About Sumo Logic – AWS Observability Solution

dev.classmethod.jp/articles/sumo-logic-aws-observability-sakumashogo-20230707

佐久間昇吾

July 7, 2023

First

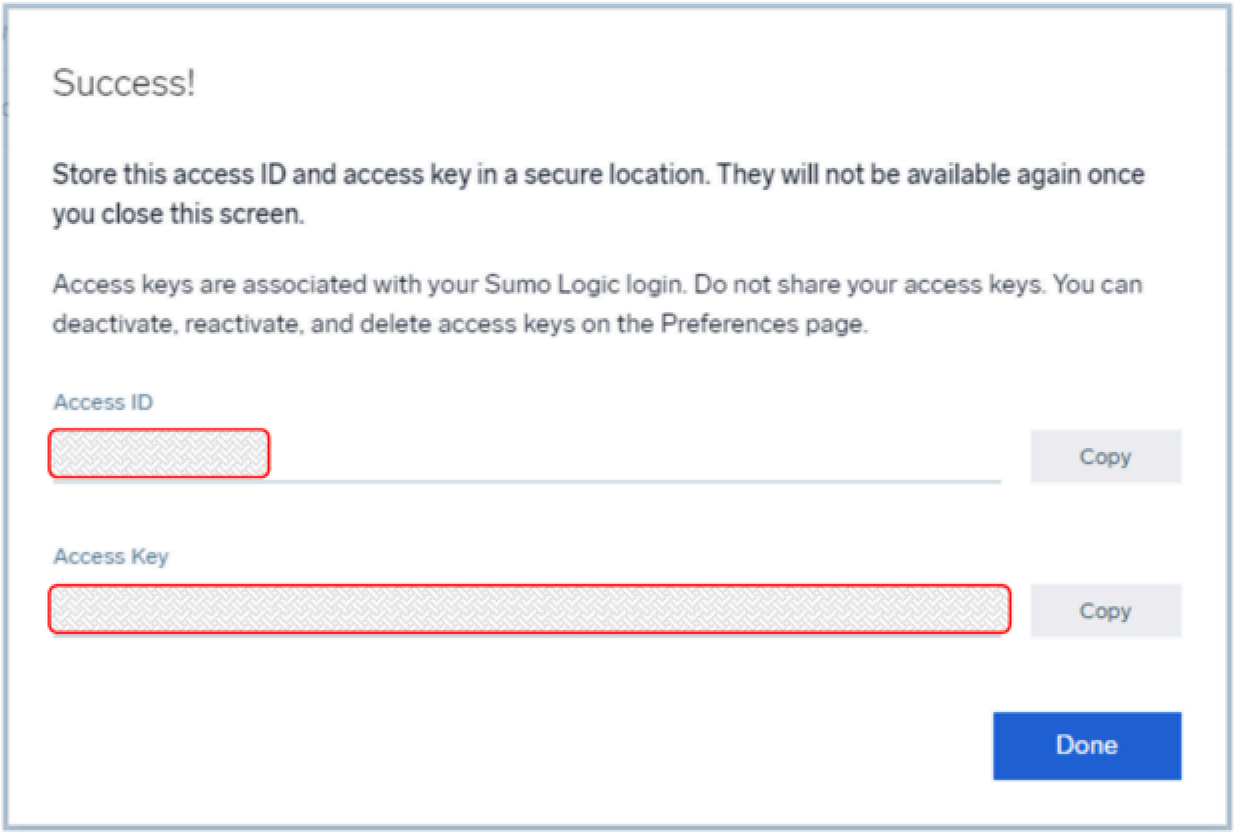
The Sumo Logic AWS Observability Solution accelerates time to operational insight into key AWS infrastructure, enabling organizations to minimize the impact of resource issues.

In this article, I would like to introduce the configuration for deploying the AWS Observability Solution and some of the completed dashboards.

Configuring AWS Observability

First, you will need to issue an "Access ID/Key" from Sumo Logic to securely connect to it.

Steps:
Go to Administration > Security > Access Keys and click the + button. Enter the Access Key Name and click Save. Copy both the Access ID and Access Key that appear. ***The Access Key can only be copied here. Be sure to write it down somewhere.**



Success!

Store this access ID and access key in a secure location. They will not be available again once you close this screen.

Access keys are associated with your Sumo Logic login. Do not share your access keys. You can deactivate, reactivate, and delete access keys on the Preferences page.

Access ID

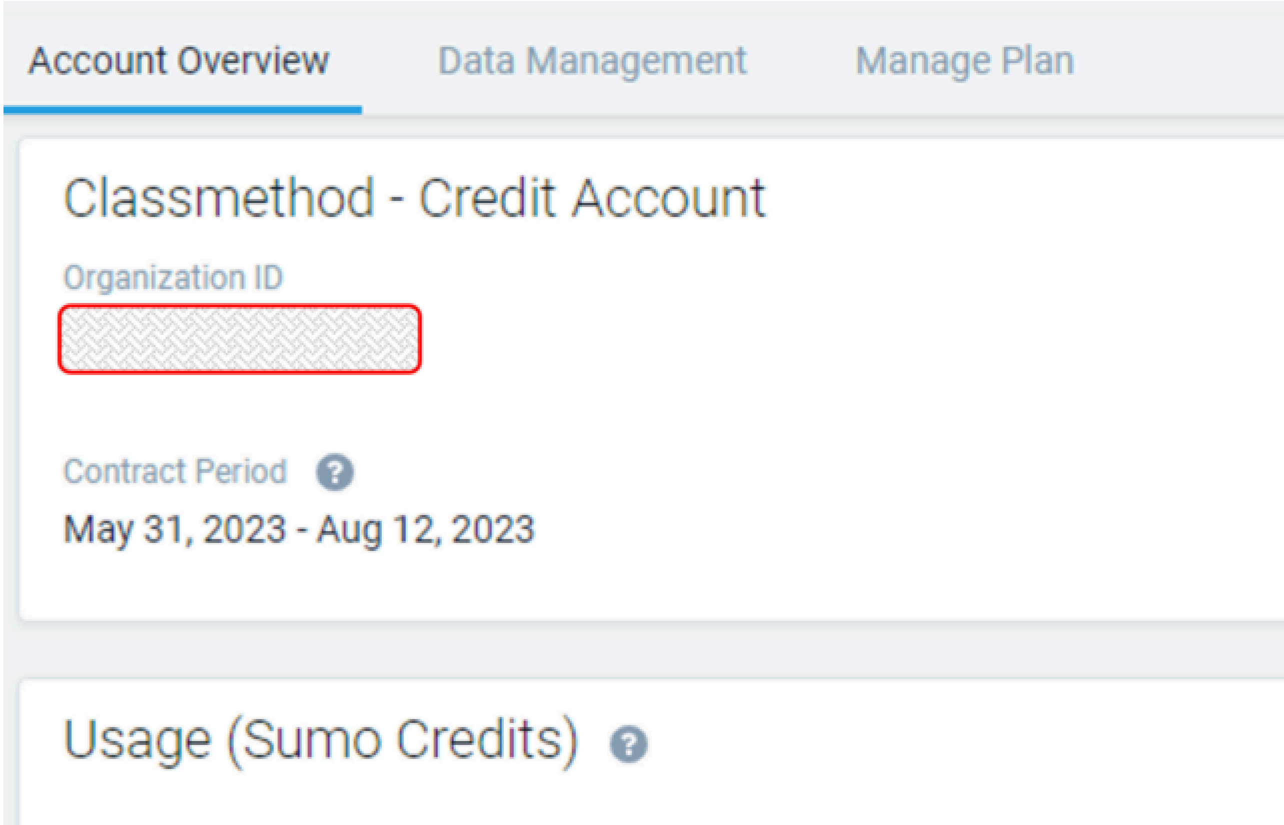
[redacted]

Access Key

[redacted]

Once you have the copy, the next step is to get your Sumo Logic Organization ID.

