

Implementation Guide:

Multi-account AWS cloud monitoring and analytics
with Cribl and AWS Control Tower



Table of Contents

Foreword	3
Solution overview and features	3
Architecture diagram	4
Deployment and Configuration Steps	5
Step 1: Cribl LogStream - Initial Setup	5
Step 2: AWS Setup – AWS Control Tower management account	5
Step 3: Test - Create a Lifecycle Event - Add a managed account	6
Step 4: View the Cribl LogStream Monitoring Dashboard	6
Solution Estimated Pricing	7
FAQs	7
Additional resources	7
Partner contact information	7

Foreword

Cribl LogStream is a purpose-built streaming pipeline for logs, metrics, and observability data. LogStream helps you implement what we call an observability pipeline, which allows you to route machine data from any source to any destination while transforming your data in motion to enrich it with additional context, secure its contents, and control costs. Parse, restructure, and enrich data in flight. Get the right data, where you want, in the formats you need.

This Implementation Guide describes how AWS Marketplace customers can deploy Cribl LogStream automatically when creating new accounts with AWS Control Tower.

Solution overview and features

By bringing together data from every account in your company's AWS environment Cribl LogStream provides a simplified approach to collect data generated in AWS and send it into any relevant destination. Through a purpose built observability pipeline, data can freely flow to an S3 bucket for long term retention and a log analytics platform avoiding vendor lock-in to any specific analytics platform.

This template provisions infrastructure in the Control Tower management account that allows creation of a Cribl LogStream single instance in a Control Tower managed accounts whenever a new Control Tower managed account is added.

- Creates a Cribl Stackset in the Control Tower management account
- Provisions an Amazon CloudWatch Events Rule that is triggered based on a Control Tower Lifecycle Event
- Provisions a Lifecycle Lambda as a target for the CloudWatch Events Rule
- The Lifecycle Lambda deploys a Cribl LogStream stack in the newly added Control Tower managed account--thus placing that account under Cribl management

Architecture diagram

The solution is deployed using AWS CloudFormation templates and integrates with AWS Control Tower Lifecycle events. When a new account is created, or an existing one is enrolled using the AWS Control Tower Account Factory, the Lifecycle event triggers an AWS Lambda function. The Lambda function creates a new CloudFormation stack instance in the vended account, creating the required an AWS Identity and Access Management (IAM) role in the newly vended account.

The stack instance also configures Cribl LogStream to use the IAM role to collect account data from IAM, resource id/tags, and CloudTrail logs from the new account. See the documentation [here](#) for more details.

