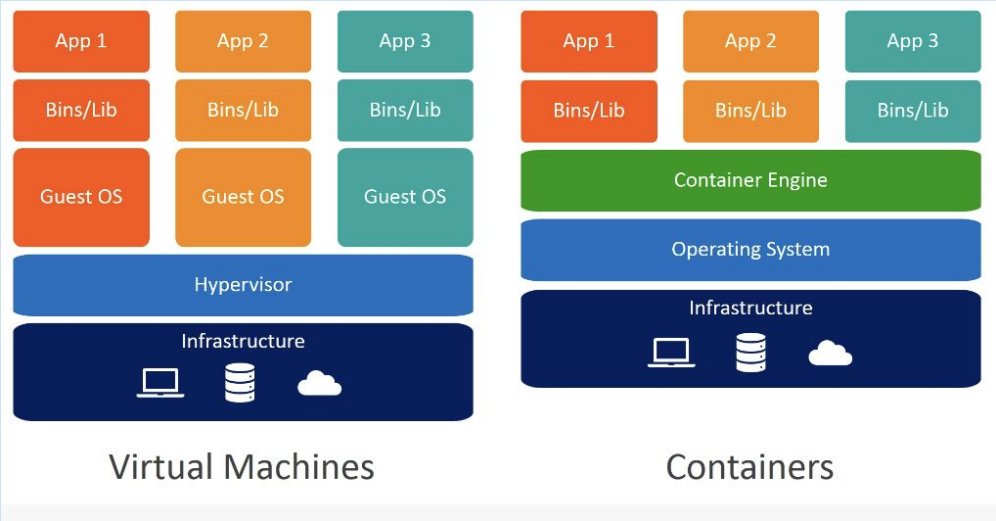
Kubernetes - security challenges of container orchestration

Containers explained

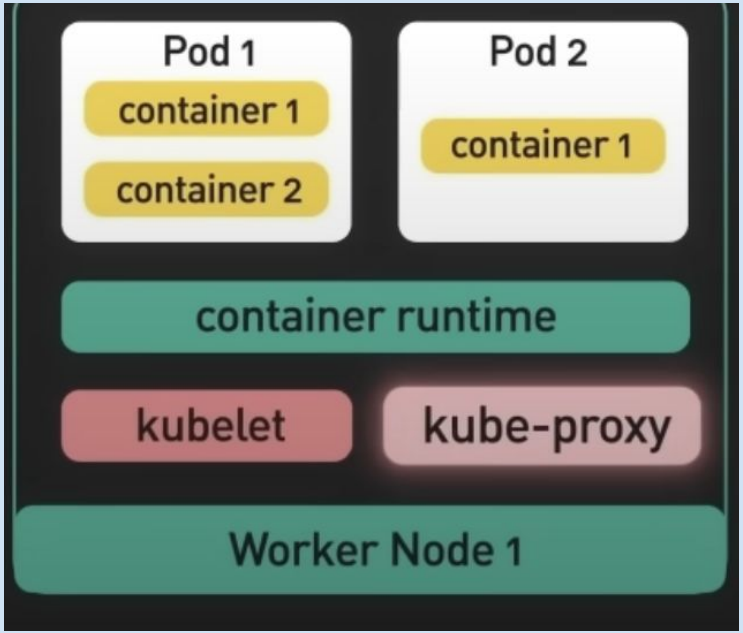
Packages of software that contain all of the necessary elements to run in any environment - answer to the problem "why my code/software won't run on your computer"



Kubernetes architecture

Pod (as in a pod of whales or pea pod) is a group of one or more containers.

Kubelet & kube-proxy manage the state and network of pods.



