aws marketplace

Implementation Guide:

Sumo Logic AWS Observability for AWS Control Tower managed accounts

Table of Contents

Foreword

The Sumo Logic Solution for AWS Observability consolidates critical operational data across key AWS services and accounts to give a unified view of AWS environments.

The purpose of this AWS Implementation Guide is to enable AWS Marketplace customer to seamlessly activate, deploy and configure the Sumo Logic AWS Observability solution in AWS Control Tower environments while taking full advantage of the resources pre-configured by AWS Control Tower as part of the initialization.

Solution overview and features

The Sumo Logic Solution for AWS Control Tower is an Operational Intelligence solution that consolidates critical operational data across key AWS services and accounts to give a unified view of AWS environments. Easily navigate and search from overview dashboards into account, region, availability zone, or service specific views. Intuitive navigation across logs and metrics data enables teams to quickly resolve issues, minimize downtime, and improve system availability.
The AWS Observability solution can be used with AWS Control Tower-managed accounts to:

- **Quickly identify and resolve issues in and across multiple accounts and services.**
    - The Sumo Logic AWS Observability Solution enables teams to seamlessly navigate and search logs and metrics data from across their AWS accounts, regions, and services. Unified service and account visibility greatly speeds troubleshooting and minimizes downtime to improve overall system availability.
- **Eliminate data silos**
    - Unified logs and metrics data across AWS accounts and services eliminates data silos and makes it easier for teams to quickly identify root causes.
- **Accelerate time-to-value**
    - Streamlined setup and pre-built dashboards provide instant insights into AWS accounts and services enabling visibility into the most important data out of the box.

For the latest information on the AWS Observability solution, see the Sumo Logic documentation.

Architecture diagram

Integrating with AWS Control Tower is a two-step process where you first set up logs and metrics data collection for non-CloudTrail logs and all metrics for your AWS services by creating an AWS CloudFormation stack in individual AWS accounts managed by AWS Control Tower. In this step, you also install the apps in the Sumo Logic Observability app. Subsequently in the next step, you will set up collection of AWS CloudTrail logs that are aggregated from all AWS Control Tower-managed accounts in a centralized log archive account.

