



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?



# Tutorial: Hands-on Exercises

## Training Environment:

Go to: [service.sumologic.com](https://service.sumologic.com)

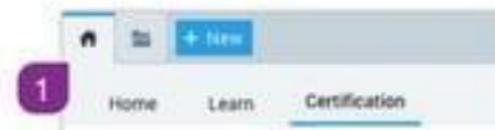
username: training+user###@sumologic.com

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



# Demo: Monitor and Troubleshoot



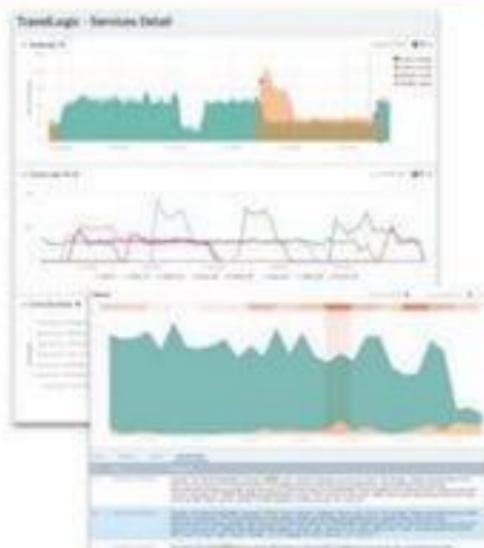
## ALERTS

notify of a critical event



## METRICS

to identify what's going on



## LOGS

to identify why it's happening

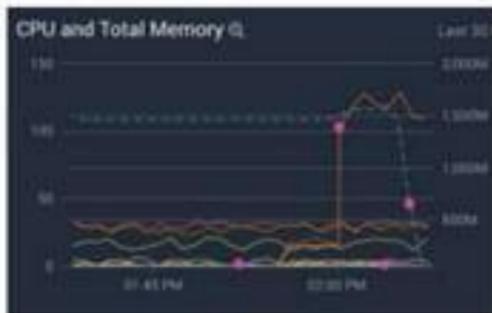


# Intro to Metrics

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.

