logic



Demo: Monitor and Troubleshoot



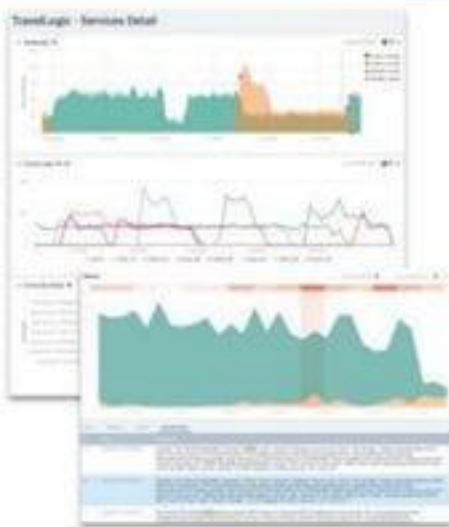
ALERTS

notify of a critical event



METRICS

to identify what's going on



LOGS

to identify why it's happening

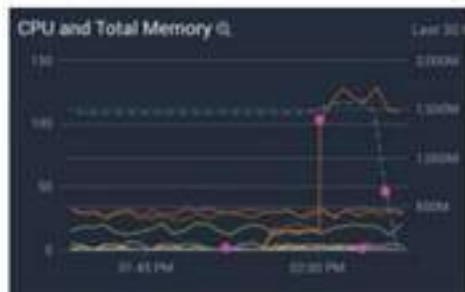


Intro to Metrics

A metric is a set of **data points** that **measure the value** of something **over time**.

Everyday Metrics:

- Measurements of temperature on an hourly basis
- Your weight once a week
- The height of your child every 6 months



Examples of how Metrics can be used in your Environments:

- Track KPIs over time to gain end-to-end visibility into application performance.
- Determine if an outage has occurred and restore service.
- Determine why an event occurred and how it might be prevented in the future.

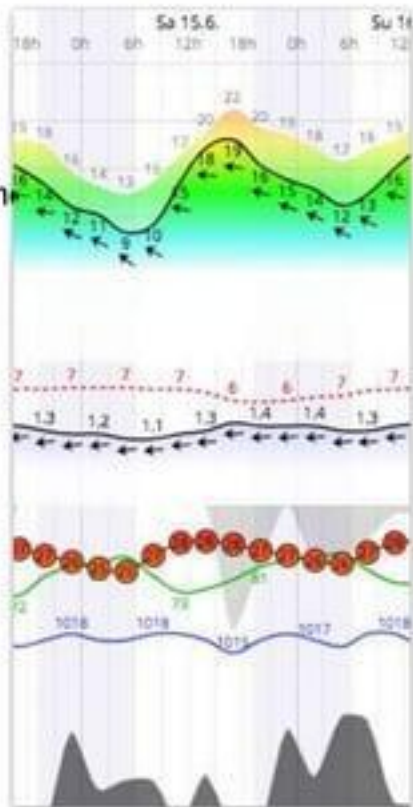
Metrics versus Logs

How are Logs different from Metrics?

- **METRICS** → Numeric measurements of data collected over time
- **LOGS** → Records of events that occurred.

Review - LOG or METRIC?

- Wind patterns for the last 24 hours
- Every time wind exceeded 20 knots
- Number of server errors on an hourly basis
- CPU Uptime for the last 15 min
- Failed login

