Sumo Logic Security Integrations on the AWS Cloud

Quick Start Reference Deployment

March 2020

Sumo Logic
AWS Quick Start team

Visit our GitHub repository for source files and to post feedback, report bugs, or submit feature ideas for this Quick Start.

Contents

This Quick Start was created by Sumo Logic in collaboration with Amazon Web Services (AWS).

Quick Starts are automated reference deployments that use AWS CloudFormation templates to deploy key technologies on AWS, following AWS best practices.

Overview

Sumo Logic is a leader in continuous intelligence, a new category of software to address the data challenges and opportunities presented by digital transformation, modern applications, and cloud computing. The Sumo Logic Continuous Intelligence Platform automates the collection, ingestion, and analysis of application, infrastructure, security, and Internet of Things (IoT) data to derive actionable insights.

Sumo Logic on AWS

Sumo Logic customers have been using the Sumo Logic app for AWS CloudTrail to track user activity, the Sumo Logic app for Amazon GuardDuty to monitor threat detection, and the Sumo Logic Global Intelligence (formerly, Benchmark) app for GuardDuty to understand how their security posture compares with the global benchmarks that Sumo Logic gathers from hundreds of Sumo Logic customers. The VPC Flow Logs and AWS WAF apps are used to monitor traffic patterns. The Threat Intel app for AWS is used to help detect threats in your environment with Sumo Logic Threat Intelligence, whereas the Sumo Logic apps for PCI DSS and CIS AWS Foundations for AWS compliance are used to simplify audits and maintain compliance.

Given that most customers use multiple security apps, Sumo Logic has created an AWS Security Integrations Quick Start that allows customers to automate the following.

- The collection of security events from AWS security services
- The installation and configuration of over 11 Sumo Logic apps designed for AWS security

Specifically, the Quick Start template automatically creates resources in your AWS account to collect logs by using various AWS services. The resources then send the logs to your pre-registered Sumo Logic account. In about 10 minutes, you can start monitoring and troubleshooting in real time. You can analyze any security threats and quickly detect indicators of compromise.

Using the Quick Start, you can automatically configure both AWS and Sumo Logic so as to get the following Sumo Logic apps setup:

- AWS CloudTrail
- Amazon GuardDuty
- Global Intelligence for Amazon GuardDuty

- Amazon VPC Flow Logs
- AWS WAF
- Threat Intel for AWS
- PCI Compliance for AWS CloudTrail
- PCI Compliance for Amazon VPC Flow Logs
- CIS AWS Foundations Benchmark
- Amazon S3 Audit
- AWS Security Hub
- AWS Config

The Sumo Logic Quick Start deployment includes best practices, built-in content, queries, and dashboards to help you detect, investigate, and respond to security threats and vulnerabilities in their AWS environments.

Cost and licenses

You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using the Quick Start.

The AWS CloudFormation template for this Quick Start includes configuration parameters that you can customize. Some of these settings, such as instance type, affect the cost of deployment. For cost estimates, see the pricing pages for each AWS service you will use. Prices are subject to change.

> **Tip:** After you deploy the Quick Start, we recommend that you enable the AWS Cost and Usage Report. This report delivers billing metrics to an Amazon Simple Storage Service (Amazon S3) bucket in your account. It provides cost estimates based on usage throughout each month and finalizes the data at the end of the month. For more information about the report, see the AWS documentation.

For pricing information, visit the Sumo Logic website.

Architecture

Deploying this Quick Start with **default parameters** builds the following environment in a specific account and Region in the AWS Cloud.

AWS Security QuickStart Architecture

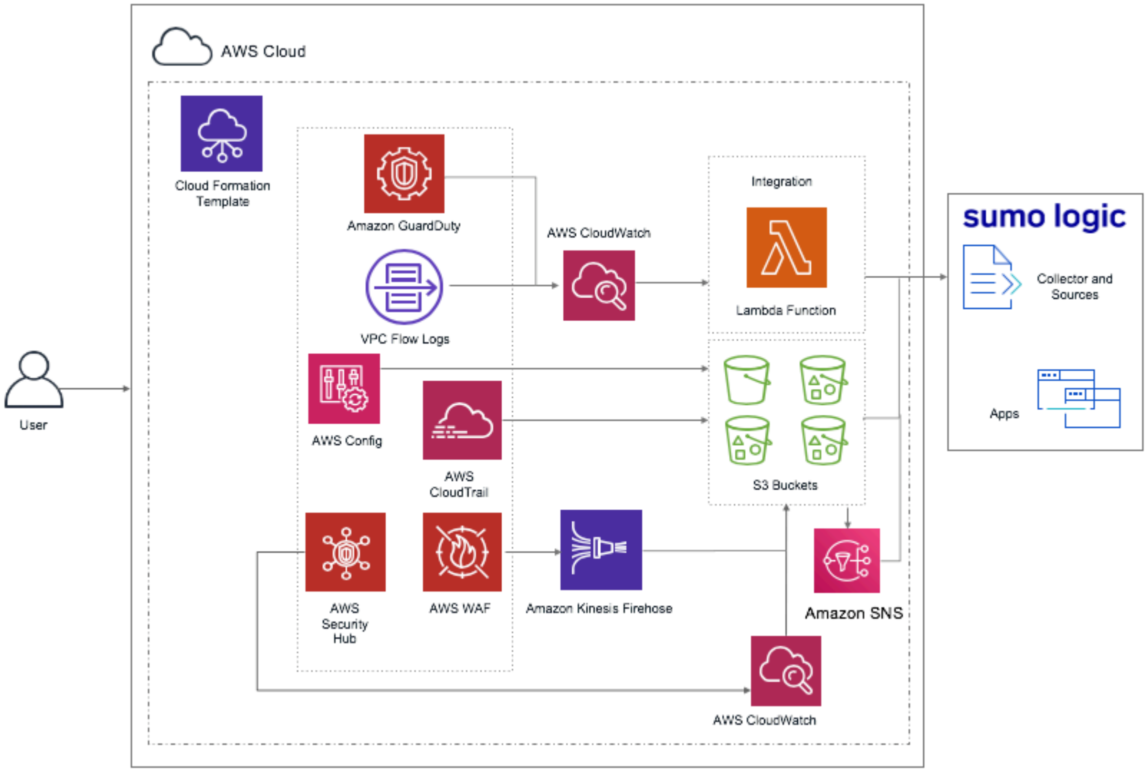


Figure 1: Quick Start architecture for Sumo Logic on AWS

This Quick Start sets up the following serverless architecture:

- Multiple CloudFormation stacks deployed in your environment. Each stack consists of more than one AWS resource, including S3 buckets, AWS Lambda functions, and Amazon Kinesis Data Firehose delivery streams.
- Lambda functions to create a collector and multiple sources, and to install apps on your Sumo Logic account.
- S3 buckets to capture the logs from the various AWS services.
- The Sumo Logic collector and sources to consume logs from the S3 buckets.
- Firehose delivery streams for transferring logs from AWS WAF to S3 buckets.
- S3 Event Notification triggers an Amazon Simple Notification Service (Amazon SNS) topic when there is a new object in a bucket.

Planning the deployment

Specialized knowledge

Before you deploy this Quick Start, we recommend that you become familiar with the following AWS services and Sumo Logic. If you are new to AWS, see Getting Started with AWS.

