08-11-2026

Amazon

Amazon is a global technology company best known for its e-commerce platform, digital streaming, consumer electronics, and cloud computing services. Amazon has grown to become one of the world's largest retailers and technology innovators, serving millions of customers worldwide across a diverse range of products and services—including Amazon Web Services (AWS), which powers cloud infrastructure for organizations of all sizes.

Before looking at documentation for specific data sources, review the Splunk Help information on general data ingestion for Splunk Enterprise, Splunk Cloud Platform or Splunk Observability Cloud.

Getting data in

We recommend starting with Following best practices for ingesting data from your AWS environment and then looking in more detail at options for the source types listed below.

Source	Add-ons and Apps	Guidance
AWS Amazon Web Services provides on-demand cloud computing platforms and APIs to individuals, companies, and governments, on a metered pay-as-you-go basis. These cloud computing web services provide various services related to networking, compute, storage, middleware, IOT, and other processing capacity, as well as software tools via AWS server farms. This frees clients from managing, scaling, and patching hardware and operating systems, and provides a way of obtaining large-scale computing capacity more quickly and cheaply than building an actual physical server farm.	**Splunk platform** • Splunk Add-on for Amazon Web Services (AWS) • Splunk App for AWS Security Dashboards **Splunk Enterprise Security** • SecKit AWS Assets Add-on for Splunk Enterprise	**Configuration** • Introduction to the Splunk Add-on for Amazon Web Services • Connect AWS to Splunk Observability Cloud • SA-AWS Assets for Splunk Enterprise Security **Splunk Lantern**

Source	Add-ons and Apps	Guidance
	Security **Splunk SOAR** • AWS GuardDuty • AWS Athena • AWS Systems Manager • AWS Inspector	**Articles** • Migrating AWS inputs to Data Inputs • Managing an Amazon Web Services environment • Monitoring user activity spikes in AWS • Detecting AWS suspicious provisioning activities • Detecting privilege escalation in your AWS environment • Analyzing AWS service action errors

CloudTrail

CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. You can use it to log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. In the Common Information Model, CloudTrail log data is typically mapped to the Authentication and Change data models.

CloudTrail data provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. It increases visibility into your user and resource activity by recording AWS Management Console actions and API calls so you can detect unusual

	Splunk SOAR • AWS CloudTrail	**Splunk Lantern Articles** • Configuring AWS CloudTrail and CloudWatch data collection • Using ingest actions to filter AWS CloudTrail logs • Managing an

Source	Add-ons and Apps	Guidance
activity.		Amazon Web Services environment • Monitoring user activity spikes in AWS • Detecting AWS suspicious provisioning activities • Detecting privilege escalation in your AWS environment
CloudWatch CloudWatch is a service that provides data and actionable insights for AWS, hybrid, and on-premises applications and infrastructure resources. CloudWatch enables you to monitor your complete stack and leverage alarms, logs, and events data to take automated actions and reduce Mean Time to Resolution (MTTR). CloudWatch collects, aggregates, and summarizes compute utilization information like CPU, memory, disk, and network data, as well as diagnostic information like container restart failures, to help DevOps engineers isolate issues and resolve them quickly. CloudWatch gives you actionable insights that help you optimize application performance, manage resource utilization, and understand system-wide operational health. It allows you to perform historical analysis for cost optimization and derive real-time insights into optimizing applications and infrastructure resources.	**Splunk platform** • AWS CloudWatch Integration	**Splunk Lantern Articles** • Configuring AWS CloudTrail and CloudWatch data collection • Managing an Amazon Web Services environment • Monitoring user activity spikes in AWS • Detecting AWS suspicious provisioning activities • Detecting privilege

Source	Add-ons and Apps	Guidance
		escalation in your AWS environment
Elastic Cloud Compute (EC2) Amazon Elastic Compute Cloud (EC2) provides scalable computing capacity in the cloud, allowing users to rent virtual servers (instances) to run applications. It offers secure, resizable compute capacity, enabling users to launch as many or as few virtual servers as needed and scale resources up or down quickly.	**Splunk SOAR** • AWS EC2	**Splunk Lantern Articles** • Managing an Amazon Web Services environment
Elastic Kubernetes Service (EKS) Elastic Kubernetes Service (EKS) is a managed container service to run and scale Kubernetes applications in the cloud or on-premises.	**Splunk Observability Cloud** • Splunk OpenTelemetry Collector for Kubernetes	**Splunk Lantern Articles** • Monitoring Amazon Elastic Kubernetes Services (EKS) with Splunk Observability Cloud • Running Edge Processor nodes in Amazon EKS • Load balancing traffic to Edge Processors in Amazon EKS **Splunk Resources** • Monitor Amazon EKS Anywhere with Splunk