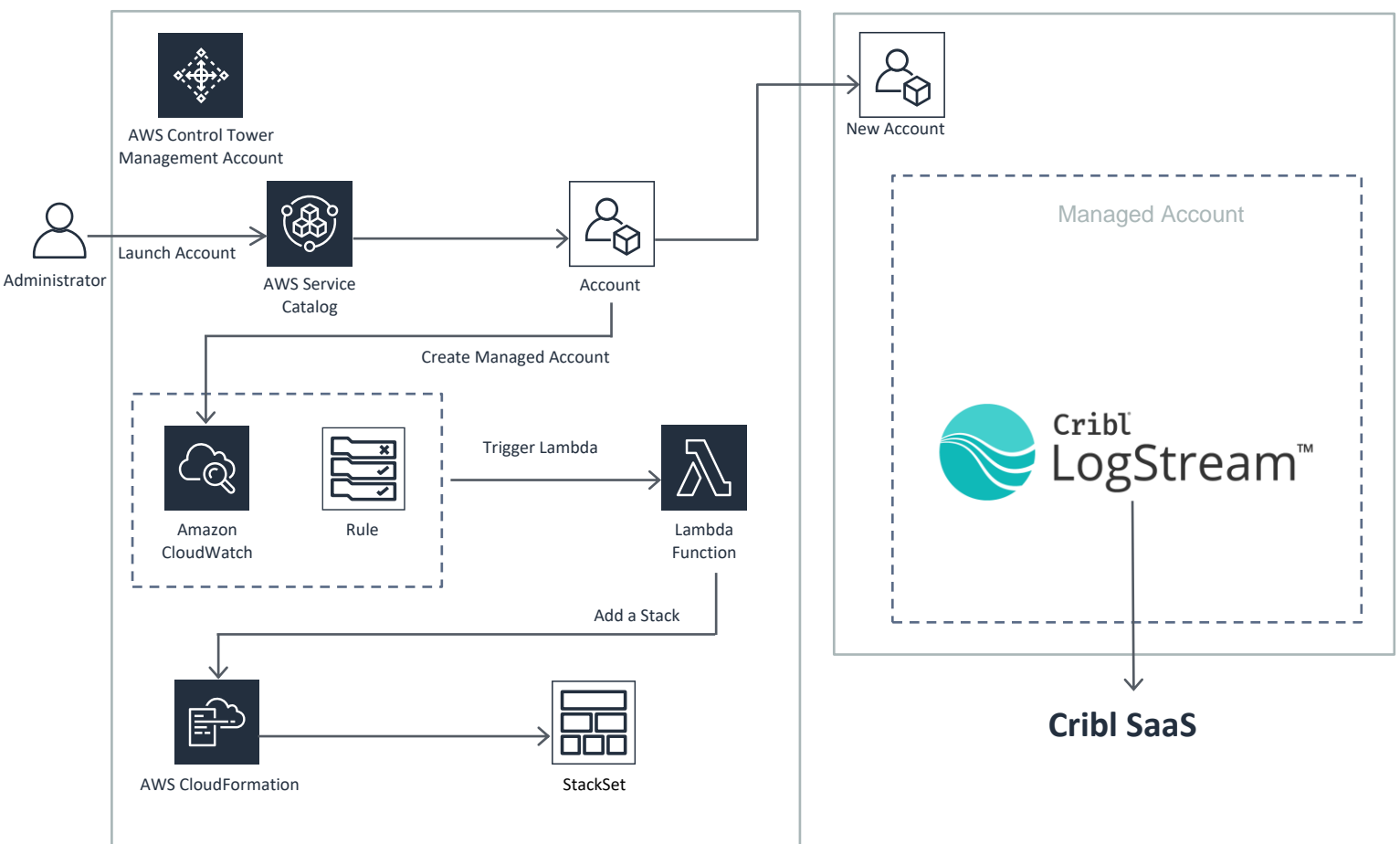


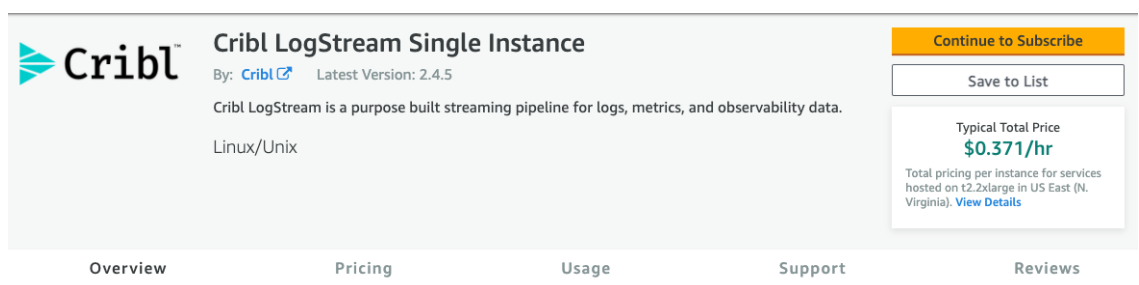
Figure 1 Cribl LogStream Architecture Diagram

Deployment and Configuration Steps

The solution can be found in the [Cribl Control Tower GitHub repository](#). It uses two AWS CloudFormation templates that you will deploy in your AWS Control Tower management account. These templates include all the components required to integrate Cribl LogStream with new AWS accounts that you create using the AWS Control Tower Account Factory.

