CERN openlab

Improving Security on Kubernetes Clusters

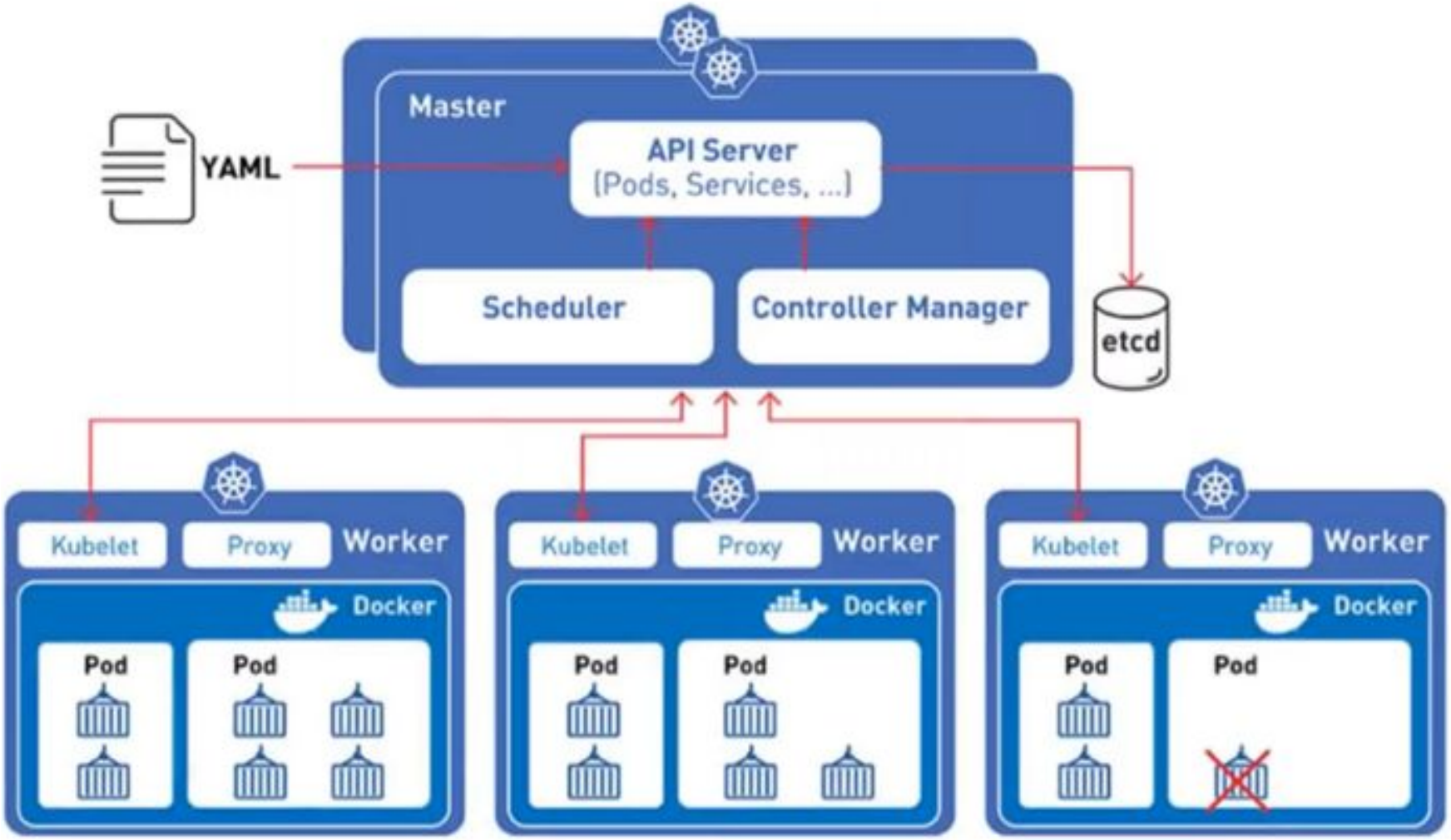
Ivan Sharankov

September 14, 2022

Supervisor: Antonio Nappi

Kubernetes

In a nutshell



Kubernetes

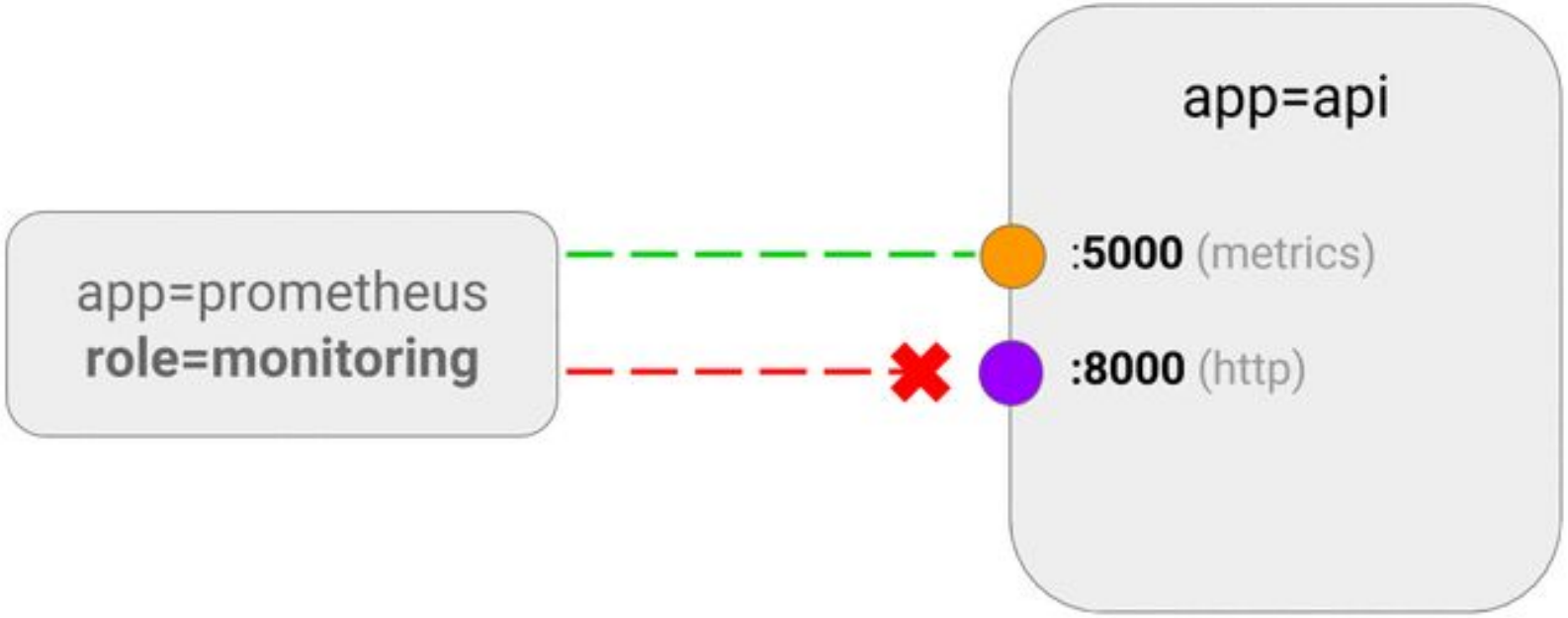
The Tradeoff

- Orchestration adds lots of abstraction
- More to deployments than just spawning containers
- Exposing services to security vulnerabilities more than the past

- Need:
  - Simple ways to lock down and manage orchestrations
    - Needs to be simple and reusable
  - Scalable policy and authorization control
    - who-can-do-what and what-can-do-what

