illuminate

Sumo Logic User Conference 2018

Become a Sumo Power User

Level 2 Certification

sumo logic

Become a Sumo Power User

1. Learn how to use a unified Logs and Metrics solution
2. Develop a Toolset for Basic and Advanced Analytics
3. Make Sumo work for you: monitor trends & critical events
4. Learn from Peer Use Cases
5. Next steps: where do you go from here?

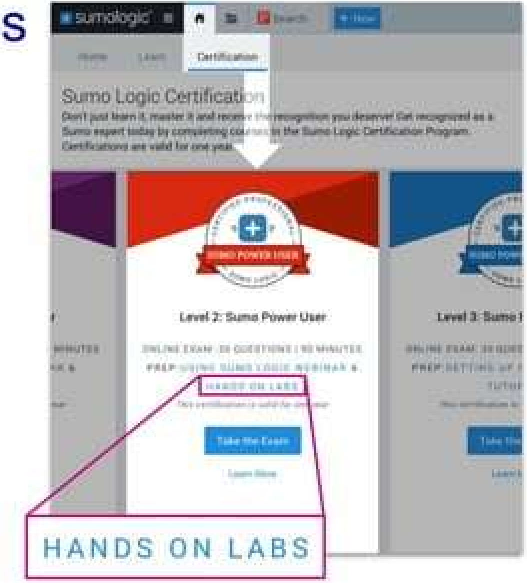
Tutorial: Hands-on Exercises

Training Environment:

1. service.sumologic.com
2. The username and password is on your handout

Level 2 Hands-on Labs:

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



Sumo Logic Certification

Don't just learn it, master it and receive the recognition you deserve! Get recognized as a Sumo expert today by completing courses in the Sumo Logic Certification Program. Certifications are valid for one year.

