Secure a Kubernetes Cluster with Falco

Introduction

We propose to make an overview about ways to build a secure Kubernetes cluster. This project will slightly touches most of the issues that can threat the Kubernetes cluster, container and cloud resources these days, from the aspect of development phase, application phase, infrastructure phase and detection phase. Mostly, we focus on the application of Falco, which is a open source standard tool for continuous risk and threat detection, on Kubernetes, and deploy a cluster that is easy-to-monitor and relatively safe from most of the threats including crypto-mining.

Proposal

As Kubernetes continues to grow in adoption, it is important for us to know how to secure it. In a dynamic infrastructure platform such as Kubernetes, detecting and addressing threats is important but also challenging at the same time.

There can be threats in many ways, we will thoroughly describe and analysis the cutting edge technology used in securing Kubernetes cluster and main attacks towards it. We will analysis the threats from four aspects, some of the techniques includes as follows.

Development Phase Create image wisely, multi-stage build to reduce size.

Application Phase Use namespace to divide the cluster, design network policy.

Infrastructure Phase Use hardened AMIs, run kube-bench for CIS benchmark.

Detection Phase Run dynamic scan on running container, enable audit logs.

Plan of work

Research: With the help of research paper and technical practice principles, we summarize the basic idea of most of popular threats over Kubernetes cluster and ways to deal with it.

Practice: There are many tools like Falco, Sysdig designed to protect the cloud native applications, as a project practice, we will go through all the principal steps from detecting a crypto-mining attacks, defend against the attacks to secure the whole deployment of cloud system, and implement other protection to free the cloud system from common threats.

Desired outcome

Research: A report about the current threats when deploying cloud-native infrastructure.

Practice: With the guidance of open source tutorial and books, we can build a Kubernetes cluster which meets the demand of daily use security including crypto-mining attack. Moreover, a security deployment plan about secure Kubernetes cluster.

Conclusions

As mentioned above, we propose our project to be composed of research of current threats to Kubernetes cluster and one practice to build a cluster to be relatively safe from most of attacks including crypto-mining attack. This project can help us to understand the latest techniques of cloud-native application security and experience in defending common threats like crypto-mining attack.