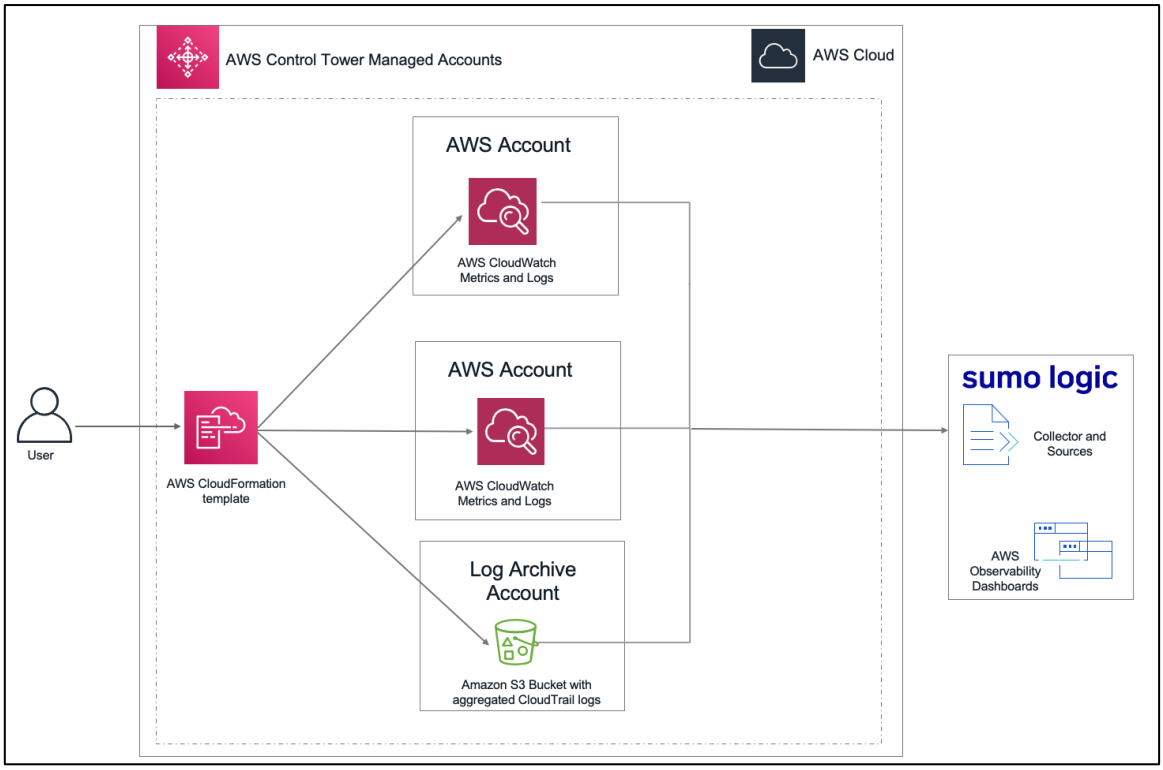
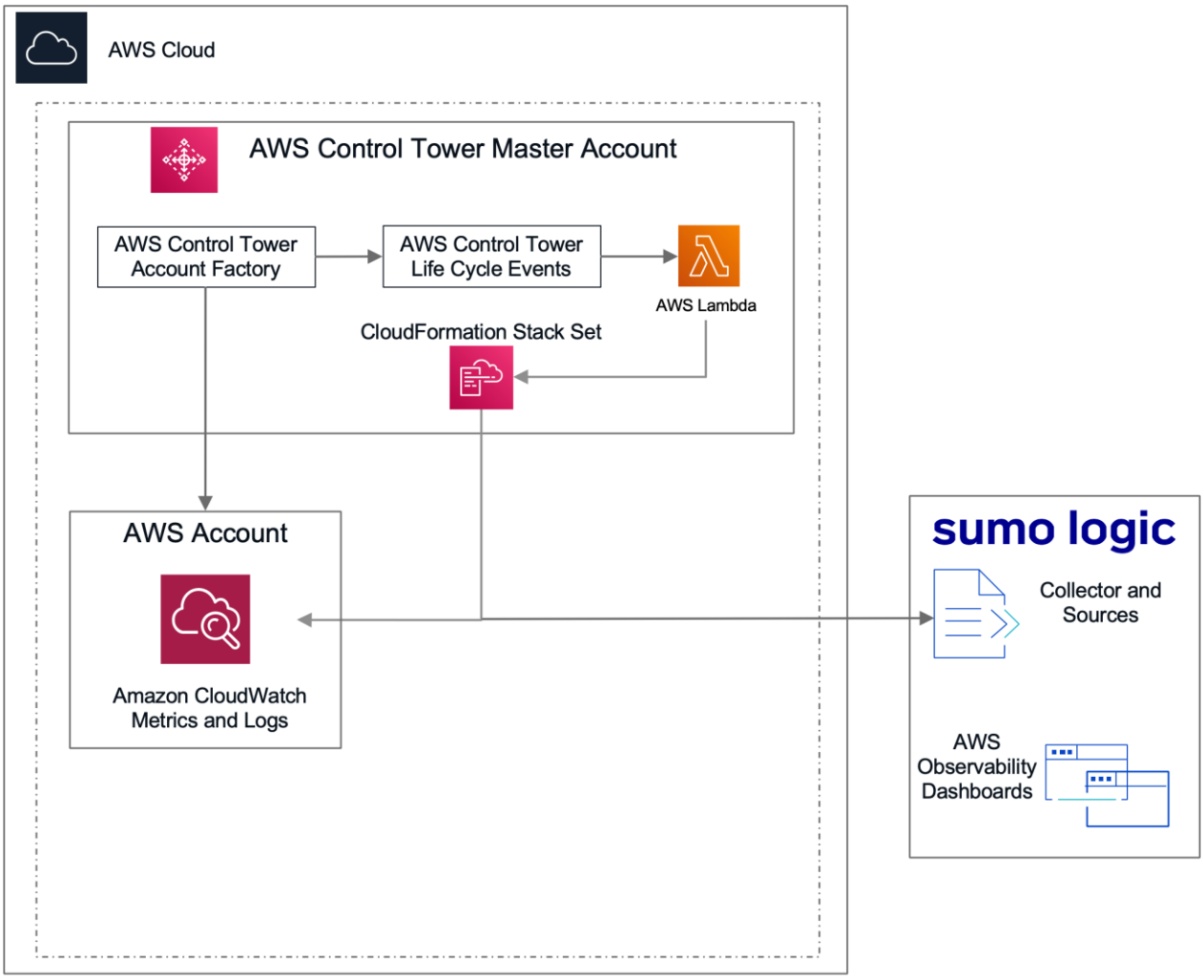


Figure 1 Sumo Logic AWS Observability for AWS Control Tower Accounts - Architecture Diagram

AWS Control Tower Life Cycle Events

For all new AWS accounts created using **AWS Control Tower Account Factory** options, the Sumo Logic AWS Observability solution can also be configured automatically using AWS Control Tower Life Cycle events. We use the CreateManagedAccount and UpdateManagedAccount life cycle events which trigger an AWS Lambda function to setup the AWS Observability Solution in the new AWS account as shown below.