Level 2: Sumo Power User

ONLINE EXAM: 30 QUESTIONS | 90 MINUTES
PREP: USING SUMO LOGIC WEBINAR & HANDS ON LABS

This certification is valid for one year

Take the Exam

Learn More

Level 3: Sumo

HANDS ON LABS

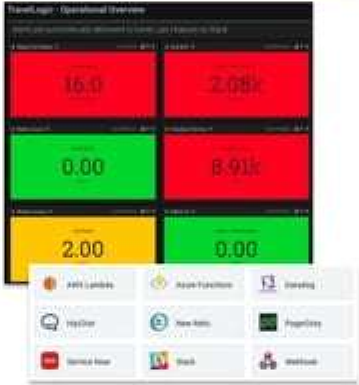
Reviewing the Basics

Demo & Dataflow

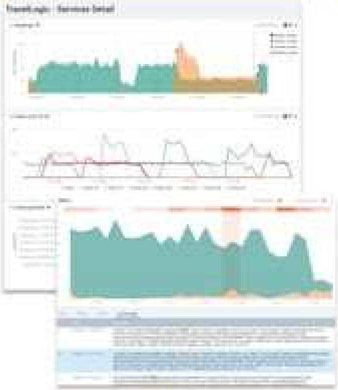
sumo logic

Demo: Monitor and Troubleshoot

ALERTS
notify of a critical event



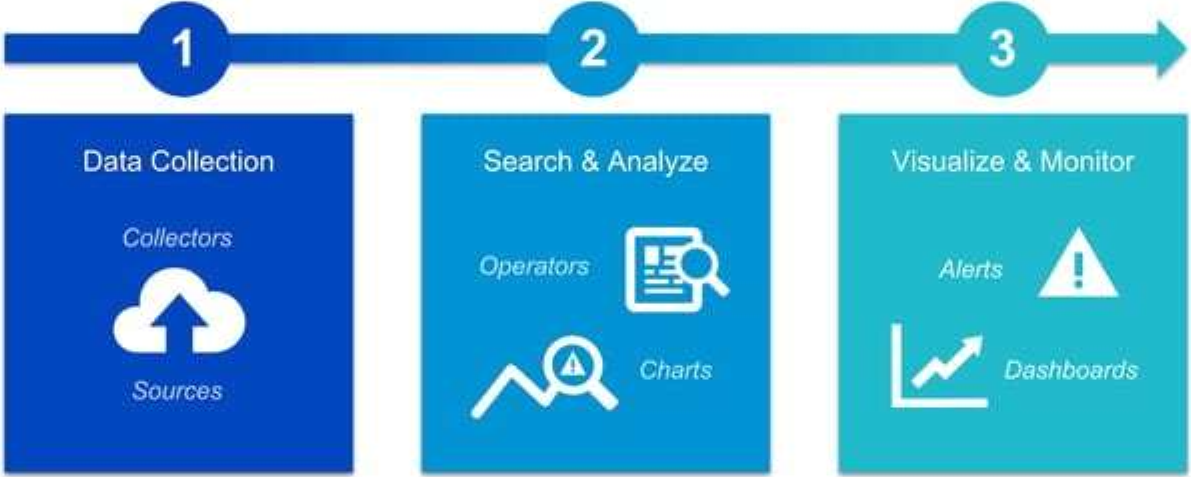
METRICS
to identify what's going on



LOGS
to identify why it's happening

sumo logic

Sumo Logic Data Flow



1

Data Collection

Collectors

Sources

2

Search & Analyze

Operators

Charts

3

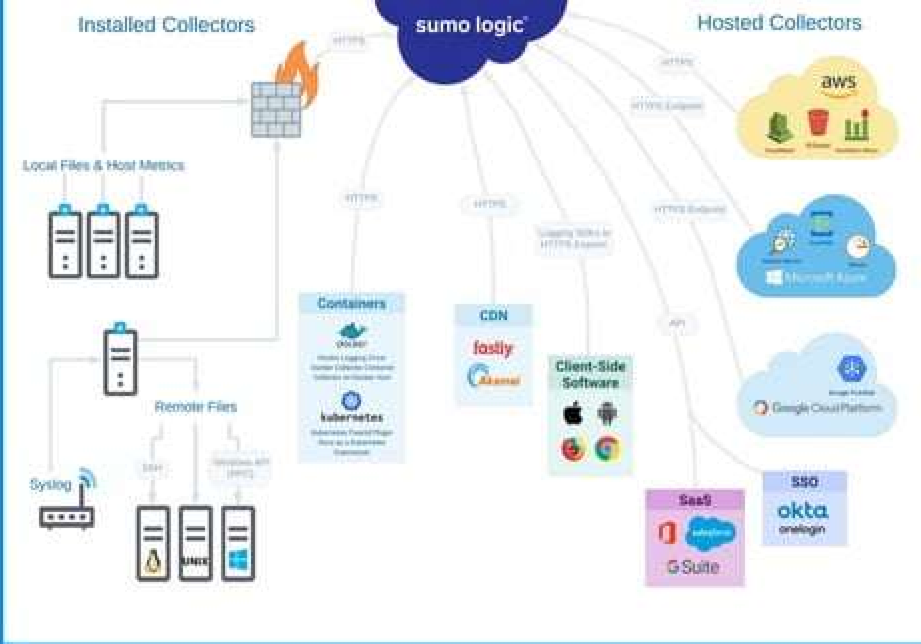
Visualize & Monitor

Alerts

Dashboards

Sending Data

- Cloud-to-cloud
- From host, send local data
- Use centralized infrastructure
- Learn more: Set Up Sumo Logic



Sending Data ⇨ Metadata

Metadata tags are associated with each log message that is collected.

Tag	Description
`_collector`	Name of the collector (defaults to hostname)
`_sourceHost`	Hostname of the server (defaults to hostname)
`_sourceName`	Name and Path of the log file
`_source`	Name of the source this data came through
`_sourceCategory`	**Can be freely configured. Main metadata tag**

Search and Parse

Filter and Provide Structure

sumo logic

Search and Parse

Search and **Filter** your data

Search and **Filter** your data

- _metadata
- Keywords
- Live Tail

Parse fields to provide structure to your data

- Query Parsing
- Implement your Field Extraction Rules

Level 2 Certification: Hands-on Labs

Using Sumo Logic

Labs 1-2: Search and Parse

- Search Basics: Metadata and Keywords
- Parsing Operators
- Grouping Results
- Field Extraction Rules

Labs 3: Parsing Options and FERs

- nodrop, parse field, parse multi

Simple Analytics

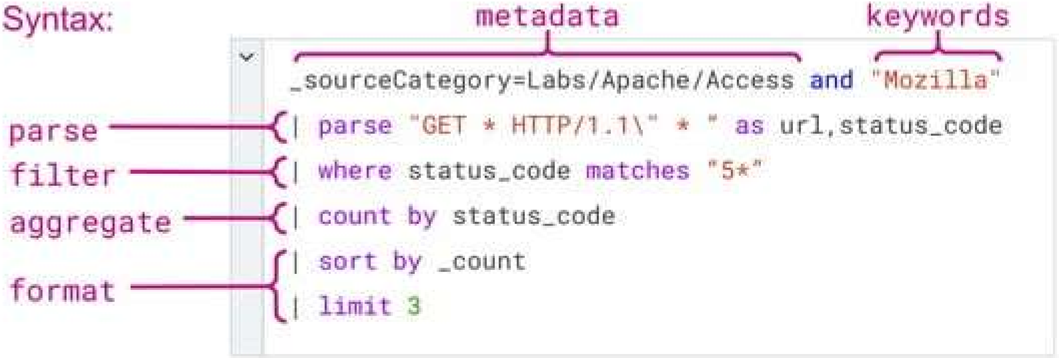
Conditional Logic, Filtering, Formatting Results

