



# Kubernetes on Sumo Logic

## K8s User Certification



# Become a Sumo Logic Kubernetes expert



1. Discover Kubernetes data and metadata in Sumo Logic
2. Explore your Kubernetes clusters with enriched metadata
3. Install apps, partner apps, and pre-built dashboards
4. Create your own custom dashboards from scratch
5. Monitor and troubleshoot with alerts and the Explore tab
6. Get certified with the Kubernetes on Sumo Logic exam

# Course Agenda



- 5 min. ● Review Kubernetes basic concepts
- 5 min. ● Review Sumo Logic data pipeline and metadata
- 5 min. ● Explain Kubernetes data collection and enrichment
- 10 min. ● Hands-on labs: Search with metadata
- 10 min. ● Sumo Logic apps available for Kubernetes
- 10 min. ● Explore tab and pre-built dashboards
- 5 min. ● Break time!

# Install apps and explore pre-built dashboards

The screenshot shows the Sumo Logic interface with a dark sidebar on the left and a light-colored main dashboard area.

**Left Sidebar:**

- Sumo logic
- App Catalog
- Manage Data
- Administration
- Help

**Main Dashboard Area:**

- Top Bar:** Home, Learn, Certification, and a search bar.
- Icons:** Log Search, Metrics, Log Tail, and Setup Wizard.
- Recently Opened Dashboards:**
  - My First K8s Dashboard
  - My X8s Dashboard
  - Apache Status Codes
  - Collective Host Binding Data
- Recently Run Searches:**
  - \_sourceCategory=Logs/Sumo\_Logic
  - sumoID:0000000000 AND \_sourceCategory = "Logs/Sumo\_Logic"
  - sumoID:0000000001
  - cluster-prod1.sumologic.info(namespace=prod-logger pod=pagentry-84...)
  - cluster-prod1.sumologic.info(namespace=prod-logger pod=carbonblack-1...)
  - sourceCategory=Logs/\_source/\_id:sumoID:0000000000
- Recommended Dashboards:**
  - Google Cloud Audit Network and Security
  - New dashboard for Group2
  - ArtFactory - Traffic
  - Google Cloud IAM Role Activity
- Pinned Searches:** No pinned searches.

# Create and customize your own dashboard

Dashboard Jul 01, 2020 04:01:01 0 All changes saved

🕒 -15m ⏪ Y | Add Panel

Create a template variable 

**Number of Active Nodes**

29 nodes

Average Disk Utilization Rate



metric=nodes\_disk utilization.org.west

**Fluentd Output Errors**

`_source=MATH_host_metric  
_deployment=fluentd  
_sourceName='Http Input'`

1,212 (3.0%)

`_source=MATH_host_metric  
_deployment=fluentd  
_sourceName='Http Input'`

31,908,13793 (79.2%)

`_source=Others  
_deployment=Others  
_sourceName=Others`



`_source=MATH_host_metric deployment=fluentd _sourceName='Http Input' prometheus_scrape=fluentd pod=fluentd.prometheus.sumologic/prometheus-operator.prometheus-instance-1`

**My First K8s Dashboard**

This dashboard shows the number of nodes that are active and some basic resource utilization statistics.

# Investigate and troubleshoot a crashed pod

sumo logic

Explore

Kubernetes Namespace View

- prod01.sumologic.com
- default
- kube-system
- prod-logger
- carbonblack-7476f8c76-fzqzr
- crowdstrike-47956fc76-7zvzr
- f5-asm-7bf987dcb-pqptk
- googleapps-7d8cf88d45-4yj6n
- mongodbs-748795fa26-v488q
- pagerduty-84d033179f-g77wv
- prometheus-operator-kube-state-metrics-45ch45d...
- proxymesh-78d9944d-4tww
- sumologic
- sumologiq

Dashboard: Kubernetes - Namespace Overview

Cluster: prod01.sumologic.com - Namespace: prod-logger

Time: -15m

Pods Running by Deployment

Deployment	Status
prod-logger.carbonblack	prod-logger.carbonblack
prod-logger.crowdstrike	prod-logger.crowdstrike
prod-logger.f5-asm	prod-logger.f5-asm
prod-logger.googleapps	prod-logger.googleapps
prod-logger.mongodb	prod-logger.mongodb
prod-logger.pagerduty	prod-logger.pagerduty
prod-logger.proxypoint	prod-logger.proxypoint

Sumo Logic Confidential

# Create your own custom alerts

The screenshot shows the Sumo Logic interface with the following elements:

- Top Bar:** Home, Learn, Certification, + New.
- Left Sidebar:** Log Search, Metrics, Live Tail, Setup Wizard.
- Recently Opened Dashboards:**
  - Kubernetes - Namespace Overview
  - Kubernetes - Cluster Overview
  - Kubernetes - API Server
  - My First K8s Dashboard
  - Kubernetes - Cluster Explorer
  - Kubernetes - Pods
  - My Kubernetes - Remote Overview
- Recently Run Searches:**
  - \_sourceCategory:Labs/Sumo\_Logic
  - (suRhnODW714DZU) AND \_sourcecategory = "Labs/Sumo\_Logic"
  - suRhnODW714DZU
  - suRhnODW714DZU
  - cluster=prod01.travellogic.info namespace=prod-loggen pod=pagerduty-64...
  - cluster=prod01.travellogic.info namespace=prod-loggen pod=carbonblack-f...
  - cluster=prod01.travellogic.info namespace=prod-loggen pod=pagerduty-64...
- Recommended Dashboards:** 0
- Pinned Searches:** Google Cloud Audit Network and Security

