

Become a

Sumo Generalist

Fundamentals Certification



sumo logic



Course Agenda

- 10 min. ● Overview of Sumo logic
- 10 min. ● Demo our monitoring and troubleshooting
- 10 min. ● Hands-on Labs:
 - View all collected data
- 30 min. ● Search, parse, and analyze data
- 20 min. ● Trending analysis and monitor critical events
- 30 min. ● Creating and modifying dashboards & create an alert
- 60 min. ● Get certified as a Sumo Generalist Fundamentals

How can Sumo Logic help you today?

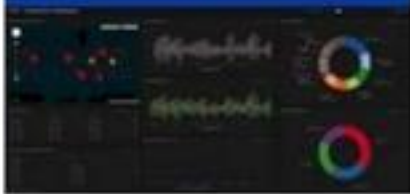
Continuous intelligence for modern apps

Operational Analytics



- ✓ Good user experience
- ✓ Better app performance
- ✓ Reduce MTTI/R

Security Analytics



- ✓ Secure cloud workloads
- ✓ Lower cost of compliance
- ✓ Compliant service

Business Analytics



- ✓ Faster time to market
- ✓ More competitive offering
- ✓ Improved customer support

1. How does Sumo Logic **help me?**

Demo & Dataflow

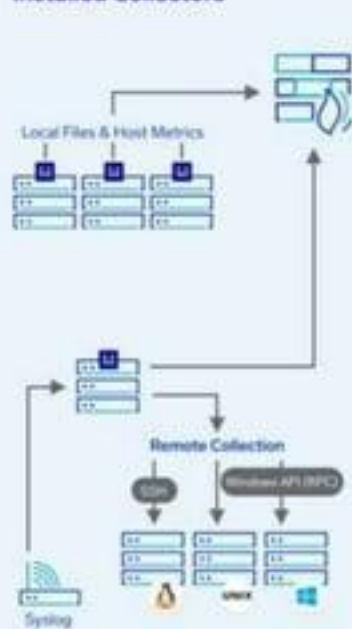
sumo logic



Sumo Logic Data Flow



Installed Collectors



Hosted Collectors



Sending Data \Rightarrow 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 (e.g. labs/apache/access)

Tutorial: Hands-on Exercises

Training Environment:

service.sumologic.com

username: training+labs@sumologic.com

password:

Hands-on Labs:

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

TUTORIAL



Fundamentals Certification

In order to get credit for the exam, go to **your own instance**, and then to **Certification Tab**.

- Online Exam
- 30 Multiple choice questions
- 60-minute time limit
- 3 attempts

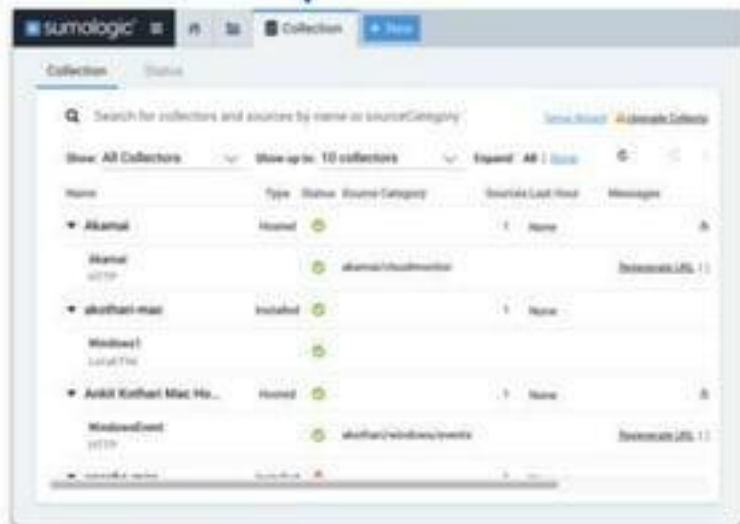


2. What data can I analyze?
What's available to me?



What Data can I Analyze?