sumo logic

Review ⇨ Query Syntax

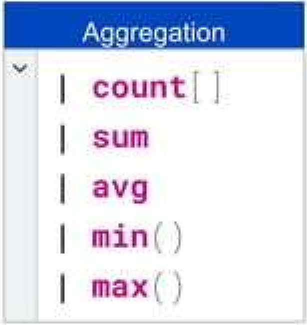
Keywords and operators, separated by pipes, that build on top of each other

Syntax:



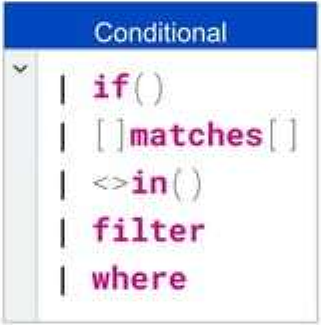
```
_sourceCategory=Labs/Apache/Access and "Mozilla"
| parse "GET * HTTP/1.1\" * " as url,status_code
| where status_code matches "5*"
| count by status_code
| sort by _count
| limit 3
```

Simple Analytics



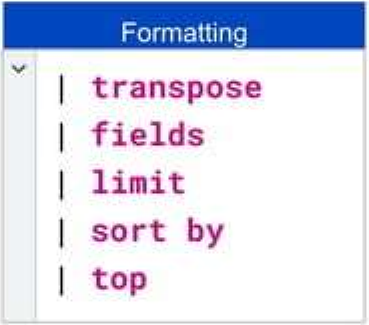
Aggregation

```
| count[]
| sum
| avg
| min()
| max()
```



Conditional

```
| if()
| []matches[]
| <>in()
| filter
| where
```



Formatting

```
| transpose
| fields
| limit
| sort by
| top
```

Level 2 Certification: Hands-on Labs

Using Sumo Logic

Labs 4-5: Conditional & Filtering Operations

- Common operators: if, matches, in, filter, where

Labs 6-7: Plotting on a Map, Formatting Results

- Geo lookup, transpose

Labs 8: Changes and Moving Averages

- Common operators: Diff, smooth

Advanced Analytics

Outliers, Trends, Needle in the Haystack

sumo logic

Advanced Analytics

Outlier

```
_sourceCategory=Labs/Apache/Access and status_code=404
| timeslice 1m
| count(status_code) as error_count by _timeslice
| outlier error_count
```

Predict

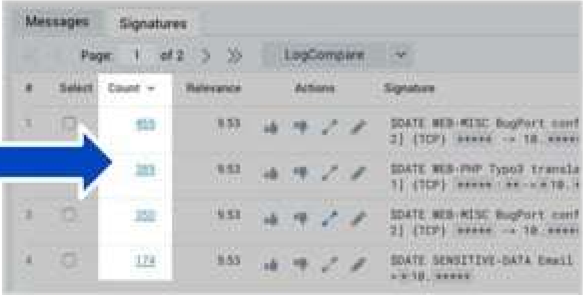
```
_sourceCategory=Labs/Apache/Access
| timeslice 5m
| count as requests by _timeslice
| predict requests by 5m forecast=12
```

Advanced Analytics

LogReduce

Find the "needle in the haystack" by identifying patterns.

```
_sourceCategory=Labs/security/snort
| logreduce
```



Messages | Signatures

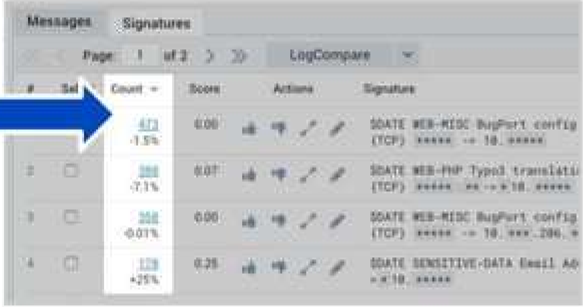
Page: 1 of 2 | LogCompare

#	Select	Count	Relevance	Actions	Signature
1	□	453	9.53		$DATE WEB-MISC BugPort conf 2] (TCP) ***** -> 10.*****
2	□	383	9.53		$DATE WEB-PHP Typo3 transla 1] (TCP) ***** :** -> *10.*
3	□	352	9.53		$DATE WEB-MISC BugPort conf 2] (TCP) ***** -> 10.*****
4	□	174	9.53		$DATE SENSITIVE-DATA Email -> *10.*****