- AWS Security Services
  - AWS CloudTrail
  - AWS CloudFormation
  - AWS CloudWatch
  - AWS IAM
  - Amazon SNS
  - AWS Lambda
  - Amazon Kinesis Firehose
  - Amazon S3
  - VPC Flow Logs
  - AWS Config
  - Amazon GuardDuty
- The Sumo Logic Console
- Determine which Sumo Logic apps you would like to use to monitor the above AWS security services:
  - AWS CloudTrail
  - Amazon GuardDuty
  - Global Intelligence for Amazon GuardDuty
  - Amazon VPC Flow Logs
  - AWS WAF
  - Threat Intel for AWS
  - PCI Compliance for AWS CloudTrail
  - PCI Compliance for Amazon VPC Flow Logs

- CIS AWS Foundations Benchmark
- Amazon S3 Audit
- AWS Security Hub
- AWS Config

Scenarios supported by this QuickStart

This QuickStart supports the following scenarios:

Scenario 1: New to AWS Security services and new to Sumo Logic
You have not already configured AWS to use one or more of the security services called out above but would like to do so and want to collect and analyze that data in Sumo Logic via apps. In this scenario, you will use the QuickStart to setup AWS security services as well as collection and apps in Sumo Logic.

Scenario 2: Using AWS Security but new to Sumo Logic
You are actively using all of the AWS Security services that you need, but have not configured Sumo Logic to set up collection and apps. In this scenario, you will use the QuickStart to setup collection and apps of these in Sumo Logic by creating the requisite resources to do so in both Sumo Logic and AWS.

Scenario 3: You are using AWS Security and are using Sumo Logic
You are actively using all of the AWS Security services you need, and are collecting and analyzing data from one or more of them in Sumo Logic. In this scenario, you will use the QuickStart to setup collection and apps in Sumo Logic by creating the requisite resources to do so in both Sumo Logic and AWS.

AWS account

If you don’t already have an AWS account, create one at https://aws.amazon.com by following the on-screen instructions. Part of the sign-up process involves receiving a phone call and entering a PIN using the phone keypad.

Your AWS account is automatically signed up for all AWS services. You are charged only for the services you use.

Technical requirements

From a technical standpoint, you need the following:

- A Sumo Logic account. If you don't already have a Sumo Logic enterprise account, create one at https://www.sumologic.com/ by following the on-screen instructions.
- An AWS account. If you don't already have an AWS account, create one at https://aws.amazon.com by following the on-screen instructions.
- The ability to launch AWS CloudFormation templates that create AWS Identity and Access Management (IAM) roles.
- Understand how Sumo Logic resources are created:
  - For Collection:
    - For Scenario 1: A new Sumo Logic hosted collected called: aws-quickstart-collector is created and sources for each app are installed under it
    - For Scenarios 2 and 3: All existing sources can be reused. All new sources are installed under a new Sumo Logic hosted collected called: aws-quickstart-collector.
  - All Sumo Logic apps are installed in your personal folder in a folder named "Sumo Logic Amazon QuickStart Apps" followed by the date. For example: "Sumo Logic Amazon QuickStart Apps
  - Understand how data sources from AWS security services map to various Sumo Logic apps:

AWS Security Service	**Sumo Logic apps**
AWS CloudTrail	AWS CloudTrail, PCI Compliance for AWS CloudTrail, CIS AWS Foundations Benchmark
Amazon GuardDuty	Amazon GuardDuty, Global Intelligence for Amazon GuardDuty
Amazon VPC Flow Logs	Amazon VPC Flow Logs, PCI Compliance for Amazon VPC Flow Logs, Threat Intel for AWS
Amazon S3 Access logging	S3 Audit App
AWS Security Hub	AWS Security Hub
AWS WAF	AWS WAF
AWS Config	AWS Config

  - Note: The Threat Intel for AWS Sumo Logic app can also report on data from AWS ELB in case you are already sending that data to Sumo Logic.

- Here's some information we recommend you collect before you proceed if you have already configured AWS security services to send their logs to S3 buckets or SNS topics. Note: If you have not performed these, this QuickStart will automatically configure the AWS Services and requisite resources for you when you choose to install the Sumo Logic apps called out in the first column.

Sumo Logic Apps	**If you have done the following:**	**Make a note of :**
CloudTrail, PCI Compliance for AWS CloudTrail, CIS AWS Foundations Benchmark apps	Configured AWS CloudTrail to send its logs to an S3 bucket	- The S3 bucket name
VPC Flow Logs, PCI Compliance for Amazon VPC Flow Logs	Configured AWS VPC Flow to send its logs to an S3 bucket	- The S3 bucket name
S3 Audit	Configured the access logging of S3 buckets	- The S3 bucket name
WAF	Configured WAF to send a Kinesis delivery stream to an S3 bucket.	- The S3 bucket name
Config	Configured AWS Config to deliver its notifications to an SNS topic.	- The SNS topic

- If you would like to use the Threat Intel app and are already sending AWS ELB load-balancer logs to Sumo Logic, please make a note of its source category in Sumo Logic.

Deployment steps

This Quick Start deployment builds a new AWS environment consisting of the infrastructure resources required to provision applications to your Sumo Logic account and necessary resources to your AWS account. During the deployment, you can choose which applications y to install.

Step 1. Prepare your Sumo Logic Account

1. If you don't already have a Sumo Logic enterprise account, create one at https://sumologic.com by following the on-screen instructions.
2. Create Access Key and Access Id from your Sumo Logic account. You need them to pass as parameters when you launch the Quick Start template in the next step.
3. You also need to pass the Organization ID, which you can get from your Sumo Logic account under **Administration** > **Account**.

> **Note:** If you want to use the Sumo Logic Threat Intel for AWS app as part of this Quick Start and have not configured collection of this data, follow the instructions in the Sumo Logic documentation. If you have already configured collection of this data, note the relevant Sumo Logic source category for this data.

Step 2. Sign in to your AWS account

1. Sign in to your AWS account at https://aws.amazon.com with an IAM user role that has the necessary permissions. For details, see Planning the deployment earlier in this guide.

Step 3. Launch the Quick Start

1. Deploy the Sumo Logic Security Integrations Quick Start.

Deploy Sumo Logic Security Integrations

Each deployment takes about 10 minutes to complete.

2. Check the Region displayed in the upper-right corner of the navigation bar, and change as necessary. This is where the infrastructure for Sumo Logic Application resources will be built.

3. On the **Create stack** page, keep the default setting for the template URL, then choose **Next**.
4. On the **Specify stack details** page, change the stack name if needed. Review the parameters for the template. Provide values for the parameters that require input. For all other parameters, review the default settings and customize them as necessary.

   When you finish reviewing and customizing the parameters, choose **Next**.

PARAMETERS TO DEPLOY THE QUICKSTART

View template

Sumo Logic Configuration:

Parameter label (name)	**Default**	**Description**
`Sumo Logic deployment name` (`Section1aSumoLogicDeployment`)	*Requires Input*	Enter the geographic location of the deployment: au, ca, de, eu, jp, us2, in, fed or us1.
`Sumo Logic Access ID` (`Section1bSumoLogicAccessID`)	*Requires Input*	Enter the Sumo Logic Console Access ID, which you received when you created the Access Key.
`Sumo Logic Access Key` (`Section1cSumoLogicAccessKey`)	*Requires Input*	Enter your Sumo Logic Access Key. You can obtain this from your Sumo Logic account (choose Administration > Security > Access Keys).
`Delete Sumo Logic Resources when stack is deleted` (`Section1eSumoLogicResourceRemoveOnDeleteStack`)	true	If this parameter is set to **true**, the collector, sources, and Sumo Logic apps will be deleted. If this parameter is set to **false** then the collector, sources, and Sumo Logic apps will not be deleted.
`Sumo Logic Organization ID` (`Section1dSumoLogicOrganizationId`)	*Requires Input*	Enter your Sumo Logic Organization ID, which you can find on your Sumo Logic console under Account.

