

云联壹云

资源编排设计与实现

云联壹云核心产品融合云 云联壹云秉承：简单、开放、融合、智能的产品理念，能够帮助企业实现异构IT基础设施的全面云化、统一管理及成本优化，提高运维效率的同时，降低企业运营成本。

郑雨 工程师 2020-09-23

目录

CONTENTS

01 方案选择--K8S

02 Pod 与虚拟机

03 应用和 Helm

04 问题与改进

01

方案选择--K8S

- 什么是资源编排
- vSphere with K8S
- Terreform vs K8S
- 云联壹云 with K8S

什么是资源编排

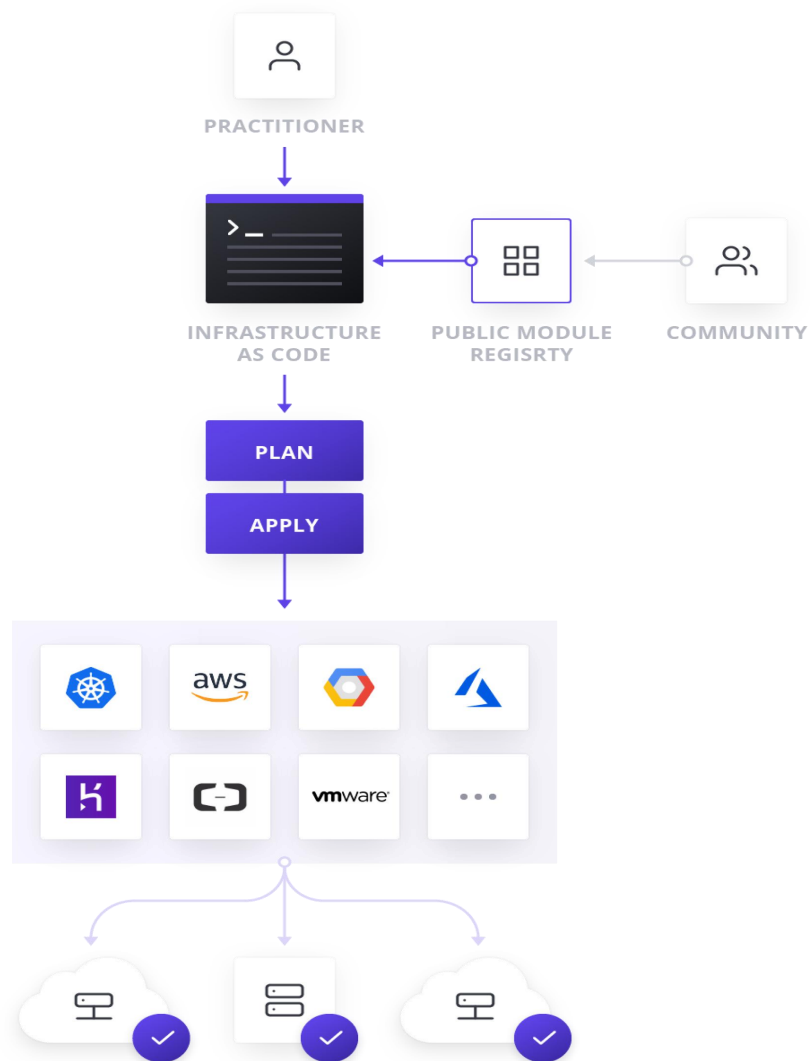
快速交付云资源+快速部署应用

1. 使用 k8s 的api 操作云资源
2. 使用 ansible 部署应用
3. 使用 helm 整合 k8s 的yaml 文件，并提供复用性。



Terraform

Use Infrastructure as Code to provision and manage any cloud, infrastructure, or service