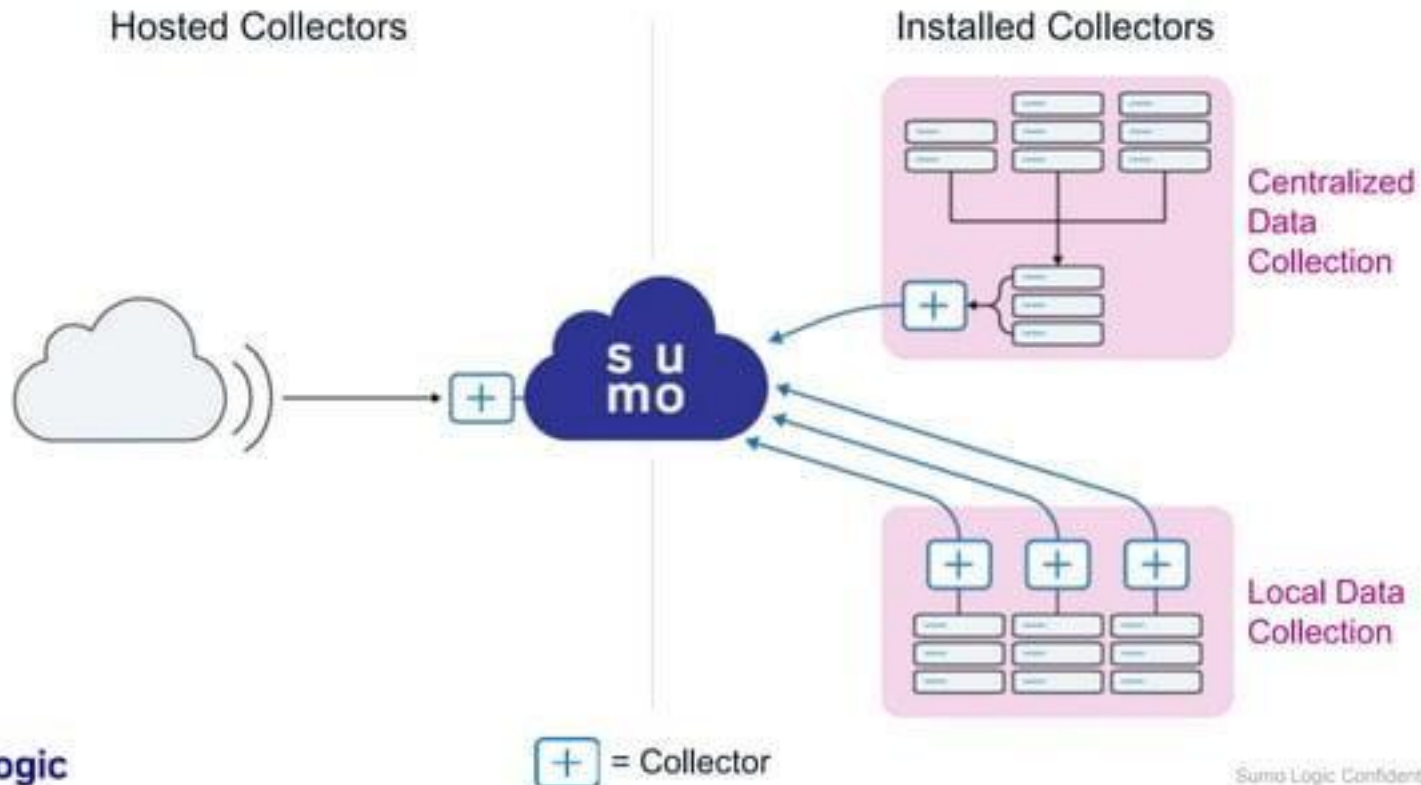


Sumo Logic Data Flow

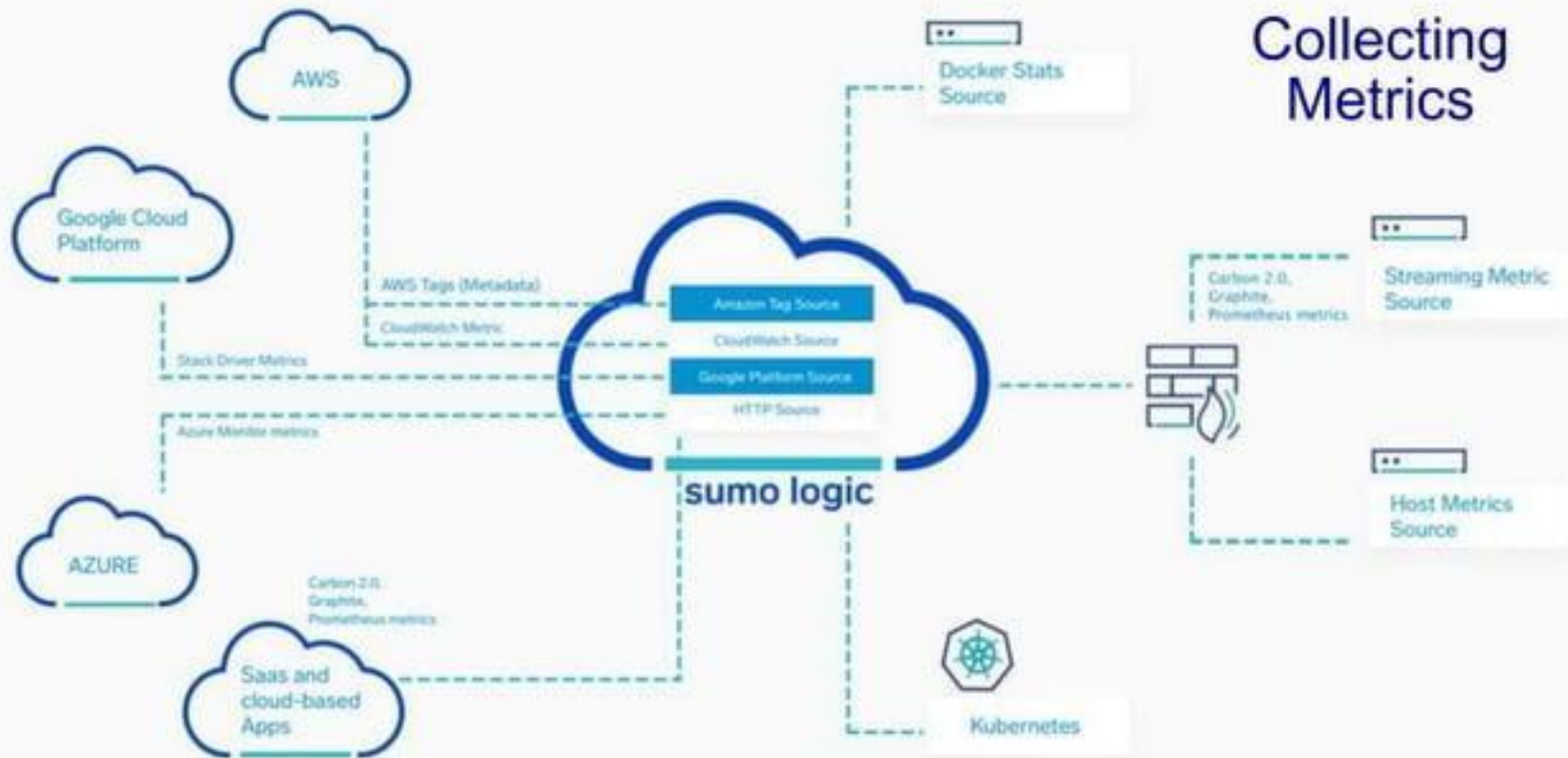


Collecting Metrics

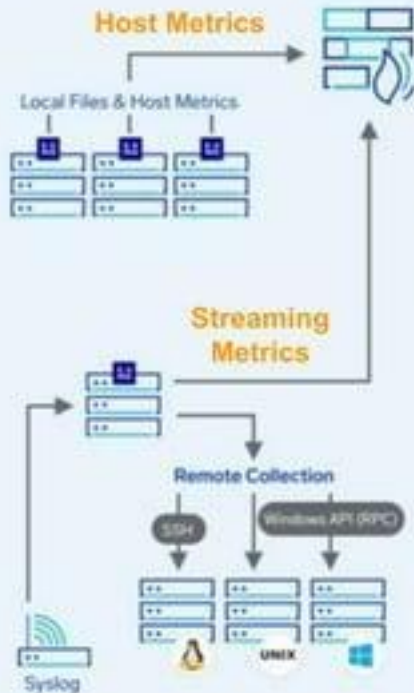
Collector and Deployment Options



Collecting Metrics



Installed Collectors



sumo logic

Logs-to-Metrics

Docker Stats

Containers

docker

Docker Logging Driver
Docker Collector Container
Collector on Docker Host

kubernetes

Kubernetes Operator Plugin
Ready for a Kubernetes Ecosystem

AWS Metrics + Metadata

Hosted Collectors

aws

CloudWatch Logs

EC2

CloudWatch Metrics

HTTP Metrics

Stackdriver

Google Cloud Platform

Microsoft Azure

Monitor

Blob Storage

CDN

fastly

Akamai

Cloudflare

Security

Carbon Black,

CYLANCE

netkope