Sumo Logic CloudTrail Apps Configuration:

- For these apps
  - Select the CloudTrail apps you need to install, which will be one of AWS CloudTrail, PCI Compliance for AWS CloudTrail, CIS AWS Foundations Benchmark apps.
  - If you already have a bucket with CloudTrail logs, skip creation of bucket.

  - If you don't have CloudTrail Source, provide the existing bucket name, along with path expression to create a CloudTrail source in Sumo Logic.
- If you already have Sumo Logic CloudTrail source, provide the source category.

Parameter label (name)	Default	Description
Install Sumo Logic AWS CloudTrail App (`Section2aInstallCloudTrailApp`)	Yes	Yes -> Install Sumo Logic AWS CloudTrail App in Sumo Logic for AWS Quick Start Solution. No -> Skip Installation of the app.
Install Sumo Logic PCI Compliance For AWS CloudTrail App (`Section2bInstallPCICloudTrailApp`)	Yes	Yes -> Install PCI Compliance For AWS CloudTrail App in Sumo Logic for AWS Quick Start Solution. No -> Skip Installation of the app.
Install Sumo Logic CIS AWS Foundations Benchmark App (`Section2cInstallCISFoundationApp`)	Yes	Yes -> Install CIS AWS Foundations Benchmark App in Sumo Logic for AWS Quick Start Solution. No -> Skip Installation of the app.
Create AWS S3 Bucket (`Section2dCloudTrailCreateBucket`)	Yes	Yes – Create a new CloudTrail bucket in AWS S3. No – Use an existing CloudTrail bucket from AWS S3 which has CloudTrail Logs.
AWS S3 Bucket Name (`Section2eCloudTrailLogsBucketName`)	-	Required when Flag = No. Provide an Existing bucket name which has CloudTrail logs.
Create Sumo Logic CloudTrail Logs Source (`Section2fCloudTrailCreateLogSource`)	Yes	Yes – Create Sumo Logic Cloud Trail Log Source with provided bucket Name. No – Skip creation of the Sumo Logic Cloud Trail Log Source.
Path Expression for the logs (`Section2gCloudTrailBucketPathExpression`)	AWSLogs/*/CloudTrail/*	Path expression to match the folder structure for CloudTrail logs. For Eg:- AWSLogs/*/CloudTrail/*
Sumo Logic CloudTrail Logs Source Category Name (`Section2hCloudTrailLogsSourceCategoryName`)	-	Required when Flag = No. Provide an existing source category name from Sumo Logic collecting CloudTrail Logs. Used for Threat Intel for AWS app installation also.

Sumo Logic GuardDuty Apps Configuration:

- For these apps
  - Select the GuardDuty apps you need to install: Amazon GuardDuty, Amazon GuardDuty Benchmark apps.
  - If you already have Sumo Logic HTTP source that is collecting GuardDuty logs, provide the source category.

Parameter label (name)	Default	Description
Install Sumo Logic Amazon GuardDuty Apps (`Section3aInstallGuardDutyApps`)	Both	GuardDuty -> Install Amazon GuardDuty App in Sumo Logic for AWS Quick Start Solution. GuardDutyBenchmark -> Install Amazon GuardDuty Benchmark App in Sumo Logic for AWS Quick Start Solution. Both -> Install Both the apps. Skip -> Skip Installation of the apps.
Create Sumo Logic HTTP Logs Source (`Section3bGuardDutyCreateHttpLogsSource`)	Yes	Yes – Create Sumo Logic HTTP Log Source to collect GuardDuty logs. No – Skip creation of the Sumo Logic HTTP Log Source.
Sumo Logic HTTP Logs Source Category Name (`Section3cGuardDutyHttpLogsSourceCategoryName`)	-	Required when Flag = No. Provide an existing source category name from Sumo Logic collecting GuardDuty Logs. Used for app installation.

Sumo Logic VPC Flow Logs Apps Configuration:

- For this app
  - Select the VPC apps you need to install: Amazon VPC Flow Logs, PCI Compliance for Amazon VPC Flow Logs apps.
  - If you already have an S3 bucket where VPC Flow logs are being stored, skip the creation of the bucket
    - If you don’t have an AWS S3 Source configured in Sumo Logic, provide the existing bucket name, along with path expression to automatically create this source in Sumo Logic.
  - If you already have Sumo Logic S3 source for VPC Flow, provide its source category when asked,

Parameter label (name)	Default	Description
Install Sumo Logic Amazon VPC Flow Logs Apps (`Section4aInstallVpcApps`)	Both	VPC -> Install Amazon VPC Flow Logs App in Sumo Logic for AWS Quick Start Solution. PCI_VPC -> Install PCI Compliance For Amazon VPC Flow App in Sumo Logic for AWS Quick Start Solution. Both -> Install Both the apps. Skip -> Skip Installation of the apps.
Create AWS S3 Bucket (`Section4bVpcCreateBucket`)	Yes	Yes – Create a new S3 bucket in AWS S3. No – Use an existing S3 bucket from AWS S3 which has VPC Logs.

Parameter label (name)	Default	Description
AWS S3 Bucket Name (`Section4cVpcLogsBucketName`)	-	Required when Flag = No. Provide an Existing bucket name which has VPC Flow logs.
Create Sumo Logic Amazon S3 Logs Source (`Section4dVpcCreateS3Source`)	Yes	Yes – Create Sumo Logic Amazon S3 Log Source with provided bucket Name. No – Skip creation of the Sumo Logic Amazon S3 Log Source.
Path Expression for the logs (`Section4eVpcBucketPathExpression`)	VPC-FLOW-LOGS/*	Path expression to match the folder structure for VPC Flow logs. For Eg:- VPC-FLOW-LOGS/*.
Sumo Logic Amazon S3 Logs Source Category Name (`Section4fVpcLogsSourceCategoryName`)	-	Required when Flag = No. Provide an existing source category name from Sumo Logic collecting VPC Flow Logs. Used for Threat Intel for AWS app installation also.

Sumo Logic Threat Intel for AWS Configurations:

Threat Intel		**- Keep Classic Elastic Load Balancer source category ready.**
Parameter label (name)	**Default**	**Description**
Install Sumo Logic Threat Intel for AWS App (`Section5aInstallThreatIntelApp`)	Yes	Yes -> Install Sumo Logic Threat Intel for AWS app in Sumo Logic for AWS Quick Start Solution. No -> Skip Installation of the app.
Sumo Logic Amazon Elastic Load Balancer Classic Category Name (`Section5bElasticLoadBalancerSourceCategory`)	-	Provide an existing Source Category from Sumo Logic with Elastic Load Balancer Classic Logs.