Step 1:
Copy the alphanumeric characters displayed in Organization ID under Administration > Account > Account Overview.



Classmethod - Credit Account

Organization ID

[redacted]

Contract Period

May 31, 2023 - Aug 12, 2023

Usage (Sumo Credits)

Now that we have all the necessary information on the Sumo Logic side, we can test the access permissions.

Permissions Test on AWS and Sumo Logic Side

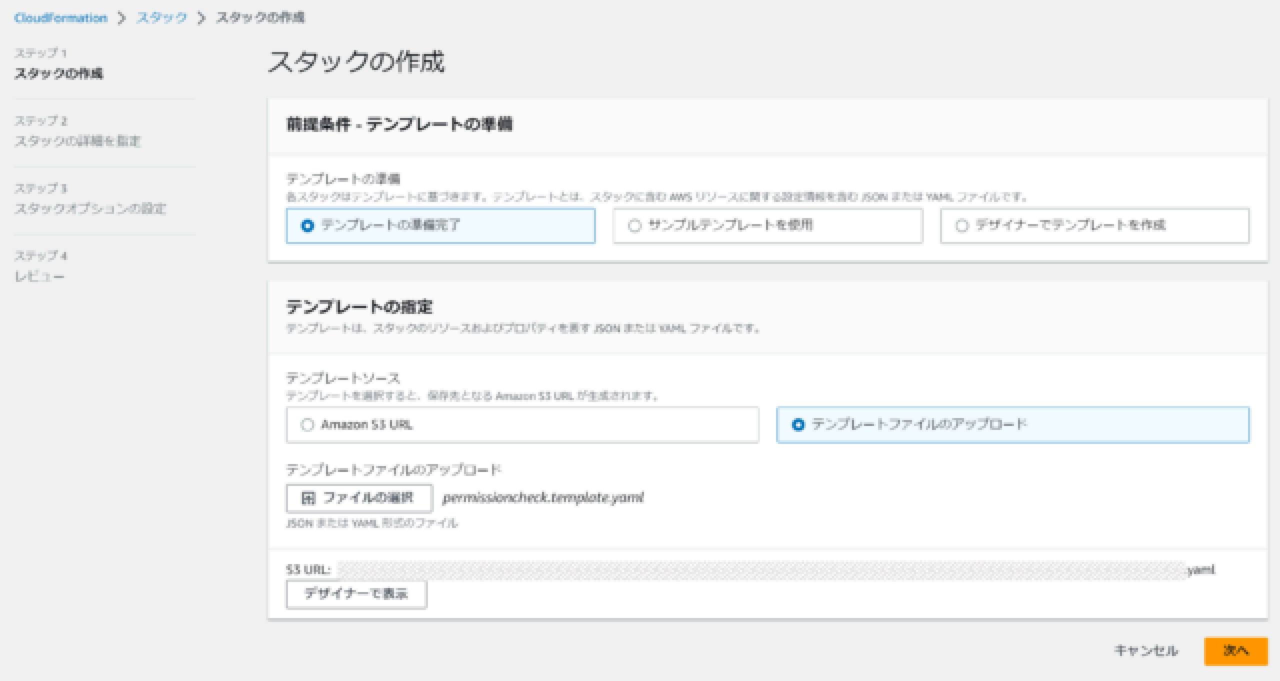
Sumo Logic provides AWS CloudFormation templates for testing permissions to deploy AWS Observability. See Before You Deploy - Verify AWS and Sumo Logic Permissions | Sumo Logic Docs.

sumologic-solution-templates | Sumo Logic Github to ensure you have the required roles.

You can see the resources that can be created at AWS Observability Resources | Sumo Logic Docs .

StepsDownload
the AWS CloudFormation template for permission testing on the above site

Then, go to the AWS CloudFormation screen and click Create Stack. This will take you to the screen below.



CloudFormation > スタック > スタックの作成

ステップ 1
スタックの作成

ステップ 2
スタックの詳細を指定

ステップ 3
スタックオプションの設定

ステップ 4
レビュー

スタックの作成

前提条件 - テンプレートの準備

テンプレートの準備
各スタックはテンプレートに基づきます。テンプレートとは、スタックに含む AWS リソースに関する設定情報を含む JSON または YAML ファイルです。

● テンプレートの準備完了　○ サンプルテンプレートを使用　○ デザイナーでテンプレートを作成

テンプレートの指定
テンプレートは、スタックのリソースおよびプロパティを表す JSON または YAML ファイルです。

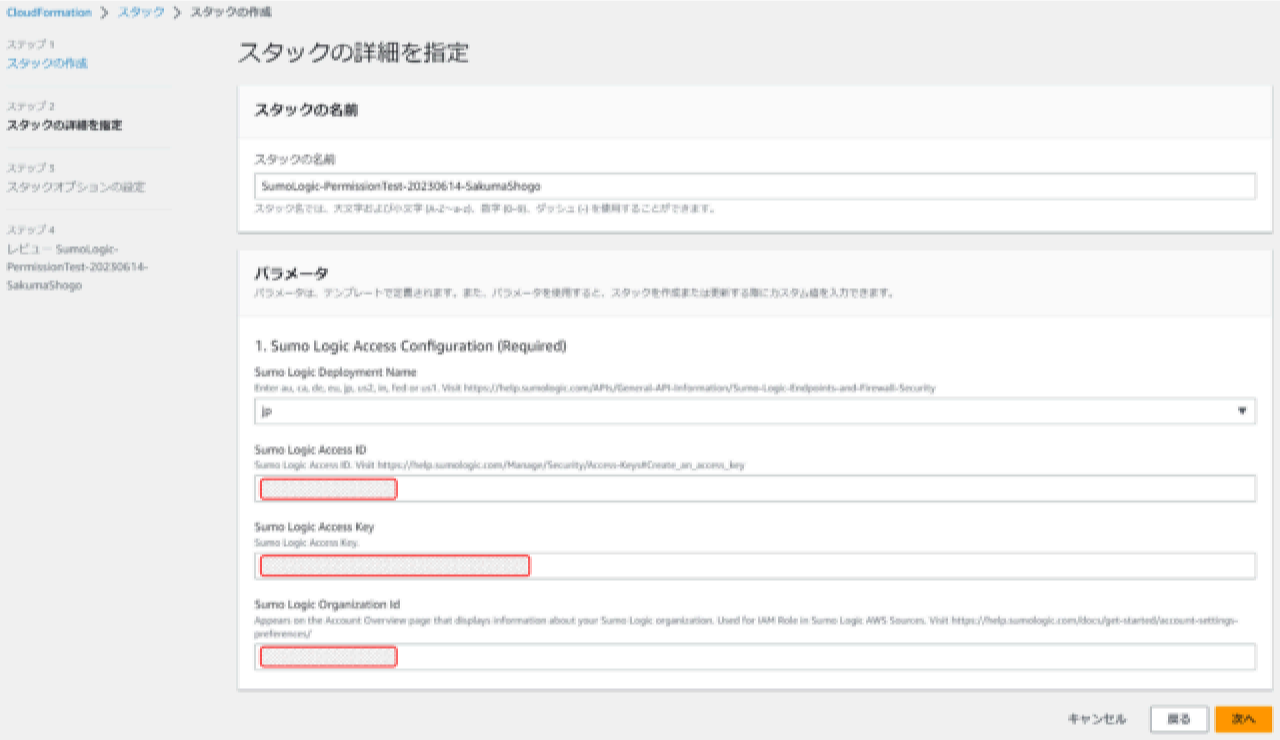
テンプレートソース
テンプレートを選択すると、保存先となる Amazon S3 URL が生成されます。