# Welcome to TravelLogic Inc!

TravelLogic

FLIGHTS

HOTEL

CAR HIRE

0 ITEMS

## Flight Search



6/20/2020

From City



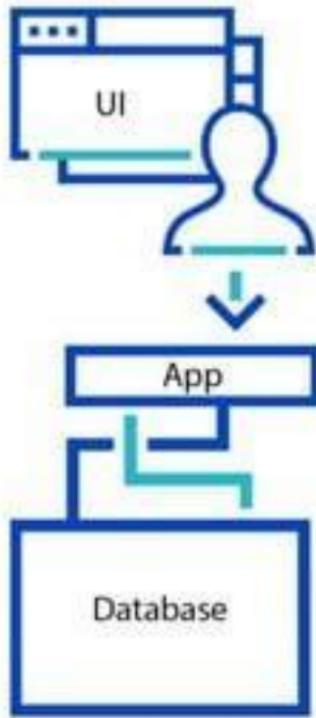
6/22/2020

To City

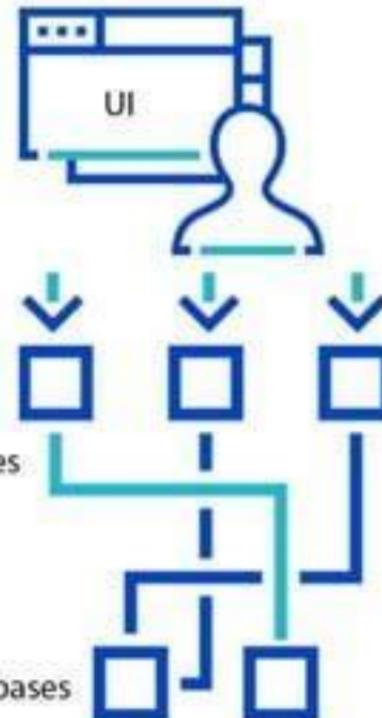
SEARCH

# Review: Kubernetes

## Monolithic Architecture



## Microservices Architecture



# What is Kubernetes?

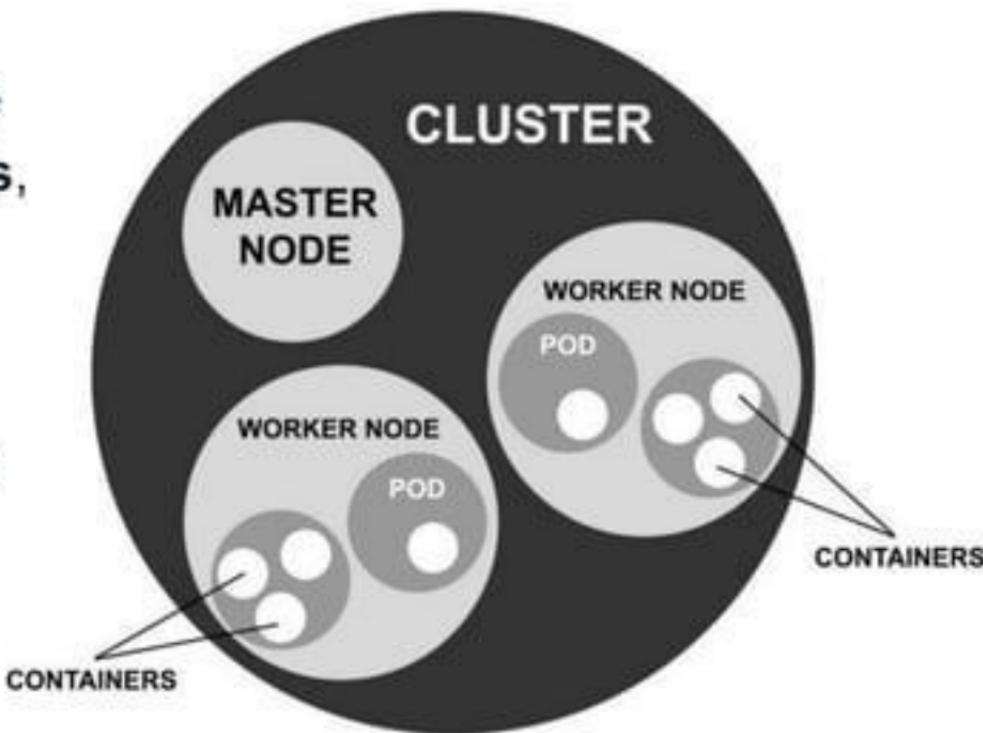
- Container orchestration system
- Open source and CNCF certified
- Guides and controls your containers, just like a ship's helmsman
- "K8s" replaces the eight letters in "ubernetes" to abbreviate Kubernetes



# Inside a Kubernetes Cluster

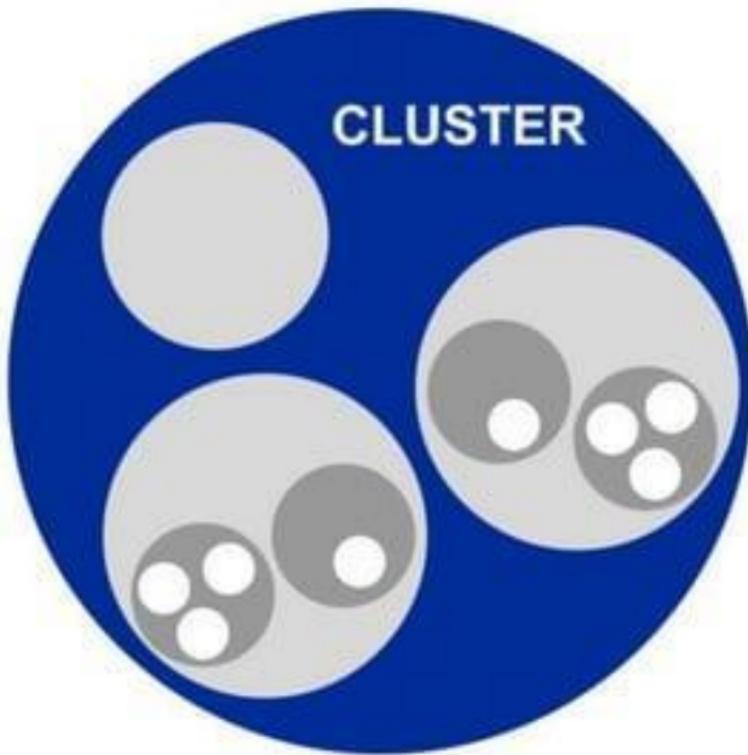
**Containers** are nested inside **pods**, which are inside **nodes**, which are inside **clusters**.

Abstract partitions like **services**, **deployments**, and **namespaces** also organize your cluster.



# Cluster

A **cluster** is a group of machines that distribute work, providing efficiency and fault tolerance.

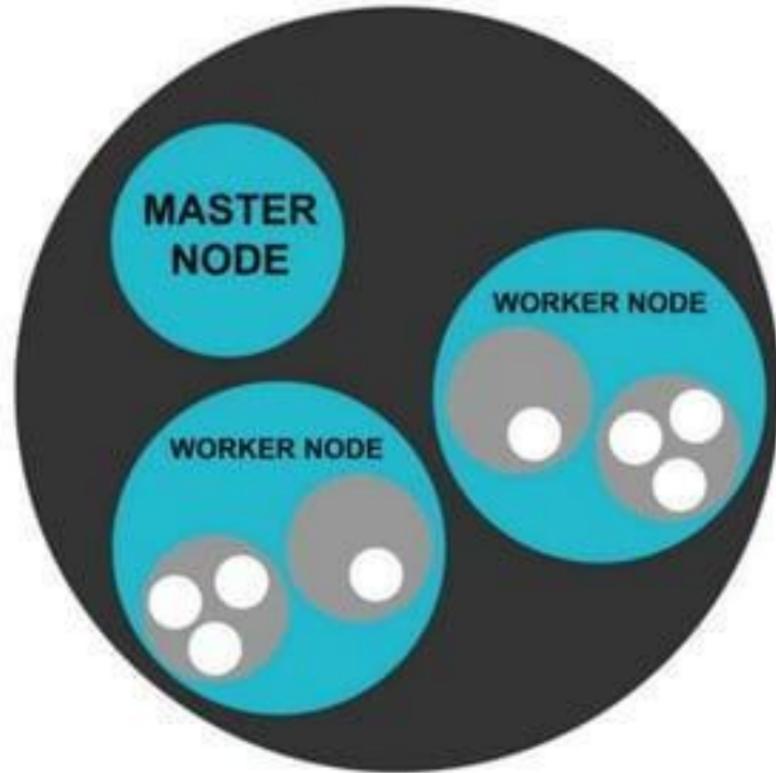


# Nodes

A **node** is a single machine inside a cluster. It can be a physical or virtual machine.

