Cluster API (CAPI) on air-gapped environments

A journey without the Internet

Hugo Prudente
@hugoprudente

Principal, Site Reliability Engineer (SRE)

Workday, Inc @ Dublin - Ireland

June 19, 2024

Agenda

- Metalhead
- Dev/Ops
- Open Source and Free Software
- Linux
- Computer Vision
- Cycling
- CKA & CKAD
- https://hugoprudente.github.io
- https://nerdweek.com.br
- Workday Inc | Private Cloud Team.

Axioms

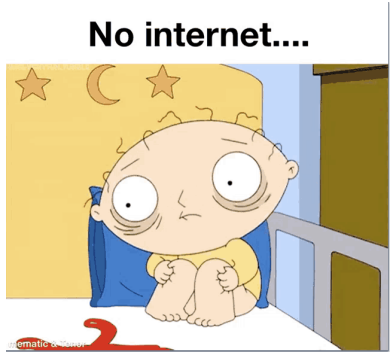

Figure: no-internet

you must know...

Air Gap is a network security measure employed to ensure that a secure computer network is physically isolated from unsecured networks, such as the public Internet.

CAPI or Cluster API is a declarative APIs and tooling to simplify provisioning, upgrading, and operating multiple Kubernetes clusters

CAPO or Cluster API Openstack Operator is the Kubernetes-native declarative infrastructure for OpenStack

CCM or Community, 2024 is a Kubernetes control plane component that embeds cloud-specific control logic.

Image created with image-builder prepared to be a Air Gapped, with containerd, kube-scheduler, kube-proxy, core-dns, and etcd cached.

Cluster API Configurations

tree -L 3 .cluster-api

```
.cluster-api
|-- clusterctl.yaml
|-- overrides
|   |-- bootstrap-kubeadm
|   |   |-- v1.6.3
|   |-- cluster-api
|   |   |-- v1.6.3
|   |-- control-plane-kubeadm
|   |   |-- v1.6.3
|   |-- infrastructure-openstack
|       |-- v0.9.0
|-- resources
    |-- cert-manager
    |   |-- v1.14.4
    |-- cilium
    |   |-- v1.15.3
    |-- metrics-server
        |-- v0.7.0
    |-- openstack_ccm
        |-- v1.30.0
        |-- :)
```

.cluster-api/clusterctl.yaml

```
EXP_CLUSTER_RESOURCE_SET: "true"
cert-manager:
  url: "${HOME}/.cluster-api/resources/cert-manager/v1.14.4/cert-manager.yaml"
  version: "v1.14.4"
images:
    cert-manager:
      repository: pvt.artifactory.nerdweek.com/jetstack
    infrastructure-openstack:
      repository: pvt.artifactory.nerdweek.com/capi-openstack
    control-plane-kubeadm:
      repository: pvt.artifactory.nerdweek.com/cluster-api
    bootstrap-kubeadm:
      repository: pvt.artifactory.nerdweek.com/cluster-api
    cluster-api:
      repository: pvt.artifactory.nerdweek.com/cluster-api
providers:
  - name: "cluster-api"
    url: "${HOME}/.cluster-api/overrides/cluster-api/v1.6.3/core-components.yaml"
    type: "CoreProvider"
  - name: "kubeadm"
    url: "${HOME}/.cluster-api/overrides/bootstrap-kubeadm/v1.6.3/bootstrap-components.yaml"
    type: "BootstrapProvider"
  - name: "kubeadm"
    url: "${HOME}/.cluster-api/overrides/control-plane-kubeadm/v1.6.3/control-plane-components.yaml"
    type: "ControlPlaneProvider"
  - name: "openstack"
    url: "${HOME}/.cluster-api/overrides/infrastructure-openstack/v0.9.0/infrastructure-components.yaml"
    type: "InfrastructureProvider"
```

