



Become a
Sumo Search Master
Search Mastery Certification



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**



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



Sumo Logic Data Flow



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

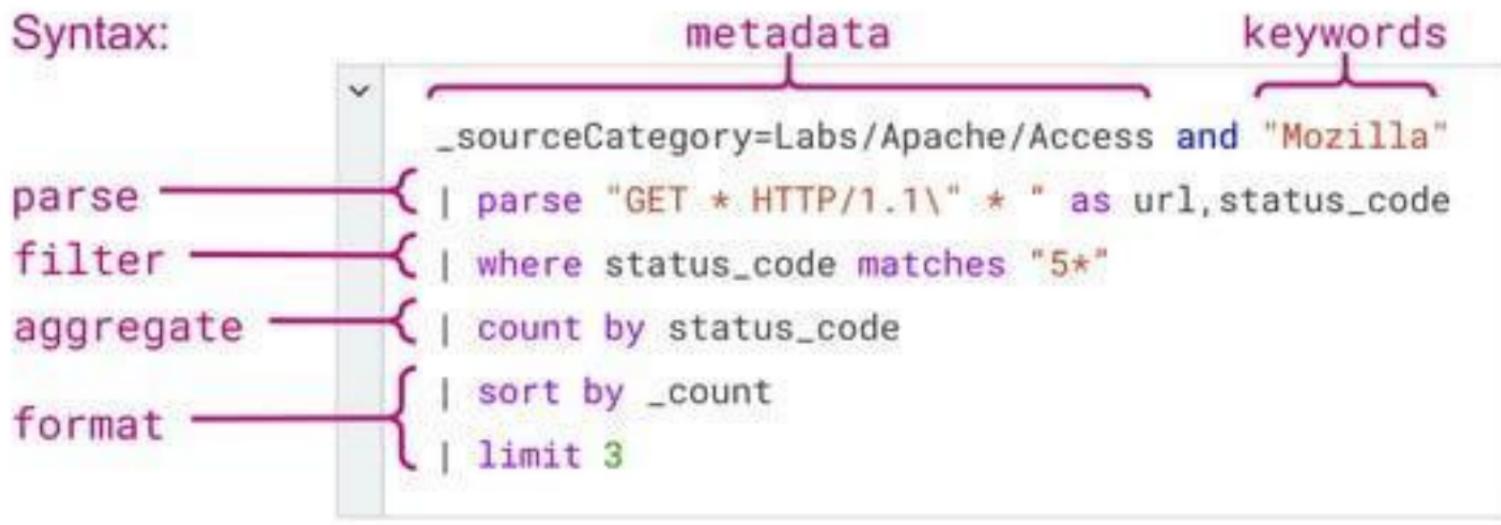


- Query Parsing
- Implement your Field Extraction Rules

Data Analytics ⇒ Query Syntax

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

Syntax:



Simple Analytics

Aggregation	Conditional	Formatting
count[] sum avg min() max()	if() []matches[] <>in() filter where	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