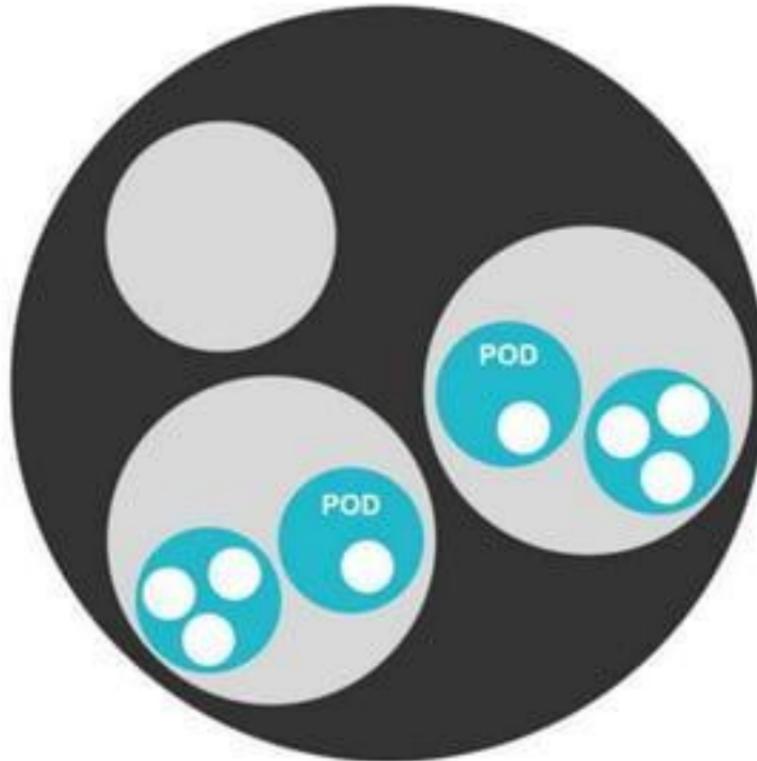
Each cluster has one **master node**. The master node assigns work to worker nodes.

**Worker nodes** run software, crunch numbers, store data, and do all the work.



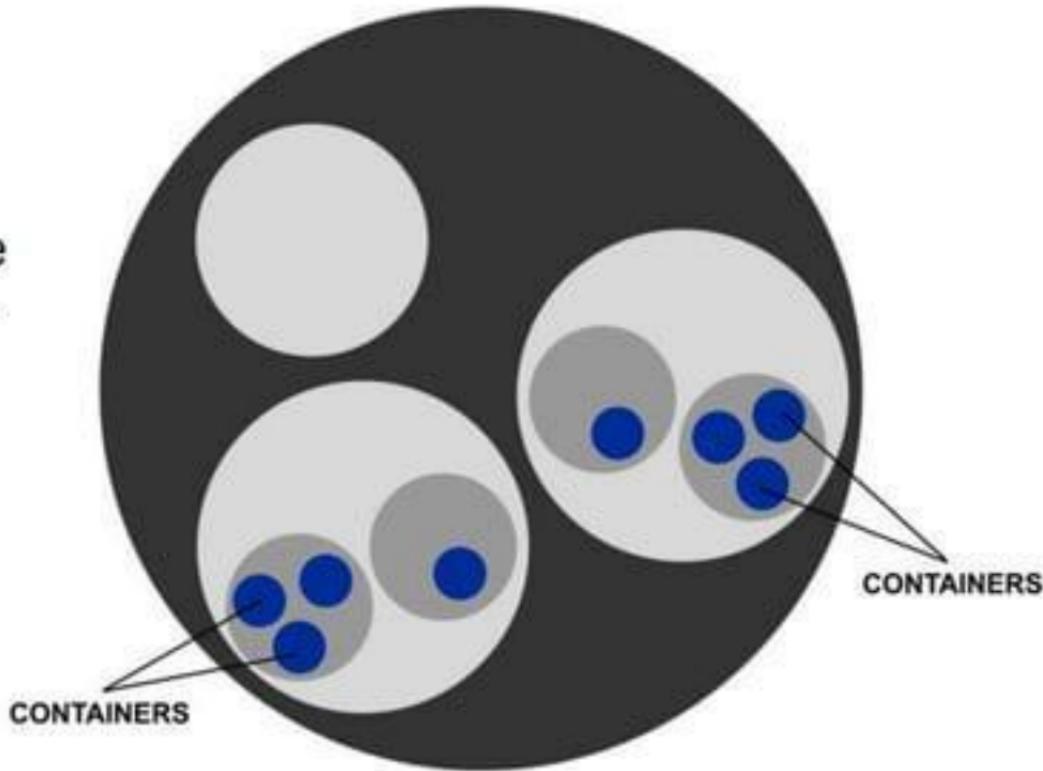
# Pods

**Pods** are the smallest unit that Kubernetes can orchestrate.



# Containers

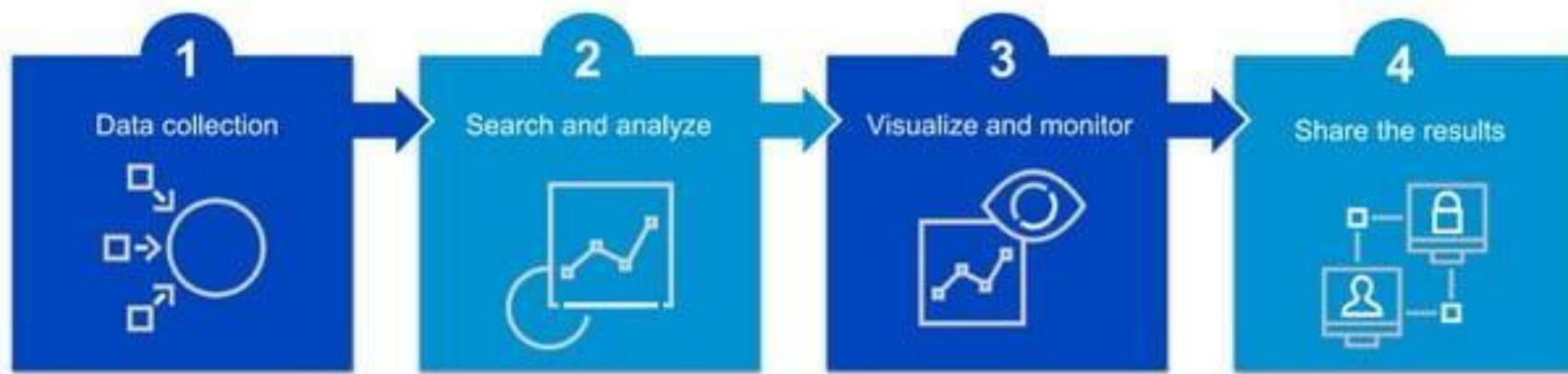
**Containers** are a package of code, data, and all their dependencies. They each run a single microservice.



