sumo logic

Become a

Sumo Administrator

Administration Certification

Course Agenda

10 min.	Download files needed for lab 1
20 min.	Data Collectors and metadata
30 min.	**Hands on labs 1, 2, & 5:** Set up a collector with two sources
25 min.	Optimization tools
20 min.	Overview Administration setup
15 min.	**Hands on labs 3 & 6**: Install an app and create an data ingest alert
60 min.	Examination

Become a Sumo Power Admin

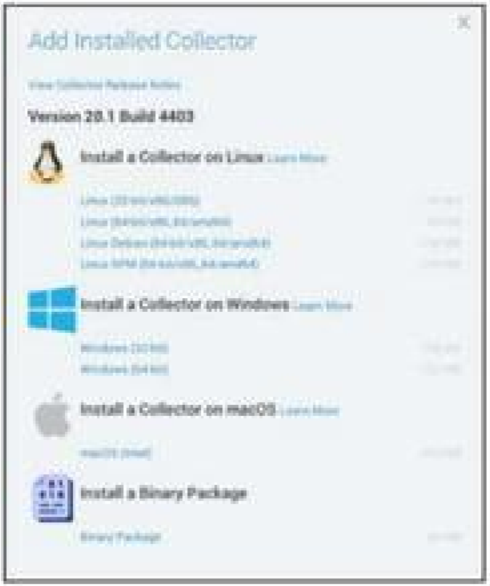
- Deploy a **data collection strategy** that best fits your environment
- Implement **best practices** around data collection
- Develop a **robust naming convention** for your metadata
- Learn to utilize **optimization tools**
- Discuss administration setup
- Create, **share and recommend** Searches and Dashboards

Download files needed for lab 1

1. Download the apache log file

   apache_access_logs_tutorial.txt

2. Download the collector installation package



Add Installed Collector

View Collector Package Notes

Version 20.1 Build 4403

Install a Collector on Linux Learn More

Linux (32-bit x86/i386) [illegible]
Linux (64-bit x86_64/amd64) [illegible]
Linux Debian (64-bit x86_64/amd64) [illegible]
Linux RPM (64-bit x86_64/amd64) [illegible]

Install a Collector on Windows Learn More

Windows (32-bit) [illegible]
Windows (64-bit) [illegible]

Install a Collector on macOS Learn More

macOS (Intel) [illegible]

Install a Binary Package

Binary Package [illegible]

Tutorial: Hands-on Exercises

Training Environment:

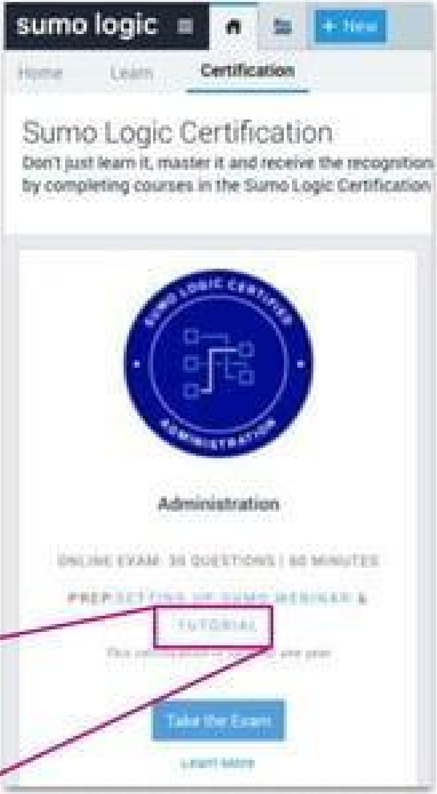
service.sumologic.com

username: training+labs@sumologic.com

password:

Hands-on Labs:

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



Sumo Logic Certification

Don't just learn it, master it and receive the recognition by completing courses in the Sumo Logic Certification

Administration

ONLINE EXAM: 30 QUESTIONS | 60 MINUTES

PREP: SETTING UP SUMO WEBINAR & TUTORIAL

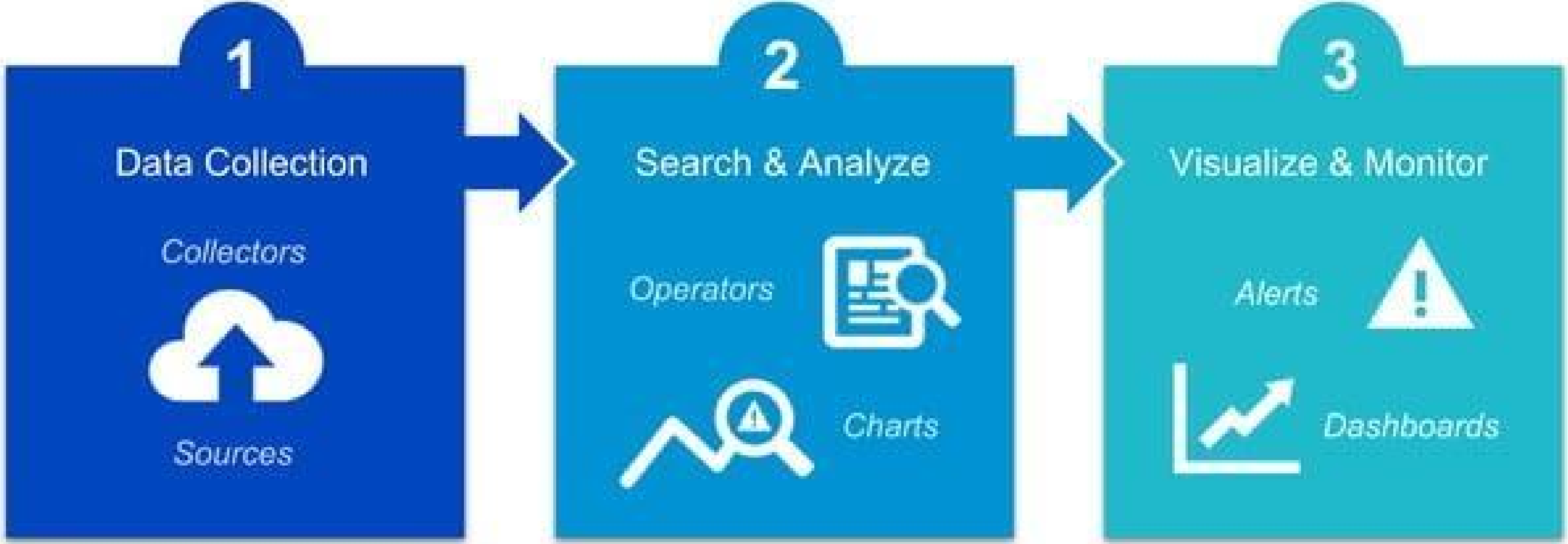
This [illegible] one year

High-Level Data Flow

Conditional Logic, Filtering, Formatting Results

sumo logic

Sumo Logic Data Flow

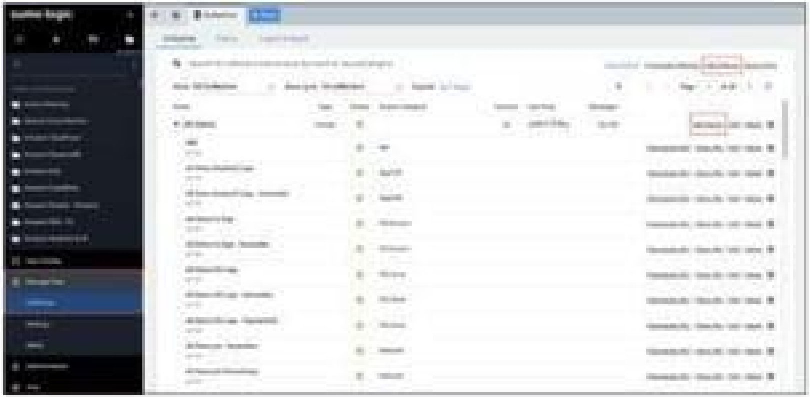


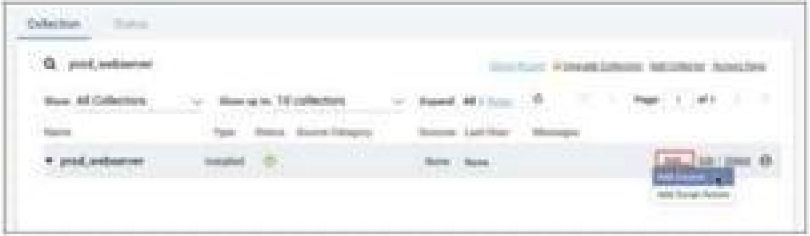
Step 1: Getting your data into Sumo

The journey of 10,000 logs begins with a single collector.

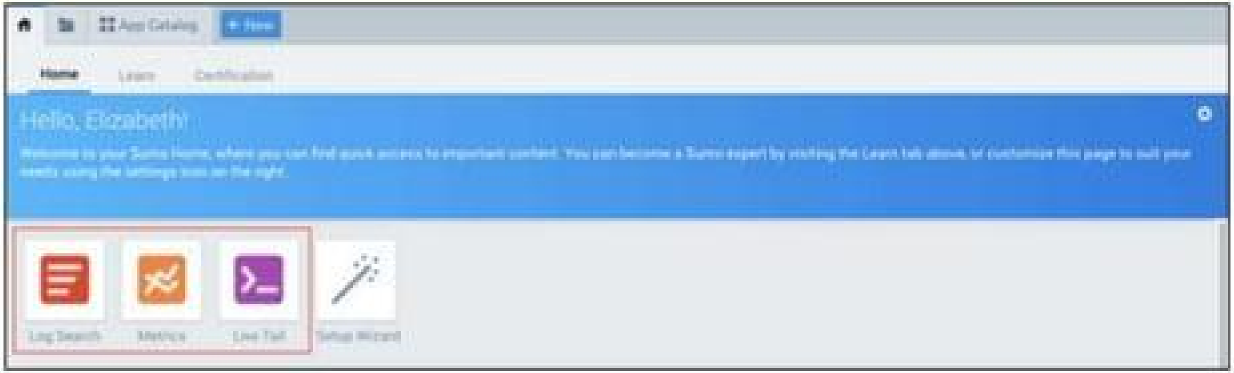
You start your data analytics journey by sending your data to Sumo.

You do this by setting up a local Installed Collector or web-Hosted Collector, then choosing the data sources that will provide the most value for you.





Step 2: Searching and analyzing your data



Hello, Elizabeth!

Welcome to your Sumo Home, where you can find quick access to important content. You can become a Sumo expert by visiting the Learn tab above, or customize this page to suit your needs using the settings icon on the right.

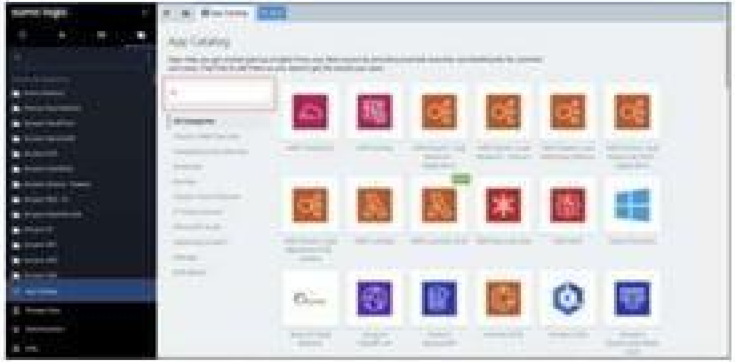
Once your data is available in Sumo, you and your co-workers can search your logs and metrics to identify unusual conditions or errors that could indicate a problem. You do this by creating queries and parsing the resulting messages.

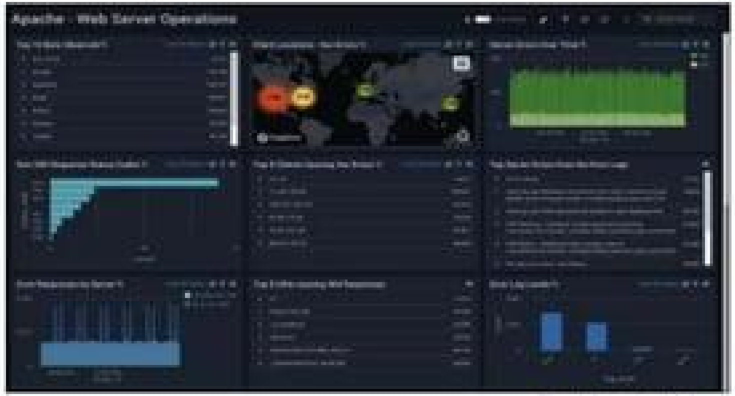
You can start a log search, metrics search, live tail, explore, or dashboard from the Sumo Home page by clicking +New. For walkthrough instructions on how to create a query and parse the messages, see the Search Log Data tutorial.

