火龙果 · 整理
uml.org.cn

Kubernetes容器平台架构

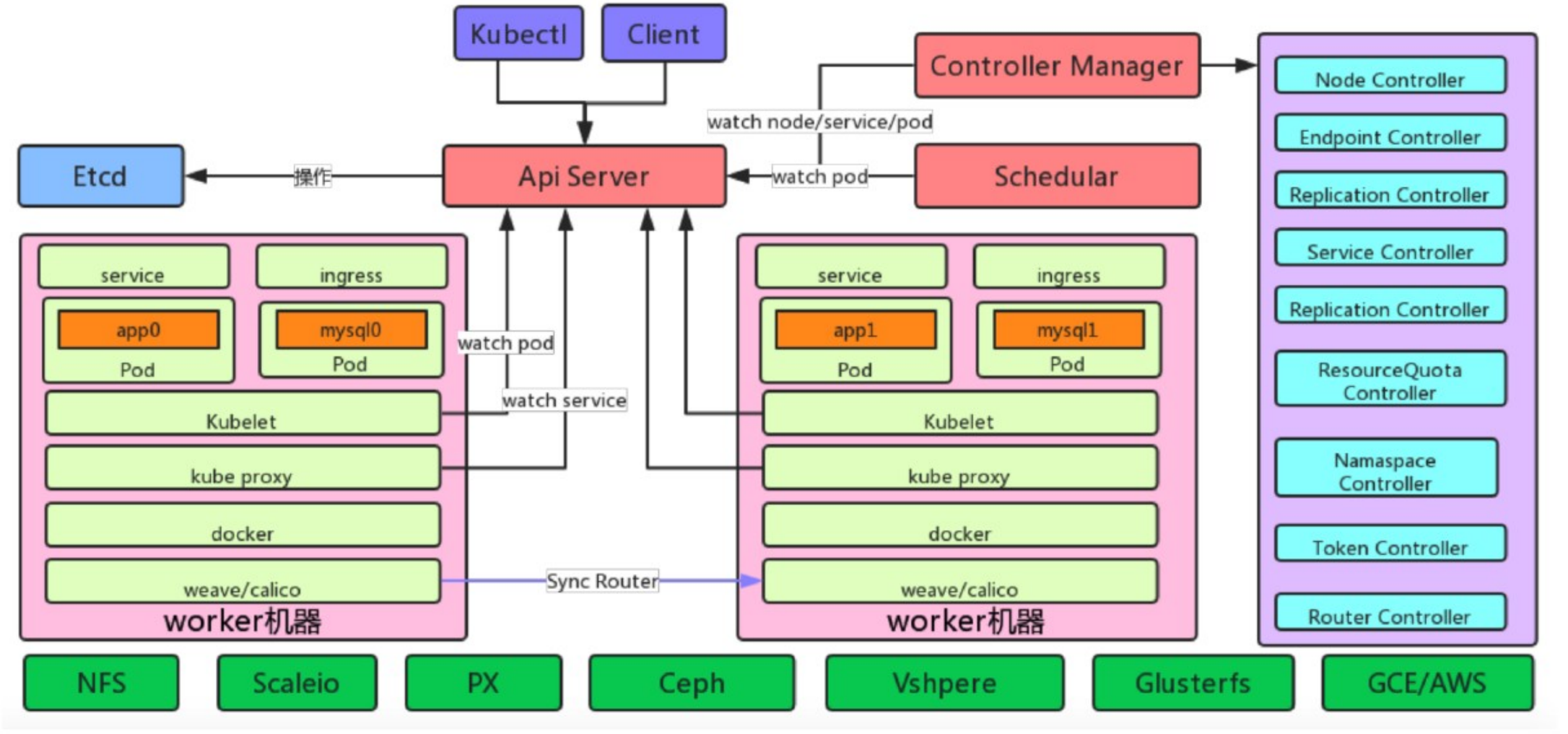
Agenda

火龙果・整理
uml.org.cn

1. Kunernetes 架构分析
2. Kubernetes Features

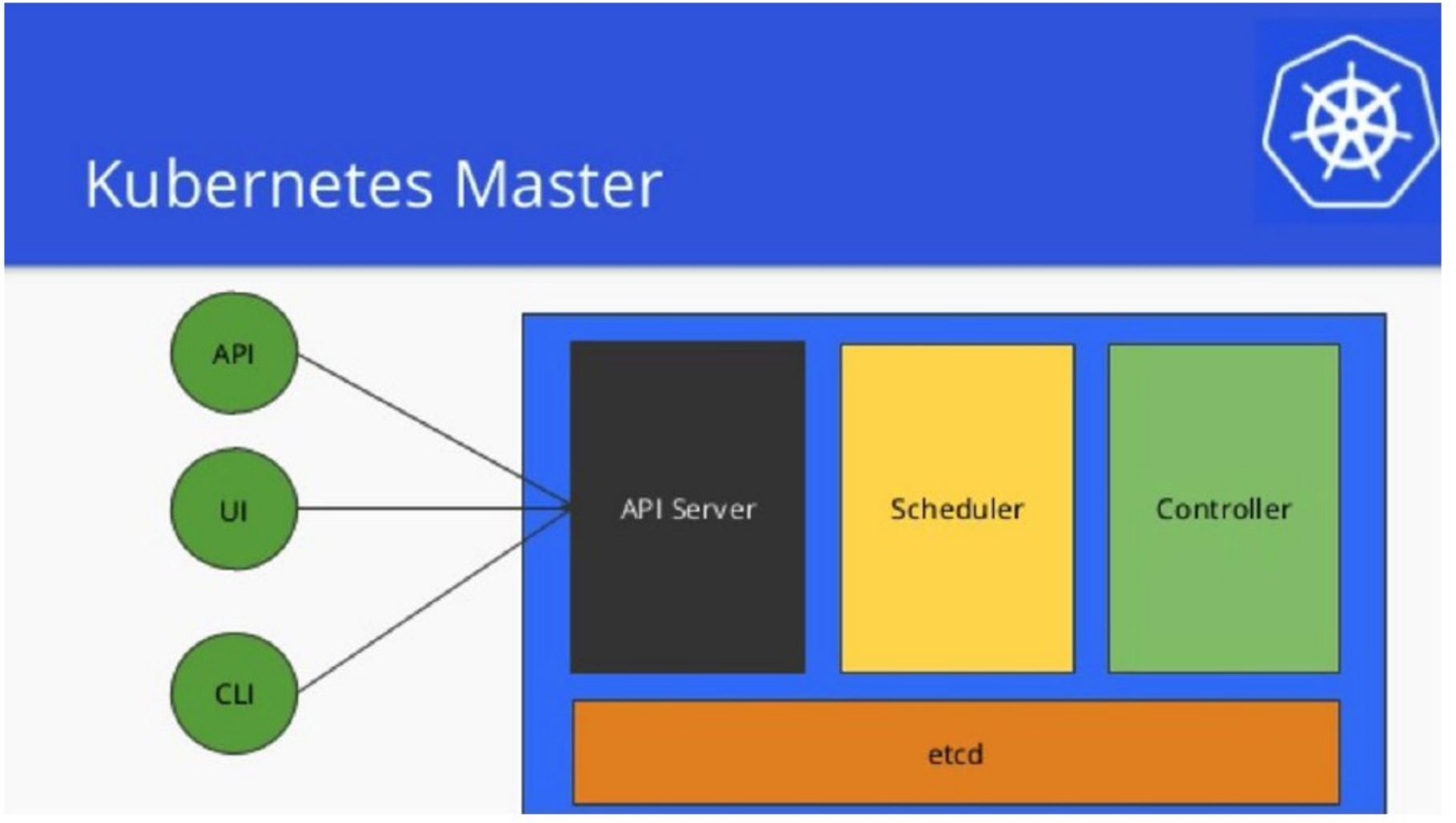
Kubernetes 架构

火龙果 · 整理
uml.org.cn

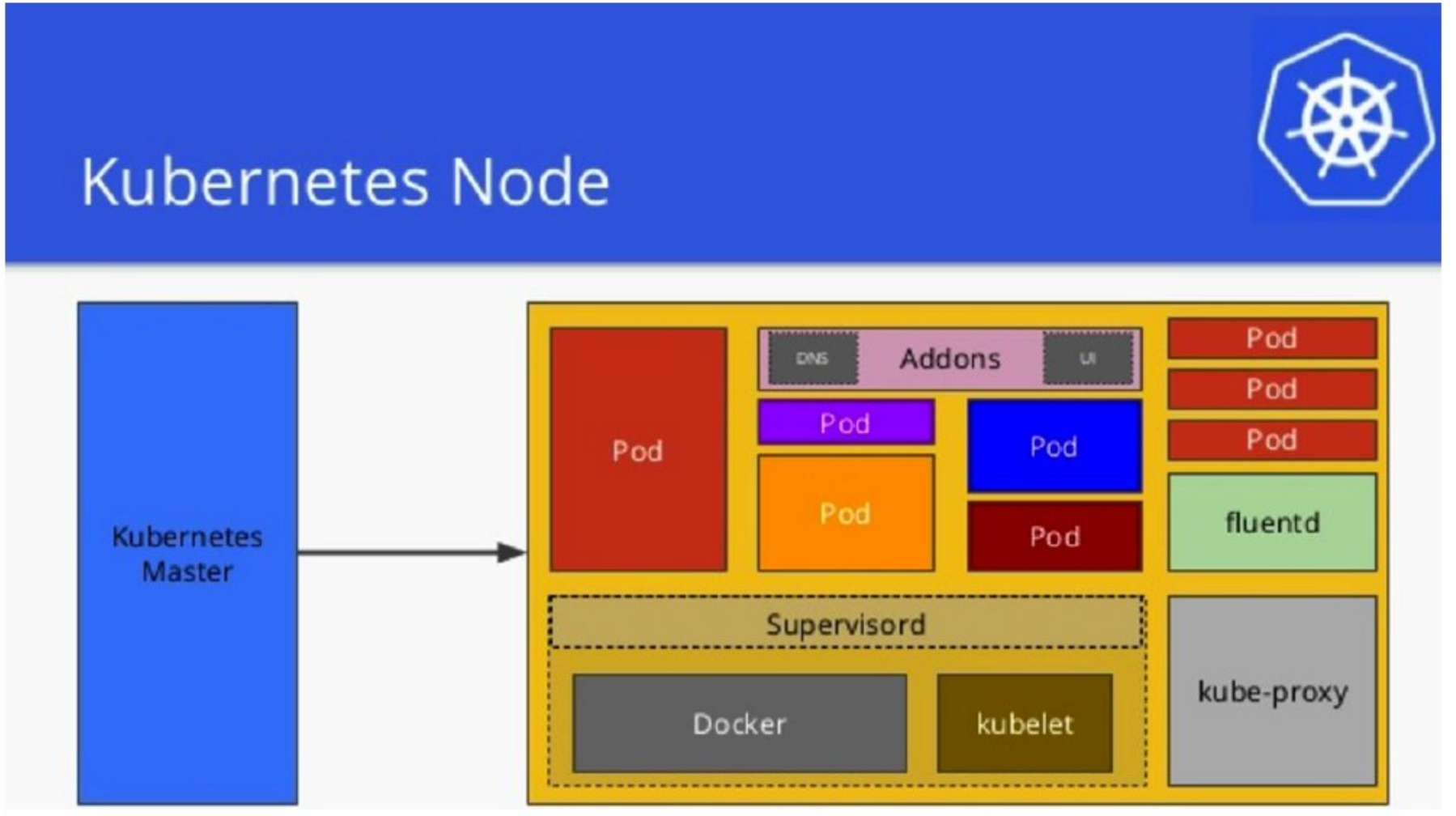


Kubernetes Master