# **Review:**

## **Sumo Logic data pipeline**

# Sumo Logic Data Pipeline



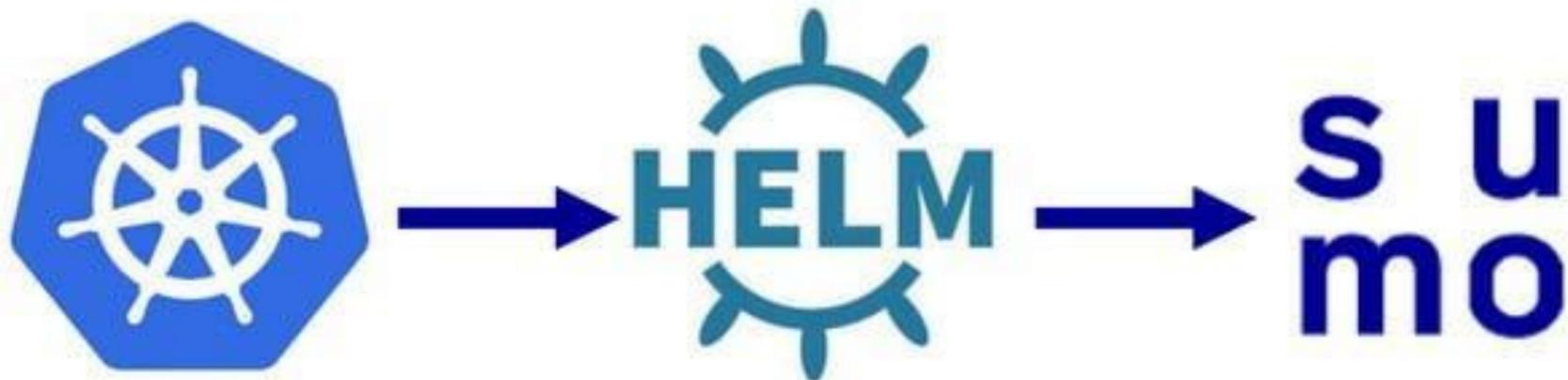
# Data collection

Data Collection

Searching and Analyzing

Visualizing and Monitoring

Sharing the Findings



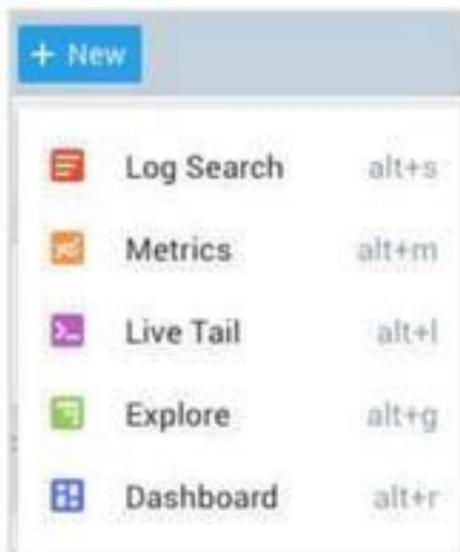
# Search and analyze

Data Collection

Searching and Analyzing

Visualizing and Monitoring

Sharing the Findings



A search interface showing a search bar with the query '\_sourceCategory=\*kube\*', and options to Save As, Info, Share, Pin, and Live Tail.

# Visualize and monitor

Data Collection

Searching and Analyzing

Visualizing and Monitoring

Sharing the Findings

The screenshot displays the Sumo Logic interface with a navigation bar at the top labeled "Data Collection", "Searching and Analyzing", "Visualizing and Monitoring" (which is highlighted in blue), and "Sharing the Findings". Below the navigation bar is a search bar with placeholder text "Search across all dashboards, logs, metrics, and events".

The main area shows a dashboard titled "My First K8s Dashboard". The dashboard includes the following components:

- Number of Active Nodes:** A large yellow number "29 nodes".
- Average CPU Utilization Rate:** A line chart showing utilization over time, with a sharp peak around July 1st.
- Planned Output Events:** A list of events including "Deployment-Ready", "Deployment-Failed", "Deployment-Error", "Deployment-Aborted", "Deployment-Canceled", and "Deployment-Unknown".
- Recently Opened Dashboards:** A list of dashboards such as "Administrator - Performance Overview", "Administrator - Cluster Overview", "Administrator - API Server", "Administrator - Metrics Overview", "Administrator - Health Overview", "Administrator - Page", "Administrator - Metric Metrics", and "Administrator - Cloud Audit Metrics and Security".
- Recently Run Queries:** A list of queries including "sumoLogicLogs", "sumoLogicLogs AND (source:k8s OR source:kubernetes)", "sumoLogs", "sumoLogs", "sumoLogs", "sumoLogs", "sumoLogs", and "sumoLogs".

The bottom left corner features the "sumo logic" logo.

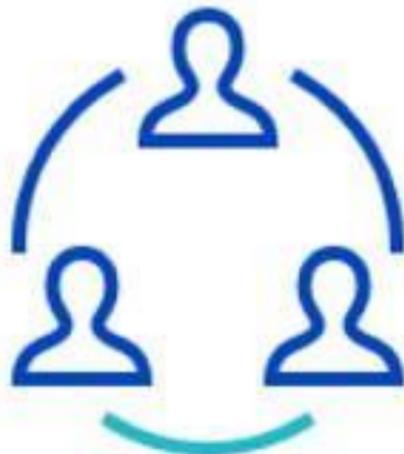
# Share

Data Collection

Searching and Analyzing

Visualizing and Monitoring

Sharing the Findings



# Data collection and metadata enrichment

# What is metadata?

- **Data:** Information stored by your app
- **Metadata:** Data about your data
- Searchable by fields, source categories, key-value pairs, etc.
- Good metadata design will save you time and money

# Using metadata

The screenshot shows the Sumo Logic interface with a search bar containing the query `_sourceCategory=*kube*`. Below the search bar are buttons for Home, Folders, Search, and a New button. A dropdown menu is open, showing the selected filter `_sourceCategory=*kube*`. To the right, a modal window titled "Edit Collector: Labs - Kubernetes" is displayed. The modal contains fields for Name (set to "Labs - Kubernetes"), Description, Category, and Fields. The "Fields" section lists "user747" with a checked checkbox and "username747".

Search: \_sourceCategory=\*kube\*

+ New

Name: Labs - Kubernetes

Description

Category

Unless overwritten by Source metadata, the Collector will set the Source category of all messages to this value.

Fields

user747

username747

# Kubernetes data pipeline



## Metadata enrichment

- Prometheus provides autodiscovery that tags pods and nodes
- Sumo Logic's metadata enrichment tags services and deployments
- Custom key-value pairs (fields) provide details on your cluster



## **Hands-on labs:**

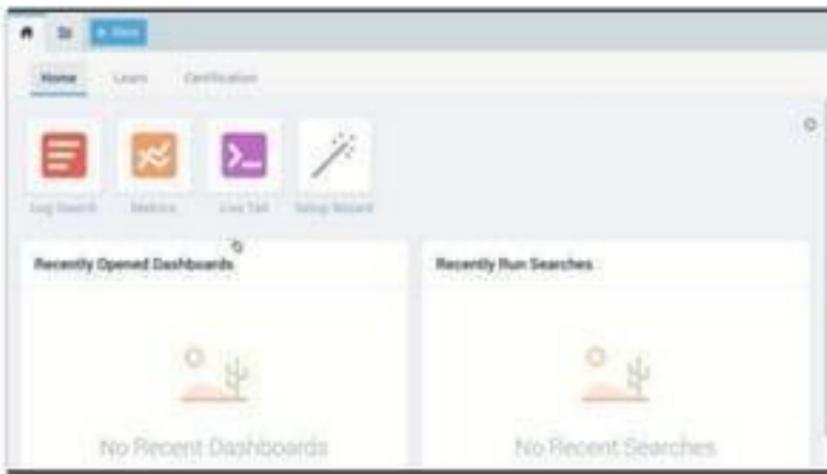
Log in to training environment

Identify metadata

Search with metadata

# Access the lab guides

1. Go to: [service.sumologic.com](https://service.sumologic.com)
2. Log in using your Sumo Logic credentials.
3. Click **Certification > Get Certified**.
4. Go to **Kubernetes > Cert Jam Lab Guide** and enroll.

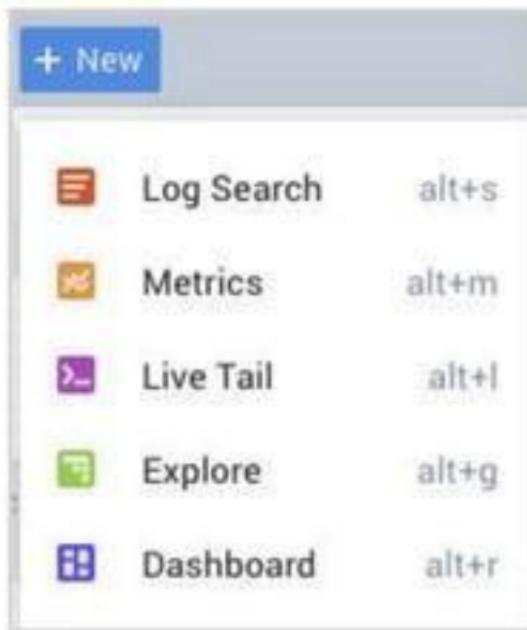


## Lab 1: Identify metadata

1. Navigate to the Sumo Logic UI.
2. Start a new **Log Search**.
3. Search for the `*kube*` metadata.
4. Click **Manage Data > Collection** for an alternate view of source category metadata.