LogCompare

Compare today's patterns with patterns in the past.

```
_sourceCategory=Labs/security/snort
| logcompare -24h
```



Messages | Signatures

Page: 1 of 2 | LogCompare

#	Sel	Count	Score	Actions	Signature
1	□	473 -1.5%	0.00		$DATE WEB-MISC BugPort config (TCP) ***** -> 10.*****
2	□	388 -7.1%	0.07		$DATE WEB-PHP Typo3 translati (TCP) ***** :** -> *10.*****
3	□	358 -0.01%	0.00		$DATE WEB-MISC BugPort config (TCP) ***** -> 10.***.206.*
4	□	178 +25%	0.25		$DATE SENSITIVE-DATA Email Ad -> *10.*****

Level 2 Certification: Hands-on Labs

Using Sumo Logic

Labs 9-12: Advanced Analytics

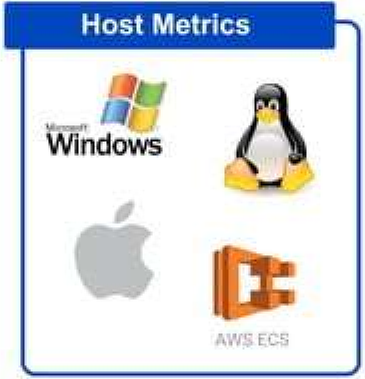
- Finding the needle in the haystack
- Comparing time periods
- Identifying Outliers
- Identifying Future trends
- Analyzing related logs

Analyzing your Metrics

Sources, Dashboards and Alerts

sumo logic

Ingesting Metrics - Sources

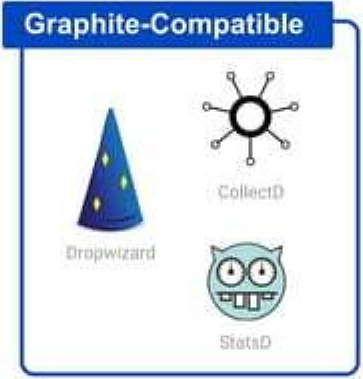


Host Metrics

✓ Learn More:
[Setting up Host Metrics]

AWS Metrics

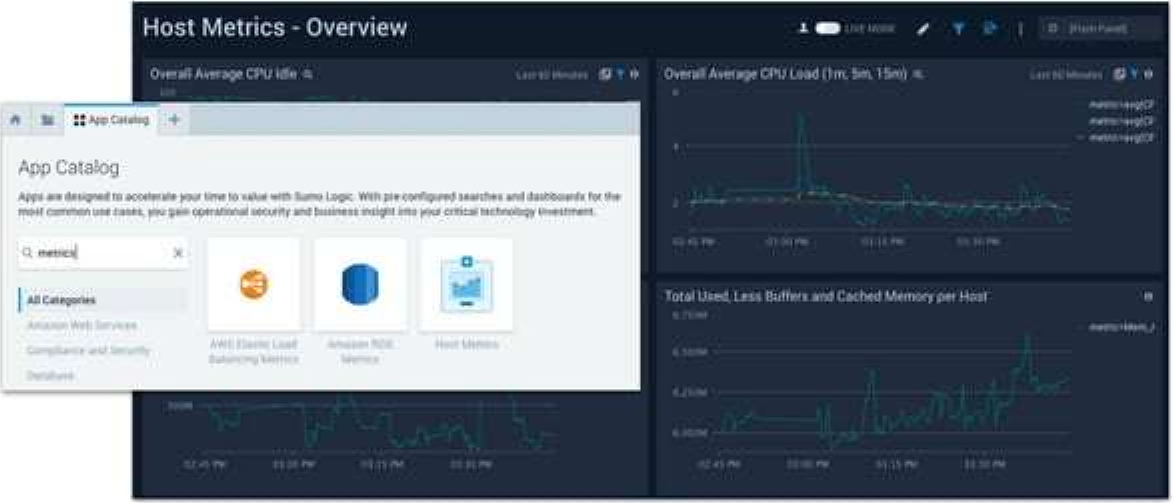
✓ Learn More:
[Setting up AWS Metrics]



Graphite-Compatible

✓ Learn More:
[Setting up Graphite Metrics]

Metrics Apps: Out-of-the-Box Content



Host Metrics - Overview

Overall Average CPU Idle

Overall Average CPU Load (1m, 5m, 15m)

