CIS Amazon EKS Benchmark

Securing cluster node configurations

Paavan Mistry – Senior Developer Advocate, AWS
August 17th 2020
Table of contents

- CISecurity.org and the CIS Kubernetes Benchmark
- The Shared Responsibility Model for Amazon EKS
- CIS Amazon EKS Benchmark
- “Show me how to use this Benchmark” - Demo
CISSecurity.org and the CIS Kubernetes Benchmark
CIS Kubernetes Benchmark

- Initially published in May 2017
- Community-driven and consensus-based security good practice guidance
- Currently publication (v1.6.0) supports Kubernetes v1.16 – v1.18
- Industry-accepted system hardening procedures
- Reviewed by Kubernetes community contributors and subject matter experts
CIS Kubernetes Benchmark – Guidance scope

Kubernetes architecture

Control plane
- Scheduler
- Controllers
- etcd
- API server

Data plane
- Node
  - Kubelet
  - Kube-proxy
  - Pods
Shared Responsibility Model – Amazon EKS
Managed Kubernetes – Amazon EKS

Kubernetes architecture

Data plane

Node
- Kubelet
- Kube-proxy
- Pods
Amazon EKS – Shared Responsibility Model

Source: https://aws.github.io/aws-eks-best-practices/
CIS Amazon EKS Benchmark
CIS Amazon EKS Benchmark

• Helps you accurately assess the security configuration of nodes running as part of your Amazon EKS clusters

• Applicable to EC2 nodes (both managed and self-managed)

• Consists of four sections:
  • Control plan logging configuration
  • Node security configurations
  • Policies
  • Managed services
Assessments using `kube-bench`

- Provide a mechanism to assess the node security configuration using `kube-bench` from the raw benchmark

- `kube-bench` is an open source tool created and maintained by Aqua Security, an AWS Advanced Technology Partner

- Introduces an opportunity to automate node security assessments against the CIS Amazon EKS Benchmark for your Amazon EKS clusters
Demo – Show me how to use this Benchmark!
Resources and call to action

- **Blog:**

- **1 hour deep dive on**
  **#ContainersFromTheCouch** **show:**
  - [https://www.youtube.com/watch?v=m-3tMXmWWQw](https://www.youtube.com/watch?v=m-3tMXmWWQw)

- **CIS Amazon EKS Benchmark:** [https://cisecurity.org/cis-benchmarks](https://cisecurity.org/cis-benchmarks)
Q&A

Ask on chat or visit our virtual booth during KubeCon EU 2020!
Thank you

Mail: paavan@amazon.com
Twitter: @98pm