## Lab 2: Search with metadata

1. Navigate to the the Sumo Logic UI.
2. Start a new **Log Search**.
3. Search for the sumologic namespace.

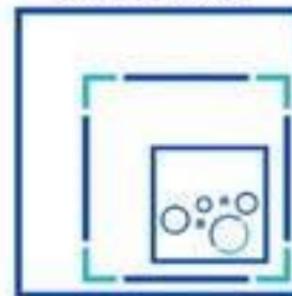


# Sumo Logic apps for Kubernetes

## Your TravelLogic app



## Your Kubernetes cluster



## Sumo Loaic's Kubernetes app



**kubernetes**

# Sumo Logic Kubernetes app

- Manage and monitor multiple clusters
- Centralized metadata enrichment
- Visibility into the worker nodes of a K8s cluster
- Namespace, deployment, and service views
- Dynamic, live pre-built dashboards
- CNCF standards and out-of-the-box security features



**kubernetes**

# Control Plane apps

- Work alongside the Kubernetes app
- Visibility into master nodes
- Open source or managed service



# DevOps and CI/CD apps

- **CircleCI.** Monitor and secure the DevOps pipeline to increase delivery velocity.
- **Istio.** CI/CD partner app, including securing, connecting, and monitoring microservices.
- **Spinnaker.** Infrastructure management platform for hybrid-cloud, multi-cloud, and Kubernetes.



# Security apps

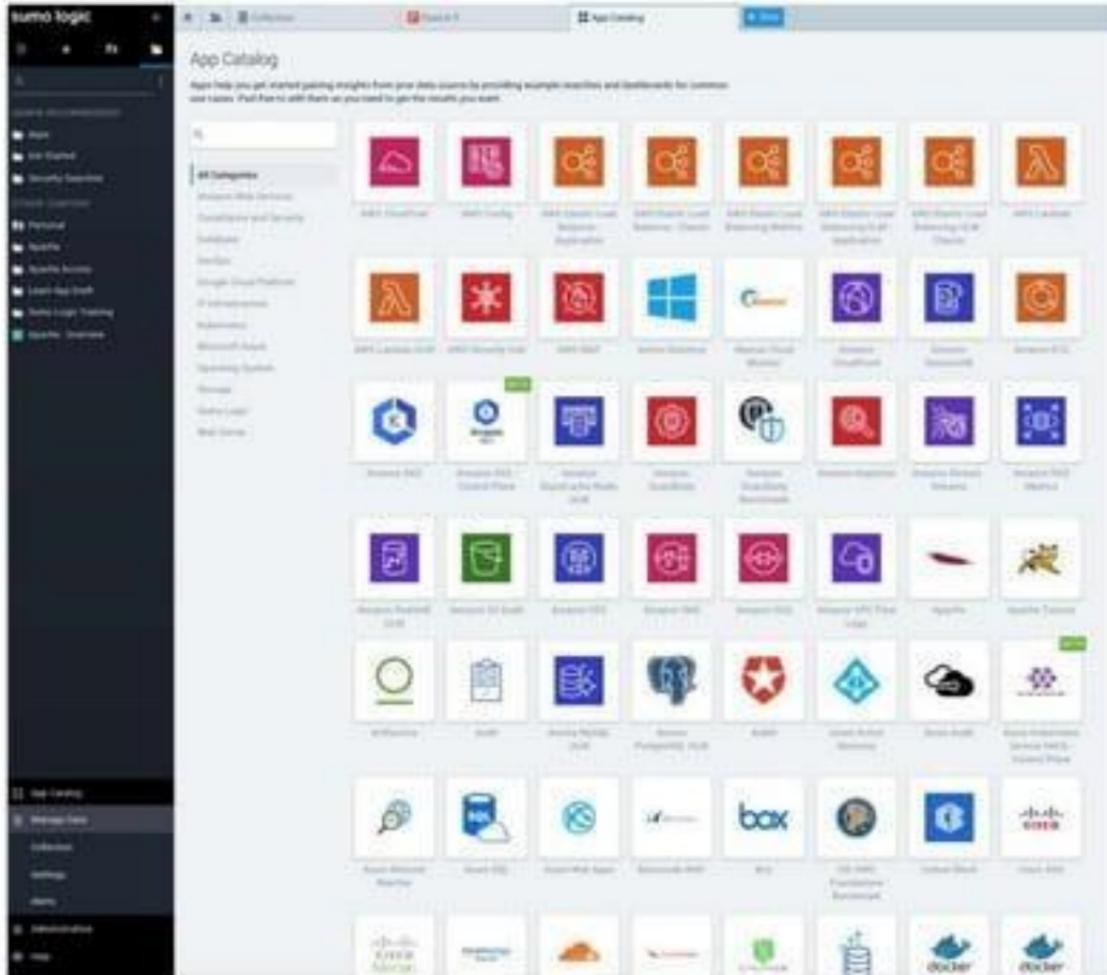
- **Alcide kAudit.** Enhanced visibility into audit logs.
- **Stackrox.** Detect vulnerabilities, compliance violations, and runtime threats.
- **Twistlock.** Monitor and analyze hosts, containers, images, and registry.
- **Aqua Security.** Provides security and compliance for cloud-native applications.
- **JFrog Xray.** Investigate vulnerabilities across deployment environments.



JFrog Xray

## Hundreds of apps

- 200+ Apps available
  - Dozens of K8s apps
  - Installed apps appear in your personal folder
  - Only install each app once per account



# The Explore Tab and pre-built dashboards

## Pre-configured dashboards

- Cluster Explorer
- Cluster Overview
- Container Logs
- Containers
- Daemonsets and StatefulSets
- Development overview
- DPM
- DPM - Timeseries
- Health Check
- Hygiene Check
- Namespace Overview
- Nodes
- Pods
- Security Overview
- Security Rules Triggered
- Service Overview

