Getting started

These topics provide basic information about your Sumo Logic account, and how to design your Sumo Logic implementation for your use case.

- Sumo Logic Components
  Sumo Logic is comprised of just a few components: Collectors, Sources, the Sumo Logic Cloud, and the Sumo Logic Web Application. Learn how these components work together here.
- Design your Deployment
  Depending on your use case, you may need to use Installed or Hosted Collectors. Use this topic to help you determine what your organization will need.
- Best Practices: Local and Centralized Data Collection
  Which method is right for you?
- System Requirements
  These topics include information on basic hardware requirements for Sumo Logic Collectors, supported web browsers for best performance, and supported log encoding.
- Preferences Page
  Set the Preferences on your personal Sumo Logic account for settings such as your password, web session timeout, default time zone, and more.

Collecting logs and metrics

To send your data to Sumo Logic, you'll need to learn how to configure Collectors and Sources.

- Metadata Naming Conventions
  Prior to configuring Collectors, it is a good idea to establish a naming convention for Sources, Collectors, and especially metadata tags.
- Compare Installed and Hosted Collectors
  Before you can send data to Sumo Logic, you'll need to decide what type of Collectors make sense for your use case: Installed Collectors or Hosted Collectors.
- Installed Collectors
  Installed Collectors are deployed in your environment, on Azure Machine Image (AMI). Installed Collectors require a software download and installation. Upgrades to Collector software are released regularly by

Sumo Logic.

- Sources
  Sources are the environments that Sumo Logic Collectors connect to collect data from a customer's site.
  - Sources for Installed Collectors
    Sources for Installed Collectors include Local and Remote File Sources, Local and Remote Windows Event Sources, Local and Remote Windows Performance Sources, Script Sources, Syslog Sources, and Script Actions.
  - Sources for Hosted Collectors
    Sources for Hosted Collectors include HTTP Sources and AWS Source Types such as AWS CloudTrail, AWS Config, AWS ELB, Amazon CloudFront, Amazon S3 Audit, and Amazon S3.
- Timestamps, Time Zones, Time Ranges, and Date Formats
  Sumo Logic supports several options for timestamps, time zones, time ranges, and dates.
- Using JSON to Configure Sources
  If you'd like to configure your Sources using JSON files, you can do that too.

Managing collection and data volume

Sumo provides a tool for tracking and managing collection and data volume.

- Log Ingest Data Volume Index
  Sumo writes messages to the index about how much log data your account is ingesting. You can query the index, and if desired, install the Sumo Logic Data Volume app, which provides pre-configured searches and dashboards for analyzing log ingestion.
- Metric Ingest Data Volume Index
  The Metrics Data Volume Index is populated with a set of index messages every five minutes. The messages contain information on how much metrics (by data points) your account is ingesting.

Searching

After configuring Sources to collect the logs you need, you can begin using search within minutes. Sumo Logic search syntax uses logical and familiar operators allowing you to create ad hoc queries quickly and efficiently.

- General Search Examples Cheat Sheet
  The search cheat sheet provides examples of useful search queries for different use cases.
- Search Basics
  This topic describes keyword searches and the basics of Sumo Logic's search syntax.
- Modify a Search from the Messages tab
  After running a search, you can modify subsequent searches by selecting text displayed in the Messages tab. After selecting text, you can choose how to modify the search using the options from a pop-up menu.
- Parsing
  Sumo Logic provides a number of ways to parse fields in your log messages.
- Aggregating
  Aggregating functions evaluate messages and place them into groups, which allows you to count and order your results. Once you have aggregate results, you can visualize your data using charts.
- Search Operators
  This section provides detailed syntax, rules, and examples for Sumo Logic Operators, Expressions, and Search Language.

Search optimization tools

Search optimization tools speed the search process, delivering query results in less time and improving productivity for forensic analysis and log management. Search speed generally depends on the amount of data and the type of query run against the data. Search optimization tools segment the data and queue it up for quick results.

- Optimize Search Performance
  Describes index-based and field-based methods for search optimization, the search optimization process, and how to choose the right tool for the job.