Step 3: Visualize & Monitor

You can view the library of available apps by selecting App Catalog in the left navigation panel, then scrolling through the library or entering a name in the search field. For more information, see the Install an App and View Data tutorial.

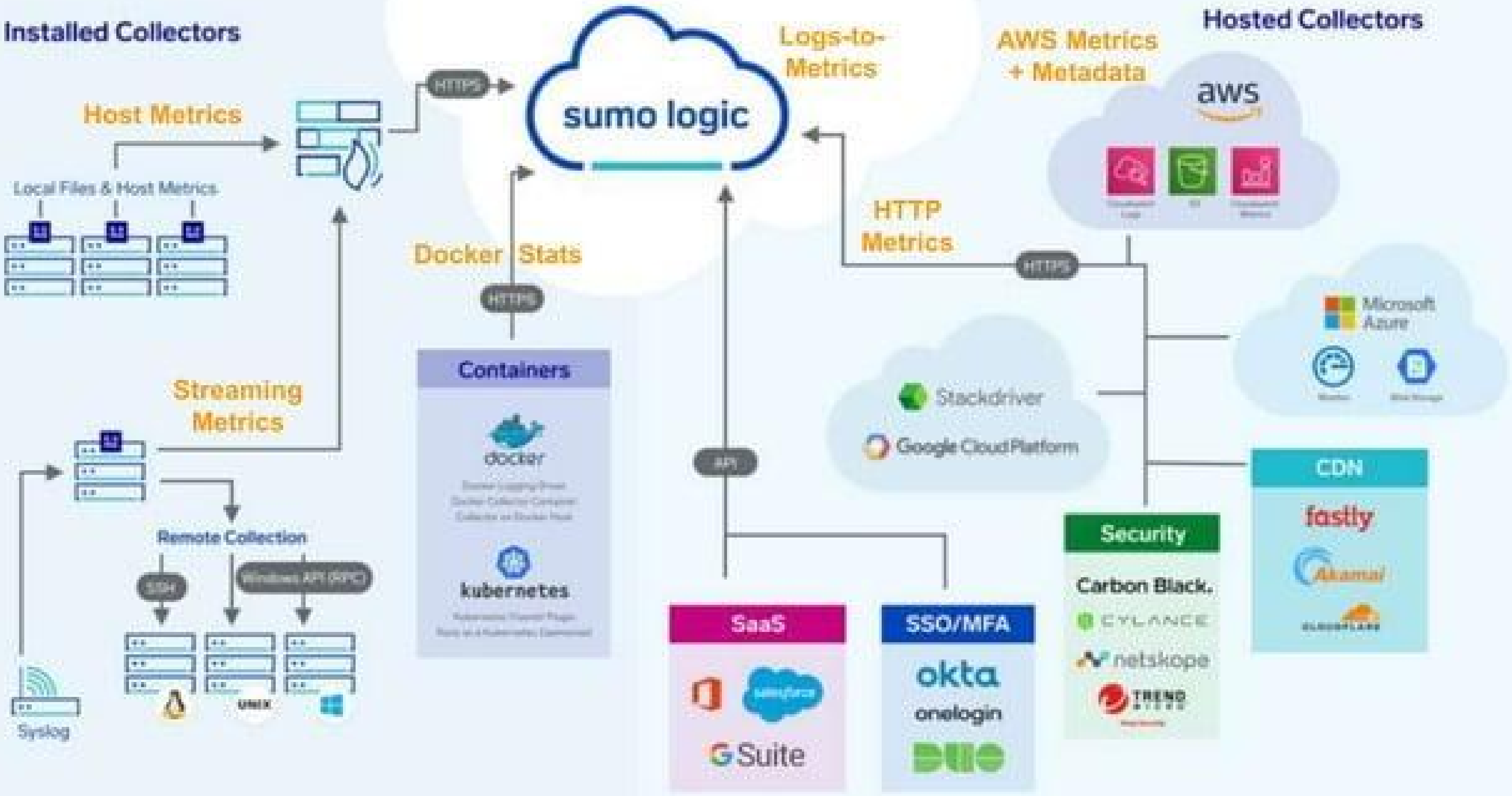
You can view your data with predefined searches and dashboards that facilitate monitoring and troubleshooting. For more information, see the Collect and Visualize Host Metrics tutorial.





Data Collection Strategy

sumo logic



Installed Collectors

Hosted Collectors

Host Metrics

Local Files & Host Metrics

Streaming Metrics

Remote Collection

Syslog

Docker Stats

Containers

Logs-to-Metrics

AWS Metrics + Metadata

HTTP Metrics

SaaS

SSO/MFA

Security

CDN

Compare Collectors

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

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

How many Collectors do you need?

An Installed Collector on a dedicated machine

When you:

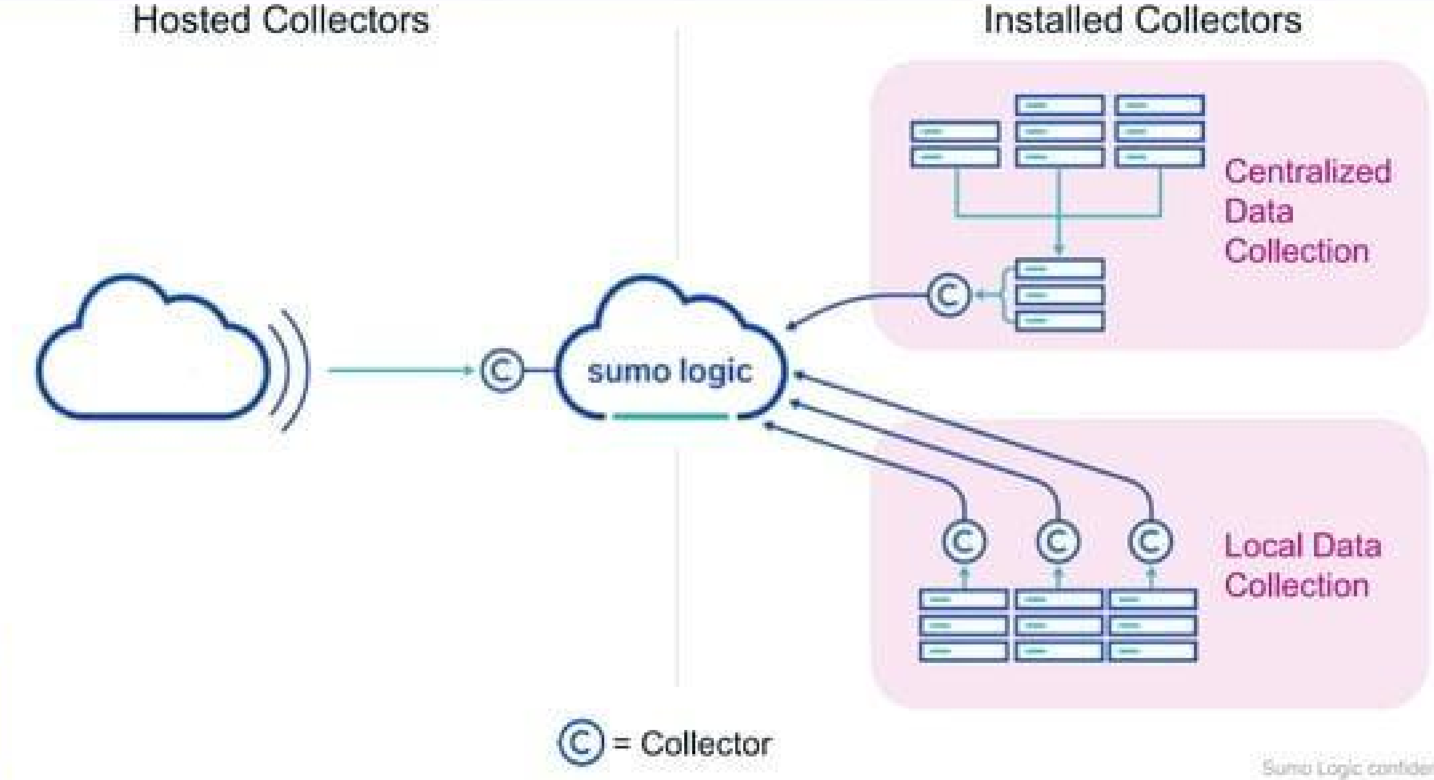
- Run a very high-bandwidth network with high logging levels. OR
- Require a central collection point for many Sources.

More than one Installed Collector

When you:

- Expect the Collector to ingest from > 500 separate files.
- Have memory or CPU limitations.
- Have geographically separated network clusters or regions.
- Expect combined logging traffic for one Collector to be > 15,000 events per second.

Collector and Deployment Options



CLOUD Data Collection

Most Data is generated in the Cloud and by Cloud Services and is collected via Sumo Logics Cloud Integrations.

Source Types

S3 Bucket

- Any data written to S3 buckets (AWS Audit or other)

HTTPS

- Lambda Scripts, Akamai, One Login, Log Appender Libraries, etc.

Google / O365

- Google API and O365

Benefits/Drawbacks

- + Hosted by Sumo Logic
- + No Software Installation
- + Can be configured with any number of sources
- + Is agentless

Typical Scenarios

Customers using Cloud infrastructure, while it's possible to rely on Cloud Data Collection entirely, this is not typical. These source types are normally just part of the overall collection strategies

LOCAL Data Collection

The Sumo Logic Collector is installed on all target Hosts and, where possible, sends log data produced on those target Hosts directly to Sumo Logic Backend via https connection.

Source Types

Local Files

- Operating Systems, Middleware, Custom Apps, etc.

Windows Events

- Local Windows Events

Docker

- Logs and Stats

Syslog (dedicated Collector)

- Network Devices, Snare, etc

Script (dedicated Collector)

- Cloud API's, Database Content, binary data

Benefits/Drawbacks

+ No Hardware Requirement

+ Automation (Chef/Puppet/Scripting)

- Outbound Internet Access Required

- Resource Usage on Target (hovers around 1% of compute memory)

Typical Scenarios

Customers with large amounts of (similar) servers, using orchestration/automation, mostly OS and application logs

- On Premise Data Centers
- Cloud Instances

CENTRALIZED Data Collection

The Sumo Logic Collector is installed on a set of dedicated machines, these collect log data from the target Hosts via various remote mechanisms and forward the data to the Sumo Logic Backend. This can be accomplished by either using Sumo Logic syslog source type or by running Syslog Servers (syslog-ng, rsyslog), write to file, and collect from there.

Source Types

Syslog

- Operating Systems, Middleware, Custom Applications, etc

Windows Events

- Remote Windows Events

Script

- Cloud API's, Database Content, binary data

Benefits/Drawbacks

+ No Outbound Internet Access

+ Leverage existing logging Infrastructure

- Scale

- Dedicated Hardware

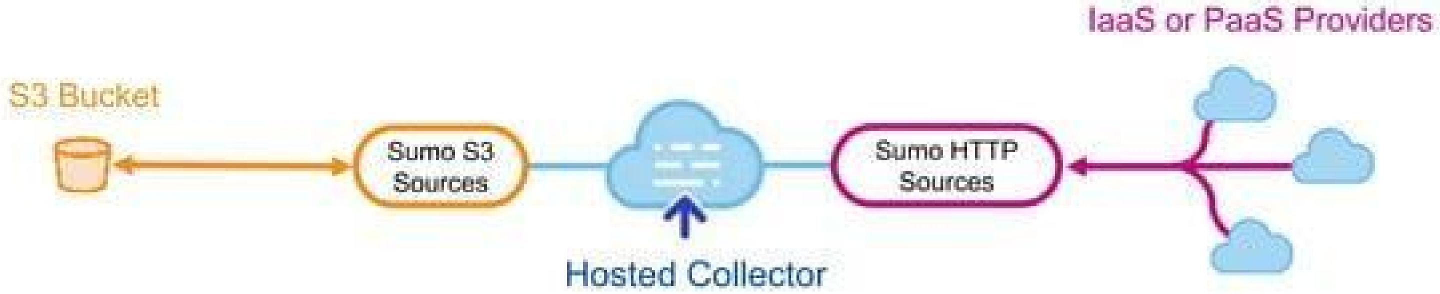
- Complexity (Failover, syslog rules)

Typical Scenarios

Customers with mostly Windows Environments or existing logging infrastructure (syslog/logstash)

- On Premise data centers

How does the data collection flow?