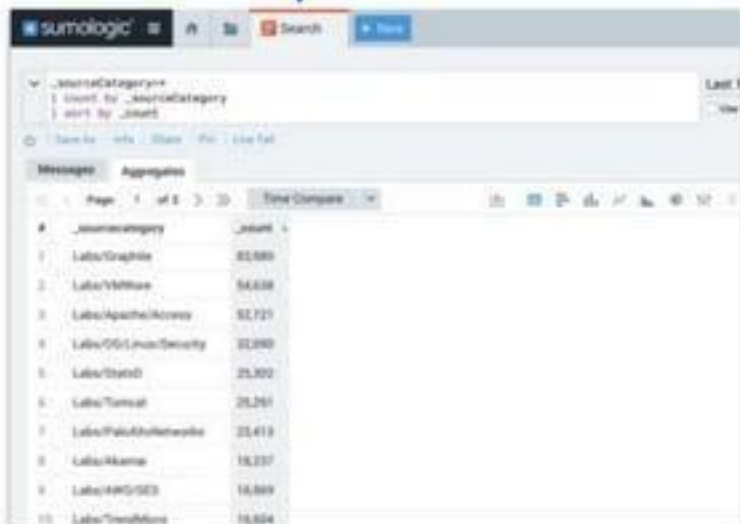
Option 1 Explore your Collectors



The screenshot shows the SumoLogic 'Collection' page. At the top, there's a search bar with the text 'Search for collectors and sources by name or sourceCategory'. Below this, there are tabs for 'Collection' and 'Status'. A table lists several collectors, including 'Akamai', 'akamai-map', and 'Avast! Kaspersky Mac Ho...'. Each row shows the collector name, type, status, source category, source last host, and messages. The 'Messages' column shows a count of messages and a link to view them.

Name	Type	Status	Source Category	Source Last Host	Messages
Akamai	Hosted	✓			
Akamai	Hosted	✓	akamai/akamaihost		See more (25, 1)
akamai-map	Hosted	✓			
akamai-map	Hosted	✓			
Avast! Kaspersky Mac Ho...	Hosted	✓			
Avast! Kaspersky Mac Ho...	Hosted	✓	avast/avast/avast		See more (25, 1)

Option 2 Search for source categories



The screenshot shows the SumoLogic 'Search' page. At the top, there's a search bar with the text 'Search for source categories'. Below this, there are tabs for 'Messages' and 'Aggregations'. A table lists source categories, including 'akamai', 'akamai-map', and 'avast/avast/avast'. Each row shows the source category name, type, status, and message count. The 'Messages' column shows a count of messages and a link to view them.

Source Category	Type	Status	Message Count
akamai	Hosted	✓	25,100
akamai-map	Hosted	✓	54,638
avast/avast/avast	Hosted	✓	52,721
avast/avast/avast	Hosted	✓	52,880
avast/avast/avast	Hosted	✓	25,302
avast/avast/avast	Hosted	✓	25,261
avast/avast/avast	Hosted	✓	25,419
avast/avast/avast	Hosted	✓	18,237
avast/avast/avast	Hosted	✓	18,849
avast/avast/avast	Hosted	✓	18,824

3. How can I analyze my data?

Search, Parse, Analyze



Data Analytics – Shared Content

Has someone already analyzed this same data?

The diagram illustrates the process of checking for shared content in Sumo Logic. It consists of three main components:

- Left Panel (Sumo Logic Interface):** Shows the 'Shared With' filter selected in the sidebar. The filter dropdown menu is open, showing options: 'Me', 'Administrator', 'Analyst', and 'Org'.
- Middle Panel (Shared With Dropdown):** A detailed view of the 'Shared With' dropdown menu, showing the selected option 'Me' and other available options: 'Administrator', 'Analyst', and 'Org'.
- Right Panel (Search Results):** Shows the search results page with the search term 'sharedwith:me'. The results table lists various items shared with the user.

Name	Location
Activity In Location	Personal/Microsoft Office 2016/4
Azure Active Directory	Personal/Microsoft Office 2016/4
Exchange	Personal/Microsoft Office 2016/4
General	Personal/Microsoft Office 2016/4
Microsoft Office 365	Personal/Microsoft Office 365
Resource Access	Personal/Microsoft Office 2016/4
SharePoint	Personal/Microsoft Office 2016/4
CW-006 DNS Request Events	Personal/CrowdStrike - Falcon PI
Demo - Get Lookup on Suspicious	Personal/Microsoft Office 2016/4

Data Analytics – Sumo Logic Apps

Is there an App for it? Search in the **App Catalog** and Install it.