Sumo Logic Amazon S3 Audit app Configuration:

- For this app
  - Select the S3 Audit app.
  - If you already have an S3 bucket where S3 Audit logs are being stored, skip the creation of the bucket
    - If you don't have an AWS S3 Source configured in Sumo Logic, provide the existing bucket name, along with path expression to automatically create this source in Sumo Logic.
  - If you already have Sumo Logic S3 source, provide the source category

Parameter label (name)	Default	Description
Install Sumo Logic Amazon S3 Audit app (`Section6aInstallS3AuditApp`)	Yes	Yes -> Install Sumo Logic Amazon S3 Audit App in Sumo Logic for AWS Quick Start Solution. No -> Skip Installation of the app.
Create AWS S3 Bucket (`Section6bS3AuditCreateBucket`)	Yes	Yes – Create a new bucket in AWS S3. No – Use an existing bucket from AWS S3 which has S3 Audit Logs.
AWS S3 Bucket Name (`Section6cS3AuditLogsBucketName`)	-	Required when Flag = No. Provide an Existing bucket name which has S3 Audit logs.
Create Sumo Logic Amazon S3 Audit Logs Source (`Section6dS3AuditCreateS3Source`)	Yes	Yes – Create Sumo Logic S3 Audit Log Source with provided bucket Name. No – Skip creation of the Sumo Logic S3 Audit Log Source.
Path Expression for the logs (`Section6eS3AuditBucketPathExpression`)	S3-AUDIT-LOGS/*	Path expression to match the folder structure for S3 Audit logs. For Eg:- S3-AUDIT-LOGS/*
Sumo Logic Amazon S3 Audit Logs Source Category Name (`Section6fS3AuditLogsSourceCategoryName`)	-	Required when Flag = No. Provide an existing source category name from Sumo Logic collecting S3 Audit Logs. Used for app installation.

Sumo Logic AWS Security Hub app Configuration:

- Security Hub App
  - Select the Security Hub app. Also, select if you need to enable security hub for your account.
  - If you already have an S3 bucket where Security Hub logs are being stored, skip creation of bucket.
    - If you don't have an AWS S3 Source configured in Sumo Logic, provide the existing bucket name, along with path expression to automatically create this source in Sumo Logic.
  - If you already have Sumo Logic S3 source, provide the source category for App install.

Parameter label (name)	Default	Description
Install Sumo Logic AWS Security Hub app (`Section7aInstallSecurityHubAuditApp`)	Yes	Yes -> Install Sumo Logic AWS Security Hub App in Sumo Logic for AWS Quick Start Solution. No -> Skip Installation of the app.
Enable Security Hub for the Region (`Section7bEnableSecurityHub`)	No	Select Yes if security hub needs to be enabled for the region else no.

Parameter label (name)	Default	Description
Create AWS S3 Bucket (`Section7cSecurityHubCreateBucket`)	Yes	Yes – Create a new bucket in AWS S3. No – Use an existing bucket from AWS S3 which has Security Hub Logs.
AWS S3 Bucket Name (`Section7dSecurityHubLogsBucketName`)	-	Required when Flag = No. Provide an Existing bucket name which has Security Hub logs.
Create Sumo Logic Amazon S3 Logs Source (`Section7eSecurityHubCreateS3Source`)	Yes	Yes – Create Sumo Logic S3 Log Source with provided bucket Name. No – Skip creation of the Sumo Logic S3 Log Source.
Path Expression for the logs (`Section7fSecurityHubBucketPathExpression`)	*securityhub*/*	Path expression to match the folder structure for Security Hub logs. For Eg:- *securityhub*/*
Sumo Logic Amazon S3 Logs Source Category Name (`Section7gSecurityHubLogsSourceCategoryName`)	-	Required when Flag = No. Provide an existing source category name from Sumo Logic collecting Security Hub Logs. Used for app installation.

Sumo Logic AWS WAF app Configuration:

- For this app
  - Select the WAF app. Also, select if you need to create a Kinesis delivery stream to send WAF logs to an S3 bucket.
  - If you already have an AWS S3 bucket where AWS WAF logs are being stored, skip the creation of a bucket.
    - If you don't have an AWS S3 Source configured in Sumo Logic, provide the existing bucket name, along with path expression to automatically create this source in Sumo Logic.
  - If you already have Sumo Logic S3 source that is collecting AWS WAF logs, provide the source category

Parameter label (name)	Default	Description
Install Sumo Logic AWS WAF app (`Section8aInstallWafApp`)	Yes	Yes -> Install Sumo Logic AWS WAF App in Sumo Logic for AWS Quick Start Solution. No -> Skip Installation of the app.
Create a Delivery Stream for the Bucket (`Section8bCreateDeliveryStream`)	Yes	Yes – to create Kinesis Delivery Stream with provided bucket Name. No – to skip creation Kinesis Delivery Stream.
Create AWS S3 Bucket (`Section8cWafCreateBucket`)	Yes	Yes – Create a new bucket in AWS S3. No – Use an existing bucket from AWS S3 which has AWS WAF Logs.

Parameter label (name)	Default	Description
AWS S3 Bucket Name (`Section8dWafLogsBucketName`)	-	Required when Flag = No. Provide an Existing bucket name which has AWS WAF logs.
Create Sumo Logic Amazon S3 Logs Source (`Section8eWafCreateS3Source`)	Yes	Yes – Create Sumo Logic S3 Log Source with provided bucket Name. No – Skip creation of the Sumo Logic S3 Log Source.
Path Expression for the logs (`Section8fWafBucketPathExpression`)	WAF_LOGS/*	Path expression to match the folder structure for WAF logs. For Eg:- WAF_LOGS/*
Sumo Logic Amazon S3 Logs Source Category Name (`Section8gWafLogsSourceCategoryName`)	-	Required when Flag = No. Provide an existing source category name from Sumo Logic collecting WAF Logs. Used for app installation.

Sumo Logic AWS Config app Configuration:

- Config App
  - Select the Config app.
  - Select If you need to enable Config (will create a bucket).
    - If Config is already enabled, select if you need to create SNS topic to deliver logs.
      - If logs are already getting delivered to an SNS topic, provide the SNS Topic Name to automatically create a HTTP Source.
  - If you already have Sumo Logic HTTP source that's collecting AWS Config logs, enter in its source category when asked.

Parameter label (name)	Default	Description
Install Sumo Logic AWS Config app (`Section9aInstallConfigApp`)	Yes	Yes -> Install Sumo Logic AWS Config App in Sumo Logic for AWS Quick Start Solution. No -> Skip Installation of the app.
Enable AWS Config for the region (`Section9bConfigEnableConfig`)	Yes	Choose Yes to enable config for the region. Choose No if config is already enabled.
Create SNS Topic for logs delivery (`Section9cConfigCreateSNSTopic`)	Yes	Choose Yes to create SNS Topic and attach the SNS topic to AWS Config setting to deliver the logs. Choose No if config logs are already delivered to an existing SNS topic.

Parameter label (name)	Default	Description
Existing Topic Name where logs are delivered (`Section9dConfigExistingTopicName`)	-	Required when flag -> No. Provide existing config SNS topic from Config settings to stream configuration changes and notifications.
Create Sumo Logic HTTP Logs Source (`Section9eConfigCreateHttpLogsSource`)	Yes	Yes – Create Sumo Logic HTTP Log Source to collect Config Logs. No – Skip creation of the Sumo Logic HTTP Log Source.
Sumo Logic Amazon HTTP Logs Source Category Name (`Section9fConfigHttpLogsSourceCategoryName`)	-	Required when Flag = No. Provide an existing source category name from Sumo Logic collecting Config Logs. Used for app installation.