Total Used, Less Buffers and Cached Memory per Host

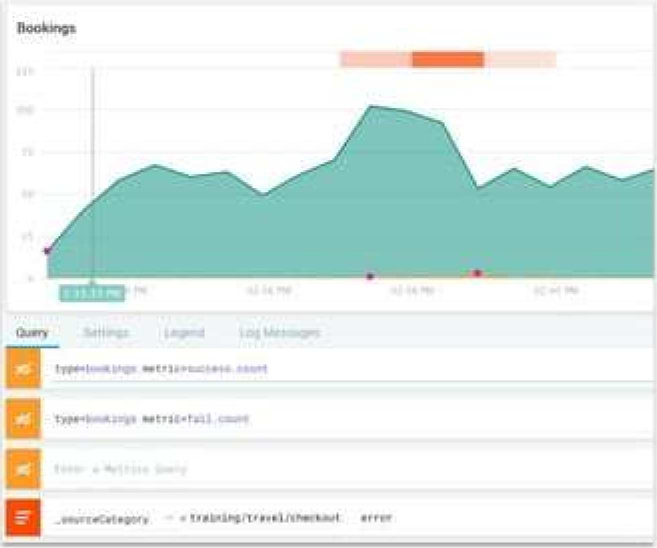
App Catalog

Apps are designed to accelerate your time to value with Sumo Logic. With pre-configured searches and dashboards for the most common use cases, you gain operational security and business insight into your critical technology investment.

Logs and Metrics - Overlay

Overlay helps you correlate metrics to the relevant logs.

- Metrics identify the **what**.
- Logs help identify **why**.



```
type=bookings metric=success.count
type=bookings metric=fail.count
Enter a Metrics Query
_sourceCategory = training/travel/checkout error
```

Level 2 Certification: Hands-on Labs

Using Sumo Logic

Labs 14-17: Analyzing your Metrics

- Basic Analytics
- Comparing KPIs at different time periods
- Identifying Rate of Change
- Correlating Logs and Metrics

Monitoring your Data

Dashboards and Alerts

sumo logic

Monitoring Your Data

Visualize your data through Dashboards

- Chart your Data
- Create Panels
- Share your Content!

Receive notification of your Critical Events

- Schedule Your Searches
- Use Webhook Connections to reach your audience
- Create Meaningful Alerts

Level 2 Certification: Hands-on Labs

Using Sumo Logic

Labs 18-22: Monitoring your Data

- Creating Dashboards
- Logs and Metrics Dashboards
- Creating Meaningful Alerts
- Installing Apps

Use Cases

“How To” Template to implement in your Environment

sumo logic

General Use Cases

How to Create and Alert on Ratios or Percentages

- Outlier

How to Compare and Alert on Historical Data

- Compare and Outlier

Detect Patterns and Changes Across Environments and Time

- LogCompare

Visualize Trends in Your Signatures

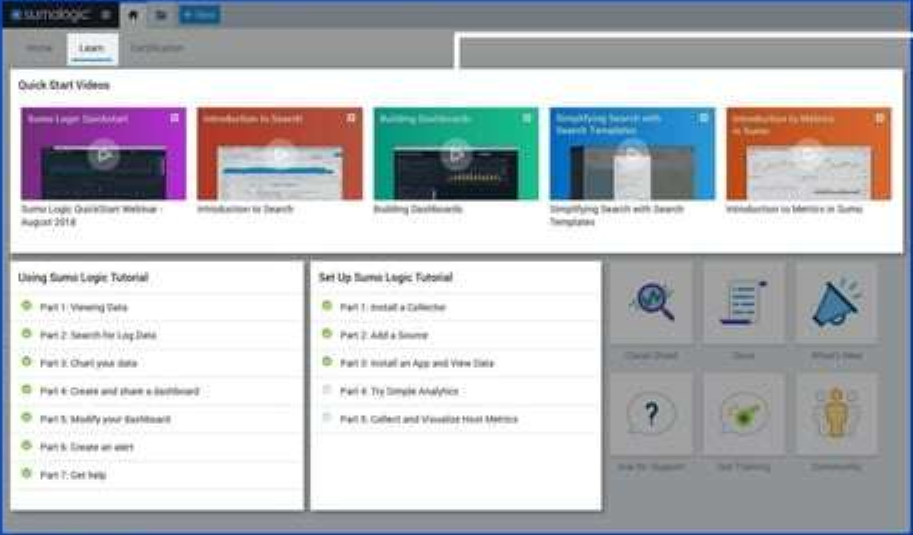
- LogReduce and Timeslice

Where do I go from here?