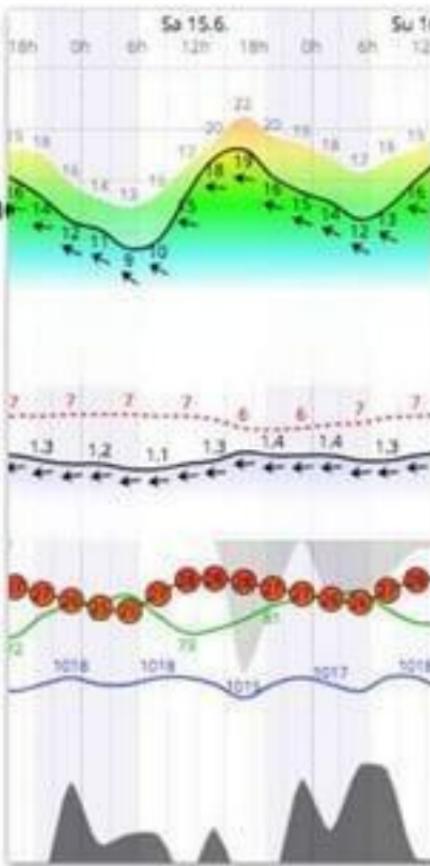
# Metrics versus Logs

## 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



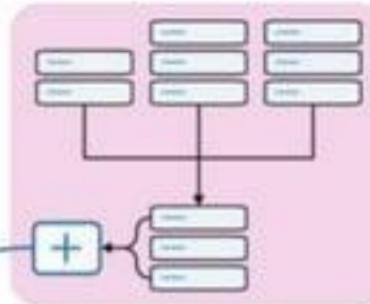
# Collecting Metrics

# Collector and Deployment Options

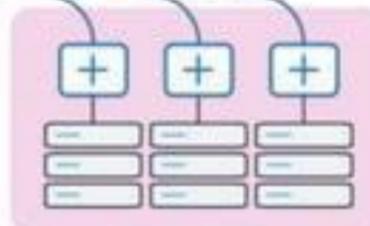
Hosted Collectors



Installed Collectors

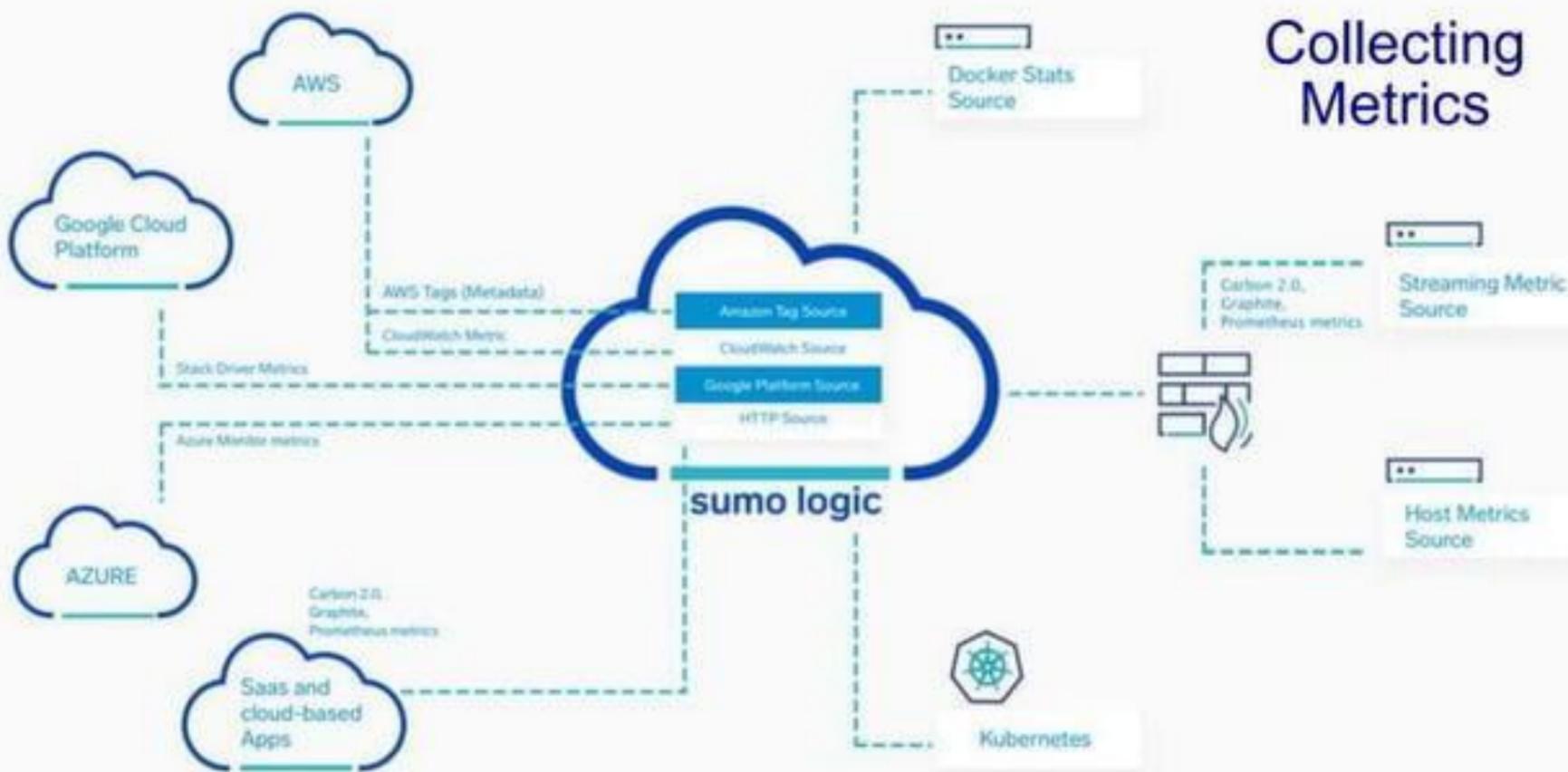


Centralized  
Data  
Collection

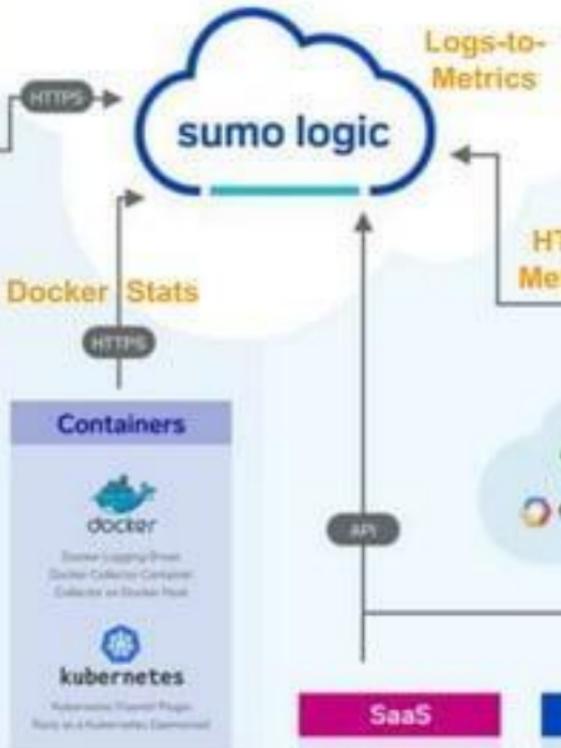
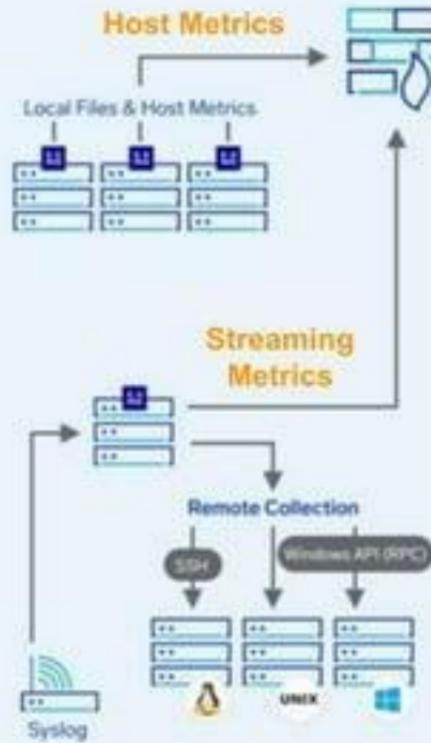


Local Data  
Collection

# Collecting Metrics



## Installed Collectors



AWS Metrics + Metadata



