Become a

Sumo Kubernetes Analyst

Advanced Metrics With K8s Certification

sumo logic

Course Agenda

kubernetes

10 min.	Intro our Kubernetes App
10 min.	Explain centralized data collection and enrichment
10 min.	Demo our Kubernetes capability
10 min.	Gain Insight into our four different views into Kubernetes
10 min.	Sumo Logic Apps available for Kubernetes
70 min.	Engage in Hands-on Labs
60 min.	Get certified as a Sumo Kubernetes Analyst

Learn about Kubernetes

Intro to Kubernetes (K8s)

kubernetes is an open source container orchestration platform developed by Google and is now managed by the Cloud Native Computing Foundation.

It provides automated deployment, scaling, and operations of applications across clusters of hosts. It provides **Desired State Management** for your cluster - define the cluster services system and it operates based on that set criteria.

Everything in Kubernetes is, by design, **ephemeral**. Kubernetes achieves its elastic ability to scale and contract by taking control over how pods—and the containers within those pods—are deployed.

And it runs anywhere, private, public cloud, or bare metal.

Meet the CLOUD NATIVE COMPUTING FOUNDATION (CNCF)

- Non-profit, part of the Linux Foundation
- Founded December 2015
- Members:
  - 18 Platinum
  - 19 Gold
  - 354 Silver
- https://www.cncf.io

Silver member: sumo logic

Key Kubernetes Terminology, Part 1

Cluster

A set of machines, called nodes, that run containerized applications managed by Kubernetes.
A cluster has at least one worker node and at least one master node. The worker node(s) host the pods that are the components of the application. The master node(s) manages the worker nodes and the pods in the cluster. Multiple master nodes are used to provide a cluster with failover and high availability.

Node

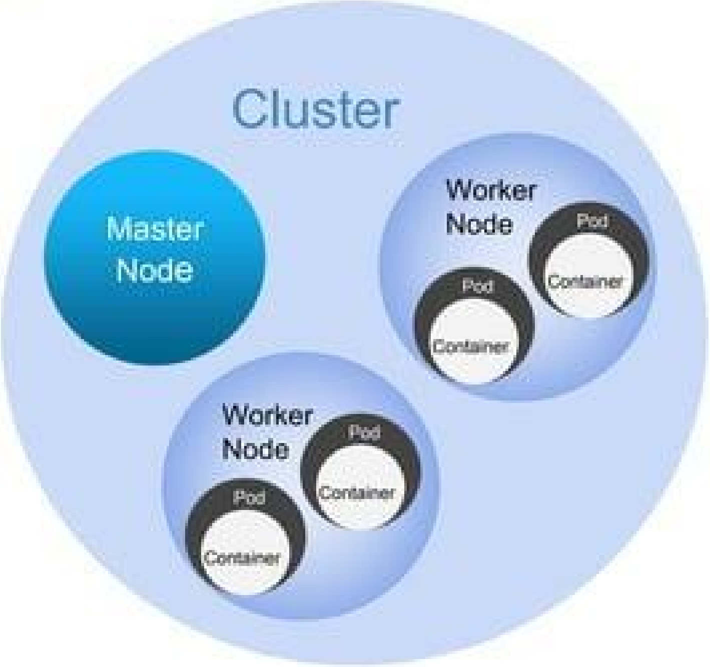
A node is a worker machine in Kubernetes. A worker node may be a VM or physical machine, depending on the cluster. It has local daemons or services necessary to run Pods and is managed by the control plane. The daemons on a node include kubelet, kube-proxy, and a container runtime implementing the CRI such as Docker.

Pod

The smallest and simplest Kubernetes object. A Pod represents a set of running containers on your cluster. A Pod is typically set up to run a single primary container. It can also run optional sidecar containers that add supplementary features like logging. Pods are commonly managed by a Deployment.

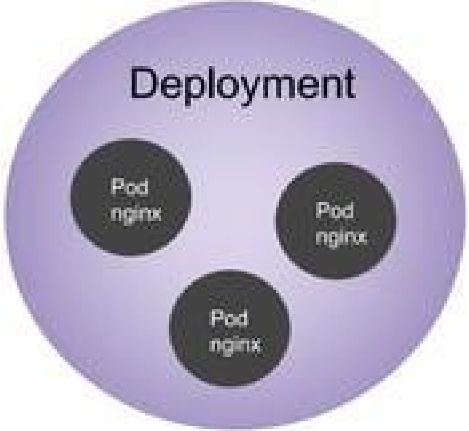
Container

A lightweight and portable executable image that contains software and all of its dependencies. *Containers decouple applications from underlying host infrastructure to make deployment easier in different cloud or OS environments, and for easier scaling.*



Source: https://kubernetes.io/docs/reference/glossary/?fundamental=true

Key Kubernetes Terminology, Part 2



Deployment

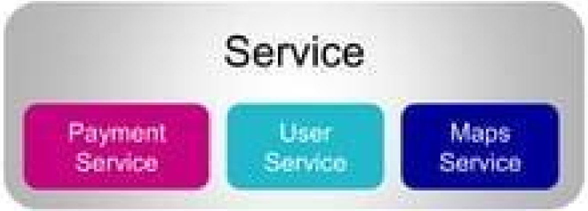
An abstraction to manage replications of a set of routines, protocols, and tools for building software applications. Each replica is represented by a pod, and the pods are distributed among the nodes of a cluster to achieve the Desired State Management.

Namespace

An abstraction to support multiple virtual clusters on the same physical cluster. Namespaces are used to organize objects in a cluster and provide a way to divide cluster resources. Names of resources need to be unique within a namespace, but not across namespaces.

Service

An abstract way to expose an application running on a set of Pods as a network service. The set of Pods targeted by a Service is (usually) determined by a selector. If more Pods are added or removed, the set of Pods matching the selector will change. The Service makes sure that network traffic can be directed to the current set of Pods for the workload.

