Become a

Sumo Generalist

Fundamentals Certification

sumo logic

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: A cloud-native data analytics platform

Sumo Logic: A cloud-native machine data analytics platform

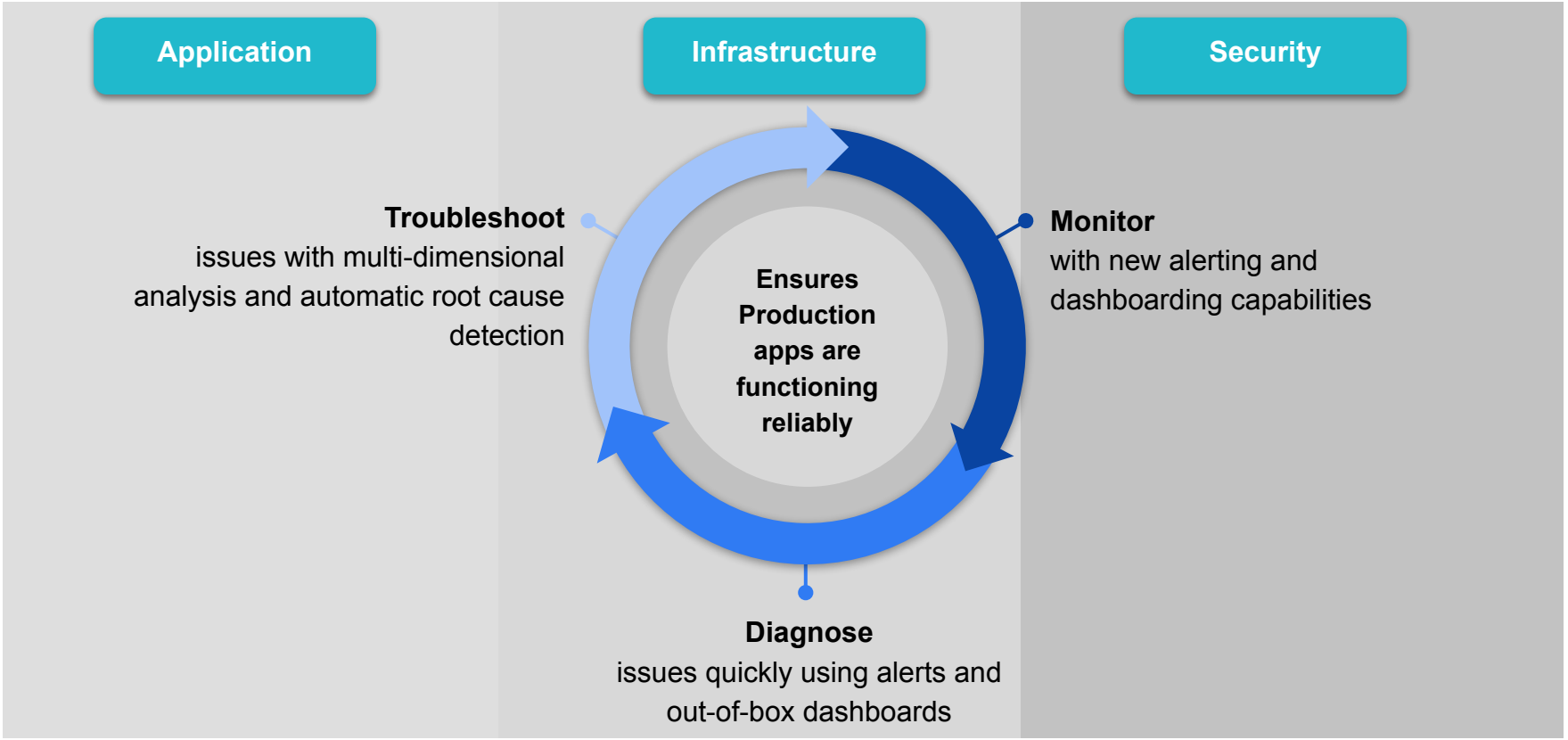
Security

Operations

Business Intelligence Use Cases

- Microservices
- Hybrid-cloud Environments
- Multi-cloud Environments

The Observability solution

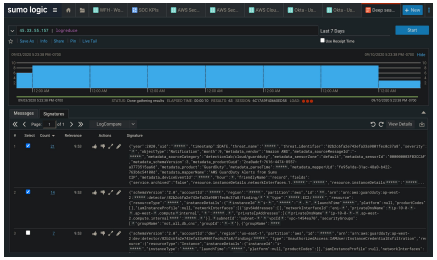


The Security Solution

Cloud Security Monitoring + Analytics

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

Audit & Compliance

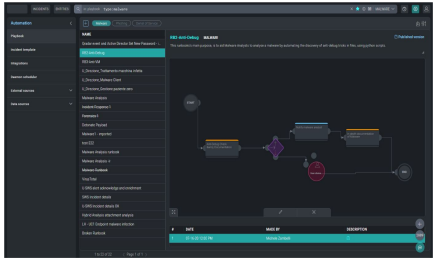


Determine compliance and posture management

Cloud SIEM

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

Cloud SOAR

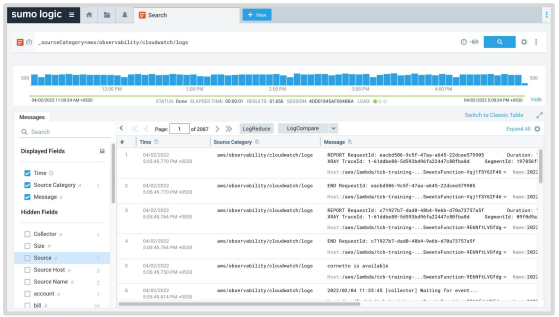


Improve SOC efficiency with progressive automation, orchestration, insightful decision-making

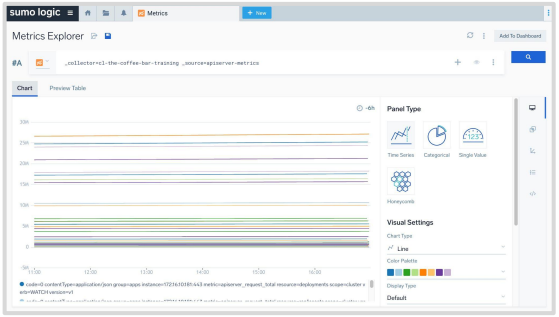
sumo logic

What kind of data does Sumo Logic ingest?

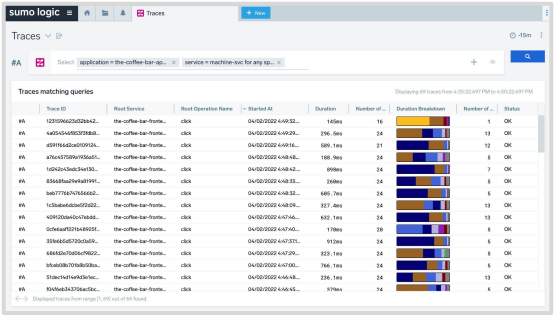
Logs
to identify why it's happening



Metrics
to identify what's going on



Traces
end-to-end visibility into user transactions across services



sumo logic

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

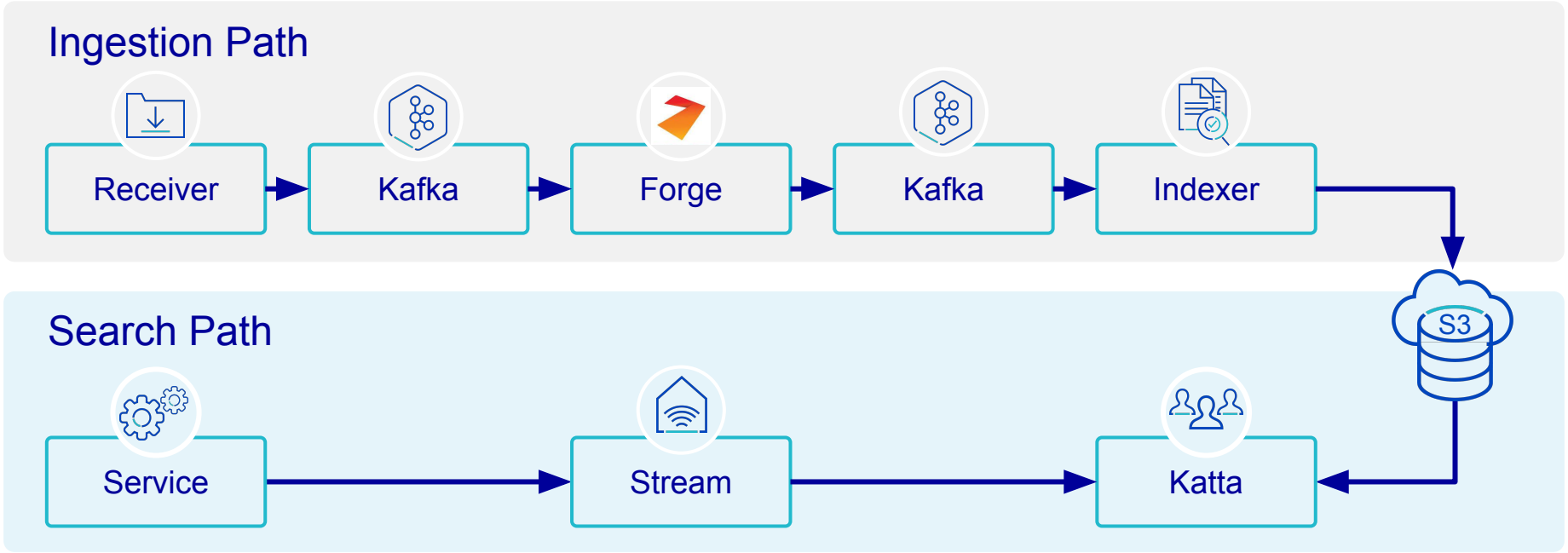
Microservices

- 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



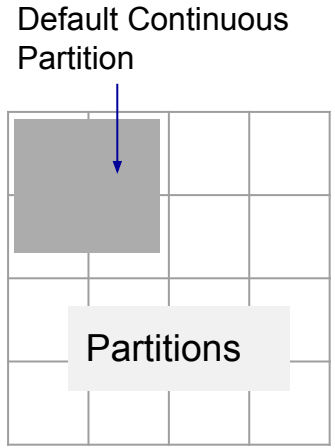
How is the data organized in Sumo Logic?

