Implementation Guide:

Logz.io Observability Platform
# Table of Contents

- Foreword 3  
- Solution overview and features 4  
- Architecture diagram 4  
- Deployment and Configuration Steps 6  
  - *Shipping Control Tower CloudTrail logs to Logz.io* 9  
  - *Creating Visualizations in Logz.io* 11  
  - *Creating a Dashboard in Logz.io* 13  
  - *Creating alerts in Logz.io* 14  
- Cleaning up 15
Foreword

The Logz.io Platform is an Observability solution that enables you to run log analysis, monitor your infrastructure and manage your Application Performance Management on the AWS cloud. Implementing this solution, you can gain observability into your systems with the world’s most popular open source observability tools— the ELK Stack, Grafana, and Jaeger—on a powerful, easy to use SaaS platform purpose-built for monitoring distributed cloud environments.

The purpose of this AWS Implementation Guide is to enable every AWS Marketplace customer to seamlessly activate, deploy and configure the Logz.io Platform in AWS Control Tower environment while taking full advantage of the resources pre-configured by AWS Control Tower as part of the initialization.
Solution overview and features

Logz.io is a cloud observability platform. At Logz.io, we believe developers are most productive when they are free to use community-driven, open-source monitoring tools such as ELK, Grafana, and Jaeger. Logz.io is on a mission to enable every developer, in every company to use the best open-source observability tools, in an easy to use, scalable and integrated way.

Modern DevOps teams need a way to simplify the job of monitoring, troubleshooting, and securing distributed cloud workloads. They need tools that are designed for modern, distributed architectures. They need fewer tools to configure and manage, not more - meaning a unified solution for logs, metrics, traces, and security data to resolve production issues and threats faster. They need a solution based on open source that delivers all the value of the community. It should fit the way they operate, not the other way around. And they need a solution that is easy to use and simplifies analytics across teams.

With Logz.io, you will benefit from the following:

✔ No Need to Learn Another SIEM | Based on the open-source ELK, fully managed. Scalability, availability, and security assured.
✔ Understand your Security Posture Within 5 Mins | Fast, easy to use, and integrates with any data source, including existing security tools.
✔ Easily Integrate Security Into Operations | Unified with operations, use the same log data for security analytics and compliance.

Architecture diagram

To effectively monitor their AWS environment, users rely on a centralized logging approach. Centralized logging entails the use of a single platform for data aggregation, processing, storage, and analysis.

- Aggregation – the collection of data from multiple sources and outputting them to a defined endpoint for processing, storage, and analysis.
- Processing – the transformation or enhancement of messages into data that can be more easily used for analysis.
- Storage – the storage of the data in a storage backend that can scale in a cost-efficient way.
- Analysis – the ability to monitor and troubleshoot with the help of search and visualization capabilities.
Pre-requisites

Logz.io Platform is a SaaS solution. As such, prerequisites are minimal. The only prerequisite is to establish a trust between Logz.io and the Amazon Simple Storage Service (Amazon S3) buckets in which the data resides.

This can be done through creating an AWS Identity and Access Management (IAM) role within your AWS account. Your AWS Control Tower data will need to be sent into a S3 bucket in order to set the ingestion channel with Logz.io native integration from the S3 bucket.

If you are new to AWS, see Getting Started with AWS: https://aws.amazon.com/getting-started/.

Figure 1 Logz.io Architecture Diagram

Figure 2 AWS -> Logz.io Flow Diagram

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

The AWS Marketplace gives access to a large variety of SaaS and API products that you can find, buy, deploy and manage the third-party software, data, services that you need to build solutions and run your businesses. One of the biggest advantages for users is the ability to benefit from an easier procurement and payment process — users can use their existing paying terms with AWS, and unify billing across all the AWS services they are consuming, including those offered in the marketplace.

Logz.io is now available on the AWS Marketplace as a SaaS product.