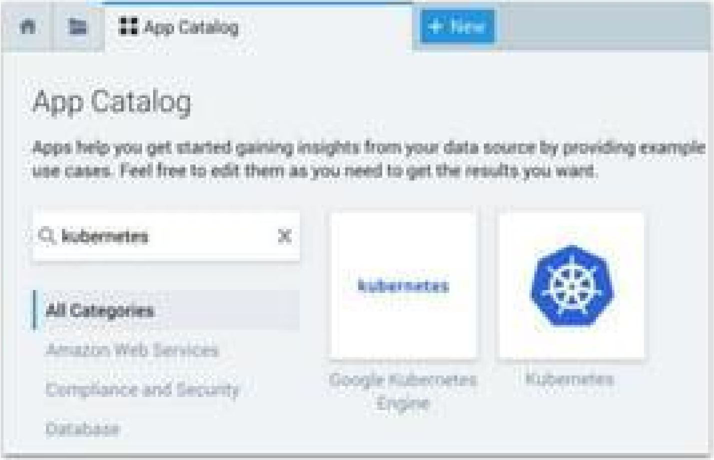


Our Kubernetes App

Provides **visibility** into the **worker nodes** and their **application logs**

You can **monitor and troubleshoot** container health, replication, load balancing, pod state and hardware resource allocation.

The App utilizes Falco events to **monitor and detect** abnormal container, application, host, and network activity.



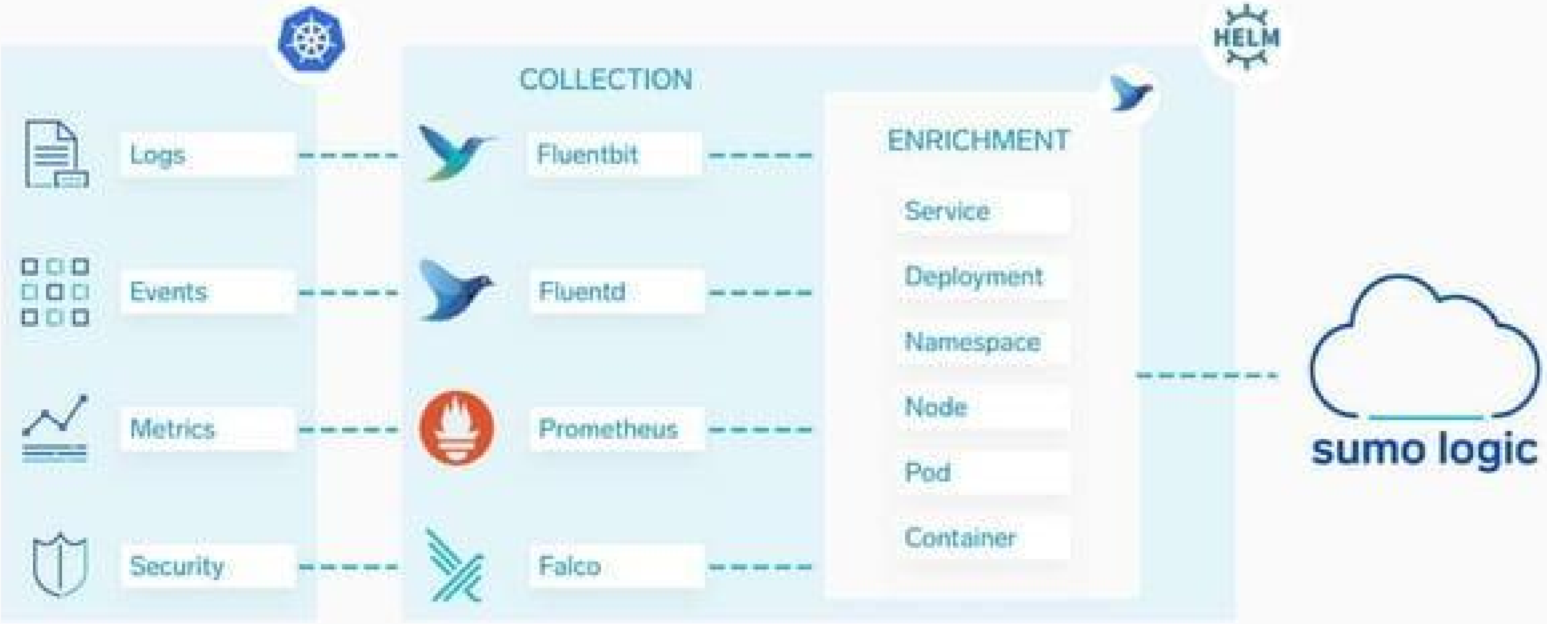
App Catalog

Apps help you get started gaining insights from your data source by providing example use cases. Feel free to edit them as you need to get the results you want.

A small 4 node k8s cluster can generate over 200,000 distinct metrics!

Data Collection and Enrichment

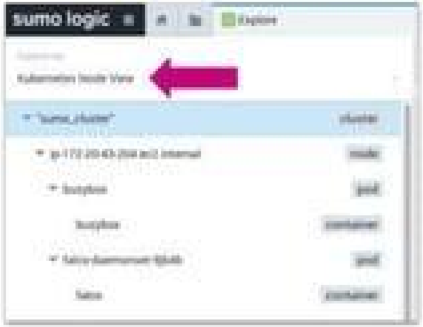
Centralized Data Collection with Sumo Logic



Demo Kubernetes

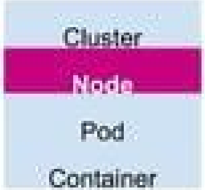
Monitoring and Troubleshooting Kubernetes at every level

Four different realtime views into your Kubernetes system

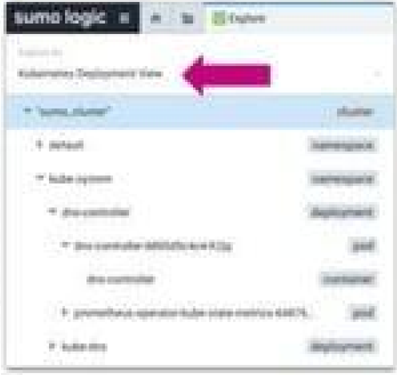


Explore By
Kubernetes Node View

- "sumo_cluster" — cluster
  - ip-172-20-43-204.ec2.internal — node
    - busybox — pod
      - busybox — container
    - falco-daemonset-[illegible] — pod
      - falco — container

