Become a

Sumo Search Master

Search Mastery Certification

sumo logic

Course Agenda

5 min.	Introduction & objectives
15 min.	**Hands-on Labs:** Search, parse, and FERs
15 min.	Conditional & filtering operations
10 min.	Plotting on a map, formatting results, and moving averages
15 min.	Trends, outliers, and comparisons
15 min.	Metrics and creating an alert
60 min.	Get certified

Tutorial: Hands-on Exercises

Training Environment:

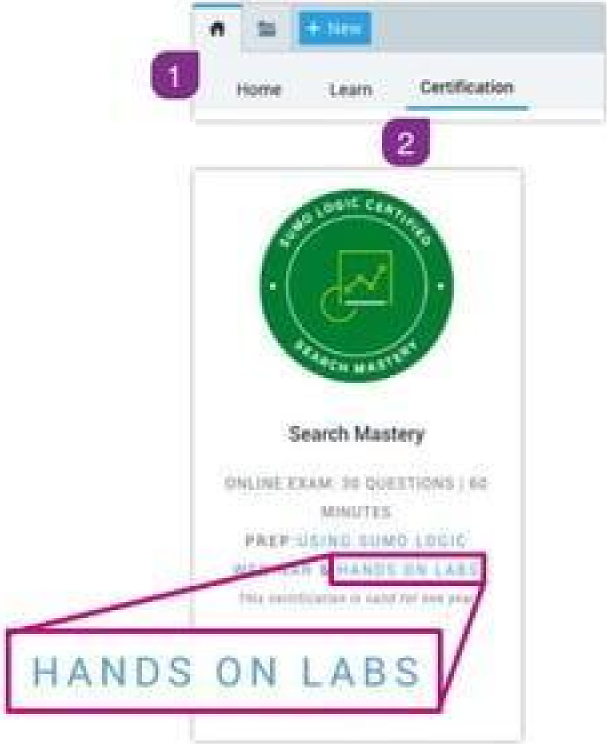
service.sumologic.com

username: training+labs@sumologic.com

password:

Level 2 Hands-on Labs:

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



Search Mastery

ONLINE EXAM: 30 QUESTIONS | 60 MINUTES

PREP: USING SUMO LOGIC WEBINAR & HANDS ON LABS

This certification is valid for one year

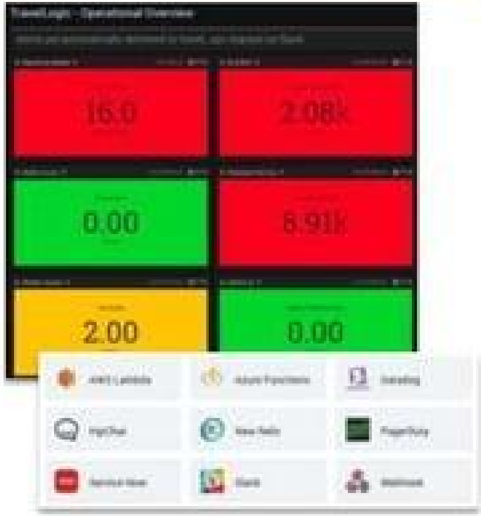
Reviewing the Basics

Demo & Dataflow

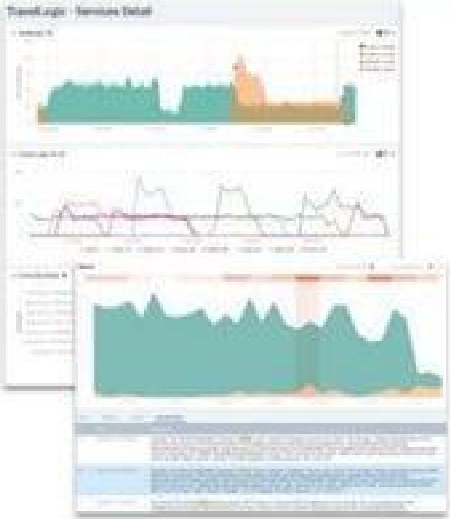
sumo logic

Demo: Monitor and Troubleshoot

ALERTS
notify of a critical event

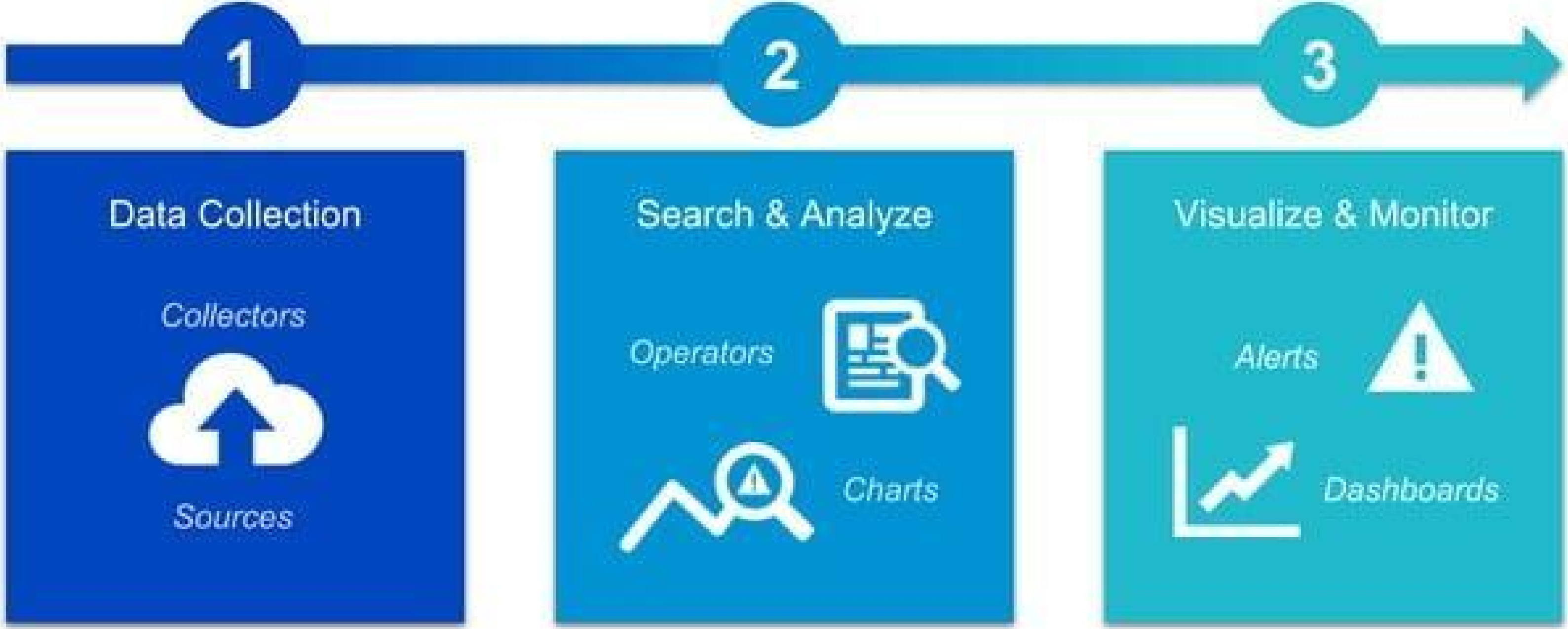


METRICS
to identify what's going on



LOGS
to identify why it's happening

Sumo Logic Data Flow



1

Data Collection

Collectors

Sources

2

Search & Analyze

Operators

Charts

3

Visualize & Monitor

Alerts

Dashboards

Search and Parse

Filter and Provide Structure

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

Search and **Filter** your data

Search and **Filter** your data

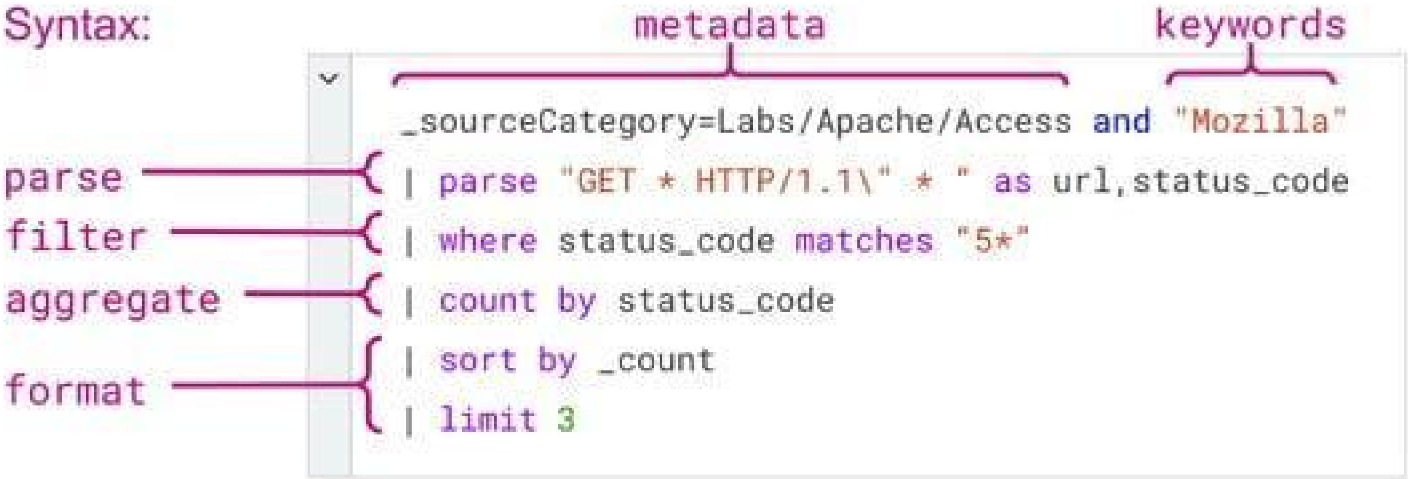
- _metadata
- Keywords
- Live Tail

Parse fields to provide structure to your data

- Query Parsing
- Implement your Field Extraction Rules

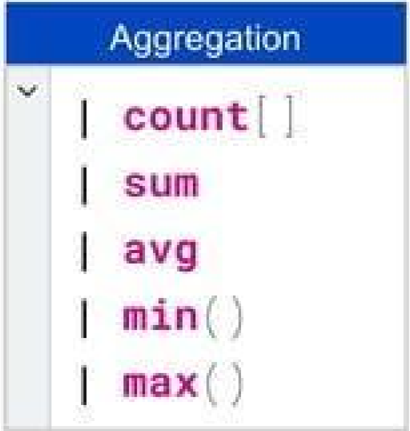
Data Analytics ⇨ Query Syntax

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



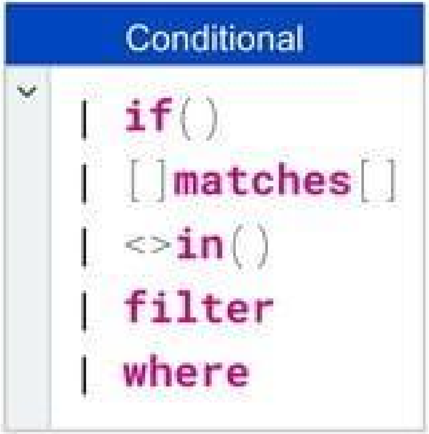
```
_sourceCategory=Labs/Apache/Access and "Mozilla"
| parse "GET * HTTP/1.1\" * " as url,status_code
| where status_code matches "5*"
| count by status_code
| sort by _count
| limit 3
```