○ Amazon S3 URL　● テンプレートファイルのアップロード

テンプレートファイルのアップロード
ファイルの選択　*permissioncheck.template.yaml*
JSON または YAML 形式のファイル

S3 URL: [redacted] yaml

After that, select "Template is ready" and "Upload template file" to upload the .yaml file you downloaded earlier. Once completed, click "Next" to move to the screen below.



CloudFormation > スタック > スタックの作成

ステップ 1
スタックの作成

ステップ 2
スタックの詳細を指定

ステップ 3
スタックオプションの設定

ステップ 4
レビュー SumoLogic-PermissionTest-20230614-SakumaShogo

スタックの詳細を指定

スタックの名前

スタックの名前
SumoLogic-PermissionTest-20230614-SakumaShogo
スタック名では、大文字および小文字 (A-Z~a-z)、数字 (0-9)、ダッシュ (-) を使用することができます。

パラメータ
パラメータは、テンプレートで定義されます。また、パラメータを使用すると、スタックを作成または更新する際にカスタム値を入力できます。

1. Sumo Logic Access Configuration (Required)

Sumo Logic Deployment Name
Enter au, ca, de, eu, jp, us2, in, fed or us1. Visit https://help.sumologic.com/APIs/General-API-Information/Sumo-Logic-Endpoints-and-Firewall-Security
jp

Sumo Logic Access ID
Sumo Logic Access ID. Visit https://help.sumologic.com/Manage/Security/Access-Keys#Create_an_access_key
[redacted]

Sumo Logic Access Key
Sumo Logic Access Key.
[redacted]

Sumo Logic Organization Id
Appears on the Account Overview page that displays information about your Sumo Logic organization. Used for IAM Role in Sumo Logic AWS Sources. Visit https://help.sumologic.com/docs/get-started/account-settings-preferences/
[redacted]

Here, enter the Access ID/Access Key and Sumo Logic Org ID explained at the beginning. Once you've finished entering the information, click "Next." From here on, you can proceed without entering anything else, and finally click "Submit" to confirm that the template is executed successfully.

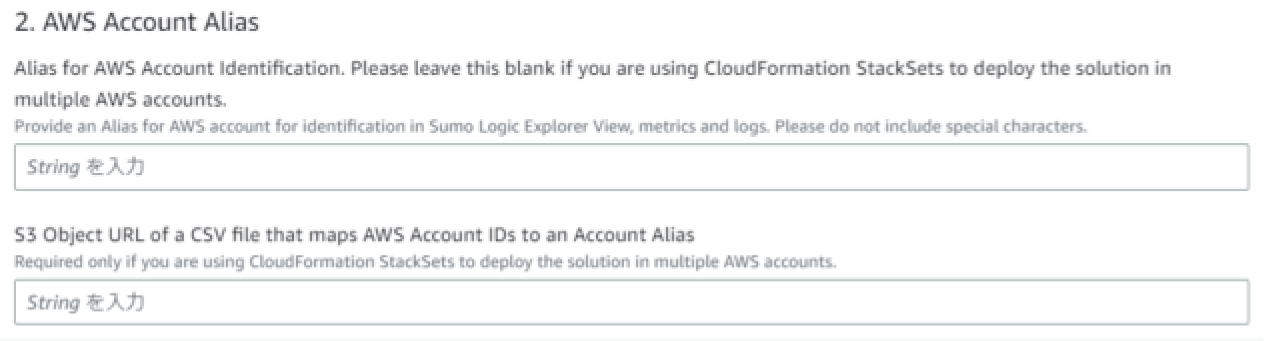
Production template deployment settings

Using the Cloud Formation template for production deployment, sumologic_observability.master.template.yaml , upload the template file on the Cloud Formation stack creation screen or use the S3 URL (https://sumologic-appdev-aws-sam-apps.s3.amazonaws.com/aws-observability-versions/v2.6.0/sumologic_observability.master.template.yaml).

Now, let's take a look at each one, with reference to Deploy with AWS CloudFormation | Sumo Logic .

1. Sumo Logic Access Configuration (Required)

Enter the same information as in the permission test template. We recommend setting "Delete Sumo Logic Resources when stack is deleted" to "true." This setting determines whether resources are deleted when deployment fails.



2. AWS Account Alias

Alias for AWS Account Identification. Please leave this blank if you are using CloudFormation StackSets to deploy the solution in multiple AWS accounts.

Provide an Alias for AWS account for identification in Sumo Logic Explorer View, metrics and logs. Please do not include special characters.

String を入力

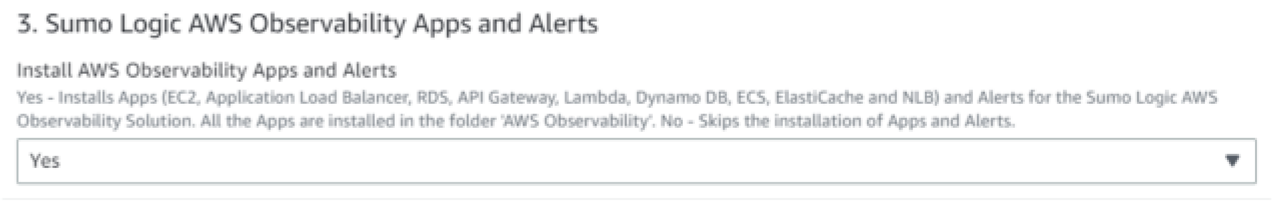
S3 Object URL of a CSV file that maps AWS Account IDs to an Account Alias

Required only if you are using CloudFormation StackSets to deploy the solution in multiple AWS accounts.

String を入力

Here, enter an alias for your AWS account. This alias will be displayed later in Sumo Logic, so it's best to use a name that indicates what the account is used for.

For the S3 Object URL of a CSV file that maps AWS Account IDs to an Account Alias field, if you have multiple AWS accounts and have uploaded a CSV file to S3 to map each account, enter the S3 URL. If you are targeting a single account, as in this case, you can leave this field blank.