Pre-requisites

Before you begin, we recommend you familiarize yourself with the AWS Observability Solution. For more information, see:

- About the AWS Observability Solution
- Set Up the AWS Observability Solution
- View the AWS Observability Dashboards

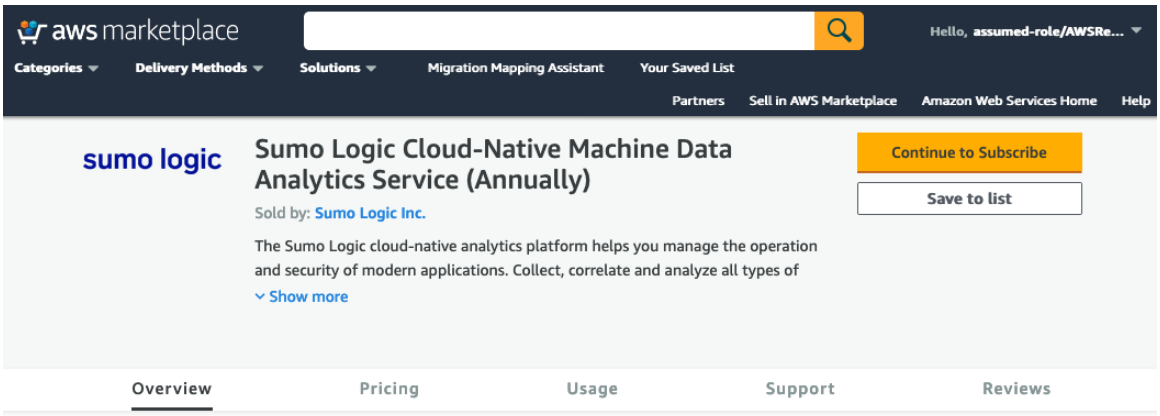
If you are new to AWS, see Getting Started with AWS: https://aws.amazon.com/getting-started/.
For additional information on AWS Marketplace, see
https://aws.amazon.com/marketplace/help/about-us?ref_=footer_nav_about_aws_marketplace.
To get started with AWS Control Tower, check out the
https://docs.aws.amazon.com/controltower/latest/userguide/getting-started-with-control-tower.html

Deployment and Configuration Steps

Step 1.1: Sign-up for a Sumo Logic account
You can sign-up for a free Sumo Logic account at:
https://www.sumologic.com/sign-up/

Step 1.2: Subscribe to the Sumo Logic Cloud-Native Machine Data Analytics Service in the AWS Marketplace

Search for the Sumo Logic Cloud-Native Machine Data Analytics Service in the AWS Marketplace (https://aws.amazon.com/marketplace/pp/B06XXVNPN2).



Click on the **Continue to Subscribe** button.

Step 1.3: Guidance on Contract Duration and Renewal

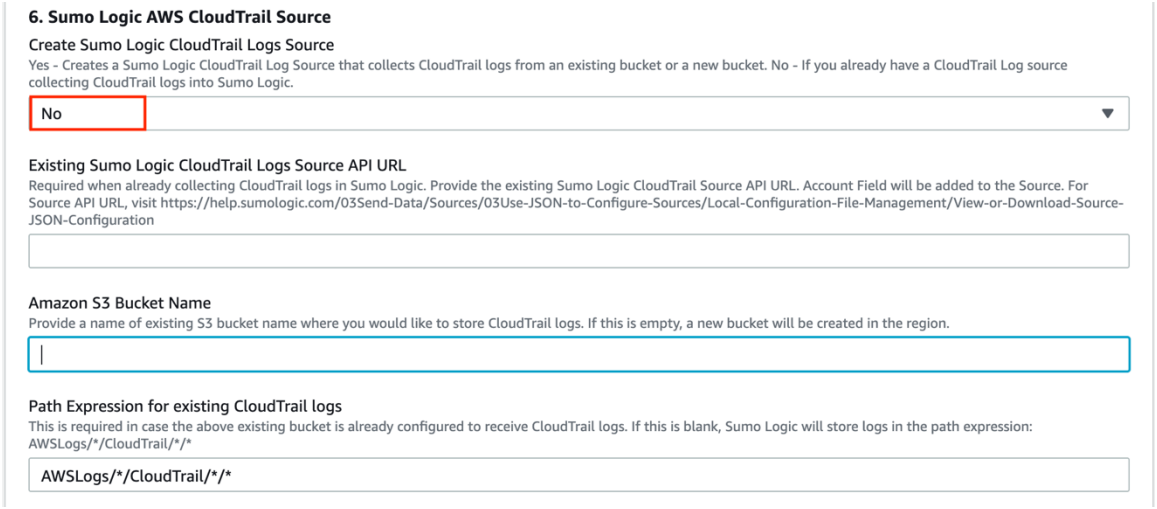
Once you are ready to purchase Sumo Logic, you select Contract Duration and daily ingestion rate in AWS Marketplace listing and click Create Contract.
You could also purchase Sumo Logic via an AWS Marketplace private offer, which gives you customized contract terms and prices. To purchase via Marketplace private offers each out to https://support.sumologic.com/hc/en-us