This means that if you’re an AWS user, you can now use Logz.io to monitor your cloud environment with a more flexible subscription mode, and:

- Use Logz.io to get visibility into various AWS services, such as Amazon CloudWatch, Amazon S3, AWS CloudTrail and Amazon Relational Database Service (Amazon RDS) using built-in integrations. Ship your data from an S3 bucket or using AWS Lambda and use built in Kibana dashboards and visualizations to start analysis.
- Use Logz.io’s alerting engine to create log-based and accurate alerts that will help you reduce alerting noise and alert fatigue.
- Leverage Logz.io’s advanced machine learning to pinpoint events taking place in your AWS environment that would otherwise have gone unnoticed.

Logz.io subscriptions are available for 1, 12 and 24 month periods, with pricing determined by the amount of data shipped daily.

To subscribe to Logz.io on the AWS Marketplace, simply search for Logz.io ELK-as-a-service or our Enterprise Edition.
Hit the **Continue to Subscribe** button.

Select the amount of data you plan on shipping to Logz.io daily and the subscription period. Please note that automatic renewal is selected and enabled by default.
Click **Create Contract**.

**Congratulations! You are now subscribed.**

Your contract is currently pending. **It may take up to 30 minutes for the payment to complete,** but you can start setting up your account immediately.

To begin using the software you will need to leave AWS Marketplace and set up your account on the Logz.io - AI-Powered ELK-as-a-Service website by clicking the button below. This page will remain open but you can revisit it any time by finding this product on **Your Software**.

> Some vendors utilize pop-up windows for product registration, so please check your browser settings to ensure pop-up windows are not blocked.

**SET UP YOUR ACCOUNT**

Your subscription is created, and you can now create your Logz.io account by clicking the Set Up Your Account button in the dialog that pops up.

If you already have a Logz.io account, you will be redirected to the application directly. If not, you will be presented with a signup page asking you to fill in your details to start using Logz.io.
Enter your details and sign up for Logz.io.

That’s all there is to it.

You can now establish the ingestion path from AWS Control Tower into Logz.io.

**Shipping Control Tower CloudTrail logs to Logz.io**

To visualize metrics, you must first connect the CloudTrail logs located in the Log Archive account’s S3 bucket to Logz.io. In your AWS account, you will create an IAM role to allow Logz.io to capture your CloudTrail logs from the S3 bucket and you will identify the S3 bucket and prefix for the logs you want to capture. The IAM role and S3 bucket information will be configured in Logz.io. To do this, follow the below steps:

1. In Logz.io, in the top bar click **Send Your Data**
2. Under **Platforms**, click **AWS** and in the drop down click **CloudTrail**
3. On the **Ship CloudTrail logs** page, scroll down to the bottom and click **+ Add a bucket** and **Authenticate with a role**

![IAM role configuration](image)

4. Logz.io will provide you an Account ID and External ID that you will use to create the IAM role in the AWS account. Log in to the Log Archive account created by Control Tower and navigate to the [IAM Management Console](https://aws.amazon.com).  
5. On the left navigation pane, click **Role** and then click **Create role**.  
6. The trusted entity will be [Another AWS account](https://aws.amazon.com).  
7. Enter the 12-digit account ID provided by Logz.io, and select **Require external ID** and enter the External ID provided to you by Logz.io. Click **Next: Permissions**.
8. **Attach the AmazonS3ReadOnlyAccess policy. Click Next: Tags**

Create role

Attach permissions policies

Choose one or more policies to attach to your new role:

- **Policy name**: AmazonS3ReadOnlyAccess
- **Used as**: Permissions policy (1)

Set permissions boundary

9. **Run through the remaining steps, enter a Role name like ControlTower-Logzio-Role and then Create role.**
10. Once the role has been created, click into the role to retrieve the Role ARN.

11. Navigate to the S3 landing page. Search for the bucket name that has the format `aws-controltower-logs-987654321012-region`. This will be the S3 bucket name.

