Rafay uses Calico on AWS to create and enforce security policies at scale

In collaboration with

Executive Summary

The Kubernetes Operations Platform (KOP) is a software as a service (SaaS) tool from Rafay that is hosted on Amazon Elastic Kubernetes Services (Amazon EKS). To secure its turnkey offering, Rafay required a scalable, Kubernetes-native networking and security solution. The solution needed to integrate the Rafay KOP with its host (Amazon EKS), provide and enforce a multi-tenant security policy, and solve IP exhaustion issues while delivering flexible IP address management (IPAM). To achieve these goals and more, Rafay onboarded Calico, a solution from AWS Advanced Technology Partner, Tigera.

Platform Growth Calls for the Augmentation of Networking and Security

Hosted on Amazon EKS, the SaaS-based KOP developed by Rafay is a centralized enterprise-grade solution that streamlines deployment, scaling, and fleet management for enterprises with limited Kubernetes expertise. To responsibly operationalize workload lifecycle management for a growing customer base at scale, Rafay needed to fortify the security of its platform. Rafay needed a solution that could seamlessly integrate with Amazon EKS and facilitate access to several Amazon Web Services (AWS) from a single panel.

The solution also needed to provide and enforce a security policy for multi-tenant environments through workload isolation with identify-aware microsegmentation. Additionally, the elimination of IP exhaustion issues and the delivery of automated, flexible IPAM were essential for agile scaling without increasing operational overhead. Rafay engaged Tigera and leveraged its open-source offering, Calico Open Source.

About customer

With the Rafay Kubernetes Operations Platform, enterprises leverage a single operations platform for Amazon EKS and app lifecycle management.

Delivering Scalable Container Networking and Security with Calico

Following a seamless deployment, Calico delivered a multifaceted networking and security solution. As a foundational control, the solution was designed to support the Rafay platform in several mission-critical ways. Calico helped Rafay seamlessly integrate with Amazon EKS. It also facilitated access to several AWS services from a single panel and simplified policy creation with a policy engine. The engine leverages microsegmentation and tenant isolation for workload isolation and compliance, while also being compatible with the Kubernetes network policy.

Calico also supported the elimination of IP exhaustion issues and delivered automated IPAM to allow for agile scaling without increasing operational overhead.

Combined with network protocols that are trusted industry-wide, these operational additions resulted in a scalable solution that was a perfect fit for Rafay's goals. With Calico's robust security policy engine integrated into Rafay's KOP, Rafay customers can enforce security policies with ease. Mohan Atreya, senior vice president of product and solutions at Rafay, elaborates on the value of the Calico solution:

"Operationalizing the workload lifecycle requires security guardrails. Calico enables a security policy engine that scales."

"Operationalizing the workload lifecycle requires security guardrails. Calico enables a security policy engine that scales."

Mohan Atreya
Senior VP of Product and Solutions, Rafay

Accelerating Security Policy Creation and Implementation to 15 Minutes

With Calico's robust security policy engine integrated into Rafay's KOP, users can enforce their security policies with ease. Using Calico, Rafay enabled a customer to support 300 developers and onboard hundreds of applications across a fleet of clusters in less than six months. Calico's active security platform helps cloud users on Amazon EKS keep their containerized workloads and Kubernetes-based applications secure. Calico also includes native integrations with AWS features, including security groups, AWS Egress Gateway, and AWS Control Tower. Atreya elaborates on the policy engine at Rafay:

"With Calico, Rafay customers can deploy clusters with secure network policies that are ready to go in just 15-20 minutes."

Solving IP Exhaustion with Calico's Flexible IPAM

Calico's IPAM system enables users to make the most of their IP resources by creating private networks inside their cluster. Calico uses IP pools to identify which IP ranges can be used to assign to pods. When using Calico's overlay mode, the IP pools can be any private network IP range.

Together with Calico, Rafay's KOP is a simple turnkey solution that can be activated without extensive Calico or Kubernetes knowledge, enabling organizations to digitally transform and scale even faster without worrying about IP exhaustion.

About partner

Tigera's active security platform prevents, detects, troubleshoots, and automatically mitigates exposure risks of security issues in the build, deploy, and runtime stages. Tigera delivers its platform as a fully managed SaaS (Calico Cloud) or a self-managed service (Calico Enterprise). Its open-source offering, Calico Open Source, is a widely adopted container networking and security solution.

aws
PARTNER

"With Calico, Rafay customers can deploy clusters with secure network policies that are ready to go in just 15-20 minutes."

Mohan Atreya
Senior VP of Product and Solutions, Rafay