Simple Analytics



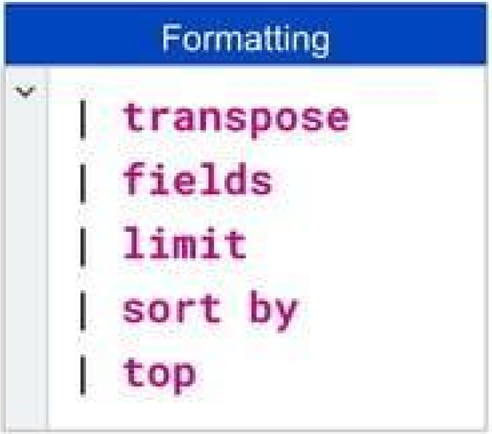
Aggregation

```
| 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 (5 ILT)

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

Lab 6: Plotting on a Map, Formatting Results

- Geo lookup, transpose

Lab 8: Changes and Moving Averages (ILT)

- 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

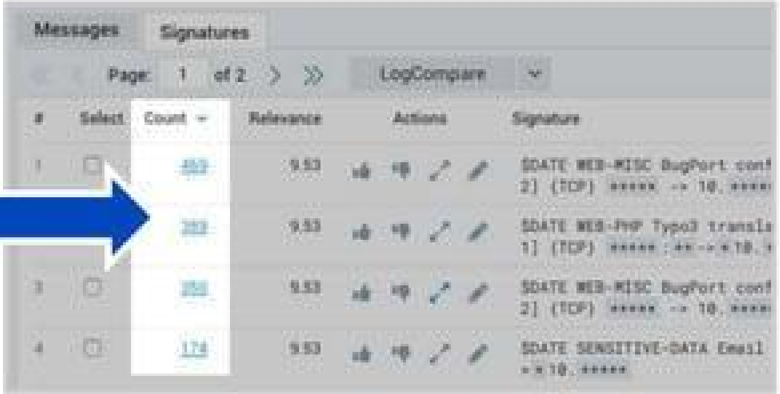
```
_sourceCategory=Labs/Apache/Access
| timeslice 5m
| count as requests by _timeslice
| predict requests by 5m forecast=12
```

Advanced Analytics

LogReduce

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

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

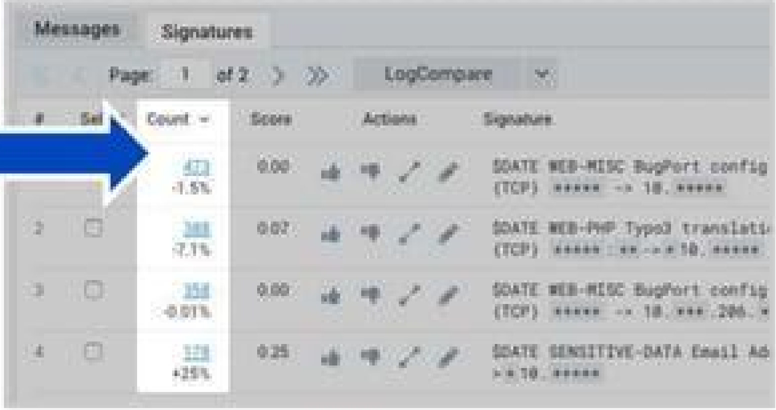


#	Select	Count	Relevance	Actions	Signature
1	☐	453	9.53		$DATE WEB-MISC BugPort conf 2] (TCP) ***** -> 10.****
		393	9.53		$DATE WEB-PHP Typo3 transla 1] (TCP) ***** :** -> *10.*
3	☐	350	9.53		$DATE WEB-MISC BugPort conf 2] (TCP) ***** -> 10.****
4	☐	174	9.53		$DATE SENSITIVE-DATA Email -> *10.*****

LogCompare

Compare today's patterns with patterns in the past.

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



#	Sel	Count	Score	Actions	Signature
		473 -1.5%	0.00		$DATE WEB-MISC BugPort config (TCP) ***** -> 10.*****
2	☐	388 -7.1%	0.02		$DATE WEB-PHP Typo3 translati (TCP) ***** :** -> *10.*****