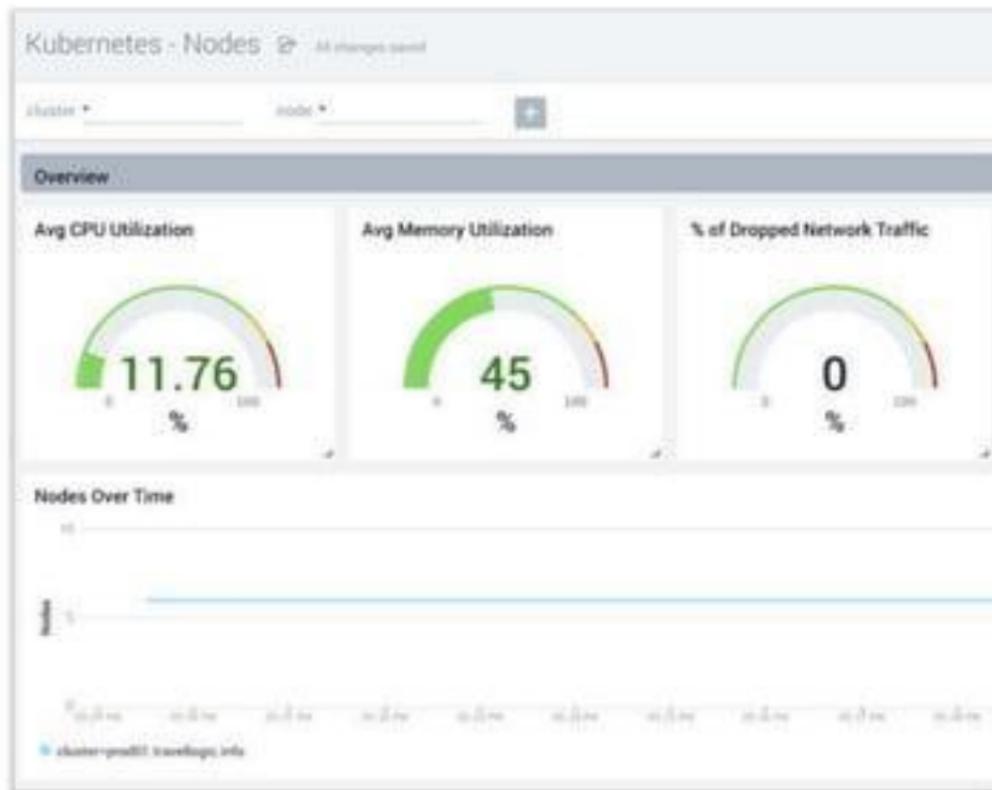
# Cluster Explorer dashboard

- Overview of memory and CPU usage per node and pod
- Each cell of the honeycomb charts represent a node or pod
- Color dynamically displays resource utilization relative to other nodes and pods



# Nodes dashboard

- Health and performance metrics for all nodes
- Compare long-term averages and trends



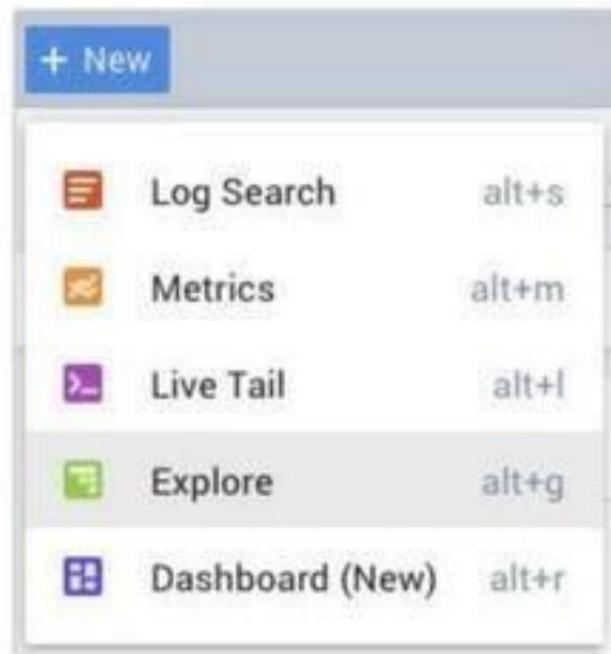
# Security Overview dashboard

- High-level details about alerts, events, and errors
- Configure rules with Falco
- See which rules, nodes, pods, or apps triggered your alerts



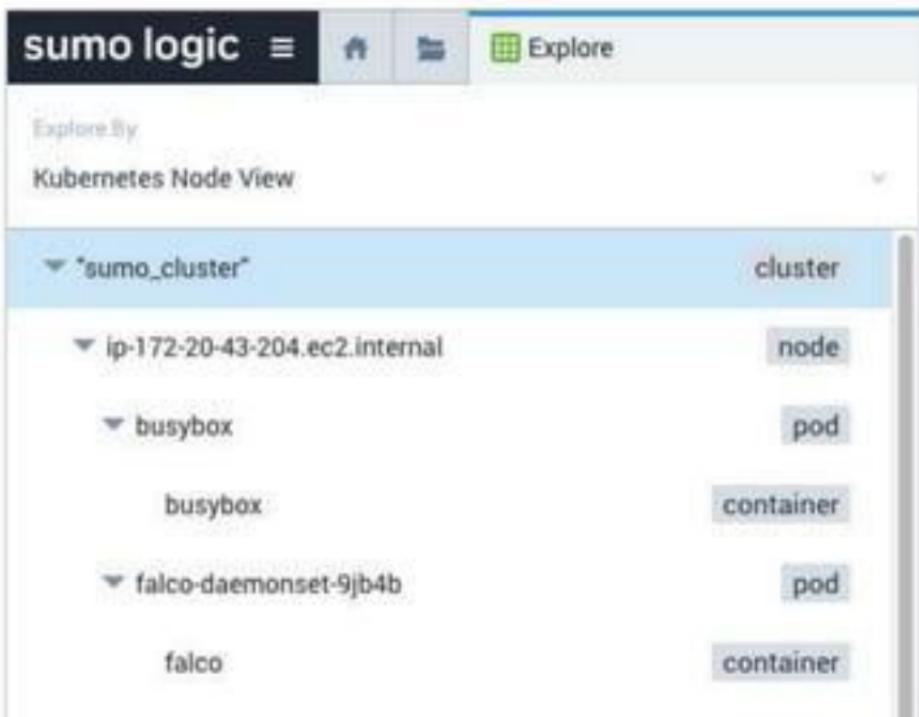
# The Explore Tab

- Different views to monitor your cluster from different perspectives.
- **Node View.** Visualize cluster hierarchy.
- **Deployment View.** Organize data by deployment to monitor performance.
- **Service View.** Organize pods and nodes used by each service.
- **Namespace View.** Track environments across teams or projects by namespace.



# Node View

- Visualize cluster hierarchy
- Explore infrastructure topology in public cloud, private cloud, or bare metal



# Deployment View

- Displays the deployments used by each namespace
- Shows which pods and containers run inside each deployment
- Monitor deployment performance and manage necessary changes



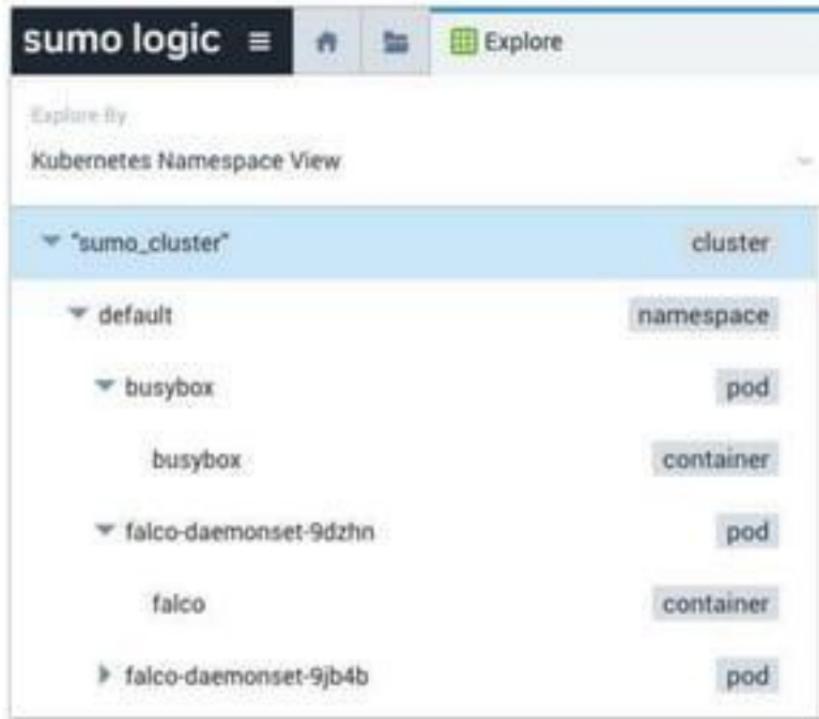
# Service View

- Displays services running in each namespace
- Monitor and improve UX



# Namespace View

- Organize your cluster into namespaces
- Useful for large clusters divided into teams or products