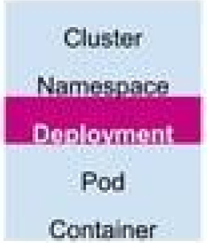


Observe the infrastructure topology of resources - private, public cloud, or bare metal

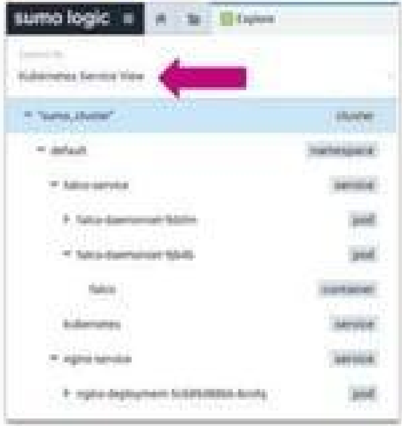


Explore By
Kubernetes Deployment View

- "sumo_cluster" — cluster
  - default — namespace
  - kube-system — namespace
    - dns-controller — deployment
      - dns-controller-[illegible] — pod
        - dns-controller — container
      - prometheus-operator-kube-state-metrics-[illegible] — pod
    - kube-dns — deployment

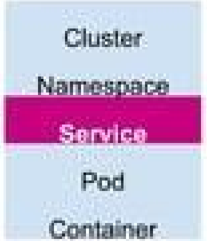


See how your deployment is performing to your set criteria and manage changes

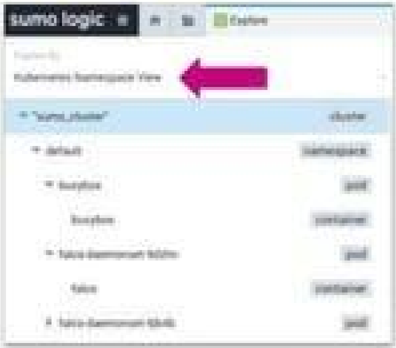


Explore By
Kubernetes Service View

- "sumo_cluster" — cluster
  - default — namespace
    - falco-service — service
      - falco-daemonset-[illegible] — pod
      - falco-daemonset-[illegible] — pod
        - falco — container
    - kubernetes — service
    - nginx-service — service
      - nginx-deployment-[illegible] — pod

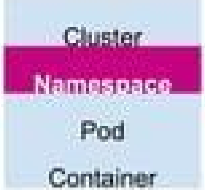


Monitor to improve your user experience



Explore By
Kubernetes Namespace View

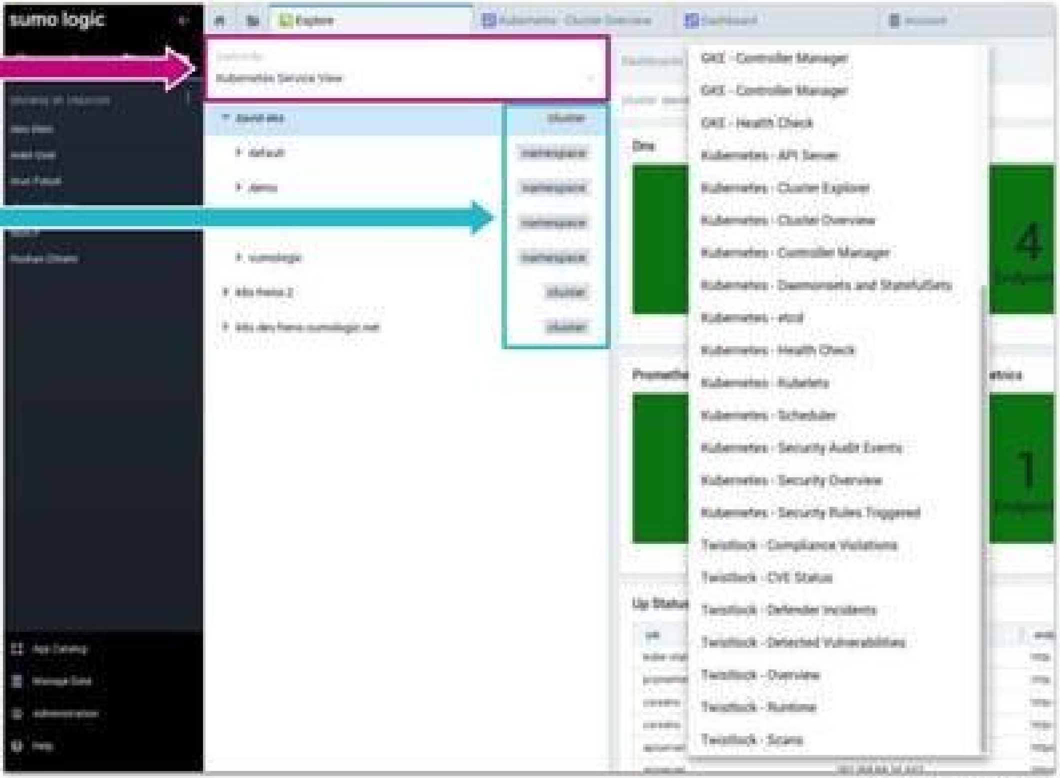
- "sumo_cluster" — cluster
  - default — namespace
    - busybox — pod
      - busybox — container
    - falco-daemonset-[illegible] — pod
      - falco — container
    - falco-daemonset-[illegible] — pod



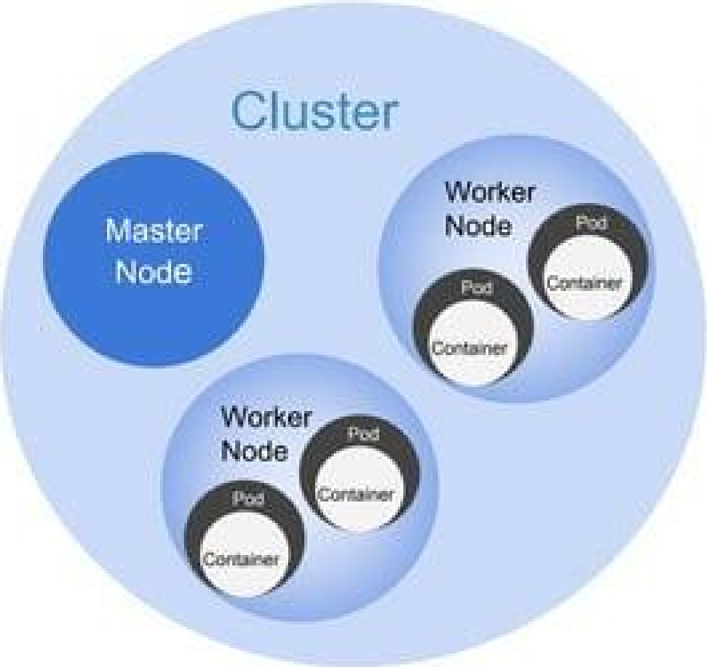
Track environments with many users spread across multiple teams, or projects like dev, lab, and prod

