

# SumoLogic on AWS Cloud

## Quick Start SumoLogic 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.....	10
GitHub Repository .....	10
Additional Resources .....	10
AWS Resources .....	10
SumoLogic.....	11
Quick Start reference deployments.....	11

This Quick Start was created by SumoLogic 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 SumoLogic registered account, and you're already familiar with AWS services and the SumoLogic 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.

A blue rectangular button with rounded corners and the word "Launch" in white text.

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

An orange rectangular button with rounded corners and the text "View template" in white.

## Overview

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

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

## SumoLogic 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 SumoLogic, creates resources in your AWS account to be able to collect logs using leveraging different services and send it to your pre-registered SumoLogic 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

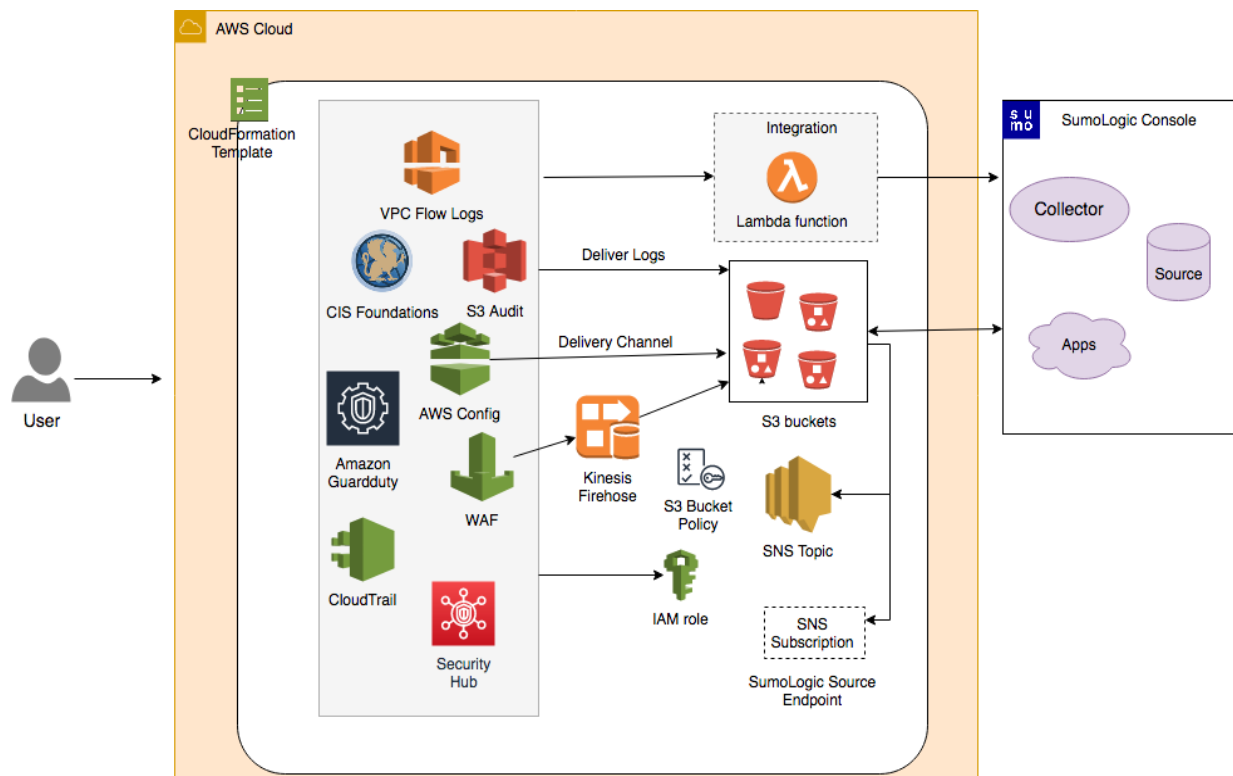
You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using the Quick Start.

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:

- SumoLogic Account. If you don't already have a SumoLogic 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 SumoLogic. (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 SumoLogic 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 SumoLogic App template resources.

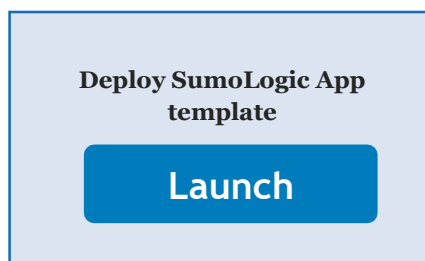
### Step 2. Prepare Your SumoLogic Account

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 SumoLogic 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 SumoLogic 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.



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 SumoLogic Application into AWS account

In the following tables, parameters are listed by category:

### *SumoLogic Configuration:*

Parameter label (name)	Default	Description
<b>SumoLogic Collector</b> (SumoLogicCollectorName)	<service-name>Collector	Hosted Collector name.
<b>SumoLogic Source</b> (SumoLogicSourceName)	<service-name>Source	Sources are the environments that Sumo Logic Collectors connect to collect data from your site. Each Source is configured to collect files in a specific way, depending on the type of Collector you're using
<b>SumoLogic Category</b> (SumoLogicSourceCategory)	AWS/Labs/<application-name>	The string used to query the logs from the source.
<b>SumoLogic Deployment</b> (SumoLogicDeployment)	<i>Requires Input</i>	Deployment assigned depending on the geographic location eg:us2, us1, au, ca etc.
<b>SumoLogic Access Key</b> (SumoLogicAccessKey)	<i>Requires Input</i>	Sumo Logic Access Key. You can create this from your sumologic account, under preferences.
<b>SumoLogic Access ID</b> (SumoLogicAccessId)	<i>Requires Input</i>	Sumo Logic Console Access ID. When you create Access Key, you will get Access ID with it.
<b>Path Expression</b> (PathExpression)	AWSLogs/*	Sumologic source captures logs from this path in your Amazon S3 bucket
<b>Remove SumoLogic Resources on Stack Delete</b> (RemoveSumoResourcesOnDeleteStack)	false	To delete collector, sources and app when stack is deleted, set this parameter to true. Default is false.
<b>SumoLogic Organization ID</b> (SumoLogicOrganizationId)	<i>Requires Input</i>	Sumologic org ID can be found on your sumologic console under Account.

### *AWS Configuration:*



Parameter label (name)	Default	Description
<b>Create Target S3 bucket</b> (CreateTargetS3Bucket)	yes	Whether you would like to create a new S3 bucket in your AWS account to store quick start assets.
<b>S3 Bucket Name</b> (S3BucketName)	<service-name>- s3-bucket- <timestamp>	Name of the S3 bucket you would like to create or use an existing one.

### *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
<b>Quick Start S3 bucket name</b> (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.
<b>Quick Start S3 key prefix</b> (QSS3KeyPrefix)	quickstart- sumologic-apps	The <a href="#">S3 key name prefix</a> 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.

- 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**.
- 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.
- Choose **Create** to deploy the stack.
- 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](#)

## SumoLogic

- [SumoLogic Website](#)
- [Apps Sumo provides for Amazon and AWS](#)
- [Source](#)
- [Hosted Collector](#)

## Quick Start reference deployments

- AWS Quick Start home page\_  
<https://aws.amazon.com/quickstart/>

## Document Revisions

Date	Change	In sections
October 2019	Initial publication	—

© 2018, Amazon Web Services, Inc. or its affiliates, and SumoLogic, Inc. 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.