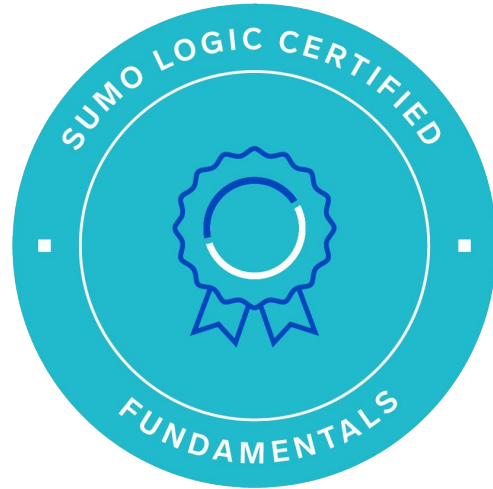


Become a Sumo Generalist Fundamentals Certification



Welcome!
Note you are
currently muted.
We will get started
shortly.

● This session is being recorded

Course Agenda

15 min.



Introduction

- What is Sumo Logic?
- What kind of data does Sumo Logic ingest?
- Sumo Logic architecture
- What is available out-of-the-box?

25 min.



Data Collection

- Preparing the data to be seen
- Collectors
- Sources
- Collection strategy

20 min.



Searching and
Analyzing Data

- How is the data organized in Sumo Logic?
- Where do I search for my data?
- Perform a search using a query

15 min.



Alerts and Monitoring

- Alert Response
- Context Cards for Troubleshooting

15 min.



Visualizing Data

- Charts, Panels, Dashboards

10 min.



Summary

- Exam, Next steps, Survey

Course Objectives

- Describe the Sumo Logic data pipeline.
- Understand how collectors and sources work.
- Install an app.
- Search logs data using Basic Mode.
- View data with charts, panels, and dashboards.

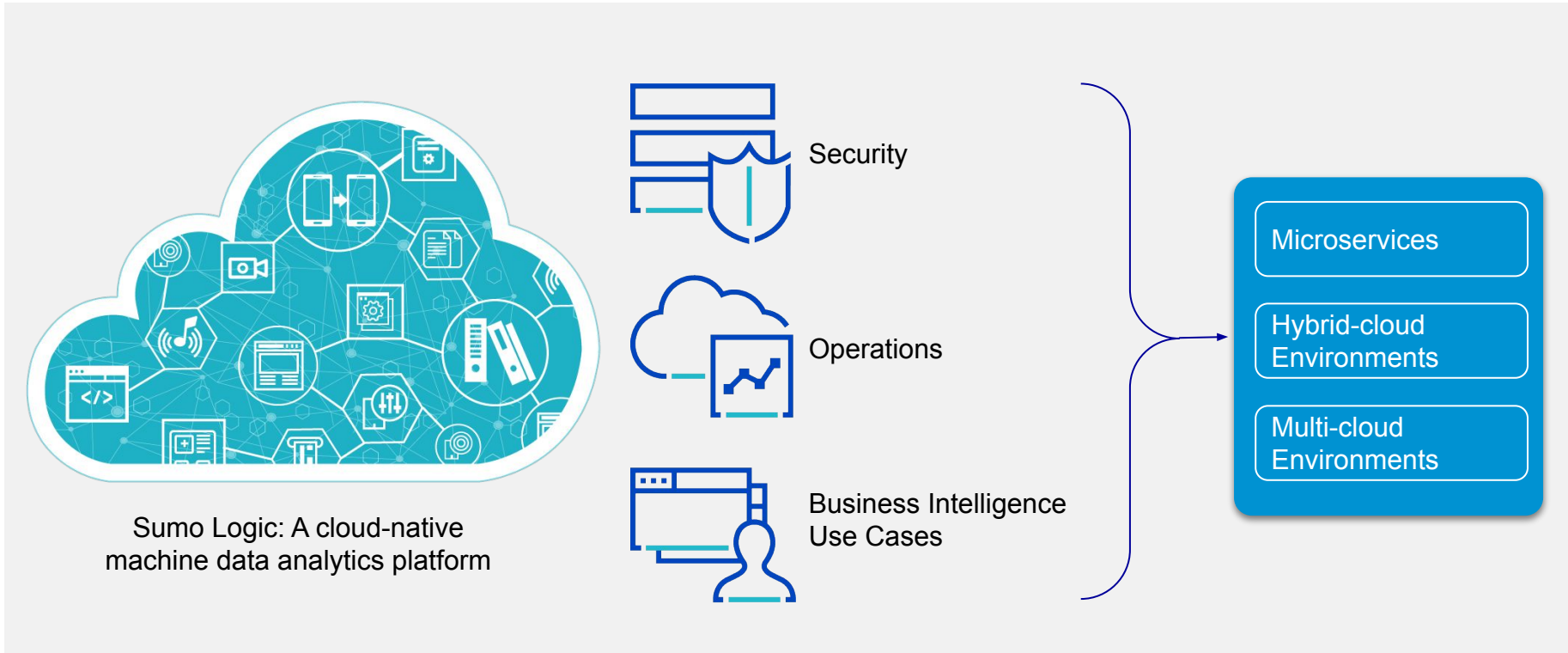
Introduction

- What is Sumo Logic?
- What kind of data does Sumo Logic ingest?
- Sumo Logic architecture
- What is available out-of-the-box?

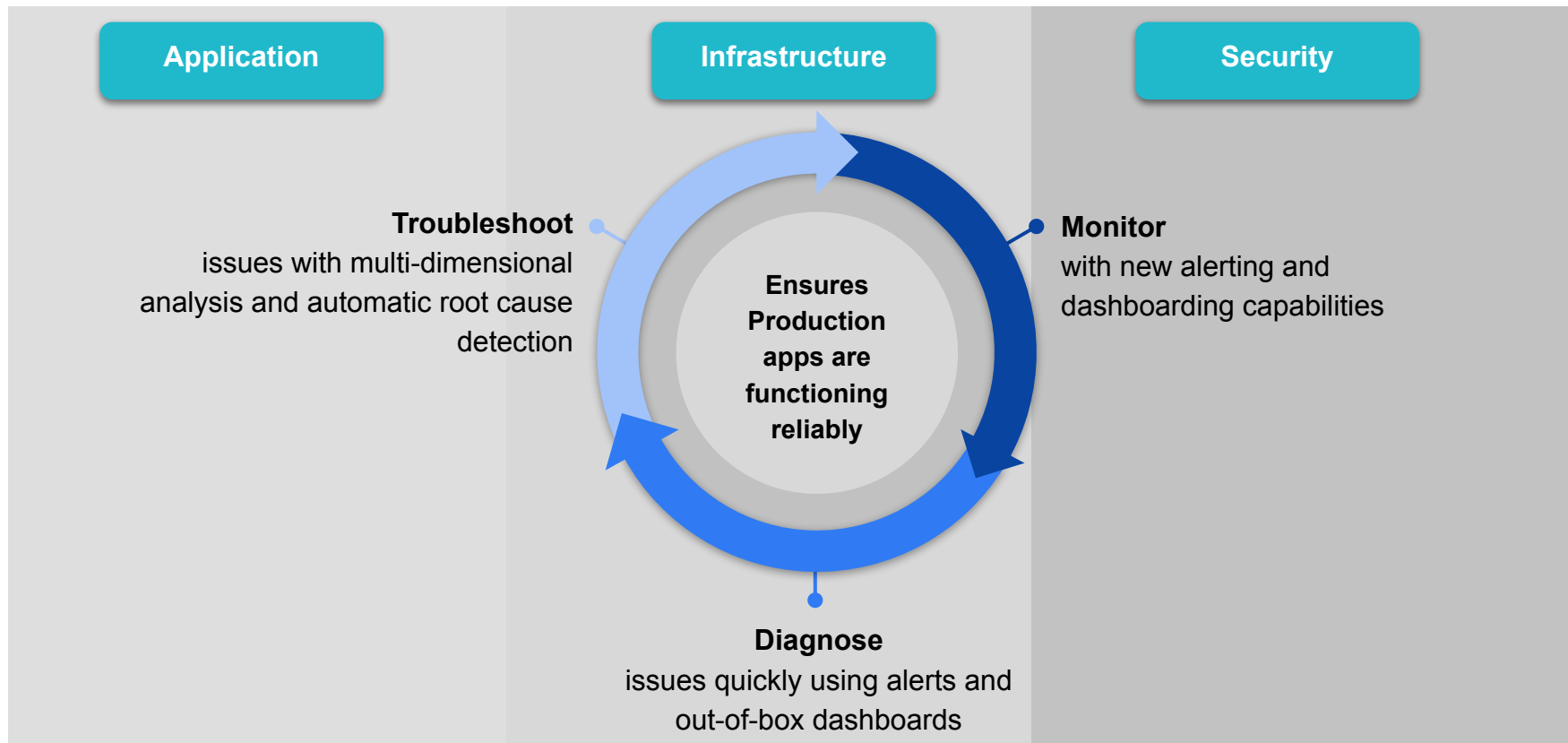
sumo logic



Sumo Logic: A cloud-native data analytics platform

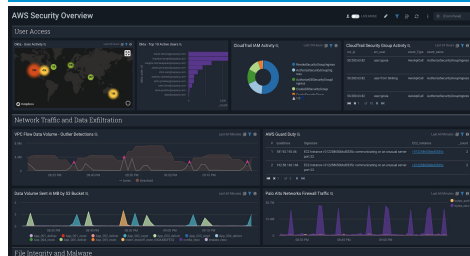


The Observability solution



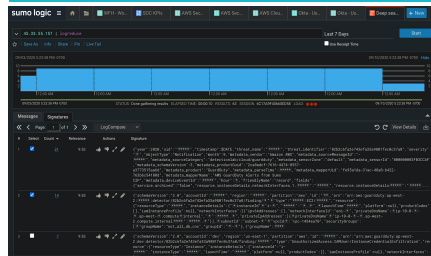
The Security Solution

Cloud Security Monitoring + Analytics



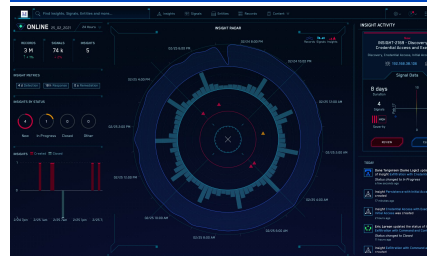
Monitor, detect, search
and investigate security
incidents with threat
benchmarking & analytics

Audit & Compliance



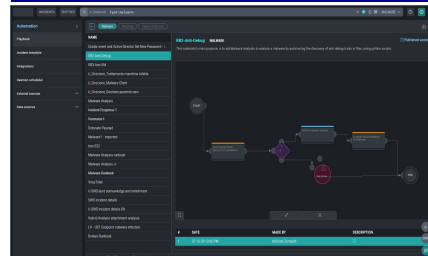
Determine compliance
and posture management

Cloud SIEM



Automatic alert triage,
automatic threat
detection, threat hunting
and investigations

Cloud SOAR



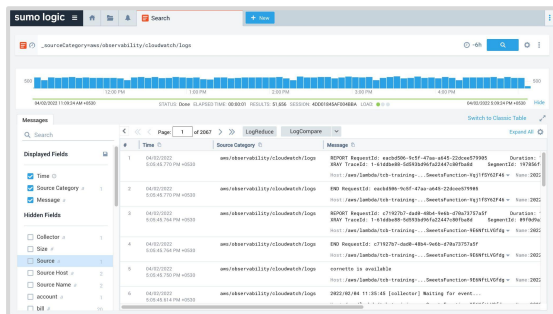
Improve SOC
efficiency with progressive
automation, orchestration,
insightful decision-making

What kind of data does Sumo Logic ingest?