The screenshot displays the Sumo Logic App Catalog interface. On the left is a dark sidebar with the Sumo Logic logo and a list of navigation items: Amazon VPC Flow Logs, Apache, AWS CloudTrail, CloudTrail - Falcon Platform, Microsoft Office 365, Palo Alto Networks, Setup Wizard Searches, Threat Intel for AWS, Threat Intel Quick Analysis, **App Catalog** (highlighted with a red box), Manage Data, Administration, Help, and Raven Kibana (Sumo Logic Tracing). The main panel is titled 'App Catalog' and includes a search bar and a list of categories: Amazon Web Services, Compliance and Security, Database, DevOps, Google Cloud Platform, IT Infrastructure, Microsoft Azure, Operating System, Storage, and Web Server. The central area features a grid of 21 app tiles, each with an icon and a title. The tiles are arranged in three rows: Row 1 includes AWS CloudTrail, AWS Config, AWS Elastic Load Balancing - Application, AWS Elastic Load Balancing - Classic, AWS Elastic Load Balancing - Metrics, AWS Elastic Load Balancing - ULM - Application, and AWS Elastic Load Balancing - ULM - Classic; Row 2 includes AWS Lambda, AWS Lambda ULM (marked with a green 'NEW' tag), Active Directory, Akamai Cloud Monitor, Amazon CloudFront, Amazon DynamoDB, and Amazon ECS; Row 3 includes a tile with a blue 'K' icon (marked with a green 'NEW' tag), a shield icon, a green download icon, a bar chart icon, a blue cube icon, an Amazon S3 icon, and a red puzzle piece icon.

Hands-on Lab

Using Sumo Logic Tutorial

Complete Part 1: Viewing Data

- Sign in
- Identify data available
- Search for existing content from other users
- Install a Sumo Logic App

Data Analytics ⇒ Query Syntax

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

Syntax:

metadata

keywords

```
_sourceCategory=Labs/Apache/Access and "Mozilla"
```

```
parse ——— { | parse "GET * HTTP/1.1\" * " as url,status_code
```

```
filter ———— { | where status_code matches "5*"
```

```
aggregate — | count by status_code
```

```
| sort by _count
```

```
format | limit 3
```

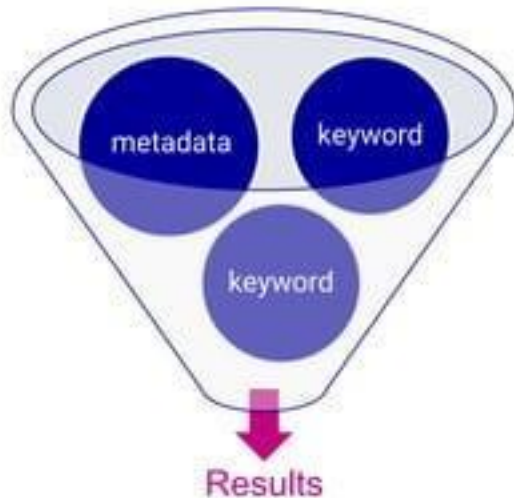
Data Analytics \Rightarrow Query Syntax

Use metadata and keywords to narrow your search scope

Syntax:

metadata + keywords

```
| parse  
| filter  
| aggregate  
| format
```



Data Analytics ⇒ Query Syntax

Extract meaningful fields to provide structure to your data

Syntax:

metadata + keywords

| **parse**
| filter
| aggregate
| format

Parse Anchor:

| **parse** " *@* " as user, domain

Parse Regex:

| **parse regex** "(?<src_ip>\d{1,3}
\\.\d{1,3}\\.\d{1,3}\\.\d{1,3})"

Other Parse Operators:

csv, json, keyvalue, split, xml

[Learn more: Parse Operators](#)

Data Analytics ⇒ Query Syntax

Further filter results using your extracted fields

Syntax:

metadata + keywords

| parse

| **filter**

| aggregate

| format

where operator:

| `where !(status_code=304)`

in operator:

| `if(status_code in("501", "502"),
"Error", "OK") as code_type`

Other Filter Operators:

`join, lookup, matches, filter,
isEmpty, isNull, isBlank`

[Learn more: Filter operator example](#)

