SECURITY

Security

Cloud Security Considerations

Keeping a cloud environment secure is an ongoing, and wide-ranging task. As more moves to the cloud, we must look at more than just Kubernetes towards the hardware, software, and configuration options for the entire environment. Starting in the design phase, care must be taken to secure safe hardware, firmware and operating system binaries.

Once the platform is hardened, the kube-apiserver has a list of considerations, tools, and settings to limit access and formalize access in an easy-to-understand manner.

As a network-intensive environment, it becomes important to secure the network both inside Kubernetes, as done with a NetworkPolicy, as well as traditional firewall tools and pod-to-pod encryption.

Minimizing base images, insisting on container immutability, and static and runtime analysis of tools is also an important part of security, which often begins with developers and is implemented in the CI/CD pipeline prior to an image being used in a production cluster. Tools like AppArmor and SELinux should also be used to further protect the environment from malicious containers.

Security is more than just settings and configuration. It is an ongoing process of issue detection using intrusion detection tools and behavioral analytics. There needs to be an ongoing process of assessment, prevention, detection, and reaction following written and often updated policies.