Training, Docs, Community, Support

sumo logic

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



Explore the tutorials

Quick Start Videos

Sumo Logic Quickstart	Introduction to Search	Building Dashboards	Simplifying Search with Search Templates	Introduction to Metrics in Sumo
Sumo Logic QuickStart Webinar - August 2018	Introduction to Search	Building Dashboards	Simplifying Search with Search Templates	Introduction to Metrics in Sumo

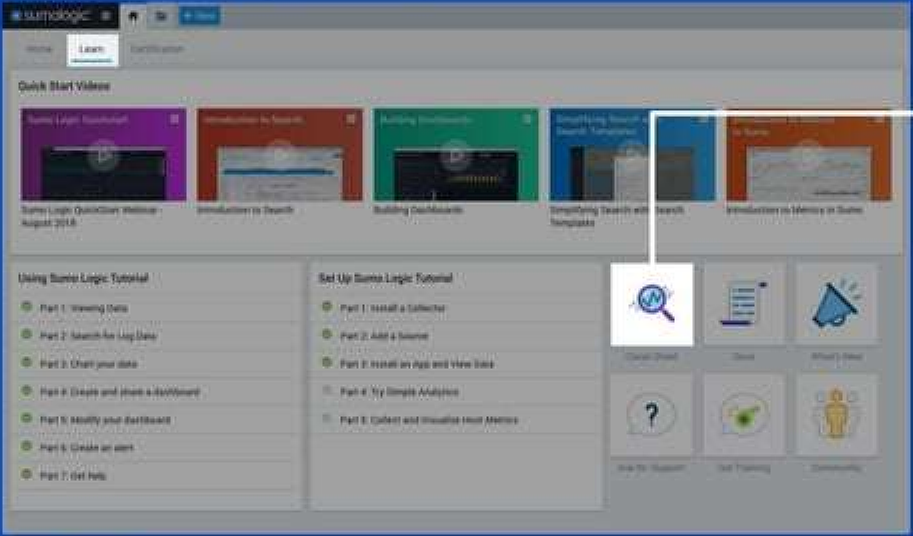
Using Sumo Logic Tutorial

- ● 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

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



Quick Start Videos

Sumo Logic QuickStart Webinar - August 2018

Introduction to Search

Building Dashboards

Simplifying Search with Search Template

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

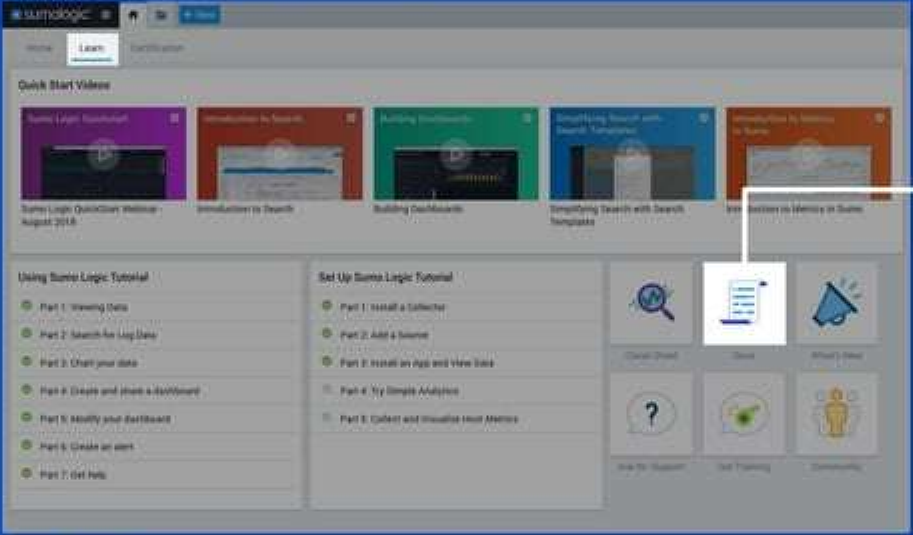
- Part 1: Install a Collector
- Part 2: Add a Source
- Part 3: Install an App and View Data
- Part 4: Try Simple Analytics
- Part 5: Collect and Visualize Host Metrics