Auto Enable Logging Configuration:

For this section:

- Select the AWS services, for which you need to enable automatically enable logging for new resources.
- Select if you need to enable logging for already existing resources.
- For S3 and VPC,
    - Provide the filter expression and Bucket prefix.

Parameter label (name)	Default	Description
Choose resource to Auto Enable S3 logging (`Section91aEnableAutoLogging`)	S3_VPC	S3 – To Enable S3 Audit Logging for new S3 buckets. VPC – To Enable VPC flow logs for new VPC, Subnets and Network Interfaces. S3_VPC – to enable logging for both.
Auto Enable logging for Existing AWS resources (`Section91bEnableLoggingForExistingResources`)	Yes	Yes – Enable Logging for existing resources. No – Skip Existing resources.
Bucket Prefix to store S3 Audit logs (`Section91cS3LoggingBucketPrefix`)	S3_AUDIT_LOGS/	Provide an bucket prefix for S3 Audit logs. It Should have / in the end.
Regex expression to Filter AWS S3 Buckets	-	Provide regular expression for matching S3 Buckets. For eg;- ‘test|prod’

Parameter label (name)	Default	Description
(`Section91dS3LoggingFilterExpression`)		
Bucket Prefix to store VPC Flow logs (`Section91eVPCLoggingBucketPrefix`)	VPC_LOGS/	Provide an bucket prefix VPC Flow logs. It Should have / in the end.
Regex expression to Filter AWS VPC Resources (`Section91fVPCLoggingFilterExpression`)	-	Provide regular expression for matching VPC resources. For eg;- ‘VpcId’: ‘t1.micro.*?’|’NetworkInterfaceId’: ‘Test.*?’]|’SubnetId’: ‘prod.*?’|test|prod’

AWS Quick Start configuration:

> **Note:** We recommend that you keep the default settings for the following three parameters, unless you are customizing the Quick Start templates for your own deployment projects. Changing the settings of these parameters automatically updates code references to point to a new Quick Start location. For additional details, see the AWS Quick Start Contributor’s Guide.

Parameter label (name)	Default	Description
Quick Start S3 bucket name (`QSS3BucketName`)	aws-quickstart	The S3 bucket you created for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. The bucket name can include numbers, lowercase letters, uppercase letters, and hyphens, but should not start or end with a hyphen.
Quick Start S3 key prefix (`QSS3KeyPrefix`)	quickstart-sumo-logic-log-centralization/	The S3 key name prefix used to simulate a folder for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. This prefix can include numbers, lowercase letters, uppercase letters, hyphens, and forward slashes.
Quick Start S3 bucket region (`QSS3BucketRegion`)	us-east-1	The AWS Region where the Quick Start S3 bucket (QSS3BucketName) is hosted. When using your own bucket, you must specify this value.

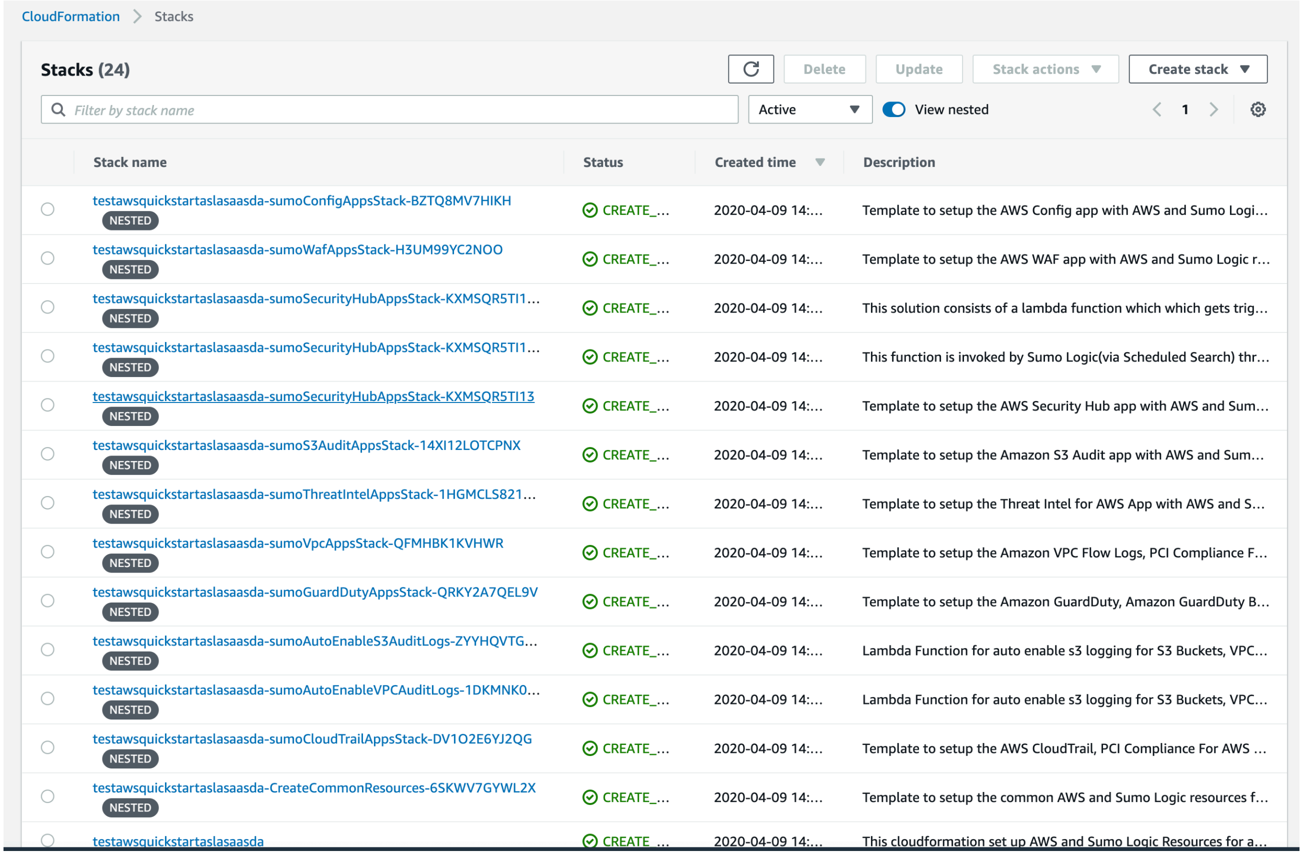
5. On the options page, you can specify tags (key-value pairs) for resources in your stack and set advanced options. When you’re done, choose **Next**.

6. On the **Review** page, review and confirm the template settings. Under **Capabilities**, select the two check boxes to acknowledge that the template creates IAM resources and might require the capability to auto-expand macros.
7. Choose **Create stack** to deploy the stack.
8. Monitor the status of the stack. When the status is **CREATE_COMPLETE**, the Sumo Logic App stack is ready.

Step 4. Test the deployment

IN YOUR AWS ACCOUNT

After the deployment has completed, you will see the main stack, QuickStartApps, as well as multiple nested stacks.

