

Implementation Guide:

Automate Tigera Calico Cloud and Amazon Elastic Kubernetes Service (EKS) clusters Integration using AWS Control Tower



TIGERA
Leader in Kubernetes Security and Observability

Table of Contents

Foreword	3
Solution overview and features	4
Architecture diagram	5
Pre-requisites	6
Deployment and Configuration Steps	7
Step 1: Subscribe to Calico Cloud on AWS Marketplace.	7
Step 2: Set up Additional configuration	9
Step 3: Deploy Calico Control Tower Integration Solution	10
Step 4: Verify EKS Cluster is connected in Calico Cloud	10
Solution Estimated Pricing	11
Additional resources	12
How to contact Tigera?	12

Foreword

Calico Cloud is a pay-as-you-go managed service to deploy a standard set of cloud workload access controls, enforce security policies consistently, ensure compliance, get end-to-end observability, and troubleshoot applications across multi-cluster and multi-cloud Kubernetes environments. It scales automatically with managed clusters to ensure security, continuous compliance, and uninterrupted real-time observability. With Calico Cloud, users get security and observability as-a-service for containers, cloud and Kubernetes in a usage-based pricing model and only pay for the services consumed. The service is up and running within minutes and works with any Kubernetes distribution across any cloud.

The purpose of this AWS Implementation Guide is to enable every AWS Marketplace customer to seamlessly activate, deploy and configure the Calico Cloud 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

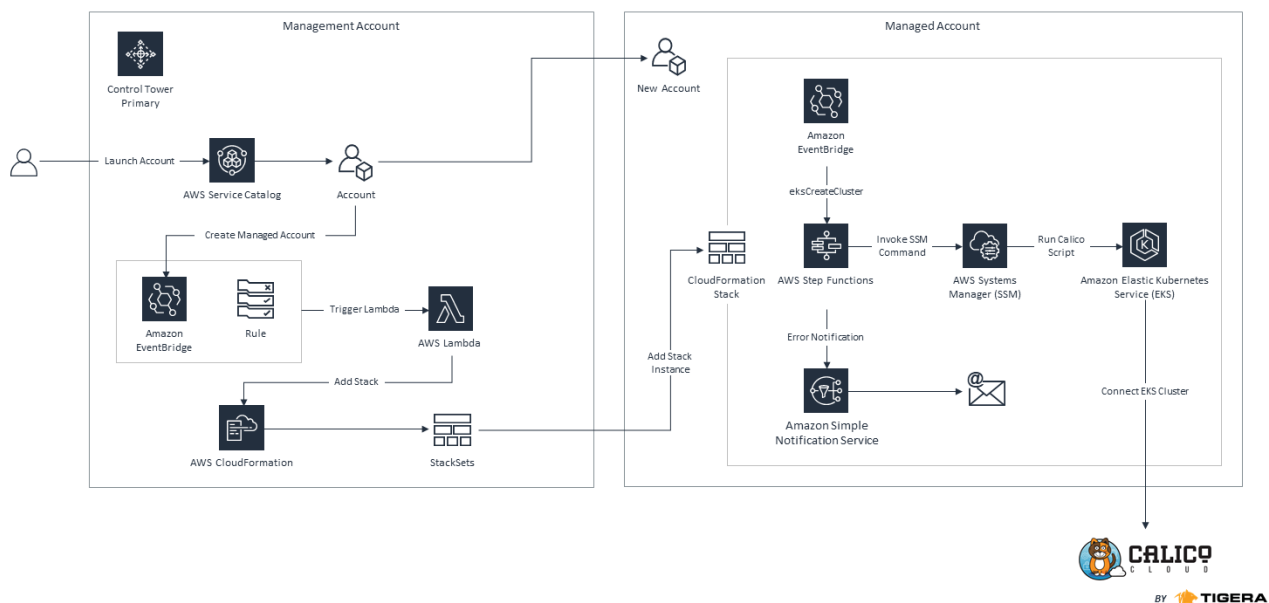
Calico Cloud is a pay-as-you-go security and observability SaaS platform for containers, Kubernetes, and cloud. Instead of managing a platform for container and Kubernetes security and observability, teams consume it as a managed service for faster analysis, relevant actions, and end results. They get an understanding of the microservices dependencies, the way to manage, analyze, and troubleshoot performance hotspots, connectivity, and detect anomalies without going through an extensive setup and deployment process. With Calico Cloud, users only pay for services consumed and are billed monthly, getting immediate value without upfront investment.