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



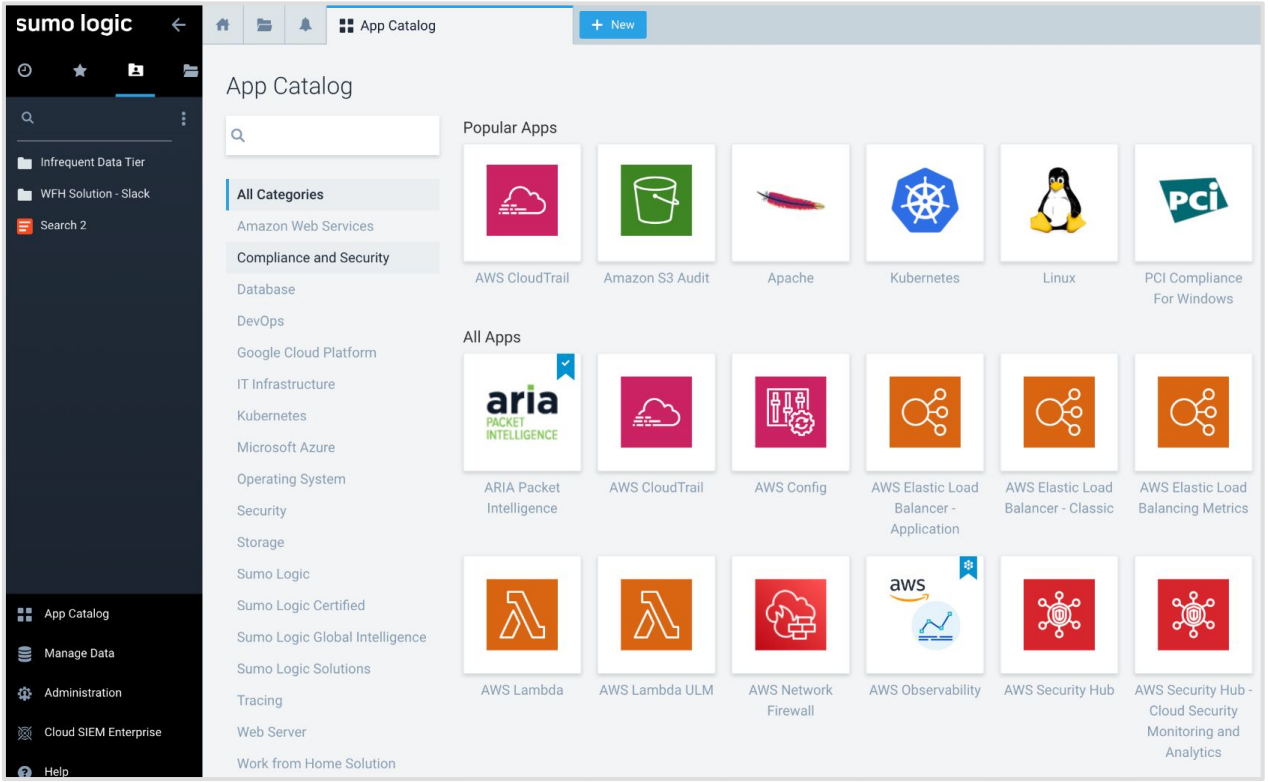
Manage Data > Logs > Partitions

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

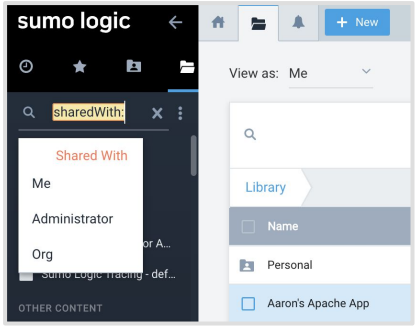
Taking advantage of App Catalog

- 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

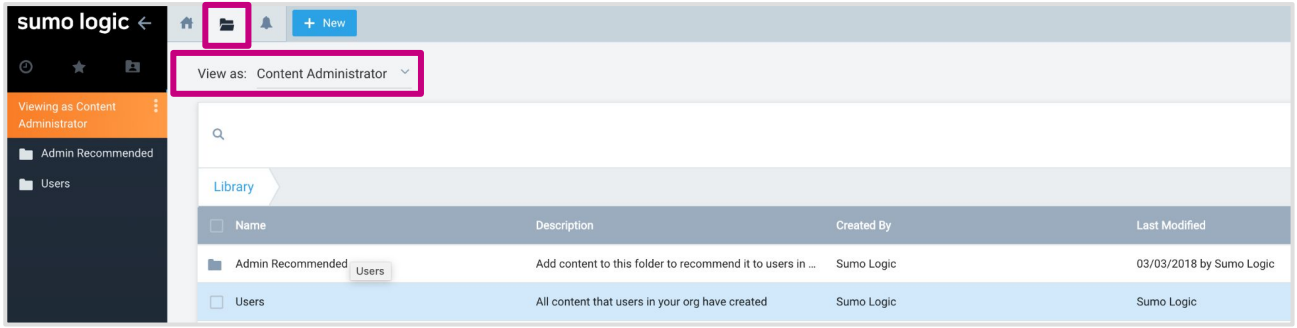


For All Users

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

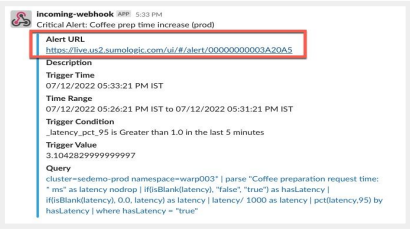
For Admin

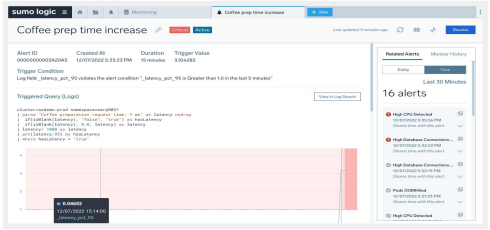
Manage content to specific users and groups.

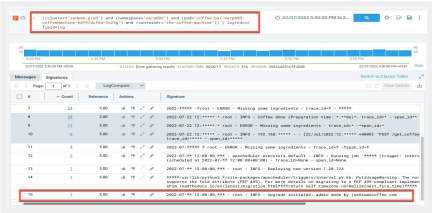


Select the **Library** Tab, under View as: Toggle to **Content Administrator** mode.

Demo: Let's See Sumo Logic in Action!

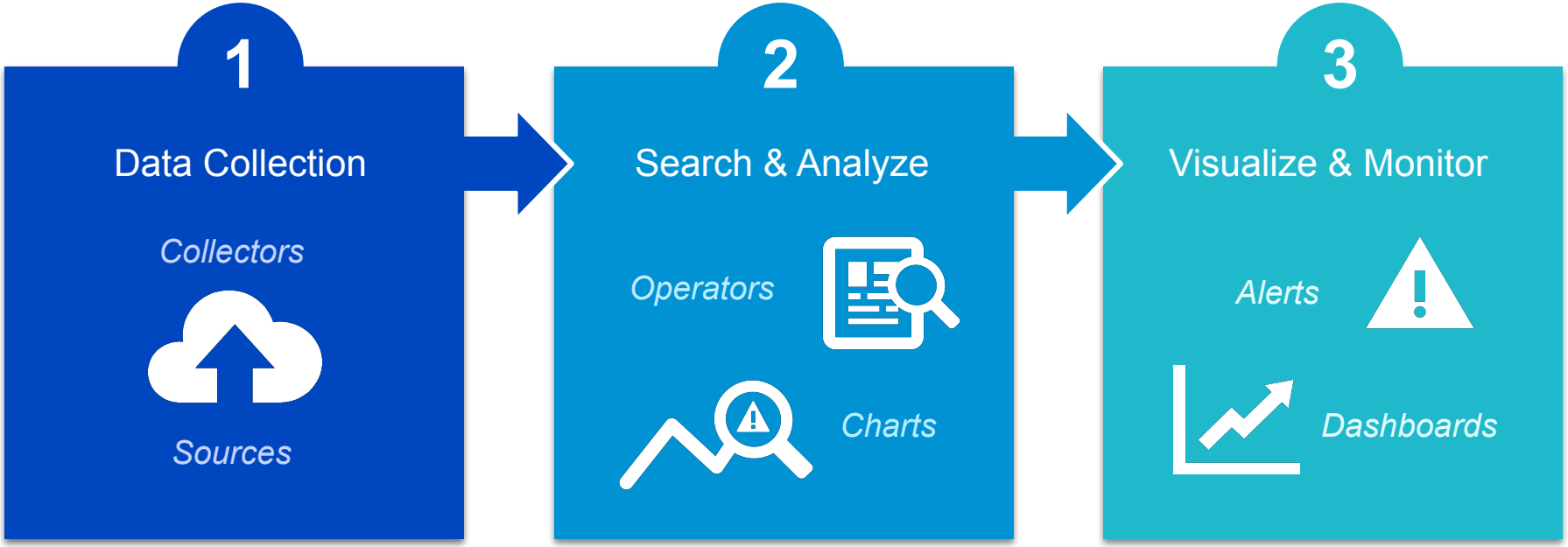






Slack Message → Alert Response → Dashboard → Log Search

Sumo Logic Data Flow



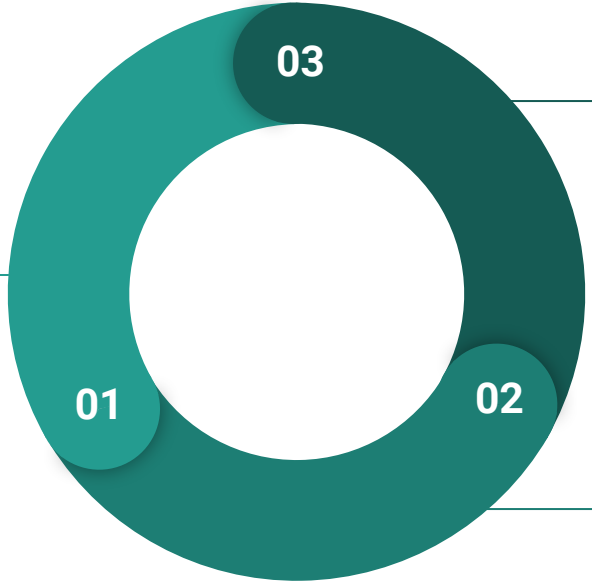
Data Collection

- 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



Where does the data reside?

Environment, Infrastructure, Files, People

`<prod> <uat> | <aws> <win> <devops> <superuser>`

What do you want to know?

Performance, Numbers, Errors, Success rate

`<errors> | <success%>`

What are the resources available to you?

Money, Time, Expertise

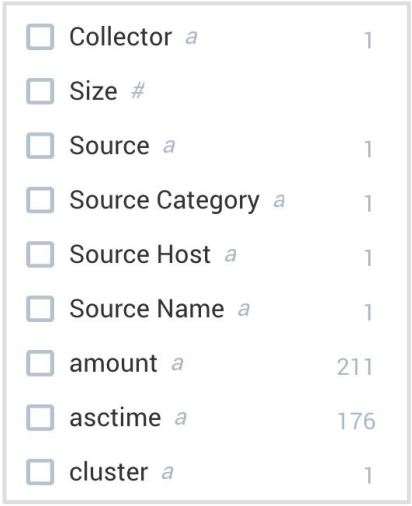
`<credits> | <totaltime>`

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

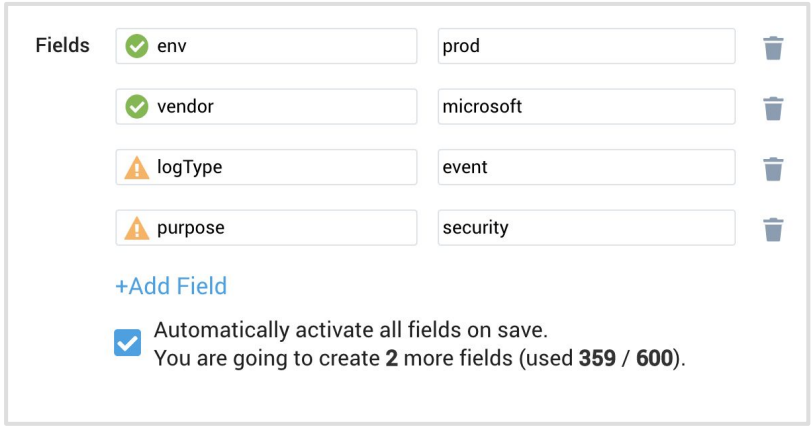
Tag	Description
`_collector`	Name of the collector (defaults to hostname)
`_sourceHost`	Hostname of the server (defaults to hostname)
`_sourceName`	Name and Path of the log file
`_source`	Name of the source this data came through
`_sourceCategory`	**Can be freely configured. Main metadata tag (e.g. labs/apache/access)**



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



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

`Prod/Web/Apache/Access`

`Dev/DB/MySQL/Error`

`Web/Apache/Access/Prod`

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

Collectors

sumo logic

Types of Collector

Installed Agents

Installed Collector

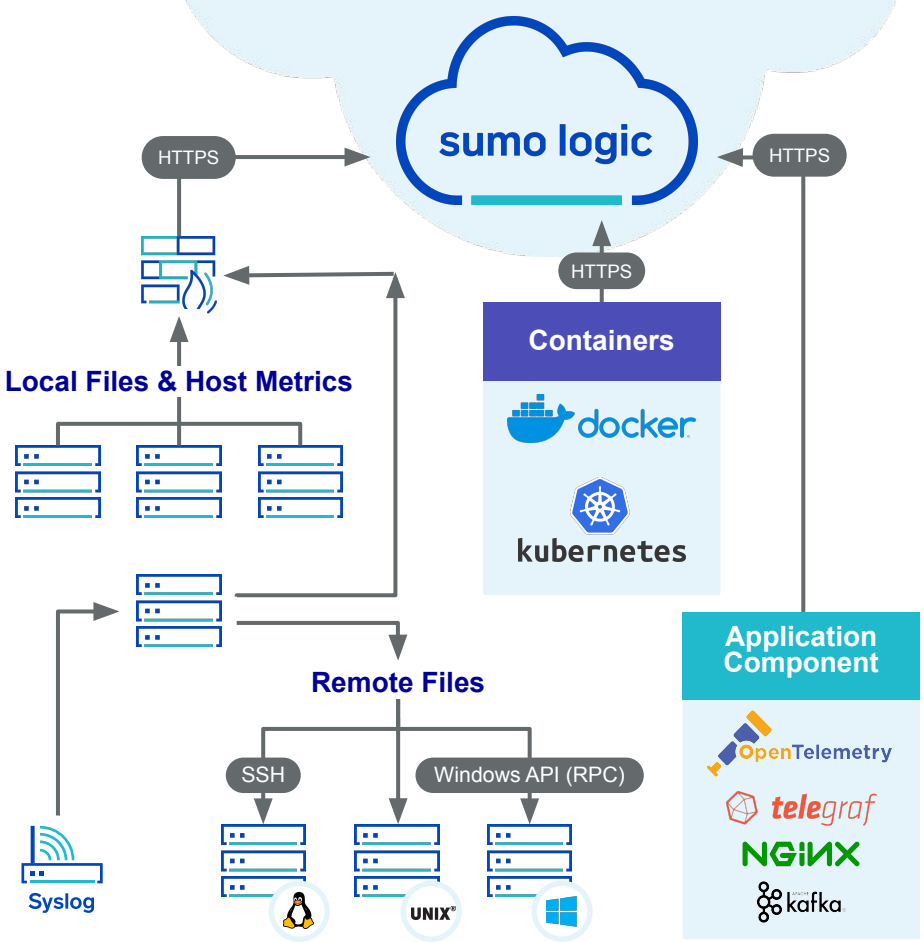
- Is installed on a system within your deployment locally or remotely
- Sources collect data available in your deployment
- Easy to troubleshoot based on Collector logs