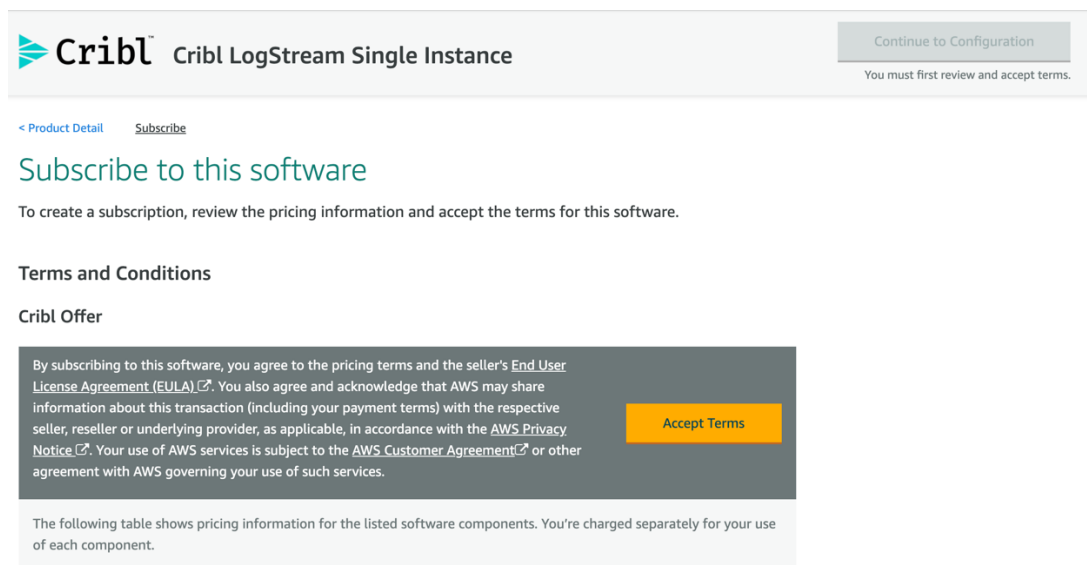
Step 1: Cribl LogStream - Initial Setup

1. Subscribe to Cribl LogStream via the [AWS Marketplace](#)
 - a. From [AWS Marketplace](#), choose **Continue to Subscribe**



The screenshot shows the AWS Marketplace product page for Cribl LogStream Single Instance. The product name is "Cribl LogStream Single Instance" by Cribl, with the latest version being 2.4.5. The description states it is a purpose-built streaming pipeline for logs, metrics, and observability data, running on Linux/Unix. A prominent orange button labeled "Continue to Subscribe" is visible in the top right corner. Below it is a "Save to List" button. A pricing box indicates a "Typical Total Price" of \$0.371/hr, with a note that this is for services hosted on t2.xlarge in US East (N. Virginia). At the bottom, there are navigation tabs for Overview, Pricing, Usage, Support, and Reviews.

- b. Click **Accept Terms**



The screenshot shows the "Accept Terms" screen for Cribl LogStream Single Instance. At the top right, there is a "Continue to Configuration" button with the text "You must first review and accept terms." Below this, there are links for "< Product Detail" and "Subscribe". The main heading is "Subscribe to this software". A sub-heading reads "To create a subscription, review the pricing information and accept the terms for this software." Under the heading "Terms and Conditions", there is a "Cribl Offer" section. A dark grey box contains the following text: "By subscribing to this software, you agree to the pricing terms and the seller's End User License Agreement (EULA). You also agree and acknowledge that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the AWS Privacy Notice. Your use of AWS services is subject to the AWS Customer Agreement or other agreement with AWS governing your use of such services." To the right of this text is an orange "Accept Terms" button. Below this box, a note states: "The following table shows pricing information for the listed software components. You're charged separately for your use of each component."