Step 2: Set up collection of logs and metrics data from your AWS accounts
In this step, you configure the collection of logs and metrics for all AWS accounts managed by AWS Control Tower and install the apps in the solution. To do so, follow these steps for each AWS account that is managed by AWS Control Tower.

1. To setup collection manually for **AWS Accounts created and managed via AWS Control Tower**

Log in to the AWS Management Console and follow the instructions in "Using the CloudFormation Template section" of the AWS Observability documentation to invoke and setup the AWS Observability CloudFormation template with the following caveat:

- In the "Sumo Logic AWS CloudTrail Source" section, select "No" for the question "Create Sumo Logic CloudTrail Logs Source" and keep the default values for all the other options in this section.



- Proceed to follow instructions for all other services as directed in the Configuration Prompts and Input section of the AWS Observability documentation.

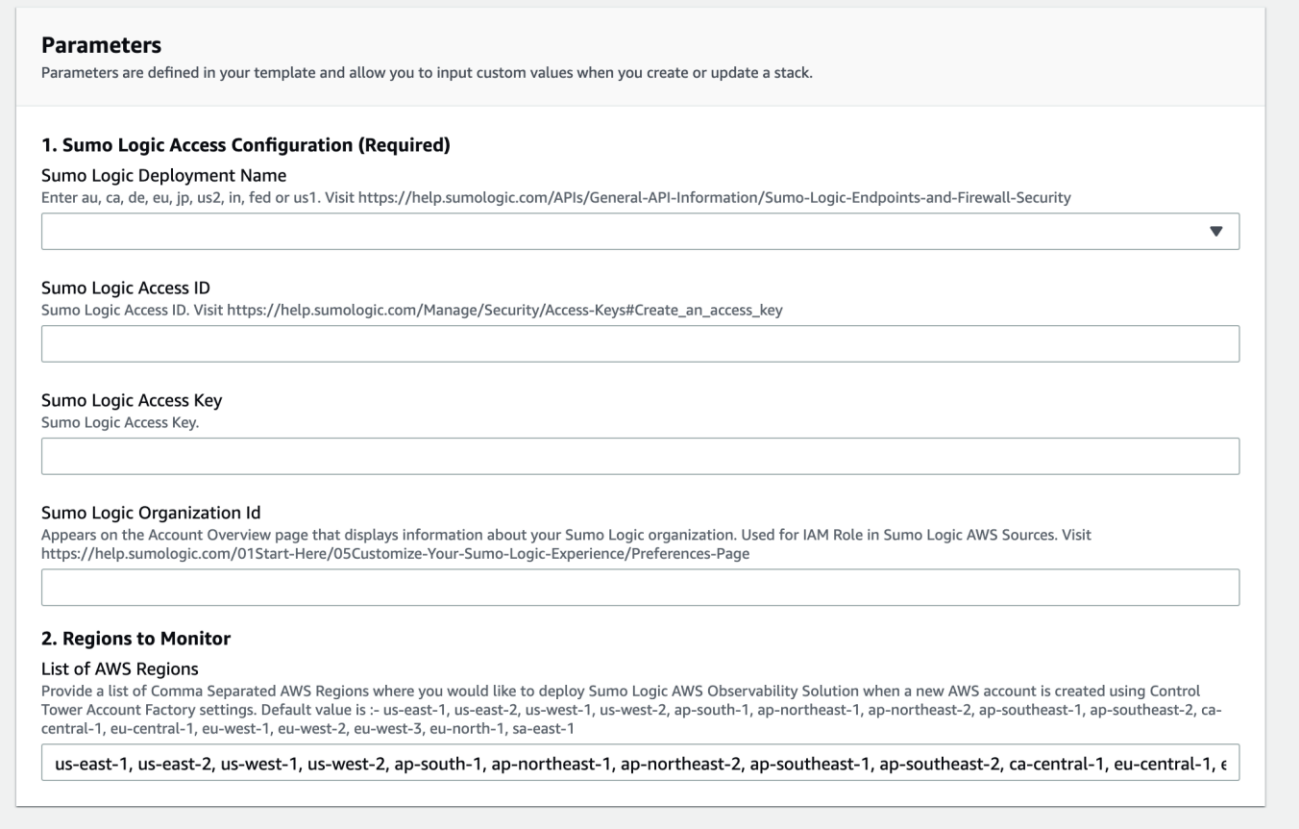
2. To automatically setup collection f**or AWS accounts created via Control Tower**