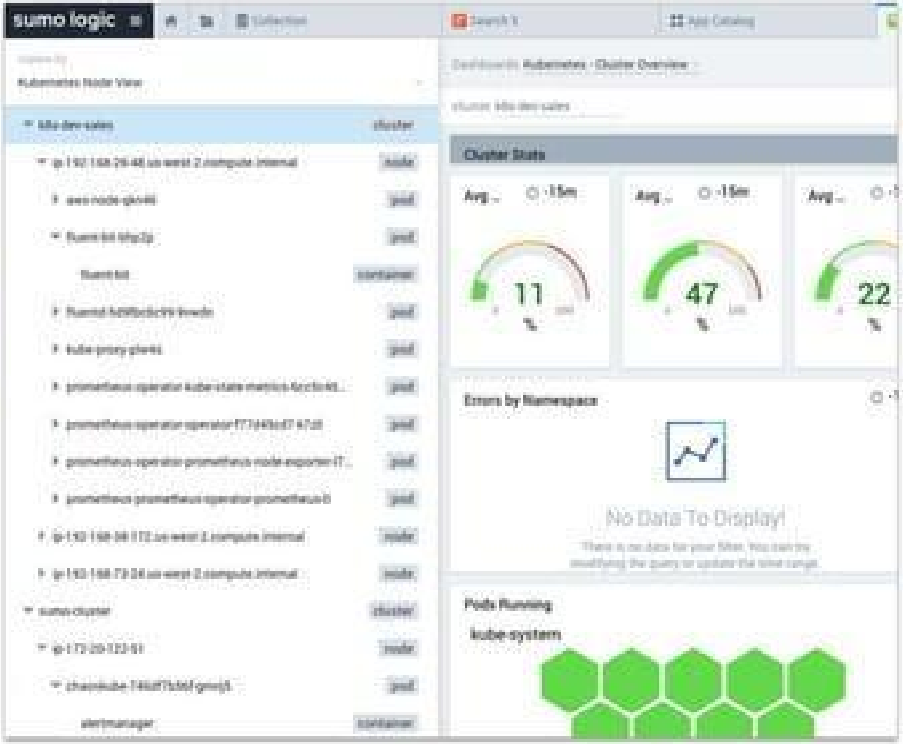
Explore tabs interconnected with dashboards

- **Dashboards are filtered** by choosing one of the four views in **Explore By**
- **Metadata** enables us to build a hierarchical view
- **Explore the Kubernetes stack** by connecting pods to their services or group nodes by cluster
- **Real-time dashboards** by tapping into the auto-discovery capabilities inherent in Prometheus, we can ensure that the hierarchy visualized in Sumo Logic is accurate and up to date.



Infrastructure-centric visibility (Node view)





Explore By
Kubernetes Node View

- k8s-dev-sales — cluster
  - ip-192-168-29-48.us-west-2.compute.internal — node
    - aws-node-gkn46 — pod
    - fluent-bit-b9p2p — pod
      - fluent-bit — container
    - fluentd-5d9f8c6c99-8nwdv — pod
    - kube-proxy-plwks — pod
    - prometheus-operator-kube-state-metrics-5cc5c45... — pod
    - prometheus-operator-operator-f77645cd7-k7zt — pod
    - prometheus-operator-prometheus-node-exporter-l7... — pod
    - prometheus-prometheus-operator-prometheus-0 — pod
  - ip-192-168-38-172.us-west-2.compute.internal — node
  - ip-192-168-73-24.us-west-2.compute.internal — node
- sumo-cluster — cluster
  - ip-172-20-123-51 — node
    - chaoskube-7460f7b56f-gmrj5 — pod
      - alertmanager — container

Dashboards › Kubernetes - Cluster Overview

cluster: k8s-dev-sales

Cluster Stats

Errors by Namespace

No Data To Display!

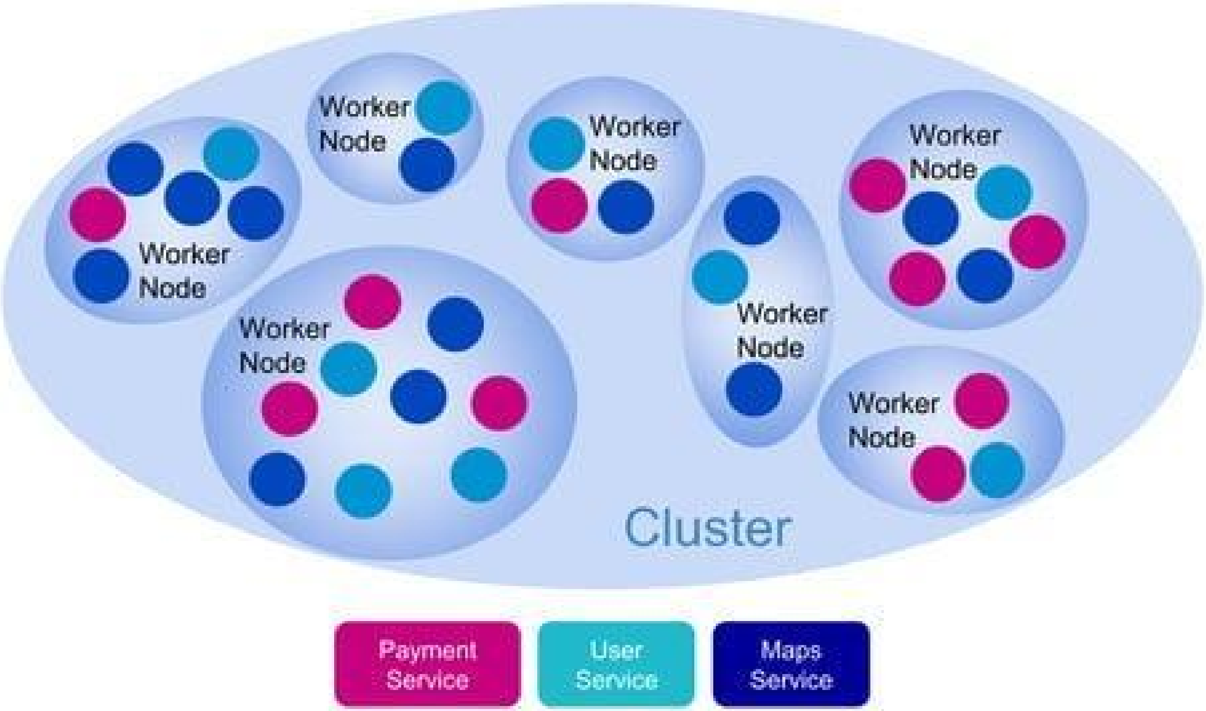
There is no data for your filter. You can try modifying the query or update the time range.