3	☐	358 -0.01%	0.00		$DATE WEB-MISC BugPort config (TCP) ***** -> 10.***.206.*
4	☐	175 +25%	0.25		$DATE SENSITIVE-DATA Email Ad -> *10.*****

sumo logic

Level 2 Certification: Hands-on Labs

Using Sumo Logic

Labs 9-12: Advanced Analytics (Lab 12 ILT)

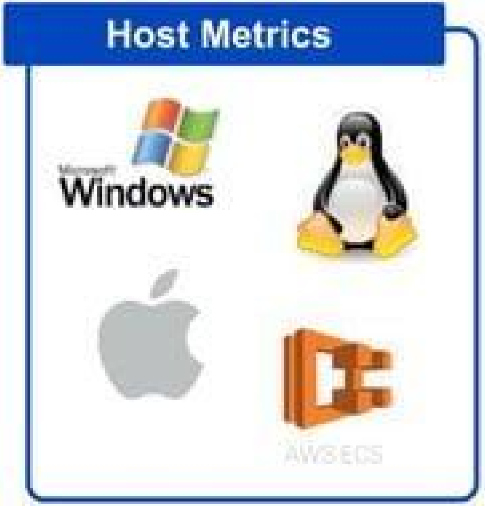
- Finding the needle in the haystack
- Comparing time periods
- Identifying Outliers
- Identifying Future trends
- Analyzing related logs

Analyzing your Metrics

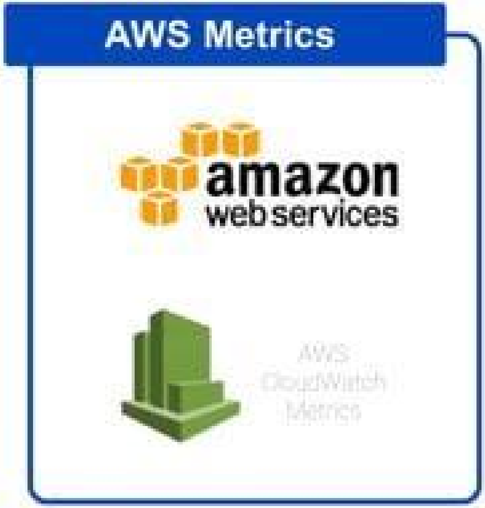
Sources, Dashboards and Alerts

sumo logic

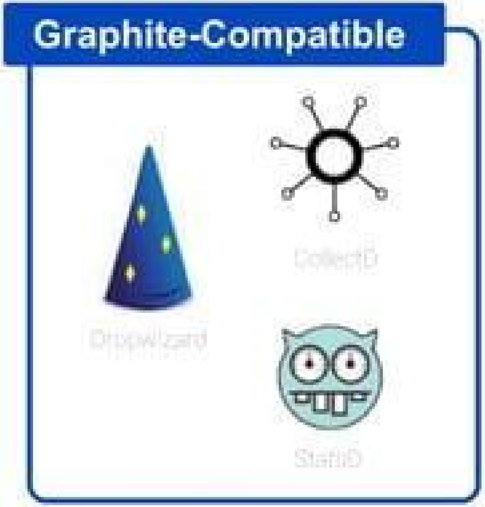
Ingesting Metrics



✓ **Learn More:**
Setting up Host Metrics

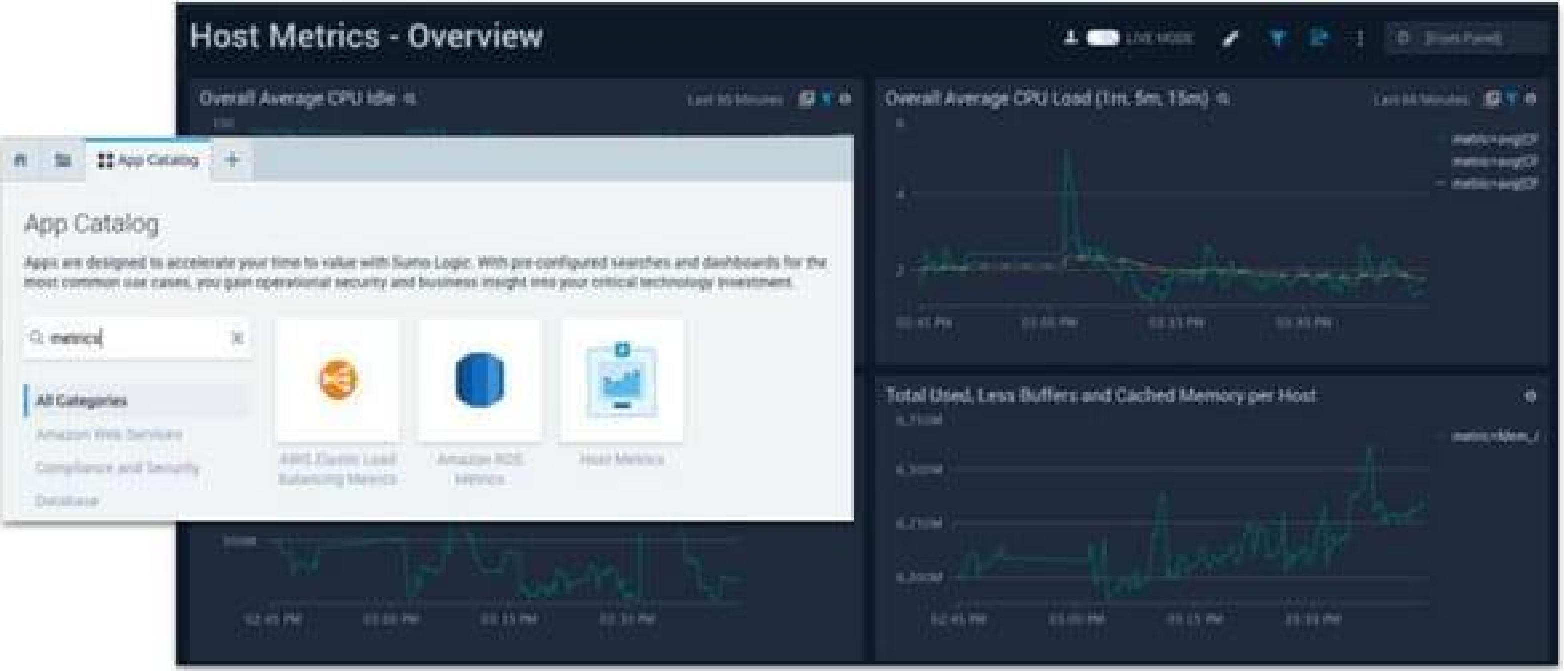


✓ **Learn More:**
Setting up AWS Metrics



✓ **Learn More:**
Setting up Graphite Metrics

Metrics Apps: Out-of-the-Box Content



App Catalog

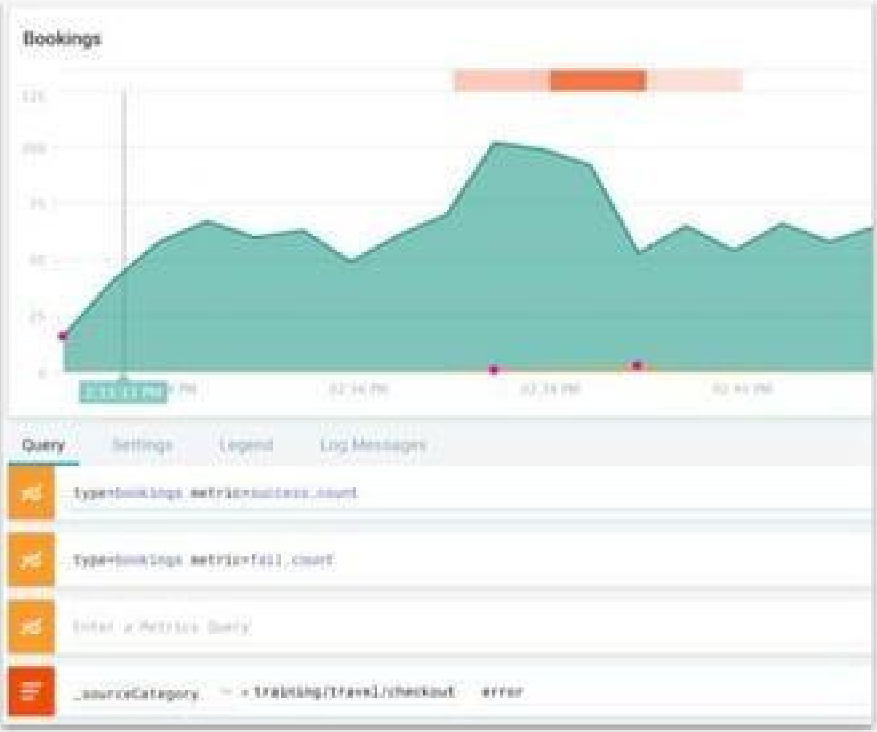
Apps are designed to accelerate your time to value with Sumo Logic. With pre-configured searches and dashboards for the most common use cases, you gain operational security and business insight into your critical technology investment.

sumo logic

Logs and Metrics - Overlay

Overlay helps you correlate metrics to the relevant logs.

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

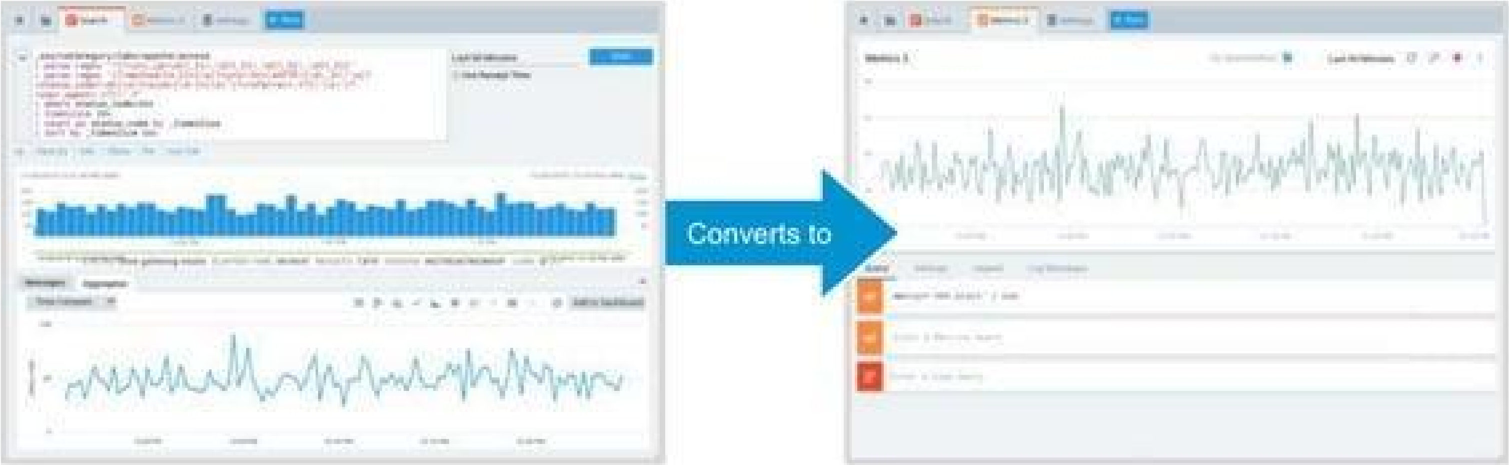