The Sumo Logic AWS Observability solution can be installed automatically to new AWS account that is created using **AWS Control Tower Account Factory** option by following the steps below:

- Log in to the AWS Master account.
- Launch the Sumo Logic CloudFormation template. Select the right region and then provide details for the prompts
    - Fill in the **Sumo Logic Access Configuration as per below guidelines**

Prompt	Guideline
Sumo Logic Deployment Name	Enter au, ca, de, eu, jp, us2, in, fed or us1. For more information on Sumo Logic deployments, see the Sumo Logic Endpoints and Firewall Security topic.
Sumo Logic Access ID	Sumo Logic Access ID. Visit.
Sumo Logic Access Key	Sumo Logic Access Key.
Sumo Logic Organization Id	You can find your org on the **Preferences** page in the Sumo Logic UI. For more information, see the Preferences Page topic. Your org ID is will be used to configure the IAM Role for Sumo Logic AWS Sources.

    - In the **Regions to Monitor** section, provide a comma separated list of AWS regions you would want AWS Observability solution to get deployed when a new AWS account is created.



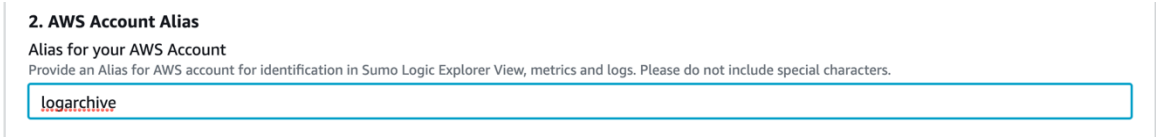
- Deploy the CloudFormation template.

Note: - CloudFormation will create a KMS Key and store the Access Key and Access ID in secret manager with the alias as CloudFormation stack name.

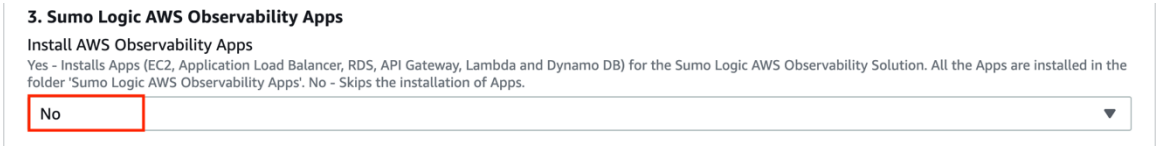
Step 3: Setup log collection from the Log Archive account

Note: In the instructions below, we assume the Log Archive AWS account is being used only for centralizing logs across AWS Control Tower-managed accounts. If this is not the case and you want to monitor AWS services in these accounts, follow the instructions in AWS Observability Solution to set up the relevant services.

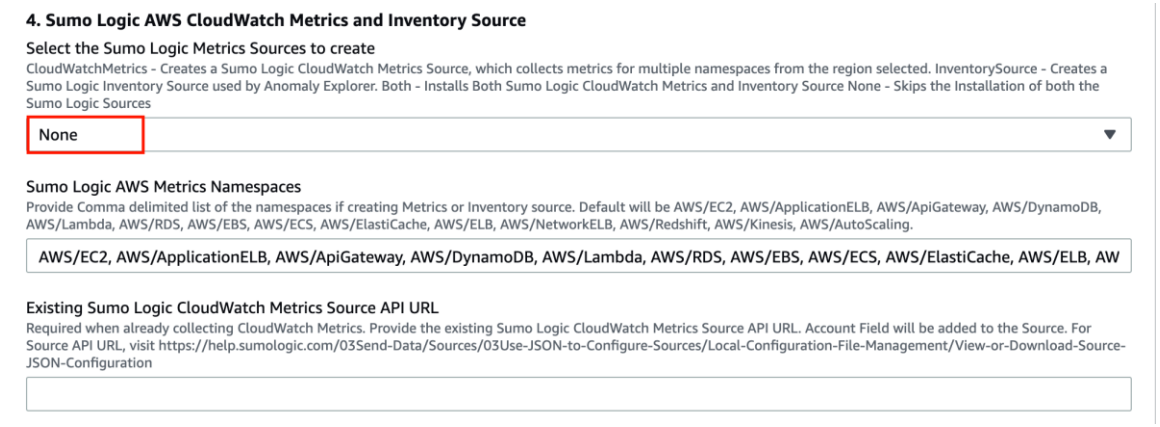
1. Log in to Log Archive account the AWS Management Console as the Log Archive AWS account user.
2. Follow the instructions in the "Using the CloudFormation Template section" of the AWS Observability documentation to launch the CloudFormation template. Please make special note of what needs to be entered in various sections called out below. (For more information, see the "Configuration Prompts and Input" section)
    1. In the **Sumo Logic Access Configuration** section of the template, fill in as required by the template.
    2. In the **AWS Account Alias** section of the template:
        - Enter "**logarchive**" as the account alias.