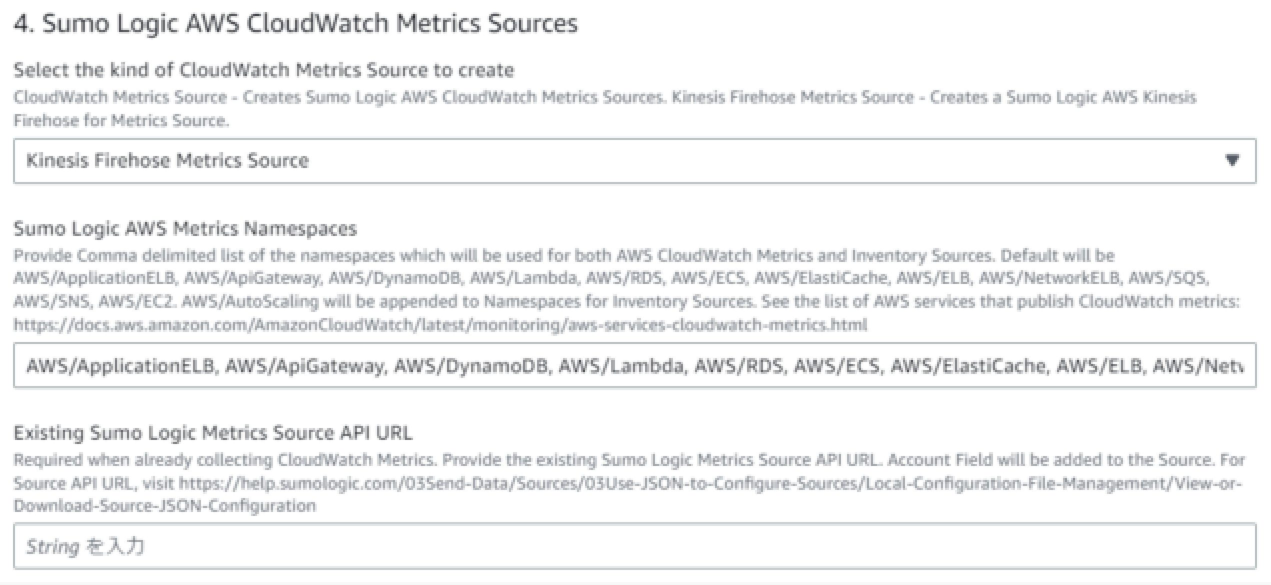
3. Sumo Logic AWS Observability Apps and Alerts

Install AWS Observability Apps and Alerts

Yes - Installs Apps (EC2, Application Load Balancer, RDS, API Gateway, Lambda, Dynamo DB, ECS, ElastiCache and NLB) and Alerts for the Sumo Logic AWS Observability Solution. All the Apps are installed in the folder 'AWS Observability'. No - Skips the installation of Apps and Alerts.

Yes ▼

If you select Yes, a dashboard will be created to visualize each resource (AWS EC2, AWS Application Load Balancer, Amazon RDS, AWS API Gateway, AWS Lambda, Amazon DynamoDB, AWS ECS, Amazon ElastiCache, Amazon Classic Load Balancer, AWS NLB, Amazon SNS, Amazon SQS) and alerts will be set up on the Sumo Logic side for observability.



4. Sumo Logic AWS CloudWatch Metrics Sources

Select the kind of CloudWatch Metrics Source to create

CloudWatch Metrics Source - Creates Sumo Logic AWS CloudWatch Metrics Sources. Kinesis Firehose Metrics Source - Creates a Sumo Logic AWS Kinesis Firehose for Metrics Source.

Kinesis Firehose Metrics Source ▼

Sumo Logic AWS Metrics Namespaces

Provide Comma delimited list of the namespaces which will be used for both AWS CloudWatch Metrics and Inventory Sources. Default will be AWS/ApplicationELB, AWS/ApiGateway, AWS/DynamoDB, AWS/Lambda, AWS/RDS, AWS/ECS, AWS/ElastiCache, AWS/ELB, AWS/NetworkELB, AWS/SQS, AWS/SNS, AWS/EC2. AWS/AutoScaling will be appended to Namespaces for Inventory Sources. See the list of AWS services that publish CloudWatch metrics: https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/aws-services-cloudwatch-metrics.html

AWS/ApplicationELB, AWS/ApiGateway, AWS/DynamoDB, AWS/Lambda, AWS/RDS, AWS/ECS, AWS/ElastiCache, AWS/ELB, AWS/Netv

Existing Sumo Logic Metrics Source API URL

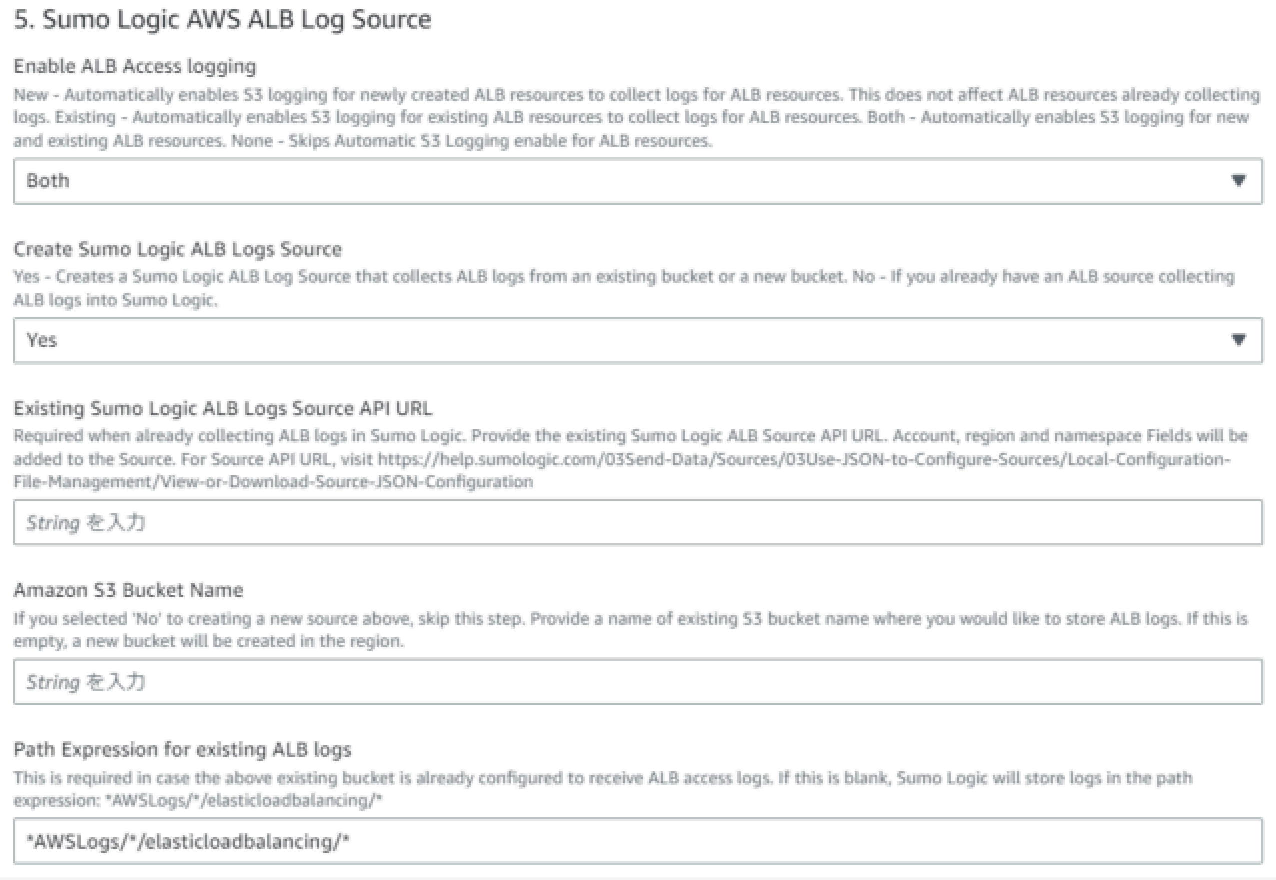
Required when already collecting CloudWatch Metrics. Provide the existing Sumo Logic Metrics Source API URL. Account Field will be added to the Source. For Source API URL, visit https://help.sumologic.com/03Send-Data/Sources/03Use-JSON-to-Configure-Sources/Local-Configuration-File-Management/View-or-Download-Source-JSON-Configuration

String を入力

Create a Sumo Logic Source to collect AWS CloudWatch Metrics data. For cost reasons, we recommend the Kinesis Firehose Metrics Source.