TREND MICRO

SaaS

Office 365
Salesforce
G Suite

SSO/MFA

okta
onelogin
Duo

Metric Ingestion and Storage

Metric Ingestion

- Sumo does not ingest metric data that is more than **one week** old.

Metric Retention

- Metrics data is stored as raw, one minute, and one hour resolutions. It's retained according to the following retention policy:
- For historical rollups (1 minute and 1 hour) Sumo calculates the max, min, avg, sum, and count values for a metric per minute or hour.

Data Type Retained	Retention Period
Raw	7 days
1 minute resolution	30 days
1 hour resolution	13 months

Analyzing Metrics

Analyzing Metrics

You can easily query metrics using a **key-value pair format**.

Let's say we are looking to analyze the wind speed in Spain for the last 24 hours.

Your initial query can look like this:

➤ If you have 255 stations across Spain, this will plot all 255 stations over time:



```
metric=wind-speed region=eu country=spain
```

➤ If you care for only the 3 stations in **Valencia**:



```
metric=wind-speed region=eu country=spain city=valencia
```

➤ If you want to see the **average** of these 3 stations:



```
metric=wind-speed region=eu country=spain city=valencia | avg
```

Analyzing Metrics - Operators

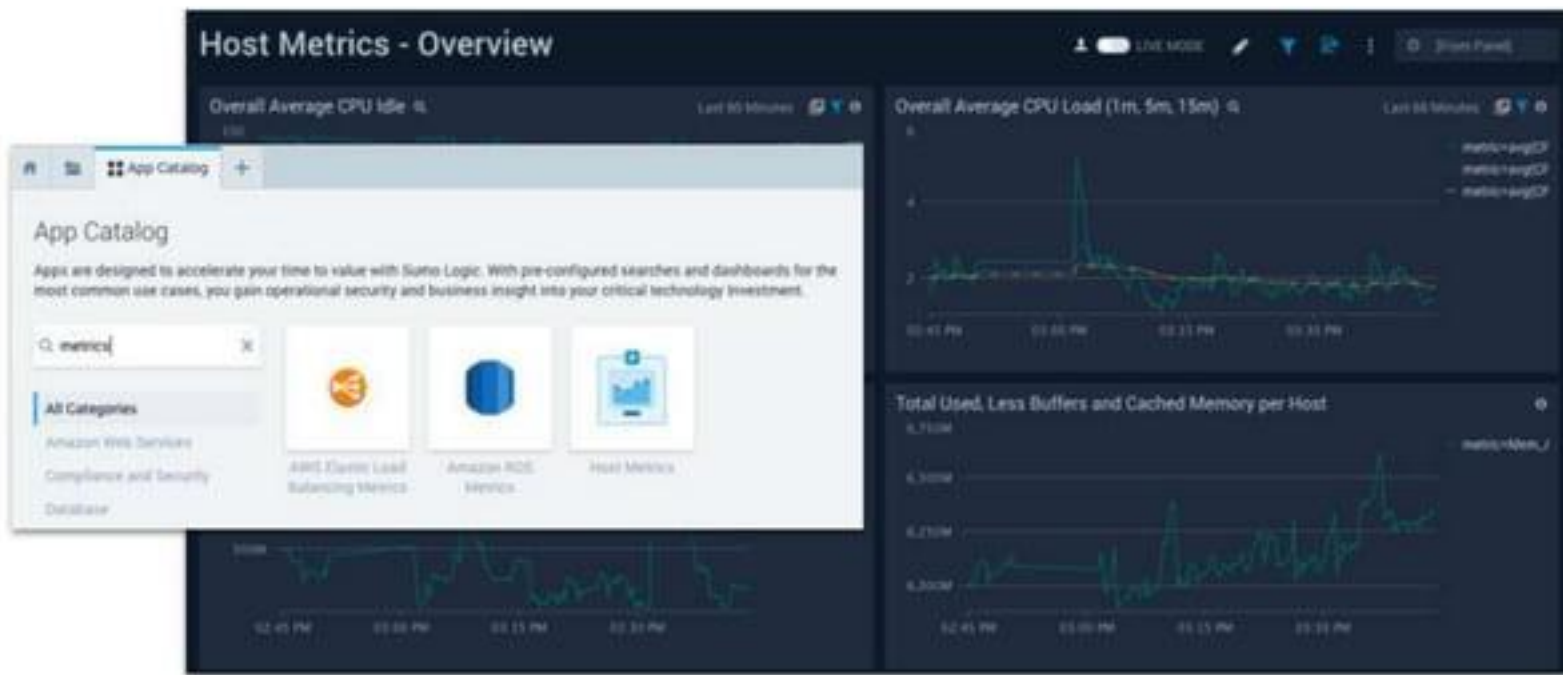


```
| accum | avg | along | bottomk | count | delta  
| eval | filter | max | min | parse | pct  
| quantize | rate | sum | timeshift | topk
```

