

## **Implementation Guide:**

# **Sumo Logic AWS Observability for AWS Control Tower managed accounts**

## Table of Contents

Foreword.....	3
Solution overview and features.....	4
Architecture diagram .....	4
Pre-requisites.....	5
Deployment and Configuration Steps .....	5
Solution Pricing .....	12
Additional resources .....	12
Partner contact information.....	12

## Foreword

The Sumo Logic Solution for AWS Observability pulls in 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 every 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 pulls in 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 ensures teams can 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.

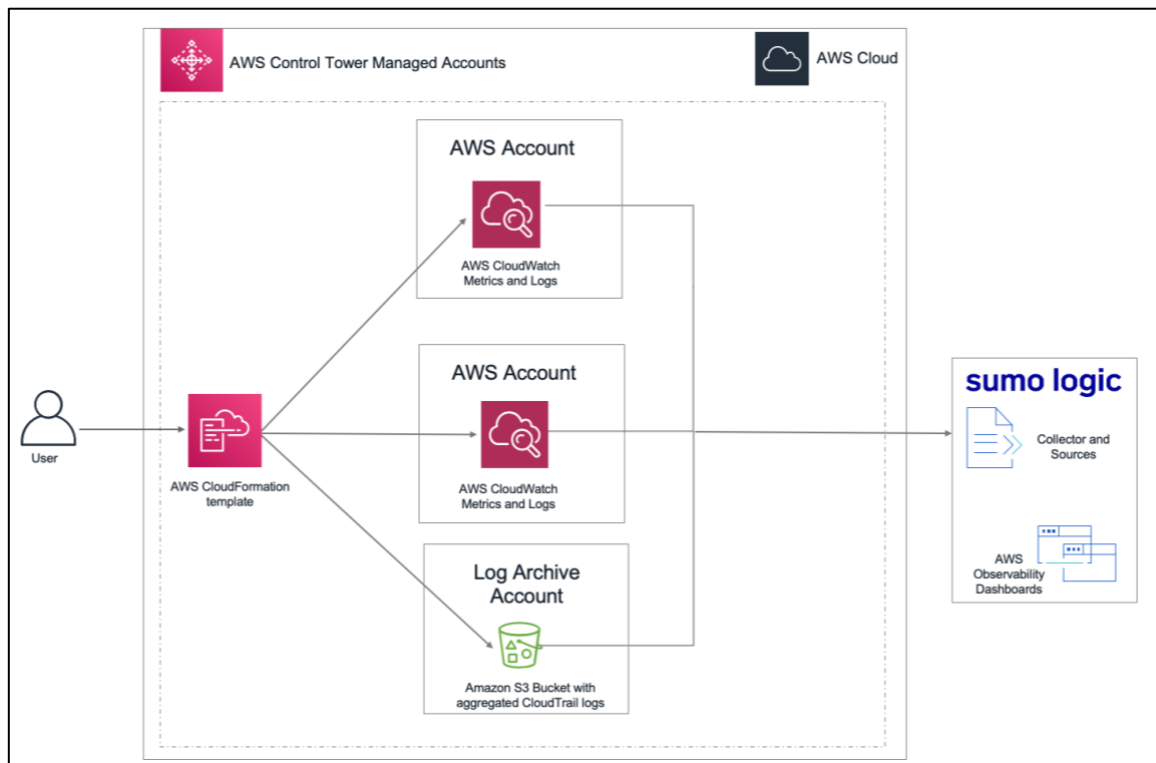


Figure 1 Sumo Logic AWS Observability for AWS Control Tower Accounts - Architecture Diagram