Explore the tutorials

Access comprehensive lists of operators and more

sumo logic

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



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

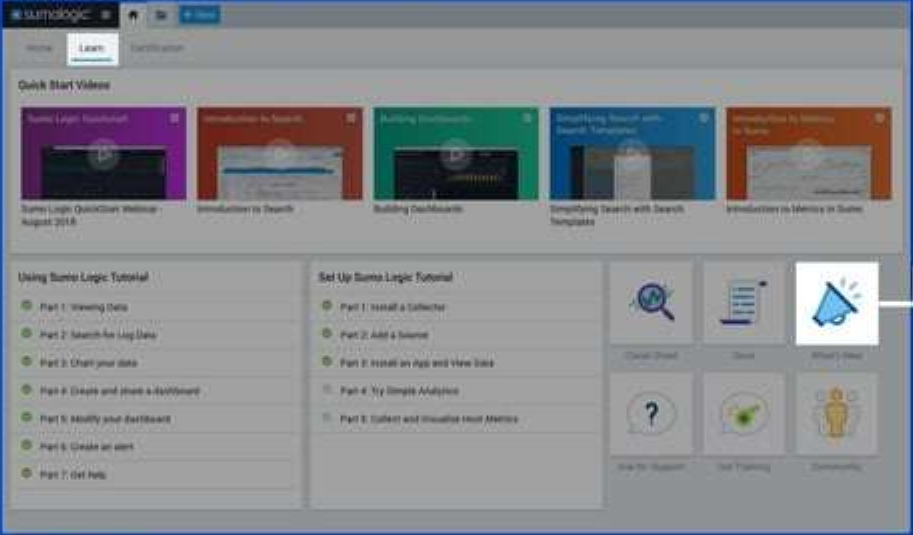
Explore the tutorials

Access comprehensive lists of operators and more

Every feature and tool covered in docs

sumo logic

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



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

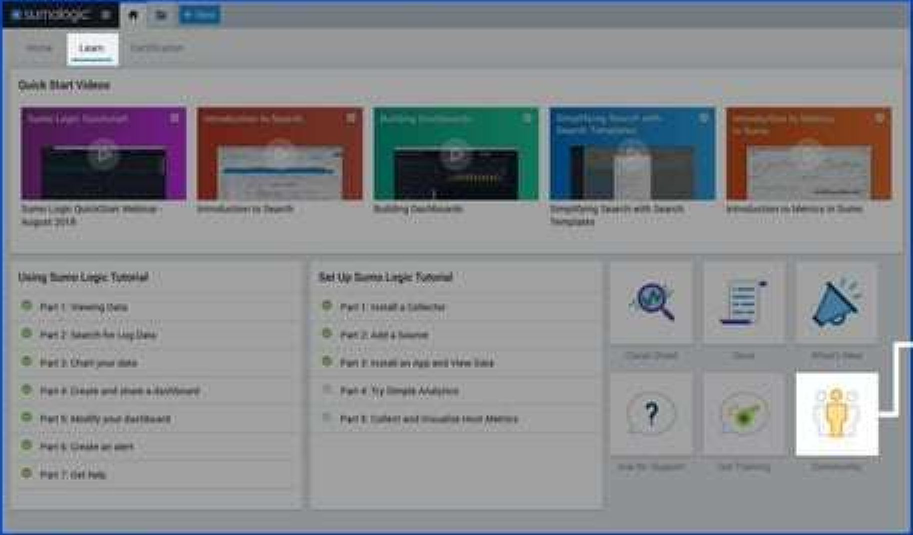
Explore the tutorials

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



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

Explore the tutorials

Access comprehensive lists of operators and more

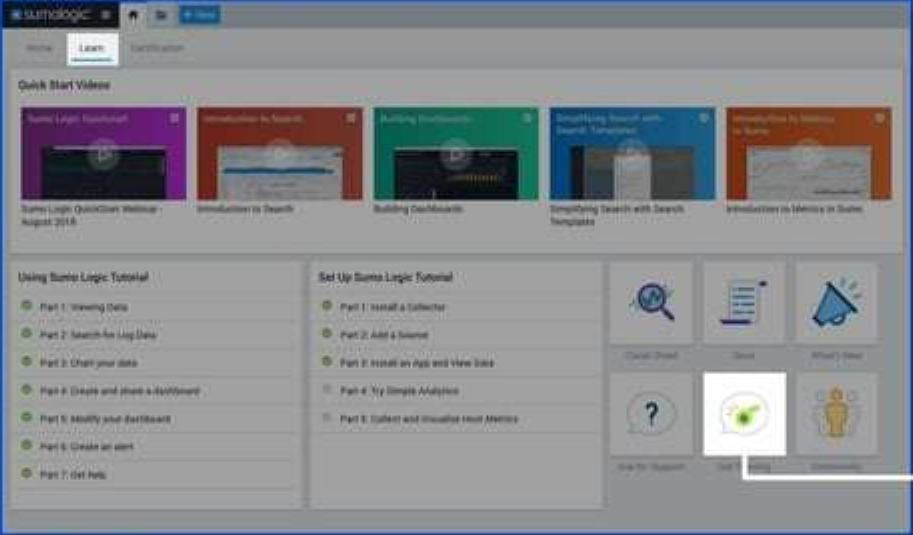
Every feature and tool covered in docs

Find out What's New

Find answers or post your questions to Community

sumo logic

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



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

Explore the tutorials

Access comprehensive lists of operators and more