Pods Running

kube-system

View your services from a cluster perspective

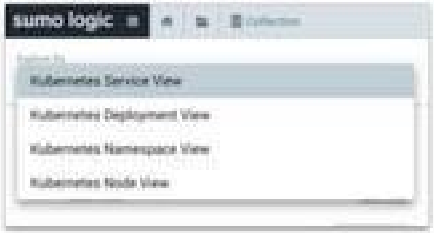
- Very **complex** to examine ephemeral services as pods are spread out in a node based view
- May be **slow** to find and troubleshoot service issues
- Node view is **disconnected** from the customer user experience



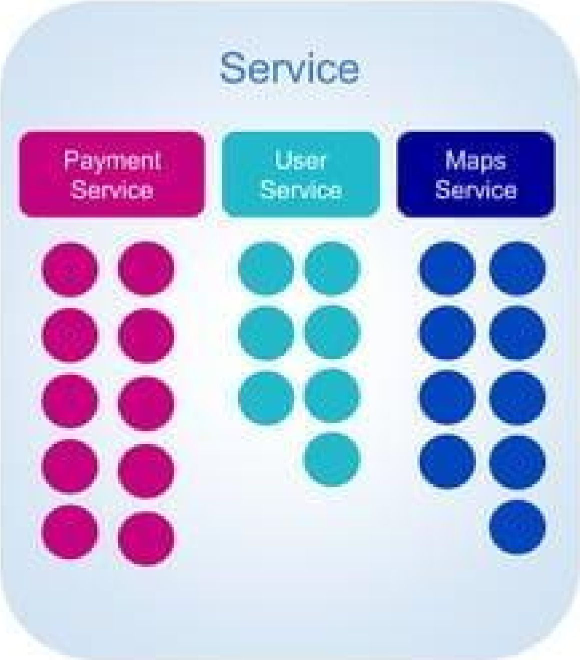
sumo logic

Sumo Logic confidential

Now, look at your services from a Service-centric view



- **Easy** to locate your services, if you look from the services view
- **Quick** to find and troubleshoot issues due to organization and filtration
- **Tightly connected** to the customer user experience to maintain the customer interface and satisfaction