## 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](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>

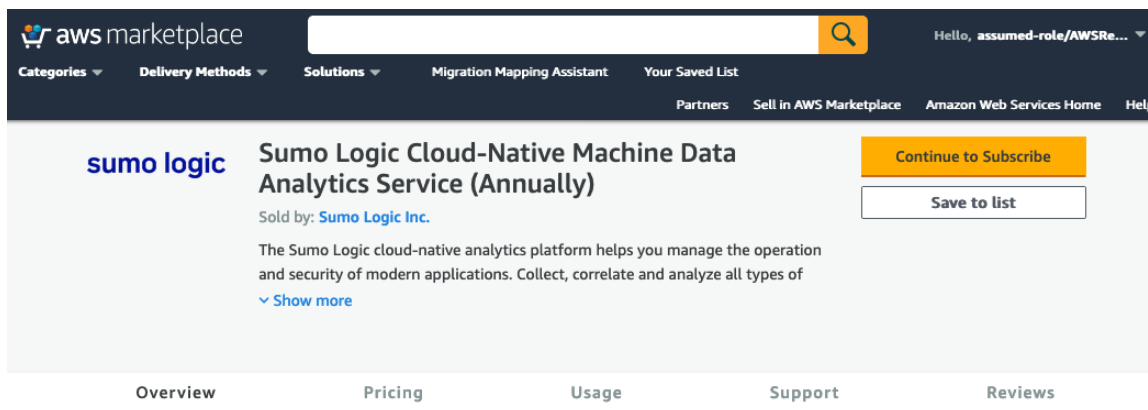
## Deployment and Configuration Steps

### Step 1.1: Sign-up for a Sumo Logic account

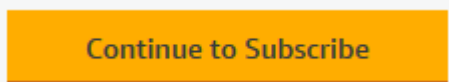
You can sign-up for a free Sumo Logic account at: <https://www.sumologic.com/sign-up/>

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

Locate 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.

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.

**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.

**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>

**Amazon S3 Bucket Name**  
 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.

**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/\*/\*

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

**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 invoke 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.

**2. AWS Account Alias**

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

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.

**3. Sumo Logic AWS Observability Apps**

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

- 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.

**4. Sumo Logic AWS CloudWatch Metrics and Inventory Source**

**Select the Sumo Logic Metrics Sources to create**  
 CloudWatchMetrics - Creates a Sumo Logic CloudWatch Metrics Source, which collects metrics for multiple namespaces from the region selected. InventorySource - Creates a Sumo Logic Inventory Source used by Anomaly Explorer. Both - Installs Both Sumo Logic CloudWatch Metrics and Inventory Source None - Skips the Installation of both the Sumo Logic Sources

**Sumo Logic AWS Metrics Namespaces**  
 Provide Comma delimited list of the namespaces if creating Metrics or Inventory source. Default will be AWS/EC2, AWS/ApplicationELB, AWS/ApiGateway, AWS/DynamoDB, AWS/Lambda, AWS/RDS, AWS/EBS, AWS/ECS, AWS/ElastiCache, AWS/ELB, AWS/NetworkELB, AWS/Redshift, AWS/Kinesis, AWS/AutoScaling.

**Existing Sumo Logic CloudWatch Metrics Source API URL**  
 Required when already collecting CloudWatch Metrics. Provide the existing Sumo Logic CloudWatch 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>

- 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

**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.

**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.

**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>

**Amazon S3 Bucket Name**  
 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.

**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: elasticloadbalancing/AWSLogs/\*

- 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.

**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.

**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>

**Amazon S3 Bucket Name**

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.

**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/\*/\*\*

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**.

Capabilities and transforms

**Transforms might require access capabilities**

A transform might add Identity and Access Management (IAM) resources that could provide entities access to make changes to your AWS account. If a transform adds IAM resources, you must acknowledge their capabilities to create or update them. Ensure that you want to create or update the IAM resources, and that they have the minimum required permissions. In addition, if they have custom names, check that the names are unique within your AWS account. [Learn more](#)

- I acknowledge that AWS CloudFormation might create IAM resources.
- I acknowledge that AWS CloudFormation might create IAM resources with custom names.
- I acknowledge that AWS CloudFormation might require the following capability: CAPABILITY\_AUTO\_EXPAND

#### 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
- **Applied At.** Ingest Time
- **Scope.** Specific Data

- **Metadata.** \_sourceCategory
- **Value.** aws/observability/cloudtrail/logs
- **Parse Expression**
  - Enter 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:

**Add Field Extraction Rule**

Save

Field Extraction Rules automatically extract field(s) from your data source, so that you can use them inside your queries. [Learn more](#)

Rule Name

**Applied At**

Ingest Time  
Typically used across data sources to extract frequently used fields in queries. The fields will be extracted and stored when data is received by Sumo Logic.

Run Time  
Use this for JSON logs to get the most flexibility in auto parsing your data. The specified fields will be extracted during the execution of a search query. [Learn more](#)

**Scope**

All Data  Specific Data

Metadata	Value
_sourcecategory	aws/observability/cloudtrail/log

[Switch To Advanced](#)

Parsed template (Optional)

**Parse Expression \***

```
1 | json "recipientAccountId"
2 // Manually map your aws account id with the AWS
3 account alias you setup earlier for individual
4 child account
5 | "" as account
6 | if (recipientAccountId = "528560886094",
7 "dev", account) as account
8 | if (recipientAccountId = "567680881046",
9 "prod", account) as account
```

**Extracted Fields (1)**

- account

### 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

Add **AWS CloudTrail** to Library

App Name \*  
AWS CloudTrail

Enter data sources to narrow down the logs that are included in the app's dashboards and searches (optional). [Learn More](#)

CloudTrail Log Source

Source Category = aws/observability/cloudtrail/logs

Source Category

aws/observability/cloudtrail/logs

▶ Advanced

Cancel Add to Library

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/>