Kubetastic

Or how to provision AWS-/Cloud Native Services for multi tenant

Problem space

Our customers

- demand AWS native services to be used out of K8s
- need access to the provisioned resources
    - through CLI
    - through AWS Web GUI
- demand access isolation through permission mgmt

Assumptions

- namespace = tenant
- cluster and native services => same account
- customers are provided a login role

Solution sketch (1/2)

General

- IAM Role per namespace with assumable accounts configured by the customer (= login roles)
- Enhanced kube2iam for injecting IAM role credentials

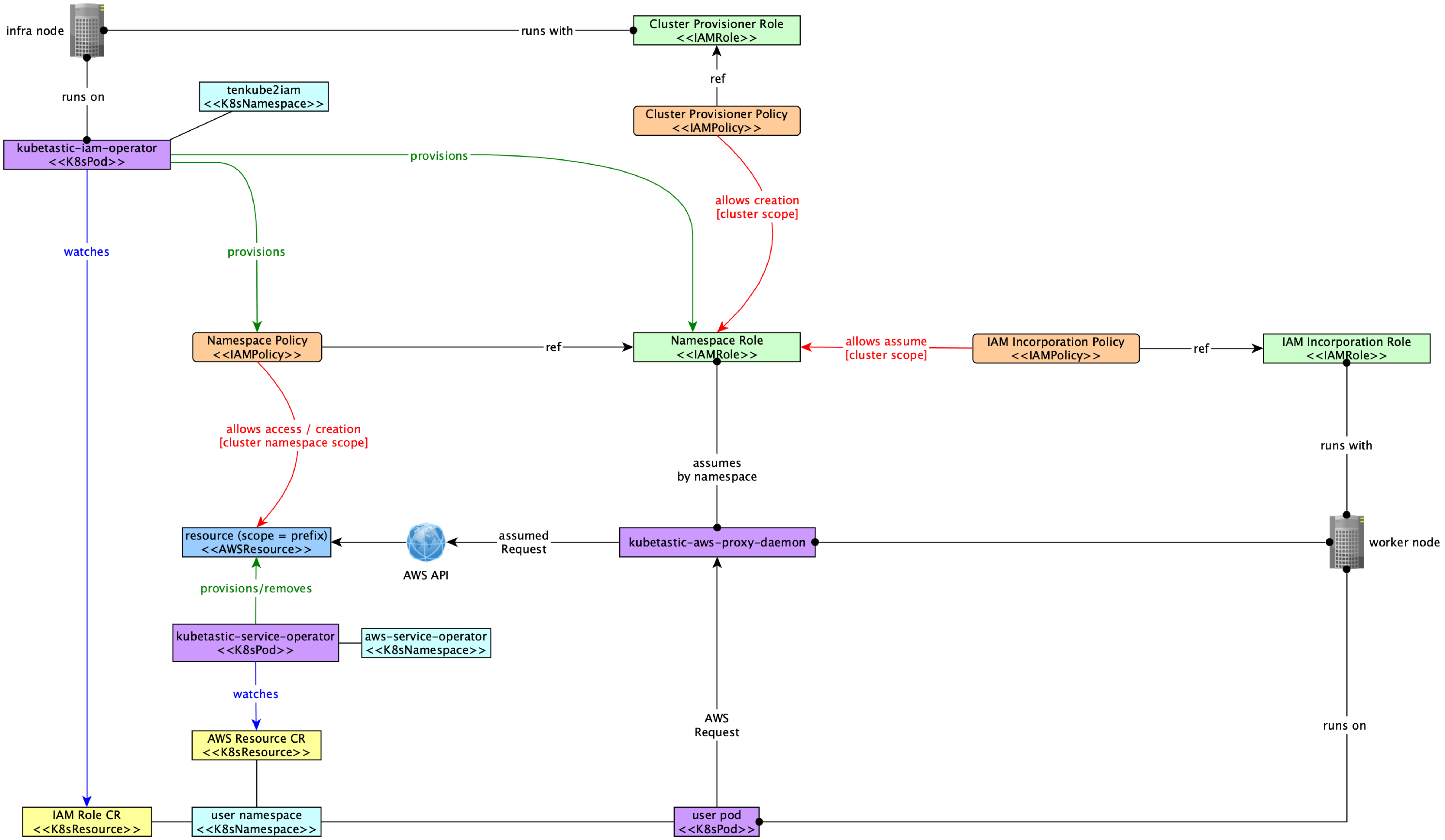
AWS services

- provisioning with scoped names (cluster + namespace)
- IAM role owner tag

Permissions

- Policies using the the IAM role owner tag

Solution sketch (2/2)


infra node
runs with
Cluster Provisioner Role <<IAMRole>>
ref
runs on
tenkube2iam <<K8sNamespace>>
Cluster Provisioner Policy <<IAMPolicy>>
kubetastic-iam-operator <<K8sPod>>
provisions
allows creation [cluster scope]
watches
provisions
Namespace Policy <<IAMPolicy>>
ref
Namespace Role <<IAMRole>>
allows assume [cluster scope]
IAM Incorporation Policy <<IAMPolicy>>
ref
IAM Incorporation Role <<IAMRole>>
allows access / creation [cluster namespace scope]
runs with
assumes by namespace
resource (scope = prefix) <<AWSResource>>
AWS API
assumed Request
kubetastic-aws-proxy-daemon
worker node
provisions/removes
kubetastic-service-operator <<K8sPod>>
aws-service-operator <<K8sNamespace>>
watches
AWS Resource CR <<K8sResource>>
AWS Request
runs on
IAM Role CR <<K8sResource>>
user namespace <<K8sNamespace>>
user pod <<K8sPod>>