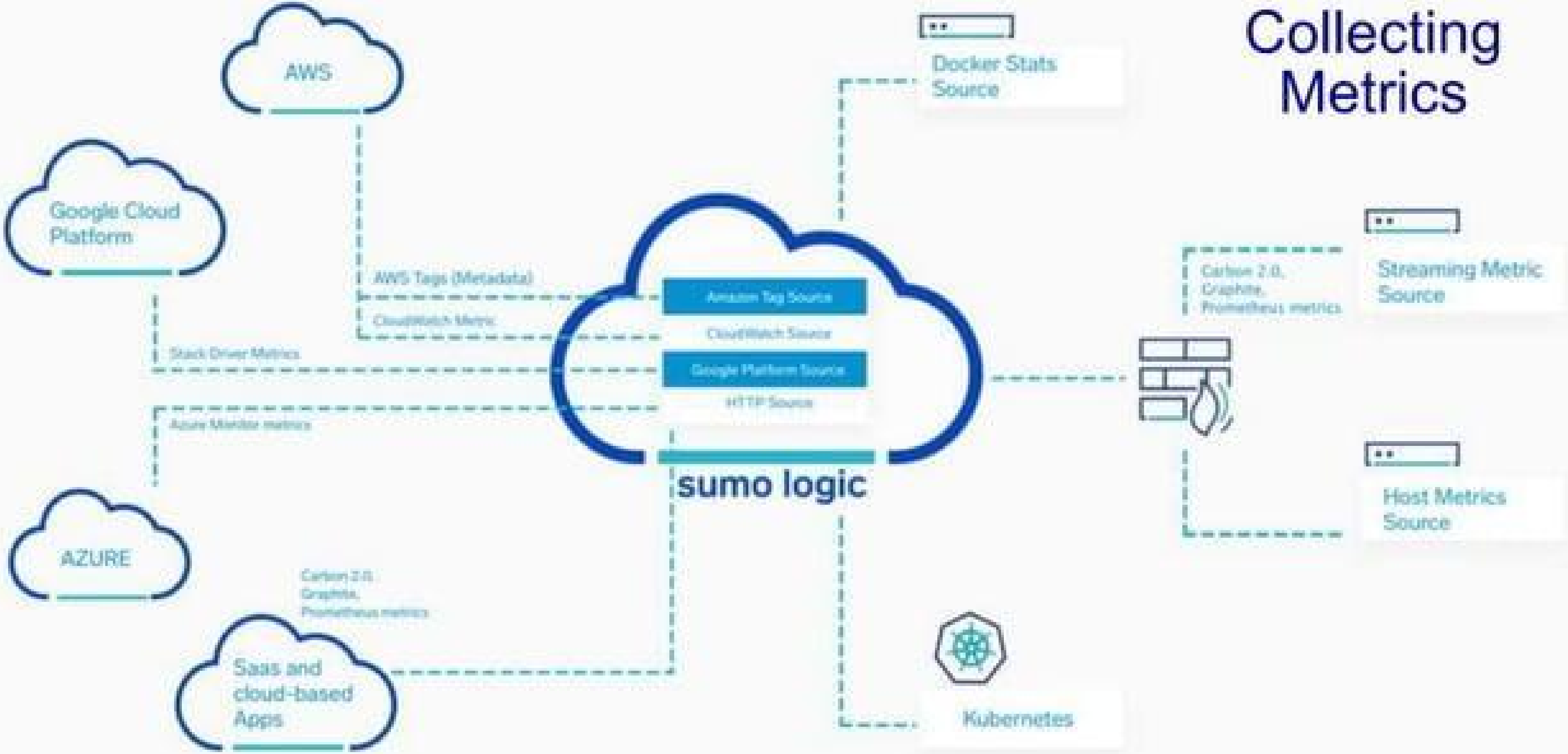
- Using IAM permissions, Sumo Logic scans the bucket at set intervals.
- SNS notifies Sumo Logic when new files are added to S3 bucket.

Examples: rsyslog, syslog-ng

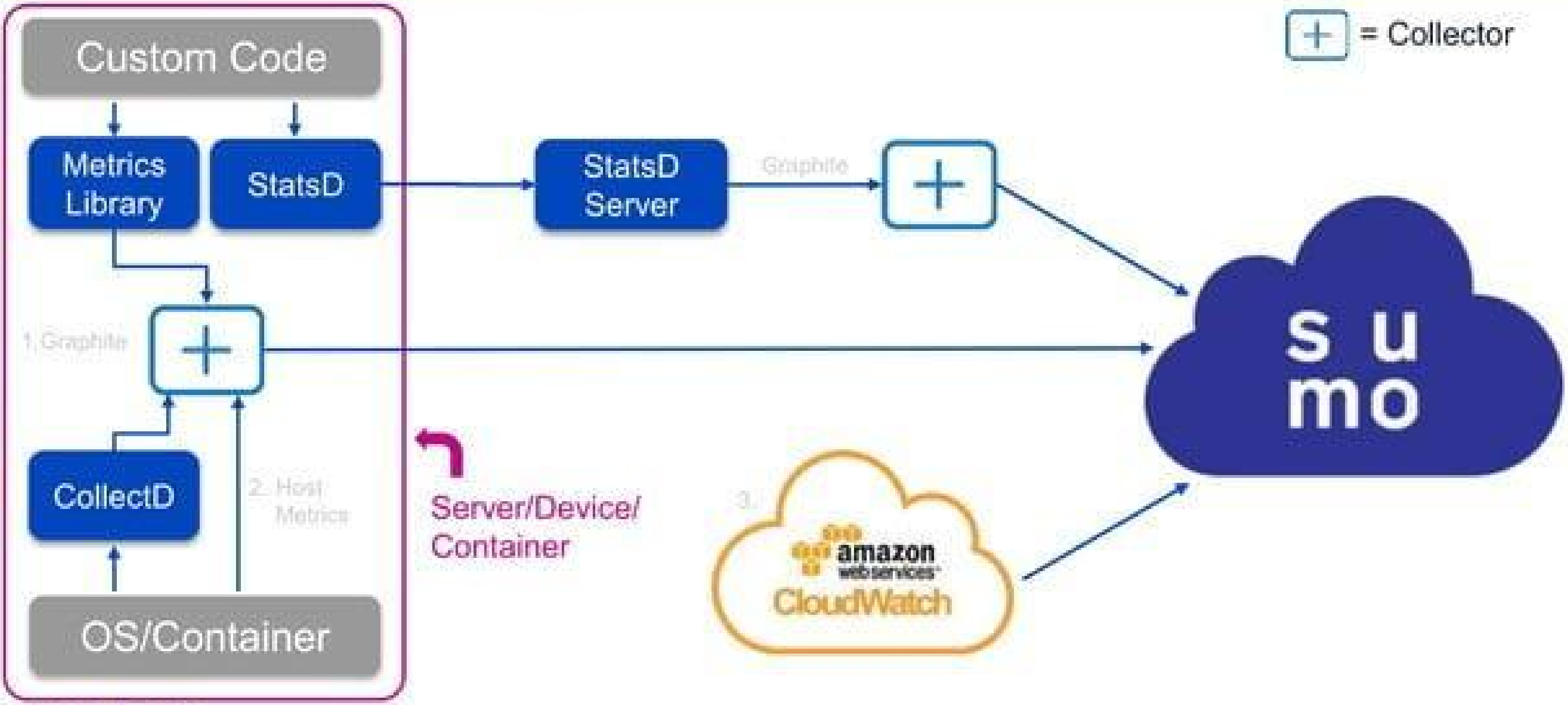
- Logs (or other data) are pointed to HTTP source, which acts as an endpoint.
- Hosted Collector can receive logs and metrics uploaded via a URL.

Examples: Kubernetes, FluentD, FluentBit

Collecting Metrics



Detailed collecting metrics



sumo logic

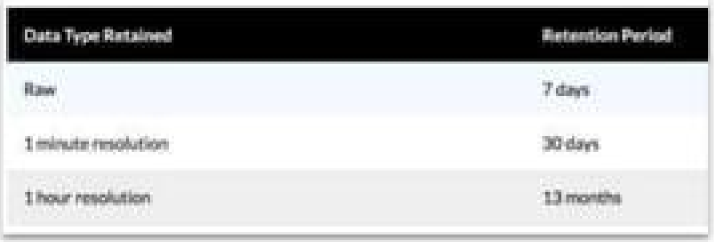
Metric Ingestion and Retention

Ingestion

- Each account is given free DPMs to apply go to **Administration>Account**
- You can ingest at a slower rate than 1 data point per minute (DPM)
- Sumo does not ingest metric data that is more than **one week** old.

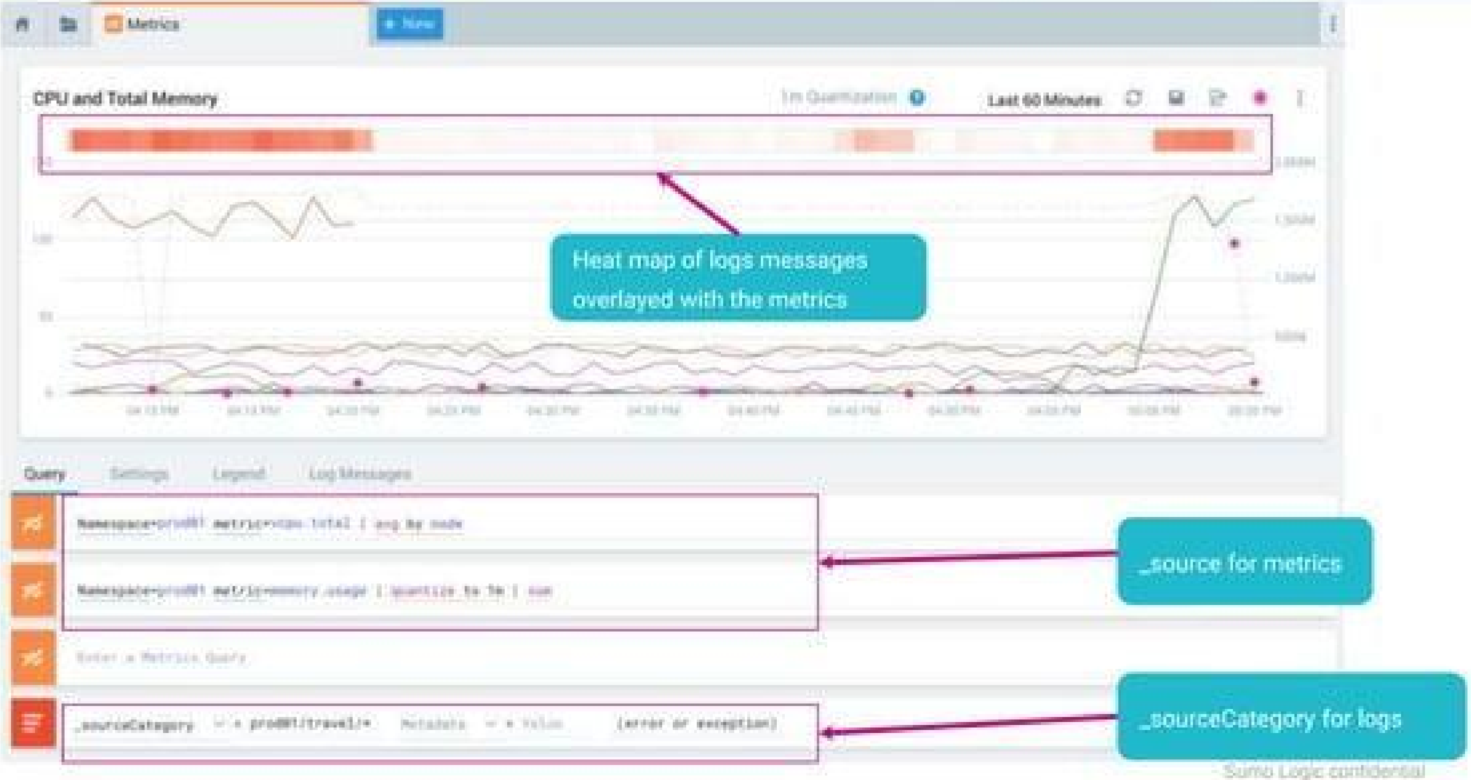
Retention

- Metrics data is stored as raw, one minute, and one hour resolutions. It's retained according to the following retention policy:
- For historical rollups (1 minute and 1 hour) Sumo calculates the max, min, avg, sum, and count values for a metric per minute or hour.