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



Installed Agents

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

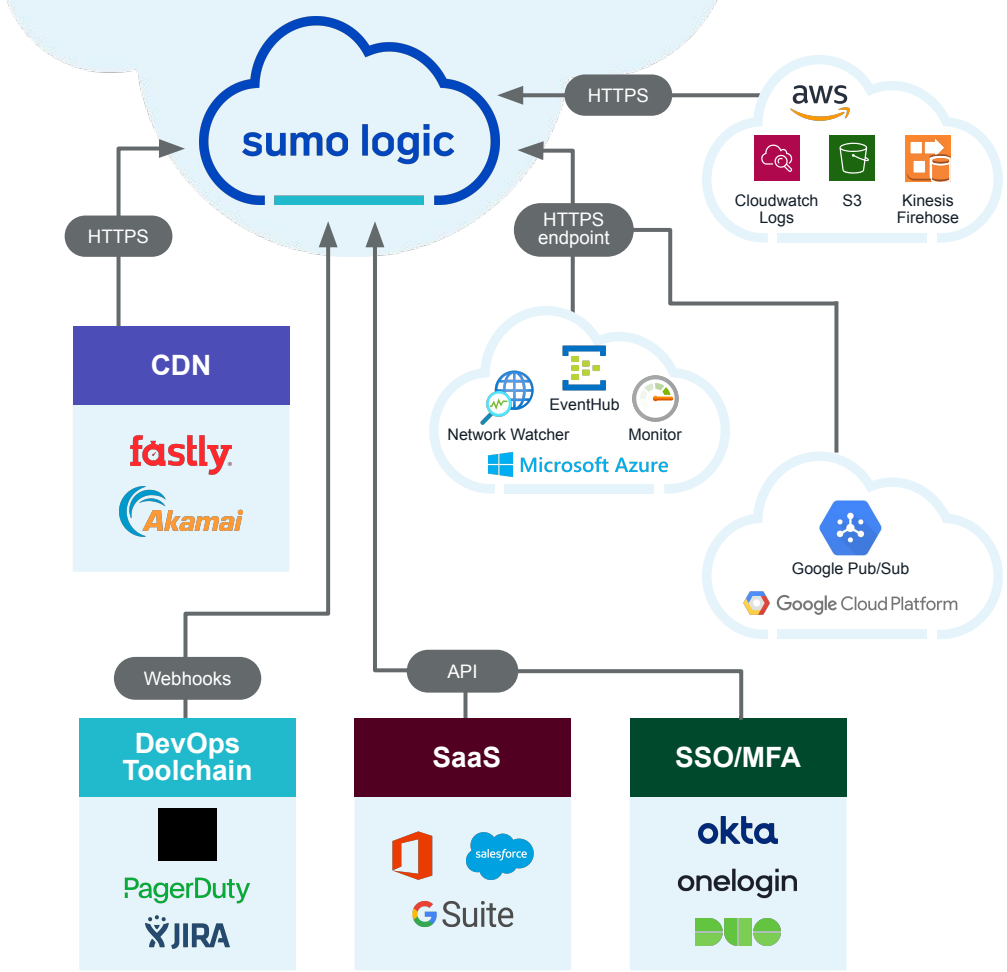
- Expect the Collector to ingest from at least 500 separate files.
- Hardware has memory or CPU limitations.
- Expect combined logging traffic for one Collector to be higher than 15,000 events per second.
- Network clusters or regions are geographically separated.
- Prefer to install many Collectors,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

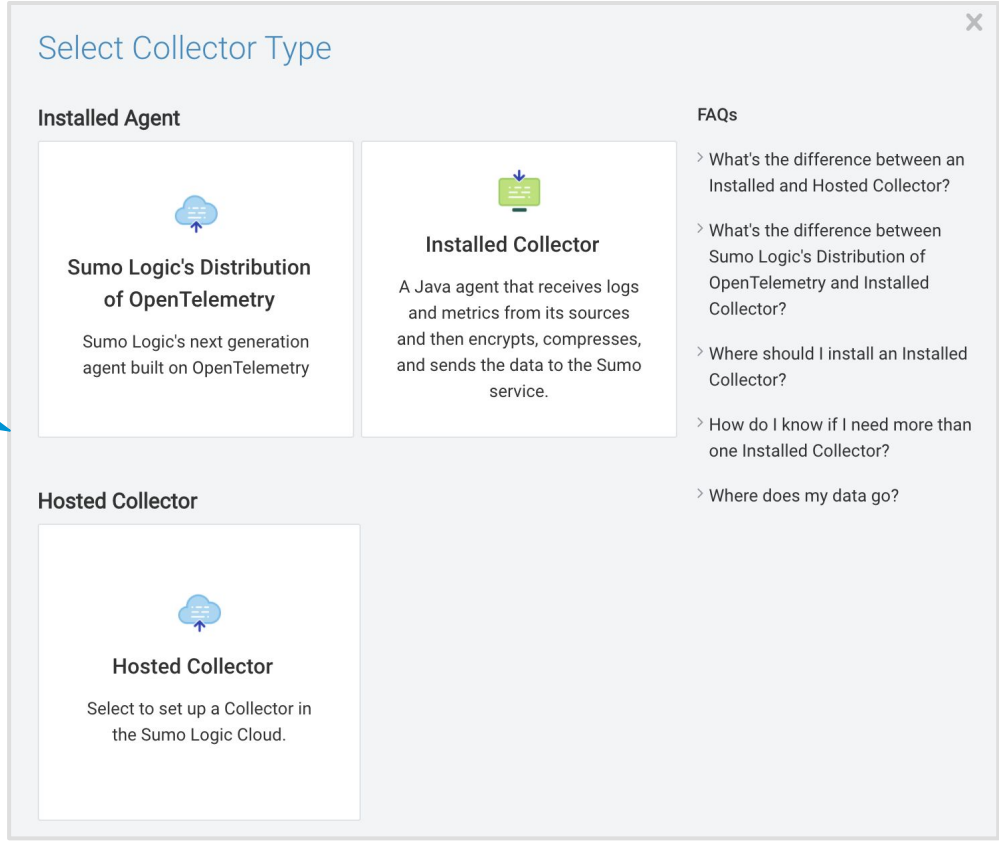
Hosted Collector

- 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?



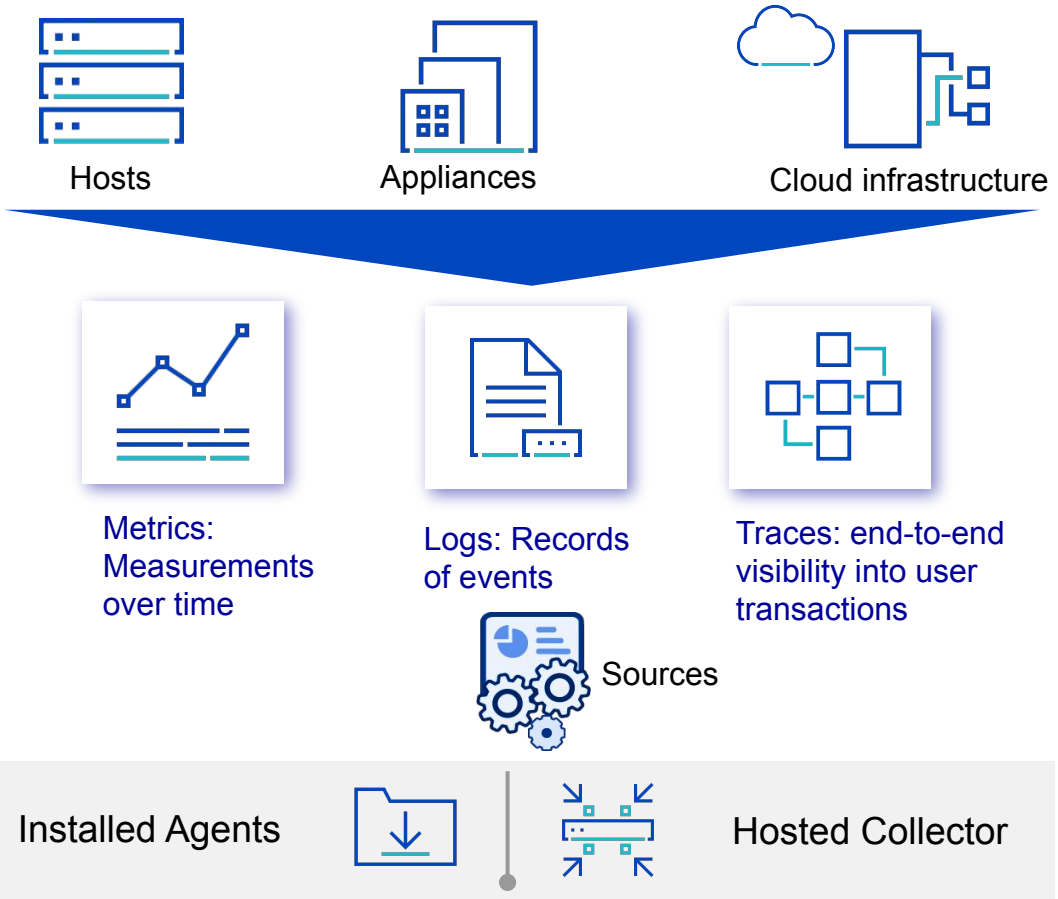
Sources

sumo logic

What is a Source?