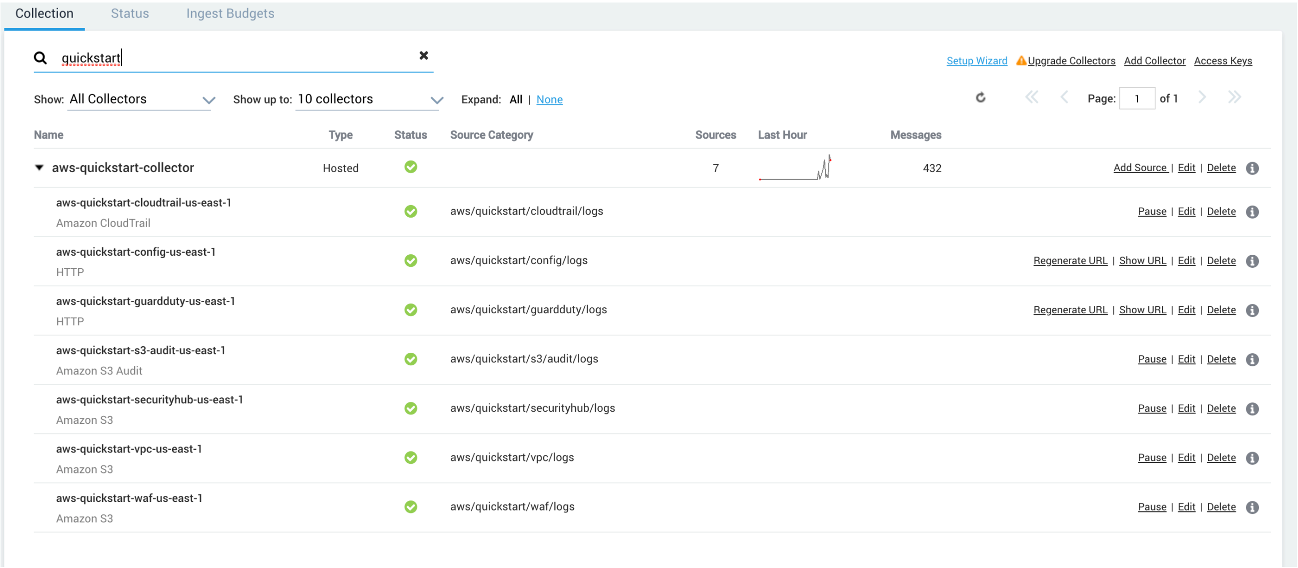


	Stack name	Status	Created time ▼	Description
○	testawsquickstartaslasaasda-sumoConfigAppsStack-BZTQ8MV7HIKH NESTED	✓ CREATE_...	2020-04-09 14:...	Template to setup the AWS Config app with AWS and Sumo Logi...
○	testawsquickstartaslasaasda-sumoWafAppsStack-H3UM99YC2NOO NESTED	✓ CREATE_...	2020-04-09 14:...	Template to setup the AWS WAF app with AWS and Sumo Logic r...
○	testawsquickstartaslasaasda-sumoSecurityHubAppsStack-KXMSQR5TI1... NESTED	✓ CREATE_...	2020-04-09 14:...	This solution consists of a lambda function which which gets trig...
○	testawsquickstartaslasaasda-sumoSecurityHubAppsStack-KXMSQR5TI1... NESTED	✓ CREATE_...	2020-04-09 14:...	This function is invoked by Sumo Logic(via Scheduled Search) thr...
○	testawsquickstartaslasaasda-sumoSecurityHubAppsStack-KXMSQR5TI13 NESTED	✓ CREATE_...	2020-04-09 14:...	Template to setup the AWS Security Hub app with AWS and Sum...
○	testawsquickstartaslasaasda-sumoS3AuditAppsStack-14XI12LOTCPNX NESTED	✓ CREATE_...	2020-04-09 14:...	Template to setup the Amazon S3 Audit app with AWS and Sum...
○	testawsquickstartaslasaasda-sumoThreatIntelAppsStack-1HGMCLS821... NESTED	✓ CREATE_...	2020-04-09 14:...	Template to setup the Threat Intel for AWS App with AWS and S...
○	testawsquickstartaslasaasda-sumoVpcAppsStack-QFMHBK1KVHWR NESTED	✓ CREATE_...	2020-04-09 14:...	Template to setup the Amazon VPC Flow Logs, PCI Compliance F...
○	testawsquickstartaslasaasda-sumoGuardDutyAppsStack-QRKY2A7QEL9V NESTED	✓ CREATE_...	2020-04-09 14:...	Template to setup the Amazon GuardDuty, Amazon GuardDuty B...
○	testawsquickstartaslasaasda-sumoAutoEnableS3AuditLogs-ZYYHQVTG... NESTED	✓ CREATE_...	2020-04-09 14:...	Lambda Function for auto enable s3 logging for S3 Buckets, VPC...
○	testawsquickstartaslasaasda-sumoAutoEnableVPCAuditLogs-1DKMNK0... NESTED	✓ CREATE_...	2020-04-09 14:...	Lambda Function for auto enable s3 logging for S3 Buckets, VPC...
○	testawsquickstartaslasaasda-sumoCloudTrailAppsStack-DV1O2E6YJ2QG NESTED	✓ CREATE_...	2020-04-09 14:...	Template to setup the AWS CloudTrail, PCI Compliance For AWS ...
○	testawsquickstartaslasaasda-CreateCommonResources-6SKWV7GYWL2X NESTED	✓ CREATE_...	2020-04-09 14:...	Template to setup the common AWS and Sumo Logic resources f...
○	testawsquickstartaslasaasda	✓ CREATE_...	2020-04-09 14:...	This cloudformation set up AWS and Sumo Logic Resources for a...

Figure 2: Resources created

IN YOUR SUMO LOGIC ACCOUNT

Confirm that the AWS CloudFormation template has installed the collectors and sources for the Sumo Logic applications that you selected.



quickstart

Show: All Collectors Show up to: 10 collectors Expand: All | None

Page: 1 of 1

Name	Type	Status	Source Category	Sources	Last Hour	Messages	
aws-quickstart-collector	Hosted	✓		7		432	Add Source | Edit | Delete
aws-quickstart-cloudtrail-us-east-1 Amazon CloudTrail		✓	aws/quickstart/cloudtrail/logs				Pause | Edit | Delete
aws-quickstart-config-us-east-1 HTTP		✓	aws/quickstart/config/logs				Regenerate URL | Show URL | Edit | Delete
aws-quickstart-guardduty-us-east-1 HTTP		✓	aws/quickstart/guardduty/logs				Regenerate URL | Show URL | Edit | Delete
aws-quickstart-s3-audit-us-east-1 Amazon S3 Audit		✓	aws/quickstart/s3/audit/logs				Pause | Edit | Delete
aws-quickstart-securityhub-us-east-1 Amazon S3		✓	aws/quickstart/securityhub/logs				Pause | Edit | Delete
aws-quickstart-vpc-us-east-1 Amazon S3		✓	aws/quickstart/vpc/logs				Pause | Edit | Delete
aws-quickstart-waf-us-east-1 Amazon S3		✓	aws/quickstart/waf/logs				Pause | Edit | Delete