Data Type Retained	Retention Period
Raw	7 days
1 minute resolution	30 days
1 hour resolution	13 months

Best Practice Unified Metrics and Logs



```
Namespace=prod01 metric=cpu_total | avg by node
Namespace=prod01 metric=memory_usage | quantize to 5m | sum
Enter a Metrics Query
_sourceCategory = prod01/travel/*   Metadata = Value     (error or exception)
```

Heat map of logs messages overlayed with the metrics

_source for metrics

_sourceCategory for logs

Metadata Design

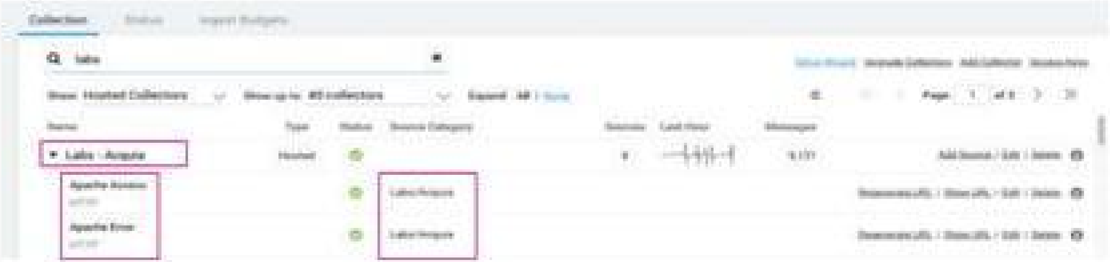
sumo logic

Sending Data ⇨ Metadata

Metadata **tags** are associated with each log message that is collected.

Metadata **values** are set through collector and source configuration.

Tag	Description
`_collector`	Name of the collector (defaults to hostname) (e.g. Labs - Acquia)
`_source`	Name of the source this data came through (e.g. Apache Error)
`_sourceCategory`	**Can be freely configured. Main metadata tag (e.g. Labs/Acquia)**



sumo logic

Source Category Best Practices

Recommended nomenclature for Source Categories

```
Component1/Component2/Component3...
```

Begin with the least descriptive, highest-level grouping, and get more descriptive with each component to the right.

prod/myapp1/apache/access prod/myapp1/apache/error prod/myapp1/cloudtrail	dev/myapp1/apache/access dev/myapp1/apache/error dev/myapp1/cloudtrail
prod/myapp2/nginx/access prod/myapp2/tomcat/access prod/myapp2/tomcat/catalina/out prod/myapp2/mysql/slowqueries	dev/myapp2/nginx/access dev/myapp2/tomcat/access dev/myapp2/tomcat/catalina/out dev/myapp2/mysql/slowqueries

Note: Not all types of logs need to have the same amount of levels.

→ Best Practices: Good Source Category, Bad Source Category

Metadata: Source Category Best Practices and Benefits

Define the scope of searches

```
_sourceCategory=networking/firewall/* (all firewall data)
_sourceCategory=networking/*/cisco/* (all Cisco data)
```

Index and partition your data

```
_sourceCategory=prod/networking*
_sourceCategory=sales/strategic/myapp*
```

Control who sees what data through RBAC

```
_sourceCategory=aws/sec/cloudtrail*
```

Metadata: Source Category Best Practices and Benefits

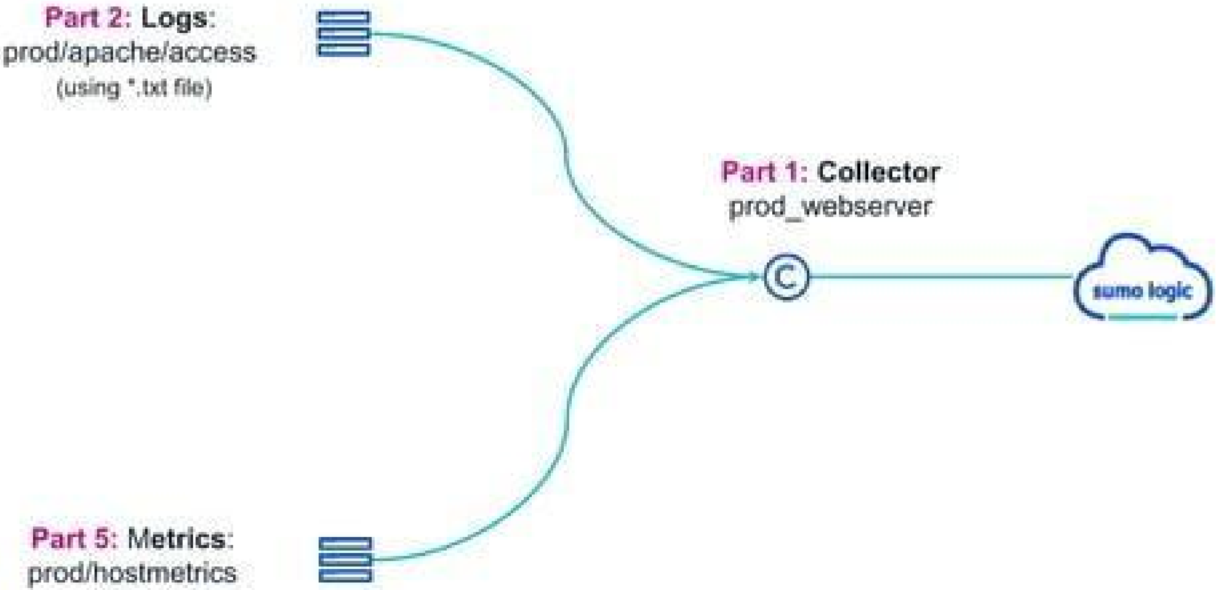
Common components (and any combination of):

- 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     Web/Apache/Access/Prod
Dev/Web/Apache/Access      Web/Apache/Access/Dev
Prod/DB/MySQL/Error        DB/MySQL/Error/Prod
Dev/DB/MySQL/Error         DB/MySQL/Error/Dev
```

Overview of Labs Part 1,2 and 5



Part 2: Logs:
prod/apache/access
(using *.txt file)

Part 1: Collector
prod_webserver

Part 5: Metrics:
prod/hostmetrics

Ⓒ = Collector

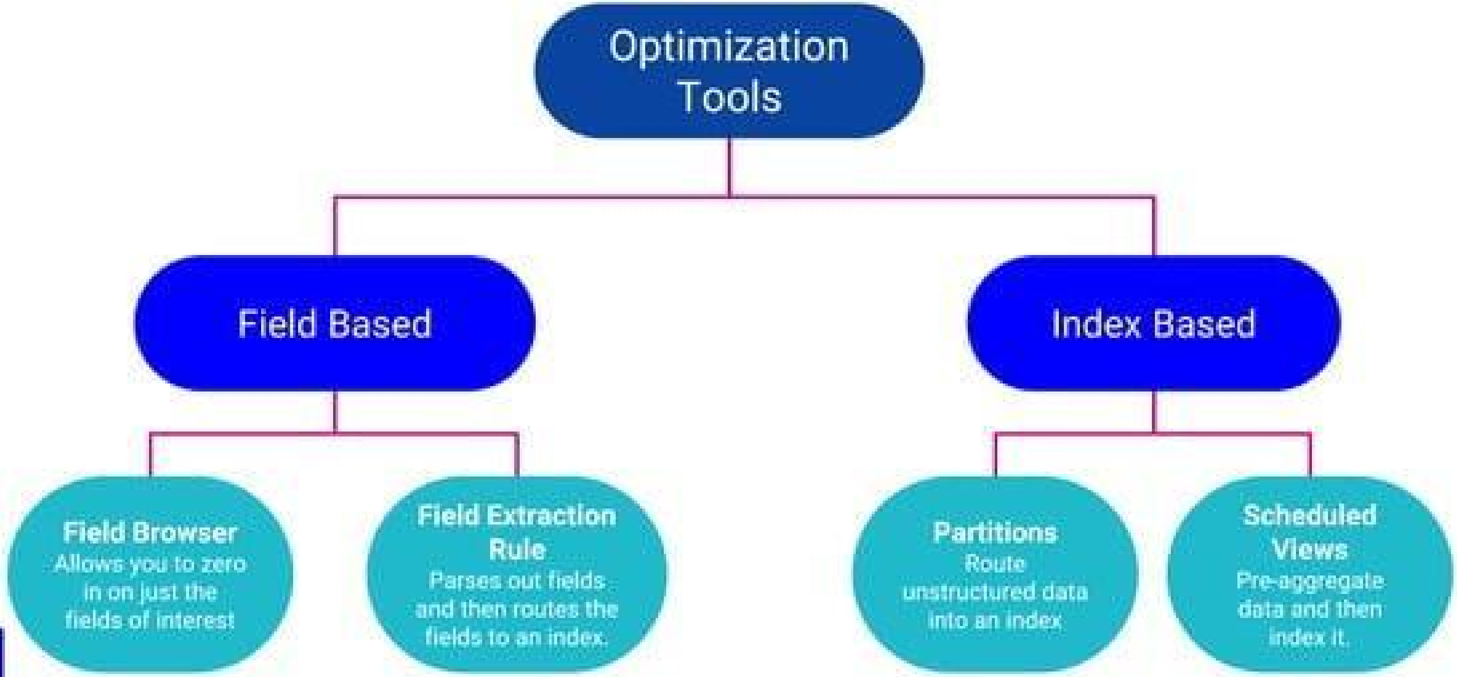
Install a collector and sources

Do Labs 1, 2, and 5

Optimization Tools

sumo logic

Optimization Tools

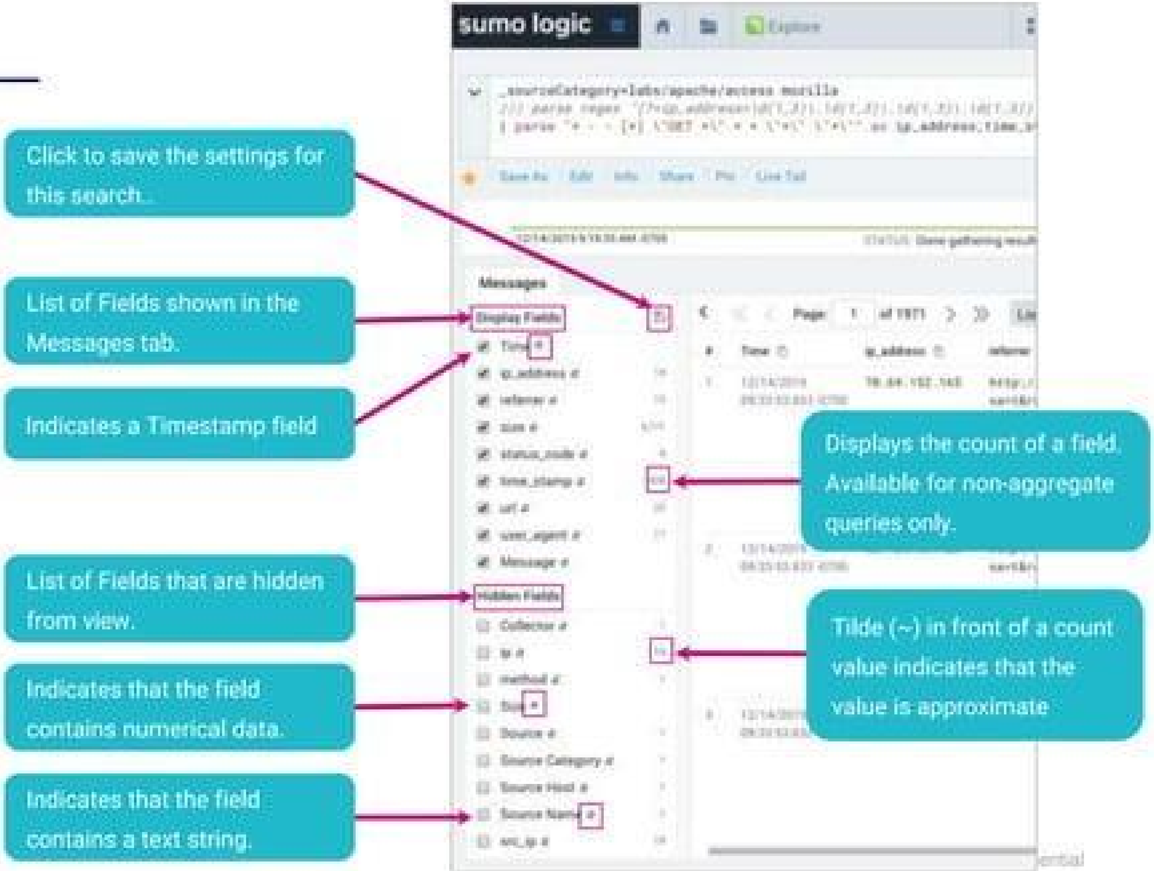


Optimization Tools
Field Based
Index Based
Field Browser
Allows you to zero in on just the fields of interest
Field Extraction Rule
Parses out fields and then routes the fields to an index.
Partitions
Route unstructured data into an index
Scheduled Views
Pre-aggregate data and then index it.

Field Browser

The Field Browser appears on the left side of the **Messages** tab of the Search page for both aggregate and non-aggregate queries.

It allows you to zero in on just the fields of interest in a search by displaying or hiding selected fields without having to parse them.