```
type=bookings metric=success.count
type=bookings metric=fail.count
Enter a Metrics Query
_sourceCategory = training/travel/checkout error
```

Logs-to-Metrics

What is it?

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



Logs-to-Metrics

Why do this?

1 Performance

2 Retention

3 Alerting

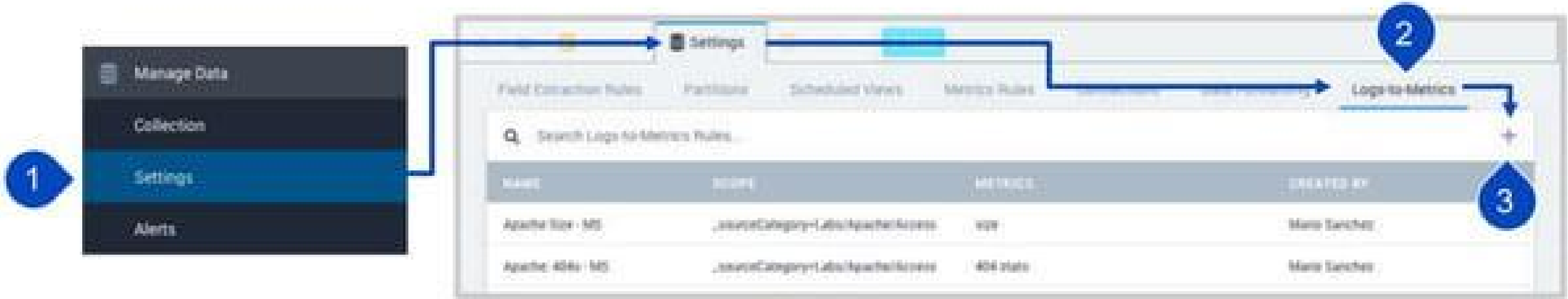
Analyzing time-series data is much faster than parsing and querying unstructured data.

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.

Logs-to-Metrics

How to create a metric from a log:



NAME	SCOPE	METRICS	CREATED BY
Apache Size - MS	_sourceCategory=Labs/Apache/Access	size	Mario Sanchez
Apache: 404s - MS	_sourceCategory=Labs/Apache/Access	404 stats	Mario Sanchez

sumo logic

Level 2 Certification: Hands-on Labs

Using Sumo Logic

Labs 13: Analyzing your Metrics (Lab 14 ILT)

- Basic Analytics
- Logs-to-Metrics

Note: *Lab 13 needs to run for -60m*

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

Lab 14: Relating your metrics and logs

Lab 15: Create meaningful alerts (ILT)

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

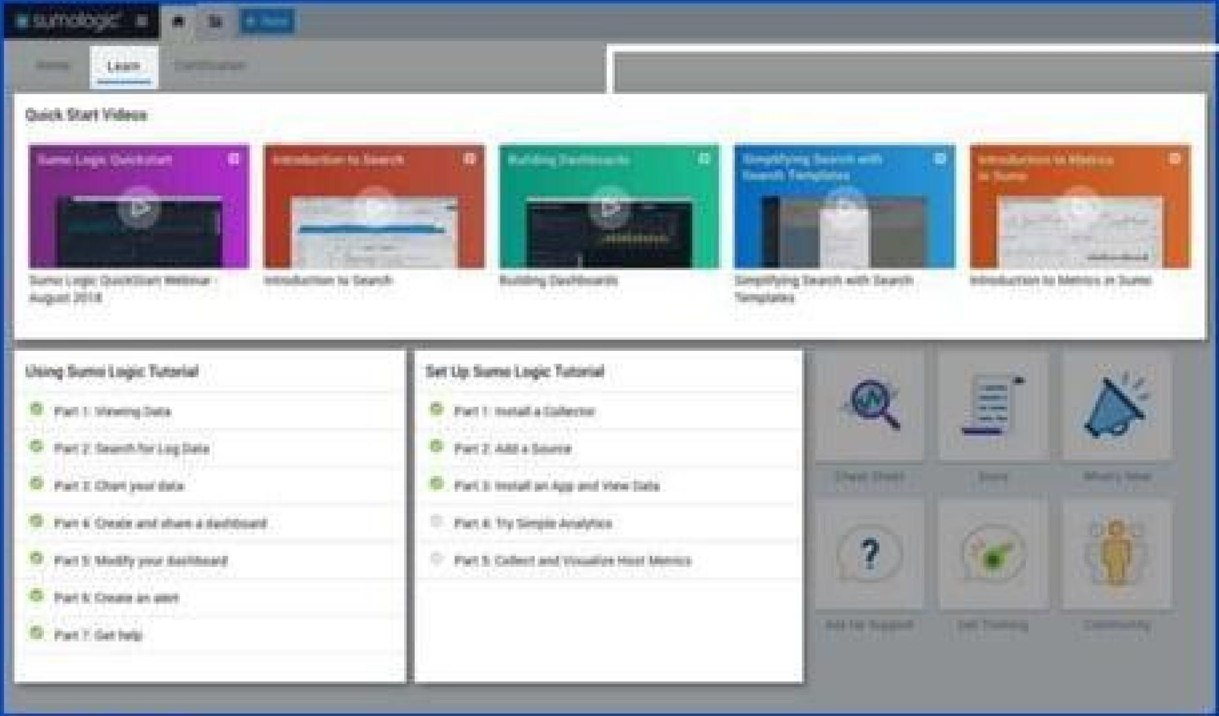
- LogReduce and Timeslice

Where do I go from here?

Training, Docs, Community, Support