# Break time!

# Course Agenda (cont.)



- 15 min. ● Hands-on labs: Install apps; pre-built dashboards; Explore
- 5 min. ● Classic Dashboards and Dashboards (New)
- 15 min. ● Hands-on lab: Create a Dashboard (New)
- 5 min. ● Monitoring and troubleshooting
- 10 min. ● Demo: Troubleshoot a pod
- 10 min. ● Hands-on lab: Create an alert
- 60 min. ● Q&A and get certified as a Kubernetes on Sumo Logic user

## **Hands-on labs:**

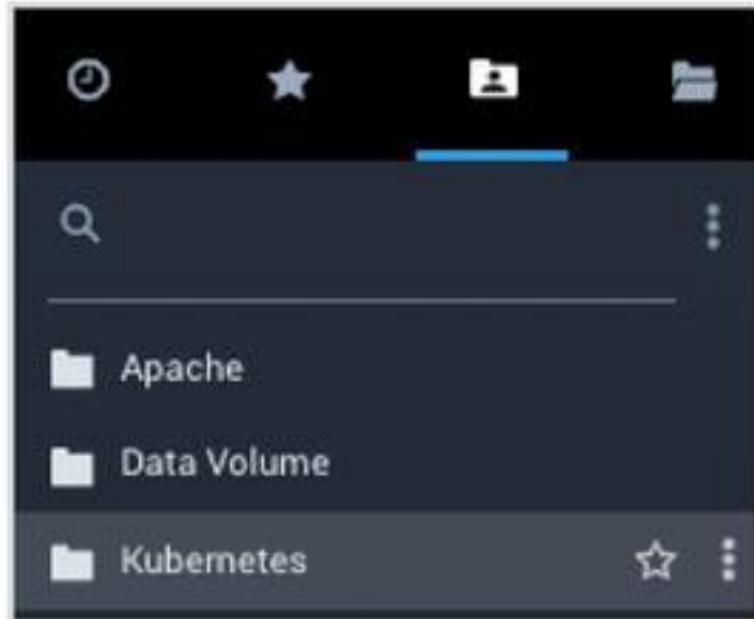
Install the Kubernetes app

View pre-built dashboards

Navigate with Explore

## Lab 3: Install the Kubernetes app

1. Check the **Personal** folder for the Kubernetes app.
2. Click **App Catalog** in the left nav.
3. Search for “Kubernetes.”
4. Install the Kubernetes app if it hasn’t already been installed.



# Lab 4: View pre-built dashboards

1. Open the **Kubernetes** folder under your personal folder.
2. Click the **Kubernetes - Cluster Overview** dashboard.
3. Use this dashboard to answer the questions in your lab guide.

The screenshot shows the Sumo Logic interface with a sidebar on the left and a main dashboard library on the right.

**Left Sidebar:**

- Personal
- Kubernetes
  - Kubernetes - Cluster Explorer
  - Kubernetes - Cluster Overview
  - Kubernetes - Container Logs
  - Kubernetes - Containers
  - Kubernetes - DowntimeSets etc.
  - Kubernetes - Deployment Over...
  - Kubernetes - DPM
  - Kubernetes - DPM - Timeseries
  - Kubernetes - Health Check
  - Kubernetes - Hygiene Check
  - Kubernetes - Namespace Over...
- App Catalog
- Manage Data
- Administration
- Help

**Right Panel:**

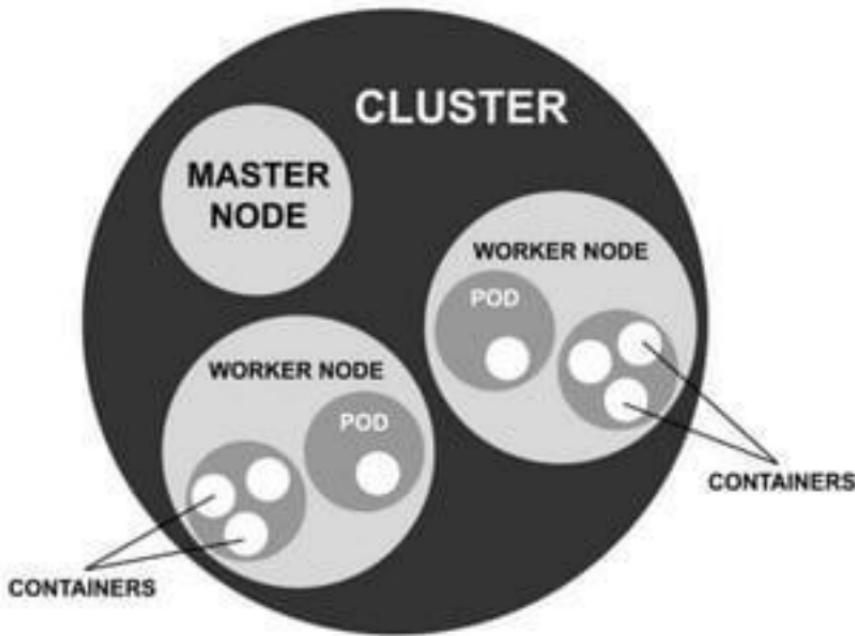
View as: Me

Library Personal Kubernetes

Name	Description
Kubernetes - Cluster Explorer	The Kubernetes - Cluster Explor...
Kubernetes - Cluster Overview	The Kubernetes - Cluster Overv...
Kubernetes - Container Logs	The Kubernetes - Container Log...
Kubernetes - Containers	The Kubernetes - Containers A...
Kubernetes - DowntimeSets etc.	The Kubernetes - Downtime Sets...
Kubernetes - Deployment Over...	The Kubernetes - Deployment Ove...
Kubernetes - DPM	The Kubernetes - DPM dashba...
Kubernetes - DPM - Timeseries	The Kubernetes - DPM Timeseri...
Kubernetes - Health Check	The Kubernetes - Health Check...
Kubernetes - Hygiene Check	The Kubernetes - Hygiene Chec...
Kubernetes - Namespace Over...	The Kubernetes - Namespace Ove...

# Lab 5: Navigate Kubernetes with Explore

1. Click **+New > Explore** to open an Explore tab.
2. Select the **Kubernetes - Node View**.
3. Drill down to find the nodes inside your cluster, the pods inside your nodes, and the containers inside your pods.



# Classic Dashboards and Dashboards (New)

## Classic Dashboard

- Basic charts, like time series and categorical
- Few color and font choices
- Panels created from search and metrics tabs
- Limited filters and queries
- Still supported

## Dashboard (New)

- New charts, like Honeycomb
- Full control over look and feel with JSON
- Build panels directly in the dashboard
- Advanced filtering and metrics query building

# Single values and text boxes

- Simplest panel types
- Single values can highlight key metrics
- Text boxes can provide explanation, like data sources or how to interpret data

Number of Active Nodes

29

nodes

## About

This dashboard shows the number of nodes that are active and some basic resource utilization statistics.