With Calico Cloud, you can:

- ✓ **Cloud Workload Access Controls:** Limits access to & from external endpoints on a "per-pod" basis that includes microservices, cloud DBs, cloud services, APIs, & legacy apps. Provides defense-in-depth protection at host, container/VM, & app level.
- ✓ **Security & Compliance:** Encrypts data-in-transit & provides intrusion detection. Detects anomalies & generates policy recommendations to be applied in milliseconds to remedy & prevent future attacks.
- ✓ **Observability & Troubleshooting:** Enable live microservices, workloads and namespace communication view and faster troubleshooting of Kubernetes workloads and applications with Dynamic Service Graph, Dynamic Packet Capture, anomaly detection, and performance hotspots, leading to shorter time-to-resolution, less application downtime, and improved quality of service

Architecture diagram

Calico Cloud with AWS control tower aims to automate the process of connecting an EKS cluster to Calico Cloud. This solution provides an event-driven automation to connect an EKS cluster with Calico cloud. The ControlTowerCalicocloudStack will be deployed in the Control Tower management account. This will create a StackSet in the management account. On every new account creation, a CloudFormation stack will be deployed in the new account via StackSet. The CloudFormation stack in individual account(s) will deploy the resources required for Calico Cloud automation.



As a part of this solution, the following resources will be created:

- **Kubernetes admin IAM role:** This is the IAM role that needs to be updated in AWS-auth configmap of kubernetes cluster. ARN for this role is available as output of CloudFormation template.
- **Event bridge rule:** An event rule is created to capture EKS CreateCluster event. This rule then triggers the state machine to initiate the automation.
- **State machine:** This state machine will orchestrate the automation of connecting eks cluster to calico cloud. As part of this automation, a node group is added to EKS cluster as pods will be deployed. Then it uses AWS Systems Manager to run command on eks nodes to run the calico script.
- **SNS Topic:** This SNS topic will be used to send the success or failure notification of calico cloud connection by state machine. Options to subscribe to one email address is available via CloudFormation parameters. Subscriptions can be added as needed after deployment as well.

CloudFormation Parameters

- CalicocloudKubeAdminRoleName: Role name for kubernetes admin role that needs to be added in AWS-auth configmap.
- CalicocloudScriptUrl: The calico cloud installs script URL.
- CalicocloudStateMachineName: State machine name, which orchestrates the automation.
- StateMachineLogRetention: State machine log retention period.
- NodeGroupRolePrefix: EKS node group role name prefix value. The node group role name would be <NodeGroupRolePrefix>-<ClusterName>-role.
- NodeGroupInstanceType: EKS node group instance type. Default: m5.large
- NodeGroupSize: Desired size for EKS node group, Default: 1
- EventFilterTagKey Tag key name to filter event for EKS cluster creation.
- EventFilterTagValue Tag key value to filter event for EKS cluster creation.
- NotificationEmailAddress: This is an optional parameter. If an email address is provided, then a SNS subscription will be created for the state machine execution status.

Pre-requisites

In order to be able to perform operation on Kubernetes, required by the calico script, this solution would need to get admin access on Kubernetes. This solution creates an IAM role that is used to perform operations on Kubernetes. Access to Kubernetes is managed via configmap; more details available [here](#). Adding access for an additional IAM role is supported by creating EKS cluster using [Amazon quickstart eks cluster](#) CloudFormation resource or [AWS CDK](#) currently. Users of this solution would need to have an automated way of getting that IAM role added as system:masters in AWS-auth configmap at the time of EKS cluster creation. If you create an EKS cluster from AWS Console or through other ways where the required IAM role is not added to configmap with cluster creation, this solution will not work.