The Sumo Logic AWS Metrics Namespaces section sets the metric namespace, which allows you to filter out metrics you want to exclude.

In the Existing Sumo Logic Metrics Source API URL field, if you have an existing Metrics Source on the Sumo Logic side, enter its Sumo Logic API URL.



5. Sumo Logic AWS ALB Log Source

Enable ALB Access logging

New - Automatically enables S3 logging for newly created ALB resources to collect logs for ALB resources. This does not affect ALB resources already collecting logs. Existing - Automatically enables S3 logging for existing ALB resources to collect logs for ALB resources. Both - Automatically enables S3 logging for new and existing ALB resources. None - Skips Automatic S3 Logging enable for ALB resources.

Both ▼

Create Sumo Logic ALB Logs Source

Yes - Creates a Sumo Logic ALB Log Source that collects ALB logs from an existing bucket or a new bucket. No - If you already have an ALB source collecting ALB logs into Sumo Logic.

Yes ▼

Existing Sumo Logic ALB Logs Source API URL

Required when already collecting ALB logs in Sumo Logic. Provide the existing Sumo Logic ALB Source API URL. Account, region and namespace Fields will be added to the Source. For Source API URL, visit https://help.sumologic.com/03Send-Data/Sources/03Use-JSON-to-Configure-Sources/Local-Configuration-File-Management/View-or-Download-Source-JSON-Configuration

String を入力

Amazon S3 Bucket Name

If you selected 'No' to creating a new source above, skip this step. Provide a name of existing S3 bucket name where you would like to store ALB logs. If this is empty, a new bucket will be created in the region.

String を入力

Path Expression for existing ALB logs

This is required in case the above existing bucket is already configured to receive ALB access logs. If this is blank, Sumo Logic will store logs in the path expression: *AWSLogs/*/elasticloadbalancing/*

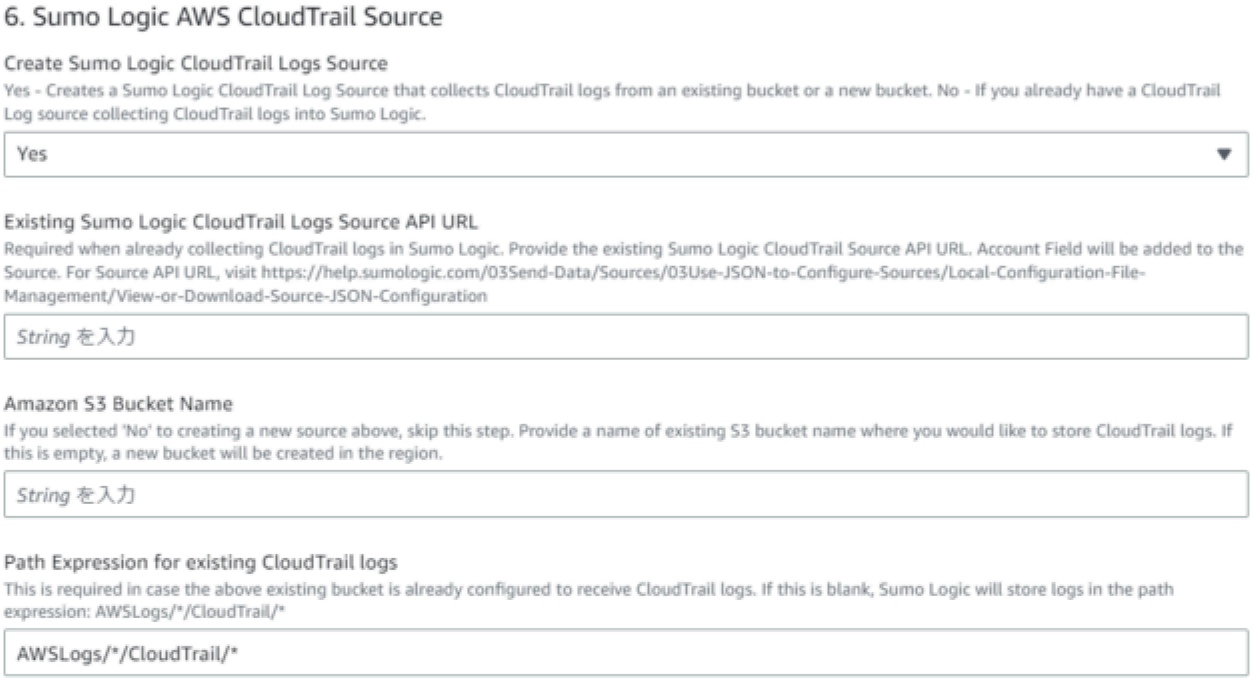
AWSLogs//elasticloadbalancing/*

Select New to collect logs for newly created ALBs, Existing to collect only existing logs, Both to collect both new and existing logs, and None to collect none.

The Create Sumo Logic ALB Logs Source item asks whether you want to create a new Source on the Sumo Logic side.

In the Existing Sumo Logic ALB Logs Source API URL field, if you have an existing Log Source on the Sumo Logic side, enter its Sumo Logic API URL.

In the Amazon S3 Bucket Name field, specify the name of an existing S3 bucket to store the ALB logs in. In the next field, Path Expression for existing ALB logs, enter the existing S3 path.



6. Sumo Logic AWS CloudTrail Source

Create Sumo Logic CloudTrail Logs Source

Yes - Creates a Sumo Logic CloudTrail Log Source that collects CloudTrail logs from an existing bucket or a new bucket. No - If you already have a CloudTrail Log source collecting CloudTrail logs into Sumo Logic.

Yes ▼

Existing Sumo Logic CloudTrail Logs Source API URL

Required when already collecting CloudTrail logs in Sumo Logic. Provide the existing Sumo Logic CloudTrail Source API URL. Account Field will be added to the Source. For Source API URL, visit https://help.sumologic.com/03Send-Data/Sources/03Use-JSON-to-Configure-Sources/Local-Configuration-File-Management/View-or-Download-Source-JSON-Configuration

String を入力

Amazon S3 Bucket Name

If you selected 'No' to creating a new source above, skip this step. Provide a name of existing S3 bucket name where you would like to store CloudTrail logs. If this is empty, a new bucket will be created in the region.

