Sumo Logic on AWS Cloud

Quick Start for Sumo Logic Security Applications

October 2019

SumoLogic
<Solutions Architect Names>, AWS

Contents

Quick Links 2

Overview 3

SumoLogic on AWS 3

Costs and Licenses 3

Architecture 4

Prerequisites 6

Technical Requirements 6

Specialized Knowledge 6

Deployment Options 6

Deployment Steps 7

Step 1. Prepare Your AWS Account 7

Step 2. Prepare Your SumoLogic Account 7

Step 3. Launch the Quick Start 7

Parameters for Deploying SumoLogic Application into AWS account 8

Troubleshooting 9

GitHub Repository 10

Additional Resources 10

AWS Resources 10

SumoLogic 10

Quick Start reference deployments 10

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.

Quick Links

The links in this section are for your convenience. Before you launch the Quick Start, please review the architecture, security, and other considerations discussed in this guide.

- If you have an AWS account as well as a Sumo Logic registered account, and you are already familiar with AWS services and the Sumo Logic console, you can launch the Quick Start to build the serverless architecture shown in Figure 1. The deployment takes approximately ten minutes. If you're new to AWS or to the SumoLogic Application Quick Start, please review the implementation details and follow the step-by-step instructions provided later in this guide.

Launch

- If you want to take a look under the covers, you can view the AWS CloudFormation template that automates the deployment.

Viewtemplate

Overview

This Quick Start reference deployment guide provides step-by-step instructions for deploying the applications on Sumo Logic.

This Quick Start is for users who intend to visualize, monitor and analyze different AWS applications on Sumo Logic console.

Sumo Logic on AWS

The Sumo Logic platform helps you make data-driven decisions and reduce the time to investigate security and operational AWS account issues so you can free up resources for more important activities.

The Quick Start template installs multiple applications on Sumo Logic, creates resources in your AWS account to be able to collect logs using leveraging different services and send it to your pre-registered Sumo Logic account.

In less than 10 mins, you can start monitoring, troubleshooting in real time. You can analyze any security threats and quickly detect indicators of compromise.

Costs 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. For cost estimates, see the pricing pages for each AWS service you will be using. Prices are subject to change.

> **Tip** After you deploy the Quick Start, we recommend that you enable the AWS Cost and Usage Report to track costs associated with the Quick Start. This report delivers billing metrics to an 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.

Architecture

Deploying this Quick Start for a serverless architecture with parameters builds the following environment in the AWS Cloud.

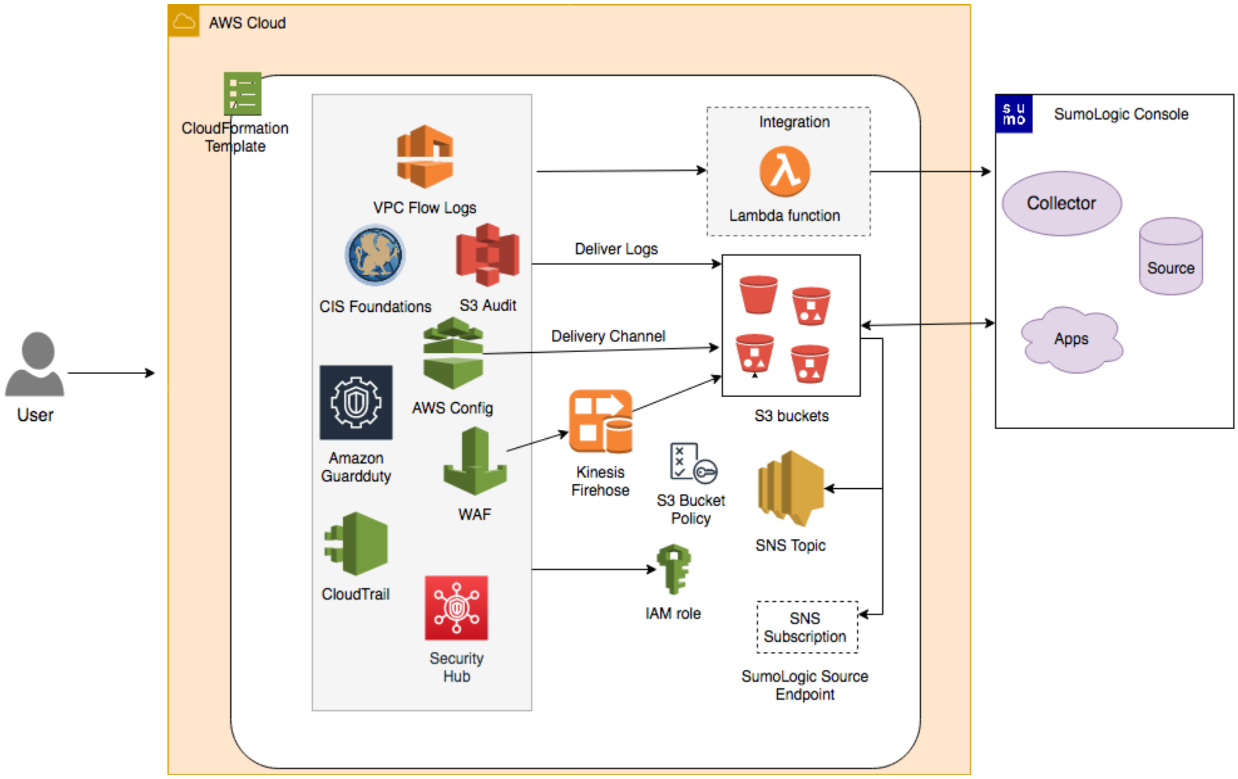

Figure 1: Quick Start Architecture

The Quick Start sets up the following serverless architecture:

