

Become a Sumo Power User

Level 2 Certification



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?

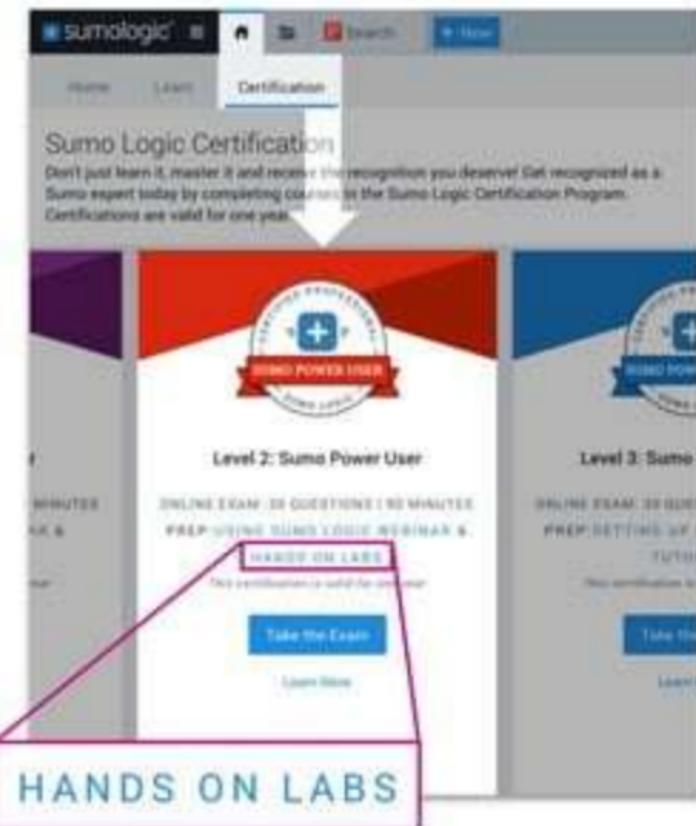
Tutorial: Hands-on Exercises

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** ►



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

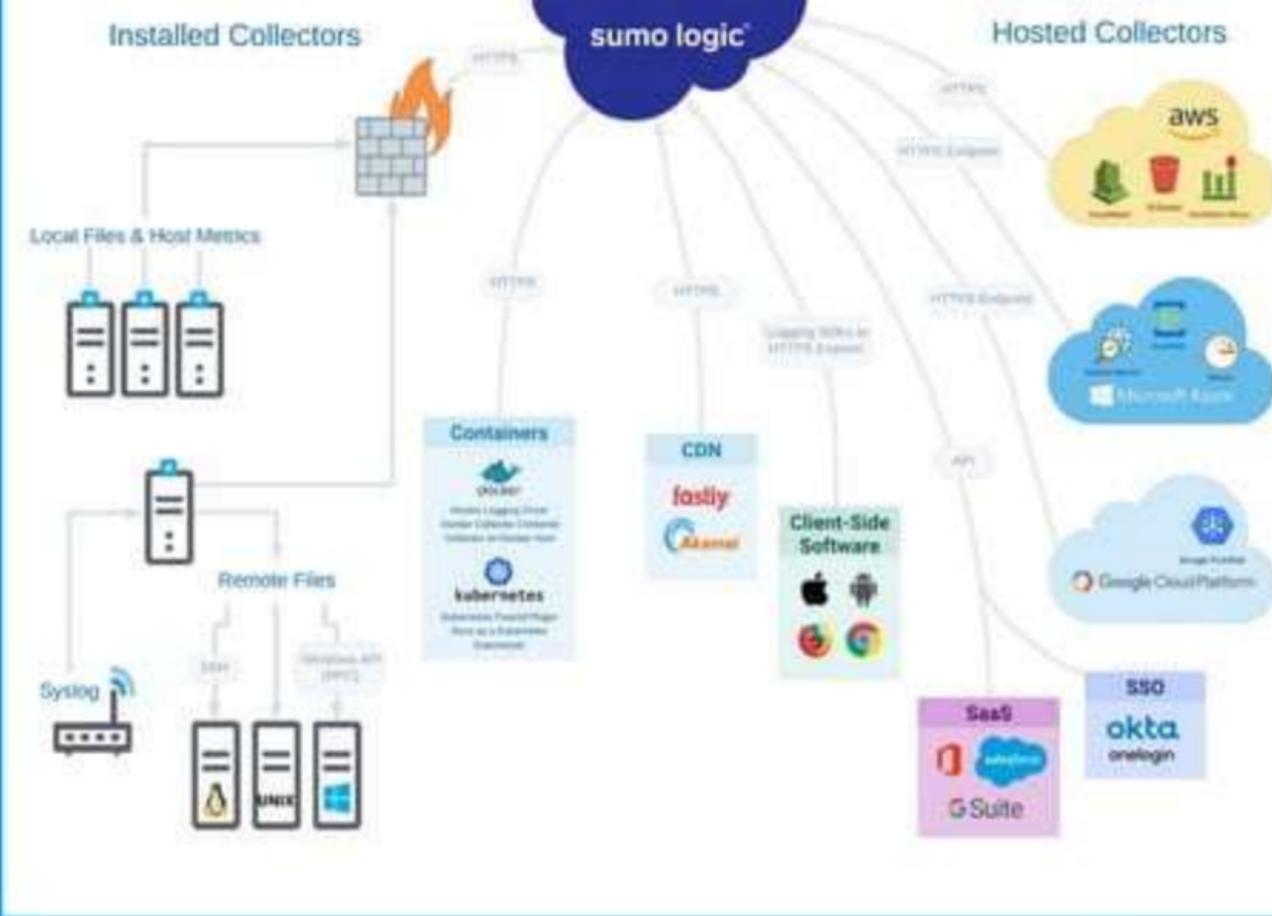