sumo logic

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



Quick Start Videos

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

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

Using Sumo Logic Tutorial

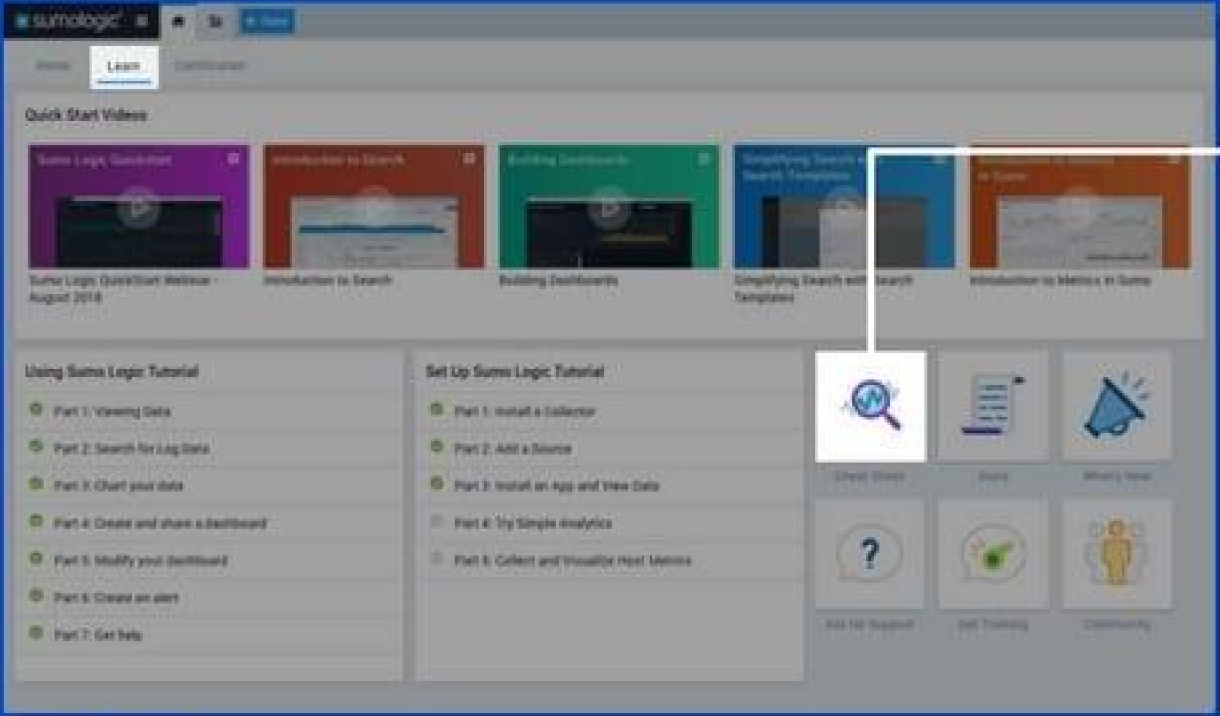
- Part 1: Viewing Data
- Part 2: Search for Log Data
- Part 3: Chart your data
- Part 4: Create and share a dashboard
- Part 5: Modify your dashboard
- Part 6: Create an alert
- Part 7: Get help

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

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

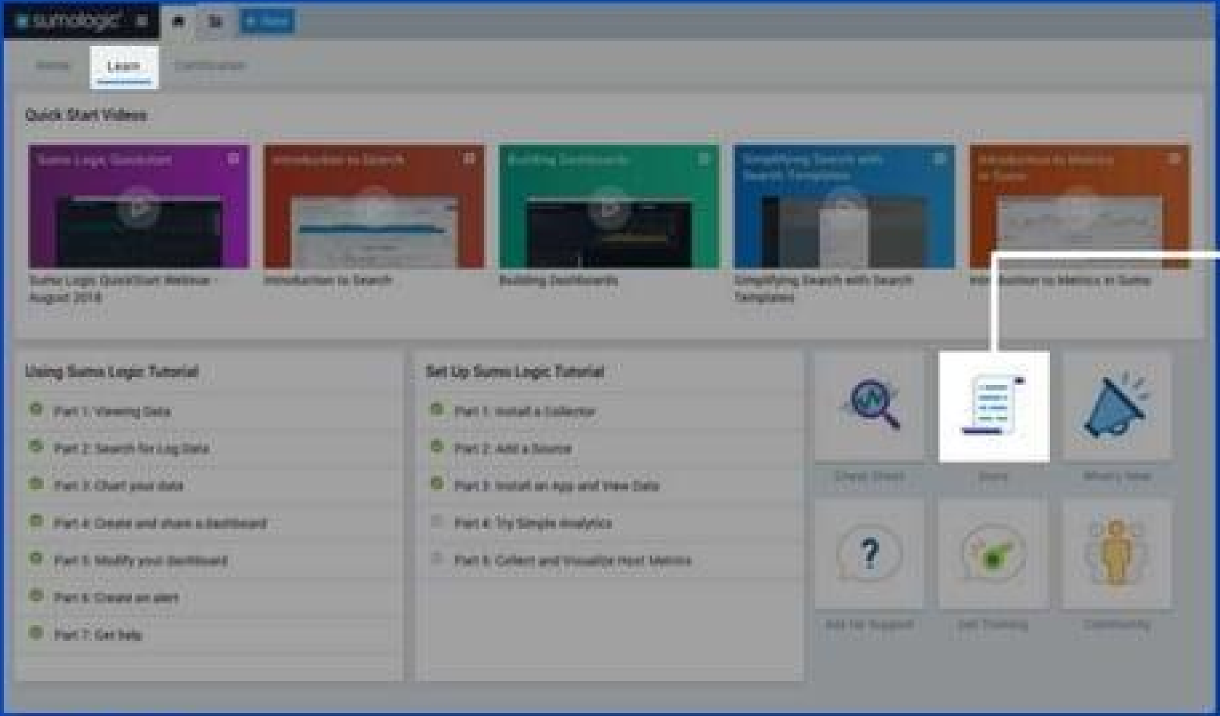
Set Up Sumo Logic Tutorial

- 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

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

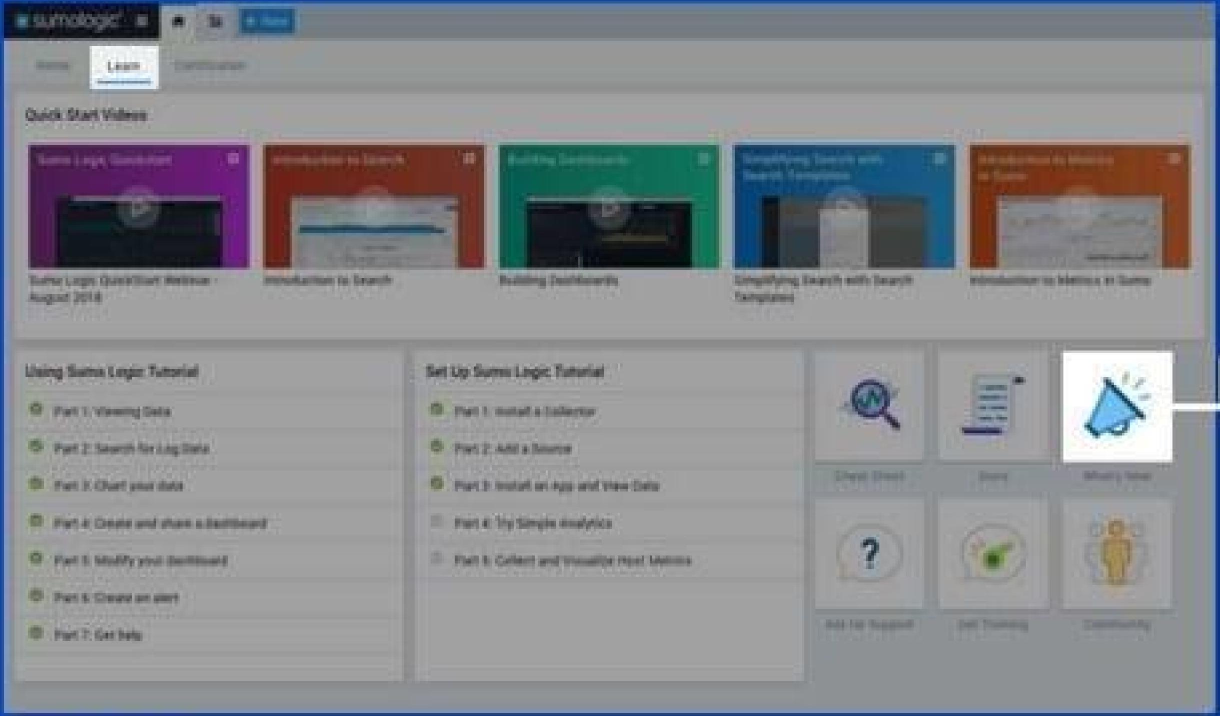
- Part 1: Install a Collector
- Part 2: Add a Source
- Part 3: Install an App and View Data
- Part 4: Try Simple Analytics
- Part 5: Collect and Visualize Host Metrics

Explore the tutorials

Access comprehensive lists of operators and more

Every feature and tool covered in docs

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

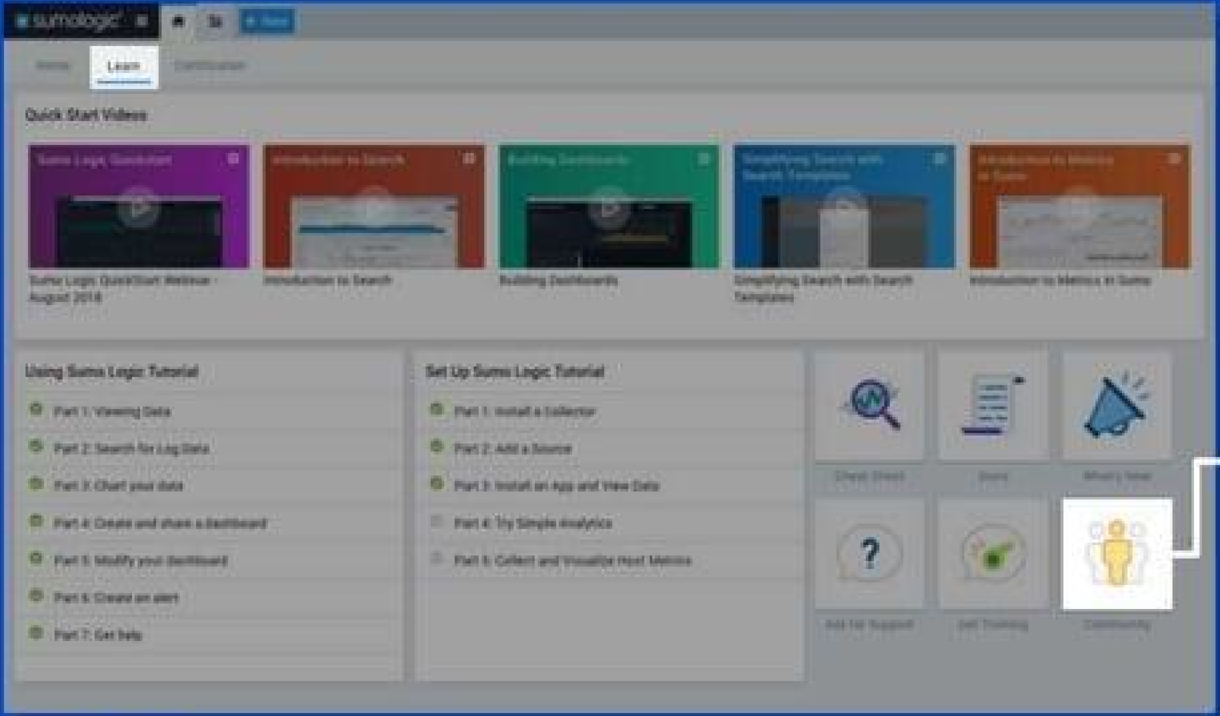
Access comprehensive lists of operators and more