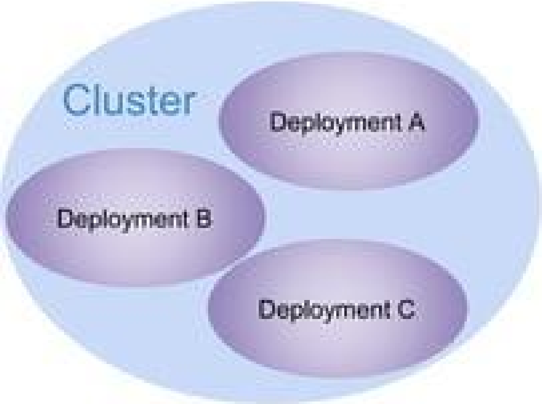
Service

Payment Service

User Service

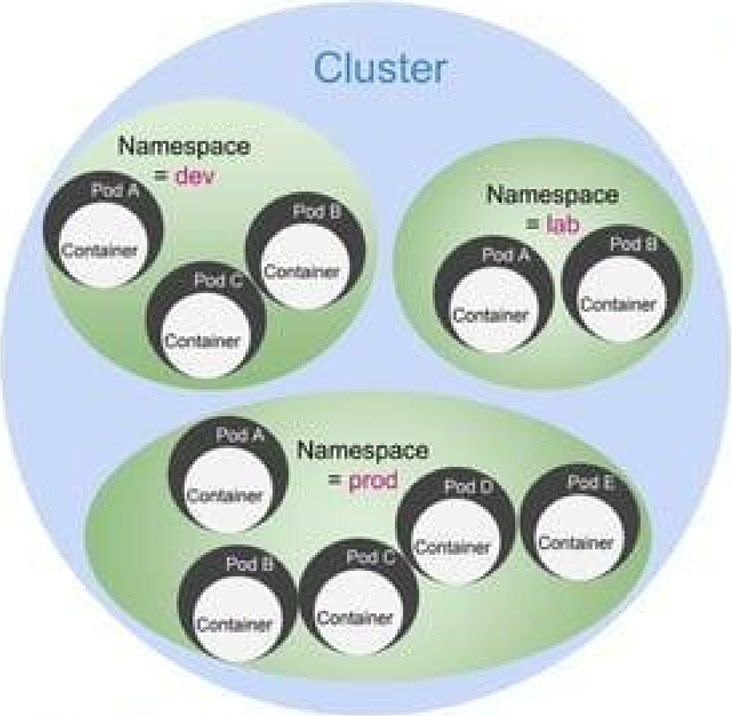
Maps Service

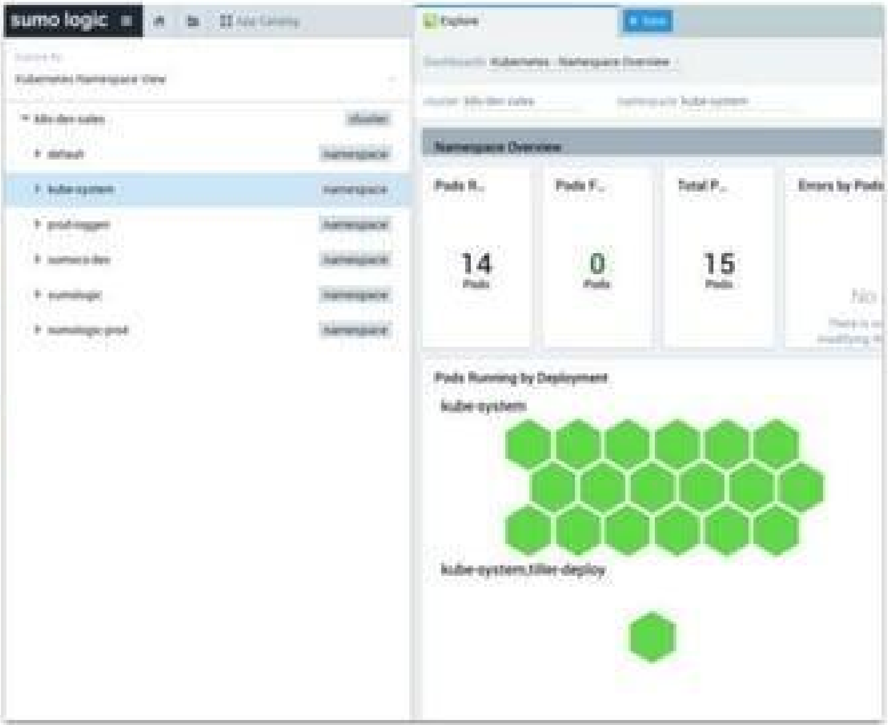
Deployment-centric visibility



This image cannot currently be displayed.

Namespace-centric visibility





Explore By

Kubernetes Namespace View

- k8s-dev-sales — cluster
  - default — namespace
  - kube-system — namespace
  - prod-logger — namespace
  - sumoco-dev — namespace
  - sumologic — namespace
  - sumologic-prod — namespace

Dashboards: Kubernetes - Namespace Overview

cluster: k8s-dev-sales namespace: kube-system

Namespace Overview

Pods R...	Pods F...	Total P...	Errors by Pods
14 Pods	0 Pods	15 Pods	No

Pods Running by Deployment

kube-system

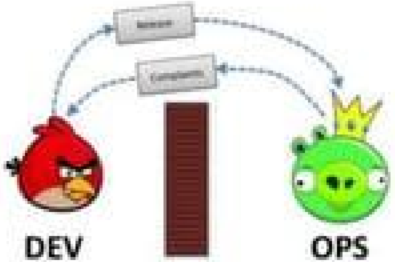
kube-system,tiller-deploy

Use Case: Helps prove and sell DevOps automation

A Continuous Integration/Continuous Delivery (CI/CD) pipeline helps software development organizations **automate** various steps in **getting software deployed to production environment.**

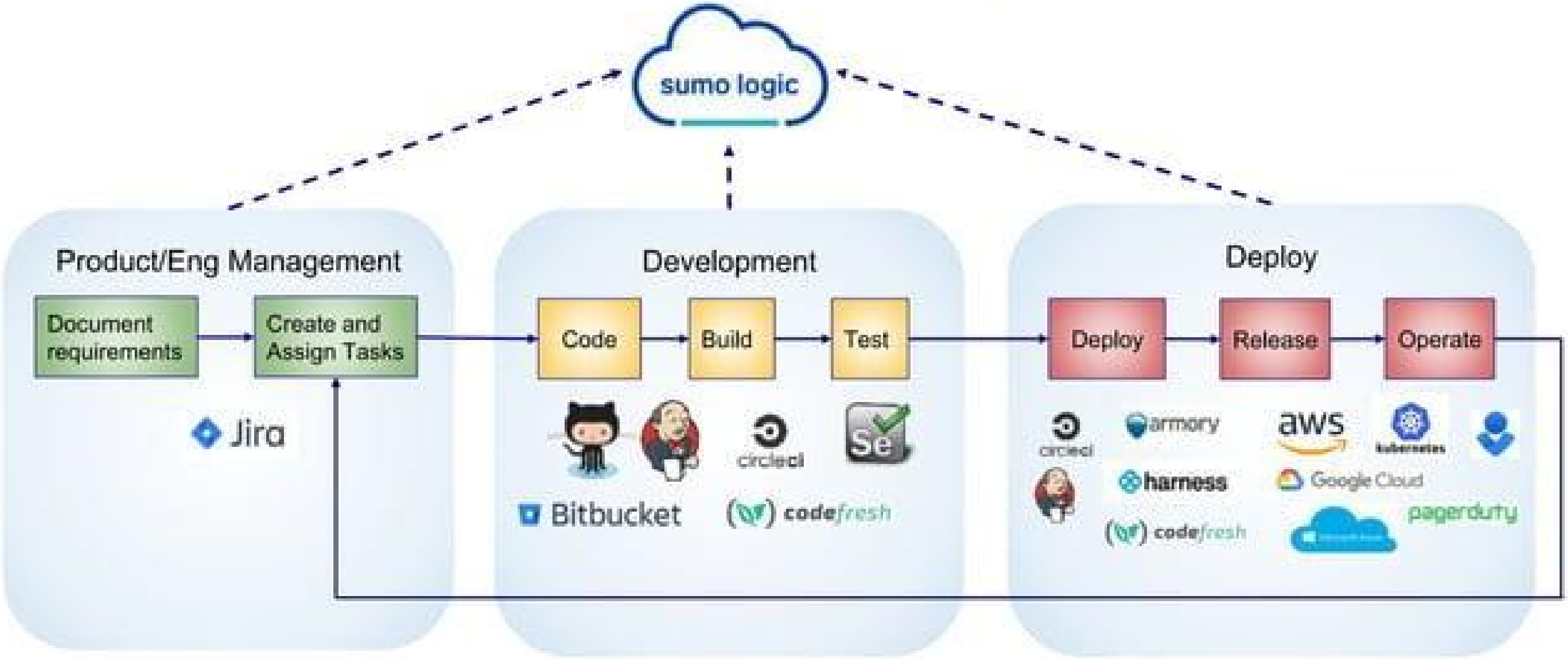
Container orchestration monitoring and troubleshooting has impacted every aspect of modern software development and deployment

"We want to launch new things whenever we want."