https://help.sumologic.com/Metrics/Metric-Queries-and-Alerts/03Metrics_Operators

Use Case 1: Host Metrics

Metrics Apps: Out-of-the-Box Content



Metrics Certification: Hands-on Labs

Using Sumo Logic

Use Case 1: Host Metrics (Labs 1-4)

- Install a Collector
- Create a Metrics Source
- Query your Metrics
- Install the Host Metrics App

Optional Labs (Labs 5-6)

- Joining Metric Queries
- Filtering Results

Use Case 2: AWS Metrics

AWS Metrics

AWS metrics are collected via CloudWatch



AWS Documentation » Amazon CloudWatch » User Guide » AWS Services That Publish CloudWatch Metrics

AWS Services That Publish CloudWatch Metrics

The following AWS services publish metrics to CloudWatch. For information about the metrics and dimensions, see the specified documentation.

Service	Namespace	Documentation
Amazon API Gateway	AWS/ApiGateway	Monitor API Execution with Amazon CloudWatch
AppStream 2.0	AWS/AppStream	Monitoring Amazon AppStream 2.0 Resources
Amazon Athena	AWS/Athena	Monitoring Athena Queries with CloudWatch Metrics
AWS Billing and Cost Management	AWS/Billing	Monitoring Charges with Alerts and Notifications
ACM Private CA	AWS/ACMPrivateCA	Supported CloudWatch Metrics
Amazon CloudFront	AWS/CloudFront	Monitoring CloudFront Activity Using CloudWatch
AWS CloudHSM	AWS/CloudHSM	Getting CloudWatch Metrics
Amazon CloudSearch	AWS/CloudSearch	Monitoring an Amazon CloudSearch Domain with

[AWS Docs]

Detail of each Metric, by source:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/aws-services-cloudwatch-metrics.html>

Collecting AWS Metrics

AWS metrics are collected via CloudWatch



Name* AWS ALB Metrics - Training
Maximum name length is 128 characters.

Description Training Example to set up a CloudWatch Metrics Source

Regions * [Select All](#) | [Select None](#)

- ☐ eu-west-3
- ☐ sa-east-1
- ☒ us-east-1
- ☐ us-east-2
- ☒ us-west-1
- ☒ us-west-2

Namespaces [Select All](#) | [Select None](#)

- ☐ AWS/EFs
- ☒ AWS/ELB
- ☐ AWS/ES

AWS Tag Filters Enter keys and values below to add filters to your metrics. Separate multiple values for the same key with semicolons. Tag filtering for extended AWS namespaces, (other than AWS/EC2) is in beta. Please read our [documentation](#) for more information.