Figure 3: Created collectors and sources

Step 5. Post-deployment steps

Using Existing S3 Bucket

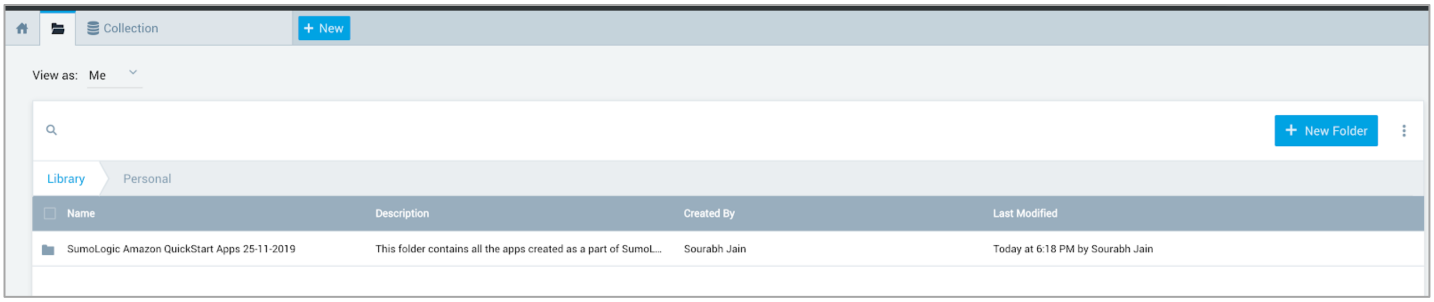
In case, you are existing buckets with logs we create a SNS topic (SumoSNSTopic-{StackName}) that is subscribed to Sumo Logic sources. Once the deployment is complete, you can add that SNS topic to S3 Bucket events.

WAF LOGS TO KINESIS STREAM

If you install WAF app, CloudFormation create a Kinesis Delivery stream (QuickStartDeliveryStream{Region}) in your kinesis configuration. You have to configure Web ACL in your WAF configuration to send the logs to the created Delivery stream. Process to send Web ACL to kinesis stream is mentioned here.

Step 6. View the Sumo Logic App dashboards

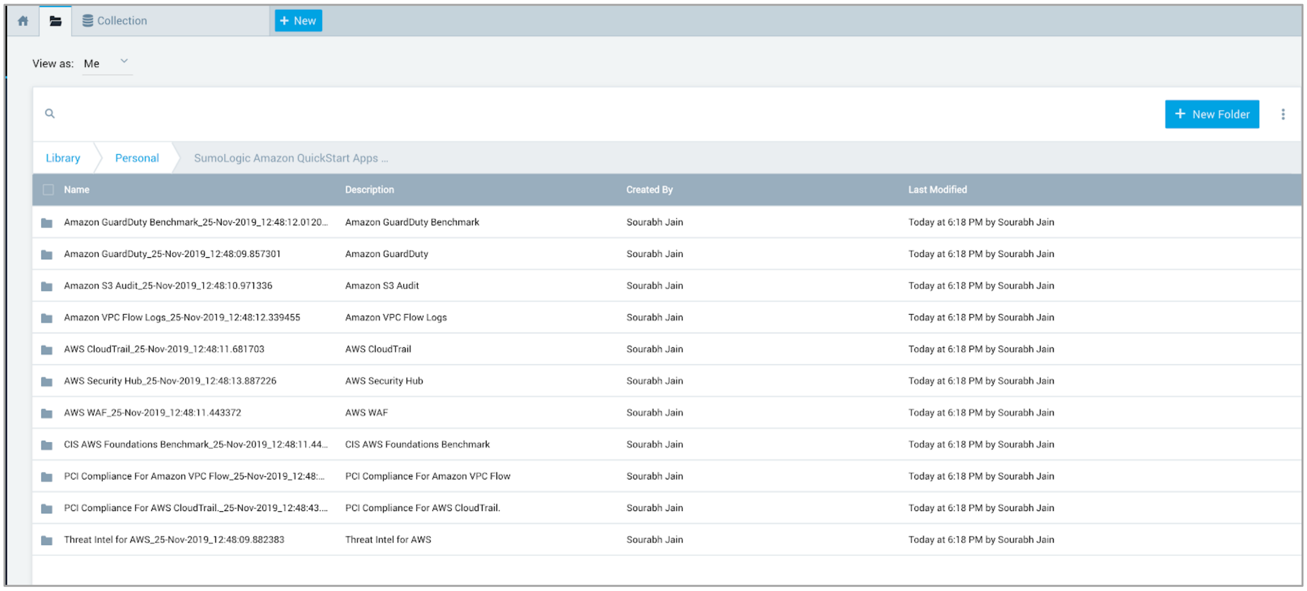
After the Quick Start has been run, the Sumo Logic apps will be added to your Sumo Logic personal account library in a folder named `SumoLogic Amazon QuickStart Apps <date>`.



Name	Description	Created By	Last Modified
SumoLogic Amazon QuickStart Apps 25-11-2019	This folder contains all the apps created as a part of SumoL...	Sourabh Jain	Today at 6:18 PM by Sourabh Jain

Figure 4: Top-level Quick Start apps folder

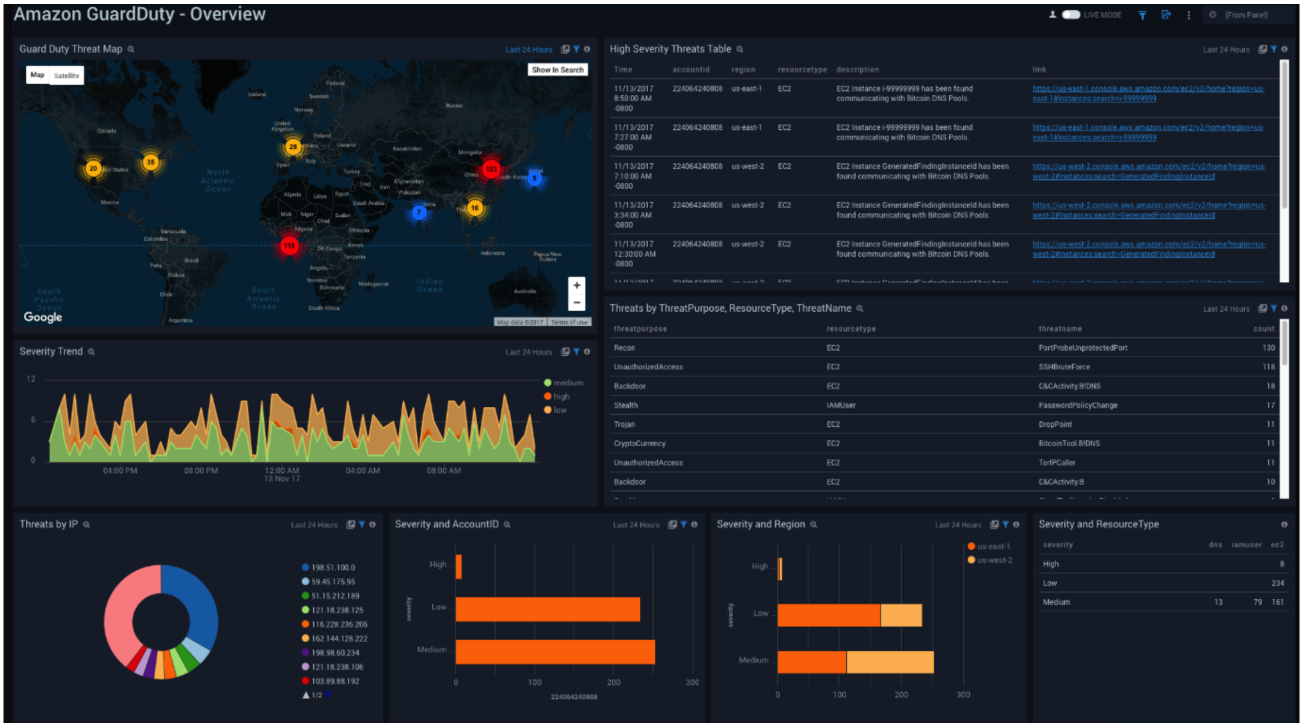
Under the `SumoLogic Amazon QuickStart Apps <date>` folder, you will see sub-folders that represent each app, along with the date and timestamp .



