This guide has documentation for all of the apps that Sumo provides for Amazon and AWS. Please also see the page for the [AWS Observability Solution](https://aws.amazon.com/sumo/).

- **Amazon Aurora MySQL ULM**

  The Sumo Logic App for Aurora MySQL ULM is a unified logs and metrics (ULM) app for your Aurora MySQL database. Logs allow you to monitor database and user activity, incoming connections, query execution time, and errors. The metrics allow you to monitor database resource utilization and throughput performance.

  - Collect logs and metrics for the Amazon Aurora MySQL ULM App
  - Install the Aurora MySQL ULM App and view the Dashboards
• **Amazon Aurora PostgreSQL ULM**

The Sumo Logic App for Aurora PostgreSQL uses unified logs and metrics (ULM) to monitor your Aurora PostgreSQL database. Logs allow you to monitor database and user activity, incoming connections, query execution time, and errors. The metrics allow you to monitor database resource utilization and throughput performance.

- Collect logs and metrics for the Amazon Aurora PostgreSQL ULM App
- Install the Aurora PostgreSQL ULM App and view the Dashboards

• **Amazon CloudFront**

The Sumo Logic App for Amazon CloudFront provides analytics on visitor information, rates and statistics, content being served, and other metrics.
• **Amazon DynamoDB**

The Sumo App for DynamoDB provides operational insight into your database environment. The app includes Dashboards that allow you to view the events, errors, latency, and capacity of your DynamoDB environment.

- Collect Logs and Metrics for the Amazon DynamoDB App
- Install the Amazon DynamoDB App and view the Dashboards

• **Amazon EKS - Control Plane**

The Sumo Logic App for Amazon EKS - Control Plane App provides visibility into the EKS control plane with operational insights into the API server, scheduler, control manager, and worker nodes. The app’s preconfigured dashboards display resource-related metrics for Kubernetes deployments, clusters, namespaces, pods, containers, and daemonsets.

- Collect Logs and Metrics for the Amazon EKS - Control Plane App
Install the Amazon EKS - Control Plane App and view the Dashboards

- **Amazon ElastiCache Redis ULM**

  ![Elasticache Icon]

  The Sumo Logic App for Amazon ElastiCache Redis ULM is a unified logs and metrics (ULM) App that provides visibility into key event and performance analytics to enable proactive diagnosis and response to system and environment issues. The app provides preconfigured dashboards for high-level analysis of event status and trends, locations, and system health and performance metrics.

  - Collect Logs and Metrics for the Amazon ElastiCache Redis ULM App
  - Install the Amazon ElastiCache Redis ULM App and view the Dashboards

- **Amazon Elastic Container Service (ECS)**

  ![Ecs Icon]
Provides preconfigured searches and Dashboards that allow you to monitor various metrics.

- Collect Logs and Metrics for the Amazon ECS App
- Install the Amazon ECS App and view the Dashboards

**Amazon GuardDuty**

The Amazon GuardDuty Sumo Logic app provides insights into the activities in your AWS account based on the findings from Amazon GuardDuty. The App includes preconfigured dashboards that allow you to detect unexpected and potentially malicious activities in your AWS account by providing details on threats by severity, VPC, IP, account ID, region, and resource type.

- Collect Logs for the Amazon GuardDuty App
- Install the Amazon GuardDuty App and view the Dashboards

**Amazon Inspector App**

Allows you to monitor your AWS resources for potential security risks.
Collect Data for the Amazon Inspector App
Install the Amazon Inspector App and view the Dashboards

• **Amazon Kinesis - Streams**

The Sumo Logic App for Amazon Kinesis - Streams is a unified logs and metrics (ULM) App which provides information on the events and metrics. The preconfigured dashboards help you monitor the events, API calls, errors, incoming and outgoing records, latencies, and throughput of Kinesis.

Collect Logs and Metrics for the Amazon Kinesis - Streams App
Install the Amazon Kinesis - Streams App and view the Dashboards

• **Amazon RDS Metrics**

The Sumo Logic App for Amazon RDS Metrics provides visibility into your Amazon Relational Database Service (RDS) Metrics collected via a CloudWatch Metrics Source.

Collect Metrics for the Amazon RDS App
Install the Amazon RDS Metrics App and view the Dashboards
• **Amazon Redshift ULM**

The Sumo Logic App for Amazon Redshift ULM helps you monitor activity in Amazon Redshift.

- Collect Logs and Metrics for the Amazon Redshift ULM App
- Install the Amazon Redshift ULM App and View the Dashboards

• **Amazon S3 Audit**

Provides a simple web services interface that can be used to store and retrieve any amount of data from anywhere on the web.

- Collect logs for the Amazon S3 Audit App
- Install the Amazon S3 Audit App and view the Dashboards
• **Amazon Security Quick Start**

The Sumo Logic AWS Security QuickStart solution helps customers automate the collection of security events from AWS security services and the installation and configuration of over 11 Sumo Logic apps designed for AWS security.