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
```

LogCompare

Compare today's patterns with patterns in the past.

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

#	Select	Count	Relevance	Actions	Signature
1	<input type="checkbox"/>	452	9.53	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	SDATE:WEB-MISC BugPort config (TCP) ***** --> 10.*****
2	<input type="checkbox"/>	302	9.53	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	SDATE:WEB-PHP Typo3 translate (TCP) ***** :--> 10.*****
3	<input type="checkbox"/>	252	9.53	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	SDATE:WEB-MISC BugPort config (TCP) ***** --> 10.*****
4	<input type="checkbox"/>	174	9.53	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	SDATE:SENSITIVE-DATA Email Ad> 10.*****

#	Select	Count	Score	Actions	Signature
1	<input type="checkbox"/>	452	0.00	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	SDATE:WEB-MISC BugPort config (TCP) ***** --> 10.*****
2	<input type="checkbox"/>	302	-1.5%	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	SDATE:WEB-PHP Typo3 translate (TCP) ***** :--> 10.*****
3	<input type="checkbox"/>	252	-7.1%	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	SDATE:WEB-MISC BugPort config (TCP) ***** --> 10.***.200.*
4	<input type="checkbox"/>	174	+25%	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	SDATE:SENSITIVE-DATA Email Ad> 10.*****

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



Ingesting Metrics

Host Metrics



AWS CloudWatch Metrics

AWS Metrics

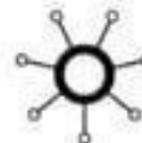


AWS
CloudWatch
Metrics

Graphite-Compatible



Dropwizard



CollectD



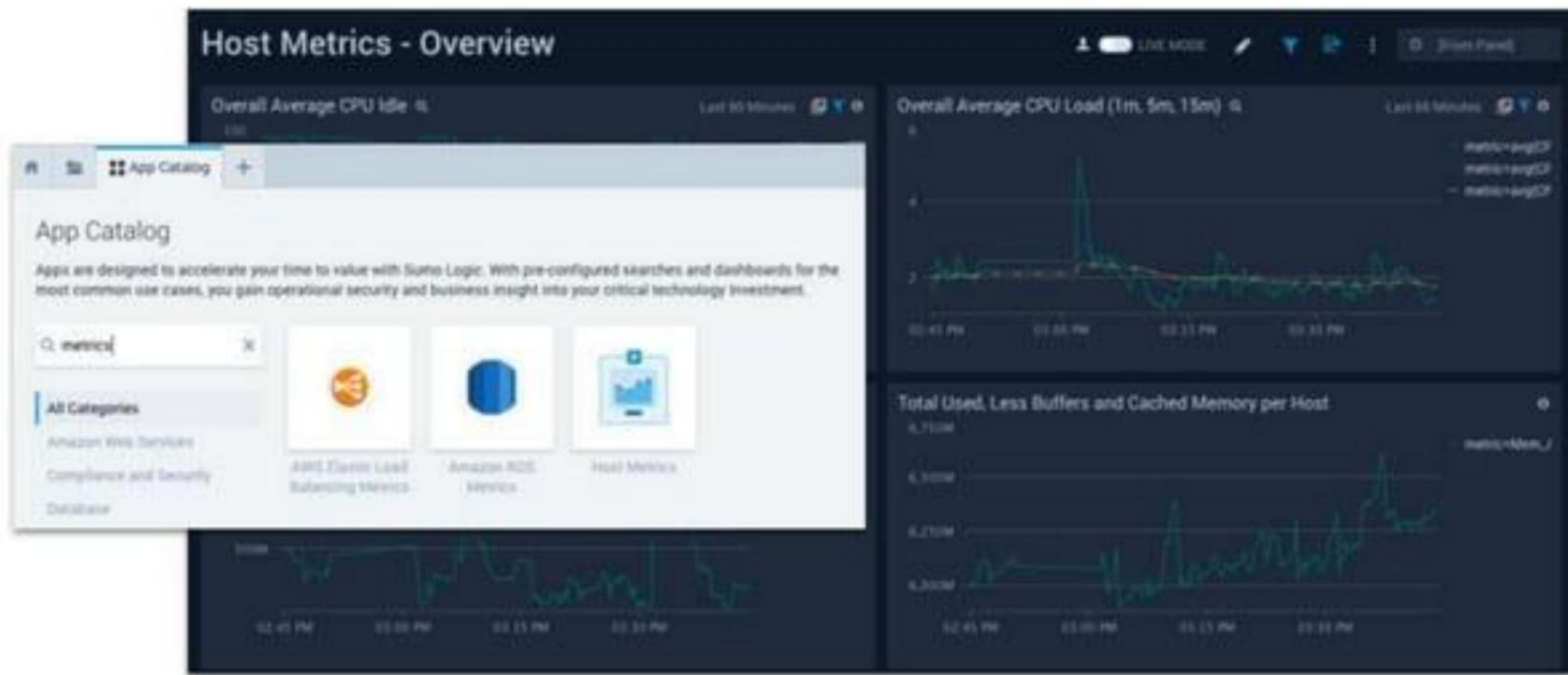
StatSD

✓ Learn More:
[Setting up Host Metrics](#)

✓ Learn More:
[Setting up AWS Metrics](#)

✓ Learn More:
[Setting up Graphite Metrics](#)

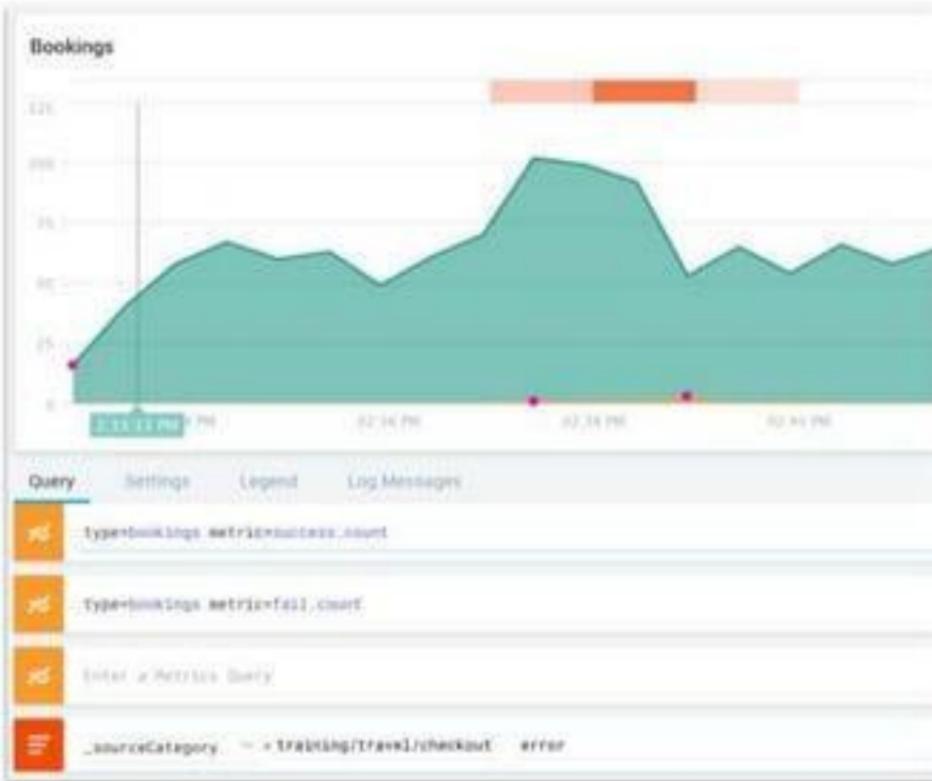
Metrics Apps: Out-of-the-Box Content



Logs and Metrics - Overlay

Overlay helps you correlate metrics to the relevant logs.

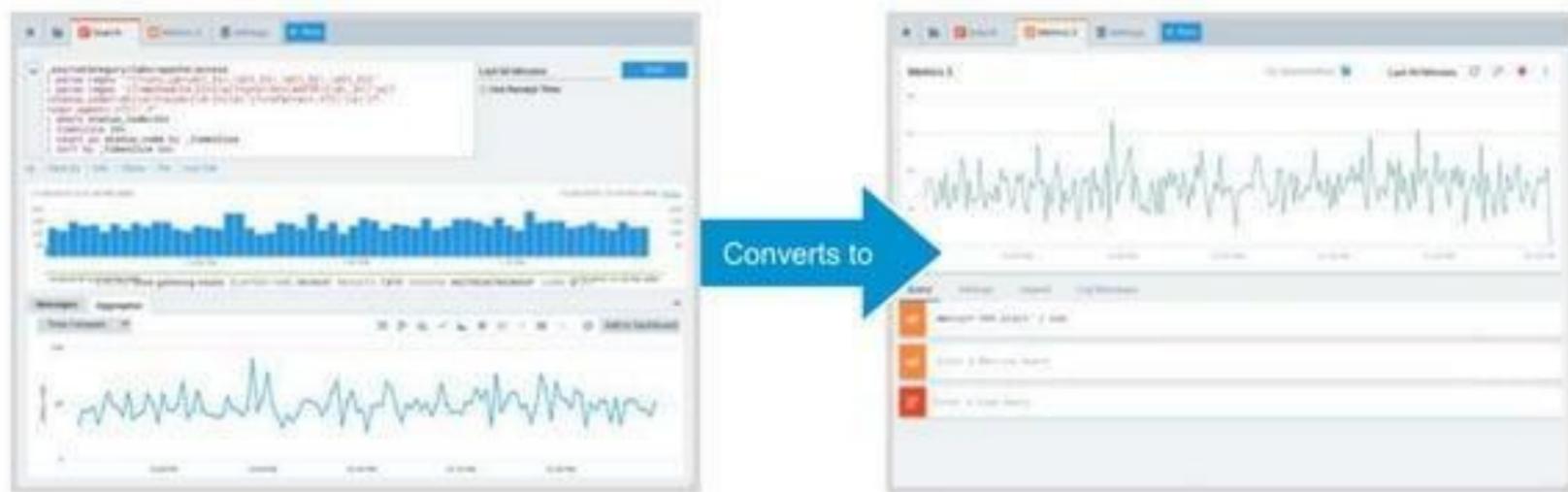