Hosted Collectors



Security

Carbon Black,  
CYLANCE  
netskope  
TREND MICRO

SSO/MFA

okta  
onelogin  
DUO

SaaS

G Suite

# 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:



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



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



# Analyzing Metrics - Operators

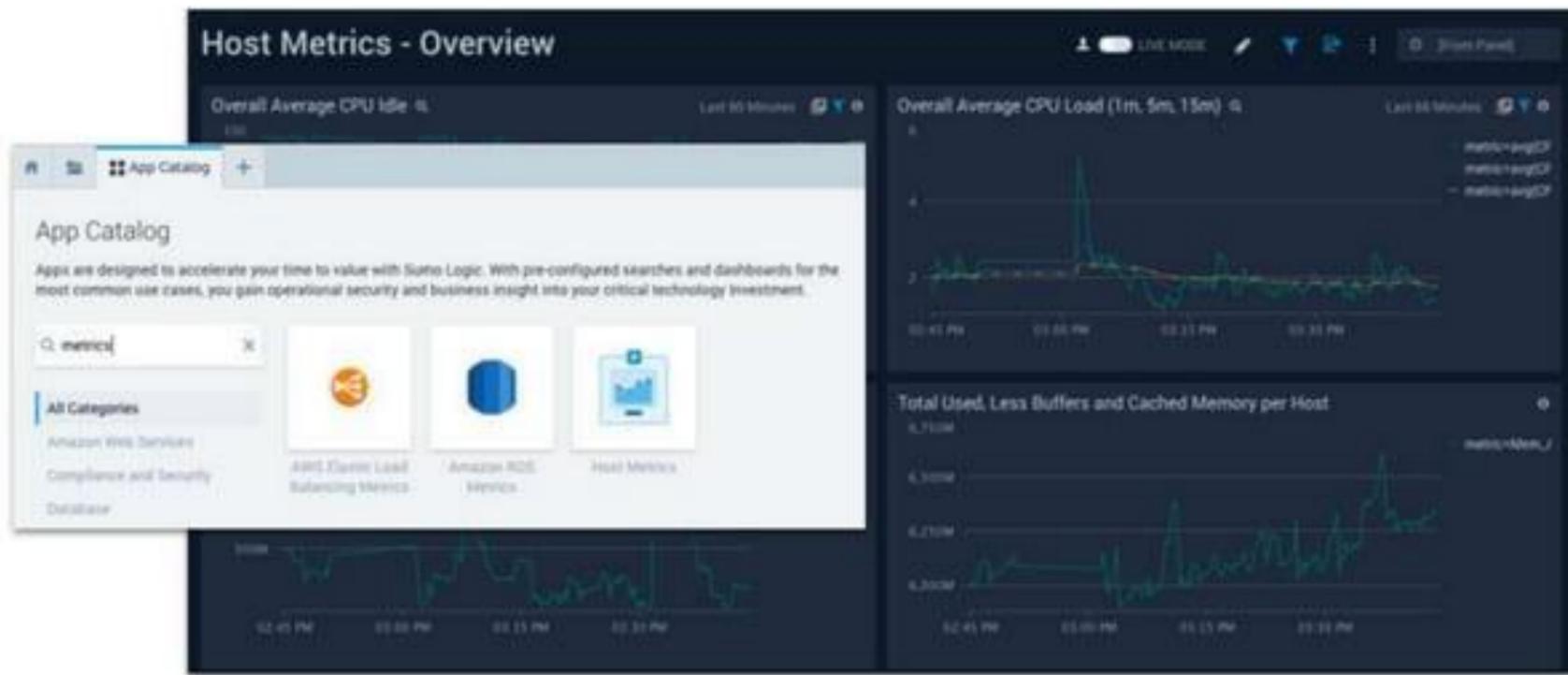


```
| accum | avg | along | bottomk | count | delta  
| eval | filter | max | min | parse | pct  
| quantize | rate | sum | timeshift | topk
```