  ◦ Security Quick Start Setup Guide

• **Amazon SES**

The Sumo App for Amazon SES provides operational insight into Amazon Simple Email Service. The app includes dashboards that allow you to view information about bounced notifications, delivered notifications, and CloudTrail events.

  ◦ Collect Logs for the Amazon SES App
  ◦ Install the Amazon SES App and view the Dashboards
• Amazon SNS

The Sumo Logic App for Amazon SNS is a unified logs and metrics (ULM) App that provides insights into the operations and utilization of your SNS service. The preconfigured dashboards help you monitor the key metrics by application, platform, region, and topic name, view the SNS events for activities, and help you plan the capacity of your SNS service.

◦ Collect Logs and Metrics for the Amazon SNS App
◦ Install the Amazon SNS App and view the Dashboards

• Amazon SQS

The Sumo Logic App for Amazon SQS is a unified logs and metrics (ULM) App that provides operational insights into your Amazon SQS utilization. The preconfigured dashboards help you monitor the key metrics, view the SQS events for queue activities, and help you plan the capacity of your SQS service utilization.

◦ Collect Logs and Metrics for the Amazon SQS App
◦ Install the Amazon SQS App and view the Dashboards
• **Amazon VPC Flow Logs**

Logs the IP network traffic of your VPC, allowing you to troubleshoot traffic and security issues.

- Collect Amazon VPC Flow Logs from CloudWatch using CloudFormation
- Collect Amazon VPC Flow Logs using an AWS S3 Source
- Install the Amazon VPC Flow Logs App and view the Dashboards

• **AWS CloudTrail**

Ingests logs of API calls made to AWS, providing greater visibility into events that allow for security and operations forensics.

- Collect Logs for the AWS CloudTrail App
- Enable Sumo to Track AWS Admin Activity
- Install the AWS CloudTrail App and view the Dashboards
- Configure the AWS CloudTrail App in Multiple Environments

• **AWS Config**

Provides a simple web services interface that can be used to track modifications made to the resources that
belong to an AWS account.

- Collect Logs for the AWS Config App
- Install the AWS Config App and view the Dashboards

**AWS Elastic Load Balancer - Application**

Use the Sumo Logic App to analyze raw Application Load Balancer data to investigate the availability of applications running behind Application Load Balancers.

- Collect Logs for the AWS Elastic Load Balancer Application App
- Install the AWS Elastic Load Balancing - Application App and view the Dashboards

**AWS Elastic Load Balancing**

Distributes incoming application traffic across multiple Amazon EC2 instances in the AWS Cloud.

- Collect Logs for the AWS Elastic Load Balancing App
- Install the AWS Elastic Load Balancing App and view the Dashboards
• **AWS Elastic Load Balancing - Classic**

Distributes incoming application traffic across multiple Amazon EC2 instances in the AWS Cloud.
- Collect Logs for the AWS Elastic Load Balancing- Classic App
- Install the AWS Elastic Load Balancer - Classic App and view the Dashboards

• **AWS Elastic Load Balancing Metrics**

The Sumo Logic App for AWS Elastic Load Balancing (ELB) Metrics lets you analyze the CloudWatch ELB metrics for the Application Load Balancer (ALB), and the Classic Load Balancer (CLB). The App provides preconfigured searches and dashboards that allow you to monitor the metrics healthy hosts, unhealthy hosts, HTTP backend codes, latency, requests, and more.
- Collect Metrics for the AWS Elastic Load Balancing App
- Install the AWS Elastic Load Balancing Metrics App and view the Dashboards
• AWS Elastic Load Balancing ULM - Application

The Sumo Logic App for AWS Elastic Load Balancing ULM - Application is a unified logs and metrics (ULM) App that gives you visibility into the health of your Application Load Balancer and target groups. Use the preconfigured dashboards to understand the latency, request and host status, threat intel, and HTTP backend codes by availability zone and target group.

◦ Collect Logs and Metrics for the AWS Elastic Load Balancing ULM - Application App
◦ Install the AWS Elastic Load Balancing ULM - Application App and view the Dashboards

• AWS Elastic Load Balancing ULM - Classic

The Sumo Logic App for AWS Elastic Load Balancing Classic is a unified logs and metrics (ULM) App which helps you monitor the classic load balancer. The preconfigured dashboards provide information on the latency, HTTP backend codes, requests, and host status, that help you investigate the issues in the load balancer.

◦ Collect Logs and Metrics for the AWS Elastic Load Balancing ULM - Classic App
◦ Install the AWS Elastic Load Balancing ULM - Classic App and view the Dashboards
• **AWS Lambda**

The AWS Lambda App helps you monitor the operational and performance trends in all the Lambda functions in your account. The App uses two data sources - AWS CloudWatch logs for Lambda, and CloudTrail Lambda Data Events.

