Alcide on AWS

aws partner network | alcide

Alcide Helps Protect EKS Deployments

Challenges
Implementing security best practices can be hard

More and more companies are implementing Kubernetes solutions; but this can be challenging. Such challenges exponentially increase when managing clusters across different hosts, slowing down operations and impeding security. Regardless, whether you're managing single or multiple hosts, there are many best practices supported by AWS that should be implemented in order to ensure your deployment is secure and compliant but many customers are not fully leveraging these controls, lacking visibility into the dynamic environment and facing exposure to security gaps. Keeping track of it all can be hard, ultimately even leading to performance trouble and even security breaches.

The Alcide Security Solution
Alcide helps launch and secure Kubernetes containers

Protect your deployment with continuous security and configuration checks, from deployment through production. Alcide enables granular control of policy segmentation, showing you all data related to policies, helping to protect against malicious attacks while also enabling smooth operation of your business apps. Natively integrating with Amazon EKS, Alcide provides panoramic visibility and deep network security monitoring across accounts, regions, VPCs and more. Our graphic map helps you visualize components and activities to quickly understand associations between security groups and virtual machines. Additionally, you can satisfy stakeholder requirements and industry regulations like HIPAA, GDPR and PCI:DSS, while addressing multi-layered concerns with centrally-orchestrated and automatically enforced security policies.

Benefits

Secure multi-cloud deployments, visualizing changes as they happen. Manage workloads granularly, enforce compliance and ensure remediation is performed on time.

Deep Visualization
Alcide provides a visual map with real-time mapping of the entire environment helping you troubleshoot and mitigate security issues.

Extending AWS security group policies
Automatically import AWS workload security groups, enabling granular control of policy segmentation, displaying all policy data, and protecting against threats.

Enforcement and threat detection
Alcide machine learning algorithms help ensure your infrastructure, policies and network activities stay safe and compliant in real time.

Continuously protect multi-cloud environments
Alcide continuously discovers and manages policies with code-to-production enforcement across networks, empowering DevSecOps teams in scaling multi-cluster deployment security.

Alcide on AWS

With a speedy integration for AWS, Alcide helps DevSecOps leverage EKS to secure Kubernetes deployments at scale. Updating as workloads spin up and down, Alcide quickly identifies threats and alerts on non-compliant, anomalous and threatening behavior. With a centralized dashboard and graphical network map, view a broad picture of all activity to troubleshoot and mitigate issues in real time. Alcide guides you in implementing native AWS guardrails, adopting and monitoring your own security policy model and gaining granular control by importing all workload security groups and policy data, protecting multiple dynamic deployments with in-context metadata and visibility.

Features

Automate security and configuration checks already from development

The Alcide Advisor automatically and continuously scans and checks security and configuration posture, helping you resolve security issues already in the development stage. The Advisor audits the cluster, node and pod configurations to ensure the cluster is tuned and runs according to best practices and internal guidelines, and provides actionable mitigation recommendations. This includes cases such as image registry whitelisting, ensuring workload and pod segregation, correct implementation of IAM and RBAC policies and more.

Real-time automated monitoring of policies and threat detection

Alcide Runtime consolidates all AWS security groups, policies and corresponding inbound and outbound rules across networks in one dashboard, helping enforce application-aware embedded policies for cloud infrastructures and microservices. Alcide also provides threat detection, including abnormal behaviors and incidents, to protect against attacks by gathering information about workload behavior and network usage, processing data with machine learning directed by security expertise, highlighting unexpected patterns and unusual data transfers, and enabling you to react in real-time.

Case Study: Reltio

Challenges

Reltio uses a microservices architecture, leveraging Kubernetes for multi-cloud deployments in Amazon EKS to support scalability and security. Multi-cloud configurations have unique complexities: management across different hosts can slow down operations and impede security.

Solution

Alcide Advisor was used to perform a security scan, scan policy customization, and actionable remediation guidelines. *Alcide Runtime (ART)* was implemented for Kubernetes infrastructure and application network visibility and security monitoring.

Results

DevOps moved faster with automated, continuous testing, avoiding security roadblocks. Stakeholders received regular updates about changes to environments, attempted attacks, and intra-cluster activity. Data exfiltration alert and monitoring saved time and budget.

Get started with Alcide solutions on AWS

Visit AWS Marketplace or Alcide to purchase or start a Free Trial today.