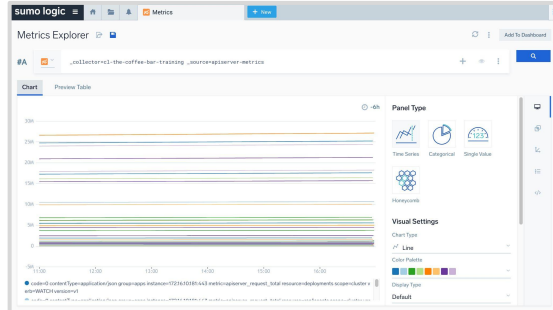
Logs

to identify why it's happening



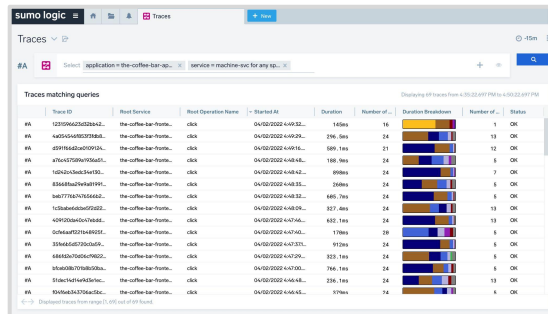
Metrics

to identify what's going on



Traces

end-to-end visibility into user transactions across services



Architecture highlights

Cloud-native

- Built in AWS from the start
- Leverages powerful AWS services to their fullest potential
- Partnership with AWS
- We monitor availability and performance 24/7 and make constant improvements

Microservices

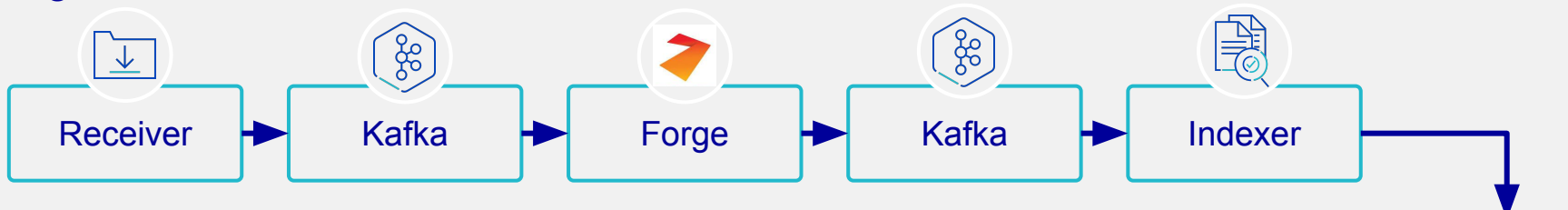
- Autoscaling
- Teams at Sumo Logic push software daily
- Increased reliability due to smaller failure domains and availability zone distribution

Multi-tenant

- Resources are shared
- Headroom to scale on short notice
- Adapts to load dynamically

Sumo Logic Data Pipeline

Ingestion Path



Search Path



How is the data organized in Sumo Logic?

Indexed Data

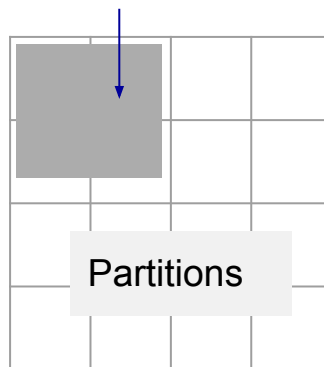
- Default continuous partition
- All ingested data that is not assigned to:
 - a partition or
 - views populated by Scheduled Searches

Data Tiers

- Continuous Tier
- Frequent Tier
- Infrequent Tier

sumo logic

Default Continuous Partition



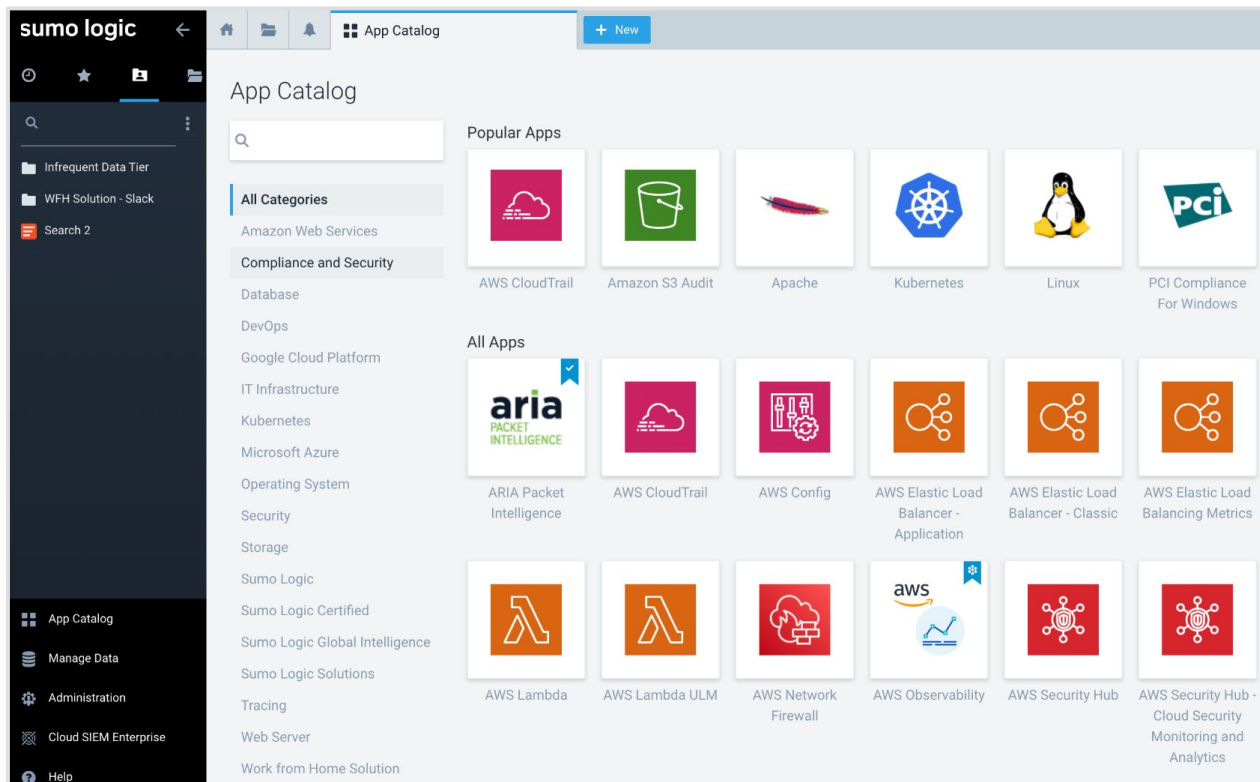
Manage Data > Logs > Partitions

- Create partitions first
- Assign those partitions to the data tiers later



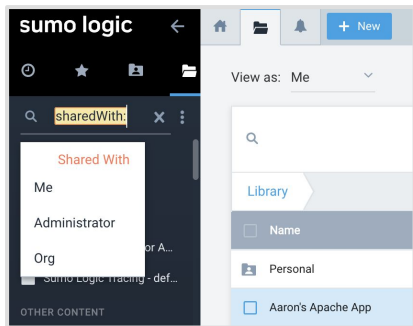
Taking advantage of App Catalog

- Deliver
 - out-of-the box dashboards,
 - saved searches, and
 - field extraction rules for popular data sources
- When an app is installed, pre-set searches and dashboards are customized with your source configurations and populated in a folder



Has someone already analyzed this same data?

– Shared Content

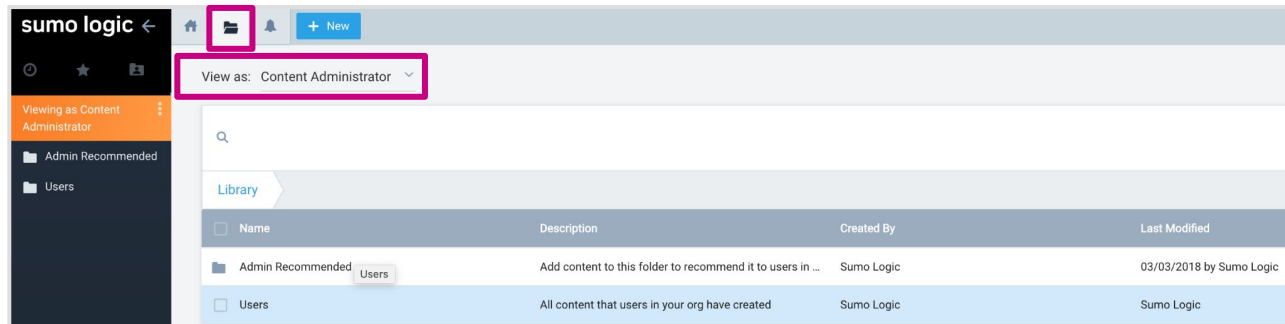


For All Users

- Share log searches, metric searches, dashboards, and folders.
- Choose how widely shared your content is within your Org.

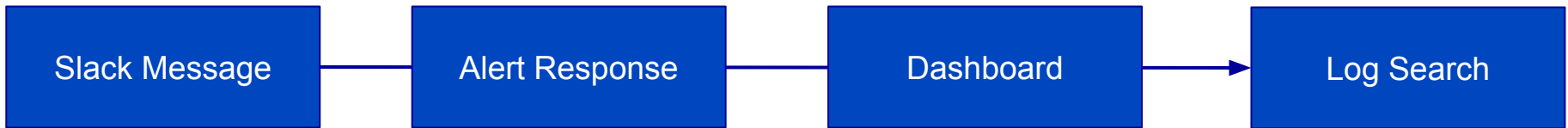
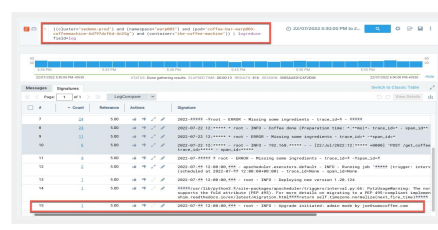
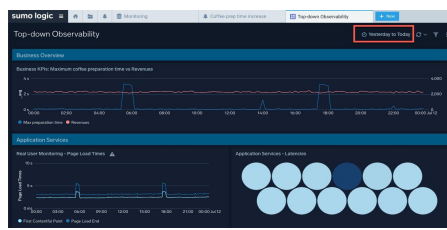
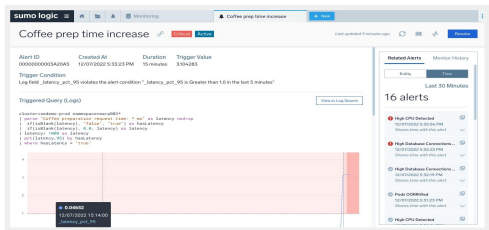
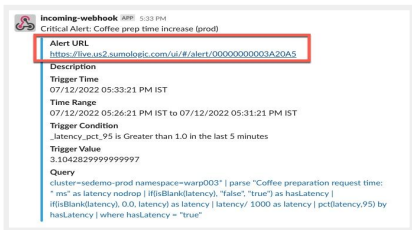
For Admin

Manage content to specific users and groups.

