SECURITY

# Security

## Overview

Security is a big and complex topic, especially in a distributed system like Kubernetes. Thus, we are just going to cover some of the concepts that deal with security in the context of Kubernetes. In-depth cloud and Kubernetes security is covered in detail in the Kubernetes Security Essentials (LFS260) course.

Then, we are going to focus on the authentication aspect of the API server and we will dive into authorization, looking at things like RBAC, which is now the default configuration when you bootstrap a Kubernetes cluster with **kubeadm**.

We are going to look at the **`admission control`** system, which lets you look at and possibly modify the requests that are coming in, and do a final deny or accept on those requests.

Following that, we're going to look at a few other concepts, including how you can secure your Pods more tightly using security contexts and pod security policies, which are full-fledged API objects in Kubernetes.

Finally, we will look at network policies. By default, we tend not to turn on network policies, which let any traffic flow through all of our pods, in all the different namespaces. Using network policies, we can actually define Ingress rules so that we can restrict the Ingress traffic between the different namespaces. The network tool in use, such as Flannel or Calico will determine if a network policy can be implemented. As Kubernetes becomes more mature, this will become a strongly suggested configuration.