Sumo Logic Security Integrations on the AWS Cloud

Quick Start Reference Deployment

May 2020

Sumo Logic

Shivansh Singh, AWS Quick Start team

Visit our [GitHub repository](https://fwd.aws/KEvGk) for source files and to post feedback,   
report bugs, or submit feature ideas for this Quick Start.

# Contents

[Contents 1](#_Toc41983688)

[Overview 2](#_Toc41983689)

[Sumo Logic on AWS 3](#_Toc41983690)

[Cost and licenses 3](#_Toc41983691)

[Architecture 4](#_Toc41983692)

[Planning the deployment 5](#_Toc41983693)

[Specialized knowledge 5](#_Toc41983694)

[Scenarios supported by this Quick Start 6](#_Toc41983695)

[AWS account 6](#_Toc41983696)

[Technical requirements 6](#_Toc41983697)

[Deployment steps 8](#_Toc41983698)

[Step 1. Prepare your Sumo Logic account 8](#_Toc41983699)

[Step 2. Sign in to your AWS account 8](#_Toc41983700)

[Step 3. Launch the Quick Start 8](#_Toc41983701)

[Parameters for deploying the Sumo Logic Quick Start 9](#_Toc41983702)

[Step 4. Test the deployment 16](#_Toc41983703)

[AWS account 16](#_Toc41983704)

[Sumo Logic account 16](#_Toc41983705)

[Step 5. Post-deployment steps 17](#_Toc41983706)

[Using existing S3 bucket 17](#_Toc41983707)

[Step 6. View the Sumo Logic dashboards 17](#_Toc41983708)

[Best practices for using Sumo Logic Security Integrations 19](#_Toc41983709)

[FAQ 20](#_Toc41983710)

[Send us feedback 20](#_Toc41983711)

[Additional resources 20](#_Toc41983712)

[Document revisions 21](#_Toc41983713)

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

[Quick Starts](http://aws.amazon.com/quickstart/) are automated reference deployments that use AWS CloudFormation templates to deploy key technologies on AWS, following AWS best practices.

# Overview

Sumo Logic is focused on continuous intelligence, a new category of software that addresses data challenges presented by digital transformations, modern applications, and cloud computing. The Sumo Logic Continuous Intelligence Platform automates the collection, ingestion, and analysis of applications, infrastructure, security, and Internet of Things (IoT) data to derive actionable insights.

Similar to security information and event management (SIEM) software, Sumo Logic uses apps to collet security events generated by AWS and other security services to provide an aggregate view of overall security and compliance posture. A Sumo Logic app is a collection of dashboards in the Sumo Logic console that provide analytics for known data streams. In minutes, users can start monitoring and troubleshooting security threats and indicators of compromise.

Please know that we may share who uses AWS Quick Starts with the AWS Partner Network (APN) Partner that collaborated with AWS on the content of the Quick Start.

## Sumo Logic on AWS

Sumo Logic has apps for each AWS security service (for example, the Sumo Logic app for AWS CloudTrail) that it supports as well as apps that support multiple AWS services (for example, Threat Intel for AWS). This Quick Start deployment is for users who want to set up and configure the Sumo Logic console for 12 AWS services that provide security analytics.

Sumo Logic customers can track user activity, monitor threats, and understand how security posture compares with global benchmarks. This deployment uses virtual private cloud (VPC) flow logs and a web application firewall (AWS WAF) to monitor traffic patterns. Sumo Logic also uses apps to audit and maintain compliance of the Payment Card Industry (PCI) Data Security Standard (DSS) and Center for Internet Security (CIS).

The included template automatically creates resources that use various AWS services to collect logs, which are sent to your preregistered Sumo Logic account.

## 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 use. Prices are subject to change.

**Tip:** After you deploy the Quick Start, we recommend that you enable the [AWS Cost and Usage Report](https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-reports-gettingstarted-turnonreports.html). 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](https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-reports-costusage.html).

For [pricing information](https://www.sumologic.com/pricing/), 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.