String を入力

Path Expression for existing CloudTrail logs

This is required in case the above existing bucket is already configured to receive CloudTrail logs. If this is blank, Sumo Logic will store logs in the path expression: AWSLogs/*/CloudTrail/*

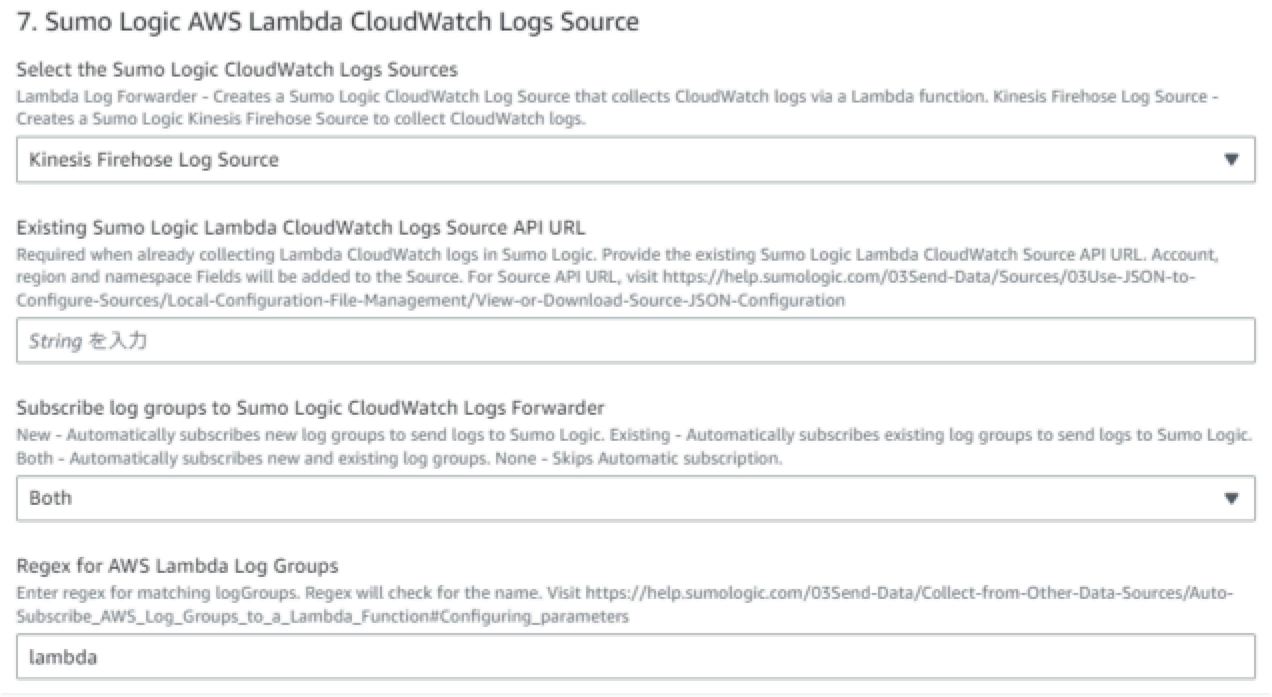
AWSLogs/*/CloudTrail/*

Sumo Logic checks to see if there is an existing CloudTrail Log Source.

In the Existing Sumo Logic CloudTrail Logs Source API URL field, if you select Yes, enter the API URL for that Log Source.

The Amazon S3 Bucket Name field specifies the name of an existing S3 bucket to store your CloudTrail logs in. Enter the existing S3 path in the next field, Path Expression for existing CloudTrail logs.

In the Existing Sumo Logic Lambda CloudWatch Logs Source API URL field, enter the Source API URL of an existing Lambda CloudWatch Source.



7. Sumo Logic AWS Lambda CloudWatch Logs Source

Select the Sumo Logic CloudWatch Logs Sources

Lambda Log Forwarder - Creates a Sumo Logic CloudWatch Log Source that collects CloudWatch logs via a Lambda function. Kinesis Firehose Log Source - Creates a Sumo Logic Kinesis Firehose Source to collect CloudWatch logs.

Kinesis Firehose Log Source ▼

Existing Sumo Logic Lambda CloudWatch Logs Source API URL

Required when already collecting Lambda CloudWatch logs in Sumo Logic. Provide the existing Sumo Logic Lambda CloudWatch Source API URL. Account, region and namespace Fields will be added to the Source. For Source API URL, visit https://help.sumologic.com/03Send-Data/Sources/03Use-JSON-to-Configure-Sources/Local-Configuration-File-Management/View-or-Download-Source-JSON-Configuration

String を入力

Subscribe log groups to Sumo Logic CloudWatch Logs Forwarder

New - Automatically subscribes new log groups to send logs to Sumo Logic. Existing - Automatically subscribes existing log groups to send logs to Sumo Logic. Both - Automatically subscribes new and existing log groups. None - Skips Automatic subscription.

Both ▼

Regex for AWS Lambda Log Groups

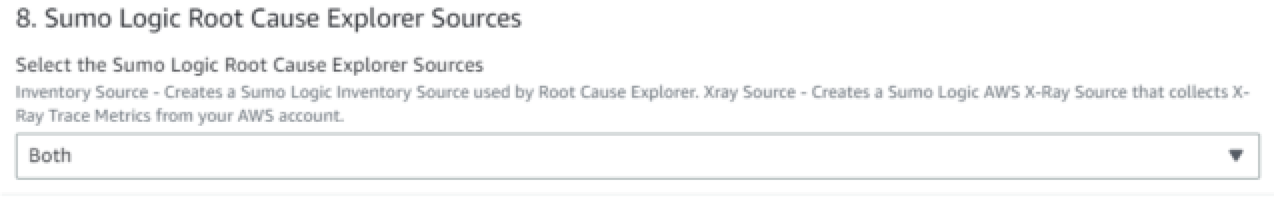
Enter regex for matching logGroups. Regex will check for the name. Visit https://help.sumologic.com/03Send-Data/Collect-from-Other-Data-Sources/Auto-Subscribe_AWS_Log_Groups_to_a_Lambda_Function#Configuring_parameters

lambda

You will be asked whether you want to create a CloudWatch Logs Source. The Lambda Log Forwarder sends logs using Lambda. The Kinesis Firehose Log Source sends logs using Kinesis Firehose as a pipeline. Both changes the Lambda Log Forwarder to a Kinesis Firehose Log Source. At this time, all log groups will be subscribed to Kinesis Firehose.

The Subscribe log groups to Sumo Logic CloudWatch Logs Forwarder item determines whether Lambda will subscribe to the log groups whose logs are collected to deploy the AWS Observability Solution. New collects only new logs, Existing collects existing logs, Both collects both new and existing logs, and None does not subscribe.

In the Regex for AWS Lambda Log Groups field, enter the regular expression that matches the log group. Refer to Configuring parameters | Sumo Logic Docs .