Data Analytics \Rightarrow Query Syntax

Evaluate messages and place them into groups

Syntax:

metadata + keywords

| parse

| filter

| **aggregate**

| format

count operator:

| `count by status_code`

avg operator:

| `avg(size) by src_ip`

pct operator:

| `pct(filesize, 75) by _sourceHost`

Other Aggregation Operators:

`sum, count_distinct, stddev, min,`

`max`

[Learn more: Aggregation operators](#)

Data Analytics ⇒ Query Syntax

Format to display desired results succinctly

Syntax:

metadata + keywords

| parse

| filter

| aggregate

| **format**

top operator:

| top 5 src_ip by avg_size

fields operator:

| fields src_ip, avg_size

transpose operator:

| transpose row src_ip column url

Other formatting Operators:

format, formatdate, limit, sort

[Learn more: Trends over time using transpose](#)

Advanced Analytics

Geo Lookup

```
_sourceCategory=Labs/Apache/Access  
| lookup latitude, longitude from geo://default on ip=src_ip  
| count by latitude, longitude
```

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.

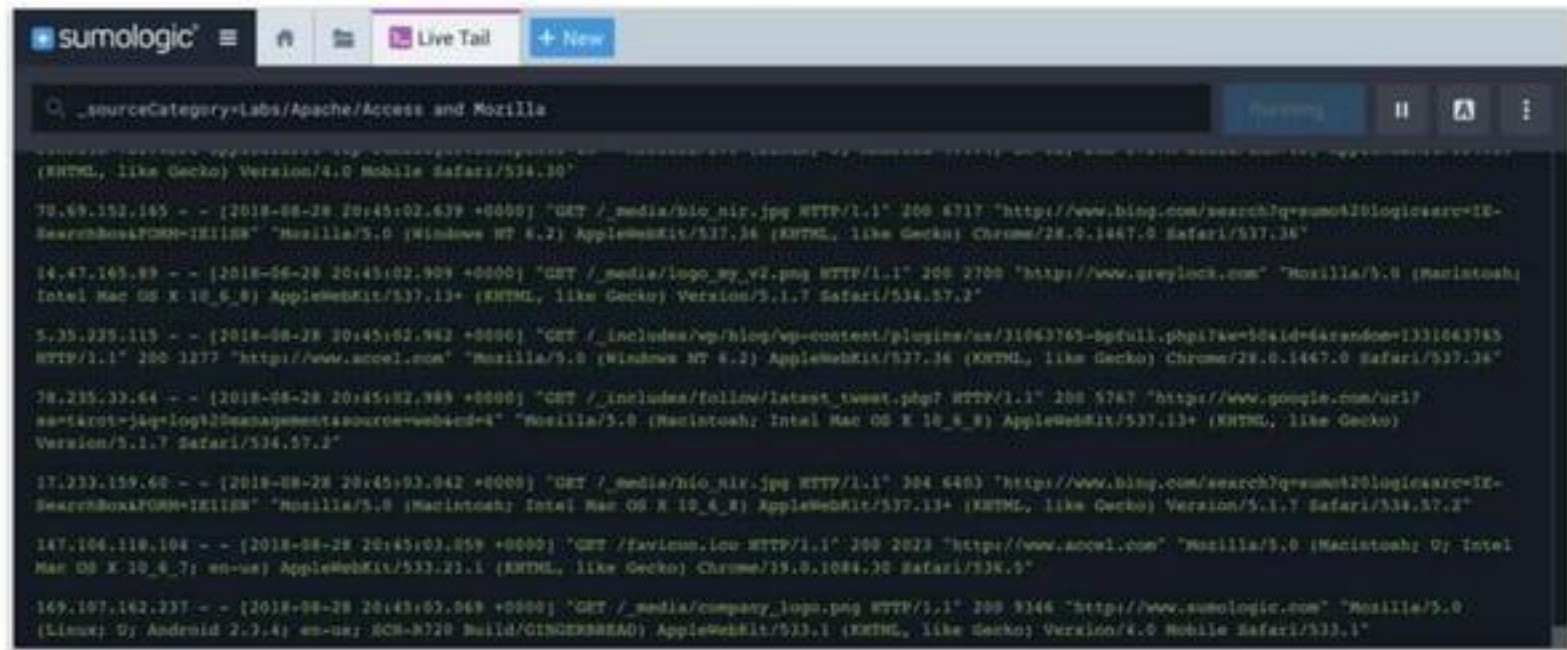
```
_sourceCategory=Labs/snort  
| logcompare -24h
```