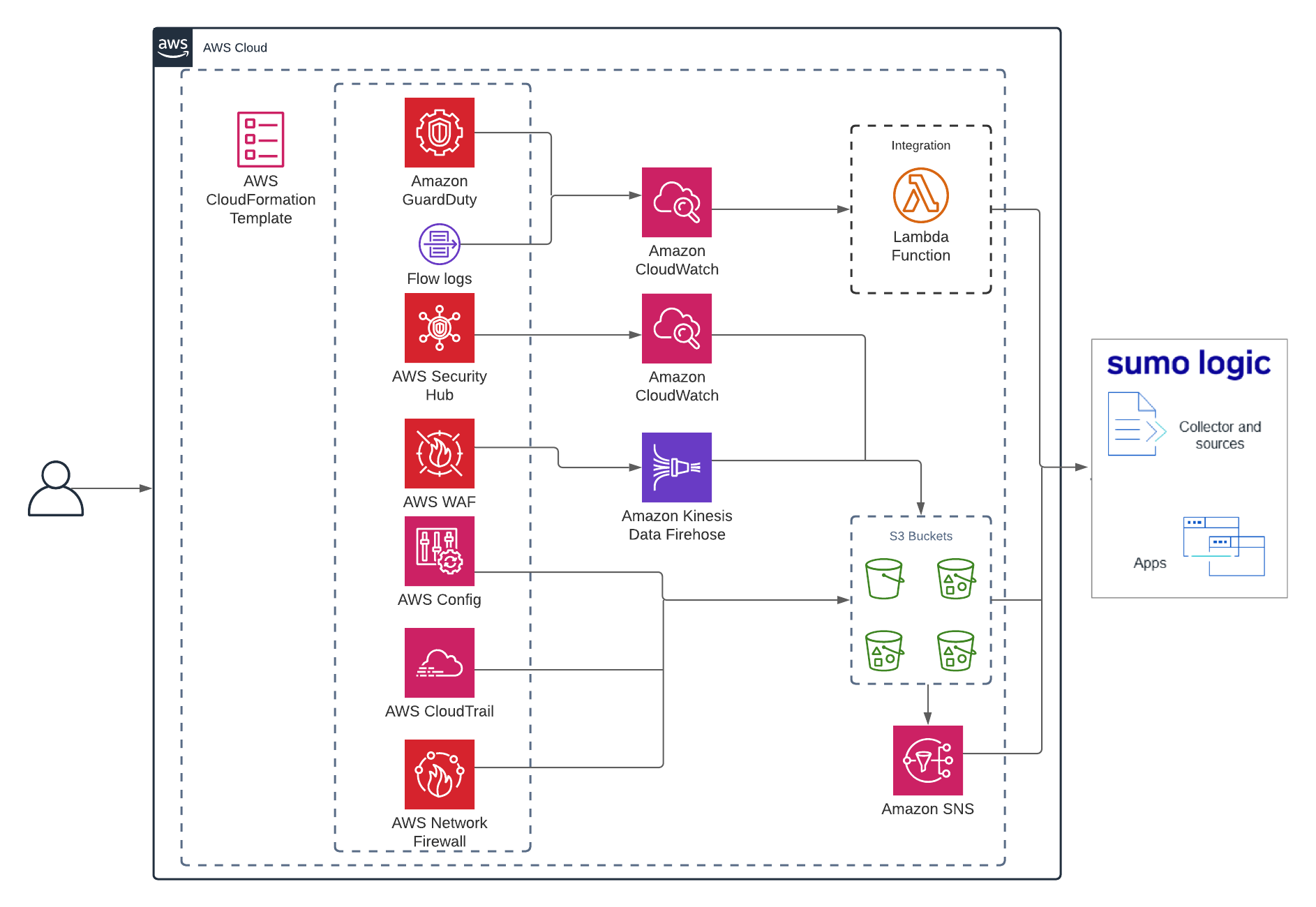


Figure 1: Quick Start architecture for Sumo Logic on AWS

This Quick Start sets up the following architecture:

* Amazon GuardDuty to detect malicious activity and behavior to protect AWS accounts and workloads
* Amazon VPC Flow Logs to capture information about IP traffic going to and from network interfaces in your VPC
* AWS Security Hub to assess security alerts and security posture across AWS accounts
* AWS WAF to protect your web applications from common web exploits
* AWS Config to record and evaluate configurations of your AWS resources
* AWS CloudTrail to track user activity and API usage
* AWS Network Firewall to deploy essential network protections for all of your Amazon Virtual Private Clouds (VPCs)
* Multiple CloudFormation stacks are deployed in your environment to setup forwarding of data to Sumo Logic. Each stack consists of more than one AWS resource, including AWS S3 buckets, AWS Lambda functions, and Amazon Kinesis Data Firehose delivery streams.
* AWS Lambda functions to create a collector and multiple sources, and to install apps on your Sumo Logic account.
* AWS S3 buckets capture logs from the various AWS services.
* The Sumo Logic collector and sources to receive logs from the S3 buckets.
* Amazon Kinesis Data Firehose delivery streams to transfer 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 Sumo Logic as well as the following AWS services. If you are new to AWS, see [Getting Started with AWS](https://aws.amazon.com/getting-started/). If you are new to Sumo Logic, see [Getting Started with Sumo Logic](https://help.sumologic.com/01Start-Here/04Getting-Started).

The following table shows how various AWS security services map to the corresponding apps in Sumo Logic. We recommend you get familiar with them.

|  |  |
| --- | --- |
| AWS security service or feature | Sumo Logic apps for the following AWS services or features |
| [AWS CloudTrail](https://aws.amazon.com/cloudtrail/) | [AWS CloudTrail](https://help.sumologic.com/07Sumo-Logic-Apps/01Amazon_and_AWS/AWS_CloudTrail), [PCI DSS compliance for AWS CloudTrail,](https://help.sumologic.com/07Sumo-Logic-Apps/01Amazon_and_AWS/PCI_Compliance_for_AWS_CloudTrail_App) [CIS AWS foundations benchmark](https://help.sumologic.com/07Sumo-Logic-Apps/01Amazon_and_AWS/CIS_AWS_Foundations_Benchmark_App), [Amazon CloudTrail - Sumo Cloud Security Monitoring and Analytics](https://help.sumologic.com/07Sumo-Logic-Apps/Cloud_Security_Monitoring_and_Analytics/Amazon_CloudTrail_-_Cloud_Security_Monitoring_and_Analytics), [Sumo Global Intelligence for AWS CloudTrail SecOps App](https://help.sumologic.com/07Sumo-Logic-Apps/01Amazon_and_AWS/Global_Intelligence_for_AWS_CloudTrail) |
| [Amazon GuardDuty](https://aws.amazon.com/guardduty/) | [Amazon GuardDuty](https://help.sumologic.com/07Sumo-Logic-Apps/01Amazon_and_AWS/Amazon_GuardDuty), [Global Intelligence for Amazon GuardDuty](https://help.sumologic.com/07Sumo-Logic-Apps/01Amazon_and_AWS/Global_Intelligence_for_Amazon_GuardDuty) |
| [Amazon VPC flow logs](https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html) | [Amazon VPC flow logs](https://help.sumologic.com/07Sumo-Logic-Apps/01Amazon_and_AWS/Amazon_VPC_Flow_Logs), [PCI DSS compliance for Amazon VPC flow logs,](https://help.sumologic.com/07Sumo-Logic-Apps/01Amazon_and_AWS/PCI_Compliance_for_Amazon_VPC_Flow_Logs) [Threat Intel for AWS](https://help.sumologic.com/07Sumo-Logic-Apps/01Amazon_and_AWS/Threat_Intel_for_AWS), [Amazon VPC Flow - Sumo Cloud Security Monitoring and Analytics](https://help.sumologic.com/07Sumo-Logic-Apps/Cloud_Security_Monitoring_and_Analytics/Amazon_VPC_Flow_-_Cloud_Security_Monitoring_and_Analytics) |
| [Amazon S3 access logging](https://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLogs.html) | [S3 audit](https://help.sumologic.com/07Sumo-Logic-Apps/01Amazon_and_AWS/Amazon_S3_Audit) |
| [AWS Security Hub](https://aws.amazon.com/security-hub/?aws-security-hub-blogs.sort-by=item.additionalFields.createdDate&aws-security-hub-blogs.sort-order=desc) | [AWS Security Hub](https://help.sumologic.com/07Sumo-Logic-Apps/01Amazon_and_AWS/AWS_Security_Hub) |
| [AWS WAF](https://aws.amazon.com/waf/) | [AWS WAF](https://help.sumologic.com/07Sumo-Logic-Apps/01Amazon_and_AWS/AWS_WAF) |
| [AWS Config](https://aws.amazon.com/config/) | [AWS Config](https://help.sumologic.com/07Sumo-Logic-Apps/01Amazon_and_AWS/AWS_Config) |
| [AWS Network Firewall](https://aws.amazon.com/network-firewall/) | [AWS Network Firewall](https://help.sumologic.com/07Sumo-Logic-Apps/01Amazon_and_AWS/AWS_Network_Firewall) |

## Scenarios supported by this Quick Start

This Quick Start supports the following scenarios:

* Scenario 1: You do not use AWS security services and Sumo Logic. You did not configure AWS to use one or more of the security services listed under Specialized knowledge, but you want to do so and want to collect and analyze that data in Sumo Logic by using Sumo Logic apps. For this scenario, use the Quick Start to set up AWS security services and configure Sumo Logic.
* Scenario 2: You use AWS security services but not Sumo Logic. You use the AWS security services listed under Specialized knowledge but have not configured Sumo Logic to set up the collection of data from AWS and have not installed the relevant Sumo Logic apps in the Sumo Logic console. For this scenario, configure the auxiliary AWS services and resources to send data to Sumo Logic. This scenario also installs the corresponding Sumo Logic apps.
* Scenario 3: You use AWS security services and Sumo Logic. You use the AWS security services listed under [Specialized knowledge](#_Specialized_knowledge) and you collect and analyze data from one or more of them in Sumo Logic. For this scenario, configure the auxiliary AWS services and resources to send data to Sumo Logic. This scenario is intended only for non-configured AWS security services and their corresponding Sumo Logic apps.