Before you implement this solution, we recommend that you become familiar with AWS Control Tower

If you are new to AWS, see [Getting Started with AWS](#)

For [additional information](#) on AWS Marketplace

To get started with AWS Control Tower, check out the [Control Tower User Guide](#)

Deployment and Configuration Steps

Step 1: Subscribe to Calico Cloud on AWS Marketplace.

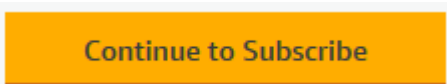
Locate the **Calico Cloud** in the [AWS Marketplace](#)

Direct link: [Calico Cloud on AWS](#)

The screenshot shows the AWS Marketplace product page for Calico Cloud. The header includes the AWS Marketplace logo, navigation menus, and a search bar. The main content area features the product title "Calico Cloud: SaaS for Kubernetes Security & Observability" with a "Continue to Subscribe" button and a "Save to list" link. Below the title is a description of the product, its benefits, and a list of features. A "Product Overview" section provides more details, and a "Highlights" box lists key features. At the bottom, there is a table with product details.

Sold by	Tigera Inc.
Product Video	See product video
Fulfillment Method	Software as a Service (SaaS)

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



Guidance on Contract Duration and Renewal <might vary for each partner>

On the new screen, you can configure your contract. You can select the **Contract Duration** and set the **Renewal Settings**.

Configure your Software Contract

Choose the contract that suits your needs. You're charged for your purchase on your AWS bill. After you purchase a contract, you're directed to the vendor's site to complete setup and begin using this software. For any software use beyond your contract limit, you're charged consumption pricing.

How long do you want your contract to run?

1 month

Renewal Settings

Auto Renew when this contract ends on - Sun Nov 28 2021?

Yes
 No

I understand that when I renew, the seller's pricing terms and end user license agreement (EULA) might have changed. On the renewal date, I will be billed based on the price and EULA applicable on that date, which I can find on the Your Marketplace Software page.

Select Contract Options

Select the Contract Options to be activated with your contract.

Configure your Software Contract

Choose the contract that suits your needs. You're charged for your purchase on your AWS bill. After you purchase a contract, you're directed to the vendor's site to complete setup and begin using this software. For any software use beyond your contract limit, you're charged consumption pricing.

How long do you want your contract to run?

1 month

Renewal Settings

Auto Renew when this contract ends on - Sun Nov 28 2021?

Yes
 No

I understand that when I renew, the seller's pricing terms and end user license agreement (EULA) might have changed. On the renewal date, I will be billed based on the price and EULA applicable on that date, which I can find on the Your Marketplace Software page.