火龙果・整理
uml.org.cn

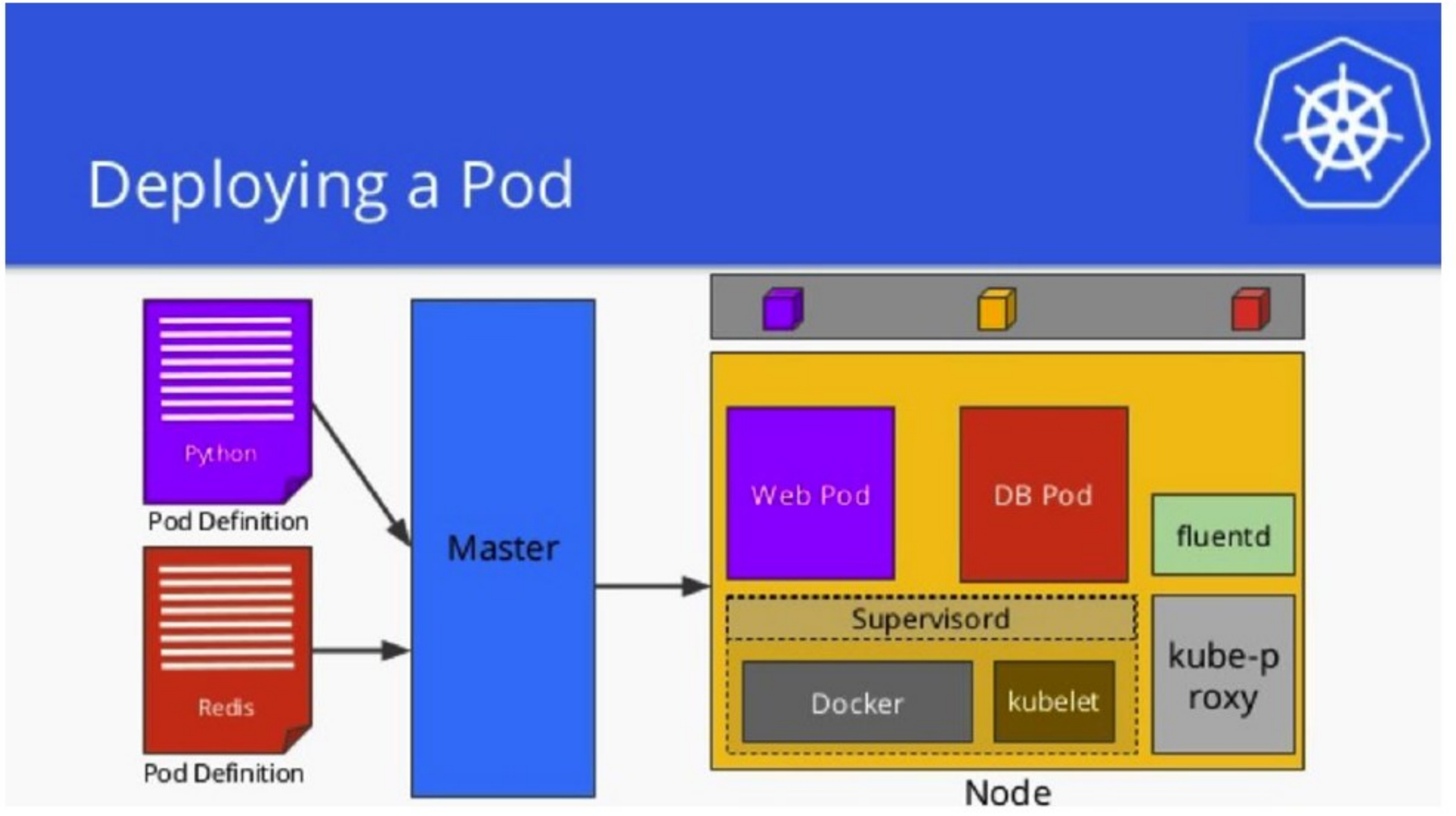


Kubernetes Node



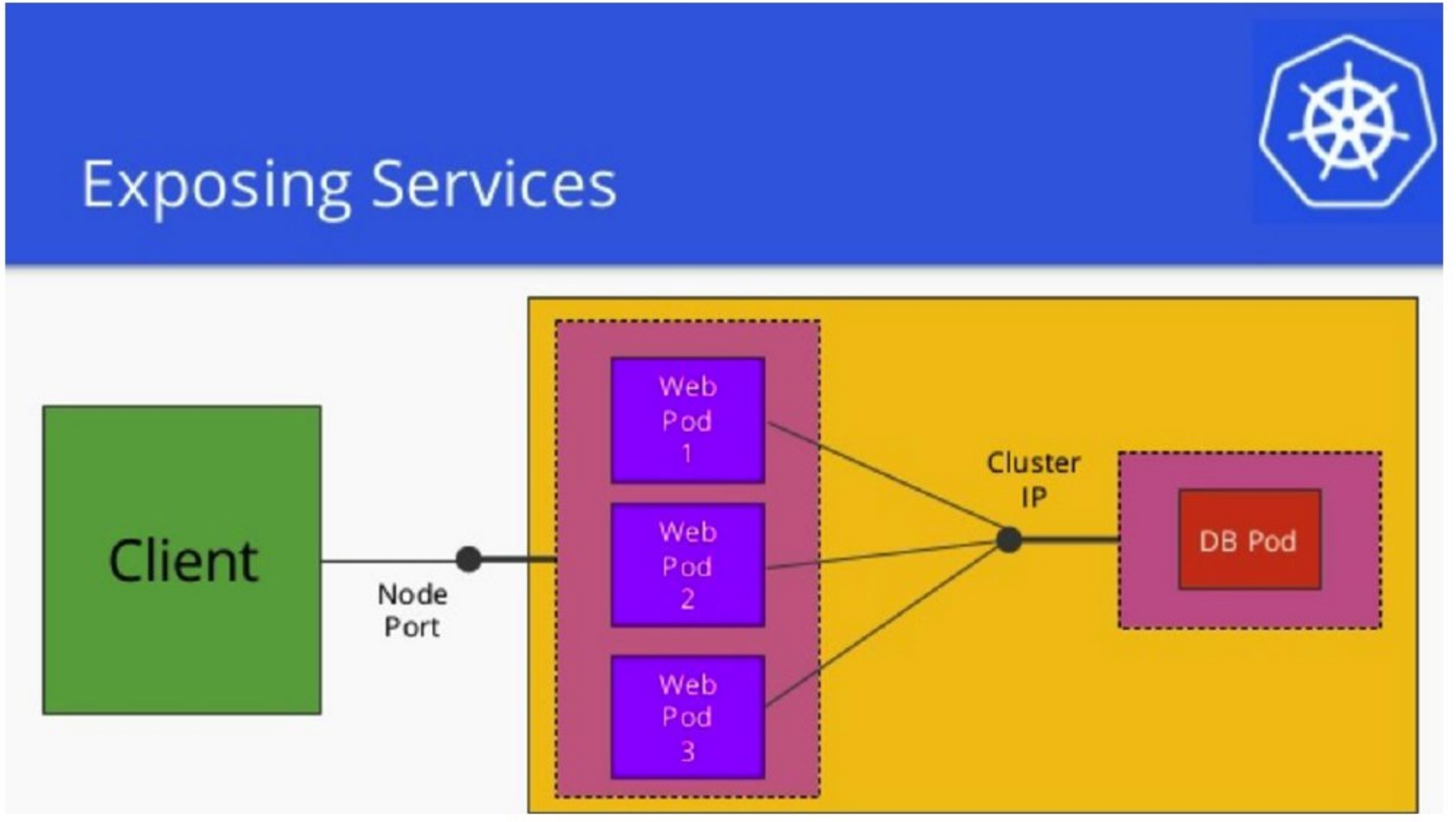
火龙果 · 整理
uml.org.cn

Kubernetes Pod



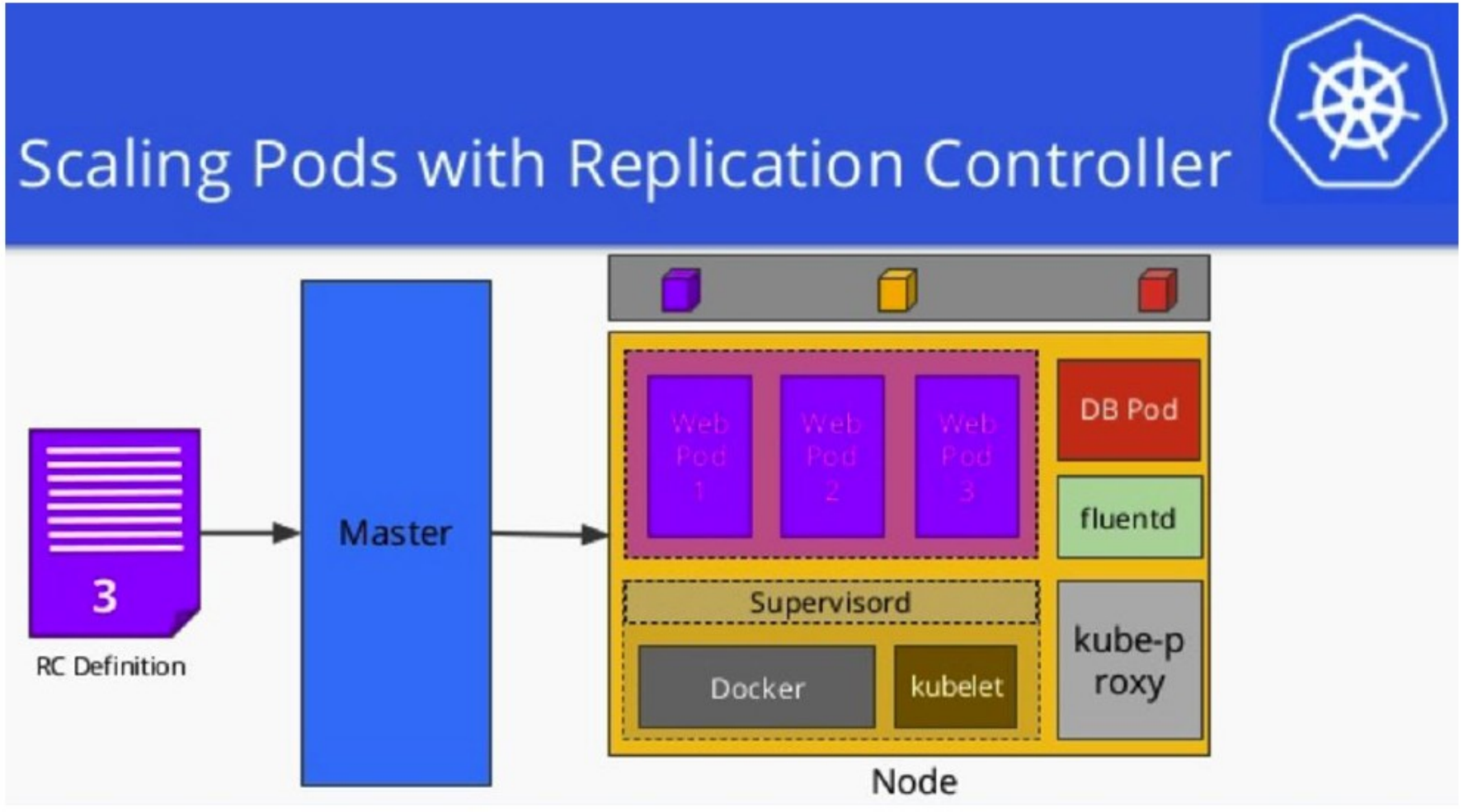
火龙果 · 整理
uml.org.cn

Kubernetes Service



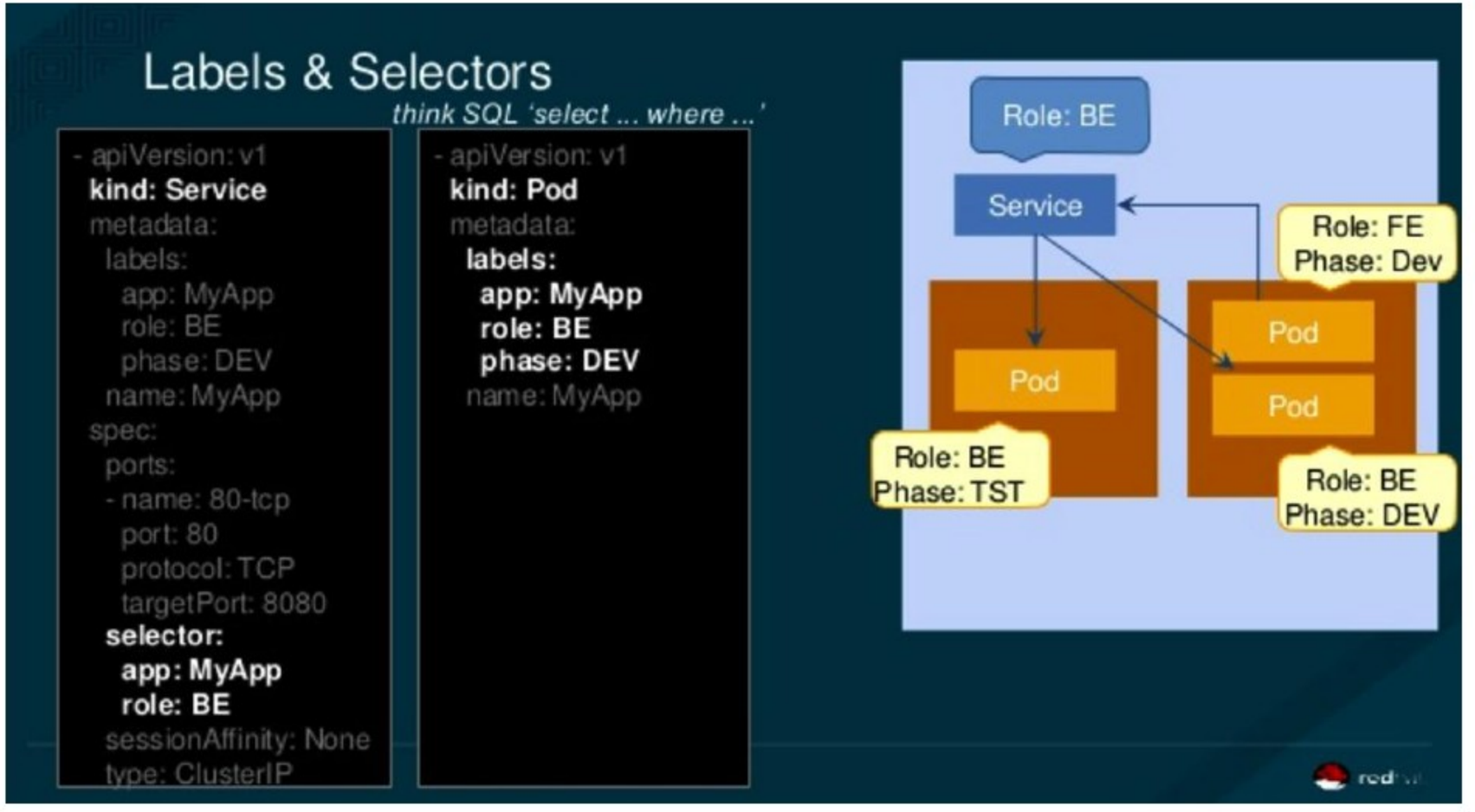
火龙果・整理