"Once everything is working, let's not change anything."

We can monitor & troubleshoot your CI/CD



sumo logic

Product/Eng Management

Document requirements → Create and Assign Tasks

Development

Code → Build → Test

Deploy

Deploy → Release → Operate

Sumo Logic Apps available for Kubernetes

Our Kubernetes Cluster Apps and Why You Need Them

App	Purpose	Details
kubernetes Core Falco	Operations and Security	Provides visibility into the operations and security of worker nodes of a cluster, as well as application logs of the worker nodes. Install only one instance of the Kubernetes app; one app can monitor multiple clusters. Utilizes Falco events to monitor and detect abnormal container, application, host, and network activity. Install one of the Control Plane apps, after the Kubernetes app is installed, based on your deployment.
kubernetes Control Plane Falco	Cluster Control Plane	Monitors the master node control plane, including the API server, etcd, kube-system and worker nodes. The App utilizes Falco Kubernetes Audit events to monitor and detect notable or suspicious activity such as creating pods that are privileged, mount sensitive host paths, use host networking, and the like.
Google Kubernetes Engine Azure Kubernetes Service (AKS)	Provider Control Planes	Provides insights into the master node / vendor-specific control plane, including the API server, control-manager, kube-scheduler, etcd and kube-system.

Our Kubernetes Partner Apps - CI/CD

App	Purpose	Details
circleci	CI/CD	Helps you monitor and secure their DevOps pipeline to ensure quality and increase delivery velocity
Istio	CI/CD	Reduces the complexity of managing Kubernetes deployments by providing a uniform platform for securing, connecting, and monitoring microservices
Spinnaker	CI/CD	Spinnaker is a continuous delivery and infrastructure management platform for hybrid-cloud, multi-cloud, and Kubernetes. Leverage Spinnaker to deploy with more consistency, automation, and safety, increasing your pace of software innovation by orders of magnitude.

Our Kubernetes Partner Apps - Security

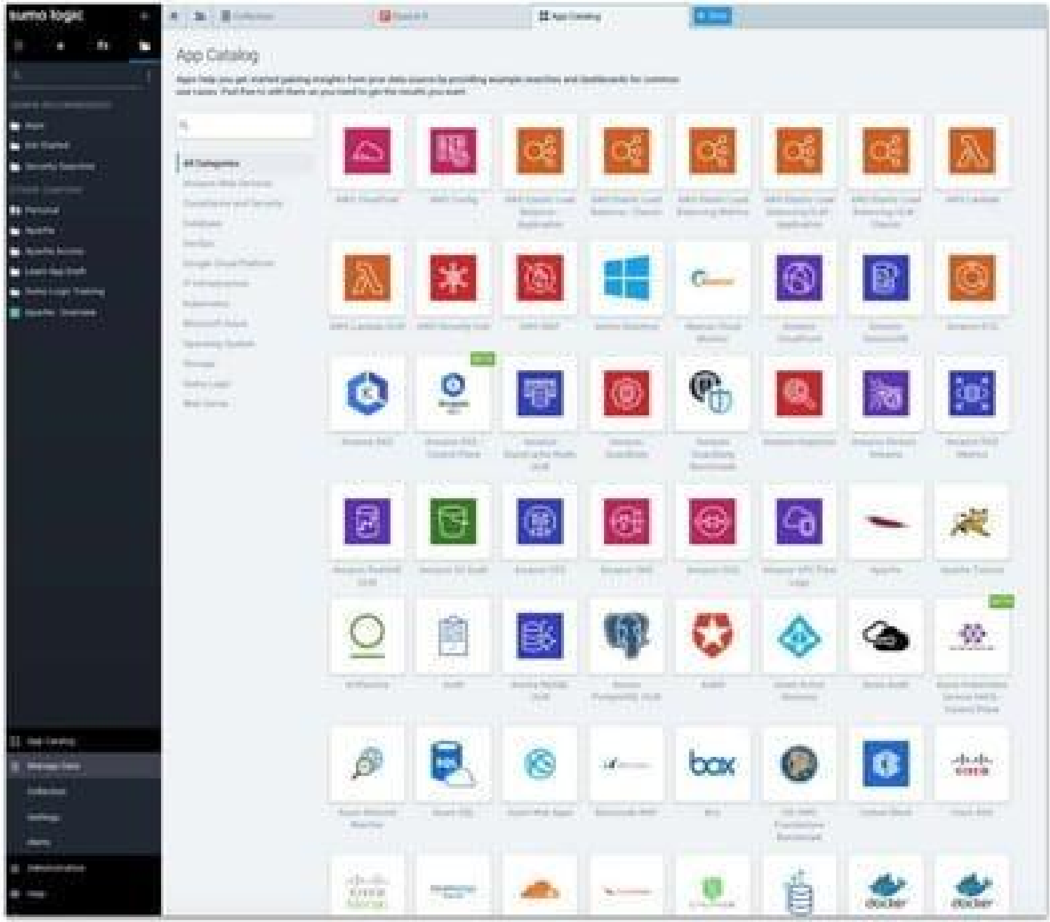
App	Purpose	Details
Twistlock	SecOps	Provides comprehensive monitoring and analysis solution for detecting vulnerabilities and potential threats throughout your environment, including hosts, containers, images and registry.
StackRox	SecOps	Helps you detect, investigate, and remediate vulnerabilities, insecure configurations, compliance violations, and runtime threats across all container and Kubernetes environments.
aqua	SecOps	Provides granular security and compliance control monitoring to DevSecOps teams throughout the cloud native application lifecycle, from development to runtime in production.
JFrog Xray	SecOps	Gives customers the ability to detect, investigate, and remediate vulnerabilities in software artifacts across your deployment environments.