Create the Contract and Pay

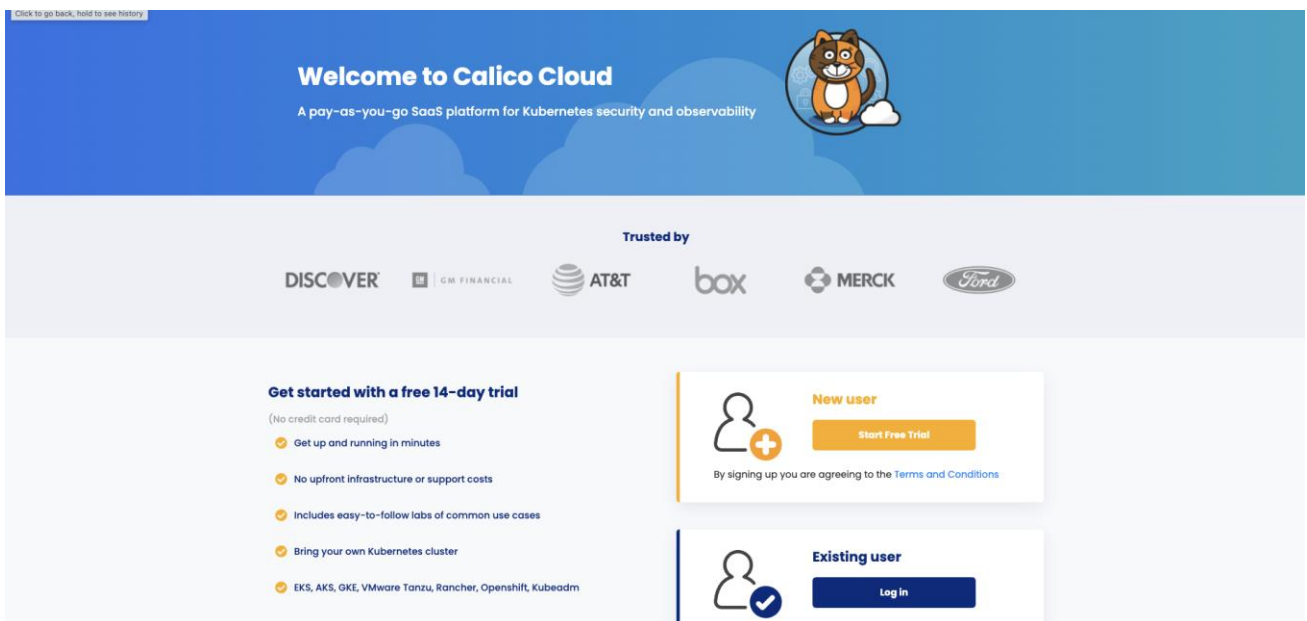
Once you have configured your contract, you can click on the Create contract button.



You will be prompted to confirm the contract. If you agree to the pricing, select the **Pay Now** button.