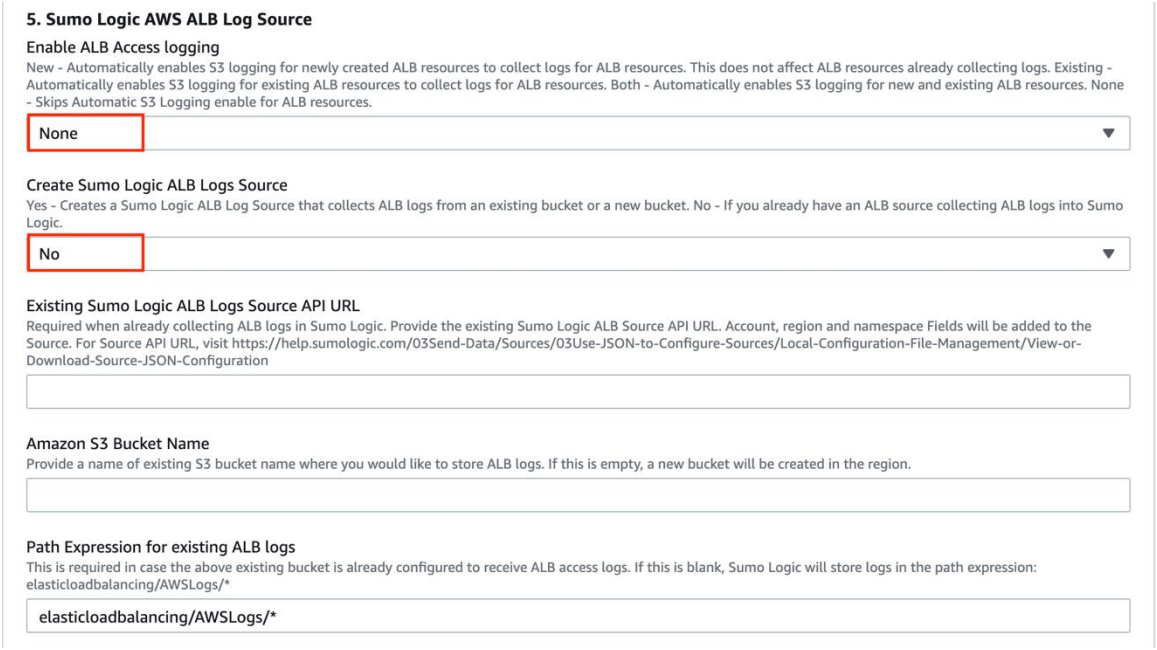
3. In the **Sumo Logic AWS Observability Apps** section of the template, select **No** for "Install AWS Observability Apps" options as they were installed in Step 2 above.



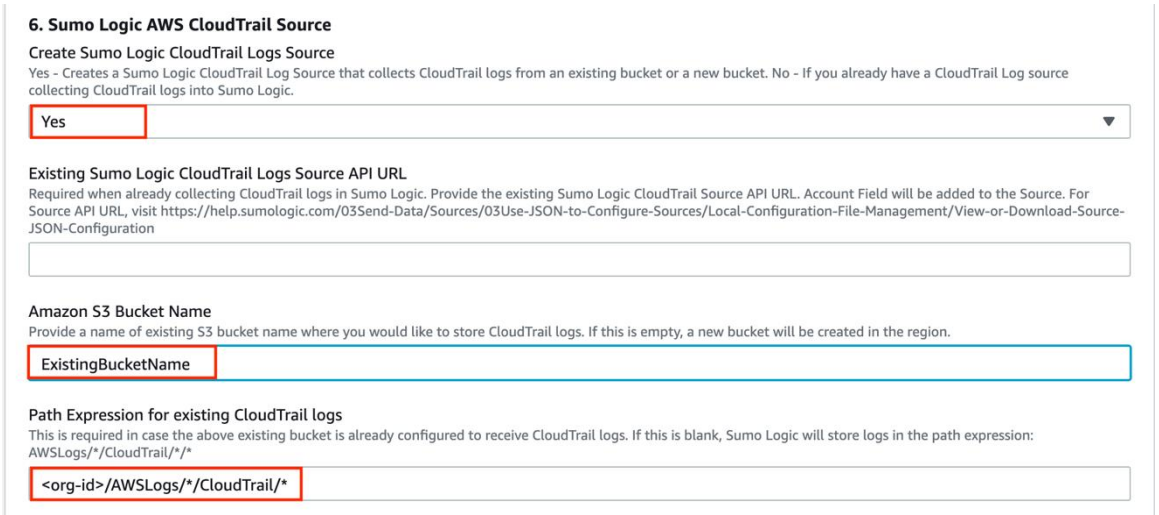
4. In the **Sumo Logic AWS CloudWatch Metrics and Inventory Source Details** section of the template, select **None** for **"Select the Sumo Logic Metrics Sources to create"**, and leave the other options blank.