```
_sourceCategory=labs/apache/access mozilla
/// parse regex "(?<ip_address>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}) [illegible]
| parse "* - - [*] \"GET *\" * * \"*\" \"*\"" as ip_address,time,[illegible]
```

Click to save the settings for this search.

List of Fields shown in the Messages tab.

Indicates a Timestamp field

List of Fields that are hidden from view.

Indicates that the field contains numerical data.

Indicates that the field contains a text string.

Displays the count of a field. Available for non-aggregate queries only.

Tilde (~) in front of a count value indicates that the value is approximate

Field Extraction Rules

Benefits

- Better Performance
- Standardized field names
- Simplified Searches

Best Practices

- Build simple, specific Rules
- Test Parse and other operations thoroughly (use nodrop and isEmpty for testing)

Limitations

- 50 rules/200 fields (Contact us to increase this)
- Not all operators supported (JSON auto)

What are Partitions?

Partitions are custom indexes that **improve search performance by searching over a smaller number of messages** at query time. By default, we store all your data in the General Index.

However, for faster searching or RBAC control, you have the ability to create additional partitions so **your searches don't scan your entire data set,** but instead, scan only the necessary partition(s).

Production
Dev
Quality Assurance
Default Index

All members of your organization can take advantage of this partition structure when they run queries.

- ✓ No overlap
- ✓ < 20 Partitions
- ✓ Ideally between 1% and 30% of total volume
- ✓ Group data that is searched together most often
- ✓ Data retention customized

Scheduled Views

Speed the search process for small and historical subsets of your data by functioning as a pre-aggregated index.

Reduce aggregate data down to the bare minimum, so it contains only the raw results that you need to generate your data.

Best Practices	• Pre-aggregated data (e.g. for long-term trends) • Find the needle in the haystack…. • Don't insert comments as it may interrupt the parsing of the pipes
Limitations	• We recommend selectivity of > 1:10000 (for every 10,000 log messages scanned there's only 1 result) • View is updated by service ~once a minute • Allows for backfilling • Search view using _view=[VIEW-NAME] • Data does count against ingest volume (if not using aggregation)

Examples of applying Scheduled Views

Web access trends

Creating a Scheduled View allows you to isolate logs related to your site, making it easy to report on web traffic patterns.

App usage metrics

A Scheduled View can help you track the usage of one or more applications over time. Depending on your deployment, you could build a Scheduled View for each application.

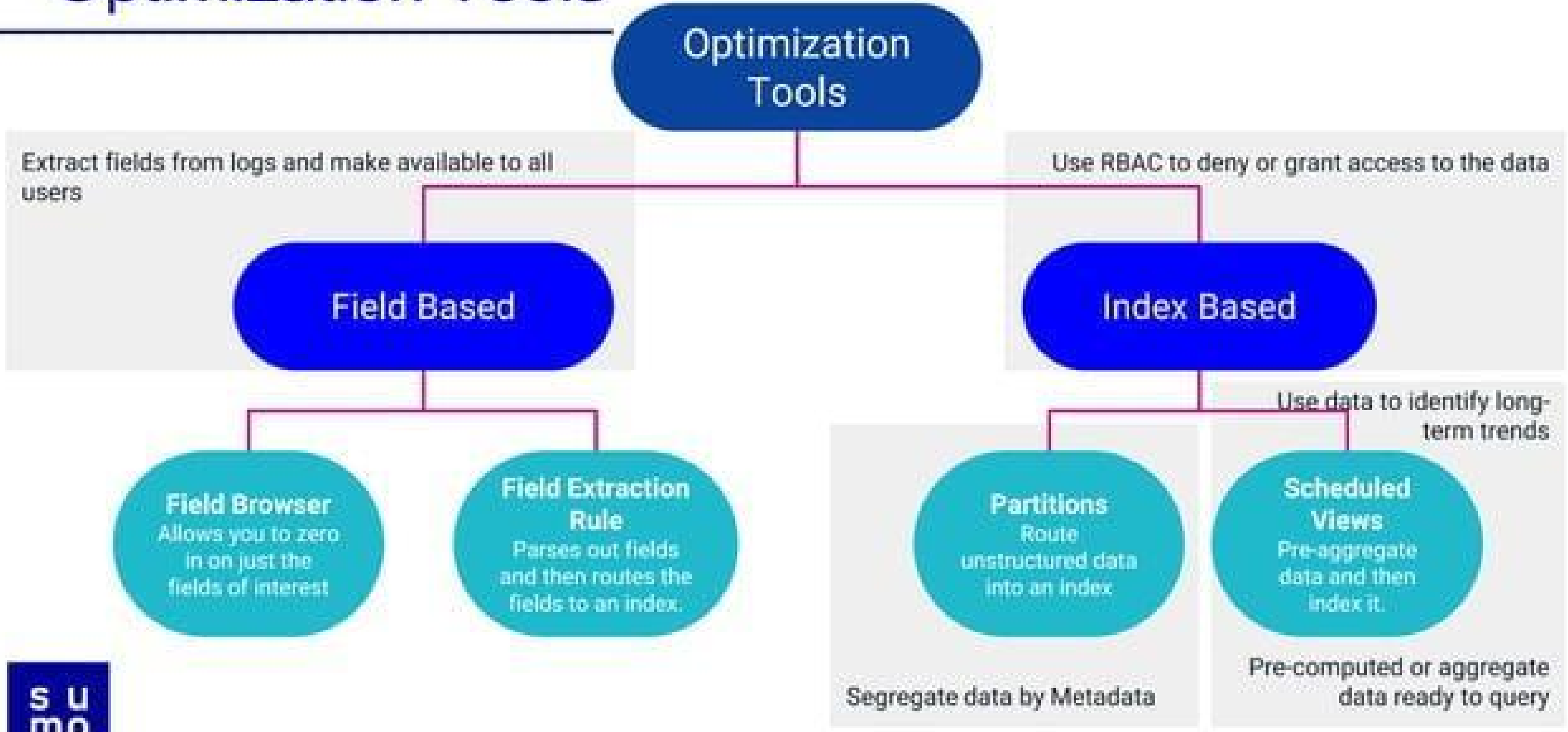
Threat analysis

Because a Scheduled View indexes any type of data, you could create a Scheduled View for firewall logs, for example. You could then leverage this Scheduled View to see how threat types and threat levels vary over time, or even which IPs from high-risk areas are hitting your site.

User behavior