Every feature and tool covered in docs

Find out What's New

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

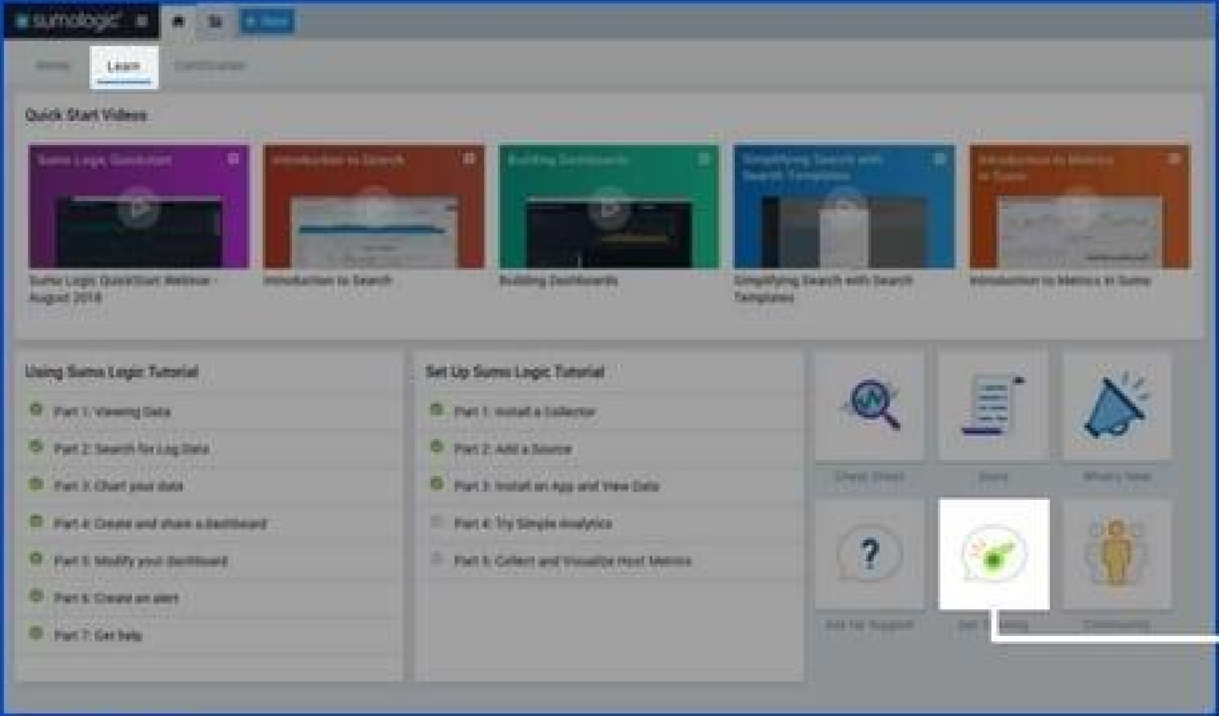
Access comprehensive lists of operators and more

Every feature and tool covered in docs

Find out What's New

Find answers or post your questions to Community

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

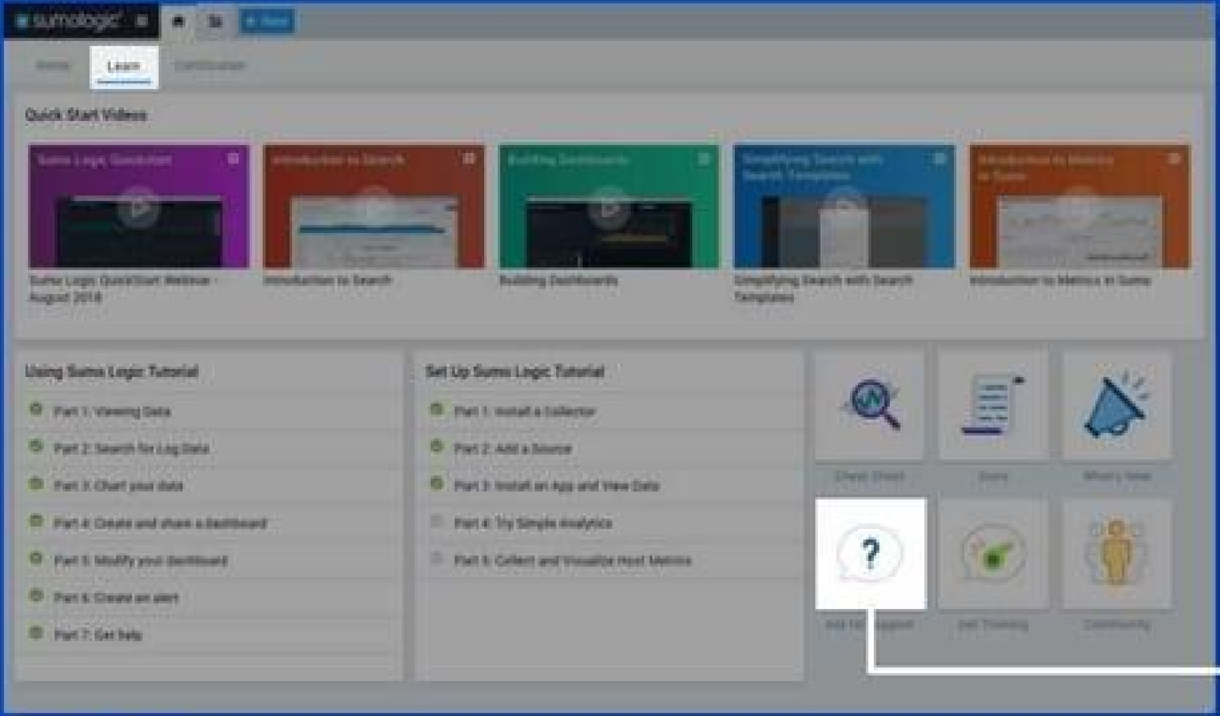
Find out What's New

Find answers or post your questions to Community

Attend/review training and get certified

sumo logic

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


sumologic
+ New
Home
Learn
Certification
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
Cheat Sheet
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

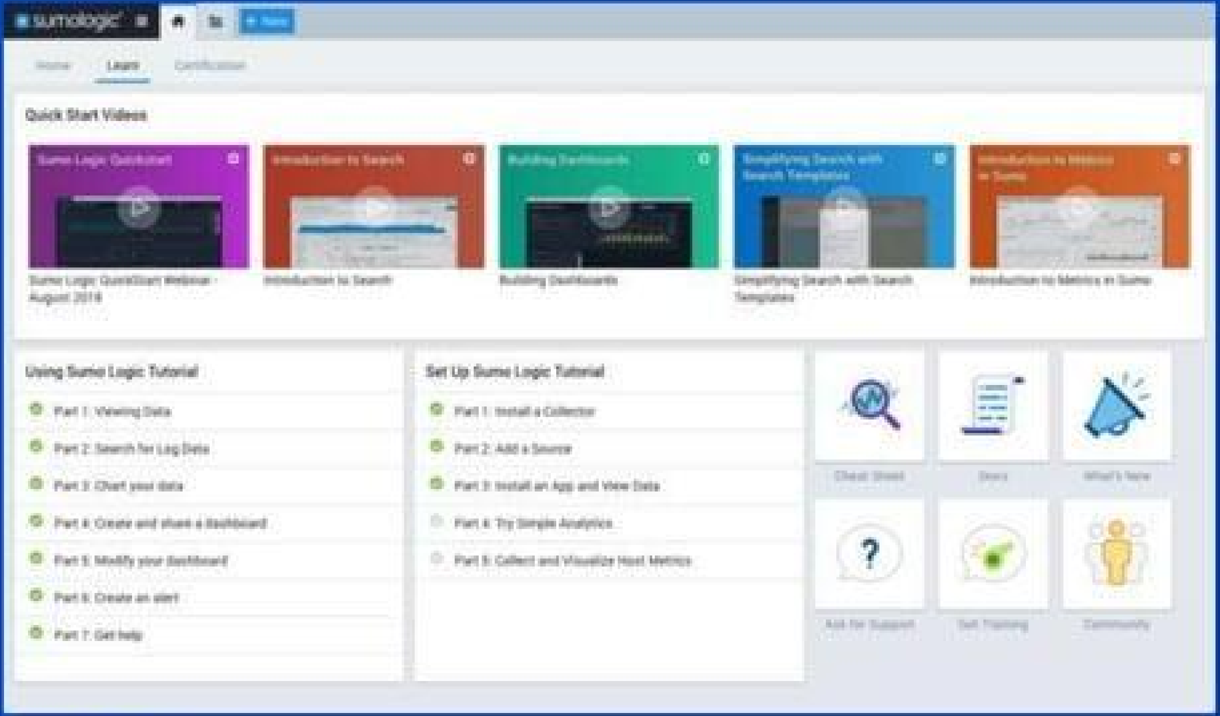
Find out What's New

Find answers or post your questions to Community

Attend/review training and get certified

Open a Support case

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

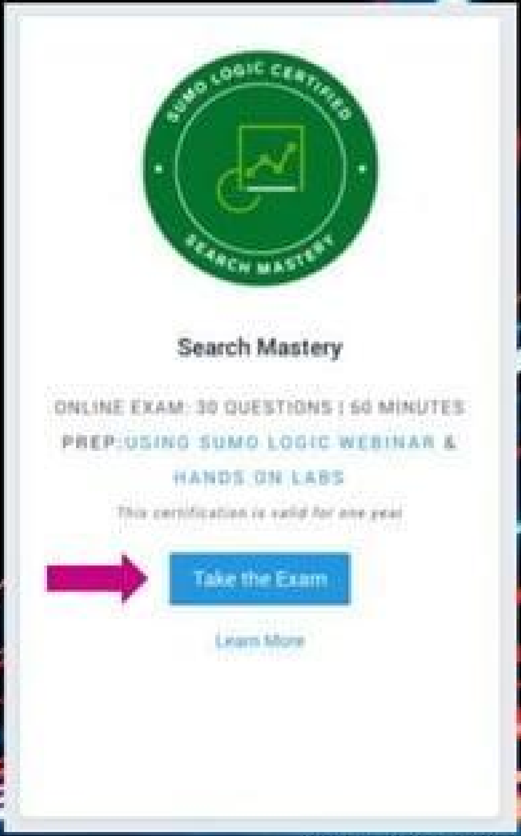
Open a Support case

Questions?

Take the exam

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
- sumologic.talentlms.com



Search Mastery

ONLINE EXAM: 30 QUESTIONS | 60 MINUTES

PREP: USING SUMO LOGIC WEBINAR & HANDS ON LABS