- Collect Logs for the AWS Lambda App
- Install the AWS Lambda App and view the Dashboards

• **AWS Lambda ULM**

The AWS Lambda ULM App is a unified logs and metrics (ULM) app for monitoring operation and performance trends of the Lambda functions in your account. Preconfigured dashboards provide insights into executions, such as memory and duration usage by function versions or aliases, as well as performance metrics such as errors, throttles, invocations, and concurrent executions.

- Collect Logs and Metrics for the AWS Lambda ULM App
- Install the AWS Lambda ULM App and View the Dashboards

• **AWS Network Firewall**

AWS Network Firewall application provides visibility into traffic flows and alerts generated by AWS Network Firewall.

- Collect Logs for AWS Network Firewall
- Install the AWS Network Firewall App and View the Dashboards
• AWS Security Hub

AWS Security Hub is an AWS security service that provides a comprehensive view of your security state within AWS and your compliance with the security industry standards and best practices. The Sumo Logic App for AWS Security Hub leverages findings data from Security Hub and visually displays the data in Dashboards. The dashboards provide a high-level view of findings, showing the type, when they occurred, the resources that were affected, their severity, and their distribution, showing the cur

- Send findings to AWS Security Hub
- Collect findings for the AWS Security Hub App
- Install the AWS Security Hub App and view the Dashboards

• AWS WAF

The Sumo Logic App for AWS Web Application Firewall (WAF) analyzes traffic flowing through AWS WAF and automatically detects threats via Sumo Logic Threat Intel.

- Collect Logs for the AWS WAF App
- Install the AWS WAF App and View the Dashboards
• **CIS AWS Foundations Benchmark App**

![CIS AWS Foundations Benchmark App logo]

This app provides alerts and visibility into an organization's AWS security posture. It is based on the CIS AWS Benchmarks Foundation recommendations.

- Collect Logs for the CIS AWS Foundation Benchmark App
- Install the CIS AWS Foundations Benchmark App and view the Dashboards

• **Global Intelligence for Amazon GuardDuty**

![Global Intelligence for Amazon GuardDuty logo]

The Sumo Logic Global Intelligence Amazon GuardDuty App integrates Global Intelligence Service (GIS) with Amazon GuardDuty for continuous machine learning and statistical baselines for KPIs (key performance indicators) and KRIs (key risk indicators). The App includes preconfigured dashboards and searches with visual displays for global threat baselines and real-time threat detection across your AWS environment.

- Configure Log Collection and Install the GI GuardDuty App
- View the GI GuardDuty App Dashboards
• **Global Intelligence for AWS CloudTrail SecOps**

The Global Intelligence for AWS CloudTrail App enables you to detect potentially malicious configuration changes in your AWS account by comparing AWS CloudTrail events in your account against a cohort of AWS customers.

- Collect Logs for the GI for AWS CloudTrail SecOps App
- Install the GI for AWS CloudTrail SecOps App and view the Dashboards

• **Global Intelligence for AWS CloudTrail DevOps**

Global Intelligence for AWS Cloud Trail - DevOps provides insights for on-call engineers, SRE, and DevOps users to help minimize AWS errors and maximize app availability.

- Collect Logs for the Global Intelligence for AWS CloudTrail DevOps App
- Install the Global Intelligence for AWS CloudTrail DevOps App and View the Dashboards

• **PCI Compliance for Amazon VPC Flow Logs**

The Sumo Logic App for Payment Card Industry (PCI) Compliance for Amazon VPC Flow Logs App offers dashboards to monitor systems, account and users activity to ensure that login activity and privileged users are within the expected ranges. The PCI Compliance for Amazon VPC Flow Logs App covers PCI requirements 01, 02, and 04.

- Collect Logs for the PCI Compliance for Amazon VPC Flow Logs App
- Install the PCI Compliance for Amazon VPC Flow Logs App and view the Dashboards
• PCI Compliance for AWS CloudTrail App

PCI

The Sumo Logic App for Payment Card Industry (PCI) Compliance for AWS CloudTrail App offers dashboards to monitor systems, account and users activity to ensure that login activity and privileged users are within the expected ranges. The PCI Compliance for AWS CloudTrail App covers PCI requirements 02, 07, 08 and 10.

◦ Collect Logs for the PCI Compliance for AWS Cloud Trail App
◦ Install the PCI Compliance for AWS Cloud Trail App and view the Dashboards

• Threat Intel for AWS

CrowdStrike

This App correlates CrowdStrike threat intelligence data with your AWS log data to help detect any threats in your environment.

◦ Collect Logs for the Threat Intel for AWS App
◦ Install the Threat Intel for AWS App and view the Dashboards