uml.org.cn

Kubernetes ReplicationController



火龙果・整理
uml.org.cn

Kubernetes Labels&Selector



Kubernetes Ingress&Router

火龙果・整理
uml.org.cn

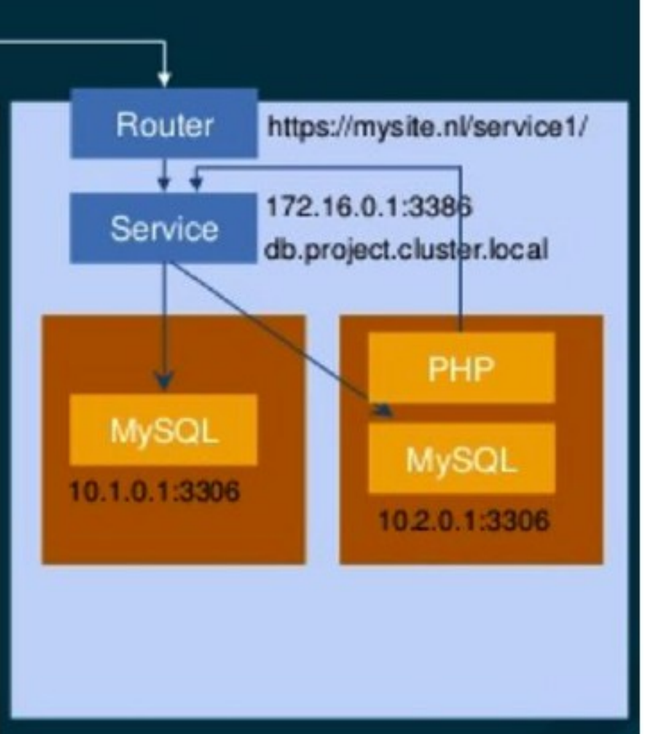
Ingress / Router

- Router Definition:
  - Layer 7 Load-Balancer / Reverse Proxy
  - SSL/TLS Termination
  - Name based Virtual Hosting
  - Context Path based Routing
  - Customizable (image)
    - HA-Proxy
    - F5 Big-IP

Examples:

- https://www.mysite.nl/myapp1/
- http://www.mysite.nl/myapp2

```
apiVersion:
extensions/v1beta1
kind: Ingress
metadata:
  name: mysite
spec:
  rules:
  - host: www.mysite.nl
    http:
      paths:
      - path: /foo
        backend:
          serviceName: s1
          servicePort: 80
      - path: /bar
        backend:
          serviceName: s2
          servicePort: 80
```



Kubernetes PersistentStorage

火龙果・整理
uml.org.cn

Persistent Storage

for Ops:

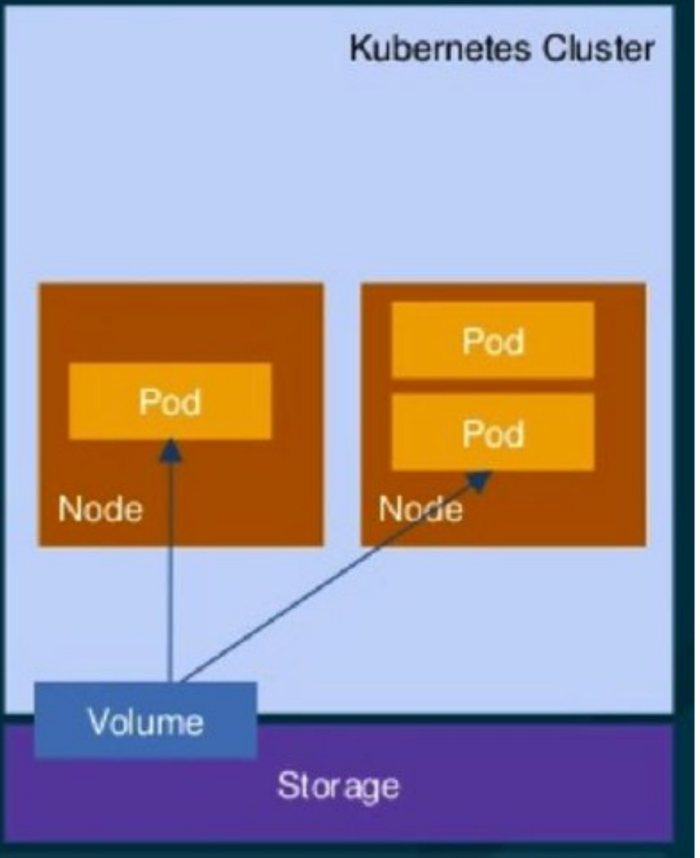
- Google
- AWS EBS
- OpenStack's Cinder
- Ceph
- GlusterFS
- NFS
- iSCSI
- FibreChannel
- EmptyDir

for Dev:

- "Claim"

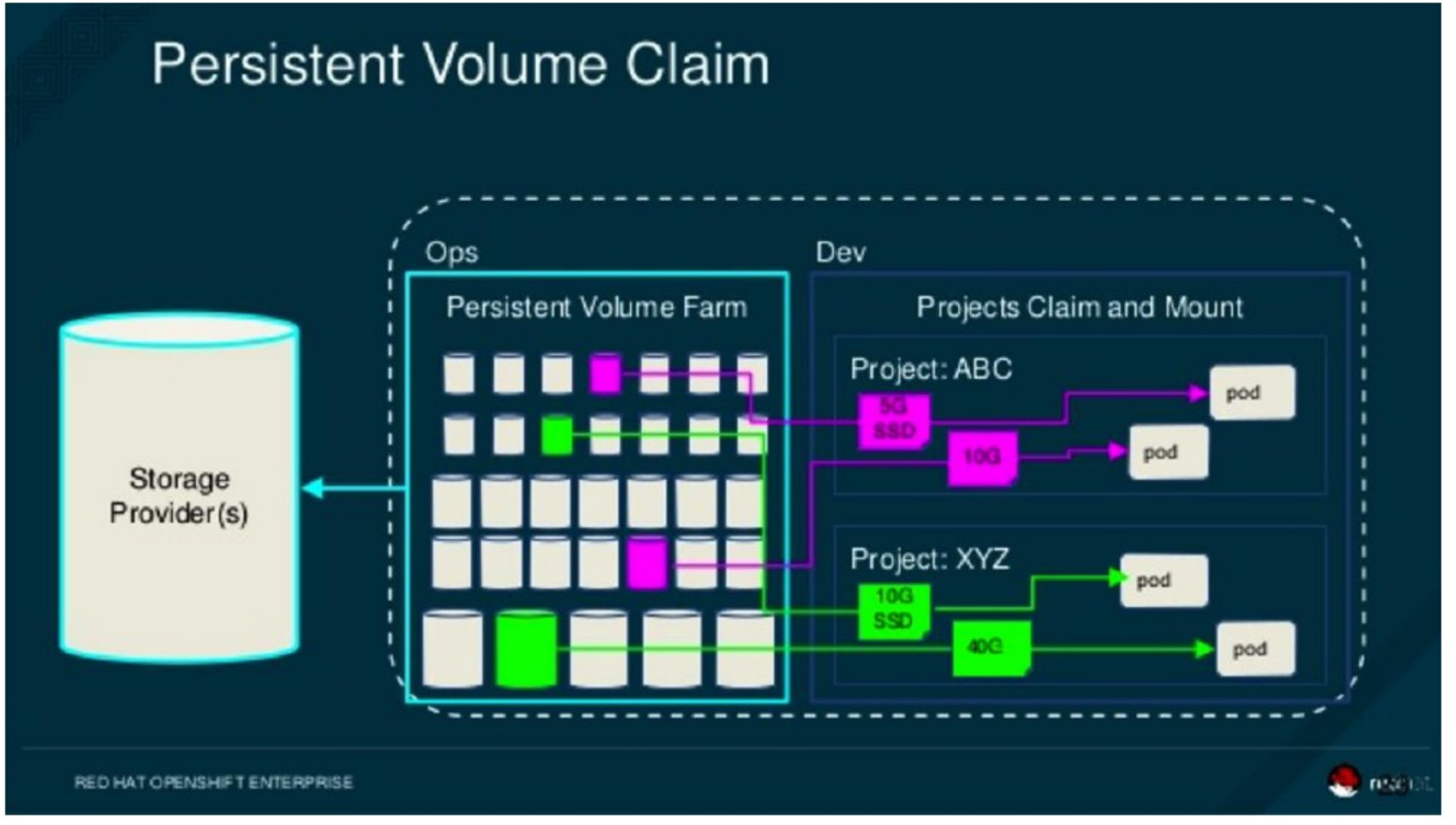
```
kind: PersistentVolume
metadata:
  name: pv0003
spec:
  capacity:
    storage: 8Gi
  accessModes:
   - ReadWriteOnce
  nfs:
    path: /tmp
    server: 172.17.0.2
```

```
kind: PersistentVolumeClaim
metadata:
  name: myclaim
spec:
  accessModes:
   - ReadWriteOnce
  resources:
    requests:
      storage: 8Gi
```