Sumo Logic Data Flow



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



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



{?<>\d}

- 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

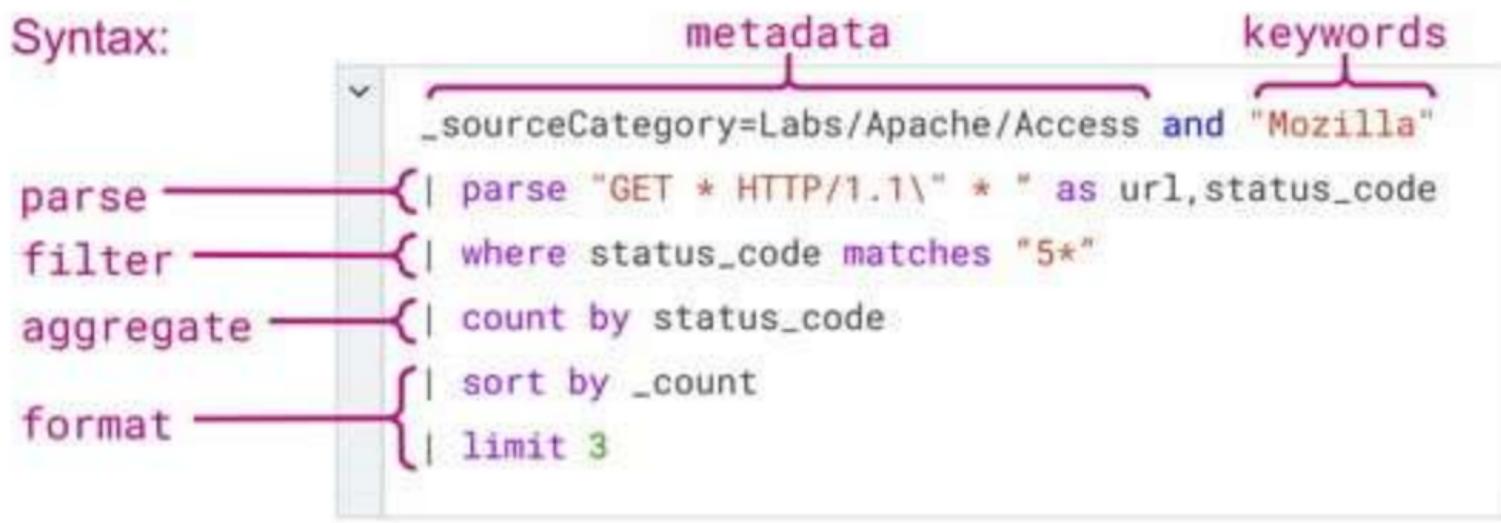
Conditional Logic, Filtering,
Formatting Results