## AWS account

If you don’t already have an AWS account, create one at [https://aws.amazon.com](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

The following are technical requirements for this Quick Start.

* A Sumo Logic account. If you don’t already have a Sumo Logic enterprise account, create one at <https://www.sumologic.com/> by following following the on-screen instructions.
* An AWS account. If you don’t already have an AWS account, create one at [https://aws.amazon.com](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.
* An understanding of how Sumo Logic resources are created.
* For data collection, scenario 1, a [new Sumo Logic hosted collector](https://help.sumologic.com/03Send-Data/Hosted-Collectors) called aws-quickstart-collector is created and sources for each app are installed under it.
* For data collection, scenarios 2 and 3, all existing sources can be reused. All new sources are installed under a new Sumo Logic–hosted collector called aws-quickstart-collector.
* All Sumo Logic apps are installed in a personal folder called SumoLogic Amazon QuickStart Apps, followed by the date.

**Note:** The Threat Intel app can report Elastic Load Balancing (ELB) data if you are already sending that data to Sumo Logic.

If you already configured AWS security services to send logs to S3 buckets or SNS topics, collect the following information before you launch the Quick Start.

**Note:** If you did not previously configure these services, this Quick Start automatically configures the AWS services and resources for you when you choose to install the Sumo Logic apps.

|  |  |  |
| --- | --- | --- |
| Sumo Logic apps | If you have done the following: | Make a note of: |
| CloudTrail, PCI DSS compliance for AWS CloudTrail, CIS AWS foundations, Amazon CloudTrail - Sumo Cloud Security Monitoring and Analytics, Sumo Global Intelligence for AWS CloudTrail SecOps App | Configured AWS CloudTrail to send its logs to an S3 bucket. | The S3 bucket name. |
| VPC flow logs, PCI DSS compliance for Amazon VPC flow logs, Amazon VPC Flow - Sumo Cloud Security Monitoring and Analytics | Configured AWS VPC flow to send its logs to an S3 bucket. | The S3 bucket name. |
| Amazon S3 audit | Configured the access logging of S3 buckets. | The S3 bucket name. |
| AWS WAF | Configured WAF to send a Kinesis Data Firehose delivery stream to an S3 bucket. | The S3 bucket name. |
| AWS Config | Configured AWS Config to deliver notifications to an SNS topic. | The SNS topic. |
| Threat Intel | Configured ELB logs to send data to Sumo Logic | The ELB source category in Sumo Logic |
| AWS Network Firewall | Configured Network Firewall and Firewall policy | Network Firewall Policy ARN |
| AWS Network Firewall | Have not configured Network Firewall | VPC ID, Subnet ID |

# 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 the [Access Key and Access ID](https://help.sumologic.com/Manage/Security/Access-Keys#manage-your-access-keys-on-preferences-page) 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 in the **Administration** section under the **Account** tab.

**Note:** If you want to use the Threat Intel app but have not configured data collection, see [Threat Intel for AWS](https://help.sumologic.com/07Sumo-Logic-Apps/01Amazon_and_AWS/Threat_Intel_for_AWS). If you already configured data collection, note the relevant Sumo Logic source category for your data.

## Step 2. Sign in to your AWS account

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](#_Planning_the_deployment) earlier in this guide.

## Step 3. Launch the Quick Start

1. Deploy Sumo Logic Security Integrations. Each deployment takes about 10 minutes to complete.

|  |
| --- |
|  |
| [Deploy Sumo Logic Security Integrations](https://fwd.aws/Nm69g) |

1. 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.
2. On the **Create stack** page, keep the default setting for the template URL, then choose **Next**.
3. 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 for deploying the Sumo Logic Quick Start

[View template](https://fwd.aws/MG4nr)

*Sumo Logic access 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**, **us1**, **in**, or **fed**. |
| Sumo Logic access ID (Section1bSumoLogicAccessID) | *Requires Input* | Enter the Sumo Logic console access ID, which you received when you created the Access Key in [Step 1](#_Step_1._Prepare). |
| Sumo Logic access key (Section1cSumoLogicAccessKey) | *Requires Input* | Enter your Sumo Logic access key. Obtain this from your Sumo Logic account (choose **Administration** > **Security** > **Access Keys**). |
| Delete Sumo Logic resources (Section1eSumoLogicResource RemoveOnDeleteStack) | 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**, the collector, sources, and Sumo Logic apps will not be deleted. |
| Sumo Logic organization ID (Section1dSumoLogicOrganization Id) | *Requires Input* | Enter your Sumo Logic organization ID, which you can find on your Sumo Logic console under **Account**. |

*AWS CloudTrail configuration:*

| **Parameter label (name)** | **Default** | **Description** |
| --- | --- | --- |
| **Install CloudTrail** (Section2aInstallCloudTrailApp) | Yes | Choose **Yes** to install AWS CloudTrail. Choose **No** to skip installation of this service. |
| **Install PCI compliance for AWS CloudTrail app** (Section2bInstallPCICloudTrail App) | Yes | Choose **Yes** to install PCI DSS compliance for AWS CloudTrail. Choose **No** to skip the installation of PCI DSS compliance. |
| **Install CIS AWS foundations benchmark app** (Section2cInstallCISFoundation App) | Yes | Choose **Yes** to install CIS AWS foundations benchmark. Choose **No** to skip installation of CIS AWS. |
| **Install Amazon CloudTrail - Cloud Security Monitoring and Analytics app**  (Section2InstallCloudTrailMonitoringAnalyticsApp) | Yes | Choose **Yes** to install Amazon CloudTrail - Cloud Security Monitoring and Analytics. Choose **No** to skip installation. |
| **Install Sumo Global Intelligence for AWS CloudTrail SecOps App**  (Section2InstallCloudTrailSecOpsApp) | Yes | Choose **Yes** to install Sumo Global Intelligence for AWS CloudTrail SecOps. Choose **No** to skip installation. |
| **Create AWS S3 bucket** (Section2dCloudTrailCreateBucket) | No | Choose **Yes** to create a new AWS CloudTrail S3 bucket in AWS. Choose **No** to use an existing CloudTrail S3 bucket. The S3 bucket must have CloudTrail log files. |
| **AWS S3 bucket name** (Section2eCloudTrailLogsBucket Name) | — | Required when Section2dCloudTrailCreateBucket is set to **No**. Provide the name of an existing S3 bucket that has CloudTrail log files. |
| **Create CloudTrail logs source** (Section2fCloudTrailCreateLog Source) | Yes | Choose **Yes** to create a CloudTrail logs source. Choose **No** to skip the creation of a CloudTrail logs source. |
| **Path expression for logs** (Section2gCloudTrailBucketPath Expression) | AWSLogs/\*/CloudTrail/\* | Path expression to match the folder structure for CloudTrail logs (for example, AWSLogs/\*/CloudTrail/\*). |
| **CloudTrail logs source category** (Section2hCloudTrailLogsSource CategoryName) | — | Used for Threat Intel app. This is required when Section2fCloudTrailCreateLog Source is set to **No**. Provide an existing source category name for collecting CloudTrail logs. |