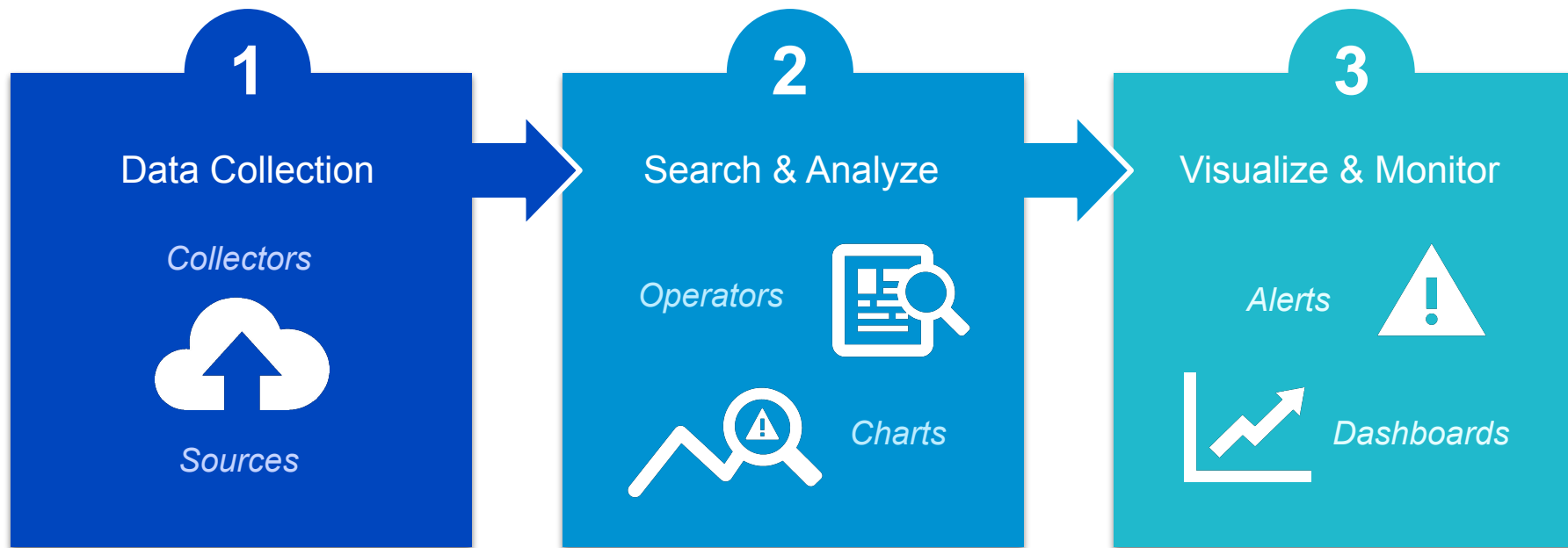


Select the **Library** Tab, under View as: Toggle to **Content Administrator** mode.

Demo: Let's See Sumo Logic in Action!



Sumo Logic Data Flow



Data Collection

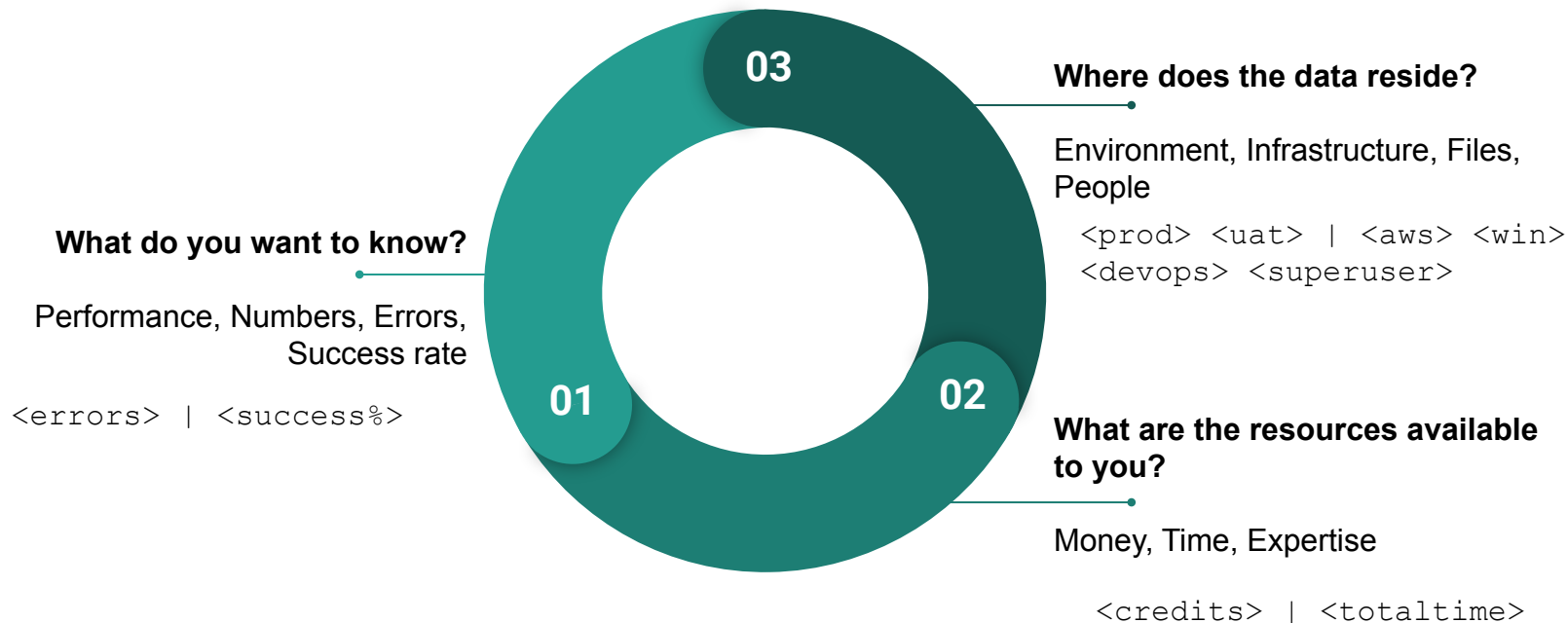
- Preparing the data to be seen
- Collectors
- Sources
- Collection strategy

sumo logic



Preparing the data to be seen

Ask three questions to decide your data collection strategy



Sending Data ➡ Metadata

Metadata tags are:

- Associated with each log message that is collected
- Attached to your log messages at collection-time
- Used to find targeted results in search queries

Tag	Description
<code>_collector</code>	Name of the collector (defaults to hostname)
<code>_sourceHost</code>	Hostname of the server (defaults to hostname)
<code>_sourceName</code>	Name and Path of the log file
<code>_source</code>	Name of the source this data came through
<code>_sourceCategory</code>	Can be freely configured. Main metadata tag (e.g. labs/apache/access)

☐ Collector <i>a</i>	1
☐ Size <i>#</i>	
☐ Source <i>a</i>	1
☐ Source Category <i>a</i>	1
☐ Source Host <i>a</i>	1
☐ Source Name <i>a</i>	1
☐ amount <i>a</i>	211
☐ asctime <i>a</i>	176
☐ cluster <i>a</i>	1

Metadata: Source Category Best Practices

Common components (and any combination of):

- Environment (Prod/UAT/DEV)
- Application Name
- Geographic Information (East vs West datacenter, office location, etc.)
- AWS Region
- Business Unit

The screenshot shows a configuration interface for metadata fields. It features a table with two columns for field names and values. The first column has a 'Fields' label. Each row in the table includes a status icon (green checkmark or yellow warning triangle), the field name, the current value, and a trash icon for deletion. Below the table is a '+Add Field' link. At the bottom, there is a checkbox labeled 'Automatically activate all fields on save.' which is checked, followed by a message: 'You are going to create 2 more fields (used 359 / 600).'

Fields	Status	Field Name	Value	Action
	✓	env	prod	✖
	✓	vendor	microsoft	✖
	⚠	logType	event	✖
	⚠	purpose	security	✖

[+Add Field](#)

☒ Automatically activate all fields on save.
You are going to create 2 more fields (used 359 / 600).

Highest level components should group the data how it is most often search together:

Prod/Web/Apache/Access

Web/Apache/Access/Prod

Dev/DB/MySQL/Error

DB/MySQL/Error/Dev

Source Category Usage Examples

Getting the Source Category naming right is KEY to getting the most out of the platform.

If I want to search for:	Suggested search
Everything that happened in my Prod Windows environment (events)	<code>_sourceCategory=prod/windows/events</code>
Production windows events and performance metrics (Performance)	<code>_sourceCategory=prod/windows/*</code>
Everything that happened across my entire Windows fleet (e.g. checking hotfixes)	<code>_sourceCategory=*/windows/events</code>
Production IIS Access Logs for server “web02” looked after by the “web” support team	<code>_sourceCategory=prod/web/iis/access</code> <code>_sourceHost=web02</code>
All Windows events & performance metrics across the entire platform.	<code>_sourceCategory=*/windows/*</code>
All access logs (apache, IIS, NGINX, etc.), from all of my web servers that are supported by the “web” team.	<code>_sourceCategory=*/web/*/access</code>

Collectors

sumo logic



Types of Collector

Installed Agents

Installed Collector

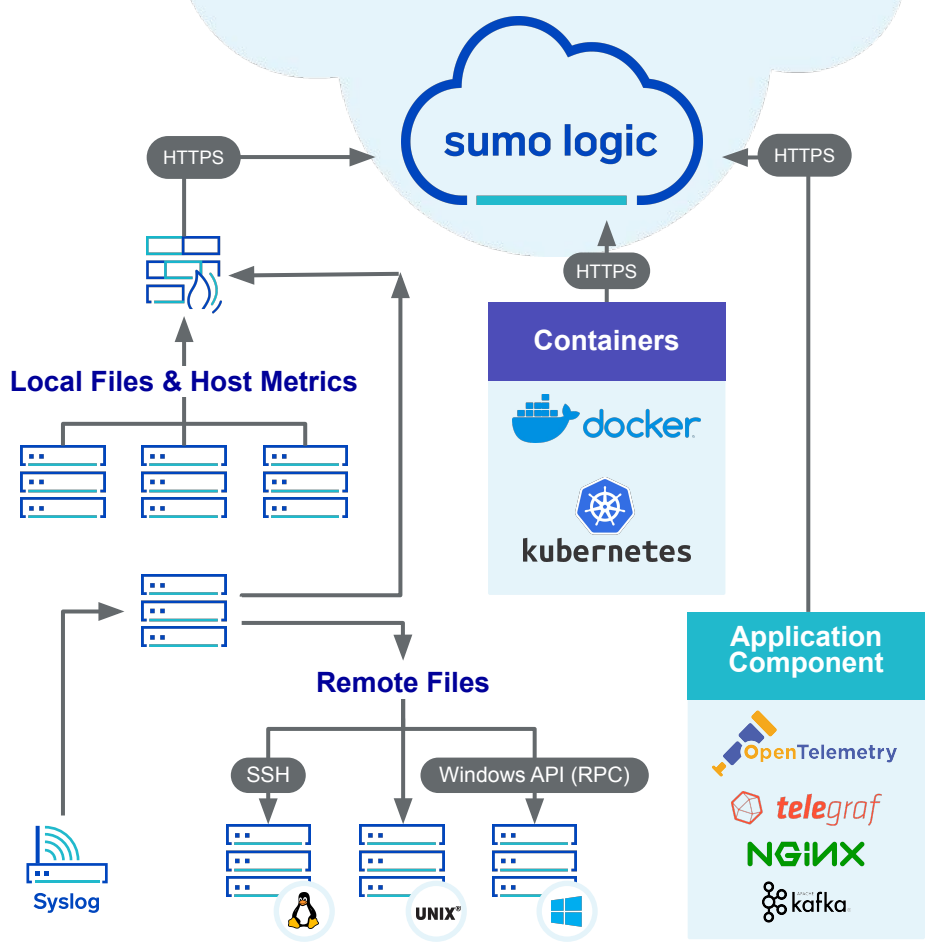
- Is installed on a system within your deployment locally or remotely
- Sources collect data available in your deployment
- Easy to troubleshoot based on Collector logs

OT Distro Agent

- Next generation agent built on OpenTelemetry
- Single framework for ALL observability data
- Puts you in charge of your data
- Supported by major cloud service providers

Hosted Collector

- Is Hosted by Sumo Logic
- Is Agentless
 - Doesn't require a software to install or activate on a system in your deployment
- Hosts Sources to collect seamlessly from AWS, Google, and Microsoft products
- Can receive logs and metrics uploaded via a URL



sumo logic

Installed Agents



When to **use more than one Installed Collector**, if you:

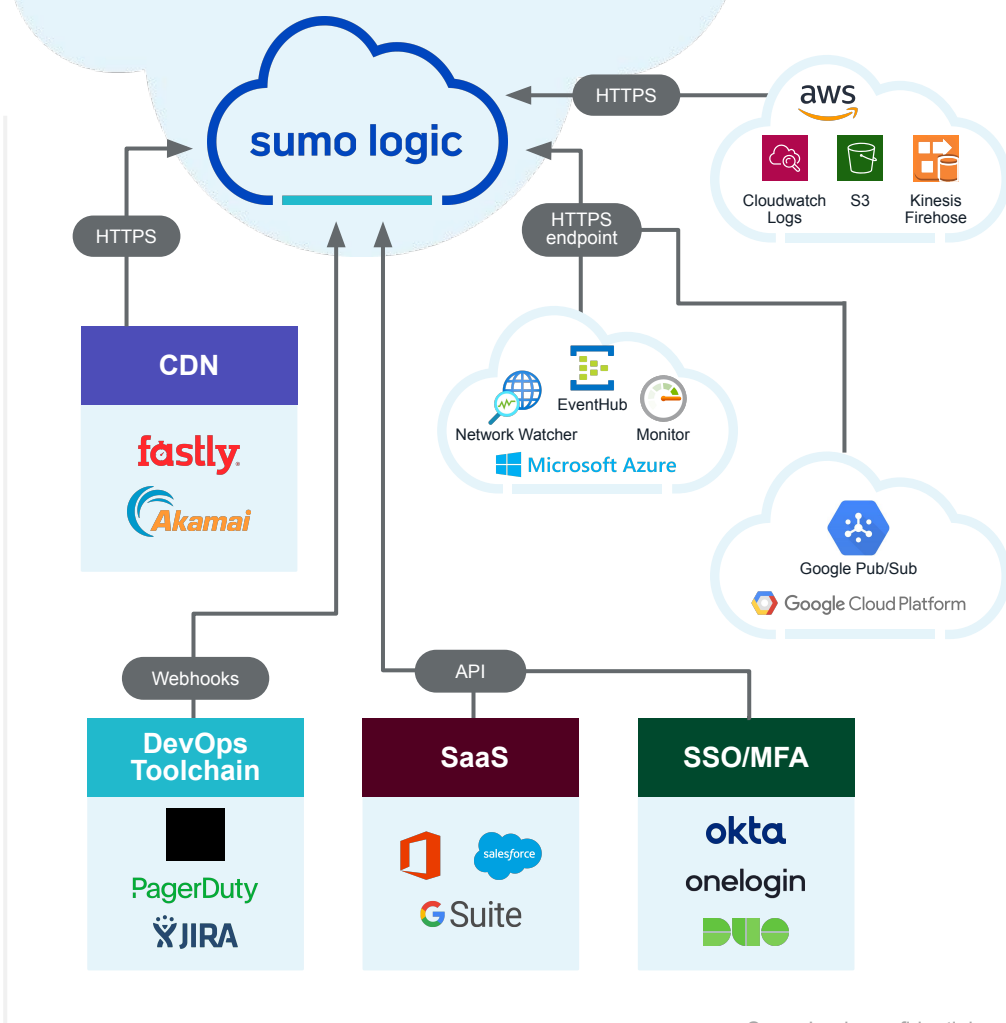
- Expect the Collector to ingest from at least 500 separate files.
- Hardware has memory or CPU limitations.
- Expect combined logging traffic for one Collector to be higher than 15,000 events per second.
- Network clusters or regions are geographically separated.
- Prefer to install many Collectors, for example, one per machine to collect local files.

When to **use OpenTelemetry**, if you:

- Leverage the Supported Sources and Supported Platforms
- Are looking for a single agent as opposed to managing multiple agents
- Are having scale issues with FluentD on Kubernetes Collection
- Are looking for ARM support

Hosted Collector

- For a single Hosted Collector, you can configure up to 1,000 sources.
- Consider setting up more than one Hosted Collector, if you'd like to tag different data types with different metadata.



Selecting a Collector type

Which collector should I use?

Select Collector Type

Installed Agent



Sumo Logic's Distribution of OpenTelemetry

Sumo Logic's next generation agent built on OpenTelemetry



Installed Collector

A Java agent that receives logs and metrics from its sources and then encrypts, compresses, and sends the data to the Sumo service.

Hosted Collector



Hosted Collector

Select to set up a Collector in the Sumo Logic Cloud.

FAQs

- > What's the difference between an Installed and Hosted Collector?
- > What's the difference between Sumo Logic's Distribution of OpenTelemetry and Installed Collector?
- > Where should I install an Installed Collector?
- > How do I know if I need more than one Installed Collector?
- > Where does my data go?

sumo logic

Sources

sumo logic



What is a Source?



Hosts



Appliances



Cloud infrastructure

A source is an object, that:

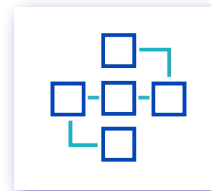
- is configured for a specific collector
- scans a particular target periodically and
- sends newly available data to the collector



Metrics:
Measurements
over time



Logs: Records
of events

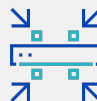


Traces: end-to-end
visibility into user
transactions



Sources

Installed Agents

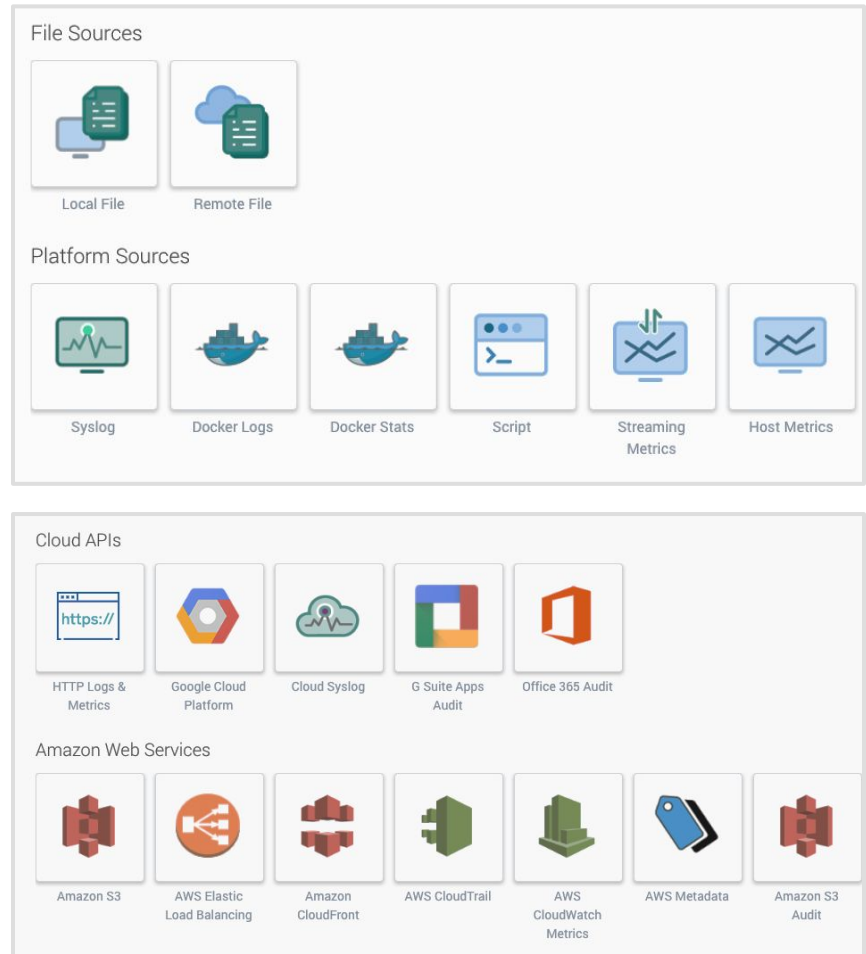


Hosted Collector

Types of Sources

Sources

- File Sources,
 - Windows Event Log Sources,
 - Docker Sources
 - Host Metrics Sources
-
- Amazon S3
 - Cloud syslog source
 - Google Apps Audit Source
 - Google Cloud
 - HTTP
 - Microsoft Office 365



Log in to the training environment

url: service.sumologic.com

email:

training+analyst###@sumologic.com

password:

- a number between 001-999, for example

training+analyst057@sumologic.com

Note: Place your ### number into chat so that everyone knows not to use the one you selected

Welcome back

Email

training+analyst057@sumologic.com

Password

●●●●●●●●●●

Sign in

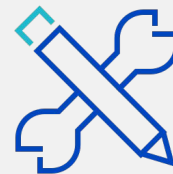
[Forgot your password?](#)

Or

Sign in with your identity provider

Hands-on Lab

Using Sumo Logic Training

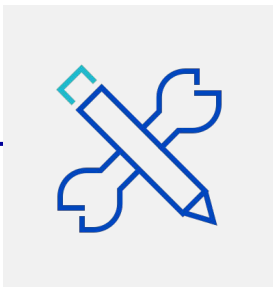


Complete Lab 1: Data Collection

- Sign in to Sumo Logic
- Navigate to Manage Data > Collection page
- Identify metadata available
- Identify collectors
- Identify sources

Hands-on Lab

Using Sumo Logic Training



Complete Lab 2: App Installation

- Install an app and view its content
- Find and display a shared dashboard

Collection Strategy

sumo logic



Deployment Options overview

Local Data Collection

The collector:

1. Is installed on all target hosts
2. Sends log data produced on those target hosts directly to Sumo Logic Backend via HTTPS connection

Centralized Data Collection

The collector:

1. Is installed on a set of dedicated machines
2. Collects log data from target hosts through various remote mechanisms
3. Forwards data to Sumo Logic Backend

Hosted (Cloud) Data Collection

The cloud service:

1. Generates most data in the cloud
2. Collects data through Sumo Logic cloud integrations

Ingesting data for Observability

App System Architecture



Application



App Components



Platform Technology



Amazon
EC2



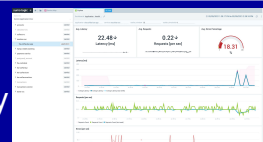
Application Infrastructure



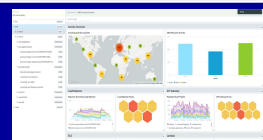
Application
Observability



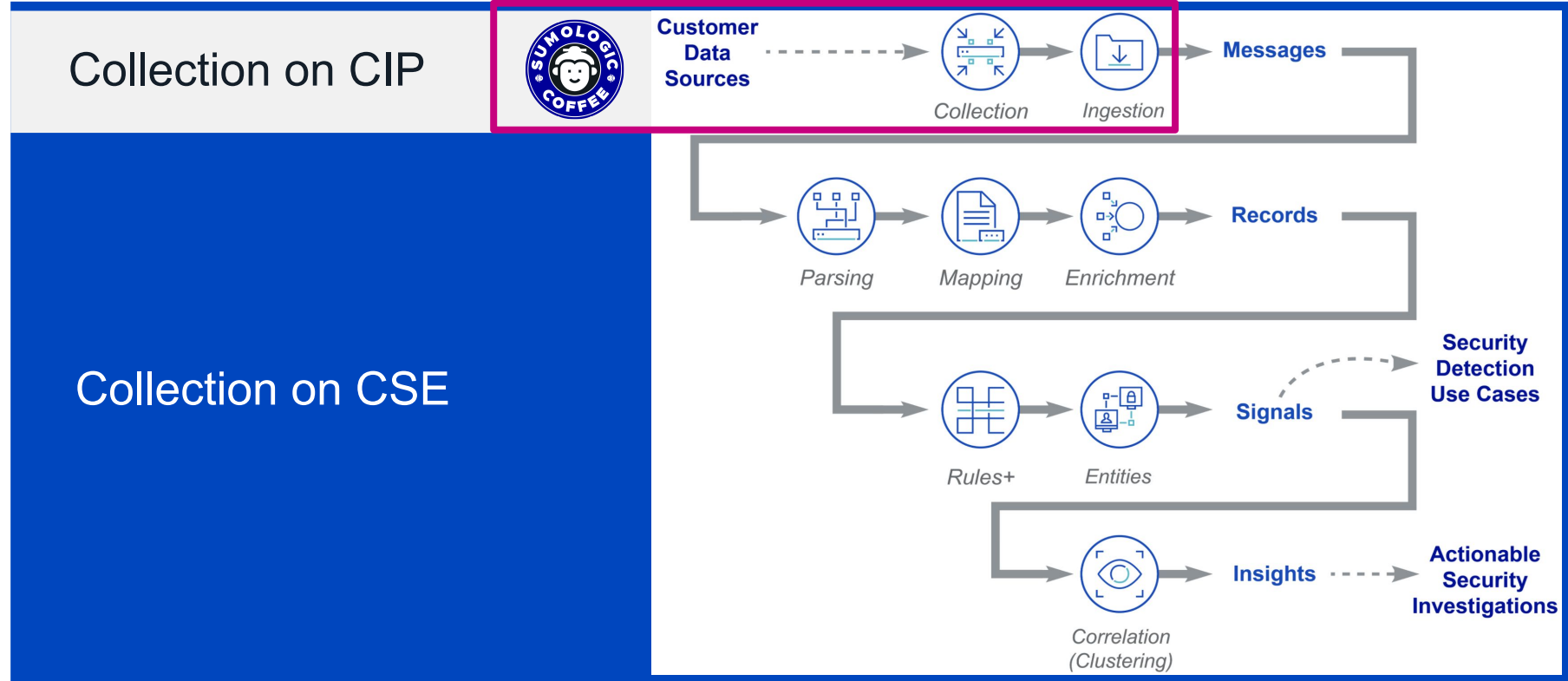
Kubernetes
Observability



Amazon Web
Services
AWS



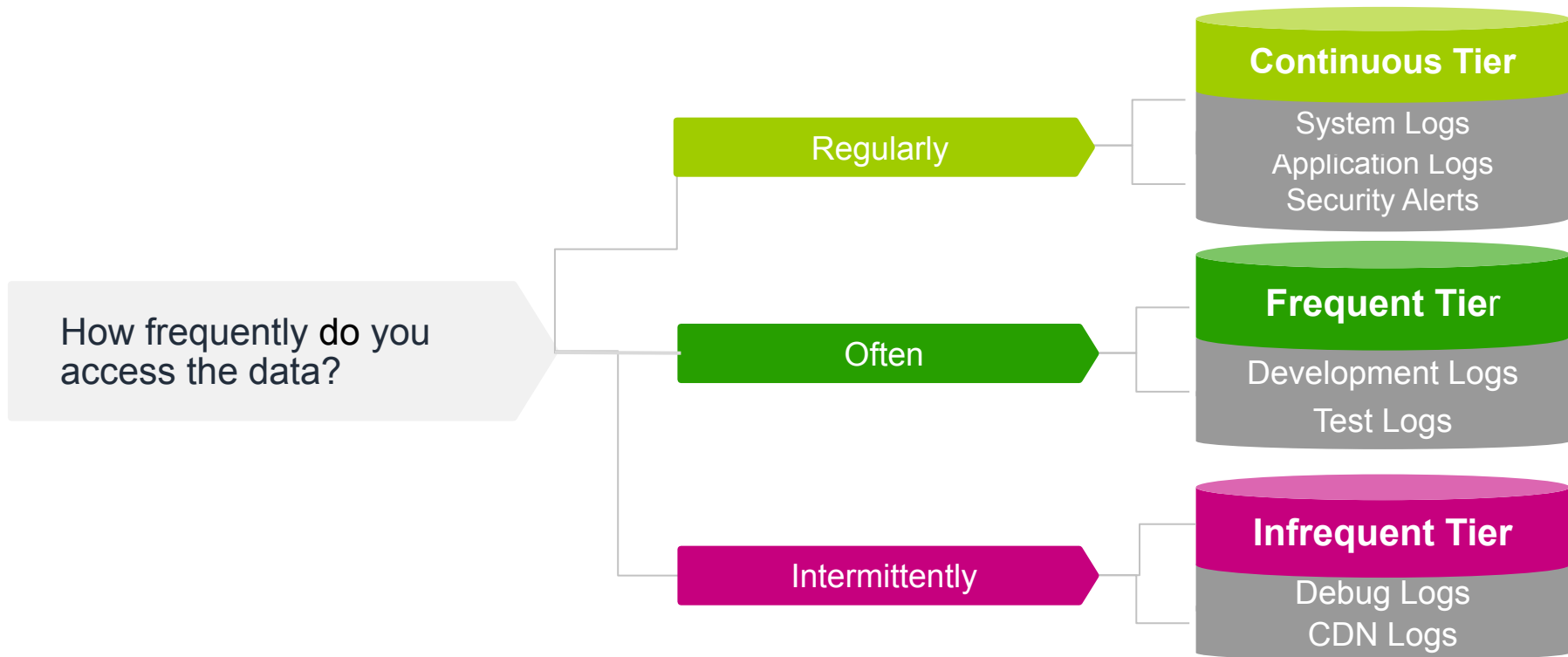
Ingesting data for Security



What is required for my business?

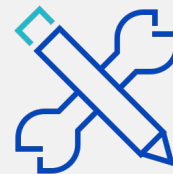
- Ability to slice and dice usage based on:
 - **Metadata:** Collector, Source Category, Source, Source Name, Source Host
 - **Data Types:** Logs, Traces, Metrics
 - **Tiers:** Continuous, Frequent, Infrequent

Which tier should I use?



Hands-on Lab

Using Sumo Logic Training Portal



Complete Lab 3: Exploring Data Tiers

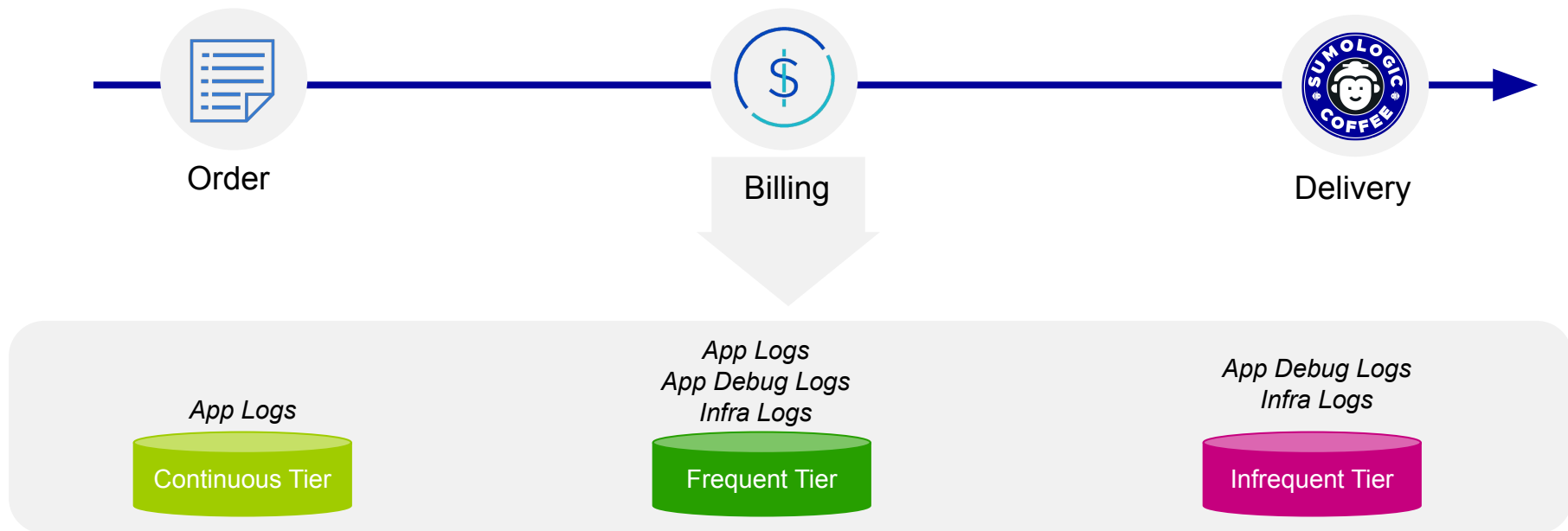
- Navigate to Manage Data > Logs > Partitions page
- Identify partitions
- Identify Data Tiers
- Click +New > Log Search > Basic Mode

Searching and Analyzing Data

- How is the data organized in Sumo Logic?
- Where do I search for my data?
- Perform a search using a query

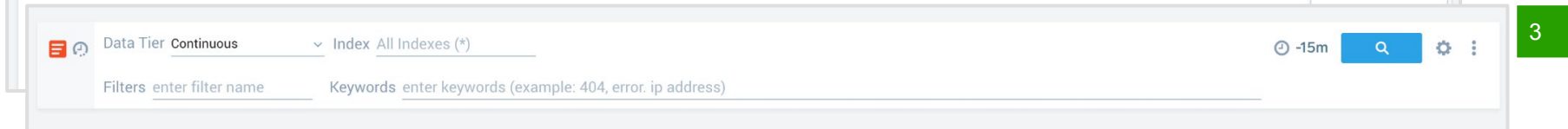
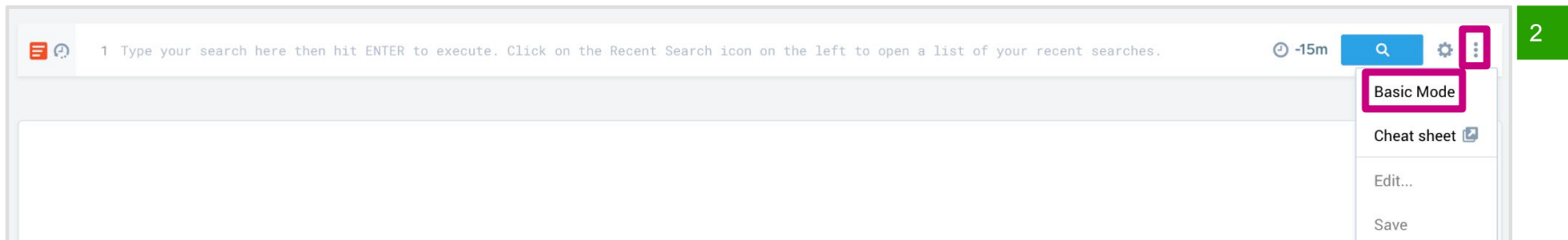
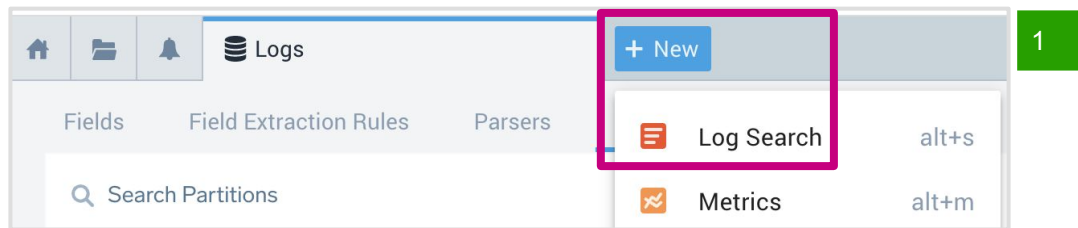


How is data organized?



Navigating to Basic Mode

1. Open a Log Search by clicking **+ New**, then select **Log Search**.
2. Click the three-dot icon on the right of the Search page and select **Basic Mode** from the menu options.
3. The user interface changes to show the simple query builder.



Logs Search Basic Mode

Recent Searches

Data Tier

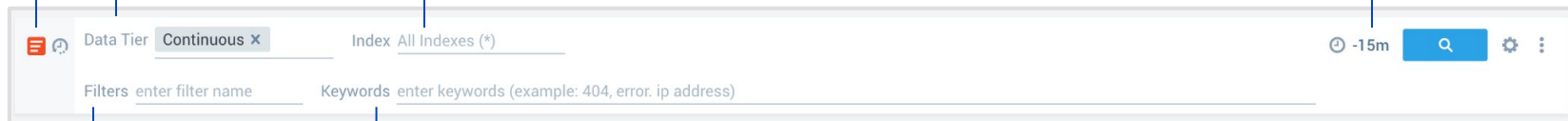
Select **Data Tier(s)** the query should run against

Index

Select **Partition(s)** the query should run against

Time Range

Set the desired range of time you want the search to run against



The screenshot shows the 'Logs Search Basic Mode' interface. At the top left, there is a 'Recent Searches' button. Below it, the 'Data Tier' is set to 'Continuous' and the 'Index' is set to 'All Indexes (*)'. On the right, the 'Time Range' is set to '-15m'. Below these, there are input fields for 'Filters' (with a placeholder 'enter filter name') and 'Keywords' (with a placeholder 'enter keywords (example: 404, error. ip address)'). A search button with a magnifying glass icon is located to the right of the 'Keywords' field. At the bottom left, the 'sumo logic' logo is visible.