Source	Add-ons and Apps	Guidance
		• Monitor Amazon EKS Distro (EKS-D) with Splunk Infrastructure Monitoring
Identity and Access Management (IAM) Identity and Access Management (IAM) provides fine-grained access control across all of AWS. With IAM, you can specify who can access which services and resources, and under which conditions. With IAM policies, you manage permissions to your workforce and systems to ensure least-privilege permissions.	**Splunk SOAR** • AWS IAM	**Splunk Lantern Articles** • Detecting privilege escalation in your AWS environment • Detecting AWS security hub alerts
Kinesis Firehose Amazon Kinesis Data Firehose is a fully managed service for delivering real-time streaming data directly to destinations like Amazon S3, Redshift, Elasticsearch, and Splunk. It simplifies the process of capturing, transforming, and loading data streams without requiring complex administration or custom processing.	**Splunk platform** • Splunk Add-on for Amazon Kinesis Firehose	**Configuration** • About the Splunk Add-on for Amazon Kinesis Firehose **Splunk Lantern Articles** • Ingesting VPC flow logs into Edge Processor via Amazon Data Firehose
	Splunk SOAR	**Configuration**

Source	Add-ons and Apps	Guidance
Lambda Lambda is a compute service that lets you run code without provisioning or managing servers. Lambda runs your code on a high-availability compute infrastructure and performs all of the administration of the compute resources, including server and operating system maintenance, capacity provisioning and automatic scaling, code monitoring and logging.	• AWS Lambda	• Instrument AWS Lambda functions for Splunk Observability Cloud • Use AWS Lambda with HTTP Event Collector **Splunk Lantern Articles** • Monitoring AWS Lambda functions • Managing an Amazon Web Services environment • Logging output from AWS Lambda functions
Relational Database Service (RDS) Amazon RDS (Relational Database Service) is a managed database service that simplifies the setup, operation, and scaling of relational databases in the cloud. It supports multiple database engines, including MySQL, PostgreSQL, and SQL Server, while automating time-consuming tasks like backups, patching, and scaling. RDS is commonly used for application databases, reporting, or data warehousing.		**Splunk Lantern Articles** • Monitoring AWS Relational Database Services
Security Token Service AWS Security Token Service (STS) is a web service that enables you to request temporary, limited-privilege credentials for AWS Identity and Access Management (IAM) users or federated users. It enhances security by providing short-lived tokens for accessing AWS resources,	**Splunk SOAR** • AWS Security Token Service	

Source	Add-ons and Apps	Guidance
reducing the risk associated with long-term access keys.		
## Security Hub AWS Security Hub is a cloud security service that provides a comprehensive view of your security alerts and compliance status across your AWS accounts. It centralizes and aggregates security findings from various AWS services and third-party tools, helping you to prioritize and respond to security issues effectively.	**Splunk SOAR** • AWS Security Hub	**Splunk Lantern Articles** • Detecting AWS security hub alerts
## Simple Storage Service (S3) Amazon Simple Storage Service (S3) is a scalable object storage service that enables users to store and retrieve any amount of data from anywhere on the web. S3 is widely used for backup, archiving, content distribution, and data analytics.	**Splunk SOAR** • AWS S3	**Splunk Lantern Articles** • Accelerating security forensics with Federated Search for Amazon S3 • Correlating data for threat insights using Federated Search for Amazon S3 • Hunting threats across Amazon S3-backed firewall logs using Federated Search in Splunk Cloud Platform • Implementing a reingestion pipeline for AWS logs using Kinesis Data Firehose • Ingesting

Source	Add-ons and Apps	Guidance
		AWS S3 data written by ingest actions • Leveraging Federated Search for Amazon S3 for key security use cases • Monitoring AWS S3 for suspicious activities • Performing data exploration and statistical analysis with Federated Search for Amazon S3 • Sending masked PII data to the Splunk platform and routing unmasked data to federated search for Amazon S3 • Simplifying compliance trails and audits with Federated Search for Amazon S3 • Streamlining threat reporting, dashboarding, and alerting with

Source	Add-ons and Apps	Guidance
		Federated Search for Amazon S3 • Using Edge Processor to filter out cardholder data for PCI DSS compliance • Using Federated Search for Amazon S3 for monitoring and detection • Using federated search for Amazon S3 to filter, enrich, and retrieve data from Amazon S3 • Using federated search for Amazon S3 with Edge Processor • Using federated search for Amazon S3 with ingest actions • Migrating from Federated Search 1.0 to 2.0 for S3 and Security Lake deployments

Source	Add-ons and Apps	Guidance
VPC Flow VPC Flow logs contain a comprehensive record of network traffic in and out of your AWS environment. By default, the record includes values for the different components of the IP flow, including the source, destination, and protocol. They are often used for troubleshooting connectivity issues across your VPCs, intrusion detection, or anomaly detection. In the Common Information Model, VPC flow log data is typically mapped to the Network Traffic Data model.		**Splunk Lantern Articles** • Managing an Amazon Web Services environment • Detecting AWS network ACL activity • Using ingest actions to filter AWS VPC Flow Logs • Detecting distributed service abuse with in-stream VPC flow aggregations
Web Application Firewall AWS Web Application Firewall (WAF) is a cloud-based security service that protects web applications from common web exploits and malicious traffic. It allows you to create custom security rules to monitor and filter HTTP(S) requests, safeguarding against attacks like SQL injection and cross-site scripting.	**Splunk platform** • AWS Web Application Firewall Add-on **Splunk SOAR** • AWS WAF V2	