Every feature and tool covered in docs

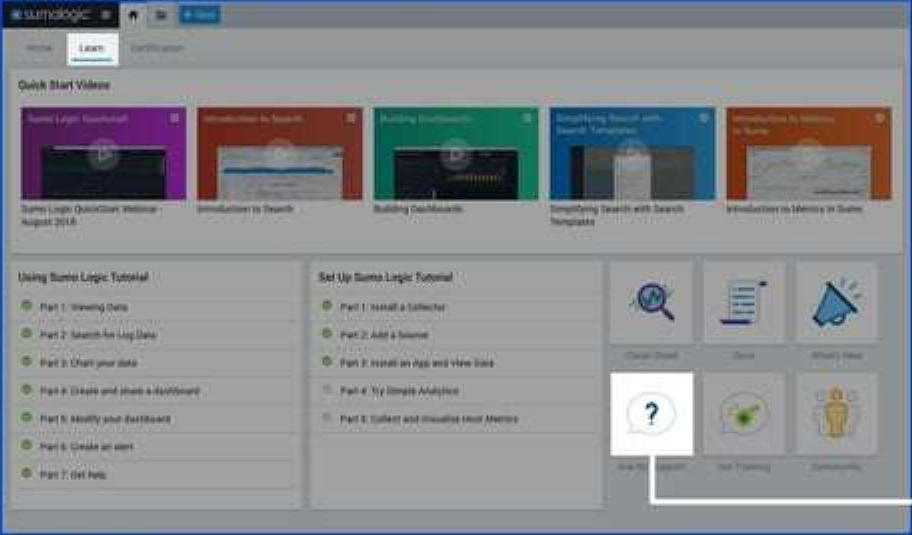
Find out What's New

Find answers or post your questions to Community

Attend/review training and get certified

sumo logic

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



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

Explore the tutorials

Access comprehensive lists of operators and more

Every feature and tool covered in docs

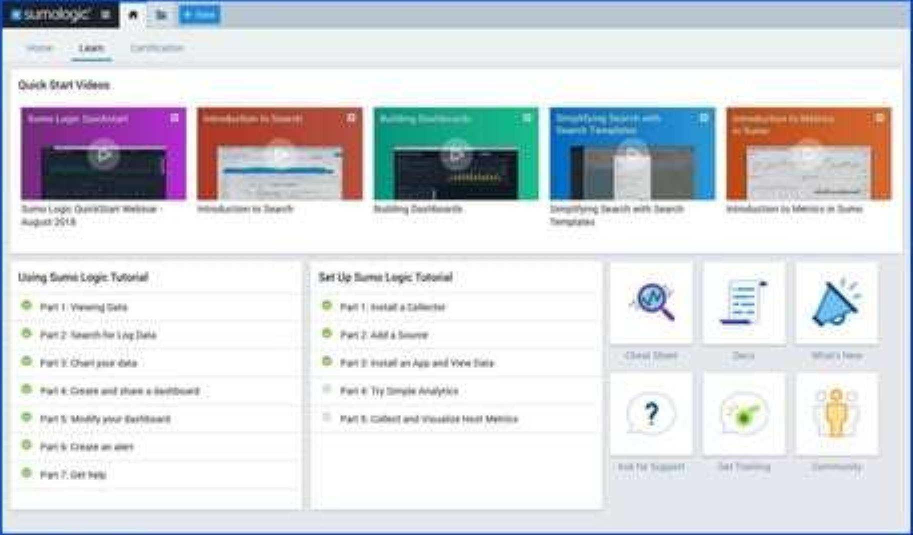
Find out What's New

Find answers or post your questions to Community

Attend/review training and get certified

Open a Support case

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



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

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

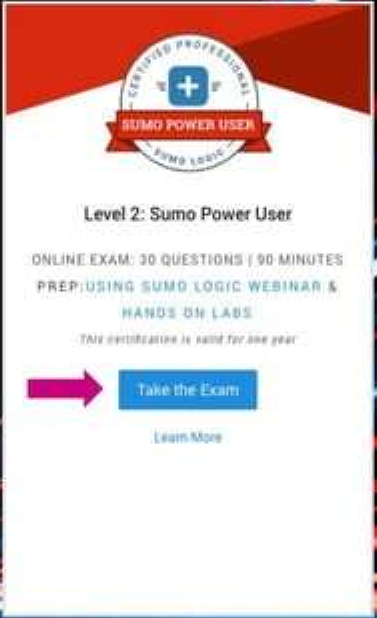
sumo logic

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



Level 2: Sumo Power User

ONLINE EXAM: 30 QUESTIONS | 90 MINUTES

PREP: USING SUMO LOGIC WEBINAR & HANDS ON LABS

This certification is valid for one year s u

Empowering the people who power modern business

m o

sumo logic