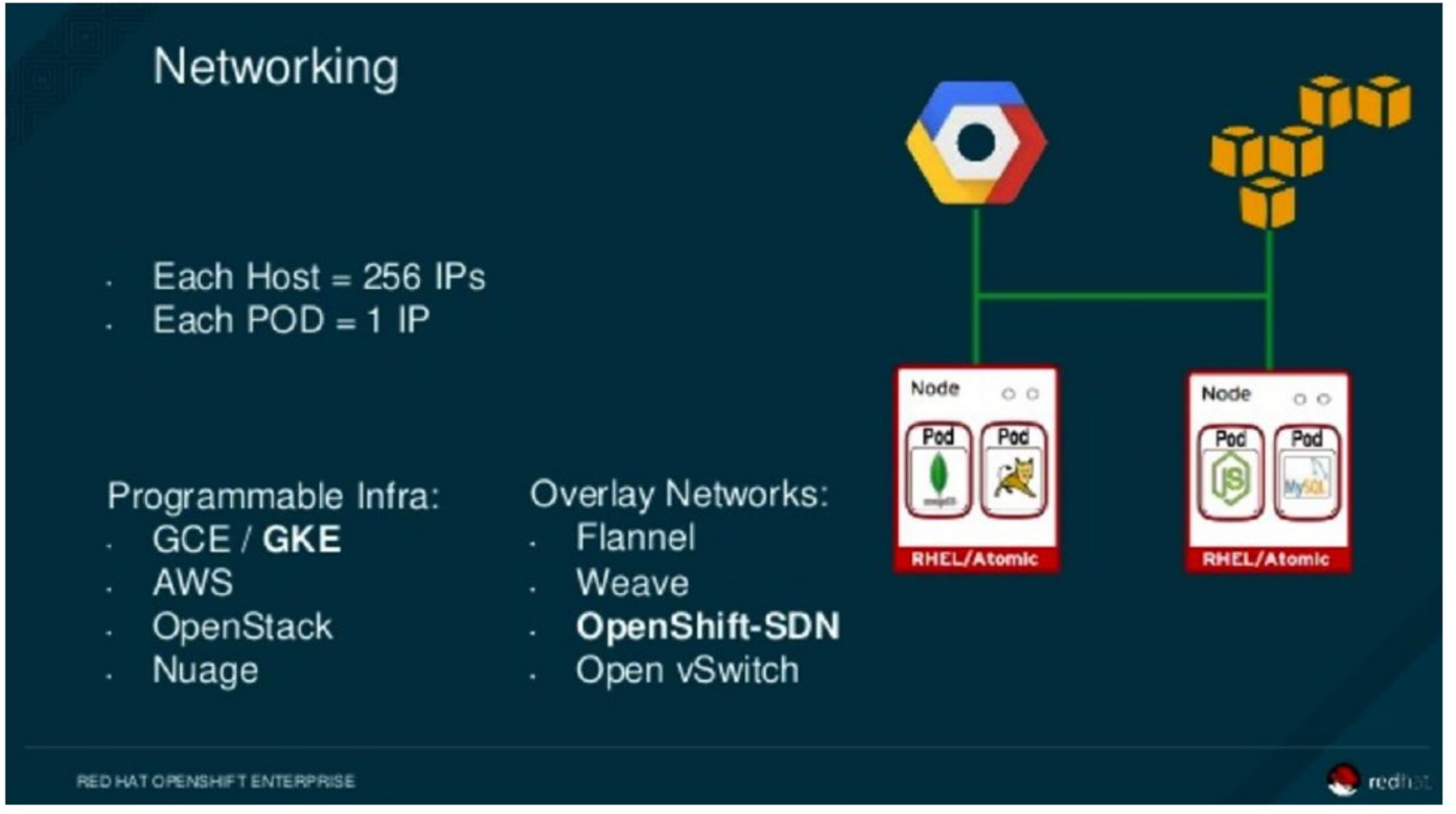


Kubernetes PersistentVolumeClaim

火龙果・整理
uml.org.cn

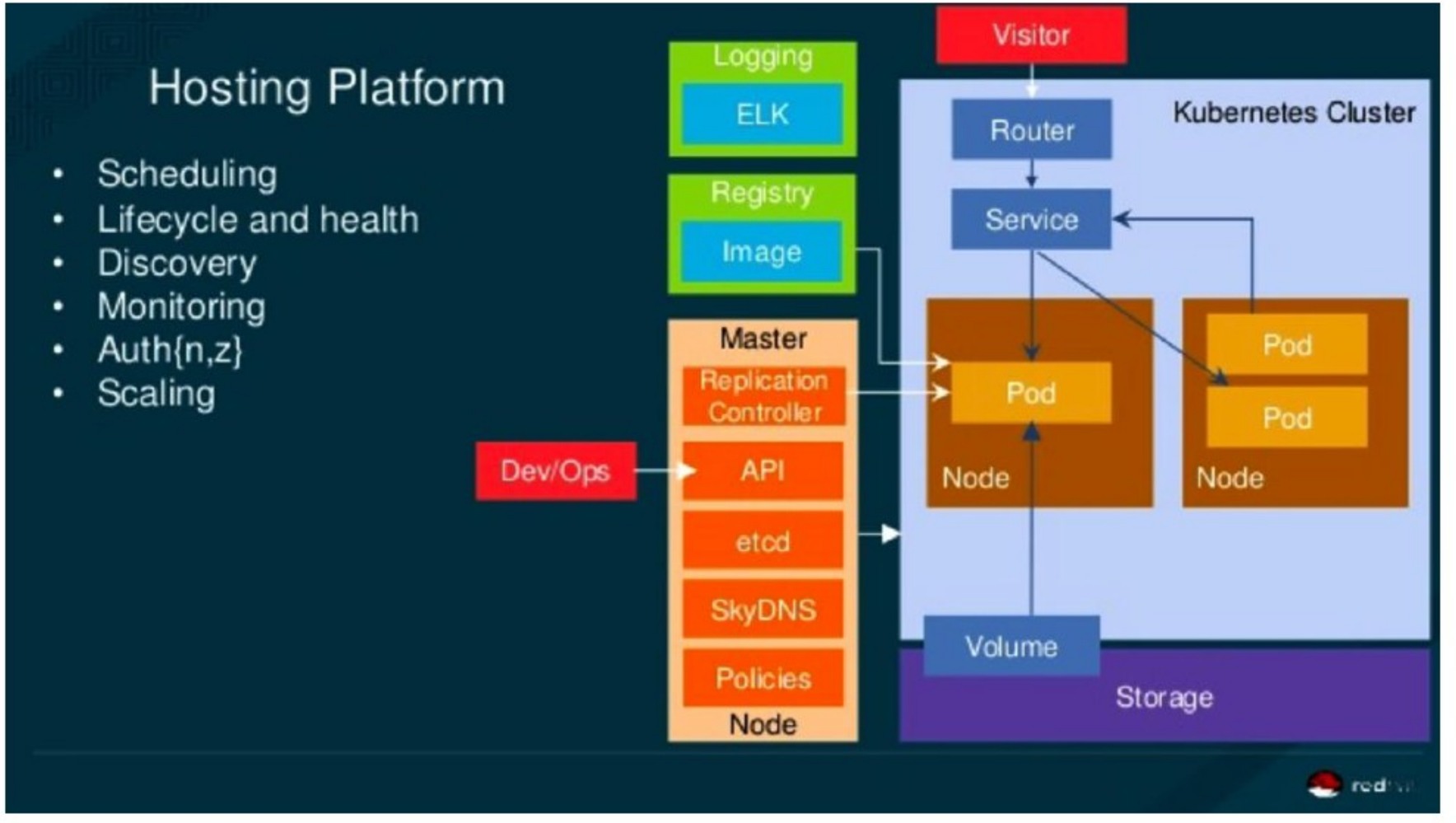


Kubernetes Networking



火龙果 · 整理
uml.org.cn

Kubernetes Overview



火龙果 · 整理
uml.org.cn

多租户

1. Namespace
2. ServiceAccount
3. Role
4. RoleBind
5. ClusterRole
6. ClusterRoleBind
7. NetworkPolicy
8. ResourceQuota
9. Secret

火龙果 · 整理
uml.org.cn

调度

火龙果 · 整理
uml.org.cn

1. Node的亲和性和反亲和性(Affinity/Anti-Affinity)
2. Node的污点和容忍(Taints and Tolerations)
3. Pod的亲和性和反亲和性(Affinity/Anti-Affinity)
4. 自定义调度器

App 高可用

火龙果・整理
uml.org.cn

1. Replication Controller
2. Deployment + Replica Set
3. Service expose 服务去代理pod
4. Deployment 的灰度发布 / 版本控制 / 回滚
5. Daemon Set
6. Stateful Set
7. Keepalived
8. Autoscale

App 访问

火龙果 · 整理
uml.org.cn

1. 外部：
   a. Service Nodeport
   b. Ingress
   c. Keepalived + Service Nodeport
   d. Service-Loadbalance
   e. Loadbalance + 云提供商
2. 内部：
   a. Service cluster ip
   b. 在pod 里 使用 Service name

服务发现

1. Service
2. Ingress
3. Kube-Dns

火龙果 · 整理
uml.org.cn

权限

1. ServiceAccount
2. Role
3. RoleBind
4. ClusterRole
5. ClusterRoleBind

火龙果・整理
uml.org.cn

Job/GPU

火龙果・整理
uml.org.cn

1. Job: 支持并行运行task
2. GPU：安装Nvidia drivers在work node

```
apiVersion: v1
kind: pod
spec:
    containers:
        - name: gpu-container-1
          resources: limits: alpha.kubernetes.io/nvidia-gpu: 2
        - name: gpu-container-2
          resources: limits: alpha.kubernetes.io/nvidia-gpu: 3
```

网络(提供接口由第三方以插件实现)

火龙果 · 整理
uml.org.cn

1. Weave