Review ⇨ 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

- 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



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
```

LogCompare

Compare today's patterns with patterns in the past.

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

Messages		Signatures		
		Page: 1 of 2 > >>	LogCompare	▼
#	Select	Count	Reference	Actions
1	<input type="checkbox"/>	953	853	
2	<input type="checkbox"/>	203	953	
3	<input type="checkbox"/>	202	953	
4	<input type="checkbox"/>	174	853	

Messages		Signatures		
		Page: 1 of 2 > >>	LogCompare	▼
#	Select	Count	Score	Actions
1	<input type="checkbox"/>	673	0.00 -1.5%	
2	<input type="checkbox"/>	202	0.07 -7.1%	
3	<input type="checkbox"/>	202	0.00 -0.01%	
4	<input type="checkbox"/>	129	0.25 +25%	

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



Ingesting Metrics - Sources

Host Metrics



AWS ECS

AWS Metrics



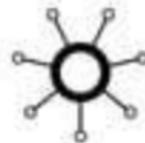
AWS
CloudWatch
Metrics

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

Graphite-Compatible



Dropwizard



CollectD



StatsD

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

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

Metrics Apps: Out-of-the-Box Content

Host Metrics - Overview

Overall Average CPU Idle is: 4% Last 60 Minutes

Overall Average CPU Load (1m, 5m, 15m) is: 1.0 Last 60 Minutes

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.

Q: metrics

All Categories

- Amazon Web Services
- Compliance and Security
- Dashboards

AWS Elastic Load Balancing Metrics

AWS Lambda Metrics

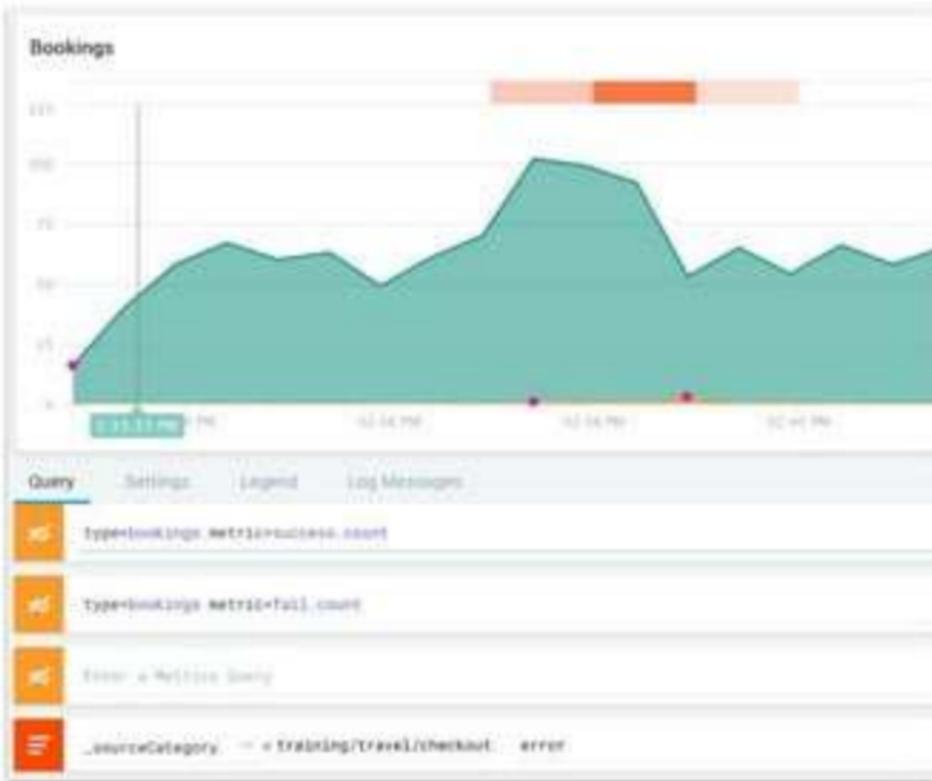
Host Metrics

The dashboard displays the overall average CPU idle percentage (4%) and CPU load (1.0) over the last 60 minutes. It includes a search bar for 'metrics' and an 'App Catalog' section listing AWS services like AWS Lambda Metrics and Host Metrics. Below the catalog are two line charts showing CPU load and total used memory over the last 60 minutes, with data points from 01:45 PM to 01:55 PM.

Logs and Metrics - Overlay

Overlay helps you correlate metrics to the relevant logs.

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



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



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



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 Sumo Logic Learn tab interface. At the top, there are tabs for Home, Learn, and Documentation. Below the tabs, there's a section for Quick Start Videos with five video thumbnails:

- Sumo Logic Dashboard
- Introduction to Search
- Building Dashboards
- Simplifying Search 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
- 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 Heat Metrics

At the bottom right, there's a "Get Help" section with icons for Contact Support, Get Training, and Community.

Explore the tutorials

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

The screenshot shows the 'Learn' tab in the Sumo Logic interface. At the top, there are 'Quick Start Videos' including 'Sumo Logic Dashboard', 'Introduction to Search', 'Building Dashboards', 'Searching, Sorting, and Filtering in Searches', 'Using Sumo Logic', and 'Introduction to Metrics in Sumo'. Below this, there are two columns of 'Using Sumo Logic Tutorial' sections:

- 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: Identify your DataModel
 - 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 Metric Metrics

At the bottom right, there are links for 'How To Support', 'Get 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 in the Sumo Logic interface. At the top, there's a navigation bar with 'Learn' selected. Below it, a 'Quick Start Videos' section displays five video thumbnails:

- Sumo Logic Dashboard
- Introduction to Search
- Building Dashboards
- Searching Events with Search Templates
- Introduction to Metrics

Below these are two main sections:

- 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: Identify your dashboard
 - Part 6: Create an alert
 - Part 7: Get Help
- Set Up Sumo Logic Tutorial**:
 - Part 1: Set up 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 Metric Metrics

At the bottom right, there's a 'Documentation' section with three icons: 'Search Document' (highlighted with a white box), 'Issue', and 'Report a Problem'. Below this are links to 'How To Support', 'Get 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 are five video thumbnails under 'Quick Start Videos': 'Sumo Logic Dashboard', 'Introduction to Search', 'Building Dashboards', 'Searching Events with Search Templates', and 'Introduction to Learning in Sumo'. Below these are two 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: Identify your dashboard