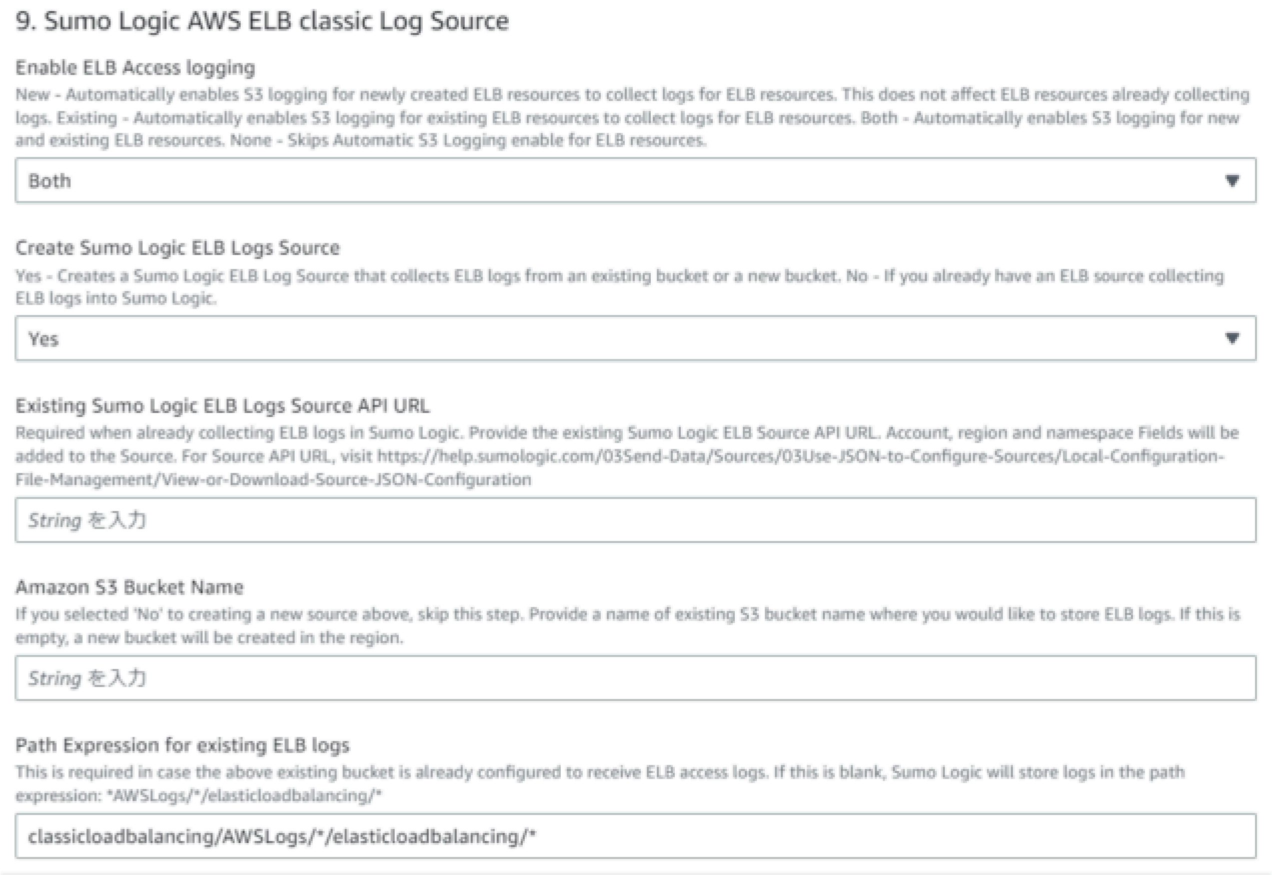
8. Sumo Logic Root Cause Explorer Sources

Select the Sumo Logic Root Cause Explorer Sources

Inventory Source - Creates a Sumo Logic Inventory Source used by Root Cause Explorer. Xray Source - Creates a Sumo Logic AWS X-Ray Source that collects X-Ray Trace Metrics from your AWS account.

Both ▼

The source type for Sumo Logic's Root Cause Explorer, a solution for quickly identifying the root cause of problems in apps and microservices, is collected by CloudWatch metrics. The source type is checked to see if it can be an Inventory Source (used to identify infrastructure spikes and throttling), an X-Ray Source (used to collect application-level metrics such as latency, throughput, and error rates; service maps can also be used), or both.



9. Sumo Logic AWS ELB classic Log Source

Enable ELB Access logging

New - Automatically enables S3 logging for newly created ELB resources to collect logs for ELB resources. This does not affect ELB resources already collecting logs. Existing - Automatically enables S3 logging for existing ELB resources to collect logs for ELB resources. Both - Automatically enables S3 logging for new and existing ELB resources. None - Skips Automatic S3 Logging enable for ELB resources.

Both ▼

Create Sumo Logic ELB Logs Source

Yes - Creates a Sumo Logic ELB Log Source that collects ELB logs from an existing bucket or a new bucket. No - If you already have an ELB source collecting ELB logs into Sumo Logic.

Yes ▼

Existing Sumo Logic ELB Logs Source API URL

Required when already collecting ELB logs in Sumo Logic. Provide the existing Sumo Logic ELB Source API URL. Account, region and namespace Fields will be added to the Source. For Source API URL, visit https://help.sumologic.com/03Send-Data/Sources/03Use-JSON-to-Configure-Sources/Local-Configuration-File-Management/View-or-Download-Source-JSON-Configuration

String を入力

Amazon S3 Bucket Name

If you selected 'No' to creating a new source above, skip this step. Provide a name of existing S3 bucket name where you would like to store ELB logs. If this is empty, a new bucket will be created in the region.

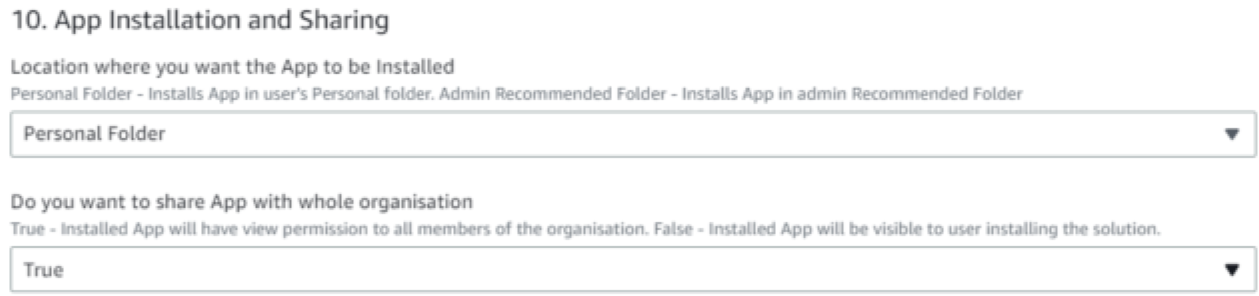
String を入力

Path Expression for existing ELB logs

This is required in case the above existing bucket is already configured to receive ELB access logs. If this is blank, Sumo Logic will store logs in the path expression: *AWSLogs/*/elasticloadbalancing/*

classicloadbalancing/AWSLogs/*/elasticloadbalancing/*

This is the CLB version of check item ⑤.



10. App Installation and Sharing

Location where you want the App to be Installed

Personal Folder - Installs App in user's Personal folder. Admin Recommended Folder - Installs App in admin Recommended Folder

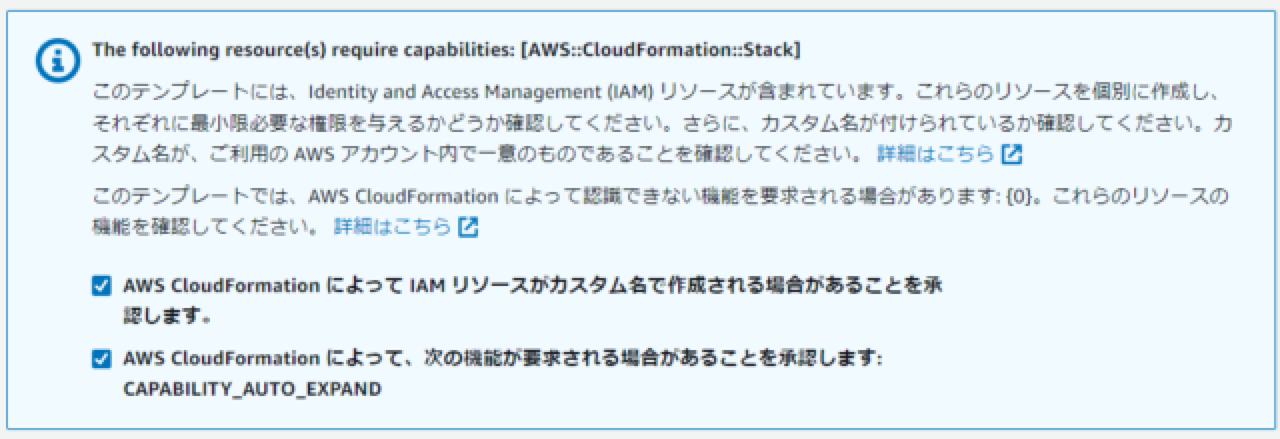
Personal Folder ▼

Do you want to share App with whole organisation

True - Installed App will have view permission to all members of the organisation. False - Installed App will be visible to user installing the solution.