*Amazon GuardDuty configuration:*

| **Parameter label (name)** | **Default** | **Description** |
| --- | --- | --- |
| **Install Amazon GuardDuty** (Section3aInstallGuardDutyApps) | Both | Install Amazon GuardDuty and Sumo Logic Global Intelligence for Amazon GuardDuty app. Choose **Both** to install both services. Choose **Skip** to not install these services. |
| **Create Sumo Logic HTTP logs source**  (Section3bGuardDutyCreateHttp LogsSource) | Yes | Choose **Yes** to create a Sumo Logic HTTP log source to collect Amazon GuardDuty logs. Choose **No** to skip creation of the Sumo Logic HTTP log source. |
| **Sumo Logic HTTP logs source category**  (Section3cGuardDutyHttpLogs SourceCategoryName) | — | Used for installing apps. This is required when Section3bGuardDutyCreateHttp LogsSource is set to **No**. Provide an existing source category name for collecting GuardDuty logs. |

*VPC flow logs configuration:*

| **Parameter label (name)** | **Default** | **Description** |
| --- | --- | --- |
| **Install Amazon VPC flow logs** (Section4aInstallVpcApps) | All | Install Amazon VPC flow logs and PCI DSS compliance. Choose **Both** to install both services. Choose **Skip** to not install these services. |
| **Create AWS S3 bucket** (Section4bVpcCreateBucket) | No | Creates a new S3 bucket. Choose **No** to use an existing S3 bucket that has VPC logs. |
| **AWS S3 bucket name** (Section4cVpcLogsBucketName) | — | Required when Section4bVpcCreateBucket is set to **No**. Provide an Existing bucket name that has VPC flow logs. |
| **Create AWS S3 bucket** (Section4dVpcCreateS3Source) | No | Choose **Yes** to create an Amazon S3 log source. Choose **No** to not create this log source. |
| **Path expression for logs** (Section4eVpcBucketPath Expression) | VPC-FLOW-LOGS/\* | Path expression to match the folder structure for VPC flow logs (for example, VPC-FLOW-LOGS/\*). |
| **Amazon S3 logs source category** (Section4fVpcLogsSourceCategory Name) | — | Used for Threat Intel. This is required when Section4dVpcCreateS3Source is set to **No**. Provide an existing source category name for collecting VPC flow logs. |

*Sumo Logic Threat Intel configuration:*

| **Parameter label (name)** | **Default** | **Description** |
| --- | --- | --- |
| **Install Sumo Logic Threat Intel** (Section5aInstallThreatIntelApp) | Yes | Choose **Yes** to install Threat Intel. Choose **No** to skip the installation. |
| **Amazon Elastic Load Balancer category** (Section5bElasticLoadBalancer SourceCategory) | — | Provide an existing source category for the Elastic Load Balancer logs. |

*Amazon S3 audit configuration:*

| **Parameter label (name)** | **Default** | **Description** |
| --- | --- | --- |
| **Install Amazon S3 audit app** (Section6aInstallS3AuditApp) | Yes | Choose **Yes** to install S3 audit app. Choose **No** to skip the installation. |
| **Create AWS S3 bucket** (Section6bS3AuditCreateBucket) | No | Choose **Yes** to create a new S3 bucket. Choose **No** to use an existing S3 buck that has S3 audit logs. |
| **AWS S3 bucket name** (Section6cS3AuditLogsBucketName) | — | Required when Section6bS3AuditCreateBucket is set to **No**. Provide an existing bucket name that has S3 audit logs. |
| **Create Amazon S3 audit logs source** (Section6dS3AuditCreateS3Source) | Yes | Choose **Yes** to create an S3 audit log. Choose **No** to skip the creation of an S3 audit log source. |
| **Path expression for the logs** (Section6eS3AuditBucketPath Expression) | S3-AUDIT-LOGS/\* | Path expression to match the folder structure for S3 audit logs (for example, S3-AUDIT-LOGS/\*). |
| **Amazon S3 audit logs source category** (Section6fS3AuditLogsSource CategoryName) | — | Used for app installation. This is required when Section6dS3AuditCreateS3Source is set to **No**. Provide an existing source category name for collecting S3 audit logs. |

*AWS Security Hub configuration:*

| **Parameter label (name)** | **Default** | **Description** |
| --- | --- | --- |
| **Install AWS Security Hub app** (Section7aInstallSecurityHubAudit App) | Yes | Choose **Yes** to install AWS Security Hub. Choose **No** skip the installation of AWS Security Hub. |
| **Enable Security Hub for the Region** (Section7bEnableSecurityHub) | No | Choose **Yes** if AWS Security Hub must be enabled for your Region. |
| **Create AWS S3 bucket** (Section7cSecurityHubCreateBucket) | No | Choose **Yes** to create a new S3 bucket. Choose **No** to use an existing S3 bucket that has Security Hub logs. |
| **AWS S3 bucket name** (Section7dSecurityHubLogsBucket Name) | — | Required when Section7cSecurityHubCreateBucket is set to **No**. Provide an Existing bucket name which has AWS Security Hub logs. |
| **Create Amazon S3 logs source** (Section7eSecurityHubCreateS3 Source) | Yes | Choose **Yes** to create an S3 log source. Choose **No** to skip the creation of an S3 log source. |
| **Path expression for the logs** (Section7fSecurityHubBucketPath Expression) | \*securityhub\*/\* | Path expression to match the folder structure for AWS Security Hub logs (for example, \*securityhub\*/\*) |
| **Amazon S3 logs source category** (Section7gSecurityHubLogsSource CategoryName) | — | Used for app installation. This is required when Section7eSecurityHubCreateS3 Source is set to **No**. Provide an existing source category name for collecting Security Hub logs. |