 - Part 6: Create an alert
 - Part 7: Get Help
- Set Up Sumo Logic Tutorial:**
 - Part 1: Set up a Collector
 - Part 2: Add a Source
 - Part 3: Install an App and View Data
 - Part 4: Try Simple Analytics
 - Part 5: Toffish and Interactive Heat Maps

At the bottom right of the main content area, there is a 'Find out What's New' section with three icons: 'Cloud Connect', 'Logs', and 'Machine Events'. Below these are three links: 'How To Support', 'Get 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 in the Sumo Logic interface. At the top, there's a navigation bar with 'Learn' selected. Below it, a 'Quick Start Videos' section displays five video thumbnails with titles like 'Sumo Logic Dashboard', 'Introduction to Search', 'Building Dashboards', 'Searching Events with Search Templates', and 'Introduction to Metrics'. Underneath this, two sections are visible: 'Using Sumo Logic Tutorial' and 'Set Up Sumo Logic Tutorial', each containing a numbered list of steps. To the right, there's a grid of icons for 'Search', 'Logs', 'Metrics', 'Cloud Connect', 'Alerts', 'New', 'What's New', 'Get Support', 'Get Training', and 'Community'. A callout bubble points from the 'Community' icon towards the right side of the slide.

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 Sumo Logic Learn tab interface. At the top, there are tabs for Home, Learn, and Documentation. Below this, there's a section for Quick Start Videos with five cards:

- Sumo Logic Dashboard
- Introduction to Search
- Building Dashboards
- Searching Events with Search Templates
- Introduction to Metrics

Below the videos, there are two main sections:

- Using Sumo Logic Tutorial:** A list of 8 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: Identity your DataModel
 - 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: Toffish and Interactive Heat Maps

At the bottom right of the interface, there are three icons: a magnifying glass labeled "Search", a document labeled "View", and a megaphone labeled "Post". A callout bubble points from the "Post" 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 'Learn' tab of the Sumo Logic interface. At the top, there's a navigation bar with 'Learn' selected. Below it, a 'Quick Start Videos' section displays five video cards:

- Sumo Logic Dashboard
- Introduction to Search
- Building Dashboards
- Searching Events with Search Templates
- Introduction to Metrics

Below these 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: Identify your dashboard
 - Part 6: Create an alert
 - Part 7: Get help
 - Part 8: Set up a collector
 - Part 9: Install an app and view data
 - Part 10: Try Simple Analytics
- Set Up Sumo Logic Tutorial:** A list of 5 steps:
 - Part 1: Set up a collector
 - Part 2: Add a source
 - Part 3: Install an app and view data
 - Part 4: Try Simple Analytics
 - Part 5: Tailored and Interactive Heat Maps

At the bottom right of the interface, there's a 'Support' button with a magnifying glass icon. A callout bubble points from this button to the text 'Open a Support case'.

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 interface. At the top, there are five video thumbnails under the heading "Quick Start Videos": "Sumo Logic Dashboard", "Introduction to Search", "Building Dashboards", "Simplifying Search with Search Templates", and "Introduction to Metrics in Sumo". Below this, there are two 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 support and community links:

- 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 certification page for 'SUMO POWER USER'. At the top is a circular badge with a blue plus sign in the center, surrounded by the text 'CERTIFIED PROFESSIONAL' at the top and 'SUMO LOGIC' at the bottom. Below the badge is a red ribbon banner with the text 'SUMO POWER USER' in white. The main text on the page reads 'Level 2: Sumo Power User'. Below this, it says 'ONLINE EXAM: 30 QUESTIONS | 90 MINUTES' and 'PREP: USING SUMO LOGIC WEBINAR & HANDS ON LABS'. A pink arrow points to a blue button labeled 'Take the Exam'. To the right of the button is the text 'Learn More'.

s

u

Empowering the people who power modern business

m

o

sumo logic