True ▼

Finally, you will be asked whether you want to place the AWS Observability Solution in your personal Sumo Logic folder or in the ADMIN RECOMMENDED folder where anyone can see it. The next item also asks whether you want to grant viewing permissions to all Sumo Logic accounts.



The following resource(s) require capabilities: [AWS::CloudFormation::Stack]

このテンプレートには、Identity and Access Management (IAM) リソースが含まれています。これらのリソースを個別に作成し、それぞれに最小限必要な権限を与えるかどうか確認してください。さらに、カスタム名が付けられているか確認してください。カスタム名が、ご利用の AWS アカウント内で一意のものであることを確認してください。 詳細はこちら

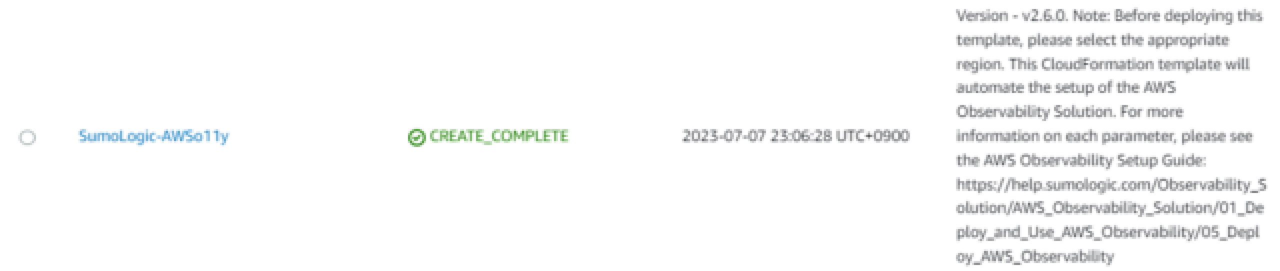
このテンプレートでは、AWS CloudFormation によって認識できない機能を要求される場合があります: {0}。これらのリソースの機能を確認してください。 詳細はこちら

☑ **AWS CloudFormation によって IAM リソースがカスタム名で作成される場合があることを承認します。**

☑ **AWS CloudFormation によって、次の機能が要求される場合があることを承認します: CAPABILITY_AUTO_EXPAND**

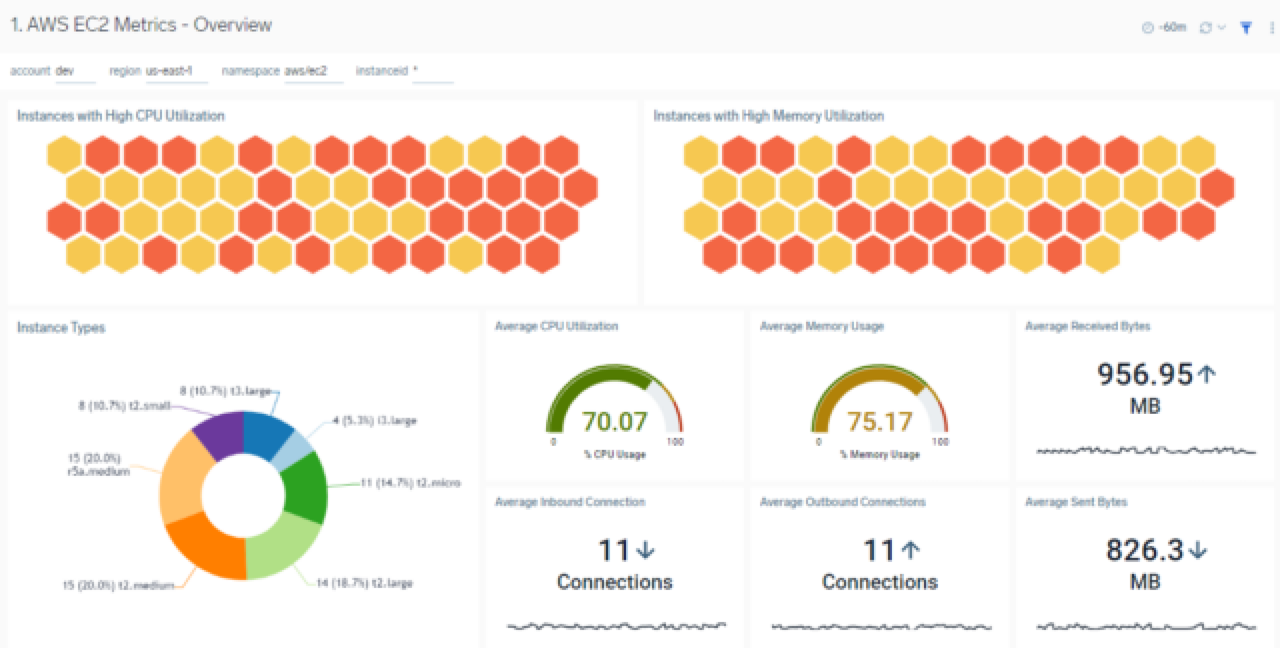
Check the checkbox to indicate your consent.

Wait for about 15 to 20 minutes, and when you see CREATE_COMPLETE as shown below, it's complete.



○ SumoLogic-AWSo11y CREATE_COMPLETE 2023-07-07 23:06:28 UTC+0900 Version - v2.6.0. Note: Before deploying this template, please select the appropriate region. This CloudFormation template will automate the setup of the AWS Observability Solution. For more information on each parameter, please see the AWS Observability Setup Guide: https://help.sumologic.com/Observability_Solution/AWS_Observability_Solution/01_Deploy_and_Use_AWS_Observability/05_Deploy_AWS_Observability

Now, you can check the Sumo Logic folder and view the data. For example, in the case of an EC2 instance, you can see the data like this without writing a complex query to view the items you need.



1. AWS EC2 Metrics - Overview

account dev region us-east-1 namespace aws/ec2 instanceid *

summary

What did you think? By deploying the AWS Observability Solution, you can visualize these key resources (AWS EC2, AWS Application Load Balancer, Amazon RDS, AWS API Gateway, AWS Lambda, Amazon DynamoDB, AWS ECS, Amazon ElastiCache, Amazon Classic Load Balancer, AWS NLB, Amazon SNS, and Amazon SQS). One of the benefits is that even if you don't have permissions on the AWS side, as long as the operator has been granted viewing permissions in their Sumo Logic account, you can check the visualized operational status like this. The setup was a bit long, so I've summarized it here. I hope it helps someone.