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

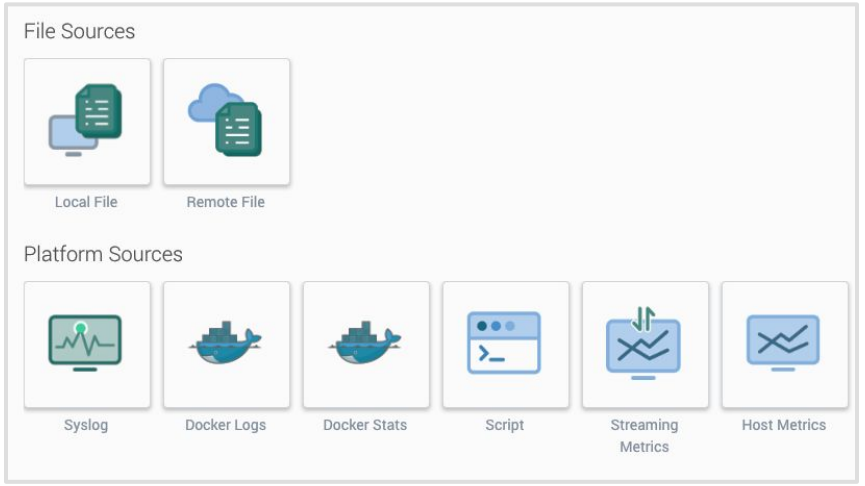


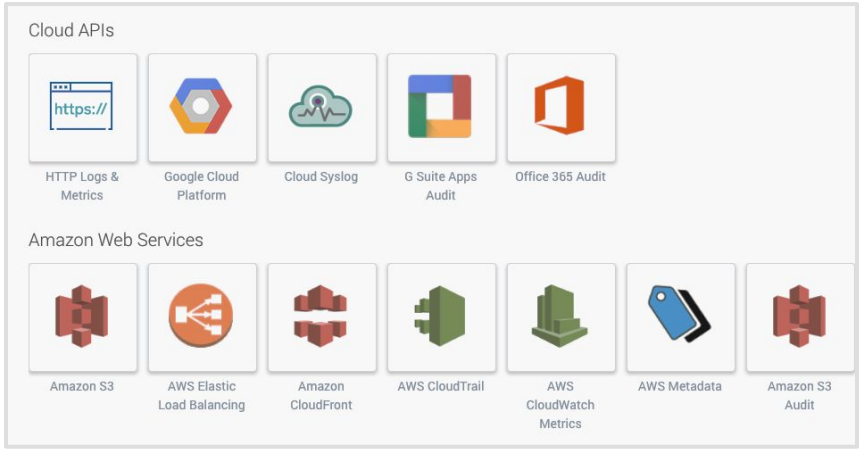
Types of Sources

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

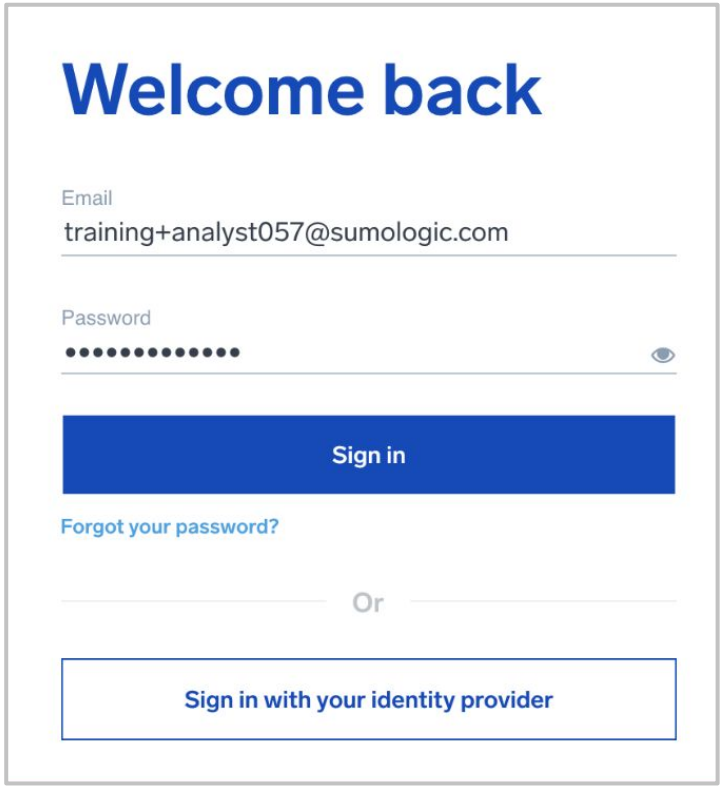
email:

training+analyst###@sumologic.com

password: *******

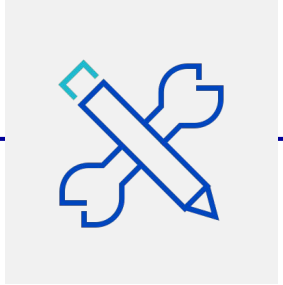
- a number between 001-999, for example training+analyst057@sumologic.com

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



Hands-on Lab

Using Sumo Logic Training

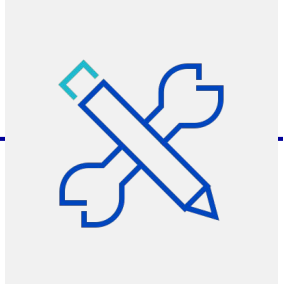


Complete Lab 1: Data Collection

- 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
- Application Infrastructure

kubernetes

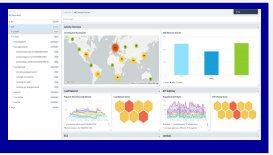
Amazon EC2

aws

Application Observability

Kubernetes Observability

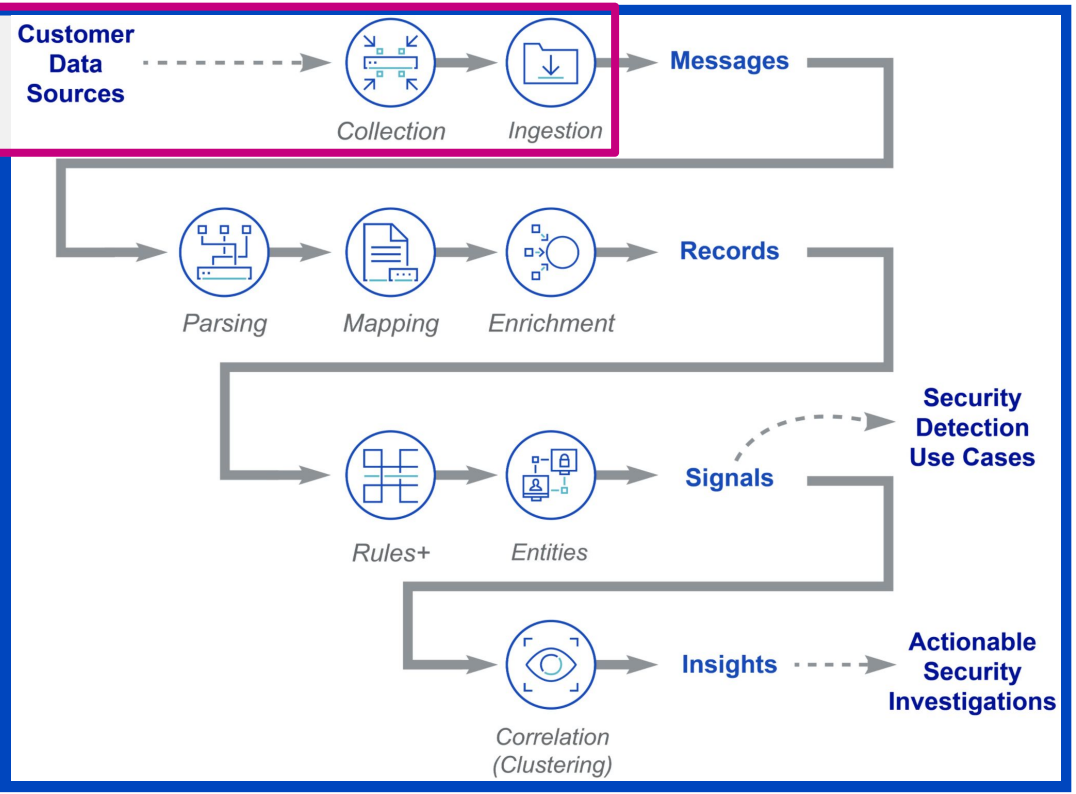
Amazon Web Services AWS



Ingesting data for Security

Collection on CIP

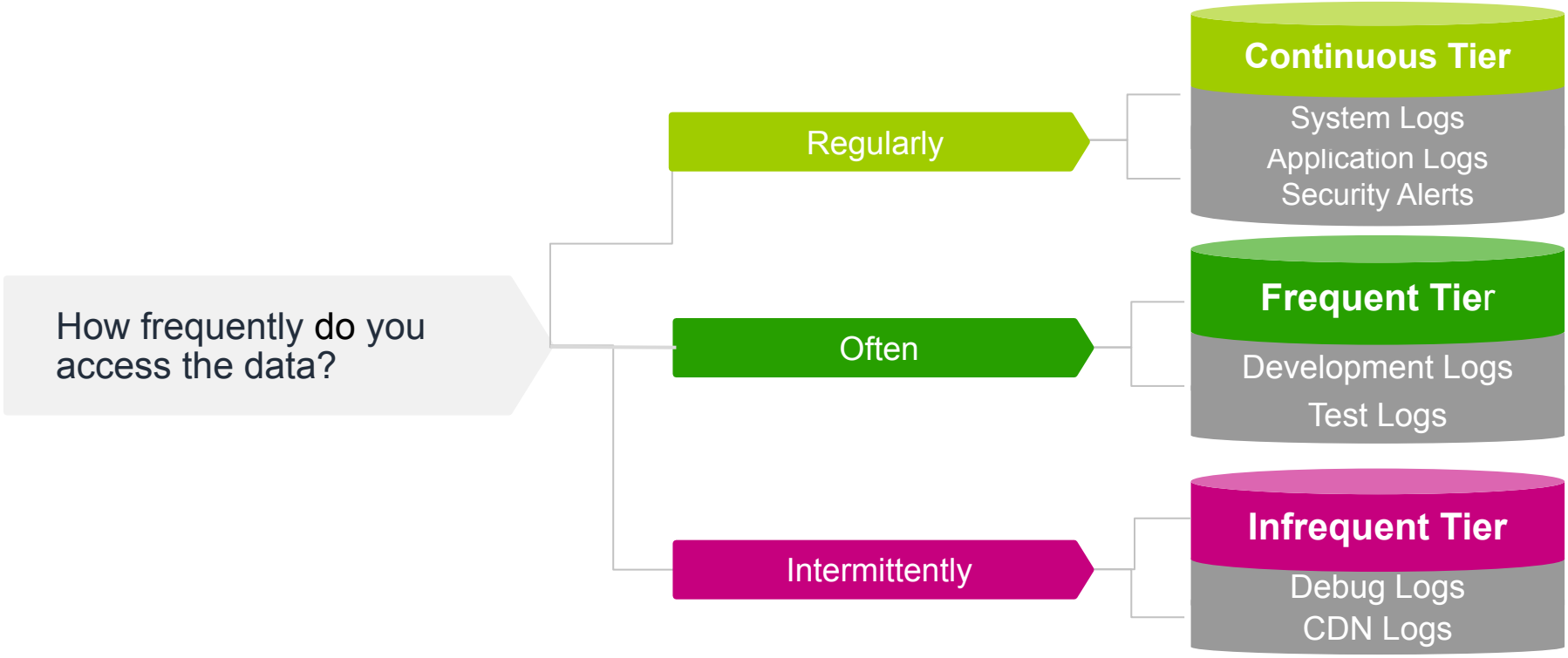
Collection on CSE



What is required for my business?

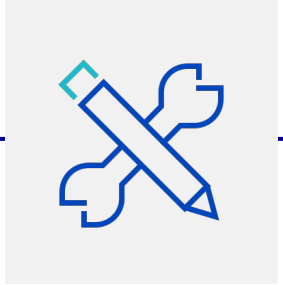
- Ability to slice and dice usage based on:
  - **Metadata**: Collector, Source Category, Source, Source Name, Source Host
  - **Data Types**: Logs, Traces, Metrics
  - **Tiers**: Continuous, Frequent, Infrequent

Which tier should I use?



Hands-on Lab

Using Sumo Logic Training Portal



Complete Lab 3: Exploring Data Tiers

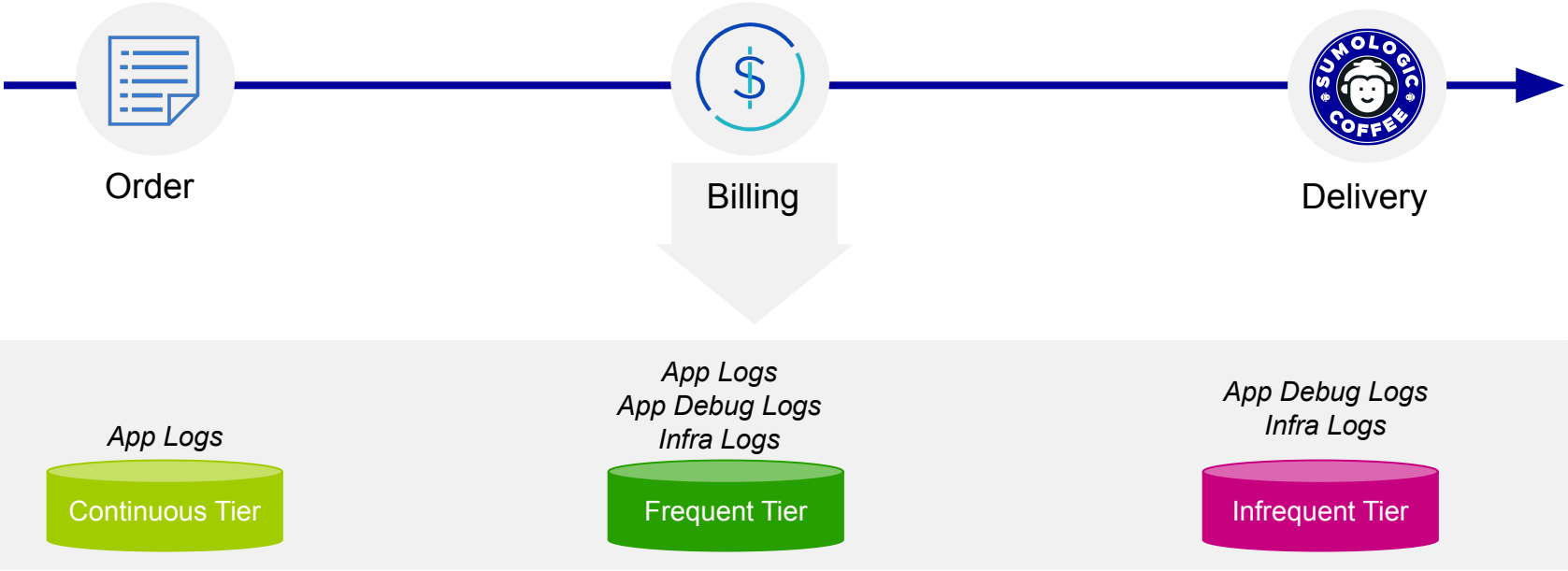
- Navigate to Manage Data > Logs > Partitions page
- Identify partitions
- Identify Data Tiers
- Click +New > Log Search > Basic Mode