- Multiple SAM Applications are deployed in your environment.
- Each SAM application consists of more than one AWS resources which includes AWS Identity and Access Management (IAM) role, Amazon S3 Buckets, SNS Topic and subscription, AWS Lambda functions, Kinesis Firehose Delivery Stream and so on.
- AWS Lambda Function creates collector, source and install apps on your SumoLogic account. You will be asked to provide Sumo Access ID, Access Key, Source Category and other Sumo Logic related parameters when you deploy this Quick Start.
- Amazon S3 Buckets are used to capture the logs from different AWS services. SumoLogic Collector and Source will consume logs from these S3 buckets.
- Bucket Policies provide access to services to read and write data to the buckets.
- Kinesis Firehose delivery streams to transfer logs from AWS Web Application Firewall

(WAF) to an S3 bucket.

- S3 Event Notification triggers an SNS topic when there is a new object in the bucket.

Prerequisites

Technical Requirements

From a technical standpoint, you'll need:

- Sumo Logic Account. If you don't already have a Sumo Logic 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 IAM roles.

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 Lambda
- AWS CloudFormation
- Amazon S3
- SumoLogic Console

Deployment Options

This Quick Start provides one deployment option:

□ **Deploy SumoLogic applications as serverless architecture** (end-to-end deployment). This 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. Users have options to select which applications they would like to install.

The Quick Start provides a template for this option.

Deployment Steps

Step 1. Prepare Your AWS Account

1. If you don't already have an AWS account, create one at https://aws.amazon.com by following the on-screen instructions.

2. Use the region selector in the navigation bar to choose the AWS Region where you want to deploy Sumo Logic App template resources.

Step 2. Prepare Your Sumo Logic Account

1. If you don't already have a SumoLogic 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 will need them to pass as parameters when you launch the Quick Start template in the next step.

3. You will also need to pass Organization ID. You can get it from your Sumo Logic account under Administration-> Account.

Step 3. Launch the Quick Start

> **Note** 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 this Quick Start. For full details, see the pricing pages for each AWS service you will be using in this Quick Start. Prices are subject to change.

1. Launch the AWS CloudFormation template into your AWS account.

Deploy SumoLogic App template

Launch

Each deployment takes about 10 minutes to complete.

2. Check the region that's displayed in the upper-right corner of the navigation bar, and change it if necessary. This is where the infrastructure for Sumo Logic Application resources will be built.

3. On the **Select Template** page, keep the default setting for the template URL, and then choose **Next**.

4. On the **Specify 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 Sumo Logic Application into AWS account

In the following tables, parameters are listed by category:

Sumo Logic Configuration:

Parameter label	Default	Description
Sumo Logic Deployment Name	*Requires Input*	Deployment assigned depending on the geographic location eg:us2, us1, au, ca etc.
Sumo Logic Access ID	*Requires Input*	Sumo Logic Console Access ID. When you create Access Key, you will get Access ID with it.
Sumo Logic Access Key	*Requires Input*	Sumo Logic Access Key. You can create this from your Sumo Logic account, Administration > Security > Access Keys.
Delete Sumo Logic Resource when stack is deleted	*Requires Input*	To delete collector, sources and app when stack is deleted, set this parameter to true. Default is false.
Sumo Logic Organization ID	*Requires Input*	Sumo Logic org ID can be found on your Sumo Logic console under Account.
Prefix For Your S3 Buckets	*Requires Input*	Provide a unique S3 Bucket prefix. This will be applied to all S3 buckets created using the Quickstart template.

AWS Quick Start configuration:

> **Note** We recommend that you keep the default settings for the following two parameters, unless you are customizing the Quick Start templates for your own deployment projects. Changing the settings of these parameters will automatically update 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

Parameter label (name)	Default	Description
		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.

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 check box to acknowledge that the template will create IAM resources.
7. Choose **Create** to deploy the stack.
8. Monitor the status of the stack. When the status is **CREATE_COMPLETE**, the AWS Sumo Logic App stack is ready.

Troubleshooting

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 will be retained and the instance will be left running, so you can troubleshoot the issue.

> **Important** When you set **Rollback on failure** to **No**, you will 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 when you create the stack. For more information about AWS CloudFormation limits, see the AWS documentation.

GitHub Repository

You can visit our GitHub repository to download the templates and scripts for this Quick Start, to post your comments, and to share your customizations with others.

Additional Resources

AWS Resources

- Getting started
- General Reference
- AWS Lambda
- AWS CloudFormation
- Amazon S3
- AWS SNS
- AWS IAM

Sumo Logic

- Sumo Logic Website
- Sumo Logic Apps for Amazon and AWS
- Hosted Collectors
- Hosted Collector Sources

Quick Start reference deployments

- AWS Quick Start home page
  https://aws.amazon.com/quickstart/

Document Revisions

Date	Change	In sections
October 2019	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.