Filters

Type in any metadata **Field** the query should run against (support all fields, metadata and custom)

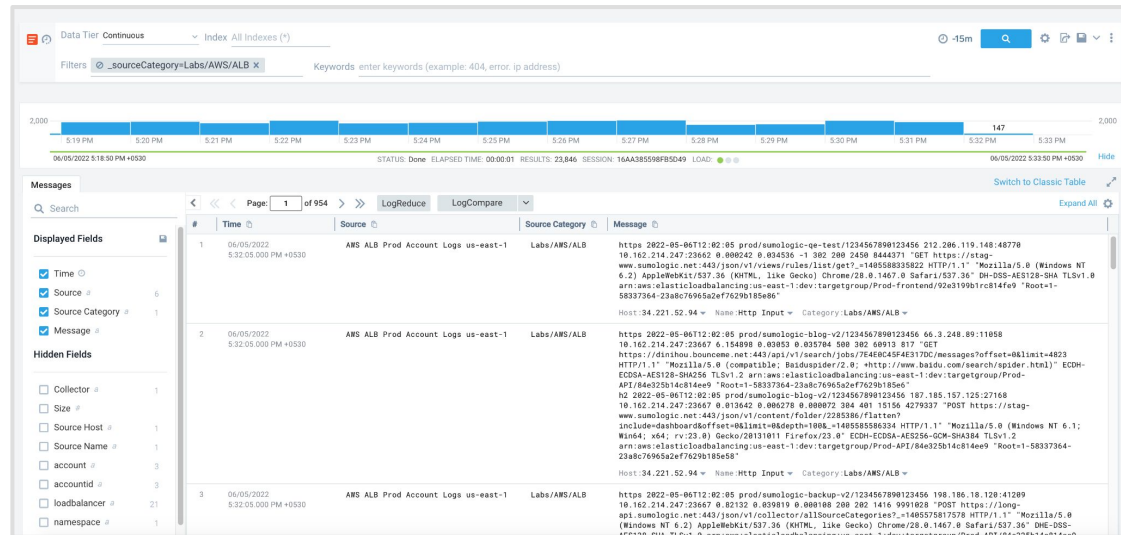
Filter logs using **Keywords**

Log Search

To investigate a **potential ongoing outage** on our **Amazon Web Services (AWS) Application Load Balancer (ALB)**.

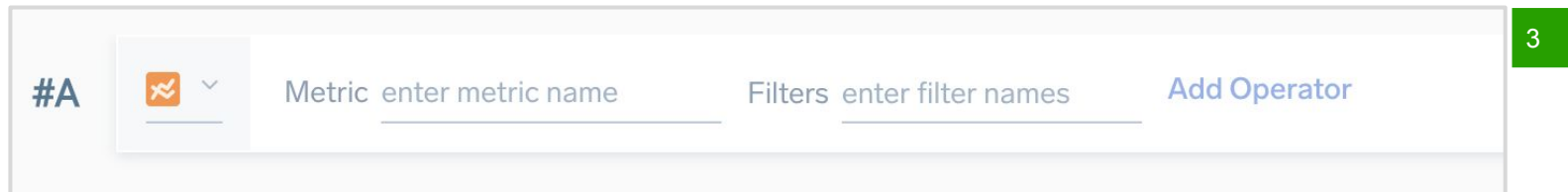
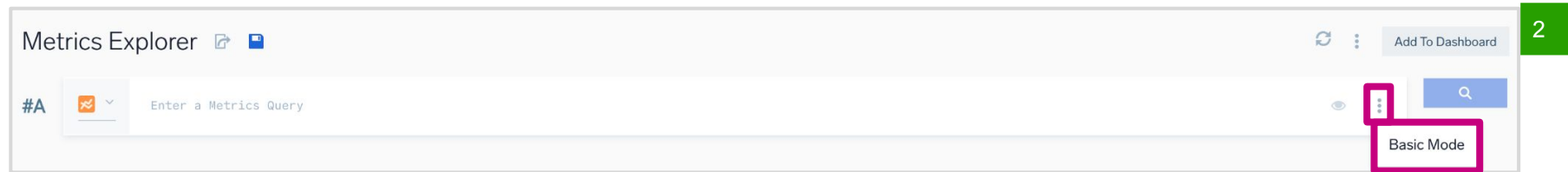
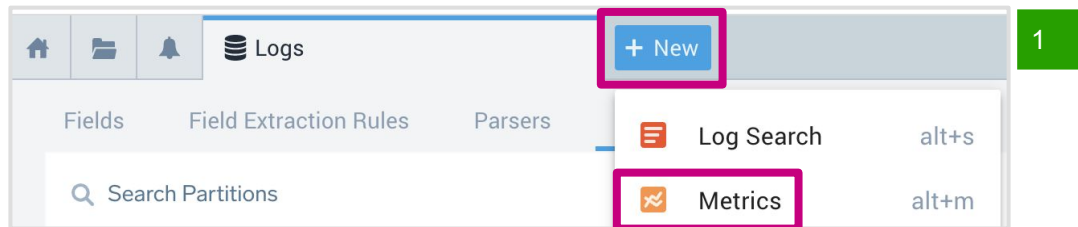
Select

- Data Tier=Continuous
- Source Category= Labs/AWS/ALB



Navigating to Metrics Explorer

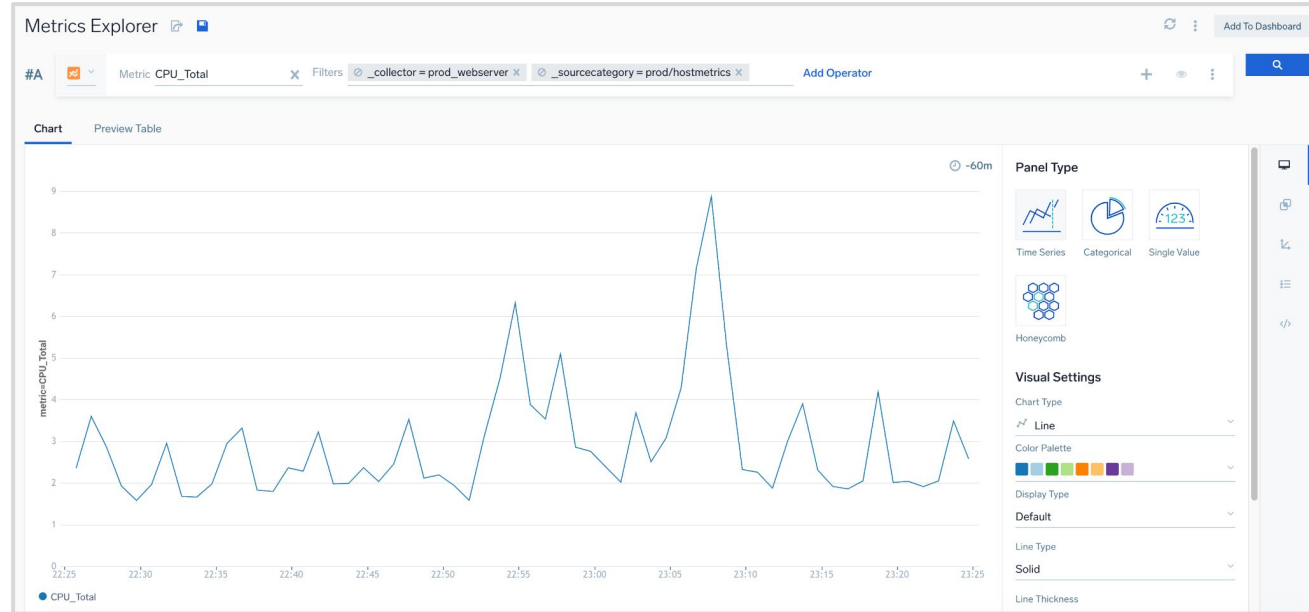
1. Open a Log Search by clicking **+ New**, then select **Metrics**.
2. Click the three-dot icon on the right and select **Basic Mode** from the menu options.
3. The user interface changes to show the simple query builder.



Metrics Search

Select

- Metric=CPU_Total
- _collector=prod_webserver
- _sourcecategory=prod/hostmetrics



Where is the data in Sumo?

Option 1 Explore your Collectors

Click **Manage Data > Collection > Collection**

Name	Health	Type	Status	Source Category	Sources	Last Hour	Messages
Admin-Training-SIEM	Healthy	Hosted			1	None	
BVT_Installed_Collecto...	Error	Installed			1	None	
cl-the-coffee-bar-traini...	Healthy	Hosted			11		20,459
client_ASA	Healthy	Installed			2	None	
connerlees-MBP	Healthy	Installed			1	None	
CSE	Healthy	Hosted		cse/windows/event	5		22
CSE-Lab-Data	Healthy	Hosted			2		715
CSE-Lab-Logger	Healthy	Installed			18		551
demo-cluster	Healthy	Hosted			11	None	
DESKTOP-E83CIAC	Error	Installed			None	None	

sumo logic

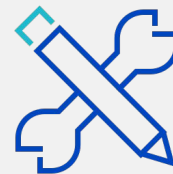
Option 2 Search for source categories

Click **+New > Search > Basic Mode**

#	Time	Collector	Source Category
1	20/04/2022 6:47:09 436 PM +0530	Labs - Apache	Labs/Apache/Error
2	20/04/2022 6:47:09 436 PM +0530	Labs - Apache	Labs/Apache/Error
3	20/04/2022 6:47:09 436 PM +0530	Labs - Apache	Labs/Apache/Error
4	20/04/2022 6:47:09 436 PM +0530	Labs - Apache	Labs/Apache/Error
5	20/04/2022 6:47:09 436 PM +0530	Labs - Apache	Labs/Apache/Error
6	20/04/2022 6:47:09 436 PM +0530	Labs - Apache	Labs/Apache/Error

Hands-on Lab

Using Sumo Logic Training Portal



Complete Lab 4: Data Searching

- Build a query in Basic mode.
- Parse and aggregate the results.
- Save the search results.

Parsing

- Extract meaningful fields to provide structure to your data
- Extract fields within a query manually and on an ad-hoc basis.

| **parse**

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](#)

LogReduce (R)

- To group messages together based on string and pattern similarity.
- To quickly assess activity patterns for things like a range of devices or traffic on a website.

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

The screenshot shows the LogReduce web interface. At the top, there are tabs for 'Messages' and 'Signatures', and a 'Switch to Classic Table' link. Below the tabs, there's a pagination bar showing 'Page: 1 of 1' and a 'LogCompare' dropdown. The main table has columns: '#', 'Count', 'Relevance', 'Actions', and 'Signature'. The 'Count' column is highlighted with a pink box. The table contains 13 rows of data, each representing a group of log messages.