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

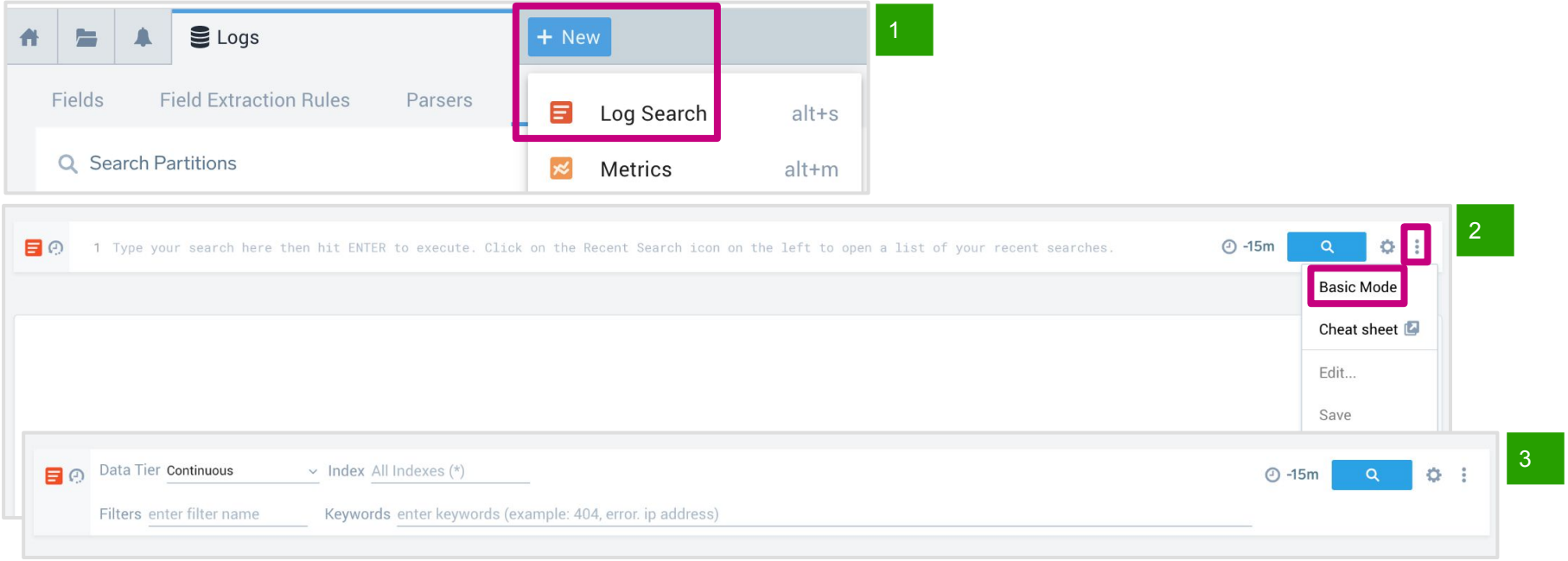
sumo logic

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.



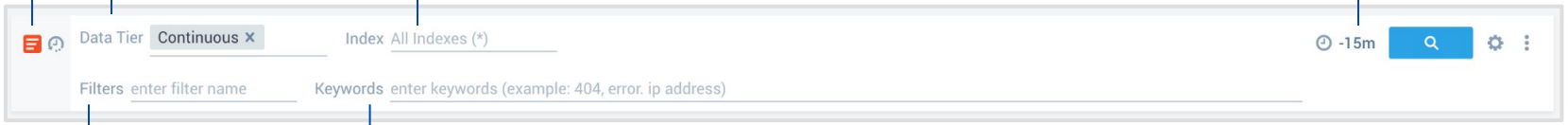
Logs Search Basic Mode

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



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

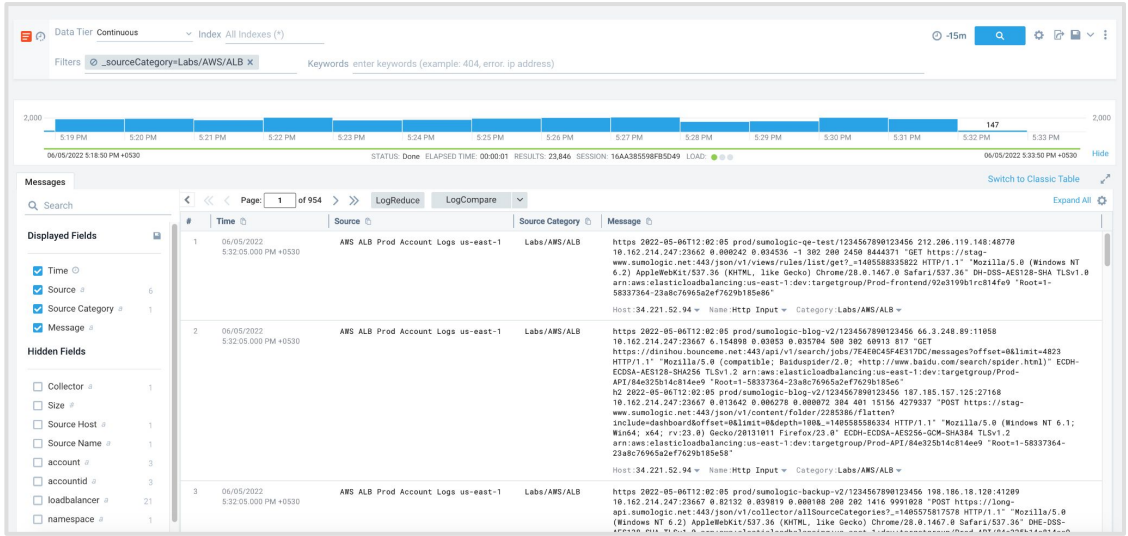
Filter logs using **Keywords**

Log Search

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

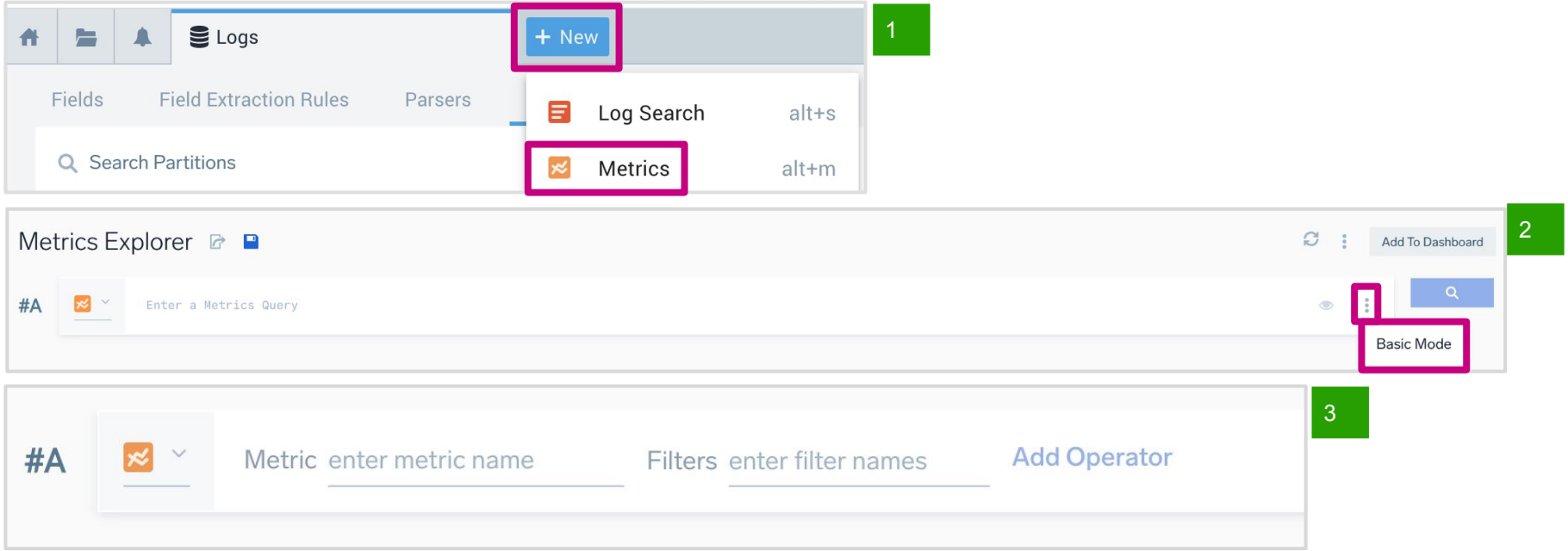
Select

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



Navigating to Metrics Explorer

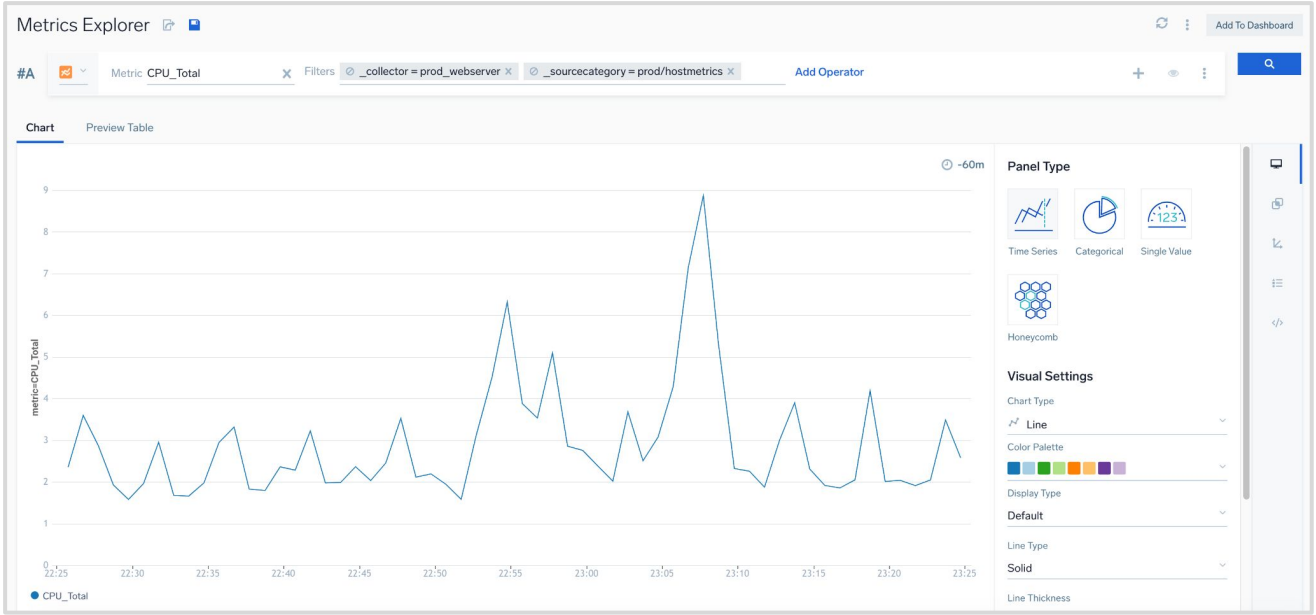
1. Open a Log Search by clicking **+ New**, then select **Metrics**.
2. Click the three-dot icon on the right and select **Basic Mode** from the menu options.
3. The user interface changes to show the simple query builder.