Namespace	Key	Values
AWS/ELB	environment	= prod
Select Namespace		=

Custom Namespaces

Enter a comma-separated list of custom namespaces from which you would like to collect logs. Custom namespaces must not be an AWS namespace, i.e. the namespace must not be prefixed with AWS/

Source Category Training/AWS/ALB/Metrics

Category metadata to use later for querying, e.g. prod/web/apache/access. This data is queried using the "_sourceCategory" key name.

Collecting and Analyzing AWS Metrics

Tips and Tricks

Only send necessary metrics (use filters):

AWS Tag Filters

Enter keys and values below to add filters to your metrics. Separate multiple values for the same key with semicolons. Tag filtering for extended AWS namespaces, (other than AWS/EC2) is in beta. Please read our [documentation](#) for more information.

Namespace

Key

Values

AWS/ELB



environment



prod



Choose the right scan intervals:

AWS reports CloudWatch metrics at different granularities (1-minute, 3-minute, and 5-minute intervals), so setting a scan interval that's too short could lead to excessive querying. Setting an interval that's too long can delay the update frequency of new metrics appearing in Sumo Logic.

Bring your AWS Metadata into Sumo:

Sumo Logic allows you to collect tags you have assigned to selected AWS resources. Create an AWS Metadata Source and bring in your tags straight into Sumo.

For EC2, save \$\$ with an installed Collector:



EC2 metrics have high latency and can increase the costs of your AWS account. For EC2 metrics, consider [installing a Collector with a Host Metrics Source](#). The advantage is near zero latency and more information at a lower overall cost.

When querying, choose the right Statistic:

CloudWatch generates the following 5 statistics for all metrics:

- Minimum
- Maximum
- Average
- Sum
- SampleCount

AWS docs recommend the relevant statistic for each metric.

Metrics Certification: Hands-on Labs

Using Sumo Logic

Use Case 2: AWS Metrics (Lab 7)

- Query the AWS ALB Metrics
- Install AWS ALB Metric App
- Reverse-engineer Advanced Metrics Queries

Use Case 3: Metric Formats

Review: Query Metrics

You can easily query metrics using a **key-value pair format**.

Let's say we are looking to analyze the wind speed in Spain for the last 24 hours.

Your initial query can look like this:

➤ If you have 255 stations across Spain, this will plot all 255 stations over time:



➤ If you care for only the 3 stations in **Valencia**:



➤ If you want to see the **average** of these 3 stations:



Supported Metric Formats

Carbon 2.0

```
cluster=cluster-1 node=node-1 cpu=cpu-1 metric=cpu-idle 97.29 1460061337
```

Prometheus

```
# HELP cpu-idle Total system cpu idle time.  
# TYPE cpu-idle counter  
cpu-idle{cluster="cluster-1" "node=node-1" "cpu=cpu-1"} 97.29 1460061337  
cpu-idle{cluster="cluster-1" "node=node-1" "cpu=cpu-1"} 94.12 1460242839
```

Graphite

```
cluster-1.node-1.cpu-1.cpu-idle 97.29 1460061337
```

Metrics Rule Editor

Convert Graphite format to key-value pair tags

Similar to log parsing, you specify field positions and provide a variable name.

Note: This parsing option is also available at query time with the **parse** operator.

Identify Metrics

Parse fields

Update Metrics Rule

Metrics rule expression *

travel *****

* is a variable in your metrics series. You can assign a position and number of characters.

Define variables:

Variable name *	Tag sequence *	
node	= \$,3	
pod	= \$,3	
metric	= \$,5	
Namespace	= \$,1	
Variable name *	Tag sequence *	
type	= \$,4	

Update Metrics Rule

TIME SERIES	node	pod	METRIC	NAMESPACE	TYPE
travel.training.timers.travel-checkout-75498f5b64-r5slp.payment.latency.upper	travel-che...	travel-che...	latency.up...	training	payment
travel.training.counters.travel-checkout-75498f5b64-r5slp.bookings.fail.count	travel-che...	travel-che...	fail.count	training	bookings
travel.training.counters.travel-checkout-75498f5b64-r5slp.bookings.fail.count	travel-che...	travel-che...	fail.count	training	bookings

Metrics Certification: Hands-on Labs

Using Sumo Logic

Use Case 3: Metric Formats (Lab 8)

- Test existing Metrics Rule
- Query your Custom TravelLogic Metrics

Use Case 4: Logs to Metrics

Logs-to-Metrics

What is it?

