Network Visibility, Security and Compliance for Amazon EKS with Calico and Calico Enterprise

Many AWS customers select Amazon EKS as the best platform to run their containers and the quickest path to deploying production ready applications. EKS is easy to adopt, scalable, and works seamlessly with a breadth of AWS services. However, running applications in production requires additional capabilities to meet compliance requirements, detect potential security incidents, and troubleshoot networking problems that can often occur. Tigera offers EKS customers two CNI solutions: Calico, and Calico Enterprise.

Calico (Project Calico) is an open source networking and network security solution for containers, virtual machines, and native host-based workloads, and supports popular upstream Kubernetes platforms and bare metal services. Calico provides network security for hosted Kubernetes services on Amazon EKS and other cloud providers running across tens of thousands of clusters. Calico's network policy engine formed the original reference implementation of Kubernetes network policy during the development of the container networking API, and implements the full set of features defined by the API.

Calico Enterprise builds on top of open source Calico to provide additional functionality and capabilities for Kubernetes networks on AWS and Amazon EKS, including a rich GUI that minimizes the need to hand code YAML. With Calico Enterprise, you can meet security and regulatory requirements with ease, manage multiple EKS clusters from a central location, and get deep visibility into the Kubernetes network to troubleshoot connectivity issues between your microservices. Calico Enterprise integrates with your existing AWS tools including **CloudWatch** and **Security Hub** so you can leverage existing processes and workflows in your EKS or Kubernetes infrastructure.

Network Visibility, Security and Compliance for Amazon EKS with Calico and Calico Enterprise

Two CNI Options from Tigera for Amazon EKS: Calico and Calico Enterprise

	Project Calico	Calico Enterprise
High performance scalable pod networking	✓	✓
Advanced IP Address Management	✓	✓
Kubernetes network policy	✓	✓
Advanced network policies	✓	✓
L7 rules in policy integrated with Istio/Envoy	✓	✓
Direct infrastructure peering without overlay	✓	✓
Hierarchical network policy		✓
FQDN / DNS based network policy		✓
Rich graphical user interface		✓
Network visualization and troubleshooting		✓
Network policy recommendations		✓
Network policy preview and staging		✓
RBAC controls with audit trail & continuous compliance		✓
Monitoring with alerting on security violations		✓
Threat defense (suspicious activity, anomaly detection)		✓
Multi-cluster management with multi-cloud federation		✓

Network Visibility, Security and Compliance for Amazon EKS with Calico and Calico Enterprise

Three Super-Powers for Your EKS Deployments

Calico Enterprise provides three powerful capabilities when deployed to EKS and Kubernetes:

1. AWS Security Group Integration: Enables you to control which pods can connect to certain VPC resources using existing Security Groups
2. Network connectivity and performance monitoring: Rapidly pinpoints problems that may cause a service disruption using a network traffic visualization engine
3. Compliance reporting: Provides detailed logs and built-in reports as evidence of compliance for PCI DSS, HIPAA, SOC I Type II, and custom frameworks

Integrate EKS Apps with AWS Security Groups

Many of the container workloads that comprise an Amazon EKS app need to access other AWS services or endpoints outside the cluster, like RDS, S3 buckets, Lambda functions, or other application APIs running on EC2 instances. Calico Enterprise integrates with AWS security groups, providing the capability to add one or more pods to a security group to ensure only the microservices that need access have access.

Troubleshoot Microservice Connectivity

Microservice-based applications depend on the network to get their work done, and when there are network problems, downtime can be expected. A problem with one microservice has a ripple effect across the rest of the application, and pinpointing the root cause is challenging. Debugging these issues is time-consuming, requiring a solution that understands Kubernetes context.

Calico Enterprise monitors and logs all network traffic in your Amazon EKS clusters, annotates the traffic with more than 20 Kubernetes metadata attributes, and displays that data as a visualization of the network and its health. An operator can quickly drill into problem areas and identify the source of performance issues, denied connections, and why traffic is being denied.

Network Visibility, Security and Compliance for Amazon EKS with Calico and Calico Enterprise

Implement Enterprise Security and Compliance Controls

Modern microservices-based applications have the same compliance requirements as traditional monolithic ones, including workload isolation (e.g., Dev cannot talk to Prod and vice-versa), or implementing network zones (e.g., DMZ can communicate with the public Internet but not your backend databases).

Using Calico Enterprise network policy, DevSecOps teams can implement hierarchical controls to meet your regulatory and corporate security and compliance requirements. Calico Enterprise provides a full audit log and change history for every control as evidence of compliance and can send audit, event and flow data to your existing logging systems like AWS Security Hub, AWS Cloudwatch, S3 buckets, as well as to SIEMS like Splunk and Sumo Logic.

Get a Free Trial

Get a free trial of Calico Enterprise on Amazon EKS

Tigera, Inc.

58 Maiden Lane, Fl 5
San Francisco, CA 94108

+1 (415) 612-9546 / www.tigera.io

For more information about Calico Enterprise and how it can help you secure your modern applications and demonstrate compliance, email us at contact@tigera.io.