Messages		Signatures		Page: 1 of 2 > >>		LogCompare		
#	Select	Count	Relevance	Actions		Signature		
1	<input type="checkbox"/>	452	9.53	👍	👎	🔍	SDATE WEB-MISC BugPort conf 2] (TCP) ***** -> 10.*****	
2	<input type="checkbox"/>	202	9.53	👍	👎	🔍	SDATE WEB-PHP Typo3 transla 1] (TCP) ***** -> * 10.*****	
3	<input type="checkbox"/>	202	9.53	👍	👎	🔍	SDATE WEB-MISC BugPort conf 2] (TCP) ***** -> 10.*****	
4	<input type="checkbox"/>	174	9.53	👍	👎	🔍	SDATE SENSITIVE-DATA Email -> * 10.*****	

Messages		Signatures		Page: 1 of 2 > >>		LogCompare		
#	Select	Count	Score	Actions		Signature		
1	<input type="checkbox"/>	473 -1.5%	0.00	👍	👎	🔍	SDATE WEB-MISC BugPort config (TCP) ***** -> 10. *****	
2	<input type="checkbox"/>	388 -7.1%	0.07	👍	👎	🔍	SDATE WEB-PHP Typo3 translati (TCP) ***** -> * 10. *****	
3	<input type="checkbox"/>	358 -0.01%	0.00	👍	👎	🔍	SDATE WEB-MISC BugPort config (TCP) ***** -> 10. ***.206. *	
4	<input type="checkbox"/>	128 +25%	0.25	👍	👎	🔍	SDATE SENSITIVE-DATA Email Ad -> * 10. *****	

Advanced Analytics

Get real time view of your logs with Live Tail



Hands-On Labs

Using Sumo Logic Tutorial

Complete Part 2: Search for Log Data

- Search and Parse

Complete Part 3: Chart Your Data

- Aggregate

- Format

- Chart your data

4. How can I monitor my data?

Dashboards and Alerts






sumo logic



Monitoring - Dashboards

- Each **Panel** processes results from a single search




- Drill down** into corresponding query or link to another Dashboard

Last 60 Minutes   

- Live Mode:** provides live stream of data

 ☐ LIVE MODE

- Use Dashboards as templates with **Filters**

Last 60 Minutes   



Let's take a 15 min break

Return promptly to play Kahoot
3 multiple choice questions

The highest score wins a prize!

The Kahoot! logo is displayed in white, bold, sans-serif font against a solid purple rectangular background. The word "Kahoot!" is written in a playful, slightly rounded style, with the exclamation mark being a large, bold dot.

Hands-On Labs

Using Sumo Logic Tutorial

Complete Part 4: Create and Share a Dashboard

- Create a Dashboard
- Change the Theme
- Share with your Organization

Complete Part 5: Modify a Dashboard

- Modify the query of an existing Dashboard Panel

Monitoring - Alerts

Scheduled Searches trigger Alerts when a condition is met.

Alert Types:

- Email
 - Webhook
 - Save to Index
 - Script Action
- [Learn More: 2 Key Principles for Creating Meaningful Alerts](#)



Hands-On Labs

Using Sumo Logic Tutorial

Complete Part 6: Create an Alert

- Schedule and test an Alert
- Delete Alert after testing

Metrics

Sources, Dashboards and Alerts



Logs and Metrics - Overlay

Overlay helps you correlate metrics to the relevant logs.

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



Ingesting Metrics

Host Metrics



AWS ECS

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

AWS Metrics



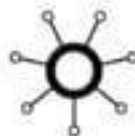
AWS
CloudWatch
Metrics

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

Graphite-Compatible



Telegraf



CollectD



Dropwizard



StatsD

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

Metrics - Dashboards and Alerts

Dashboards can contain Metrics and Logs Panels



Metric Monitors alert on thresholds
(Critical, Warning, Missing Data)