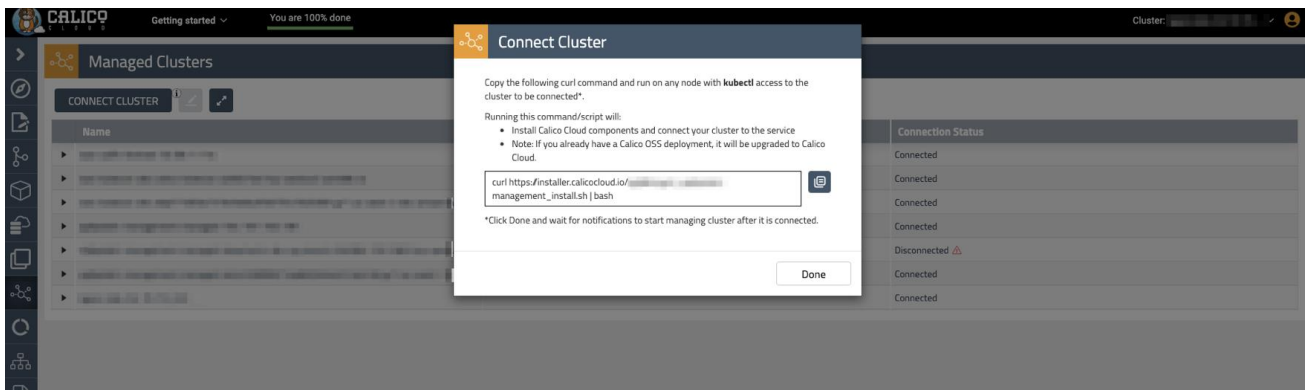
Step 2: Set up Additional configuration

- **Log in with your username and password to www.calicocloud.io**



- **Get CalicoCloud installation script**

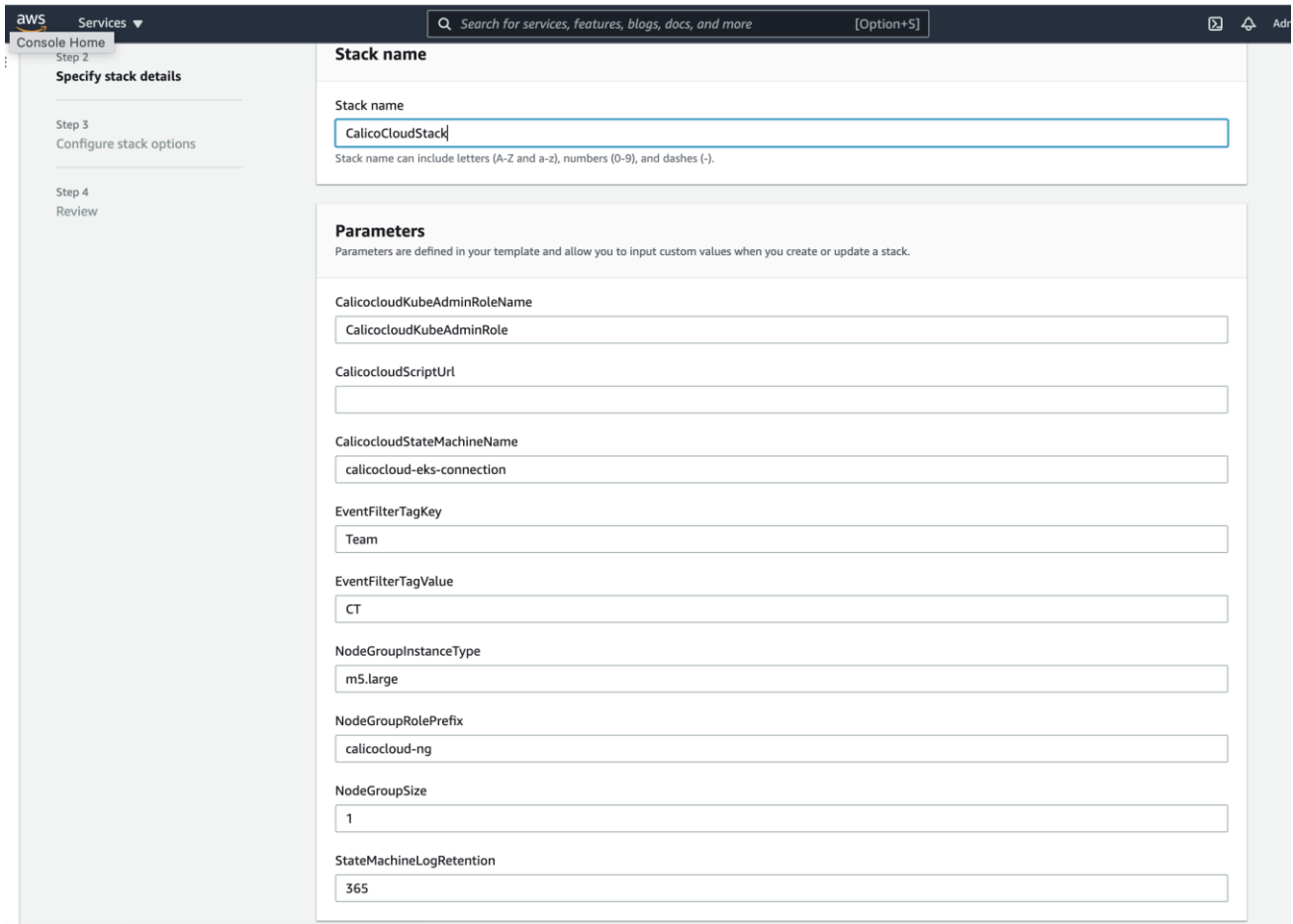
Once you log in click on **Managed clusters**, then click **connect cluster**, select **Amazon EKS**, click Next



Save the script URL

Step 3: Deploy Calico Control Tower Integration Solution

- Download the ControlTowerCalicocloudStack from https://github.com/tigera-solutions/CalicoCloud_AWS-Control-Tower/blob/main/ControlTowerCalicocloudStack.yml
- Launch the AWS CloudFormation template into your AWS account.
- From AWS CloudFormation, create a new stack using ControlTowerCalicocloudStac.yml
- Enter the installation script that we got in step 2