5. In the **Sumo Logic AWS ALB Log Source** section of the template:
   - Set **"Enable ALB Access logging"** to **None**.
   - Set **"Create Sumo Logic ALB Logs Source"** to **No**.
   - Keep the default values for all the other options in this section



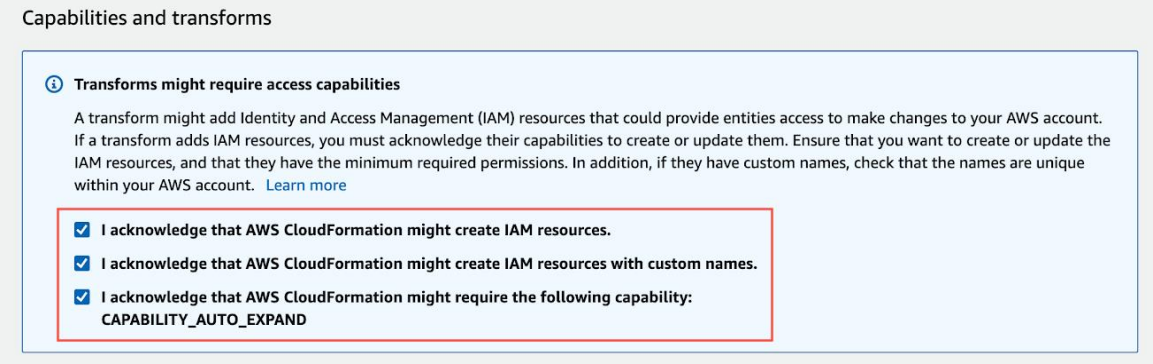
6. In the **Sumo Logic AWS CloudTrail Source** section of the template:
    - If you haven't already set up a CloudTrail source to collect data in Sumo Logic.
        - Select "**Yes**" for "**Create Sumo Logic CloudTrail Logs Source**".
        - Provide the name of CloudTrail Bucket in "**Amazon S3 Bucket Name**". Please refer to the AWS Control Tower documentation to collect the Bucket Name
        - Provide the path expression for the Logs in "**Path Expression for existing CloudTrail logs**", By default the path expression for AWS Control Tower CloudTrail logs is: <org-id>/AWSLogs/*/CloudTrail/*/*. Please replace <org-id> with the relevant AWS Organization ID.



7. In the **Sumo Logic AWS Lambda CloudWatch Logs** section of the template:
    - Select **No** for **Create Sumo Logic CloudWatch Logs Source**