12. To identify the S3 prefix, drill into the S3 folders, until you reach the AWS account ID and then go one file further to include CloudTrail. Your prefix will look similar to: `o-bc1defgh2j/AWSLogs/<account-ID>/CloudTrail`

13. Add the IAM and S3 information to Logz.io and click Save. Within a few minutes the CloudTrail logs from the account ID you specified will show up in Logz.io

---

**Creating Visualizations in Logz.io**

Once log events are generated within Logz.io, Logz.io will manage parsing these event logs. Some parameters that are helpful to know are:

- `eventName`: this identifies lifecycle events
- `requestParameters.evaluations.complianceType`: compliant or not compliant
- `requestParameters.organizationalUnitId`: Organizational Unit ID
- `requestParameters.organizationalUnitName`: Organization Unit Name
- `serviceEventDetails.disableGuardrailStatus.guardrails.guardrailBehavior`: preventive or detective
- `serviceEventDetails.createManagedAccountStatus.account.accountId`: account ID that has been created

To begin building visualizations:

1. Click the `Create visualization` icon on the left pane to navigate to the Visualization page. Click + Create visualization and select **Vertical Bar**.
2. To Choose a source type and select `logzioCustomerIndex`*
3. To evaluate all events generated from Control Tower, click + Add filter, in the Field drop down, type eventSource. In the Operator drop down select is. In the Value drop down type and select controltower.amazonaws.com. Click Save.

4. To add additional filters to focus on certain lifecycle events, click + Add filter, in the Field drop down, type eventName. In the Operator drop down select is one of. In the Value drop down type and enter EnableGuardrail followed by DisableGuardrail. Click Save.

5. Under Buckets, select X-axis. In the Aggregation drop down menu type and select Terms. In the Field drop down, select requestParameters.guardrailName. Click the blue Play button. This will show a visualization of all guardrails that have been enabled or disabled.
6. Once you have the parameters you are looking for in place, click **Save** on the top left and add a **Title** for your visualization and click **Confirm Save**.

*Creating a Dashboard in Logz.io*

As you create various visualizations that suit your needs, you can compile these visualizations together into a dashboard.

1. Click the 🗄️ icon to navigate to Dashboard. Click + **Create new dashboard**
2. Click **Add** on the top left to add visualizations you have saved to begin creating your dashboard.

3. After making the changes required click **Save**, give the dashboard a Title and the click **Confirm Save**.
Creating alerts in Logz.io

In addition to visualizing Control Tower events, you can create alerts to be notified when certain events take place, for example disabling a guardrail. To create this, you will navigate to the Discover page in Logz.io.

1. Add in the appropriate filters. To create an alert for disabling guardrails, filter so the eventName is DisableGuardrail. Click Create alert.

2. Enter an Alert Name, under Accounts to search select All accounts.
3. Under Trigger if... you can create a tiered triggered determining severity level depending on the number of logs in this case, or other variable of your choosing.
4. Finally, you can choose which individuals you would like to notify when an alert has been triggered by adding their email address under Who to send it to.
5. Click Save to save the alert.
Cleaning up

If you will be using the solution on a regular basis, you can leave the configuration settings that you have set up. If you would like to stop using the solution, delete the S3 bucket linked to Logz.io under Send Your Data in the Logz.io platform to avoid incurring additional charges.
Best Practices

- Ship CloudTrail logs. You'll need: s3:ListBucket and s3:GetObject permissions for the required S3 bucket
  - Send your logs to an S3 bucket - Logz.io fetches your CloudTrail logs from an S3 bucket. For help with setting up a new trail, see Overview for Creating a Trail from AWS.
  - Add the S3 bucket information - Add a bucket
    Important: Logz.io fetches logs that are generated after configuring an S3 bucket. Past logs are not sent to Logz.io.
  - Check Logz.io for your logs - Give your logs a few minutes to get from your system to ours, and then open Kibana. If you still don't see your logs, see log shipping troubleshooting.

Solution Estimated Pricing

For more information about Logz.io’s pricing, please visit this page:
https://logz.io/pricing/

FAQs

- for any question, please contact our Support team: https://support.logz.io/

Additional resources

- For more blogs from Logz.io: https://logz.io/blog
- Case Studies: https://logz.io/case-studies
- Documentation (APIs, Shipping methods, Examples): https://docs.logz.io

Partner contact information

- Sales & Customer Support
  - sales@logz.io
  - help@logz.io
- General Information
  - info@logz.io