2. Calico
3. Cni
   a. bridge plugin
   b. dhcp plugin
   c. host local
   d. ipvlan
   e. macvlan
   f. ptp
   g. tuning

存储(内置插件)

火龙果・整理
uml.org.cn

1. StorageClass
2. PersistentVolume
3. PersistentVolumeClaim
4. ConfigMap

支持：
NFS,Scaleio,PX,Ceph,Vsphere,Glusterfs,GCE,AWS,HostPath,EmptyDir

监控

火龙果・整理
uml.org.cn

1. Heapster + influxdb + grafana
2. Promethues + Kubelet + NodeExporter
3. Sysdig
4. Kube-state-metrics + Promethues

日志

1. Logspout + Graylog/ELK

火龙果 · 整理
uml.org.cn

UI

1. Kubernetes Dashboard

火龙果・整理
uml.org.cn

集群高可用

火龙果 · 整理
uml.org.cn

1. Etcd 集群
2. 多api service 提供loadbalance
3. 多Controller Manager（ master / standby 机制 ）
4. 多 Schedular（ master / standby 机制 ）

多集群

火龙果・整理
uml.org.cn

1. Federation API Server 提供一个标准的Kubernetes API
2. Federation Controller Manager 是Federation 的控制中心
3. 支持跨kubernetes集群的service，支持跨集群的dns 服务发现

Question?

火龙果 · 整理
uml.org.cn

1. Kubernetes 的容器运行在哪里？
2. Kubernetes 的容器怎样expose出去，以及支持几种访问方式？
3. Kubernetes 的容器存储支不支持动态create volume？
4. Kubernetes 的存储支不支持portworx？
5. Kubernetes 的网络支持不支持weave和calico，以及有没有macvlan ？
6. Kubernetes 的网络支持不支私有网络？
7. Kubernetes 的应用支持不支持健康检查？以及支持几种检查方式？
8. Kubernetes 支不支持有状态的服务？
9. Kubernetes 支不支持复杂容器编排，如排它 / 粘性，指定主机，多租户隔离？
10. Kubernetes 支不支持applb的访问方式？
11. Kubernetes 支不支持多集群调度和管理？
12. Kubernetes 支不支持复杂权限管理，如基于group, user和role 的细粒度控制？
13. Kubernetes 支不支持灰度发布和自动伸缩？
14. Kubernetes 支不支持配置中心？
15. Kubernetes 有没有自带的监控？
16. Kubernetes 部署app的方式有几种？
17. Kubernetes 能不能做到一键安装？
18. Kubernetes 支不支持多job 和 gpu？