Install any App from our Catalog

200+ Apps available

Your can preview an Apps capability

Once installed, Apps will appear in your personal folder



sumo logic

Hands-on Labs

Tutorial: Hands-on Exercises

Training Environment:

Go to: service.sumologic.com

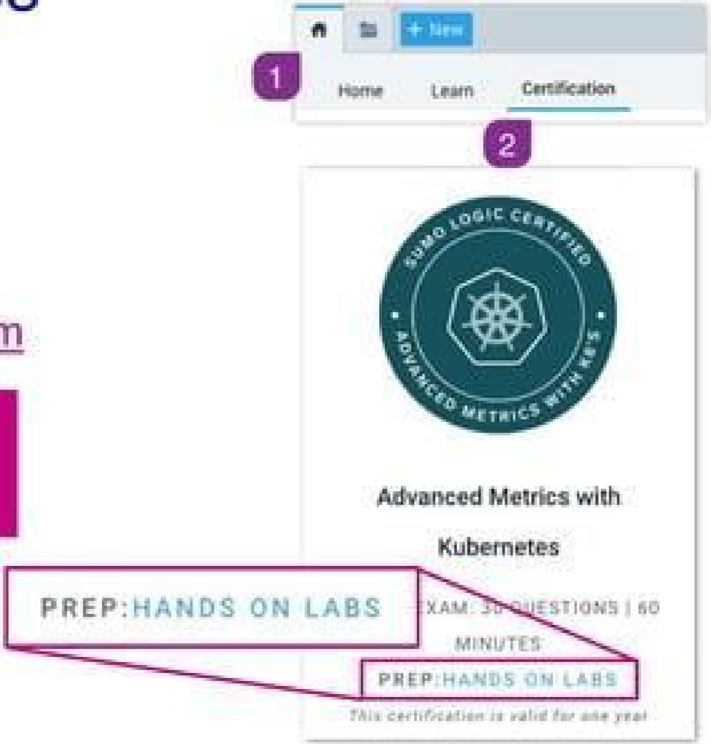
username: training+user###@sumologic.com

password:

will be a number between 000 and 800

Hands-on Labs:

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



Advanced Metrics with Kubernetes

EXAM: 30 QUESTIONS | 60 MINUTES

PREP:HANDS ON LABS

This certification is valid for one year s u

Empowering the people who power modern business

m o

sumo logic

Labs 1-5

Kubernetes App Features

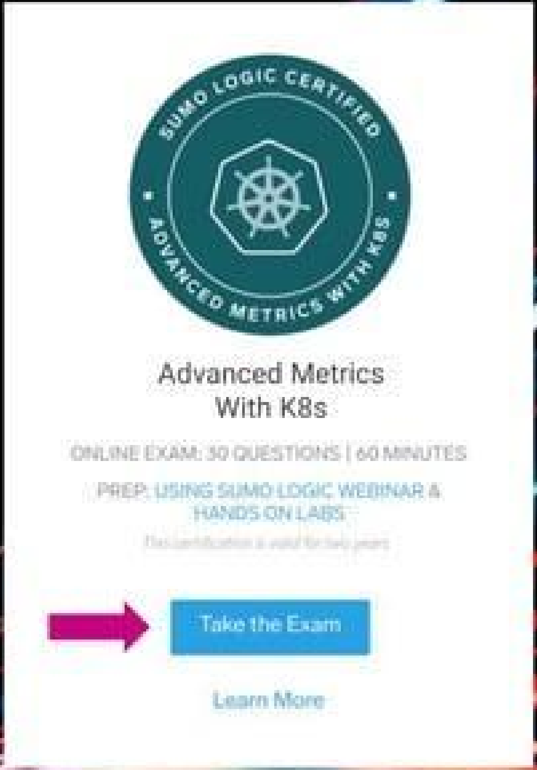
1. Centralized metadata enrichment enabling consistent tagging across logs, metrics, events
2. Service-centric, node-centric, deployment and namespace views
3. Dynamic live state dashboards to keep up with your Kubernetes environment
4. Unified visibility combines metrics + logs + events in a real-time view
5. Cloud Native Computing Foundation (CNCF) standards-based
6. Out of the box security that integrates easily into existing dashboards

Questions?

In order to get credit for the exam,

In YOUR OWN INSTANCE, go to Certification Tab.

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



Advanced Metrics
With K8s

ONLINE EXAM: 30 QUESTIONS | 60 MINUTES

PREP: USING SUMO LOGIC WEBINAR & HANDS ON LABS

This certification is valid for two years

Sumo Logic Certification

- Make sure to log out of the training account you were using and sign in with your own account
- If you do not have a working login, go to sumologic.talentlms.com to sign up for an account

sumo logic

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

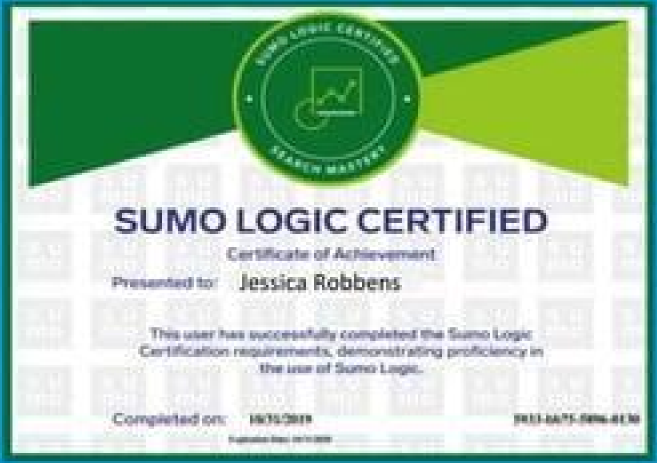
- Click on Help in the black left bar
- Click Community in the black left bar
- An email verification should be sent
- Once you verify, you should able to take the exam without any issues

sumo logic

Sumo Logic Confidential

For passing the exam, you will earn:

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



SUMO LOGIC CERTIFIED
SEARCH MASTERY

SUMO LOGIC CERTIFIED

Certificate of Achievement

Presented to: Jessica Robbens

This user has successfully completed the Sumo Logic Certification requirements, demonstrating proficiency in the use of Sumo Logic.

Completed on: 10/31/2019 [illegible]

[illegible]

How did we do?

Please take our survey:

https://forms.gle/2KMtxPuD9cSYV8SJ6

sumo logic

s u

Empowering the people who power modern business

m o

sumo logic