*AWS WAF configuration:*

| **Parameter label (name)** | **Default** | **Description** |
| --- | --- | --- |
| **Install AWS WAF** (Section8aInstallWafApp) | Yes | Choose **Yes** to install AWS WAF. Choose **No** to skip the installation of AWS WAF. |
| **Create a delivery stream** (Section8bCreateDeliveryStream) | No | Choose **Yes** to create Kinesis Data Firehose delivery stream. Choose **No** to skip the creation of a Kinesis Data Firehose delivery stream. |
| **Create AWS S3 bucket** (Section8cWafCreateBucket) | No | Choose **Yes** to create an S3 bucket. Choose **No** to use an existing S3 bucket that has AWS WAF logs. |
| **AWS S3 bucket name** (Section8dWafLogsBucketName) | — | Required when Section8cWafCreateBucket is set to **No**. Provide an existing bucket name that has AWS WAF logs. |
| **Create Amazon S3 logs source** (Section8eWafCreateS3Source) | Yes | Choose **Yes** to create an S3 log source. Choose **No** to skip the creation of an S3 log source. |
| **Path expression for logs** (Section8fWafBucketPath Expression) | WAF\_LOGS/\* | Path expression to match the folder structure for WAF logs (for example, WAF\_LOGS/\*). |
| **Amazon S3 logs source category** (Section8gWafLogsSourceCategory Name) | — | Used for app installation. This is required when Section8eWafCreateS3Source is set to **No**. Provide an existing source category name for collecting WAF logs. |

*AWS Config configuration:*

| **Parameter label (name)** | **Default** | **Description** |
| --- | --- | --- |
| **Install AWS Config**  (Section9aInstallConfigApp) | Yes | Choose **Yes** to install AWS Config. Choose **No** to skip the installation of AWS Config. |
| **Enable AWS Config for Region** (Section9bConfigEnableConfig) | No | Choose **Yes** to enable AWS Config for the Region. Choose **No** if AWS Config is already enabled. |
| **Create SNS topic for logs delivery** (Section9cConfigCreateSNSTopic) | No | Choose **Yes** to create an SNS topic and attach it to AWS Config to deliver the logs. Choose **No** if AWS Config logs are already delivered to an existing SNS topic. |
| **Existing topic name where logs are delivered** (Section9dConfigExistingTopic Name) | — | Required when Section9cConfigCreateSNSTopic is set to **No**. Provide an existing AWS Config SNS topic to stream configuration changes and notifications. |
| **Create Sumo Logic HTTP logs source** (Section9eConfigCreateHttpLogs Source) | Yes | Choose **Yes** to create an HTTP log source to collect AWS Config logs. Choose **No** to skip the creation of an HTTP log source. |
| **Amazon HTTP logs source category** (Section9fConfigHttpLogsSource CategoryName) | — | Used for app installation. Required when Section9eConfigCreateHttpLogs Source is set to **No**. Provide an existing source category name from Sumo Logic collecting AWS Config logs. |

*AWS Network Firewall configuration:*

| **Parameter label (name)** | **Default** | **Description** |
| --- | --- | --- |
| **Install Network Firewall App**  (Section11InstallNFWApp  ) | Yes | Choose **Yes** to install Network Firewall App. Choose **No** to skip the installation. |
| **Create AWS Network Firewall** (Section11CreateNewFW  ) | No | Choose **Yes** to create Network Firewall for the Region. Choose **No** if Network Firewall already exists. |
| **VPC ID for new AWS Network Firewall** (Section11VPCID  ) | - | Required when Section11CreateNewFW is set to Yes. Provide the existing VPC ID in which network firewall will be created. |
| **SubnetID for new AWS Network Firewall** (Section11SubnetID) | - | Required when Section11CreateNewFW is set to Yes. Provide the existing Subnet ID in which network firewall will be created. |
| **Create a Policy for new Network Firewall** (Section11CreateFirewallPolicy) | No | Choose **Yes** to create a firewall policy and attach it to Network Firewall.  Choose **No if**  firewall policy already exists. |
| **ARN of existing Network Policy** (Section11FirewallPolicyArn) | - | Required when Section11CreateFirewallPolicy is set to No. Provide ARN of existing firewall policy. |
| **Create default stateful rule group for Network Policy** (Section11StatefulRule  ) | - | Required when Section11CreateFirewallPolicy is set to Yes. Provide a stateful rule  Ex: pass tcp 10.20.20.0/24 45400:45500 <> 10.10.10.0/24 5203 (msg:\"test\";sid:1;rev:1;). |
| **Create default stateless rule group for Network Policy** (Section11StatelessRule  ) | 80 | Required when Section11CreateFirewallPolicy is set to Yes. Provide an allowed port  Ex: 80 |
| **Create AWS S3 Bucket** (Section11NFWCreateS3Bucket  ) | No | Choose **Yes** to create an S3 bucket .  Choose **No** if Network firewall logs are already delivered to an existing S3 bucket. |
| **AWS S3 Bucket Name** (Section11NFWLogsS3BucketName  ) | - | Required when Section11NFWCreateS3Bucket is set to **No**. Provide an Existing bucket name which has AWS Network Firewall logs.. |
| **AWS S3 Bucket Prefix** (Section11NFWLogsNFWBucketPrefix  ) | NFW/ | Provide S3 key prefix for Network Firewall logs. |
| **Create Sumo Logic Amazon S3 Logs Source** (Section11NFWCreateS3Source  ) | Yes | Choose **Yes** to create an S3 log source. Choose **No** to skip the creation of an S3 log source. |
| **Path Expression for the logs** (Section11NFWS3BucketLogsPathExpression  ) | \*AWSLogs/\*/network-firewall/\* | Path expression to match the folder structure for WAF logs (for example, \*AWSLogs/\*/network-firewall/\*). |
| **Amazon S3 Logs Source Category Name** (Section11NFWS3SourceCategoryName  ) | AWS/NFW/Flow/Logs | Used for app installation. This is required when Section7eSecurityHubCreateS3 Source is set to **No**. Provide an existing source category name. |