8. Keep the default values in the rest of the prompts

9. Select all of the IAM checkboxes and click **Create the stack**.



Step 4: Create a Field Extraction rule

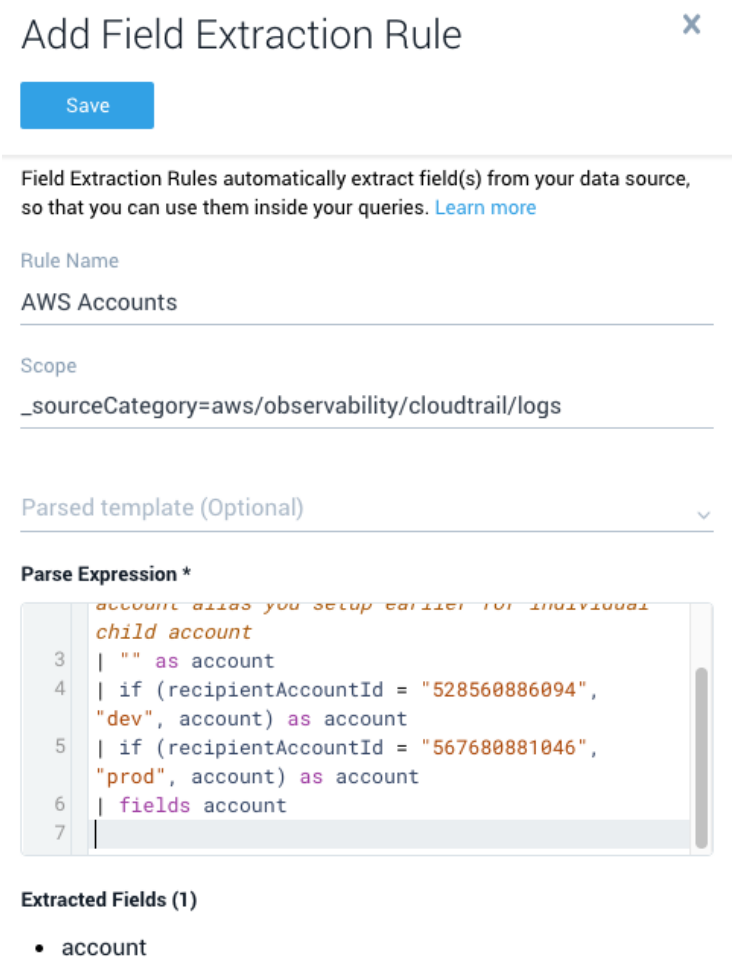
In this step, you create a Field Extraction Rule (FER) that will tag logs with the account aliases you set up for each child account in the previous step.

Log in to the Sumo Logic web UI with a supported browser, as an administrator that has the Manage Field Extractions role capability and follow the instructions in Create a Field Extraction Rule using the following values:

- **Rule Name.** AWS Accounts
- **Scope**
  - _sourceCategory=aws/observability/cloudtrail/logs
- **Parse Expression**
  - **E**nter a parse expression to create an “account” field that maps to the alias you set for each child account in the previous step. For example, if you used the “dev” alias for an AWS account with ID "528560886094" and the “prod” alias for an AWS account with ID "567680881046", your parse expression would look like:

```
| json "recipientAccountId"
// Manually map your aws account id with the AWS account alias
you setup earlier for individual child account
| "" as account
| if (recipientAccountId = "528560886094", "dev", account) as
account
| if (recipientAccountId = "567680881046", "prod", account) as
account
| fields account
```

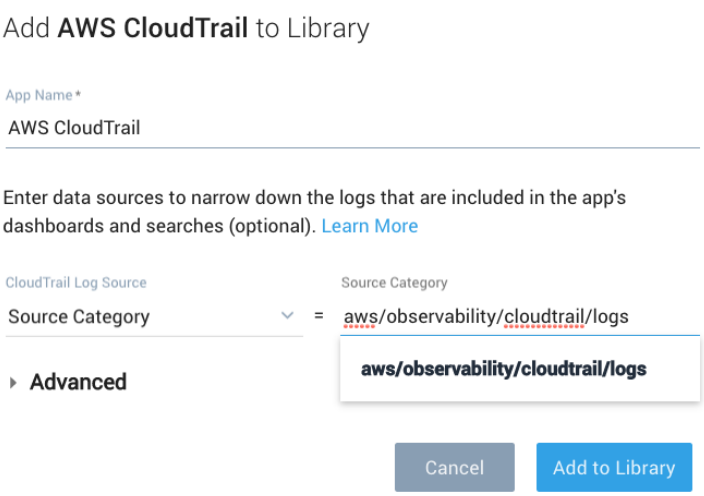
This screenshot shows for how this would look in Sumo Logic:



Step 5: View the AWS Observability dashboards
Now you can start monitoring your AWS services in various AWS Control Tower managed accounts as outlined in the AWS Observability docs**.**

Step 6: Get security insight across your AWS Control Tower managed accounts (optional)
To get instant insights into security activities including user and administrator activity, logins, network and operations security of all your AWS Control Tower managed accounts, we recommend you install the Sumo Logic app for AWS CloudTrail by following these instructions.

For the app installation section (Step 2), enter in:
- Select **Source Category** as the CloudTrail Log Source
- Enter in **aws/observability/cloudtrail/logs** as the Source Category value



Once the app is installed, you will be able to monitor AWS CloudTrail logs from all your AWS Control Tower managed accounts:

Solution Pricing

Please see the Sumo Logic Pricing page for details on pricing for Sumo Logic logs and metrics

Additional resources

- The Sumo Logic DocHub
- About the AWS Observability Solution
- Set Up the AWS Observability Solution
- View the AWS Observability Dashboards

Partner contact information

Please visit the Sumo Logic website to contact us.
https://www.sumologic.com/contact-us/