Metrics Search

Select

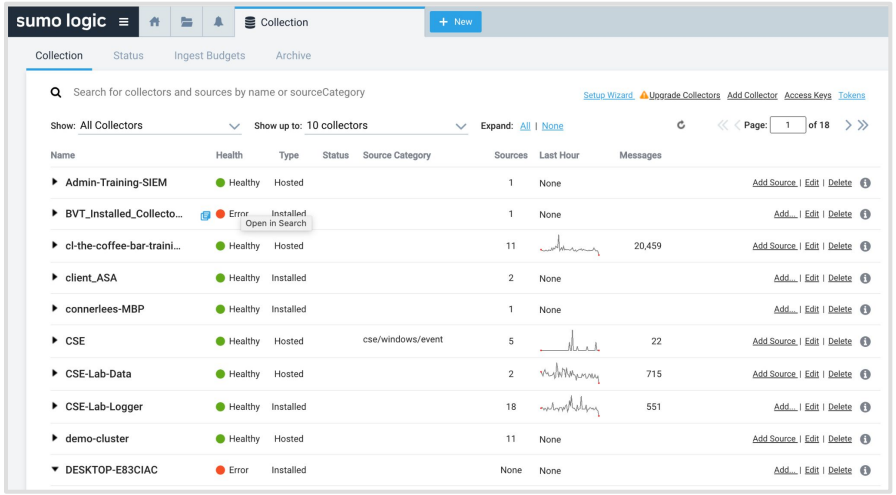
- Metric=CPU_Total
- _collector=prod_webserver
- _sourcecategory=prod/hostmetrics



Where is the data in Sumo?

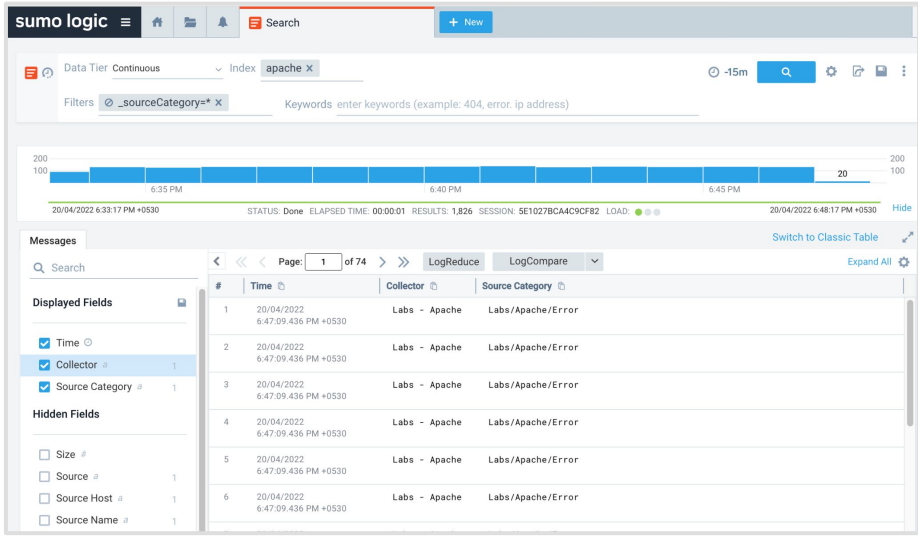
Option 1
Explore your Collectors

Click **Manage Data** > **Collection** > **Collection**



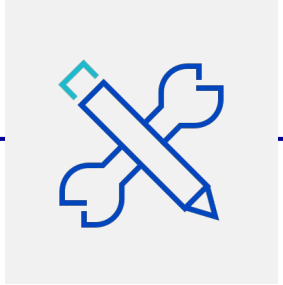
Option 2
Search for source categories

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



Hands-on Lab

Using Sumo Logic Training Portal

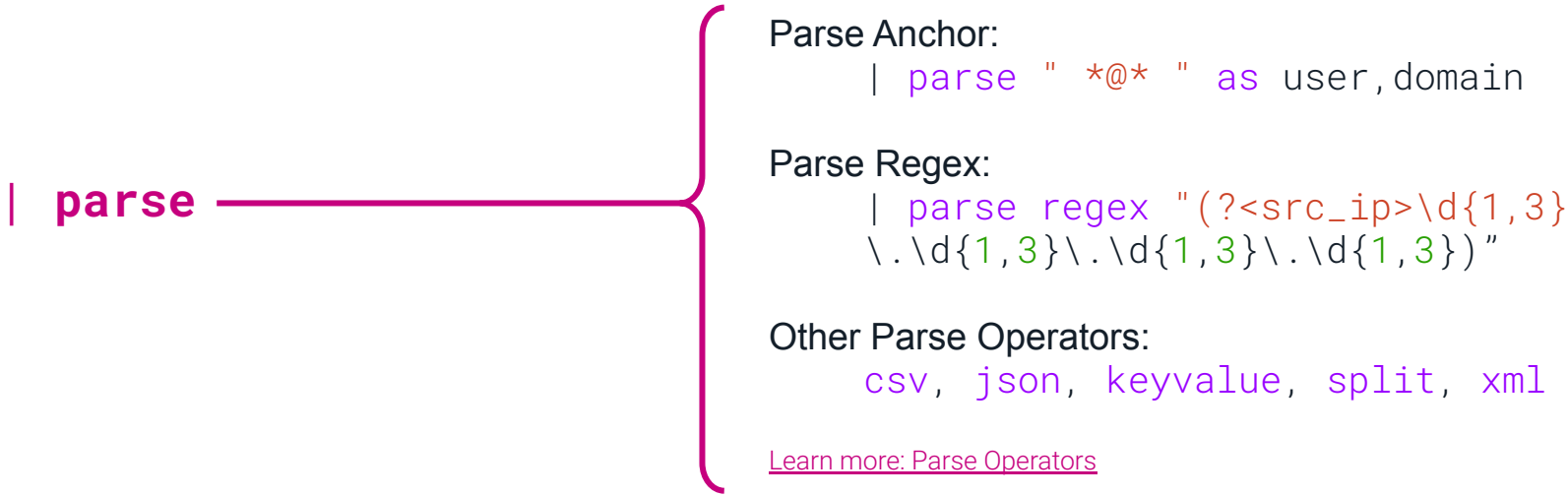


Complete Lab 4: Data Searching

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

Parsing

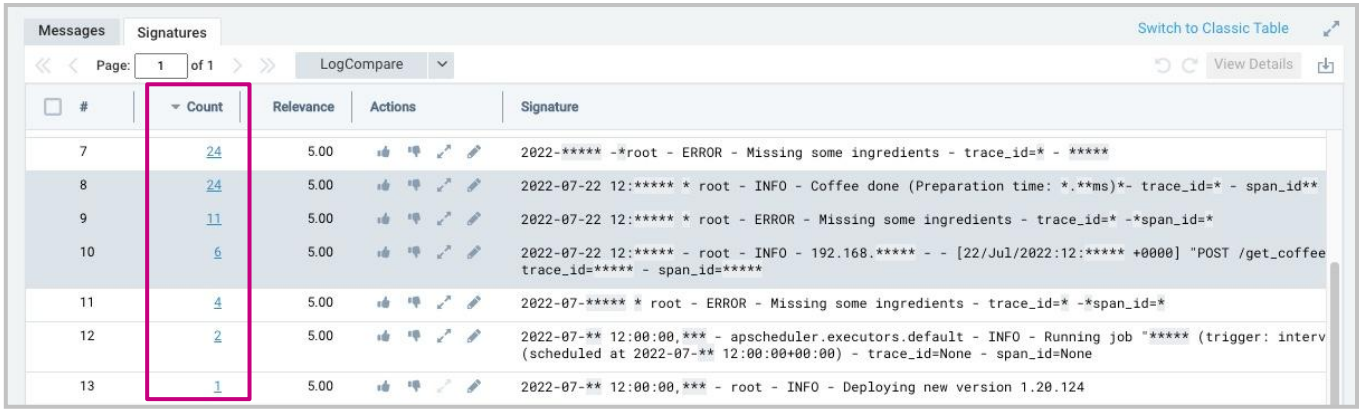
- Extract meaningful fields to provide structure to your data
- Extract fields within a query manually and on an ad-hoc basis.