clusterctl config repositories | grep -v https

NAME	TYPE	URL	FILE
cluster-api	CoreProvider	/root/.cluster-api/overrides/cluster-api/v1.6.3/	core-components.yaml
kubeadm	BootstrapProvider	/root/.cluster-api/overrides/bootstrap-kubeadm/v1.6.3/	bootstrap-components.yaml
kubeadm	ControlPlaneProvider	/root/.cluster-api/overrides/control-plane-kubeadm/v1.6.3/	control-plane-components.yaml
openstack	InfrastructureProvider	/root/.cluster-api/overrides/infrastructure-openstack/v0.9.0/	infrastructure-components.yaml

clusterctl custom crd

```
apiVersion: addons.cluster.x-k8s.io/v1beta1
kind: ClusterResourceSet
metadata:
  name: cloud-controller-manager
  namespace: default
spec:
  clusterSelector:
    matchLabels:
      cloud-controller-manager: openstack
  resources:
  - kind: ConfigMap
    name: cloud-controller-manager-cm
```

infrastructure-openstack/*/cluster-template.yaml

```
apiVersion: bootstrap.cluster.x-k8s.io/v1beta1
kind: KubeadmConfigTemplate
metadata:
  name: ${CLUSTER_NAME}-md-0
spec:
  template:
    spec:
      preKubeadmCommands:
        - systemctl restart containerd
        - systemctl restart chronyd.service
      files:
        - path: /tmp/dummy
          content: |
            dummy
      clusterConfiguration:
        imageRepository: "pvt.artifactory.nerdweek.com/"
        dns:
          imageRepository: "pvt.artifactory.nerdweek.com/coredns"
      joinConfiguration:
        nodeRegistration:
          kubeletExtraArgs:
            cloud-provider: external
            provider-id: openstack:///'{{ instance_id }}'
          name: '{{ local_hostname }}'
```

infrastructure-openstack/*/cluster-template.yaml

```
apiVersion: controlplane.cluster.x-k8s.io/v1beta1
kind: KubeadmControlPlane
metadata:
  name: ${CLUSTER_NAME}-control-plane
  annotations:
spec:
  kubeadmConfigSpec:
    clusterConfiguration:
      networking:
        serviceSubnet: 192.170.0.1/16
      apiServer:
        extraArgs:
          cloud-provider: external
          profiling: "false"
          audit-log-path: /var/log/kube-apiserver/audit.log
          audit-log-maxage: "30"
          audit-log-maxbackup: "10"
          audit-log-maxsize: "100"
      controllerManager:
        extraArgs:
          cloud-provider: external
          profiling: "false"
      scheduler:
        extraArgs:
          profiling: "false"
      imageRepository: "pvt.artifactory.nerdweek.com/"
      dns:
       imageRepository: "pvt.artifactory.nerdweek.com/coredns"
    initConfiguration:
      skipPhases:
        - addon/kube-proxy
      nodeRegistration:
        kubeletExtraArgs:
          cloud-provider: external
          provider-id: openstack:///'{{ instance_id }}'
        name: '{{ local_hostname }}'
    joinConfiguration:
      nodeRegistration:
        kubeletExtraArgs:
          cloud-provider: external
          provider-id: openstack:///'{{ instance_id }}'
        name: '{{ local_hostname }}'
  machineTemplate:
    infrastructureRef:
      apiVersion: infrastructure.cluster.x-k8s.io/v1alpha7
      kind: OpenStackMachineTemplate
      name: ${CLUSTER_NAME}-control-plane
  replicas: ${CONTROL_PLANE_MACHINE_COUNT}
  version: ${KUBERNETES_VERSION}
```

Demo

References

- Community, Kubernetes (2024). Cloud Controller Manager. URL: https://kubernetes.io/docs/concepts/architecture/cloud-controller/.
- KubeSigs, Kubernetes (2024). Cluster API. URL: https://cluster-api.sigs.k8s.io/.
- KubeSigs, Openstack (2024). Cluster API Openstack Operator. URL: https://cluster-api-openstack.sigs.k8s.io/getting-started.

powered by LaTeX

Thank You!

Figure: Linkedin

Figure: We are Hiring!!!

Hugo Prudente
@hugoprudente

Principal, Site Reliability Engineer (SRE)

workday.

- github.com/hugoprudente/presentations-pub
- hugoprudente.github.io
- nerdweek.com.br