Network Policies

Use Cases



Network Policies

Limitations

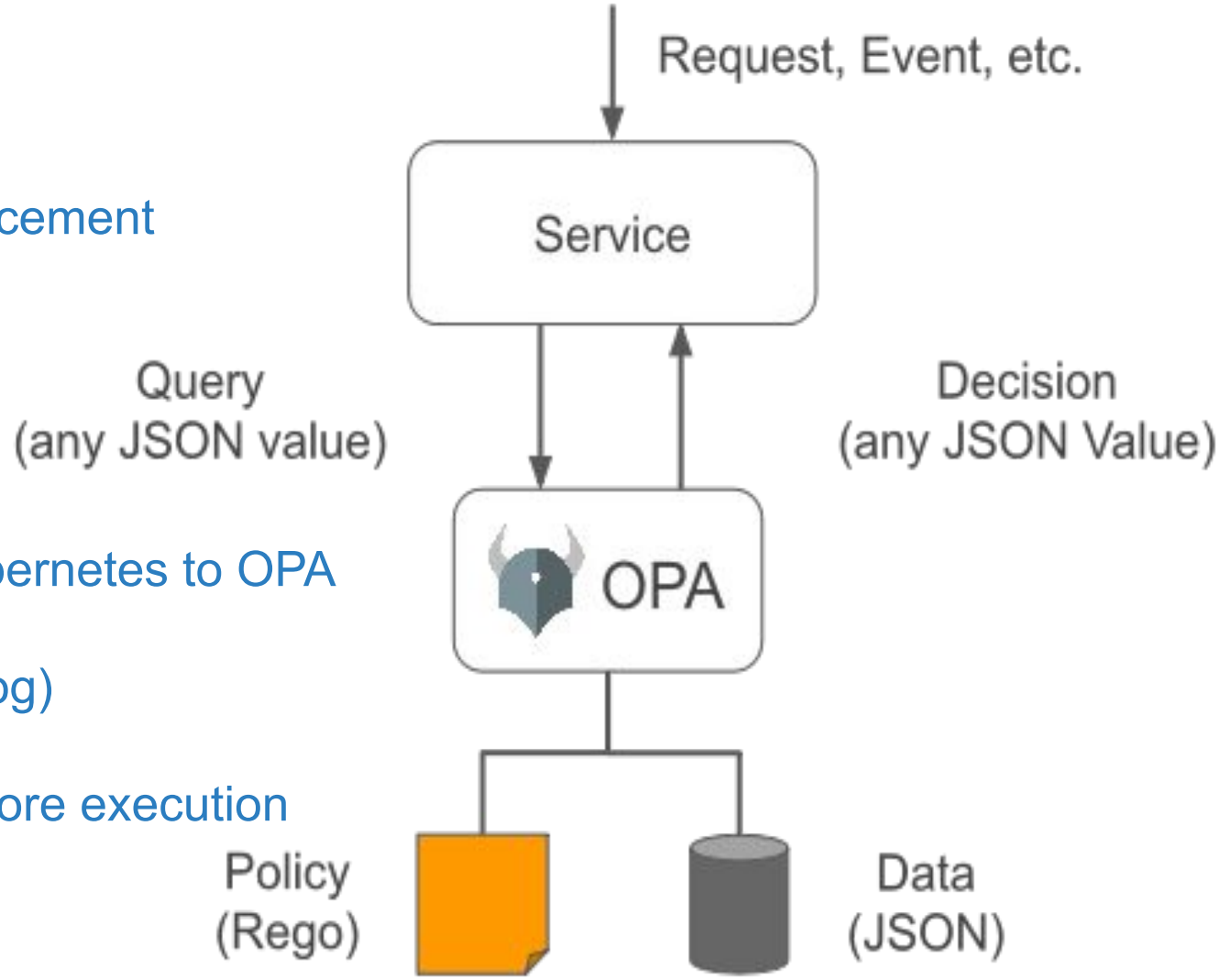
- Focuses on ingress and egress

- Can’t…
  - Target services by name (labels help, but require maintenance)
  - Create policies targeting specific nodes (CIDR notation helps a bit)
  - Log network security events
  - Explicitly deny policies (well, kind of…, only allow)
    - Can’t create default policy for ALL namespaces/pods
  - Any third party management of policies

Open Policy Agent

A generalized security mechanism

- General purpose policy engine
  - decouple policy decision from enforcement
- Used in many different cloud solutions
  - Jenkins, NodeJS, Nginx, API, SSH, Terraform, Kafka, Minio, etc.
- OPA not tied to Kubernetes, neither Kubernetes to OPA
- Uses declarative language Rego (datalog)
- Intercepts requests after verification/before execution



Open Policy Agent

Use cases and examples

- Which users can perform an action on a given resource
- Which clusters are allowed to deploy workloads?
- Only install pods from trusted registries
- What OS functions the container can perform
- When will the system be accessed at what time of day?
- Enforcing authorization in a microservice API
- Require human review when a recourse is deleted/updated
- Require commits to be of certain size or quality
- Determine blast radius of an action such as create/update/delete instances
- Adhering to best practices, ISO standards, or conventions
- SSH authentication, verification, node/instance checking, etc.

Closing

Remarks and next steps

- Network policies
  - Simple, easy to use, included with kubernetes
- OPA
  - General purpose, can be implemented with anything
  - Simple declarative language
- Helm
  - Helm charts were created to automate and simplify deployment
- Next step
  - Automate deployment via git ops

Thank you!