5. Where do I go from here?

Training, Docs, Community,
Support



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

sumologic

Home Learn Dashboards

Quick Start Videos

Sumo Logic QuickStart
August 2018

Introduction to Search

Building Dashboards

Simplifying Search with Search Templates

Introduction to Metrics in Sumo

Using Sumo Logic Tutorial

- Part 1: Winning 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

Check Status Docs What's New

Ask for Support Get Training Community

Explore the tutorials

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

sumologic

Learn

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

Check Status

Docs

Share Your Idea

Ask for Support

Get Training

Community

Explore the tutorials

Access comprehensive
lists of operators and
more

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

Explore the tutorials

Access comprehensive lists of operators and more

Every feature and tool covered in docs

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

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

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

sumologic

Home Search **Learn**

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

Check Status Docs What's New

Get 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

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

sumologic

Home Learn Dashboard

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

Check Status Docs What's New

Get Training Community

Open a Support case

Explore the tutorials

Access comprehensive lists of operators and more

Every feature and tool covered in docs

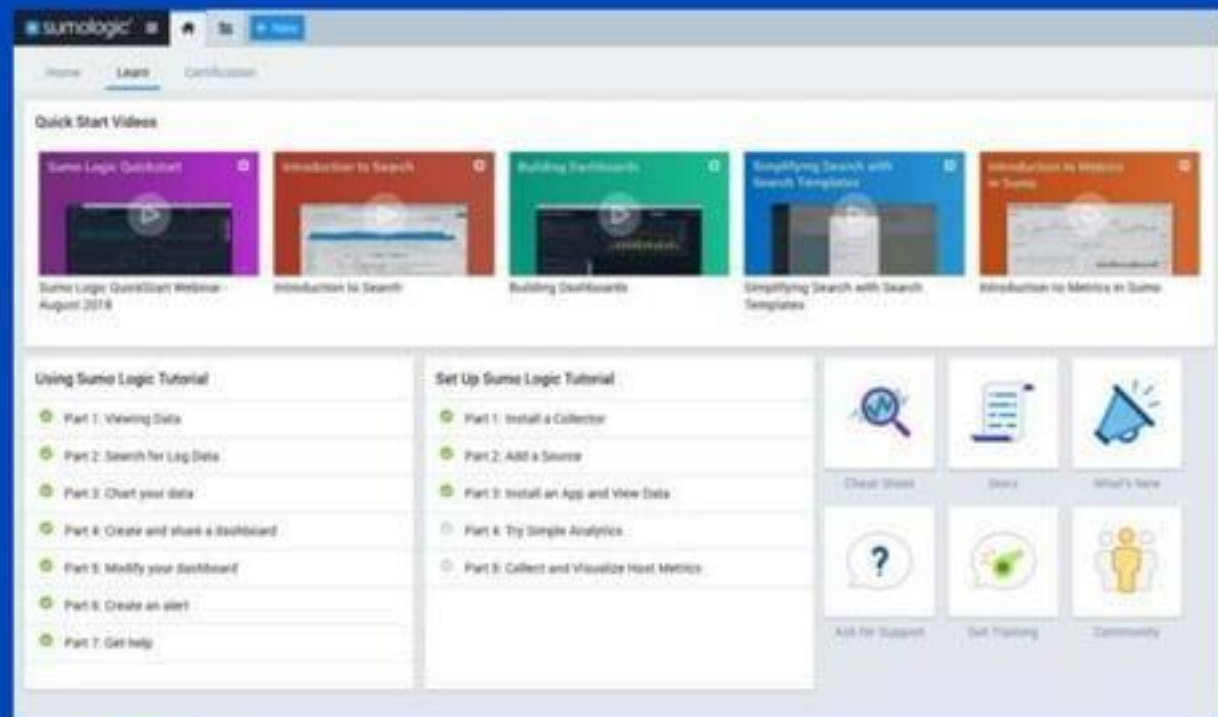
Find out What's New

Find answers or post your questions to Community

Attend/review training and get certified

Open a Support case

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



sumologic

Home Learn Certification

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

Check Status

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

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
- sumologic.talentlms.com



Fundamentals

ONLINE EXAM: 30 QUESTIONS | 60 MINUTES

PREP: QUICKSTART WEBINAR &
TUTORIAL

This certification is valid for two years



Take the Exam

[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

u

Empowering the
people who power
modern business

m

o

sumo logic

s

u

Empowering the
people who power
modern business

m

o

sumo logic