[https://help.sumologic.com/Metrics/Metric-Queries-and-Alerts/03Metrics\\_Operators](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



AWS  
CloudWatch  
Metrics

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

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		=

Namespaces Select All | Select None

- AWS/EFS
- AWS/ELB
- AWS/ES

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. The 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

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.

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.

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.



# 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.



# Logs-to-Metrics

Why do this?

1

Performance

2

Retention

3

Alerting



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

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

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

The screenshot shows the 'Learn' tab of the Sumo Logic interface. At the top, there's a navigation bar with 'Learn' highlighted. Below it, a section titled 'Quick Start Videos' displays five video thumbnails:

- Sumo Logic Overview
- Introduction to Search
- Building Dashboards
- Simplifying Search with Search Templates
- Introduction to Metrics in Sumo

Below these videos, two sections of tutorials are listed:

- 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

On the right side of the interface, there are several icons with corresponding links:

- Search icon: Direct Search
- Document icon: Docs
- Bell icon: Notify Me
- Question mark icon: Ask for Support
- Person icon: Self Training
- Community icon: Community

Explore the tutorials

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

The screenshot shows the 'Learn' tab of the Sumo Logic interface. At the top, there's a navigation bar with 'Home', 'Learn' (which is highlighted), and 'Community'. Below this, there's a section titled 'Quick Start Videos' featuring six video cards:

- Sumo Logic Overview
- Introduction to Search
- Building Dashboards
- Simplifying Searches with Templates
- Search
- Introduction to Metrics in Sumo

Below these videos, there are two main sections:

- Using Sumo Logic Tutorial:** A list of 10 parts:
  - 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:** A list of 6 parts:
  - 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

On the right side of the interface, there are several icons with labels:

- Search icon: Search
- Document icon: Docs
- Bell icon: Notify Me
- Question mark icon: Ask for Support
- Checkmark icon: Self Training
- Person icon: Community

Explore the tutorials

Access comprehensive lists of operators and more

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

The screenshot shows the Sumo Logic interface with the 'Learn' tab selected. The page is divided into several sections:

- Quick Start Videos:** A row of five video thumbnails with titles: "Sumo Logic Overview", "Introduction to Search", "Building Dashboards", "Simplifying Searches with Search Templates", and "Introducing Metrics in Sumo".
- Using Sumo Logic Tutorial:** A list of 10 parts:
  - 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
  - Part 8: Set up a collector
  - Part 9: Add a source
  - Part 10: Install an app and view data
- Set Up Sumo Logic Tutorial:** A list of 6 parts:
  - 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
- Documentation and Support:** A grid of icons with labels: "Search", "Docs", "Metrics", "Dashboard", "Alerts", "Logs", "Collectors", "Sources", "Apps", "Analytics", "Host Metrics", "Help", "Get Help", "Self Training", and "Community".

Explore the tutorials

Access comprehensive lists of operators and more

Every feature and tool covered in docs

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

The screenshot shows the 'Learn' tab of the Sumo Logic interface. At the top, there's a navigation bar with 'Home', 'Learn' (which is selected), and 'Community'. Below the navigation is a section titled 'Quick Start Videos' featuring five video thumbnails:

- Sumo Logic Overview
- Introduction to Search
- Browsing Dashboards
- Simplifying Searches with Search Templates
- Introduction to Metrics in Sumo

Below these videos is a section titled 'Using Sumo Logic Tutorial' containing a numbered list of steps:

- 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

Next to this is another section titled 'Set Up Sumo Logic Tutorial' with its own numbered list:

- 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

At the bottom right of the main content area are several icons:

- Search icon: Direct Search
- Document icon: Docs
- Bell icon: What's New
- Question mark icon: Ask for Support
- Checkmark icon: Self Training
- User icon: Community

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

The screenshot shows the 'Learn' tab of the Sumo Logic interface. At the top, there's a navigation bar with 'Home', 'Learn' (which is selected), and 'Community'. Below this is a section titled 'Quick Start Videos' featuring five video thumbnails:

- Sumo Logic Overview
- Introduction to Search
- Browsing Dashboards
- Simplifying Searches with Search Templates
- Introduction to Metrics in Sumo

Below the videos is a section titled 'Using Sumo Logic Tutorial' with a numbered list of steps:

- 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

Next to it is another section titled 'Set Up Sumo Logic Tutorial' with a numbered list:

- 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

On the right side of the interface, there are several icons in a grid:

- Search icon: 'Search'
- Document icon: 'Docs'
- Bell icon: 'Notify Me'
- Question mark icon: 'Ask for Support'
- Checkmark icon: 'Skill Training'
- Community icon: '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

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

The screenshot shows the 'Learn' tab of the Sumo Logic interface. At the top, there's a navigation bar with 'Home', 'Learn' (which is highlighted), and 'Community'. Below the navigation, there's a section titled 'Quick Start Videos' featuring five video thumbnails:

- Sumo Logic Overview
- Introduction to Search
- Browsing Dashboards
- Simplifying Searches with Search Templates
- Introduction to Metrics in Sumo

Below the videos, there are two main sections:

- Using Sumo Logic Tutorial:** A list of 10 parts:
  - 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
  - Part 8: Set up a collector
  - Part 9: Add a source
  - Part 10: Install an app and view data
- Set Up Sumo Logic Tutorial:** A list of 6 parts:
  - 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
  - Part 6: Get Help

On the right side of the interface, there are several icons with labels: 'Search', 'Logs', 'Metrics', 'Dashboard', 'Alerts', 'Support', and 'Community'. A callout bubble points to the 'Community' icon.

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

The screenshot shows the 'Learn' tab of the Sumo Logic interface. At the top, there's a navigation bar with 'Home', 'Learn' (which is highlighted), and 'Community'. Below the navigation is a section titled 'Quick Start Videos' featuring five video thumbnails:

- Sumo Logic Overview
- Introduction to Search
- Browsing Dashboards
- Simplifying Searches with Search Templates
- Introduction to Metrics in Sumo

Below the videos is a section titled 'Using Sumo Logic Tutorial' with a numbered list of steps:

- 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

Next to it is another section titled 'Set Up Sumo Logic Tutorial' with its own numbered list:

- 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

On the right side of the main content area, there are several icons representing different features:

- Search icon: Direct Search
- Document icon: Docs
- Bell icon: Notify Me
- Question mark icon: Ask for Support (highlighted with a blue box and a callout)
- Checkmark icon: Self Training
- Person icon: 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

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

The screenshot shows the 'Learn' tab of the Sumo Logic interface. At the top, there's a navigation bar with 'Home', 'Learn' (which is highlighted in blue), and 'Certifications'. Below the navigation bar, there are sections for 'Quick Start Videos' and 'Using Sumo Logic Tutorial'.

- Quick Start Videos:** A grid of five video thumbnails:
  - Sumo Logic Overview
  - Introduction to Search
  - Building Dashboards
  - Simplifying Search with Search Templates
  - Introduction to Metrics in Sumo
- Using Sumo Logic Tutorial:** A list of 10 tutorial parts:
  - 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
  - Part 8: Set up a collector
  - Part 9: Add a source
  - Part 10: Try simple analytics
- Set Up Sumo Logic Tutorial:** A list of 5 setup steps:
  - 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
- Support & Training:** A grid of three icons:
  - Check Smart
  - Smart
  - Smart & Simple
- Community:** A grid of three icons:
  - Ask for Support
  - Self 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

The screenshot shows a landing page for the "Metrics Mastery" certification. At the top is a teal circular badge with the text "SUMO LOGIC CERTIFIED" around the top and "METRICS MASTERY" around the bottom, featuring a line graph icon in the center. Below the badge, the text "Metrics Mastery" is displayed. Further down, it says "ONLINE EXAM: 30 QUESTIONS | 60 MINUTES" and "PREP: USING SUMO LOGIC WEBINAR & HANDS ON LABS". A small note below states "This certification is valid for 6 months". A large pink arrow points to a blue button labeled "Take the Exam". Below the button is a "Learn More" link. The footer of the page includes the text "Sumo Logic Confidential".

s

# Empowering the people who power modern business

m

sumo logic

o