*Auto-enable logging configuration:*

| **Parameter label (name)** | **Default** | **Description** |
| --- | --- | --- |
| **Choose resource to auto-enable S3 logging** (Section91aEnableAutoLogging) | Skip | Choose **S3** to enable S3 audit logging for new buckets. Choose **VPC** to enable VPC flow logs for a new VPC, subnets, and network interfaces. Choose Firewall to enable Network Firewall logs for new Firewall. Choose **All** to enable logging for all (S3, VPC and Firewall). Choose Skip to skip new resources. |
| **Auto-enable logging for existing AWS resources** (Section91bEnableLoggingFor ExistingResources) | No | Choose **Yes** to enable logging for existing resources. Choose **No** to skip existing resources. |
| **Bucket prefix to store S3 audit logs** (Section91cS3LoggingBucket Prefix) | S3\_AUDIT\_LOGS/ | Provide a bucket prefix for S3 audit logs. It must end with a forward slash (/). |
| **Regex expression to filter AWS S3 buckets** (Section91dS3LoggingFilter Expression) | — | Provide regular expression for matching S3 buckets (for example, ‘test|prod’). |
| **Bucket prefix to store VPC flow logs** (Section91eVPCLoggingBucketPrefix) | VPC\_LOGS/ | Provide a bucket prefix for VPC flow logs. It must end with a forward slash (/). |
| **Regex expression to filter AWS VPC resources** (Section91fVPCLoggingFilter Expression) | — | Provide regular expression for matching VPC resources (for example, ‘VpcId’: ‘t1.micro.\*?’|’NetworkInterfaceId’: ‘Test.\*?’]|’SubnetId’: ‘prod.\*?’|test|prod’). |
| **Regex expression to filter firewall resources** (Section91FireWallLoggingFilterExpression) | — | Provide regular expression for matching Firewall resources (e.g., 'FirewallName': 'firewall-example.\*?'). |

*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](https://aws-quickstart.github.io/option1.html).

|  |  |  |
| --- | --- | --- |
| 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](https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMetadata.html) 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. |

1. On the options page, you can [specify tags](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-resource-tags.html) (key-value pairs) for resources in your stack and [set advanced options](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-add-tags.html). When you’re done, choose **Next**.
2. 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.
3. Choose **Create stack** to deploy the stack.
4. Monitor the status of the stack. When the status is **CREATE\_COMPLETE**, the Sumo Logic app stack is ready.

## Step 4. Test the deployment

### AWS account

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

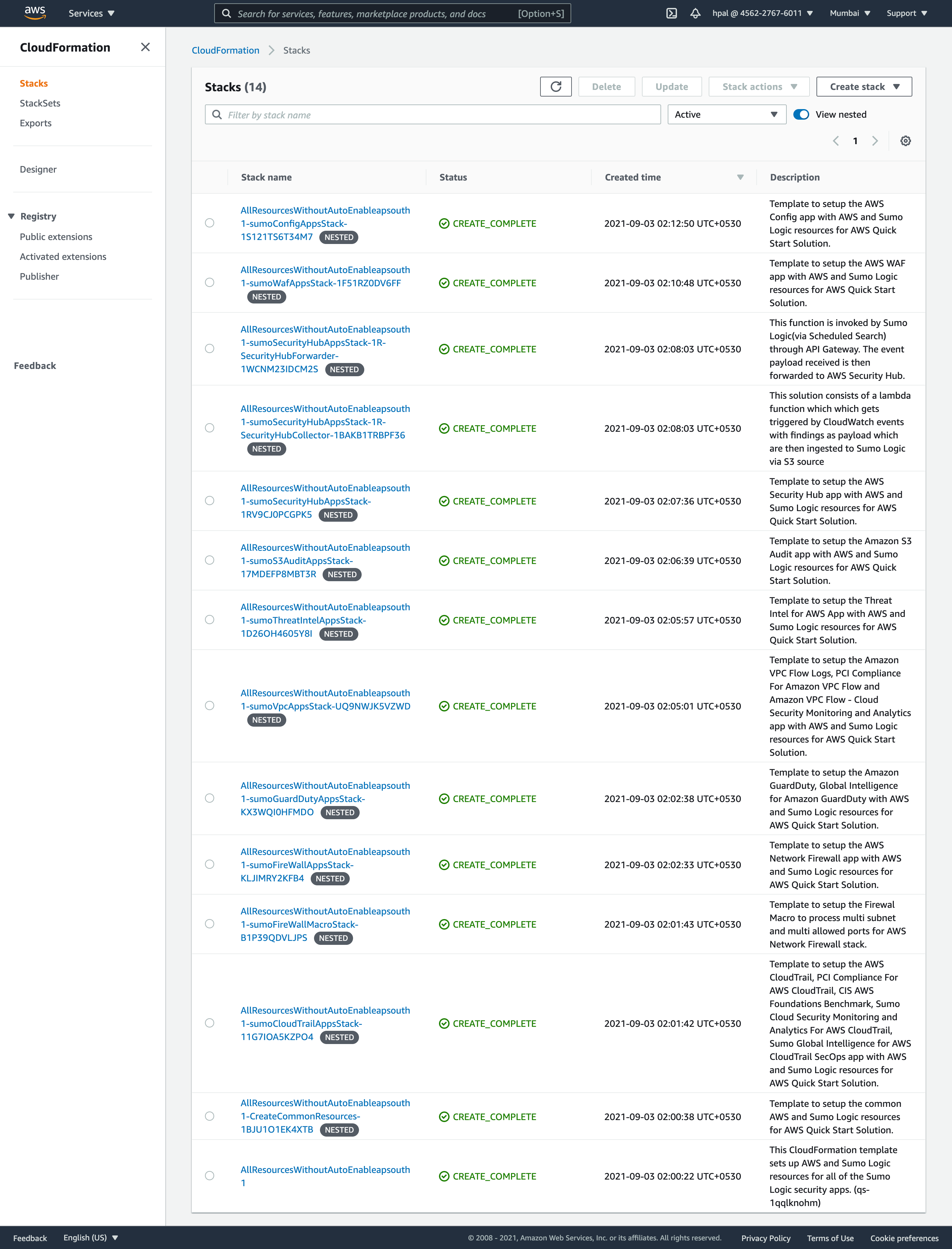


Figure 2: Example output of created resources

### Sumo Logic account

Confirm that the AWS CloudFormation template installed the collectors and sources for the selected Sumo Logic apps.