Control Plane

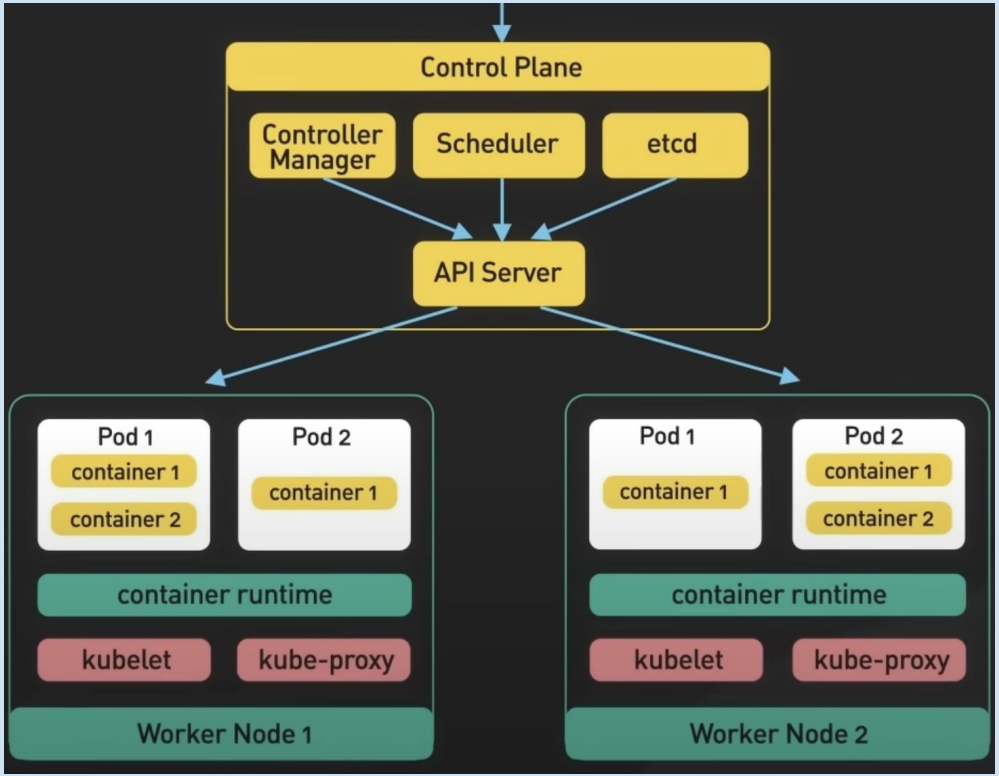
Responsible of global decisions of the cluster.

etcd - key value store for storing Kubernetes cluster data.

Scheduler - responsible for assigning newly created pods to nodes.

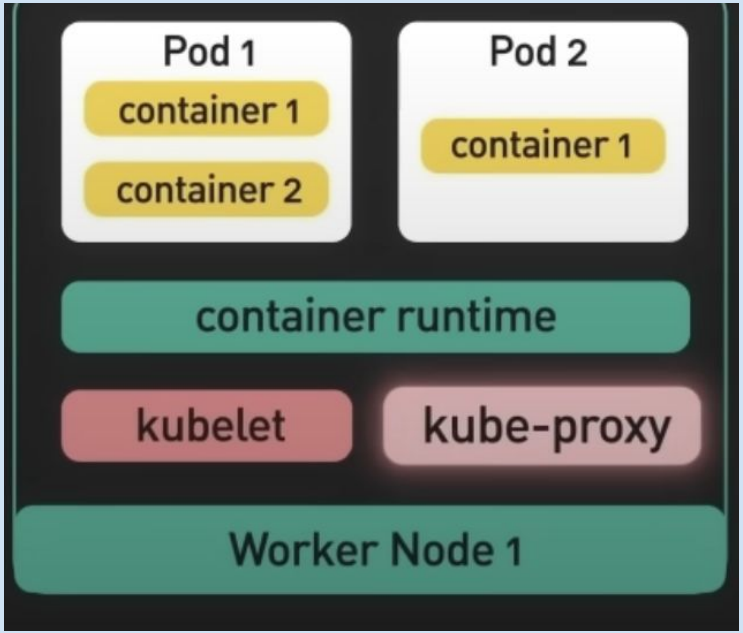
Controller Manager - monitors the state of the cluster and changes the state to match the desired state in the cluster's configuration.

API Server - exposes an HTTP API that lets end users, different parts of your cluster, and external components communicate with one another.



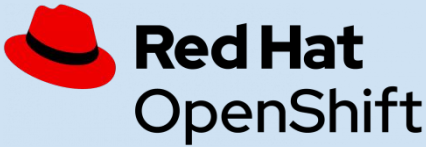
Kubernetes security considerations

- Pod security
- Network segmentation
- Authentication and authorization
- Audit Logging and Threat Detection



Managed versions

- **Customer's responsibilities: application code, build files, container images, data, Role-based access control (RBAC)/IAM policy, and containers and pods that you are running, monitoring.**



Security needs to be considered in every stage of the life cycle.