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
```



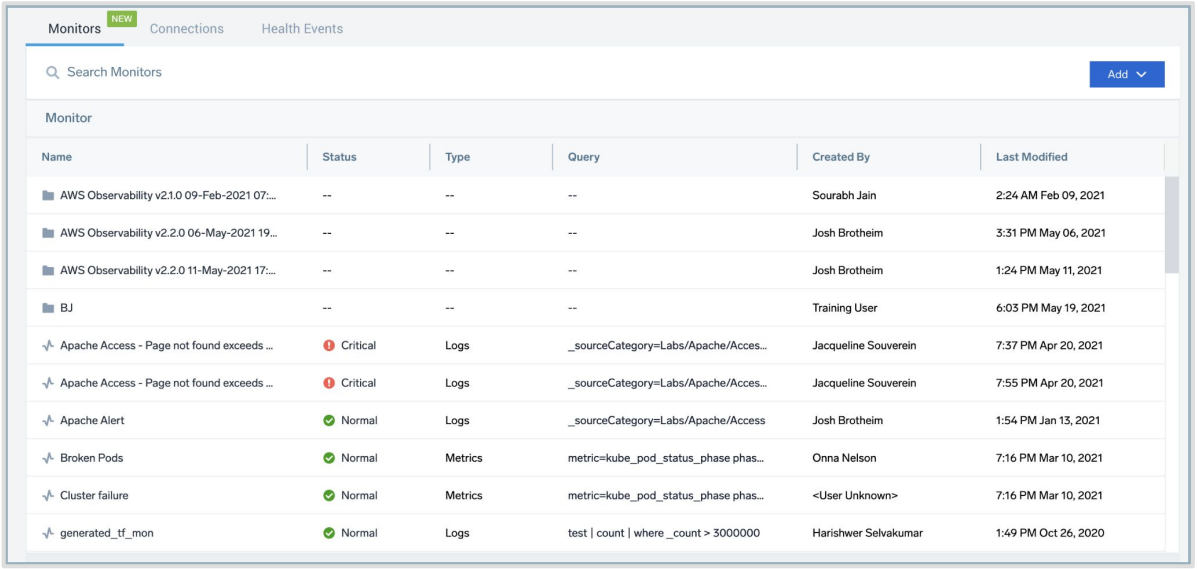
Monitoring and Visualizing Data

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

sumo logic

Alert Response overview

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

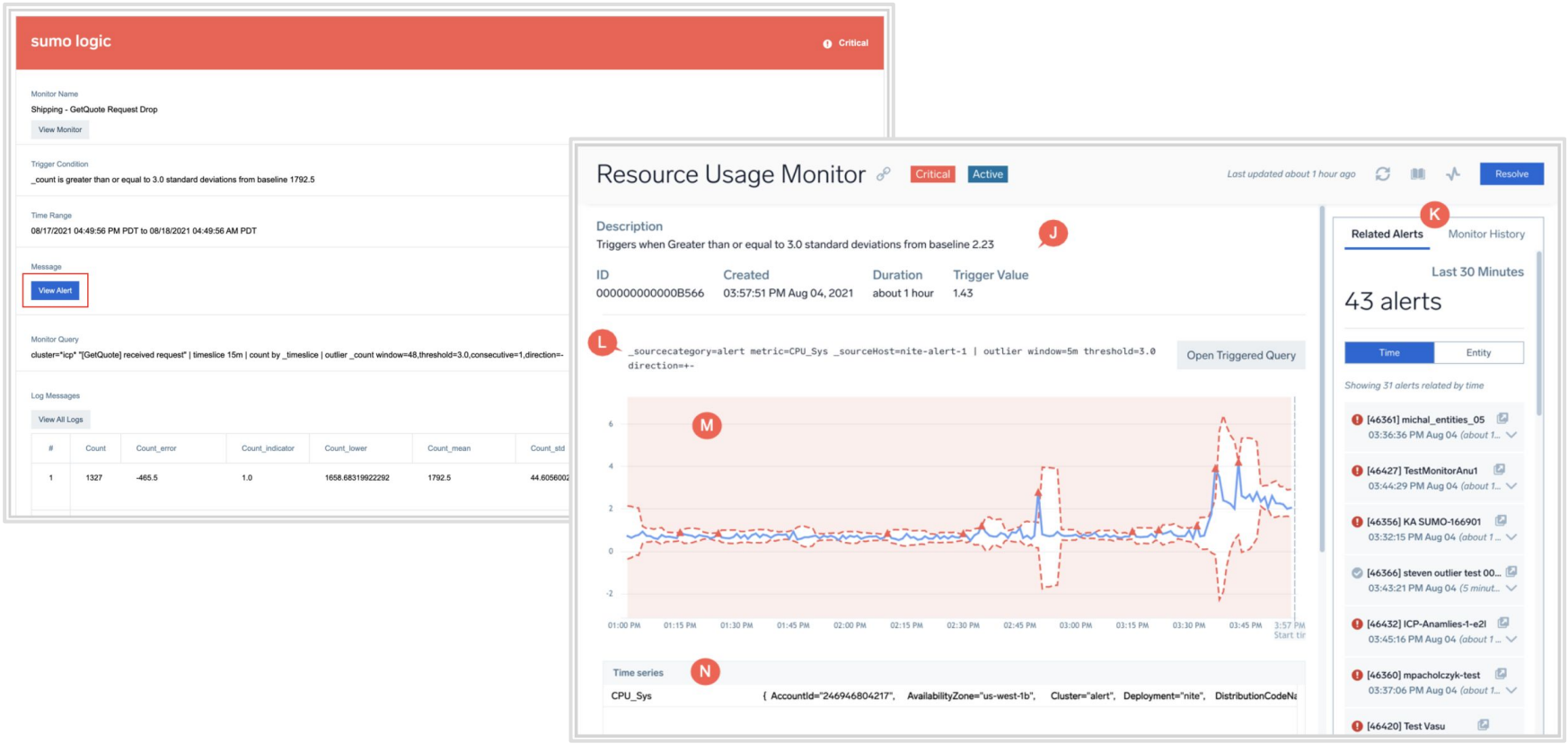


Unified Monitors alert on thresholds (Critical, Warning, Missing Data)

Alert Response - Context Cards

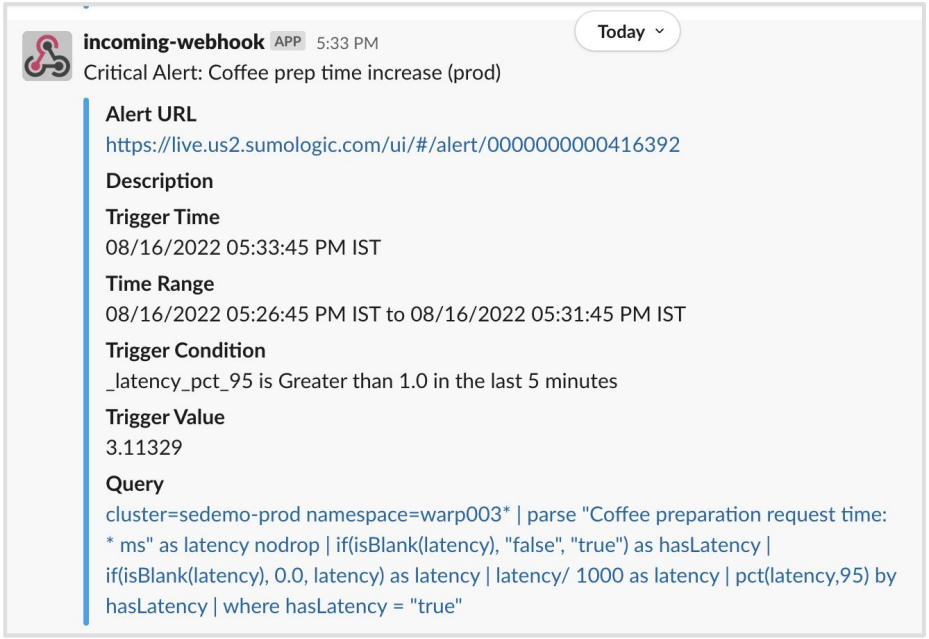
Log Fluctuation 	Identify changes in Log patterns/signatures that might help explain the underlying issue
Anomaly 	Find anomalies in metrics data reported by various related entities over time
Dimensional Explanation 	Analyze app log data and surface dimensions that might explain the alert condition
Benchmarks 	Surface abnormalities in data reported by various entities when compared with other Sumo cohort

Alert Response - Troubleshooting



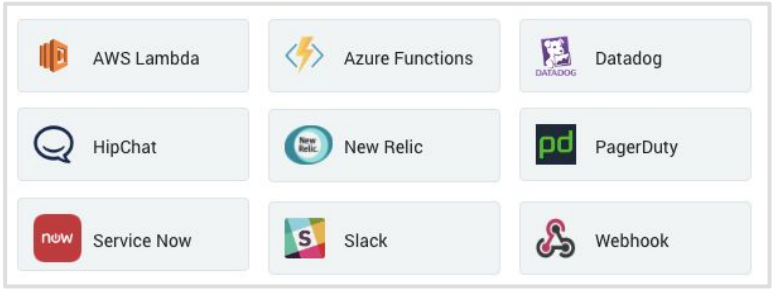
Monitoring - Alerts

Scheduled Searches trigger Alerts when a condition is met.



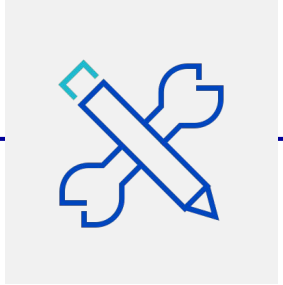
Alert Types:

- Email
- Webhook
- Save to Index
- Script Action



Hands-on Lab

Using Sumo Logic Training Portal



Complete Lab 5: Data Monitoring

- Create an email alert

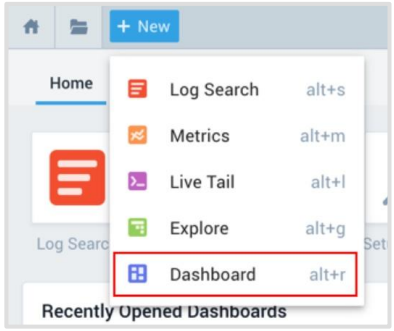
Dashboards, Charts, Panels

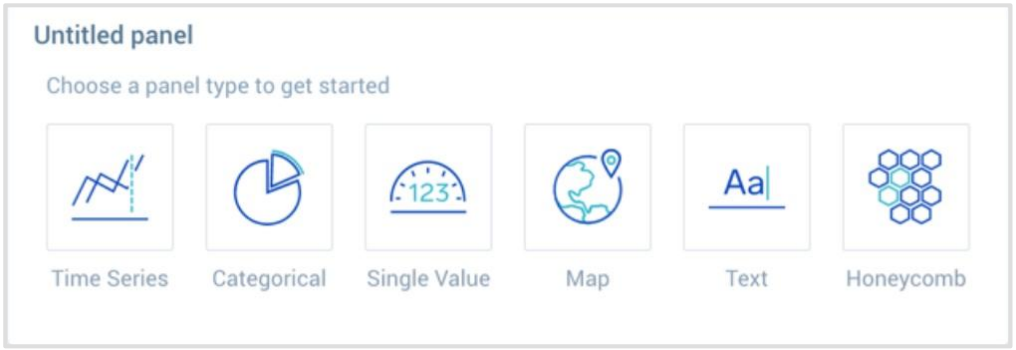
Visualization

sumo logic®

Panels

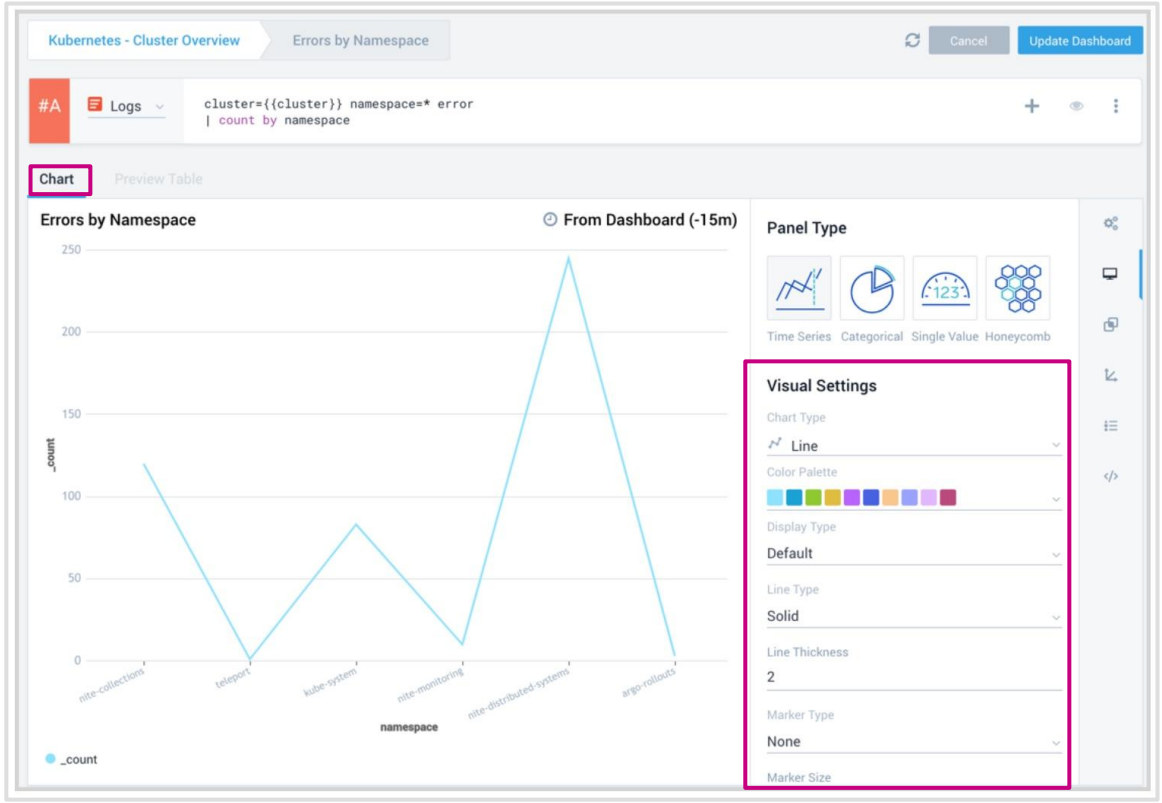
- **Panels** are the building blocks used to create a dashboard.
  - Time Series