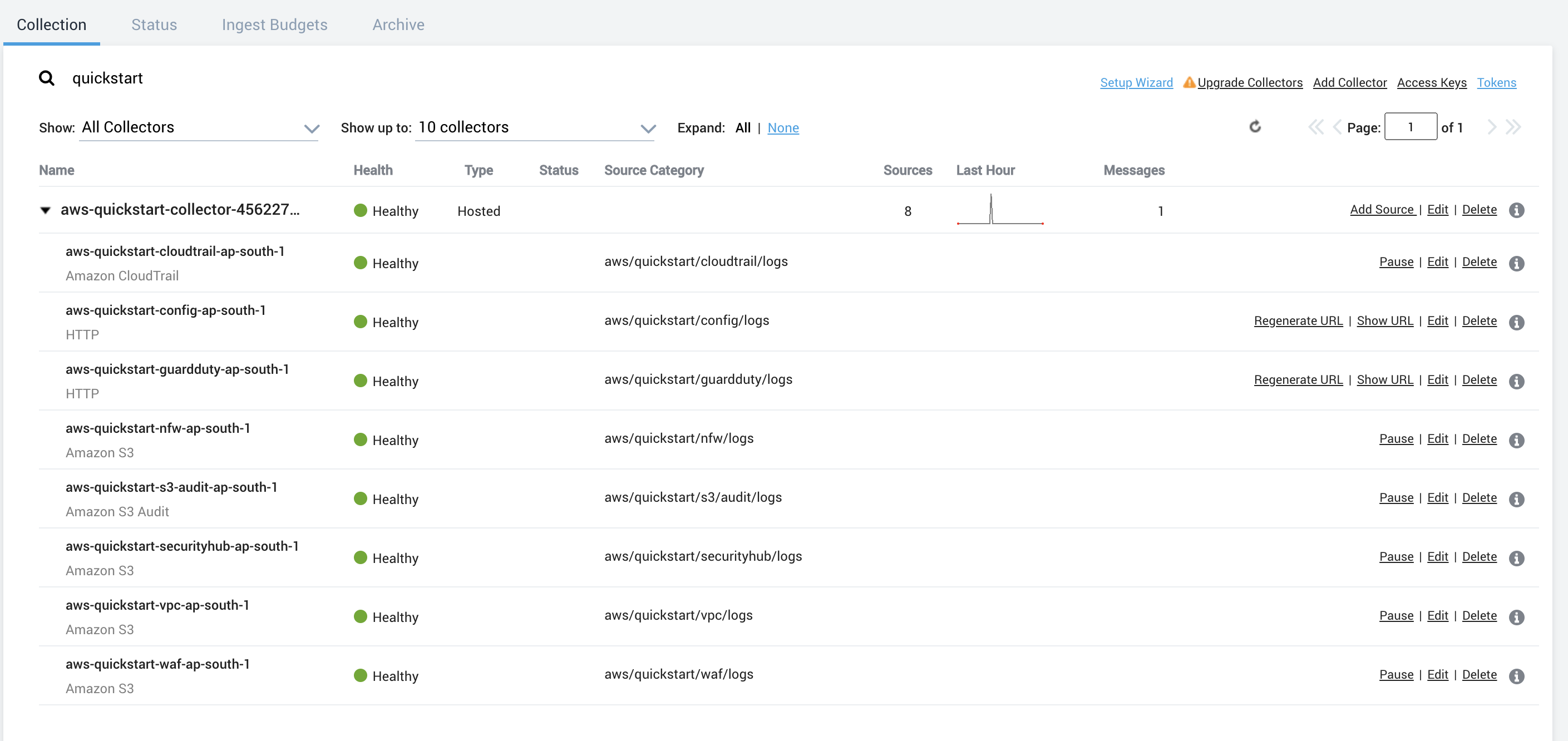


Figure 3: Example output of collectors and sources

## Step 5. Post-deployment steps

### Using existing S3 bucket

If you use an existing S3 bucket with logs, create an SNS topic (SumoSNSTopic-{StackName}) that subscribes to the Sumo Logic sources. Once the deployment completes, add that SNS topic to the S3 bucket events. For more information, see [How do I enable and configure event notifications for an S3 Bucket?](https://docs.aws.amazon.com/AmazonS3/latest/user-guide/enable-event-notifications.html)

**AWS WAF logs for Amazon Kinesis Data Firehose delivery stream**

If you install AWS WAF, CloudFormation creates a Kinesis delivery stream (QuickStartDeliveryStream{Region}) in your Kinesis configuration. You must configure Web ACL in your WAF configuration to send logs to the delivery stream. For more information, see [Logging Web ACL traffic information](https://docs.aws.amazon.com/waf/latest/developerguide/logging.html).

## Step 6. View the Sumo Logic dashboards

After the deployment completes, the Sumo Logic apps are added to your Sumo Logic personal-account library in a folder named SumoLogic Amazon QuickStart Apps <date>.

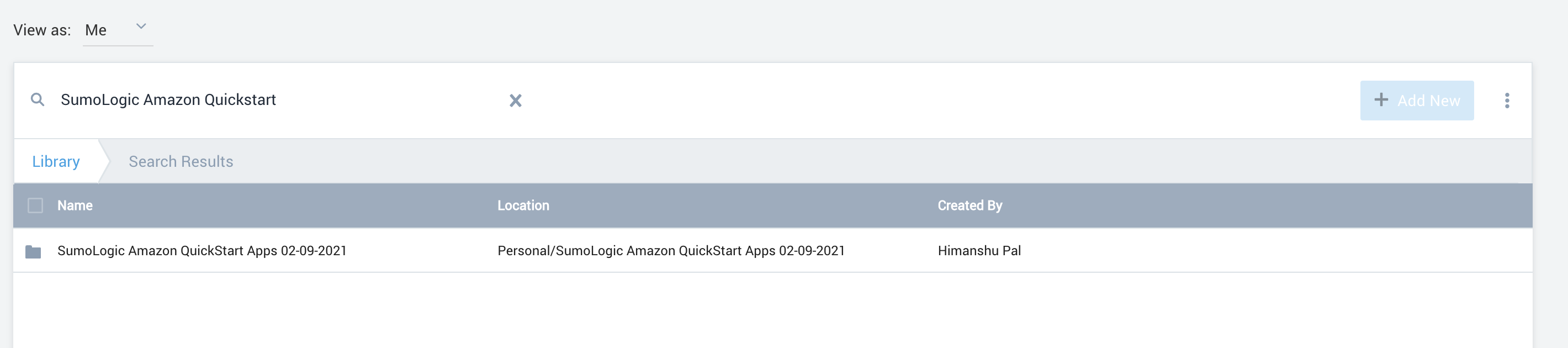


Figure 4: Top-level Quick Start apps folder

Under the SumoLogic Amazon QuickStart Apps <date> folder, there are sub-folders that represent each app, along with the date and timestamp.