A Scheduled View can be used to parse logins by user ID across your entire deployment, so you can answer audit-related questions quickly. Faster query results on this dataset allow for high-level investigations, such as checking to see if users have logged in during the past 60 days (or as far back as your retention period).

Optimization Tools

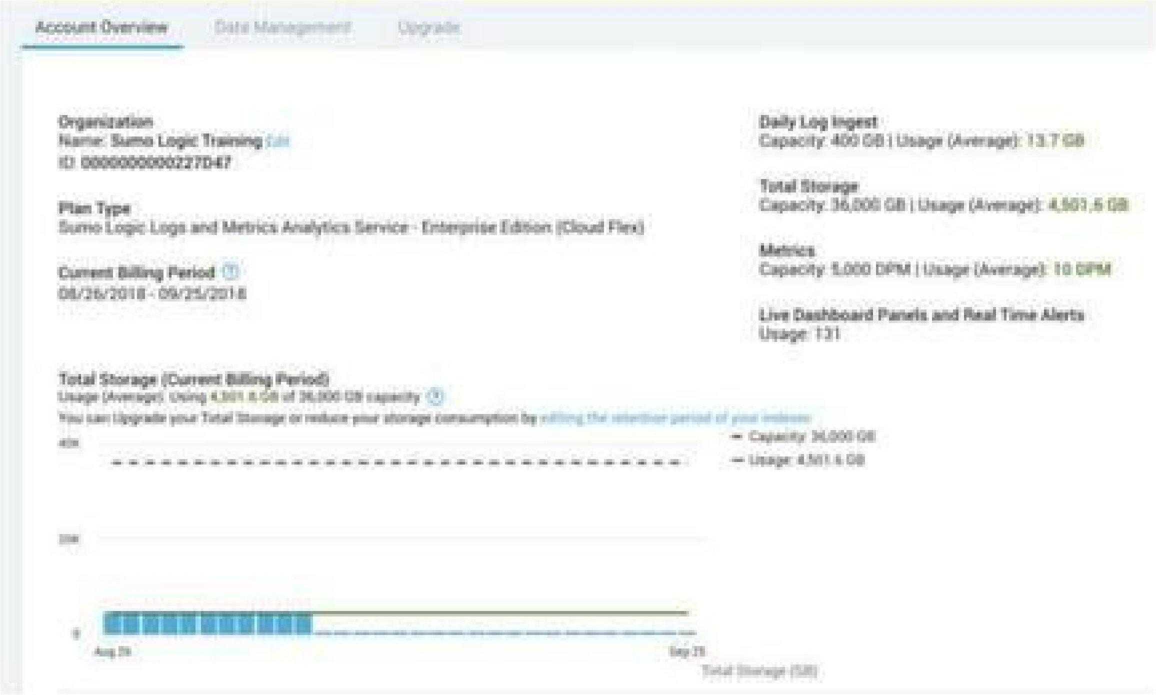


Optimization Tools
Extract fields from logs and make available to all users
Use RBAC to deny or grant access to the data
Field Based
Index Based
Use data to identify long-term trends
Field Browser
Allows you to zero in on just the fields of interest
Field Extraction Rule
Parses out fields and then routes the fields to an index.
Partitions
Route unstructured data into an index
Scheduled Views
Pre-aggregate data and then index it.
Segregate data by Metadata
Pre-computed or aggregate data ready to query

Overview and Data Management

sumo logic

Account Overview



Organization
Name: Sumo Logic Training Edit
ID: 0000000000227D47

Plan Type
Sumo Logic Logs and Metrics Analytics Service - Enterprise Edition (Cloud Flex)

Current Billing Period ⓘ
08/26/2018 - 09/25/2018

Daily Log Ingest
Capacity: 400 GB | Usage (Average): 13.7 GB

Total Storage
Capacity: 36,000 GB | Usage (Average): 4,501.6 GB

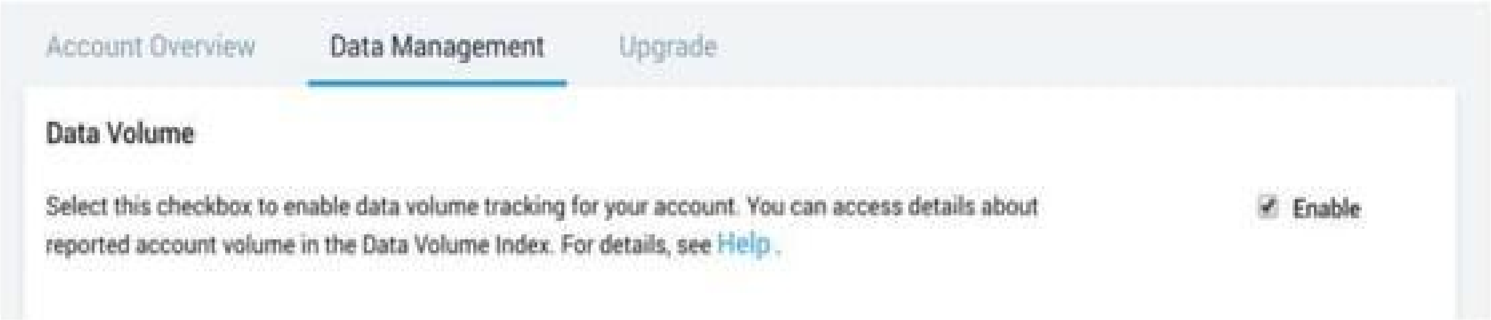
Metrics
Capacity: 5,000 DPM | Usage (Average): 10 DPM

Live Dashboard Panels and Real Time Alerts
Usage: 131

Total Storage (Current Billing Period)
Usage (Average): Using 4,501.6 GB of 36,000 GB capacity ⓘ
You can Upgrade your Total Storage or reduce your storage consumption by editing the retention period of your indexes

sumo logic

Data Management



Data Volume

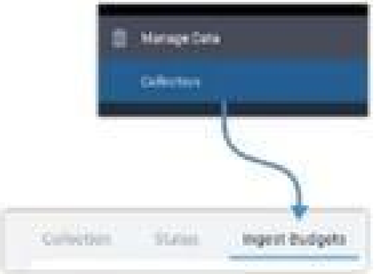
Select this checkbox to enable data volume tracking for your account. You can access details about reported account volume in the Data Volume Index. For details, see Help .

☑ Enable

Ingest Budget Monitoring and Control

How They Work

- Collectors monitor total ingested data
- Collector usage is aggregated to a namespace
- Usage is monitored as a percentage of a total capacity you set for each namespace
- Use **Stop** or **Keep** actions for a namespace when capacity is reached



Use Cases

- Teams may ingest data unevenly. Some teams more than others. Sometimes by a lot. Use ingest budgets to set guardrails for overconsumption and cost sharing

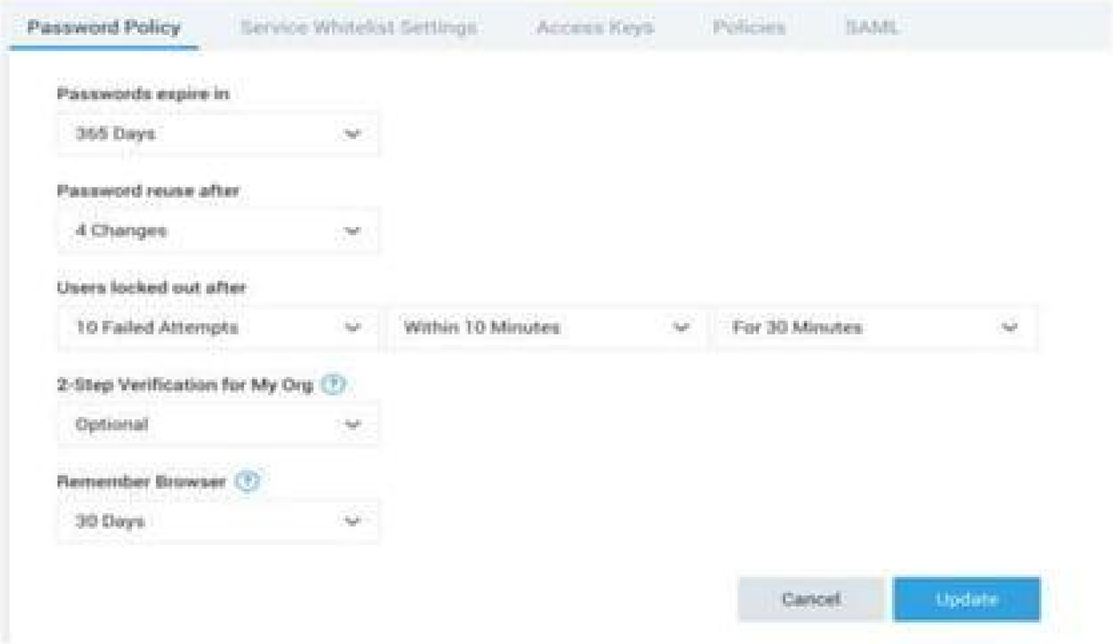
Best Practices

- Assign or recognize collectors owned by a given team
- Allocate ingest budget by namespace (Dev, QA, Security, etc.)

Global Security Settings

sumo logic

Password Policy



Passwords expire in
365 Days

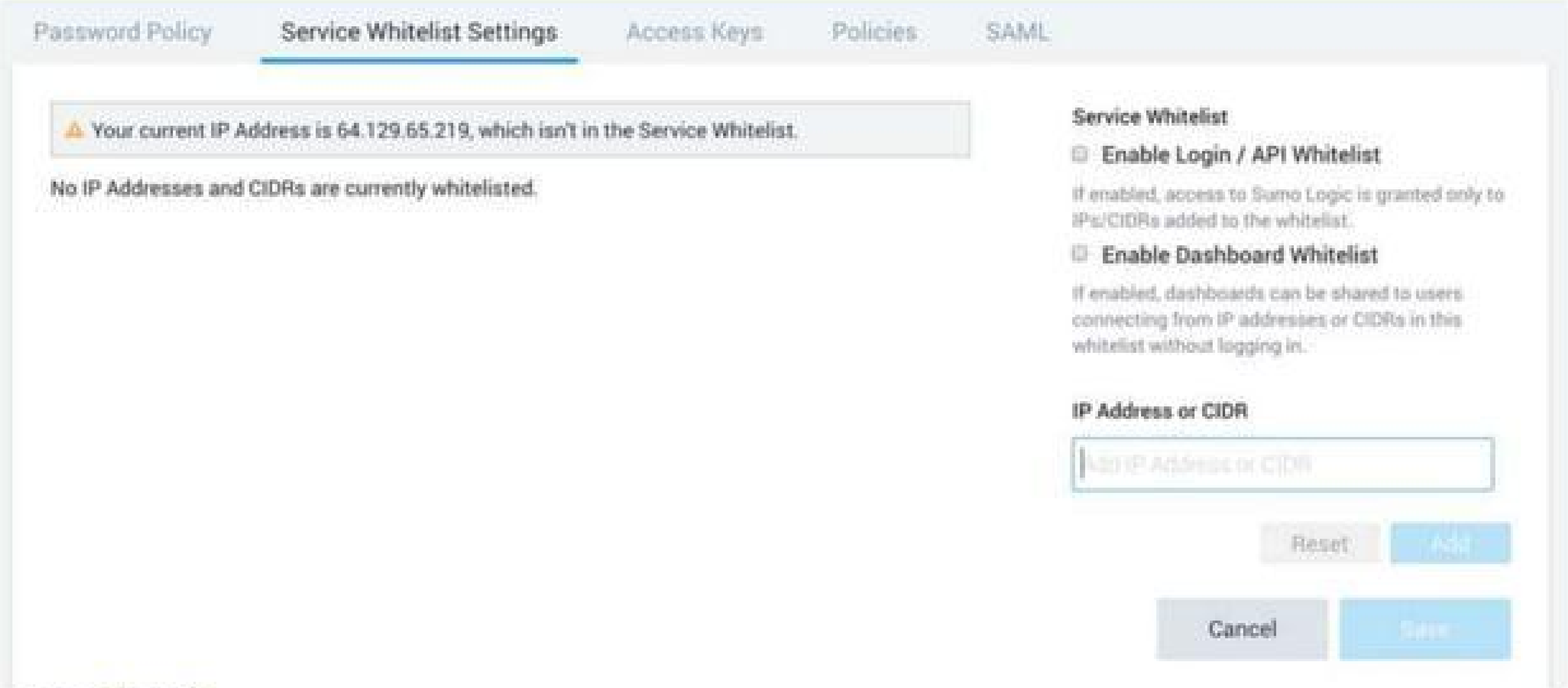
Password reuse after
4 Changes

Users locked out after
10 Failed Attempts | Within 10 Minutes | For 30 Minutes

2-Step Verification for My Org
Optional

Remember Browser
30 Days

Service Whitelist Settings



⚠ Your current IP Address is 64.129.65.219, which isn't in the Service Whitelist.

No IP Addresses and CIDRs are currently whitelisted.

Service Whitelist

□ **Enable Login / API Whitelist**

If enabled, access to Sumo Logic is granted only to IPs/CIDRs added to the whitelist.

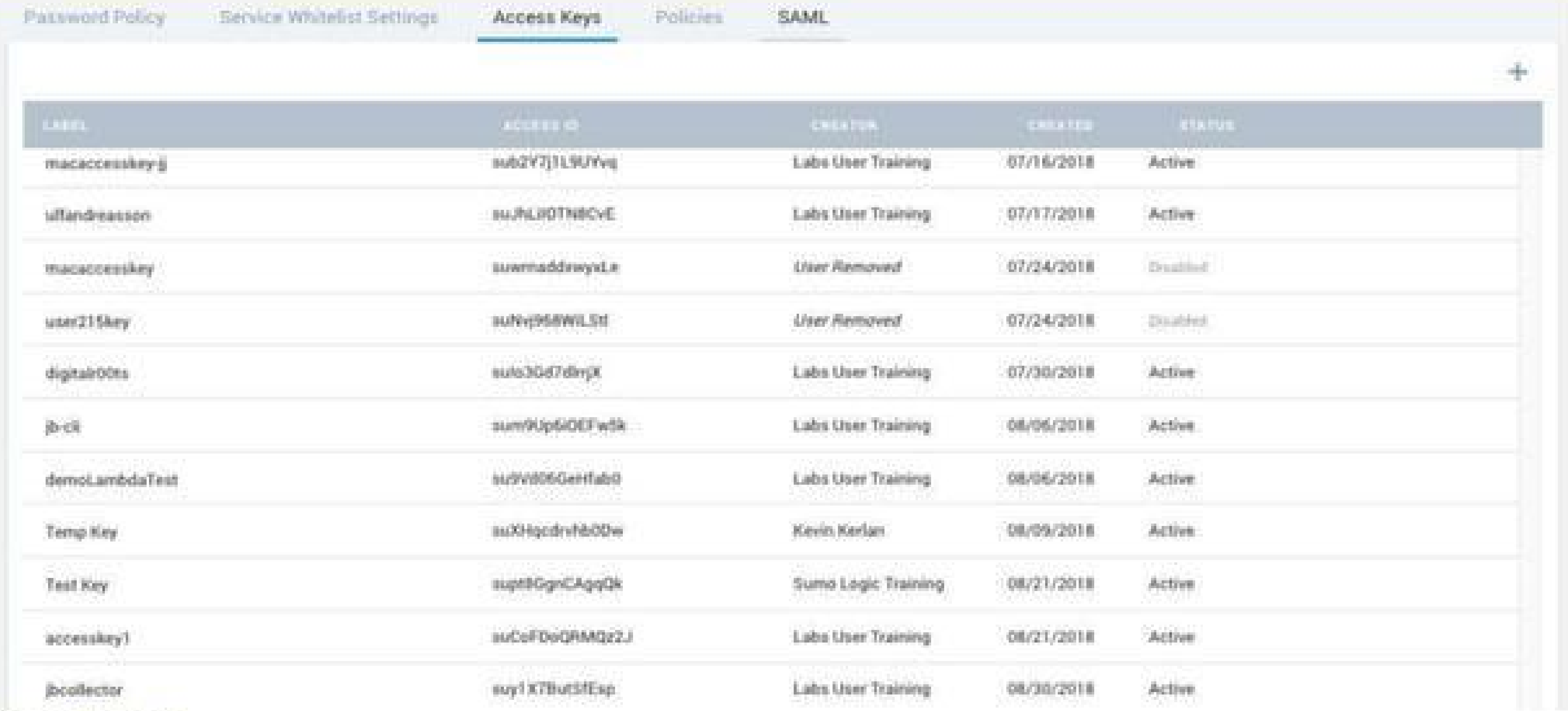
□ **Enable Dashboard Whitelist**

If enabled, dashboards can be shared to users connecting from IP addresses or CIDRs in this whitelist without logging in.

IP Address or CIDR

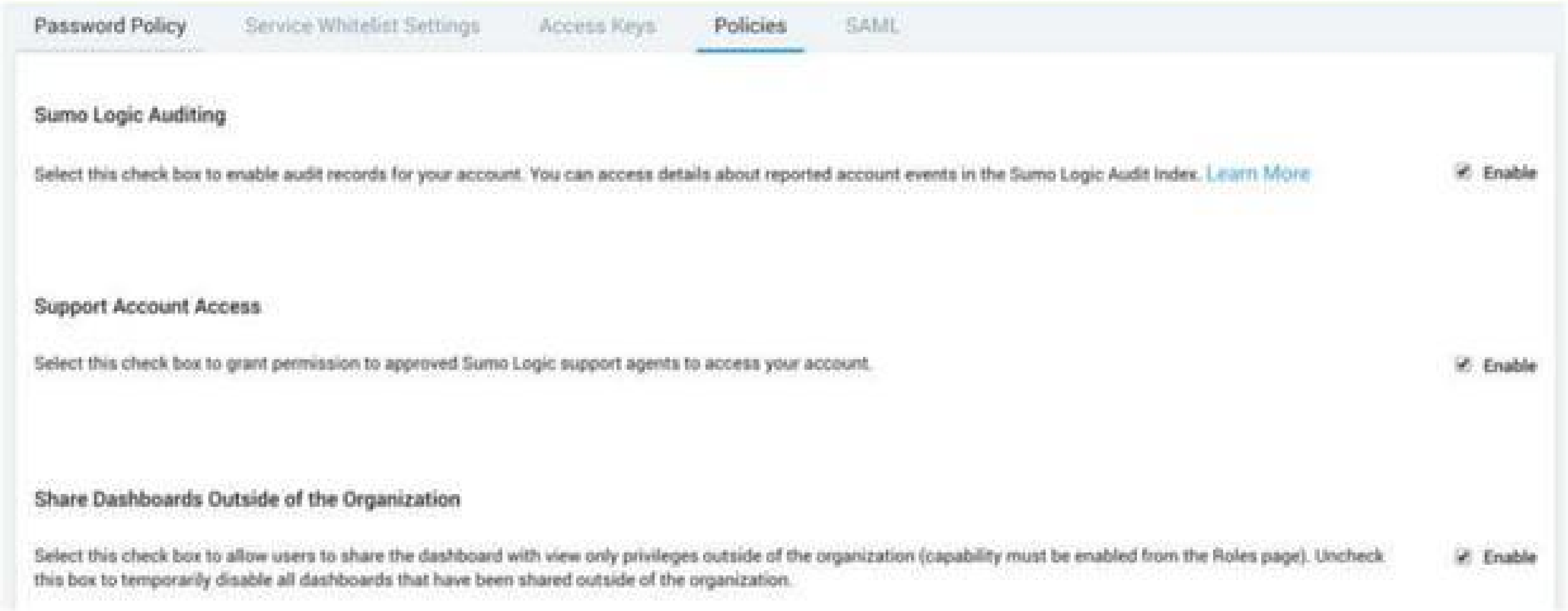