  - Categorical
  - Single Value
  - Map
  - Text
  - Honeycomb





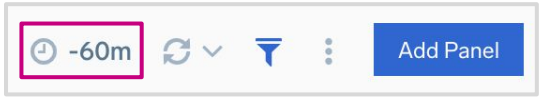
Charts

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



Dashboards

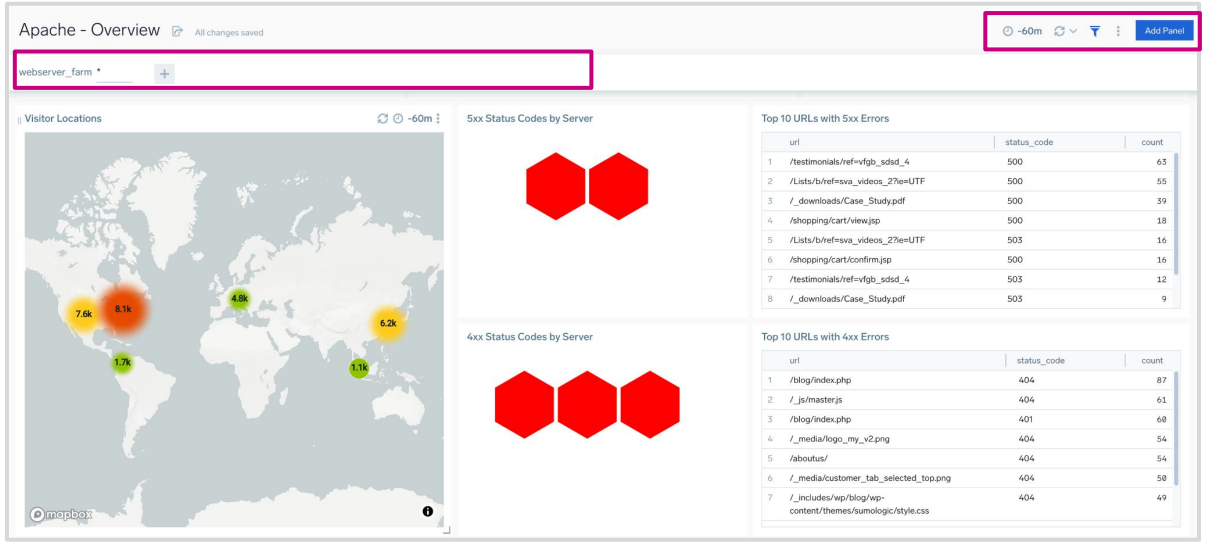
- Select **Time range** to view data for the corresponding panel



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

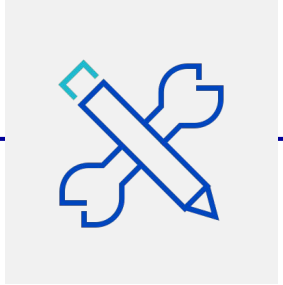
- Ability to add panels inline through **Add a Panel** button

- 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

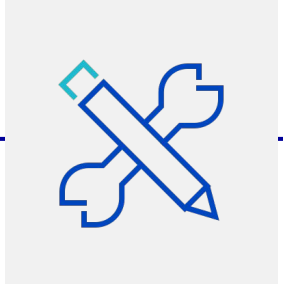
Resources

Training, Docs, Community, Support

sumo logic

Hands-on Lab

Using Sumo Logic Training Portal

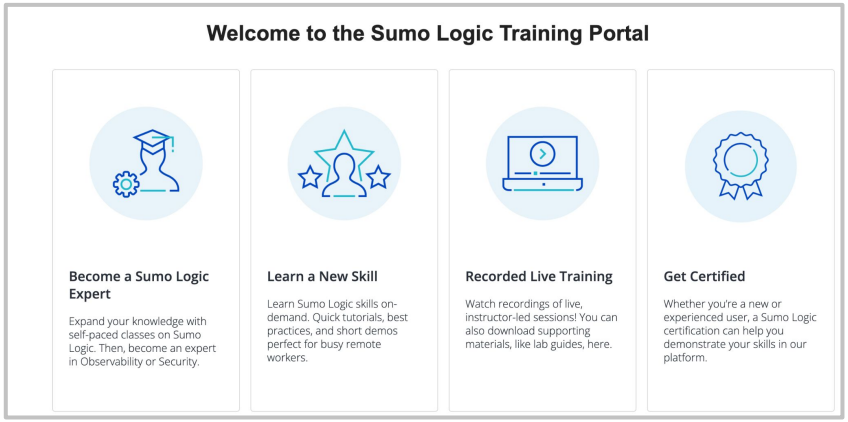


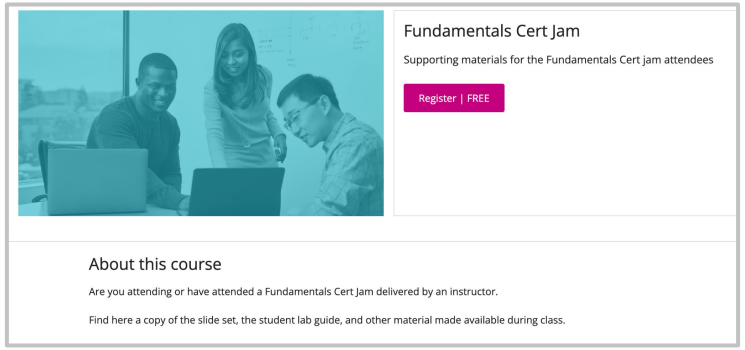
Complete Lab 7: Get Help

- 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**



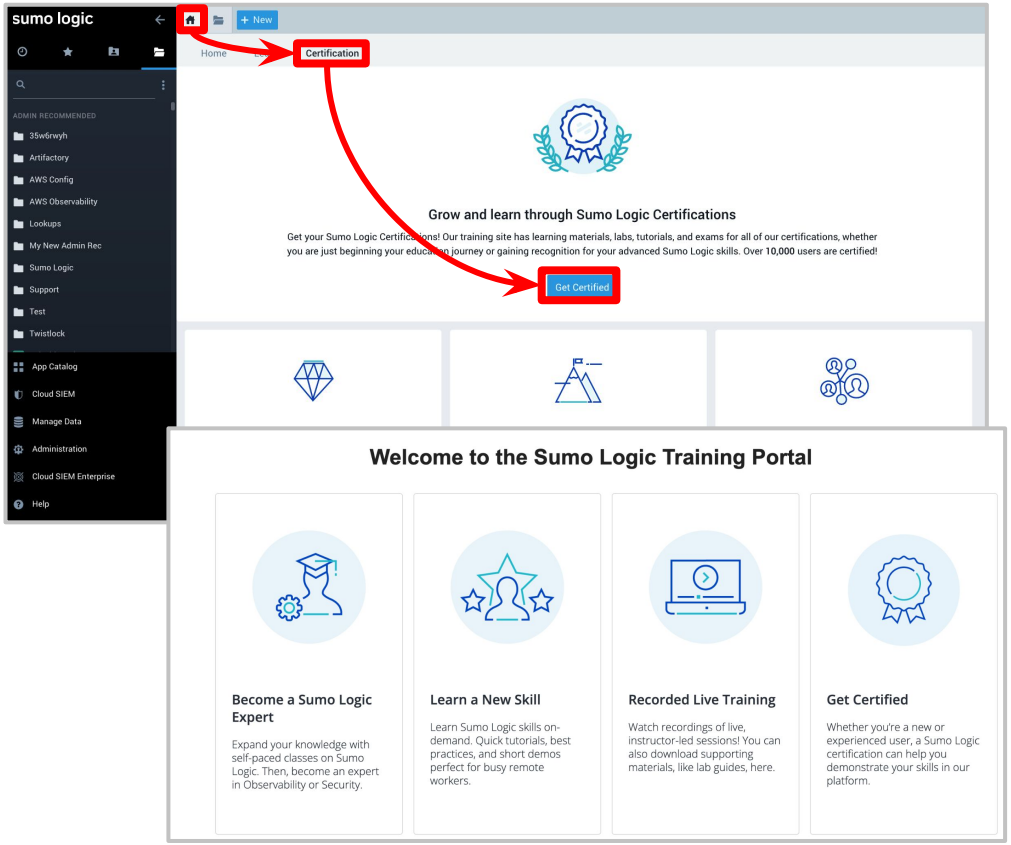


Certification

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

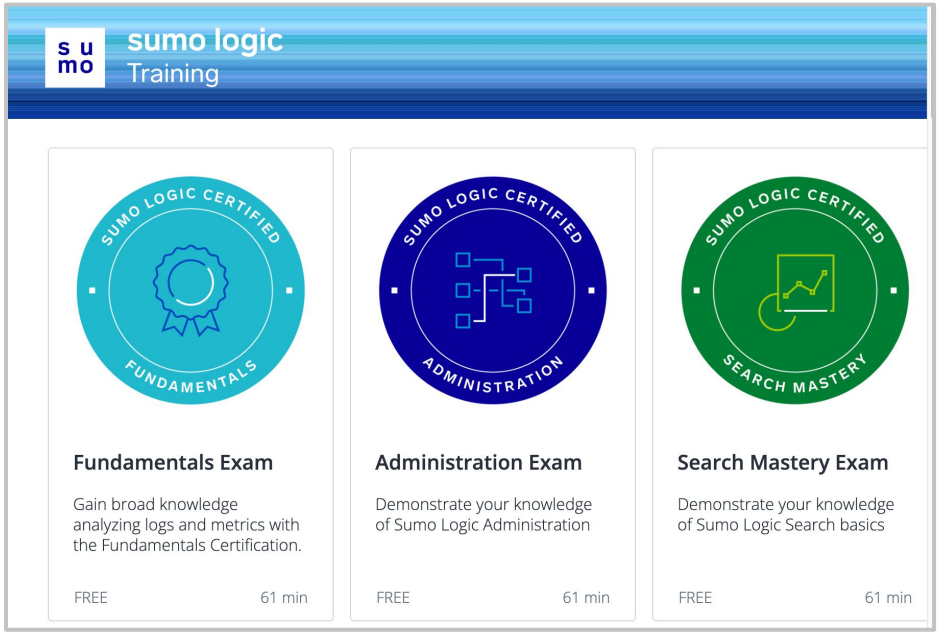
Assessment:

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**



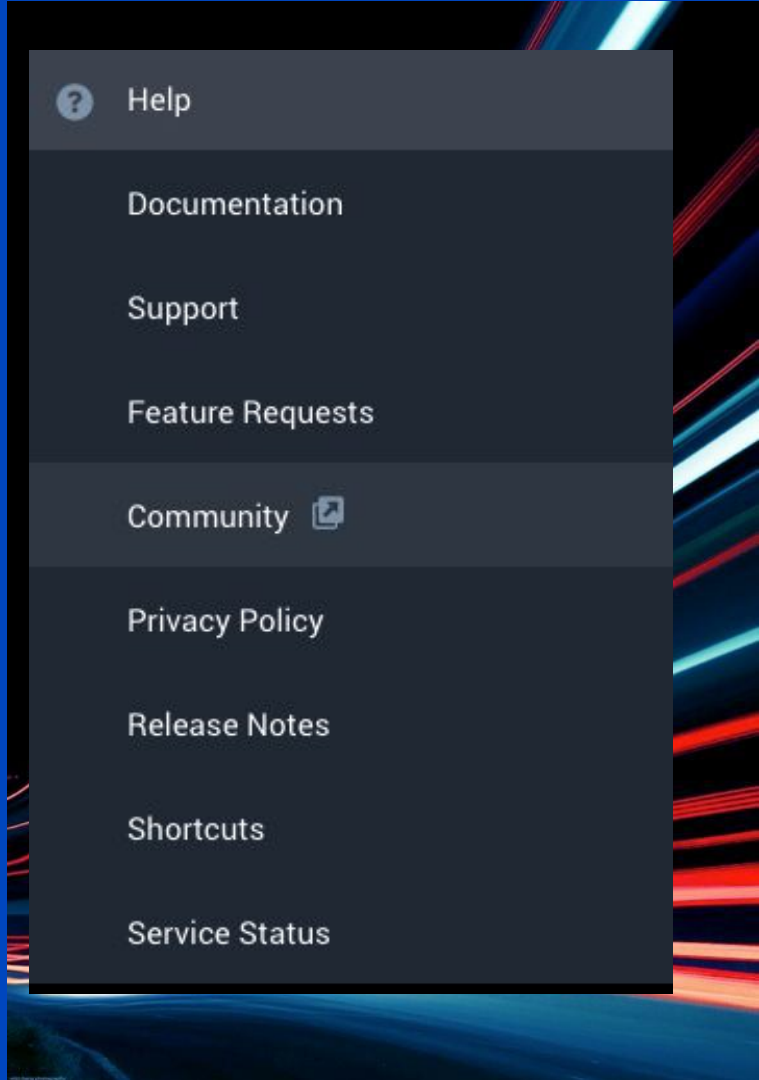
Assessment description

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



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 able to take the exam without any issues

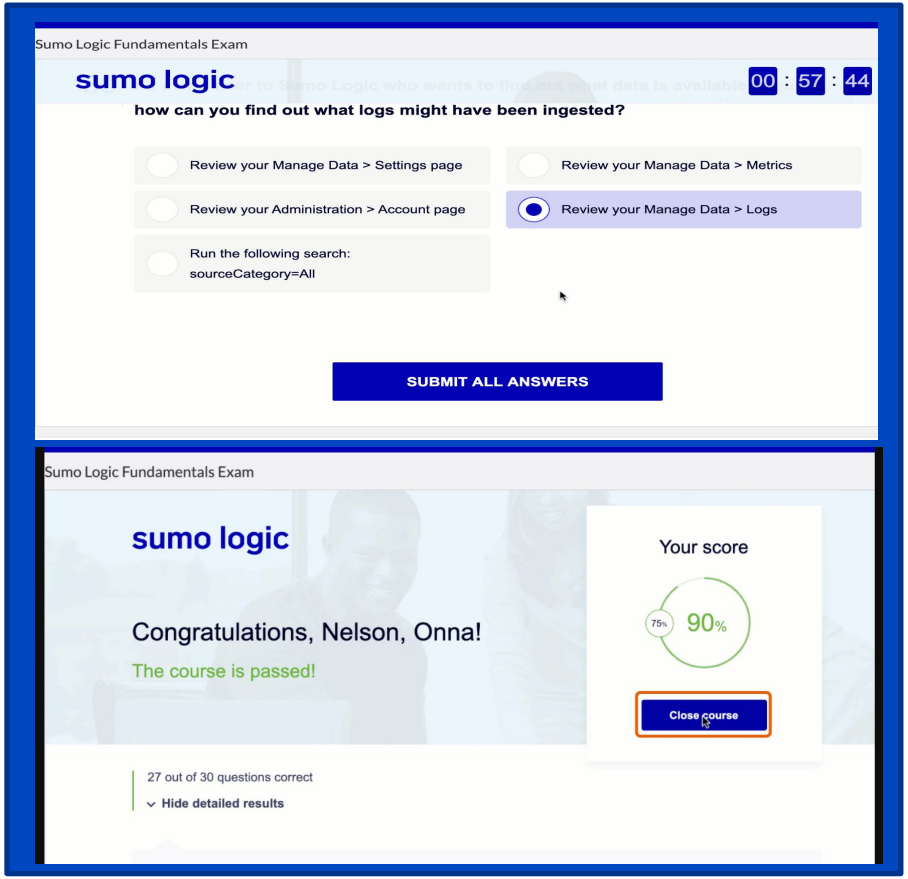


sumo logic®

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**.



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

s u

Empowering the people who power modern business

m o

sumo logic