#	Count	Relevance	Actions	Signature
7	24	5.00	👍 🗑️ 🔍 📄	2022-***** -*root - ERROR - Missing some ingredients - trace_id=* - *****
8	24	5.00	👍 🗑️ 🔍 📄	2022-07-22 12:***** * root - INFO - Coffee done (Preparation time: *.*ms)*- trace_id=* - span_id**
9	11	5.00	👍 🗑️ 🔍 📄	2022-07-22 12:***** * root - ERROR - Missing some ingredients - trace_id=* - *span_id=*
10	6	5.00	👍 🗑️ 🔍 📄	2022-07-22 12:***** - root - INFO - 192.168.***** - - [22/Jul/2022:12:***** +0000] "POST /get_coffee trace_id=***** - span_id=*****
11	4	5.00	👍 🗑️ 🔍 📄	2022-07-***** * root - ERROR - Missing some ingredients - trace_id=* - *span_id=*
12	2	5.00	👍 🗑️ 🔍 📄	2022-07-*** 12:00:00,*** - apscheduler.executors.default - INFO - Running job "*****" (trigger: interval (scheduled at 2022-07-*** 12:00:00+00:00) - trace_id=None - span_id=None
13	1	5.00	👍 🗑️ 🔍 📄	2022-07-*** 12:00:00,*** - root - INFO - Deploying new version 1.20.124

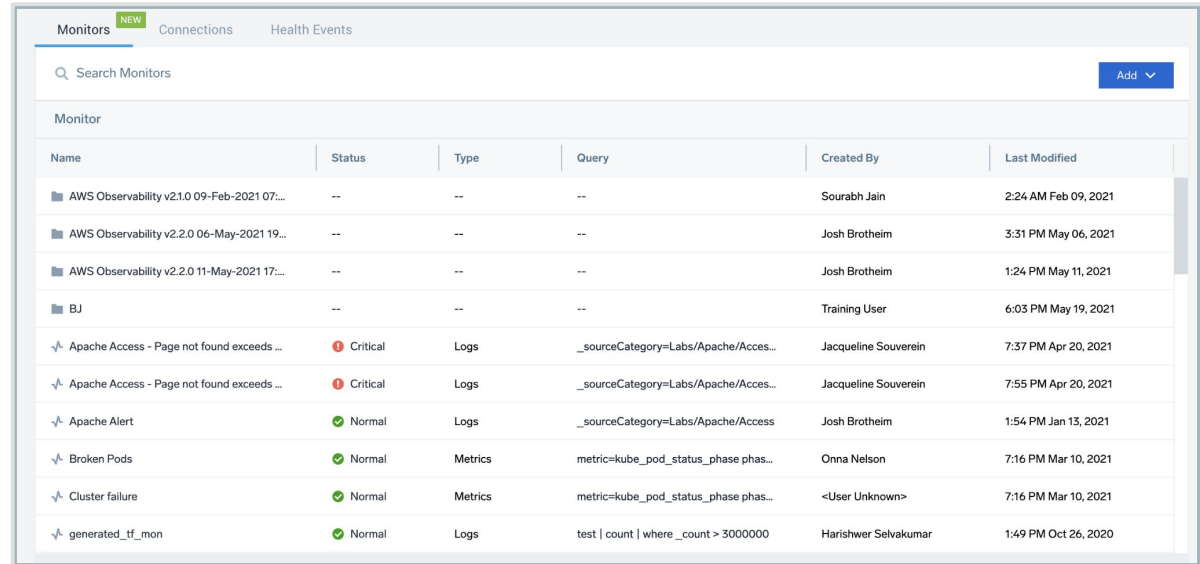
Monitoring and Visualizing Data

- Alert Response
- Context Cards for Troubleshooting
- Charts, Panels, Dashboards



Alert Response overview

- Find relevant details about triggered alerts
- Identify the root cause using Context Cards
- Quickly resolve the underlying issue



The screenshot displays the 'Monitors' tab in a dashboard. It features a search bar at the top and a table of monitors. The table has columns for Name, Status, Type, Query, Created By, and Last Modified. The first four rows show AWS Observability monitors with a status of '--'. The next six rows show various alerts with status icons (red for Critical, green for Normal) and specific queries or metrics.

Name	Status	Type	Query	Created By	Last Modified
AWS Observability v2.1.0 09-Feb-2021 07:...	--	--	--	Sourabh Jain	2:24 AM Feb 09, 2021
AWS Observability v2.2.0 06-May-2021 19:...	--	--	--	Josh Brotheim	3:31 PM May 06, 2021
AWS Observability v2.2.0 11-May-2021 17:...	--	--	--	Josh Brotheim	1:24 PM May 11, 2021
BJ	--	--	--	Training User	6:03 PM May 19, 2021
⚡ Apache Access - Page not found exceeds ...	🔴 Critical	Logs	_sourceCategory=Labs/Apache/Access...	Jacqueline Souverein	7:37 PM Apr 20, 2021
⚡ Apache Access - Page not found exceeds ...	🔴 Critical	Logs	_sourceCategory=Labs/Apache/Access...	Jacqueline Souverein	7:55 PM Apr 20, 2021
⚡ Apache Alert	🟢 Normal	Logs	_sourceCategory=Labs/Apache/Access	Josh Brotheim	1:54 PM Jan 13, 2021
⚡ Broken Pods	🟢 Normal	Metrics	metric=kube_pod_status_phase phas...	Onna Nelson	7:16 PM Mar 10, 2021
⚡ Cluster failure	🟢 Normal	Metrics	metric=kube_pod_status_phase phas...	<User Unknown>	7:16 PM Mar 10, 2021
⚡ generated_tf_mon	🟢 Normal	Logs	test count where _count > 3000000	Harishwer Selvakumar	1:49 PM Oct 26, 2020

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

Alert Response - Context Cards

Log
Fluctuation



Identify changes in Log patterns/signatures that might help explain the underlying issue

Anomaly



Find anomalies in metrics data reported by various related entities over time

Dimensional
Explanation



Analyze app log data and surface dimensions that might explain the alert condition

Benchmarks



Surface abnormalities in data reported by various entities when compared with other Sumo cohort

Alert Response - Troubleshooting

sumo logic

Critical

Monitor Name

Shipping - GetQuote Request Drop

View Monitor

Trigger Condition

_count is greater than or equal to 3.0 standard deviations from baseline 1792.5

Time Range

08/17/2021 04:49:56 PM PDT to 08/18/2021 04:49:56 AM PDT

Message

View Alert

Monitor Query

cluster="icp" [GetQuote] received request | timeslice 15m | count by _timeslice | outlier _count window=48,threshold=3.0,consecutive=1,direction=-

Log Messages

View All Logs

#	Count	Count_error	Count_indicator	Count_lower	Count_mean	Count_std
1	1327	-465.5	1.0	1658.68319922292	1792.5	44.6056002

Resource Usage Monitor

Critical

Active

Last updated about 1 hour ago

Refresh

Alerts

Resolve

Description

Triggers when Greater than or equal to 3.0 standard deviations from baseline 2.23

ID

Created

Duration

Trigger Value

000000000000B566

03:57:51 PM Aug 04, 2021

about 1 hour

1.43

L

_sourcecategory=alert metric=CPU_Sys _sourceHost=nite-alert-1 | outlier window=5m threshold=3.0 direction=+-

Open Triggered Query

Time series

N

CPU_Sys

{ AccountId="246946804217", AvailabilityZone="us-west-1b", Cluster="alert", Deployment="nite", DistributionCodeNs

Related Alerts

Monitor History

Last 30 Minutes

43 alerts

Time

Entity

Showing 31 alerts related by time

[46361] michal_entities_05

03:36:36 PM Aug 04 (about 1...

[46427] TestMonitorAnu1

03:44:29 PM Aug 04 (about 1...

[46356] KA SUMO-166901

03:32:15 PM Aug 04 (about 1...

[46366] steven outlier test 00...

03:43:21 PM Aug 04 (5 minu...

[46432] ICP-Anamies-1-e2l

03:45:16 PM Aug 04 (about 1...

[46360] mpacholczyk-test

03:37:06 PM Aug 04 (about 1...

[46420] Test Vasu

Monitoring - Alerts

Scheduled Searches trigger Alerts when a condition is met.

 **incoming-webhook** APP 5:33 PM Today ▾

Critical Alert: Coffee prep time increase (prod)

Alert URL
<https://live.us2.sumologic.com/ui/#/alert/0000000000416392>

Description

Trigger Time
08/16/2022 05:33:45 PM IST

Time Range
08/16/2022 05:26:45 PM IST to 08/16/2022 05:31:45 PM IST

Trigger Condition
_latency_pct_95 is Greater than 1.0 in the last 5 minutes

Trigger Value
3.11329

Query
cluster=sedemo-prod namespace=warp003* | parse "Coffee preparation request time: * ms" as latency nodrop | if(isBlank(latency), "false", "true") as hasLatency | if(isBlank(latency), 0.0, latency) as latency | latency/ 1000 as latency | pct(latency,95) by hasLatency | where hasLatency = "true"

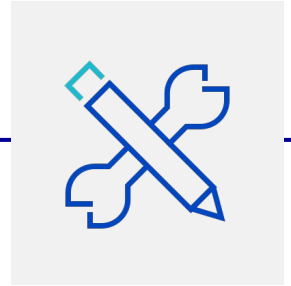
Alert Types:

- Email
- Webhook
- Save to Index
- Script Action

 AWS Lambda	 Azure Functions	 Datadog
 HipChat	 New Relic	 PagerDuty
 Service Now	 Slack	 Webhook

Hands-on Lab

Using Sumo Logic Training Portal



Complete Lab 5: Data Monitoring

- Create an email alert

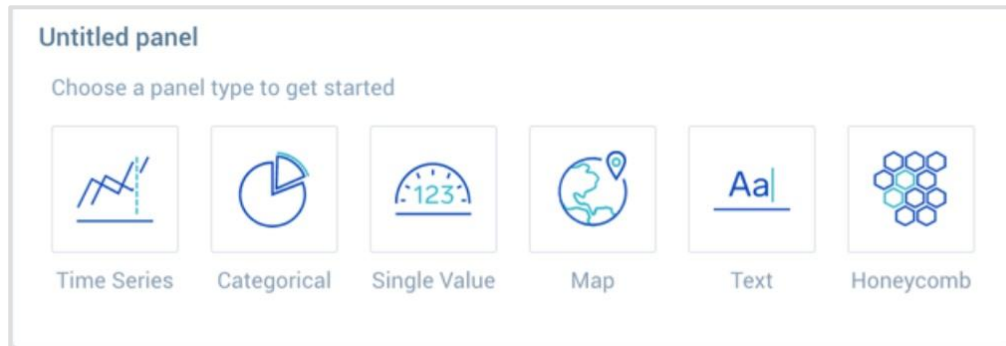
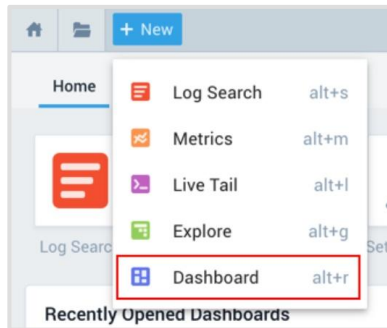
Dashboards, Charts, Panels

Visualization



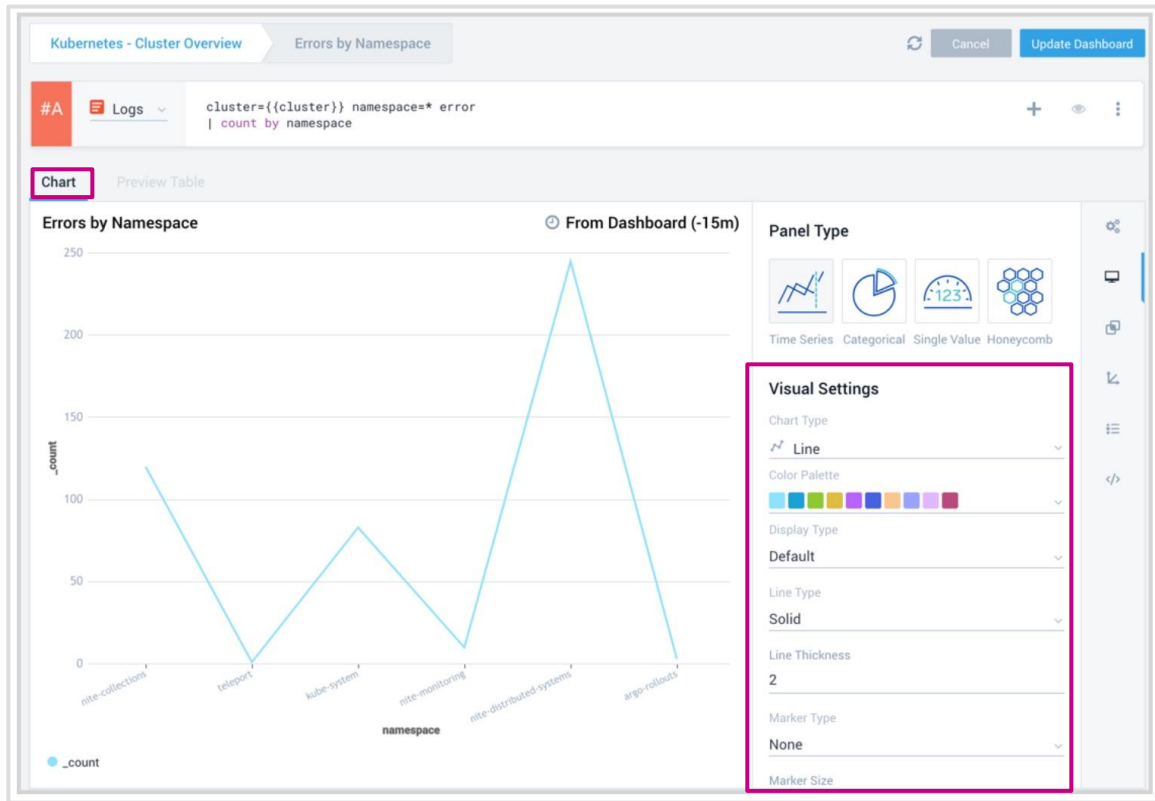
Panels

- **Panels** are the building blocks used to create a dashboard.
 - Time Series
 - Categorical
 - Single Value
 - Map
 - Text
 - Honeycomb