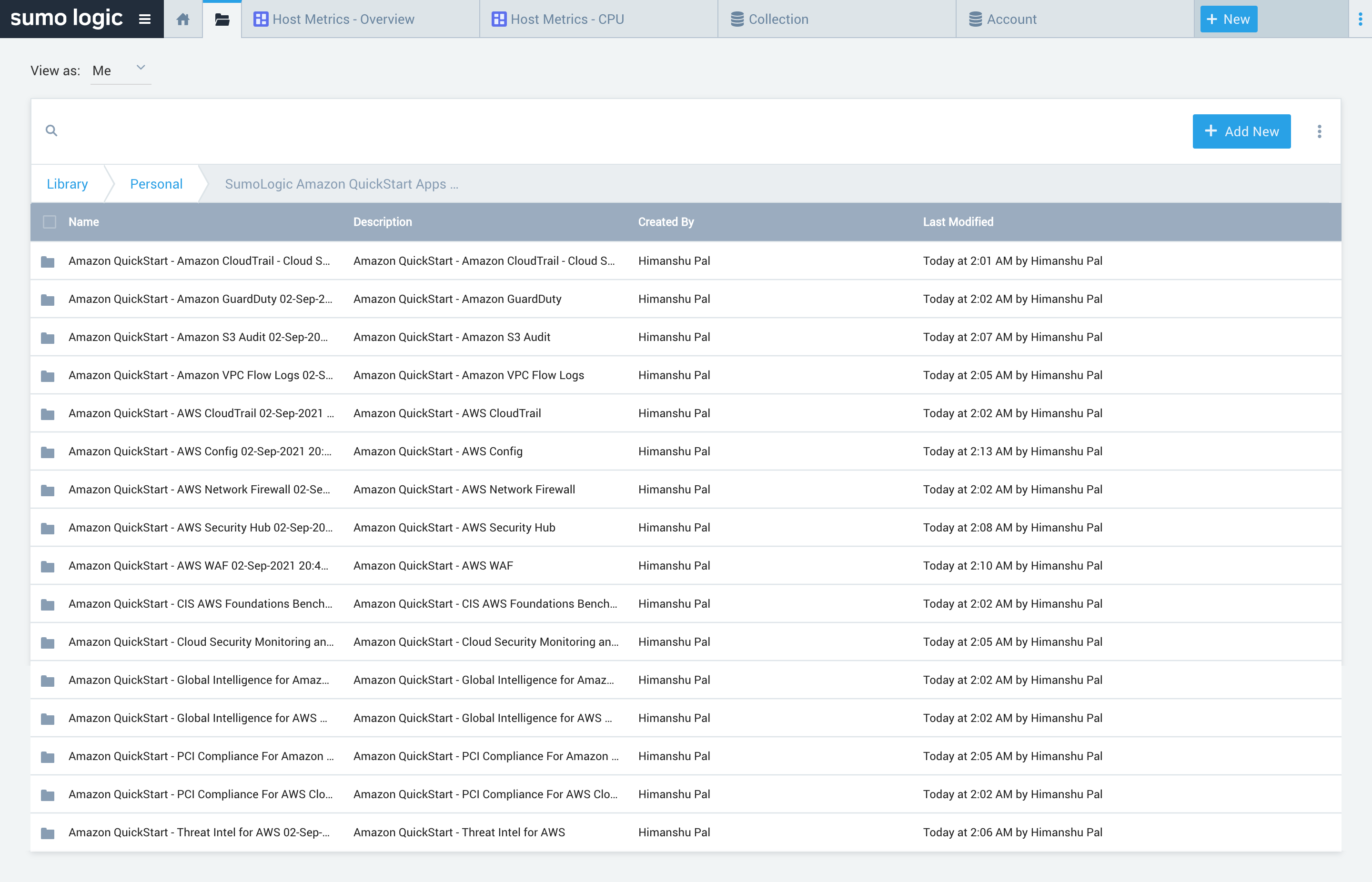


Figure 5: Individual service folders

To open the services dashboard, choose its folder in the Sumo Logic console. For instance, under the **Amazon GuardDuty** folder, open the **Amazon GuardDuty – Overview** dashboard to see detected threats.­

A screen shot of a computer

Description automatically generated

Figure 6: Amazon GuardDuty dashboard

# Best practices for using Sumo Logic Security Integrations

At the end of the deployment, if you want to use this Quick Start across multiple AWS accounts and Regions, rename the top-level parent folder of your Sumo Logic account (under your personal folder) to reflect the correct account and Region.

For each S3 bucket, follow the [AWS documentation](https://aws.amazon.com/premiumsupport/knowledge-center/secure-s3-resources/) best practices to secure all of your S3 objects. Sumo Logic Security Integrations can 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 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 **Disabled**. (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 **Disabled**, you continue to incur AWS charges for the stack. Please ensure to delete the stack when you finish troubleshooting.

For additional information, see [Troubleshooting AWS CloudFormation](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/troubleshooting.html) 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](http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cloudformation-limits.html).

# Send us feedback

To post feedback, submit feature ideas, or report bugs, use the **Issues** section of the [GitHub repository](https://fwd.aws/KEvGk) for this Quick Start. If you’d like to submit code, please review the [Quick Start Contributor’s Guide](https://aws-quickstart.github.io/).

# Additional resources

AWS resources

* [Getting Started Resource Center](https://aws.amazon.com/getting-started/)
* [AWS General Reference](https://docs.aws.amazon.com/general/latest/gr/)
* [AWS Glossary](https://docs.aws.amazon.com/general/latest/gr/glos-chap.html)

AWS services used by the deployment

* [AWS CloudFormation](https://docs.aws.amazon.com/cloudformation/)
* AWS [CloudWatch](https://aws.amazon.com/cloudwatch/)
* [AWS IAM](https://docs.aws.amazon.com/iam/)
* [Amazon SNS](https://aws.amazon.com/sns/)
* [AWS Lambda](https://aws.amazon.com/lambda/)
* [Amazon Kinesis Data Firehose](https://aws.amazon.com/kinesis/data-firehose/)
* [Amazon S3](https://aws.amazon.com/s3/)

Sumo Logic documentation

* [Sumo Logic Amazon and AWS apps](https://help.sumologic.com/07Sumo-Logic-Apps/01Amazon_and_AWS)
* [Sumo Logic Doc Hub](https://help.sumologic.com/07Sumo-Logic-Apps/01Amazon_and_AWS)
* [Sumo Logic Cloud SIEM](https://www.sumologic.com/solutions/security-intelligence/)

Other Quick Start reference deployments

* [AWS Quick Start home page](https://aws.amazon.com/quickstart/)

# Document revisions

|  |  |  |
| --- | --- | --- |
| Date | Change | In sections |
| May 2020 | Initial publication | — |
| Sep 2021 | 3 New Sumo Logic App Installation  1 App renamed  Network Firewall AWS Services and Sumo Apps |  |

© 2020, Amazon Web Services, Inc. or its affiliates, and Sumo Logic. All rights reserved.

**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.

The software included with this paper is licensed under the Apache License, Version 2.0 (the "License"). You may not use this file except in compliance with the License. A copy of the License is located at <http://aws.amazon.com/apache2.0/> or in the "license" file accompanying this file. This code is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.