Name	Description	Created By	Last Modified
Amazon GuardDuty Benchmark_25-Nov-2019_12:48:12.0120...	Amazon GuardDuty Benchmark	Sourabh Jain	Today at 6:18 PM by Sourabh Jain
Amazon GuardDuty_25-Nov-2019_12:48:09.857301	Amazon GuardDuty	Sourabh Jain	Today at 6:18 PM by Sourabh Jain
Amazon S3 Audit_25-Nov-2019_12:48:10.971336	Amazon S3 Audit	Sourabh Jain	Today at 6:18 PM by Sourabh Jain
Amazon VPC Flow Logs_25-Nov-2019_12:48:12.339455	Amazon VPC Flow Logs	Sourabh Jain	Today at 6:18 PM by Sourabh Jain
AWS CloudTrail_25-Nov-2019_12:48:11.681703	AWS CloudTrail	Sourabh Jain	Today at 6:18 PM by Sourabh Jain
AWS Security Hub_25-Nov-2019_12:48:13.887226	AWS Security Hub	Sourabh Jain	Today at 6:18 PM by Sourabh Jain
AWS WAF_25-Nov-2019_12:48:11.443372	AWS WAF	Sourabh Jain	Today at 6:18 PM by Sourabh Jain
CIS AWS Foundations Benchmark_25-Nov-2019_12:48:11.44...	CIS AWS Foundations Benchmark	Sourabh Jain	Today at 6:18 PM by Sourabh Jain
PCI Compliance For Amazon VPC Flow_25-Nov-2019_12:48:...	PCI Compliance For Amazon VPC Flow	Sourabh Jain	Today at 6:18 PM by Sourabh Jain
PCI Compliance For AWS CloudTrail._25-Nov-2019_12:48:43....	PCI Compliance For AWS CloudTrail.	Sourabh Jain	Today at 6:18 PM by Sourabh Jain
Threat Intel for AWS_25-Nov-2019_12:48:09.882383	Threat Intel for AWS	Sourabh Jain	Today at 6:18 PM by Sourabh Jain

Figure 5: Individual app folders

To open an app's dashboard, choose its app folder in the Sumo Logic console. For instance, under the Amazon GuardDuty app folder, you can open up the **Amazon GuardDuty – Overview** dashboard to get insight into all threats detected by GuardDuty.



High Severity Threats Table

Last 24 Hours

Time	accountid	region	resourcetype	description	link
11/13/2017 8:50:00 AM -0800	224064240808	us-east-1	EC2	EC2 Instance i-99999999 has been found communicating with Bitcoin DNS Pools.	https://us-east-1.console.aws.amazon.com/ec2/v2/home?region=us-east-1#Instances:search=i-99999999
11/13/2017 7:27:00 AM -0800	224064240808	us-east-1	EC2	EC2 Instance i-99999999 has been found communicating with Bitcoin DNS Pools.	https://us-east-1.console.aws.amazon.com/ec2/v2/home?region=us-east-1#Instances:search=i-99999999
11/13/2017 7:10:00 AM -0800	224064240808	us-west-2	EC2	EC2 Instance GeneratedFindingInstanceId has been found communicating with Bitcoin DNS Pools.	https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#Instances:search=GeneratedFindingInstanceId
11/13/2017 3:34:00 AM -0800	224064240808	us-west-2	EC2	EC2 Instance GeneratedFindingInstanceId has been found communicating with Bitcoin DNS Pools.	https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#Instances:search=GeneratedFindingInstanceId
11/13/2017 12:30:00 AM -0800	224064240808	us-west-2	EC2	EC2 Instance GeneratedFindingInstanceId has been found communicating with Bitcoin DNS Pools.	https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#Instances:search=GeneratedFindingInstanceId

Threats by ThreatPurpose, ResourceType, ThreatName

Last 24 Hours

threatpurpose	resourcetype	threatname	count
Recon	EC2	PortProbeUnprotectedPort	130
UnauthorizedAccess	EC2	SSHBruteForce	118
Backdoor	EC2	C&CActivity.B!DNS	18
Stealth	IAMUser	PasswordPolicyChange	17
Trojan	EC2	DropPoint	11
CryptoCurrency	EC2	BitcoinTool.B!DNS	11
UnauthorizedAccess	EC2	TorIPCaller	11
Backdoor	EC2	C&CActivity.B	10

Severity and ResourceType

severity	dns	iamuser	ec2
High			8
Low			234
Medium	13	79	161

Figure 6: Dashboard from the Amazon GuardDuty app

Best practices for using Sumo Logic Security Integrations on AWS

To use this Quick Start across multiple AWS accounts and Regions, at the end of each deployment, rename the top-level parent folder in your Sumo Logic account (created under your Personal folder) to reflect the correct account and Region.

Security

For each S3 bucket, follow the AWS documentation best practices to secure all the objects in the bucket.

By using Sumo Logic Security Integrations for AWS, you will now be able to monitor the following security and compliance aspects of your AWS environment:

- Threat monitoring and other security findings
- Configuration and audit
- PCI DSS compliance
- CIS AWS Foundations compliance

FAQ

Q. I encountered a **CREATE_FAILED** error when I launched the Quick Start.

A. If AWS CloudFormation fails to create the stack, we recommend that you relaunch the template with **Rollback on failure** set to **No**. (This setting is under **Advanced** in the AWS CloudFormation console, **Options** page.) With this setting, the stack's state is retained and the instance is left running, so you can troubleshoot the issue. (For Windows, look at the log files in `%ProgramFiles%\Amazon\EC2ConfigService` and `C:\cfn\log`.)

> **Important:** When you set **Rollback on failure** to **No**, you continue to incur AWS charges for this stack. Please make sure to delete the stack when you finish troubleshooting.

For additional information, see Troubleshooting AWS CloudFormation on the AWS website.

Q. I encountered a size limitation error when I deployed the AWS CloudFormation templates.

A. We recommend that you launch the Quick Start templates from the links in this guide or from another S3 bucket. If you deploy the templates from a local copy on your computer or from a non-S3 location, you might encounter template size limitations. For more information about AWS CloudFormation quotas, see the AWS documentation.

Send us feedback

To post feedback, submit feature ideas, or report bugs, use the **Issues** section of the GitHub repository for this Quick Start. If you'd like to submit code, please review the Quick Start Contributor's Guide.

Additional resources

AWS resources

- Getting Started Resource Center
- AWS General Reference
- AWS Glossary

AWS services used by the deployment

- AWS CloudFormation

- AWS CloudWatch
- AWS IAM
- Amazon SNS
- AWS Lambda
- Amazon Kinesis Firehose
- Amazon S3

Sumo Logic documentation

- Sumo Logic Amazon and AWS apps
- Sumo Logic Doc Hub
- Sumo Logic Cloud SIEM

Other Quick Start reference deployments

- AWS Quick Start home page

Document revisions

Date	Change	In sections
March 2020	Initial publication	—

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.