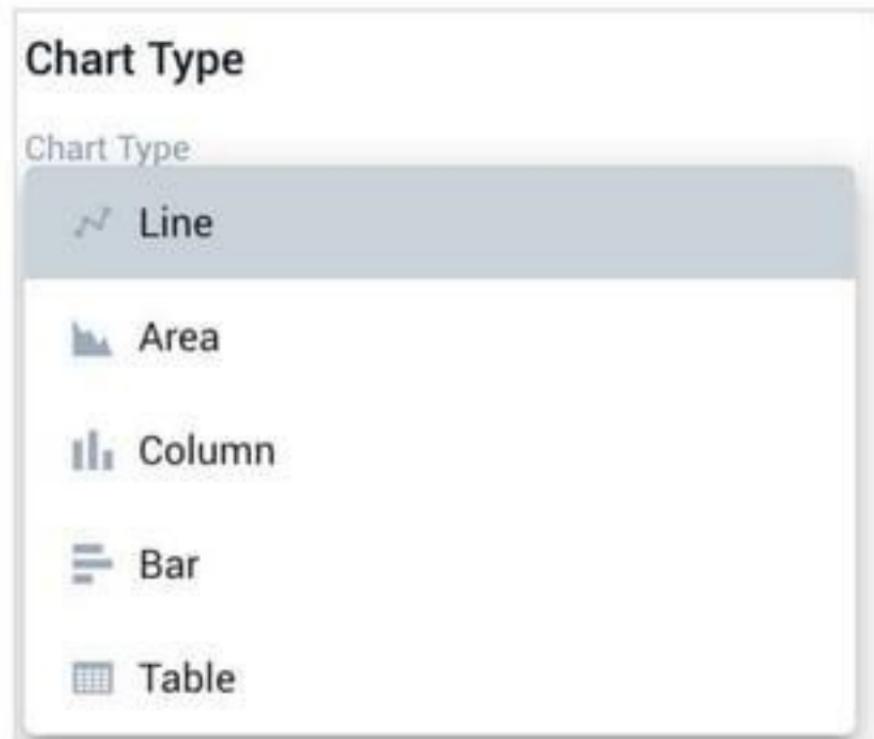
# Categorical charts

- Compare data across categories
- Pie charts to compare percentage of errors by error type
- Works best with **counts** or other categories



# Time series charts

- Compare data over time, like errors per minute or amount of resources used per hour
- Data must be **timesliced**



# Honeycombs and maps

- Map charts are great for geolocation data
- Honeycombs are great for comparing relative data
- Both display hotspots: physically or virtually



% of CPUs Limit by Pod



# **Hands-on labs:**

## Create a Dashboard (New)

# Lab 6: Create and share a Dashboard (New)

1. Create a four panel dashboard. The labs guide you through creating a text panel, single value, time series, and categorical chart.
2. Customize your dashboard. Try using your favorite colors or your company's brand colors.
3. Save and share your dashboard.



# Monitoring and Troubleshooting

# Troubleshooting and monitoring

- Does every alert or warning need your immediate attention?
- How can you find more information about an issue?
- How can you resolve the issue?



## Basic cluster checks

- How many worker nodes are unhealthy?
- What disk, CPU, and memory resources are being used up?
- Have any pods crashed?
- Is my autoscaler scaling out as expected?
- Are my requests getting routed as I expected?

# Common alerts

- **Crash loop.** Replication service keeps restarting pods.
- **Nodes not ready.** Insufficient resources allocated to a node.
- **Memory limits exceeded.** Container requests too much memory and may be destroyed and restarted.



## Ask for help

- 1. Get your company info.** Your company's account information and the your Sumo Logic account rep's contact.
- 2. Get your cluster info.** Details like cluster name, YAML files, version numbers, and how you collect data into Sumo Logic.
- 3. Describe the problem.** Document and gather things like log files, error codes, and a description of the problem.
- 4. Submit a ticket.** Go to <https://support.sumologic.com/>

# Demo

Troubleshoot a pod



# **Hands-on labs:**

## Create an alert

## Lab 8: Create an alert

1. Click **Manage Data > Alerts** to create a new metrics query.
2. Write your query and click the **Alerts** icon (bell).
3. Set up rules for when your alert is triggered, who gets notifications, and how those notifications are delivered.



Questions?

# Assessment

# Assessment Description

- 20+ questions
- 60 minutes to take it
- Need a 70% to pass
- Open Resource (slides, labs, and documentation)

The screenshot shows the Sumo Logic Training website. At the top, there's a navigation bar with icons for Home, Log In, and Sign Up. Below it is a header with the Sumo Logic logo and the text "Training". The main content area has a blue header with the text "Welcome to Sumo Logic Training!". Below this, there are two sections: "New to Sumo? Check our Onboarding Learning Path, it can get you up and running in just a few hours." and "Check out our Self-Paced Training to build your skills and when you are ready to get the credit you deserve, take our Certifications.". Underneath, there's a section titled "All Courses" with a grid of eight course thumbnails. Each thumbnail includes a small image, the course name, and the number of courses available.

Course Category	Thumbnail Image	Course Name	Number of Courses
Onboarding		Learning the Navigation Tips	1 Course
		Onboarding	3 Courses
Fundamentals		Fundamentals	4 Courses
		Fundamentals	3 Courses
Administration		Administration	4 Courses
		Administration	3 Courses

# Certification

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

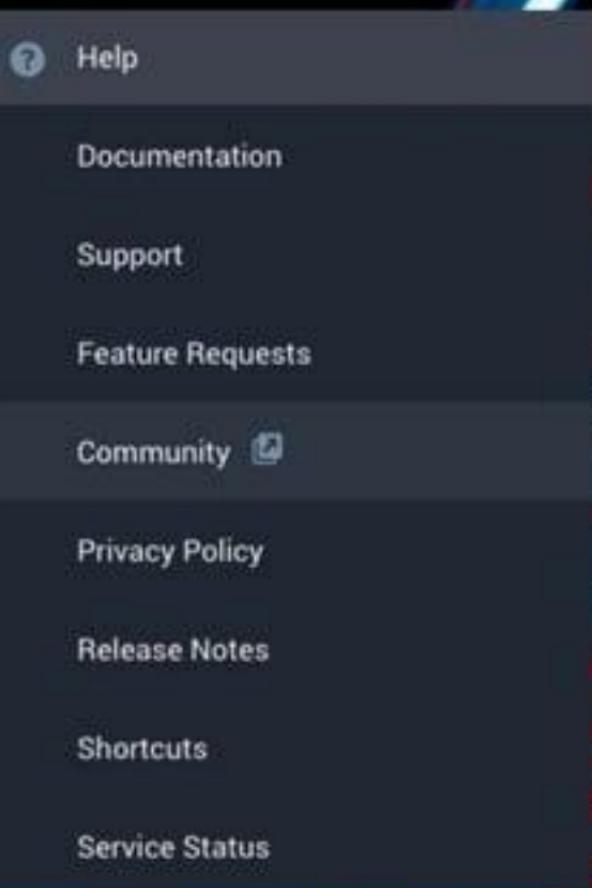
## Assessment:

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



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



# 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**

The image displays two screenshots of a web-based assessment interface. The top screenshot shows the 'sumo logic' logo and a question about finding a logo in a stack. It lists several review links and a search bar. The bottom screenshot shows the results page for the 'sumo logic' exam, displaying a 'Congratulations, Nelson, Onnal' message, a green circular progress bar at 90%, and a 'Close course' button.

# For passing the exam, you will earn:

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





Like Sumo Logic?  
Write a Gartner  
Peer Insights  
Review!



We'd love to hear from YOU!

Gartner Peer Insights is an anonymized, peer-to-peer collection of **enterprise product and service evaluations** from customers.

If you like Sumo Logic share your experience with your peers! Click on the QR code to start your review.

**Start your review today**  
*(it should only take 10-15 minutes)*



s

# Empowering the people who power modern business

u

sumo logic

o