- Partitions
  Partitions speed the search process by allowing you to filter a subset of the log messages in an index.
- Scheduled Views
  Scheduled Views speed the search process for small and historical subsets of your data by functioning as a pre-aggregated index.
- Field Extraction
  Field Extraction speeds the search process by parsing fields as log messages are ingested. The parsing is done automatically, so you don't need to run a query to parse the fields.
- Field Browser
  The Field Browser 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. You can focus on the fields you're interested in, avoiding the "noise" of fields you don't want to see.
- Search Templates
  You can set up search templates to simplify searches for your users. Search templates shield users from search syntax and allow them to select search parameter values from a selector list.

Users, roles and security

Sumo provides a number of tools for managing users' access to Sumo and configuring security policies. You can:

- Set password policies
  Set rules for password expiration, reuse, and lock out.
- Create an Allowlist for IP or CIDR addresses
  Service Allowlist Settings allow you to explicitly grant access to specific IP addresses and/or CIDR notations for logins, APIs, and dashboard access.
- Manage access keys
  Access keys are used in sumo to securely register new collectors and for accessing Sumo APIs.
- Sumo audit index
  If you enable the audit index, Sumo captures information on the internal events that occur in your account associated with account management, user activity, scheduled searches, and more.

- Support account access
  You can enable a Sumo Logic support account, which grants very select Sumo Logic support agents access to your organization's account, better helping those agents to resolve issues that arise. Admins can choose to keep the support account enabled full-time, or the account can be disabled when no issues are being investigated.
- Set Up SAML for Single Sign-On
  Enterprise accounts can provision Security Assertion Markup Language (SAML) 2.0 to enable Single Sign-On (SSO) for user access to Sumo Logic. In addition to basic SAML functionality, you can choose optional on-demand user creation (using SAML 2.0 assertions), and designate custom login and/or logout portals.
- Role-based access control (RBAC). Sumo Logic supports RBAC. Users are not assigned permissions directly, but inherit permissions through roles (or even through a single role). Role assignments grant users specific capabilities, and govern what data users can view.

Metrics

Sumo supports several metric formats: Carbon 2.0, Prometheus, and Graphite. To learn about metrics in Sumo, see Overview of Metrics in Sumo. Metrics-related features for administrators include:

- Metric Rules Editor
  An interface you can use to tag metrics with data derived from the metric identifier. Then, users can use those tags in metric queries.
- Logs-to-Metrics
  Sumo's Logs-to-Metrics features allow you to extract or create metrics from log data:
  - You can extract metrics that are embedded in logs. For example, your logs might contain numerical values for latency, bytes sent, request time, and so on. You can extract multiple metrics from a single log.
  - You can count logs as a metric. For example, you might count the number of log messages that contain a 404 status code.

APIs

For customers with Enterprise accounts, Sumo Logic provides different APIs to interact with third-party scripts and applications.

- Sumo Logic Endpoints
  Sumo Logic has five deployments, or pods, that are assigned depending on the geographic location and the date a Sumo Logic account is created.
- Collector Management API
  The Collector Management API allows you to define an initial Source configuration for your Collectors using a JSON file. It also allows you to create, update, and delete Collectors and Sources from an HTTP endpoint.
- Search Job API
  Sumo Logic exposes the Search Job API for access to resources and log data from third-party scripts and applications. The API follows Representational State Transfer (REST) patterns and is optimized for ease of use and consistency.

Sumo Logic apps

Sumo Logic Applications deliver out-of-the-box Dashboards, reports, saved searches, and field extraction for popular data sources. When you install a Sumo Logic App, these pre-set searches and Dashboards are customized with your Source configurations and populated in a folder in the Library selected by you.

- Using the Library
  The Library provides a central location for shared and saved content in your Sumo Logic account, as well as content shared by others in your organization. All Sumo Logic Apps are available through the Library.
- Run Searches from Sumo Logic Apps
  Sumo Logic Apps provide a host of pre-built saved searches for popular data Sources that you can run against your data without installing the App itself. This way, you can try the searches in an App against your data before you decide to install it. Or you can view the searches to see how good example queries are written.
- Install Apps from the Library
  Sumo Logic Apps are available in the Library. Select from a long list of

popular data Sources and install them right from the Library. Certain Apps have specific installation requirements. Be sure to check the Help topic for your App for specific instructions.

- Log Analysis QuickStart App
  The Log Analysis QuickStart App, created especially for new users of Sumo Logic, includes searches to extract important information from your log files, independent of where they get generated. Whether you are new to log management or plan to migrate from other products, the Log Analysis QuickStart app will bring you up to speed with the Sumo Logic search, visualization, and analytics capabilities.