Logs-to-Metrics is a feature that converts the results of a log search to a metric view.



Converts to



Logs-to-Metrics

Why do this?

1

Performance



Analyzing time-series data is much faster than parsing and querying unstructured data.

2

Retention



Metrics are retained for 13 months by default. Good for long-term KPIs or operational trends.

3

Alerting



High-performing, near real-time alerts optimized for time-series data.

Metrics Certification: Hands-on Labs

Using Sumo Logic

Use Case 4: Logs to Metrics (Lab 9)

- Review your existing Apache Logs for count of 404s
- Create a Logs-to-Metrics Rule
- Query your new Apache Metrics

Monitoring Metrics

Monitoring your Metrics

Charts >> Panels >> Dashboards



Metric Monitors >> Alerts



Metrics Certification: Hands-on Labs

Using Sumo Logic

Monitoring your Metrics (Lab 10)

- Create a Dashboard using metrics charts from previous labs
- Create an Metric Monitor that Alerts on a given threshold
- **IMPORTANT:**
 - **DELETE** your Metric Monitor so you do not receive notifications after this training

Where do I go from here?

Training, Docs, Community, Support



Need knowledge? ⇒ try the **Learn** tab

sumo logic

Learn

Quick Start Videos

Sumo Logic QuickStart
August 2018

Introduction to Search

Building Dashboards

Simplifying Search with Search Templates

Introduction to Metrics in Sumo

Using Sumo Logic Tutorial

- Part 1: Winning Data
- Part 2: Search for Log Data
- Part 3: Chart your data
- Part 4: Create and share a dashboard
- Part 5: Modify your dashboard
- Part 6: Create an alert
- Part 7: Get help

Set Up Sumo Logic Tutorial

- Part 1: Install a Collector
- Part 2: Add a Source
- Part 3: Install an App and View Data
- Part 4: Try Simple Analytics
- Part 5: Collect and Visualize Host Metrics

Check Status

Docs

What's New

Ask for Support

Get Training

Community

Explore the tutorials

Need knowledge? ⇒ try the **Learn** tab

sumo logic

Home Learn Dashboard

Quick Start Videos

Sumo Logic QuickStart Webinar - August 2018

Introduction to Search

Building Dashboards

Simplifying Search with Search Templates

Introduction to Metrics in Sumo

Using Sumo Logic Tutorial

- Part 1: Viewing Data
- Part 2: Search for Log Data
- Part 3: Chart your data
- Part 4: Create and share a dashboard
- Part 5: Modify your dashboard
- Part 6: Create an alert
- Part 7: Get help

Set Up Sumo Logic Tutorial

- Part 1: Install a collector
- Part 2: Add a source
- Part 3: Install an app and view data
- Part 4: Try Simple analytics
- Part 5: Collect and visualize host metrics

Check Status Docs Share Your Idea

Ask for Support Get Training Community

Explore the tutorials

Access comprehensive
lists of operators and
more

Need knowledge? ⇒ try the **Learn** tab

sumo logic

Learn

Quick Start Videos

Sumo Logic QuickStart Webinar - August 2018

Introduction to Search

Building Dashboards

Simplifying Search with Search Templates

Introduction to Metrics in Sumo

Using Sumo Logic Tutorial

- Part 1: Viewing Data
- Part 2: Search for Log Data
- Part 3: Chart your data
- Part 4: Create and share a dashboard
- Part 5: Modify your dashboard
- Part 6: Create an alert
- Part 7: Get help

Set Up Sumo Logic Tutorial

- Part 1: Install a collector
- Part 2: Add a source
- Part 3: Install an app and view data
- Part 4: Try Simple analytics
- Part 5: Collect and visualize host metrics