Add IP Address or CIDR

Access Keys



LABEL	ACCESS ID	CREATOR	CREATED	STATUS
macaccesskey-jj	sub2Y7j1L9UYvq	Labs User Training	07/16/2018	Active
ulfandreasson	suJhLJ0TN8CvE	Labs User Training	07/17/2018	Active
macaccesskey	suwmaddxwyxLe	*User Removed*	07/24/2018	Disabled
user215key	suNvj958WiLStl	*User Removed*	07/24/2018	Disabled
digitalr00ts	sulo3Gd7dlnjX	Labs User Training	07/30/2018	Active
jb-cli	sum9Up6iOEFw5k	Labs User Training	08/06/2018	Active
demoLambdaTest	su9Vd06GeHfab0	Labs User Training	08/06/2018	Active
Temp Key	suXHqcdrvhb0Dw	Kevin Kerlan	08/09/2018	Active
Test Key	supt8GgnCAgqQk	Sumo Logic Training	08/21/2018	Active
accesskey1	suCoFDoQRMQz2J	Labs User Training	08/21/2018	Active
jbcollector	suy1X7ButSfEsp	Labs User Training	08/30/2018	Active

Policies



Sumo Logic Auditing

Select this check box to enable audit records for your account. You can access details about reported account events in the Sumo Logic Audit Index. Learn More

☑ Enable

Support Account Access

Select this check box to grant permission to approved Sumo Logic support agents to access your account.

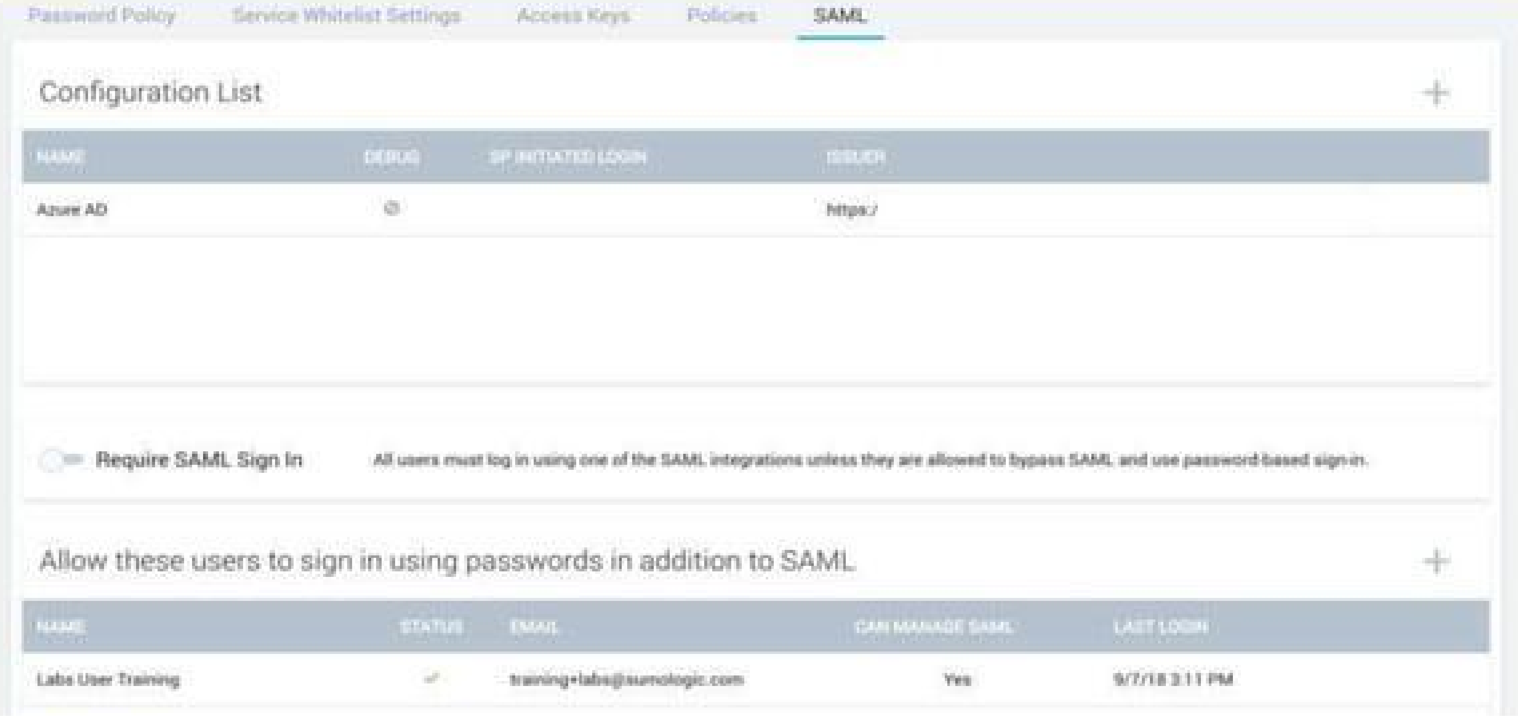
☑ Enable

Share Dashboards Outside of the Organization

Select this check box to allow users to share the dashboard with view only privileges outside of the organization (capability must be enabled from the Roles page). Uncheck this box to temporarily disable all dashboards that have been shared outside of the organization.

☑ Enable

SAML Single Sign On



Configuration List

NAME	DEBUG	SP INITIATED LOGIN	ISSUER
Azure AD	⊘		https:/

○ Require SAML Sign In — All users must log in using one of the SAML integrations unless they are allowed to bypass SAML and use password-based sign-in.

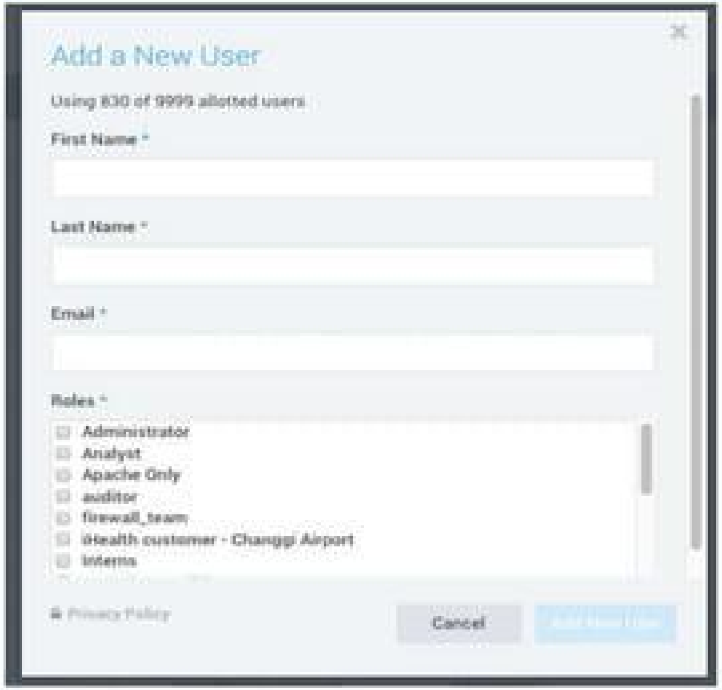
Allow these users to sign in using passwords in addition to SAML

NAME	STATUS	EMAIL	CAN MANAGE SAML	LAST LOGIN
Labs User Training	✓	training+labs@sumologic.com	Yes	9/7/18 3:11 PM

User and Role Management

sumo logic

Adding New Users



Add a New User

Using 830 of 9999 allotted users

First Name *

Last Name *

Email *

Roles *

- □ Administrator
- □ Analyst
- □ Apache Only
- □ auditor
- □ firewall_team
- □ iHealth customer - Changgi Airport
- □ interns

Default User Roles

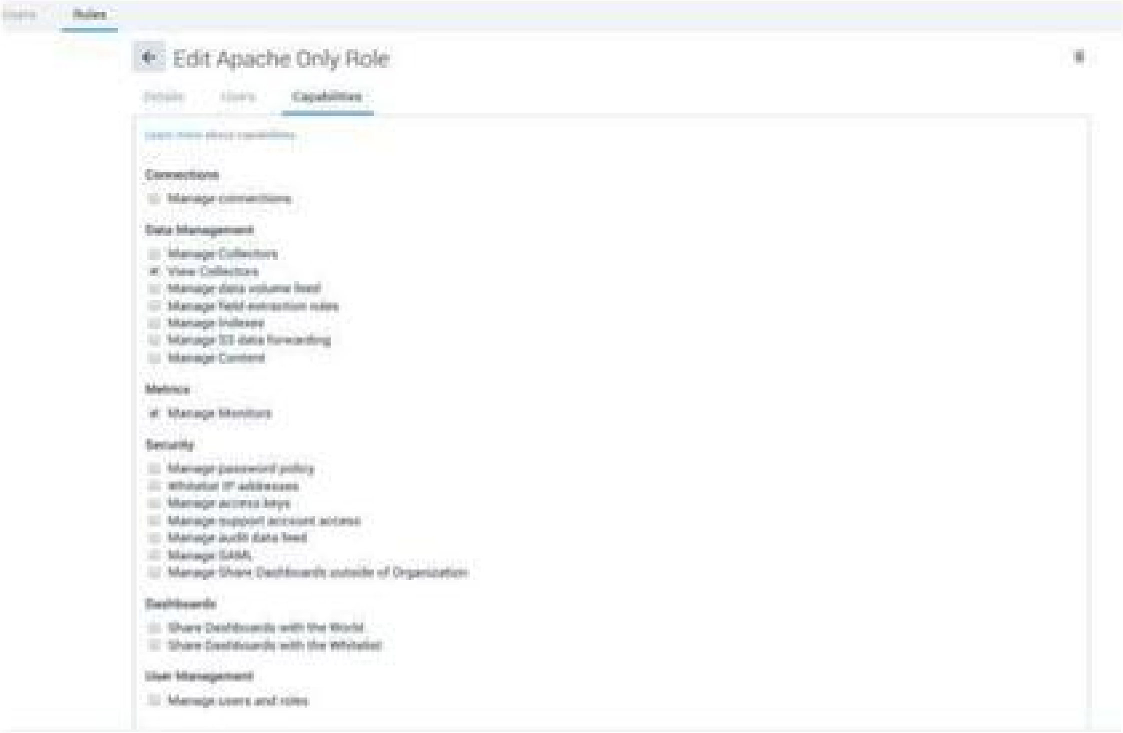
Administrator

- Manage users and roles
- View and manage collectors

Analyst

- Full data access
- No user and collector management

Users and Roles - Capabilities



Edit Apache Only Role

Learn more about capabilities

Connections

□ Manage connections

Data Management

□ Manage Collectors
☑ View Collectors
□ Manage data volume feed
□ Manage field extraction rules
□ Manage Indexes
□ Manage S3 data forwarding
□ Manage Content

Metrics

☑ Manage Monitors

Security

□ Manage password policy
□ Whitelist IP addresses
□ Manage access keys
□ Manage support account access
□ Manage audit data feed
□ Manage SAML
□ Manage Share Dashboards outside of Organization

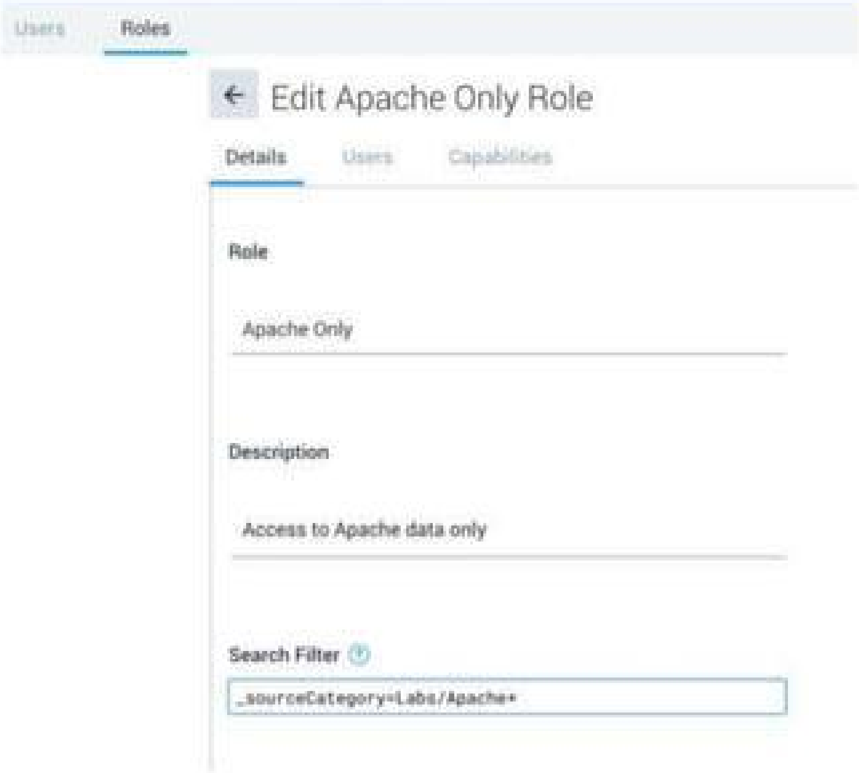
Dashboards

□ Share Dashboards with the World
□ Share Dashboards with the Whitelist

User Management

□ Manage users and roles

Users and Roles - Role Details



Edit Apache Only Role

Role

Apache Only

Description

Access to Apache data only

Search Filter

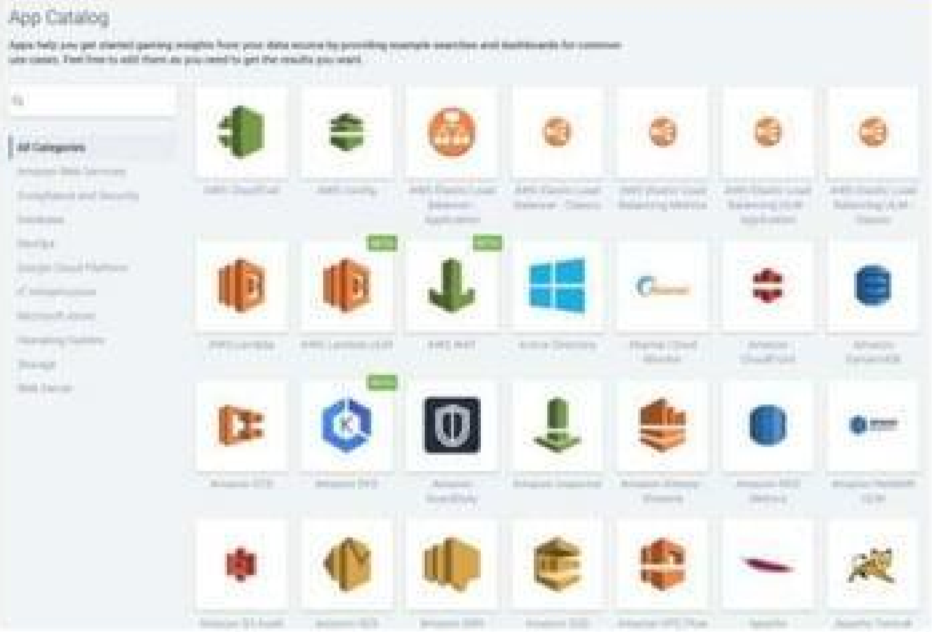