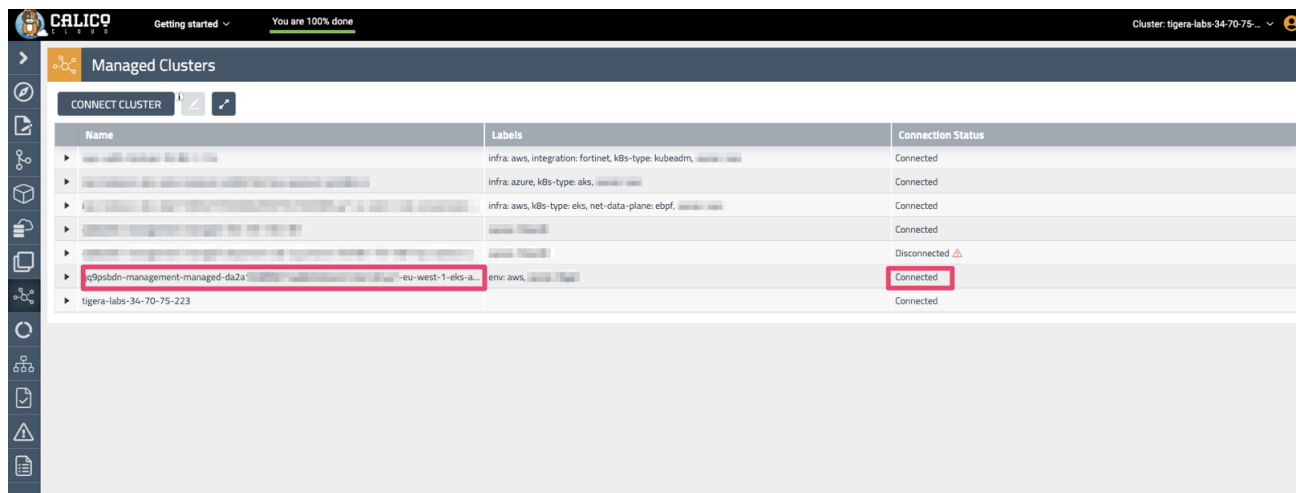
- Once the stack gets created, the stack status should be "CREATE_COMPLETE"

Stack name	Status	Created time	Description
CalicoCloudStack	CREATE_COMPLETE	2021-10-29 14:20:51 UTC+0100	-

Step 4: Verify EKS Cluster is connected in Calico Cloud

We create a new EKS cluster that has IAM role (CalicocloudKubeAdminRole) added as system:masters in AWS-auth configmap while EKS Cluster creation. You can refer to AWS documentation on adding the role to Kubernetes configmap by creating eks cluster using [Amazon quickstart eks cluster](#) CloudFormation resource

or [AWS CDK](#). The cluster will connect automatically to the calico cloud. You can verify this by Log in to www.calicocloud.io to see the new cluster under the connected clusters.



Solution Estimated Pricing

Below are the total costs for these different subscription durations.

Additional taxes or fees may apply.

Calico Cloud: SaaS for Kubernetes Security & Observability		
Units	Description	1 Month
Pro Subscription	Includes 200GB of ingested log data(Counts towards Pro Node Hours)	\$500
Starter Subscription	Includes 100GB of ingested log data(Counts towards Starter Node Hours)	\$300

Additional usage fees	
<i>You will be billed monthly for additional usage costs if your usage exceeds your contract. Your additional usage costs will be determined by the number of units you use above your contract.</i>	
Description	Fees
Pro Node Hour (Up to 4 vCPU in each node)	\$0.08/unit
Starter Node Hour (Up to 4 vCPU in each node)	\$0.05/unit
Additional Ingested Log Data per GB	\$0.25/unit

Additional resources

[Calico Cloud UI portal](#)

[Calico Cloud Documentations](#)

How to contact Tigera?

contact@tigera.io