- Metrics identify the **what**.
- Logs help identify **why**.



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



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

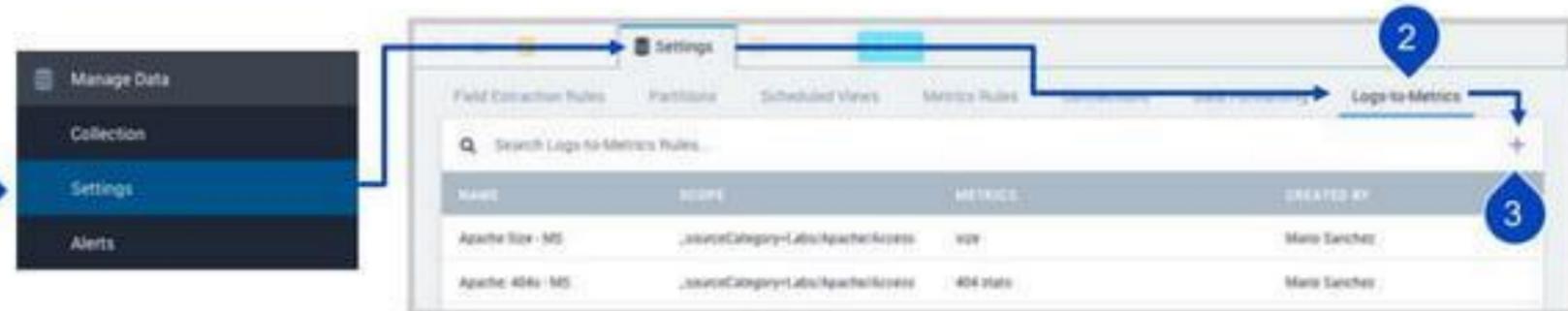
Alerting



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

Logs-to-Metrics

How to create a metric from a log:



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



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



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



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, there are two main sections of tutorials:

- 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 representing different support and community resources:

- 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 is a section titled 'Quick Start Videos' featuring six video thumbnails:

- Sumo Logic Quickstart Webinar - August 2018
- Introduction to Search
- Building Dashboards
- Simplifying Searches with Search Templates
- Search
- 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 main content area, there are several icons with labels:

- Search (with a magnifying glass icon)
- Logs
- Metrics
- Dashboard
- Help
- Self Training
- Community

Below these icons are three buttons: 'Add to Support', 'Self Training', and 'Community'.

Explore the tutorials

Access comprehensive
lists of operators and
more

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 Searches with Search Templates
- From Summary 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
 - 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

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

- Search icon: Direct Search
- Document icon: Docs
- Bell icon: Notify
- Question mark icon: Help
- Checkmark icon: Self Training
- User icon: 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 this is a section titled 'Quick Start Videos' featuring five video thumbnails:

- Sumo Logic Overview - August 2018
- 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:

- Search icon with a magnifying glass
- Document icon with a pencil
- Speaker icon with sound waves
- Question mark icon
- Checkmark icon with a green checkmark
- Person icon with a yellow outline

Below these icons are links: 'Create New', 'Edit', 'Delete', 'Add to Support', 'Self Training', and '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 'Learn' highlighted. Below it, a section titled 'Quick Start Videos' displays five video thumbnails. The first video is 'Sumo Logic Overview' from August 2018. The second is 'Introduction to Search'. The third is 'Building Dashboards'. The fourth is 'Simplifying Searches with Search Templates'. The fifth is 'Introduction to Metrics in Sumo'. Below this, there are two main sections: 'Using Sumo Logic Tutorial' and 'Set Up Sumo Logic Tutorial'. The 'Using Sumo Logic Tutorial' section lists seven 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, and Part 7: Get help. The 'Set Up Sumo Logic Tutorial' section lists six 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, and Part 6: Get Help. To the right of these sections is a grid of icons: 'Search' (magnifying glass), 'Logs' (document with lines), 'Metrics' (megaphone), 'Dashboard' (chart), 'Alert' (question mark), 'Self Training' (checkmark), and 'Community' (people icon). A blue 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

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 for '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 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
 - 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 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
 - 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 from the 'Community' icon to the text 'Attend/review training and get certified'.

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 Sumo Logic Learn tab interface. At the top, there are tabs for Home, Learn (which is selected), and Community. Below the tabs, there's a section for Quick Start Videos with five cards:

- 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

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

- Search icon: **Search**
- Document icon: **Docs**
- Bell icon: **Notify Me**
- Question mark icon: **Ask for Support**
- Checklist 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 are sections for 'Quick Start Videos' and 'Using Sumo Logic Tutorial'. Below these are two columns of links for 'Set Up Sumo Logic Tutorial' and 'Find out What's New'. At the bottom right are links for 'Add for Support', 'Self Training', and 'Community'.

Quick Start Videos

- Sumo Logic Overview
- 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

Find out What's New

- Check Sheet
- Docs
- What's New

Add 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?

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

sumo logic

The screenshot shows a white card-like interface against a dark background with colorful diagonal stripes. At the top is a green circular badge with a white checkmark icon and the text "SUMO LOGIC CERTIFIED" around the top and "SEARCH MASTERY" around the bottom. Below the badge is the title "Search Mastery". Underneath the title, the text "ONLINE EXAM: 30 QUESTIONS | 60 MINUTES" is displayed. Below that, "PREP: USING SUMO LOGIC WEBINAR & HANDS ON LABS" is shown. A note states "This certification is valid for one year". To the right of the text is a blue button with the text "Take the Exam" and a pink arrow pointing towards it. Below the button is a smaller link "Learn More".

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



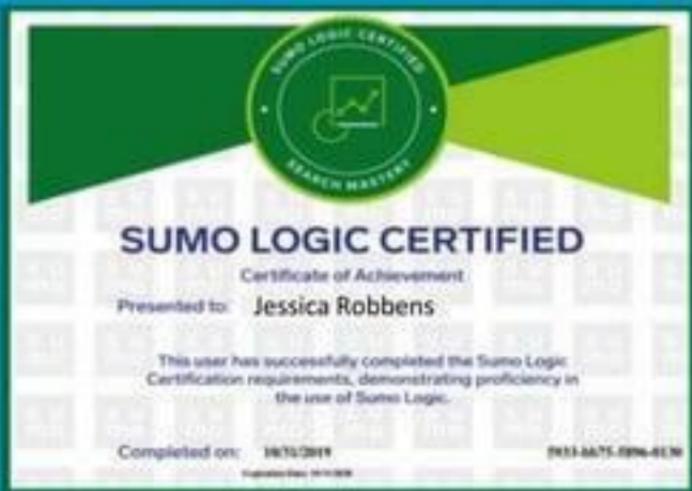
If you find your login is cycling back to the exam screen, do the following:

- 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 be able to take the exam without any issues



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...



How did we do?

Please take our survey:

<https://forms.gle/2KMtxPuD9cSYV8SJ6>

sumo logic



s

Empowering the people who power modern business

m

sumo logic

o