Step 2: AWS Setup – AWS Control Tower management account

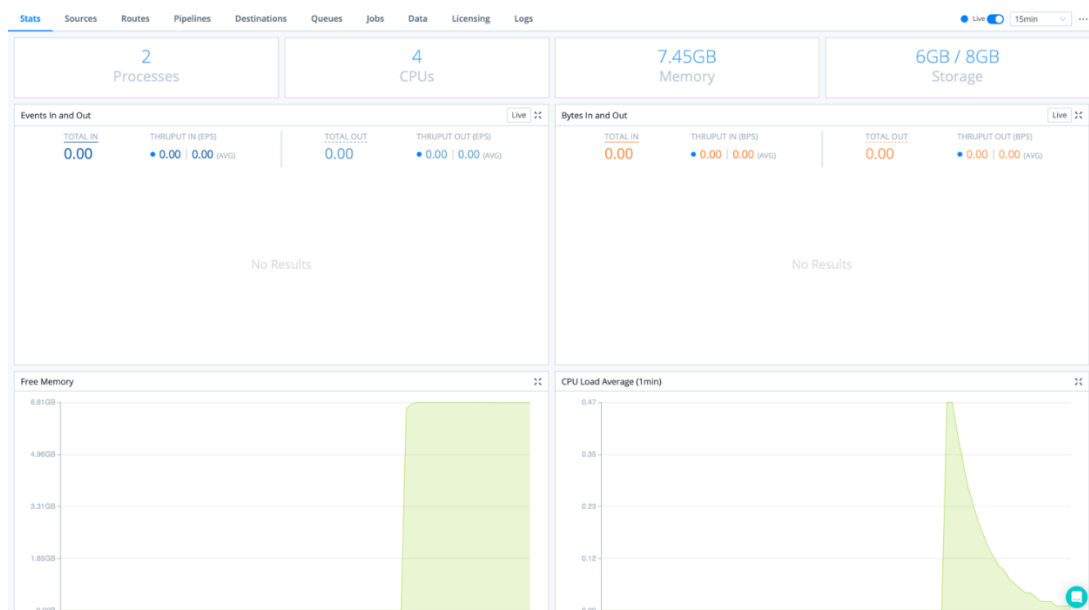
1. Launch the [aws-cribl-controltower.yml](#) template in the AWS Control Tower Managed account
 - a. Ensure that an AWS CloudFormation StackSet is successfully created
 - b. Ensure that an Amazon CloudWatch Events rule is successfully created with a Lambda target to handle Control Tower lifecycle events

Step 3: Test - Create a Lifecycle Event - Add a managed account

1. From the AWS Control Tower Master Account:
 - a. Use Account Factory or quick provision or AWS Service Catalog to create a new managed account in the AWS Control Tower Organization OR
 - b. Use AWS Service Catalog (AccountFactory Product) to update an existing managed account - e.g., change the OU of an existing managed account
 - c. This can take up to 30 mins for the account to be successfully created and the AWS Control Tower Lifecycle Event to trigger
 - d. Login to the AWS Control Tower managed account
 - i. Validate that an AWS CloudFormation stack instance has been provisioned that launches the Cribl LogStream single instance template in the managed account

Step 4: View the Cribl LogStream Monitoring Dashboard

1. After you log into your single instance, you can either navigate to <http://<instance>:9000/dashboard/stats> or click on the Monitoring link in the navigation bar



Solution Estimated Pricing

Contact [Cribl Team](#) to learn more.

FAQs

You can find a list of FAQs for the Cribl LogStream AWS Integration in our documentation [here](#).

Additional resources

- [Cribl AWS Solutions page](#)
- [Cribl AWS Sources page](#)
- [Cribl AWS Destinations page](#)

Partner contact information

For general inquiries, contact info@cribl.io.