```
_sourceCategory=Labs/Apache*
```

sumo logic

Taking Advantage of Apps

- 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



App Catalog

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

Recommended Apps

- Data Volume
  - Need to enable Data Volume index
  - View your account's data usage volume by category, Collector, Source name, and hosts
- Audit
  - Need to enable the Audit Index
  - Analyze audit events to provide insight into overall Sumo Logic usage

Content Sharing

sumo logic

Sharing and Recommending: Searches and Dashboards

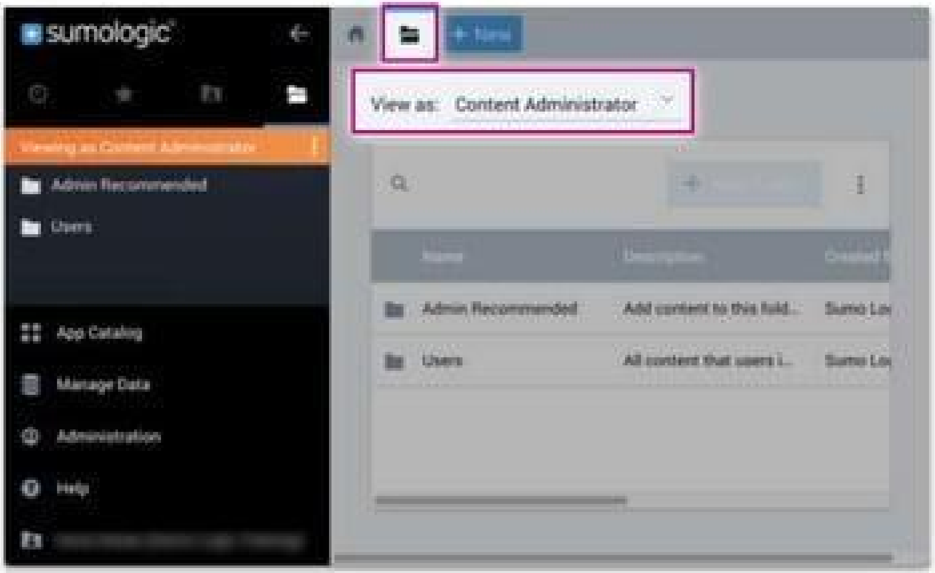
Enable your users by sharing and recommending content that is meaningful to them

Share Content

- Grant View, Edit, Manage

Admin Recommended

- Call attention to content



View as: Content Administrator

Name	Description	Created
Admin Recommended	Add content to this fold...	Sumo Lo
Users	All content that users i...	Sumo Lo

Install an app and create an alert

Do Labs 3 and 6

In Summary, you can…

- Ingest any type of logs (structured and unstructured)
- Select a deployment option that best fits your sources
- Develop a robust naming convention for your metadata
- Start sharing and recommending content that is useful to your users
- Take advantage of Optimization Tools
- **Call to Action:**
    - Set up a **collector** deployment option that best fits your environment
    - Ensure you have a robust **_SourceCategory** naming convention
    - At the very least, set up **field extraction rules** for your popular data sources
    - Set up your general index into useful **partitions**

Questions?

Tutorial: Hands-on Exercises

Training Environment:

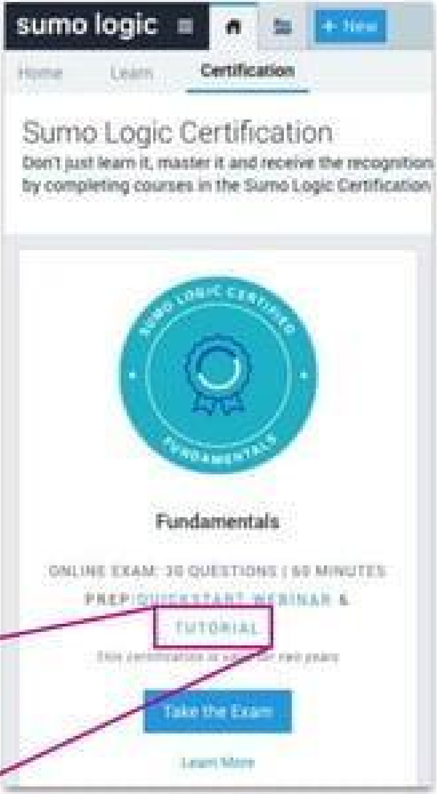
service.sumologic.com

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

password: Sum0Labs!

Hands-on Labs:

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



Sumo Logic Certification

Don't just learn it, master it and receive the recognition by completing courses in the Sumo Logic Certification

Fundamentals

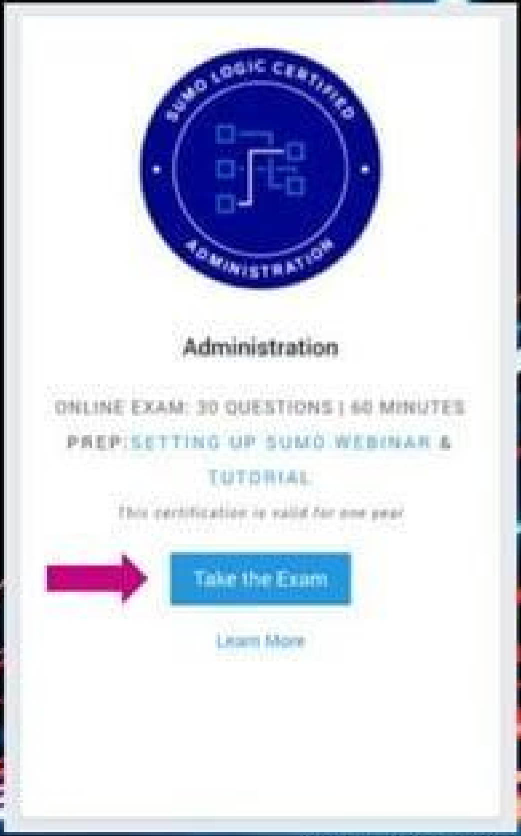
ONLINE EXAM: 30 QUESTIONS | 60 MINUTES

PREP: QUICKSTART WEBINAR & TUTORIAL

This certification is valid for two years

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



Administration

ONLINE EXAM: 30 QUESTIONS | 60 MINUTES

PREP: SETTING UP SUMO WEBINAR & TUTORIAL

This certification is valid for one year

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

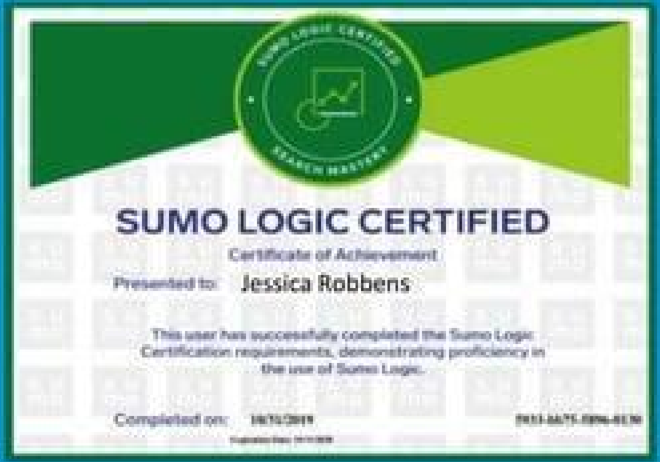
If you find your login is cycling back to the exam screen, do the following:

- 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

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 MASTERS

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

Tutorial: Hands-on Exercises

Training Environment:

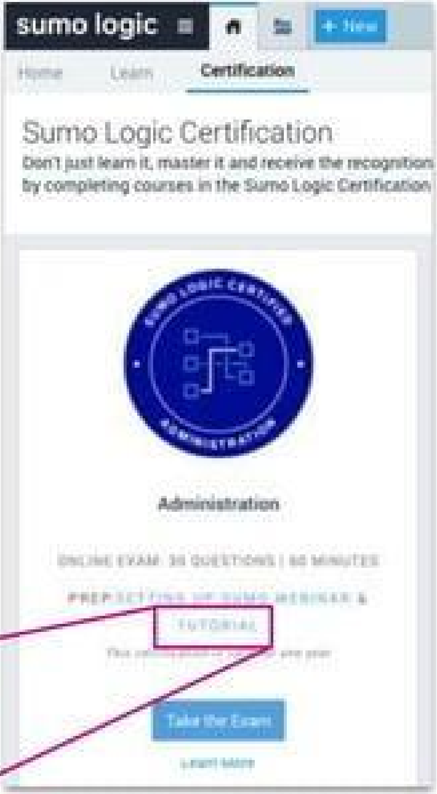
service.sumologic.com

username: training+labs@sumologic.com

password: Sum0Labs!

Hands-on Labs:

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



Sumo Logic Certification

Don't just learn it, master it and receive the recognition by completing courses in the Sumo Logic Certification

Administration

ONLINE EXAM: 30 QUESTIONS | 60 MINUTES

PREP: SETTING UP SUMO WEBINAR & TUTORIAL s u

Empowering the people who power modern business

m o

sumo logic