Charts

- Edit/Modify the **Chart** type to analyze the data in another format.
 - Area, Bar
 - Column, Line, Table

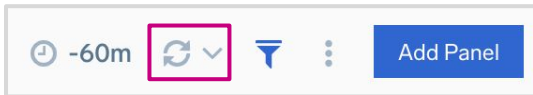


Dashboards

- Select **Time range** to view data for the corresponding panel



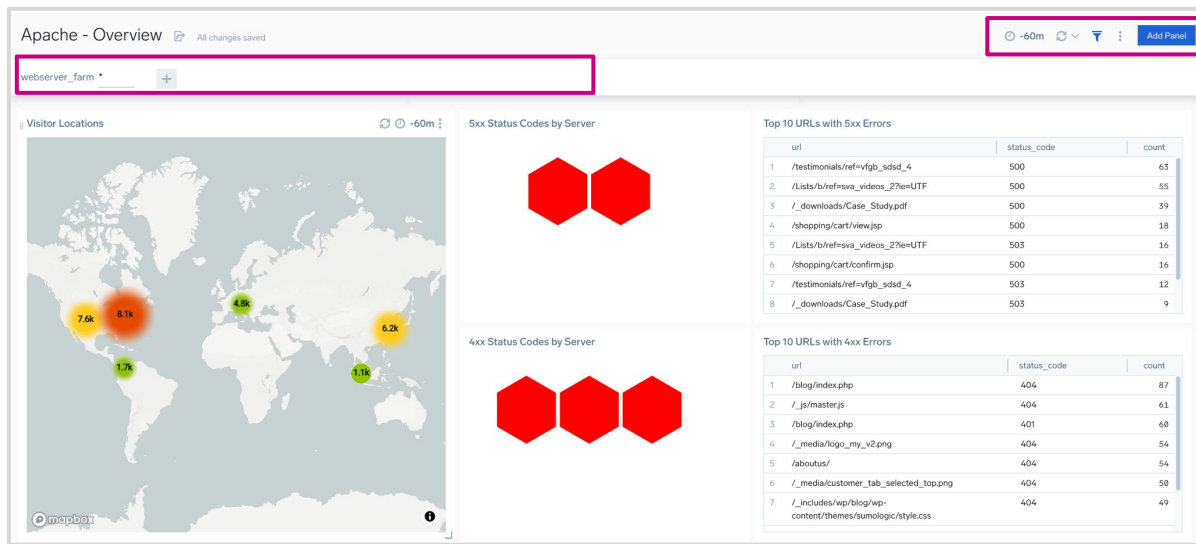
- Auto Refresh:** Ability to configure the refresh interval rate



- Ability to add panels inline through **Add a Panel** button

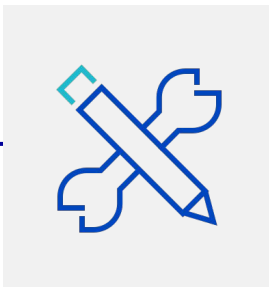


- Each **Panel** processes results from a single search.
- The variables work across both log and metric panels.



Hands-on Lab

Using Sumo Logic Training Portal



Complete Lab 6: Data Visualization

- Create and modify a chart.
- Create, share, modify a dashboard.
- Create a panel and add it to a dashboard.
- Add a text panel.

Quick recap



1. Demo a use case to familiarize you with our capability
2. Learned what data is available and where to find it
3. Learned to search using basic mode and analyze data
4. Learned to do trending analysis and monitor critical events

Next, we continue to get “Fundamentals Certified”

What's next?

This is just the beginning of your Sumo journey!

1

Get certified!

Take the
Fundamentals Exam

2

Take more classes!

Self-paced
Fundamentals,
Administration,
Search Mastery
courses

3

**Join the
community!**

Sumo Logic user
group on LinkedIn

Resources

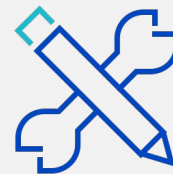
Training, Docs, Community, Support

sumo logic



Hands-on Lab

Using Sumo Logic Training Portal



Complete Lab 7: Get Help

- Get Help with Sumo Logic
- Check out the Release Notes
- Search DocHub
- Visit the Learn Page in Sumo
- Post a question on the Sumo Community
- Try our Customer Slack channel
- Log a Support Ticket

Hands-on Lab Guides

1. Click **Home > Certification > Get Certified**
2. Select **Recorded Live Training**
3. Select **Fundamentals Cert Jam**
4. Click **Register**

Welcome to the Sumo Logic Training Portal



Become a Sumo Logic Expert

Expand your knowledge with self-paced classes on Sumo Logic. Then, become an expert in Observability or Security.



Learn a New Skill

Learn Sumo Logic skills on-demand. Quick tutorials, best practices, and short demos perfect for busy remote workers.



Recorded Live Training

Watch recordings of live, instructor-led sessions! You can also download supporting materials, like lab guides, here.



Get Certified

Whether you're a new or experienced user, a Sumo Logic certification can help you demonstrate your skills in our platform.



sumo logic
Training



Fundamentals Cert Jam

Supporting materials for the Fundamentals Cert jam attendees

FREE 120 min



Administration Cert Jam

Supporting materials for the Administration Cert Jam attendees

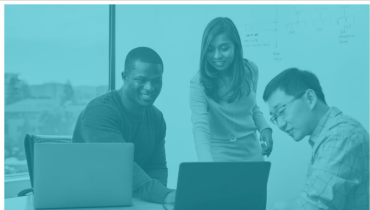
FREE 120 min



Search Mastery Cert Jam

Supporting materials for the Search Mastery Cert jam attendees

FREE 120 min



Fundamentals Cert Jam

Supporting materials for the Fundamentals Cert Jam attendees

[Register](#) | [FREE](#)

About this course

Are you attending or have attended a Fundamentals Cert Jam delivered by an instructor.

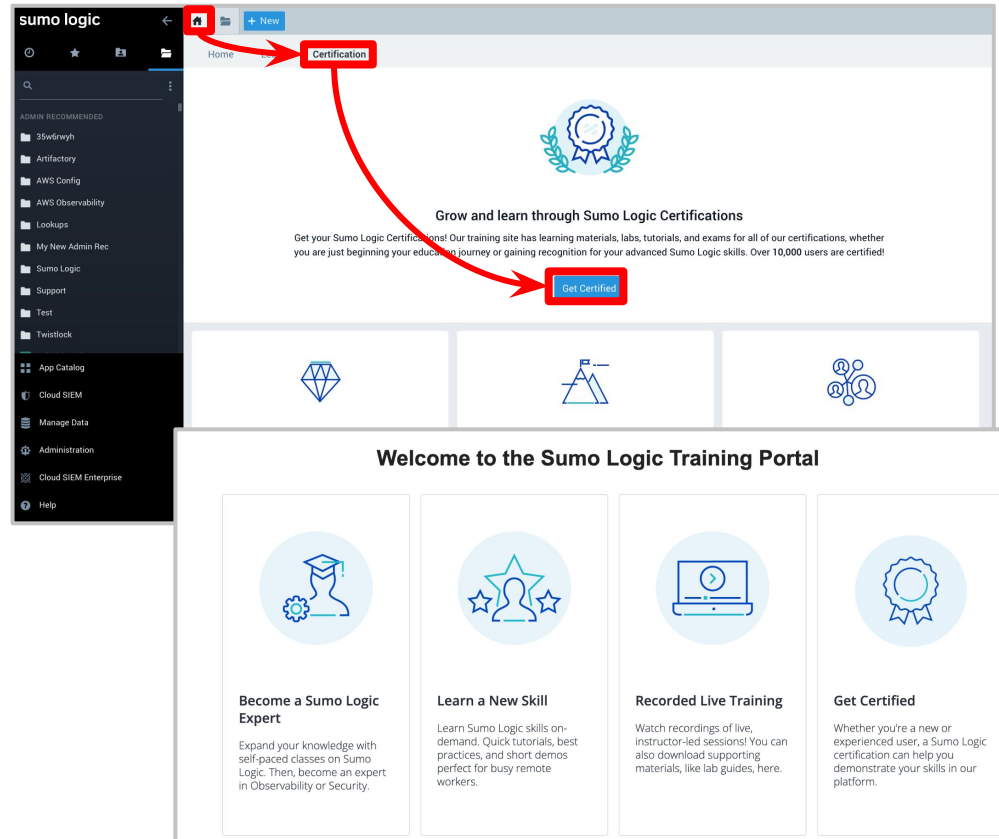
Find here a copy of the slide set, the student lab guide, and other material made available during class.

Certification

In order to get credit for the exam, go to **your own Sumo account and login** (your company account, not the training account)

Assessment:

1. Click  > **Certification** > **Get Certified**
2. Click **Get Certified**
3. Click <course name>
4. Click **Register | FREE**
5. Under **Read Me First**, click **Before you start**
6. Click **Next**
7. Click **START ASSESSMENT**



Assessment description

- 30 questions
- 60 minutes to take it
- Need a 75% to pass
- 3 Attempts
- Open Resource (slides, labs, and documentation)



sumo logic

 **sumo logic**
Training

 Fundamentals Exam Gain broad knowledge analyzing logs and metrics with the Fundamentals Certification. FREE 61 min	 Administration Exam Demonstrate your knowledge of Sumo Logic Administration FREE 61 min	 Search Mastery Exam Demonstrate your knowledge of Sumo Logic Search basics FREE 61 min
--	---	--

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

- In the black left bar, click **Help**
- Click **Community**
- An email verification should be sent to your inbox
- Once you verify, you should be able to take the exam without any issues



Help

Documentation

Support

Feature Requests

Community 

Privacy Policy

Release Notes

Shortcuts

Service Status

In order to get credit for the assessment

Follow these steps:

1. After each section, click **Next** or **Submit**.
2. When you get to the last section, click **Go to results**.
3. When you passed the class, you'll get a congratulations message. Then click **Submit results**.
4. After your feedback, you can click **Close course**.

Sumo Logic Fundamentals Exam

sumo logic

00 : 57 : 44

how can you find out what logs might have been ingested?

☐ Review your Manage Data > Settings page

☐ Review your Administration > Account page

☐ Run the following search:
sourceCategory=All

☐ Review your Manage Data > Metrics

☒ Review your Manage Data > Logs

SUBMIT ALL ANSWERS

Sumo Logic Fundamentals Exam

sumo logic

Congratulations, Nelson, Onna!

The course is passed!

27 out of 30 questions correct
▼ Hide detailed results

Your score

75% 90%

Close course

For passing the exam, you will earn:

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



Thank you

sumo logic

s

u

Empowering the
people who power
modern business

m

o