Check Status

Docs

Share Your Idea

Ask for Support

Get Training

Community

Explore the tutorials

Access comprehensive lists of operators and more

Every feature and tool covered in docs

Need knowledge? ⇒ try the **Learn** tab

Explore the tutorials

Access comprehensive lists of operators and more

Every feature and tool covered in docs

Find out What's New

Need knowledge? ⇒ try the **Learn** tab

Explore the tutorials

Access comprehensive lists of operators and more

Every feature and tool covered in docs

Find out What's New

Find answers or post your questions to Community

Need knowledge? ⇒ try the **Learn** tab

sumo logic

Learn

Quick Start Videos

Sumo Logic QuickStart Webinar - August 2018

Introduction to Search

Building Dashboards

Simplifying Search with Search Templates

Introduction to Metrics in Sumo

Using Sumo Logic Tutorial

- Part 1: Viewing Data
- Part 2: Search for Log Data
- Part 3: Chart your data
- Part 4: Create and share a dashboard
- Part 5: Modify your dashboard
- Part 6: Create an alert
- Part 7: Get help

Set Up Sumo Logic Tutorial

- Part 1: Install a collector
- Part 2: Add a source
- Part 3: Install an app and view data
- Part 4: Try Simple analytics
- Part 5: Collect and visualize host metrics

Check Status

Docs

What's New

Get Support

Get Training

Community

Explore the tutorials

Access comprehensive lists of operators and more

Every feature and tool covered in docs

Find out What's New

Find answers or post your questions to Community

Attend/review training and get certified

Need knowledge? ⇒ try the **Learn** tab

Explore the tutorials

Access comprehensive lists of operators and more

Every feature and tool covered in docs

Find out What's New

Find answers or post your questions to Community

Attend/review training and get certified

Open a Support case

Need knowledge? ⇒ try the **Learn** tab

The screenshot shows the Sumo Logic 'Learn' tab. At the top, there's a navigation bar with 'Home', 'Learn' (active), and 'Certification'. Below this is a 'Quick Start Videos' section with five video thumbnails: 'Sumo Logic QuickStart Webinar - August 2018', 'Introduction to Search', 'Building Dashboards', 'Simplifying Search with Search Templates', and 'Introduction to Metrics in Sumo'. Below the videos are two columns of links. The left column, 'Using Sumo Logic Tutorial', lists seven parts from 'Viewing Data' to 'Get help'. The right column, 'Set Up Sumo Logic Tutorial', lists five steps from 'Install a Collector' to 'Collect and Visualize Host Metrics'. To the right of these columns is a grid of six icons: 'Check Status' (magnifying glass), 'Docs' (document), 'What's New' (megaphone), 'Ask for Support' (question mark), 'Get Training' (lightbulb), and 'Community' (person with speech bubble).

sumo logic

Home Learn Certification

Quick Start Videos

Sumo Logic QuickStart Webinar - August 2018

Introduction to Search

Building Dashboards

Simplifying Search with Search Templates

Introduction to Metrics in Sumo

Using Sumo Logic Tutorial

- Part 1: Viewing Data
- Part 2: Search for Log Data
- Part 3: Chart your data
- Part 4: Create and share a Dashboard
- Part 5: Modify your Dashboard
- Part 6: Create an alert
- Part 7: Get help

Set Up Sumo Logic Tutorial

- Part 1: Install a Collector
- Part 2: Add a Source
- Part 3: Install an App and View Data
- Part 4: Try Simple Analytics
- Part 5: Collect and Visualize Host Metrics

Check Status

Docs

What's New

Ask for Support

Get Training

Community

Explore the tutorials

Access comprehensive lists of operators and more

Every feature and tool covered in docs

Find out What's New

Find answers or post your questions to Community

Attend/review training and get certified

Open a Support case

Questions?



In order to get credit for the exam,
In YOUR OWN INSTANCE, go to
Certification Tab.

- Online Exam
- 30 Multiple choice questions
- 60-minute time limit
- 3 attempts



Metrics Mastery

ONLINE EXAM: 30 QUESTIONS | 60 MINUTES

PREP: USING SUMO LOGIC WEBINAR &
HANDS ON LABS

This certification is valid for two years



Take the Exam

[Learn More](#)

s

u

Empowering the
people who power
modern business

m

o

sumo logic