This certification is valid for one year

Sumo Logic Certification

- Make sure to log out of the training account you were using and sign in with your own account
- If you do not have a working login, go to sumologic.talentlms.com to sign up for an account

sumo logic

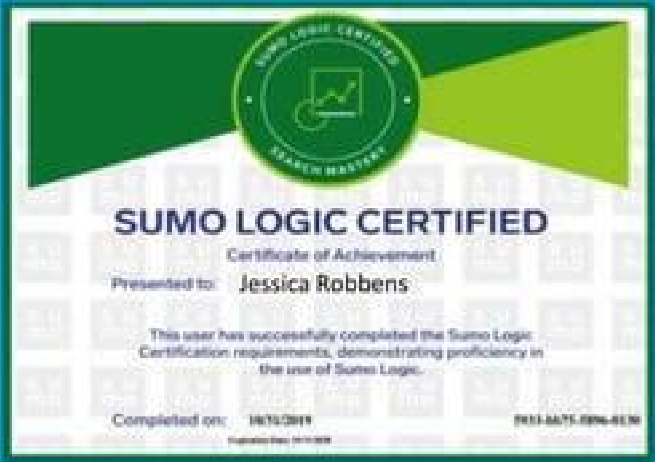
If you find your login is cycling back to the exam screen, do the following:

- Click on Help in the black left bar
- Click Community in the black left bar
- An email verification should be sent
- Once you verify, you should able to take the exam without any issues

sumo logic

For passing the exam, you will earn:

- SWAG
- A Certificate
- An invitation to our LinkedIn Group
- The respect of your peers
- Fame, Fortune and more...


SUMO LOGIC CERTIFIED
SEARCH MASTERY

SUMO LOGIC CERTIFIED

Certificate of Achievement

Presented to: Jessica Robbens

This user has successfully completed the Sumo Logic Certification requirements, demonstrating proficiency in the use of Sumo Logic.

Completed on: 10/31/2019 [illegible]

[illegible]

How did we do?

Please take our survey:

https://forms.gle/2KMtxPuD9cSYV8SJ6

sumo logic

s u

Empowering the people who power modern business

m o

sumo logic