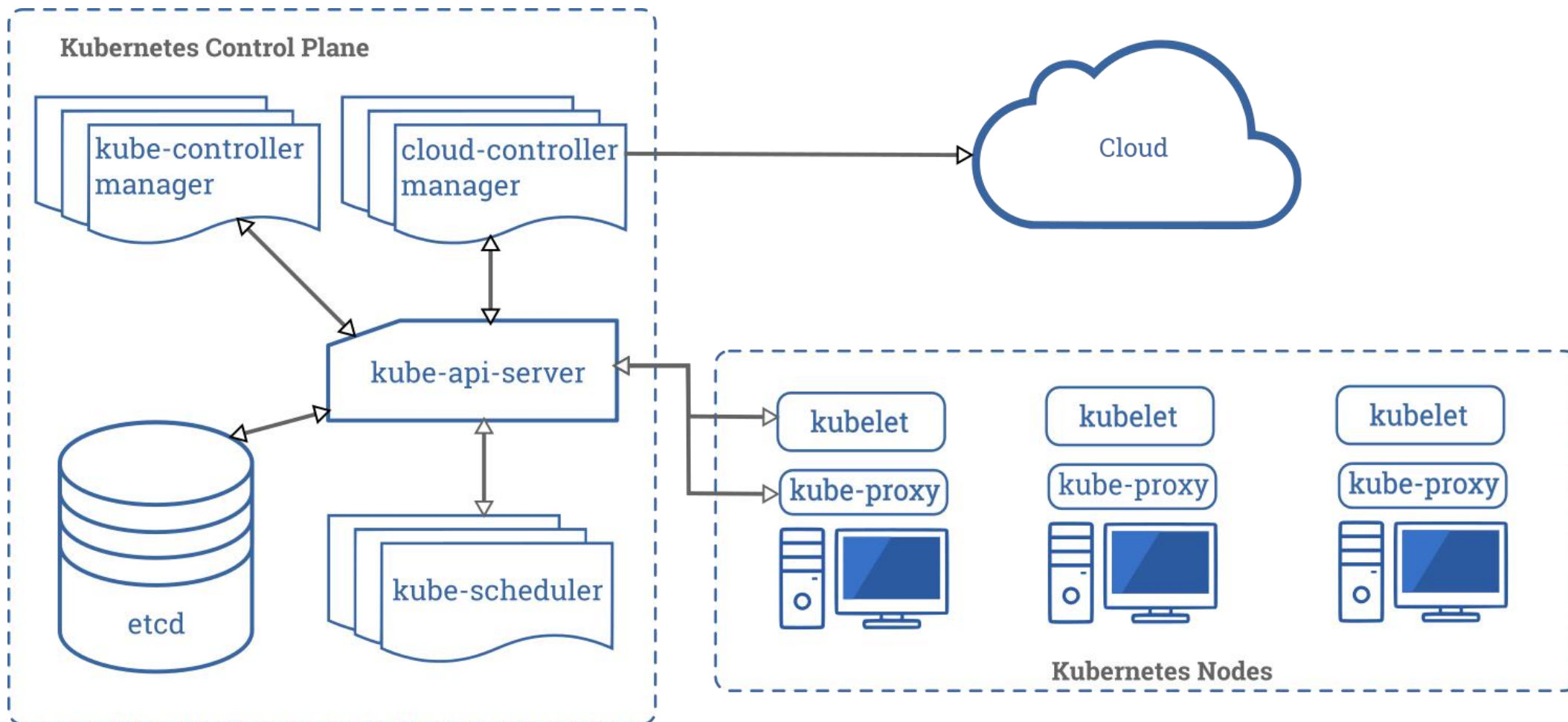


Terraform CLI读取配置文件并提供更改的执行计划，然后进行应用和配置。

依赖于可扩展的 provider，Terraform管理广泛的资源，包括硬件，IaaS，PaaS和SaaS服务。

Kubernetes

一个可移植的、可扩展的开源平台，用于管理容器化的工作负载和服务，可促进声明式配置和自动化。



Terraform vs K8S



VS



优点:

1. 为IAC而设计，各大云提供商有着广泛的支持；一次配置，到处使用
2. 架构简单，上手容易
3. 扩展方便，只需要在框架下开发对应的provider

缺点:

1. 状态保存在 tfstate 文件中，只是一个CLI。对云上资源的状态没有同步的机制

优点:

1. 设计良好，应用广泛
2. 开发灵活，深度定制
3. 不只是一个CLI

缺点:

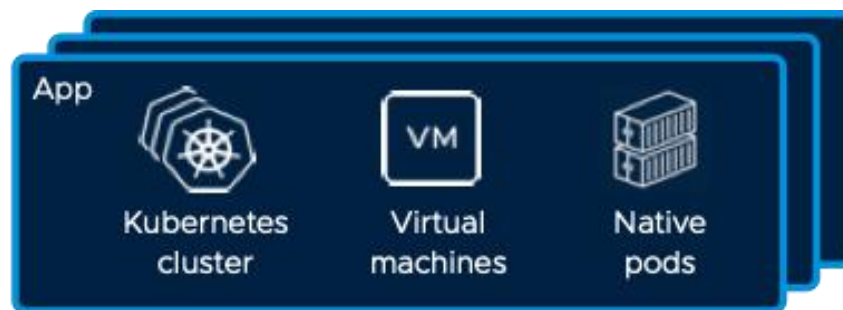
1. 配置复杂，上手不易
2. 云提供商之间的api不统一

得益于云联壹云统一了对各个云的操作，第二个缺点是可以克服的。

vSphere with K8S

Project Pacific 在 vSphere 平台上原生集成了 Kubernetes

```
kind: VirtualMachine
apiVersion: vms.vmware.com/v1
metadata:
  name: LegacyApp
spec:
  className: large
  imageName: my-app.ova
  powerState: poweredOn
  policy:
    restartPolicy: OnFailure
```



vSphere



Supervisor Kubernetes Cluster

ESXi Cluster

Networking

Storage

vCenter

开发人员



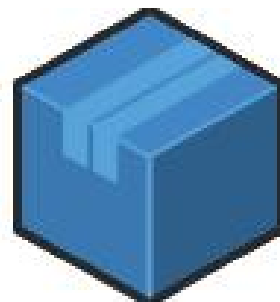
Project Pacific 看起来像 vSphere，但是具有管理整个应用程序的新功能，而不必总是处理组成它的单个 VM。



IT管理员

云联壹云 with K8S

调用 K8S api 通过 云联壹云 来管理私有云、公有云资源



Supervisor Kubernetes Cluster

云联壹云

未云化基础设施

私有云

公有云

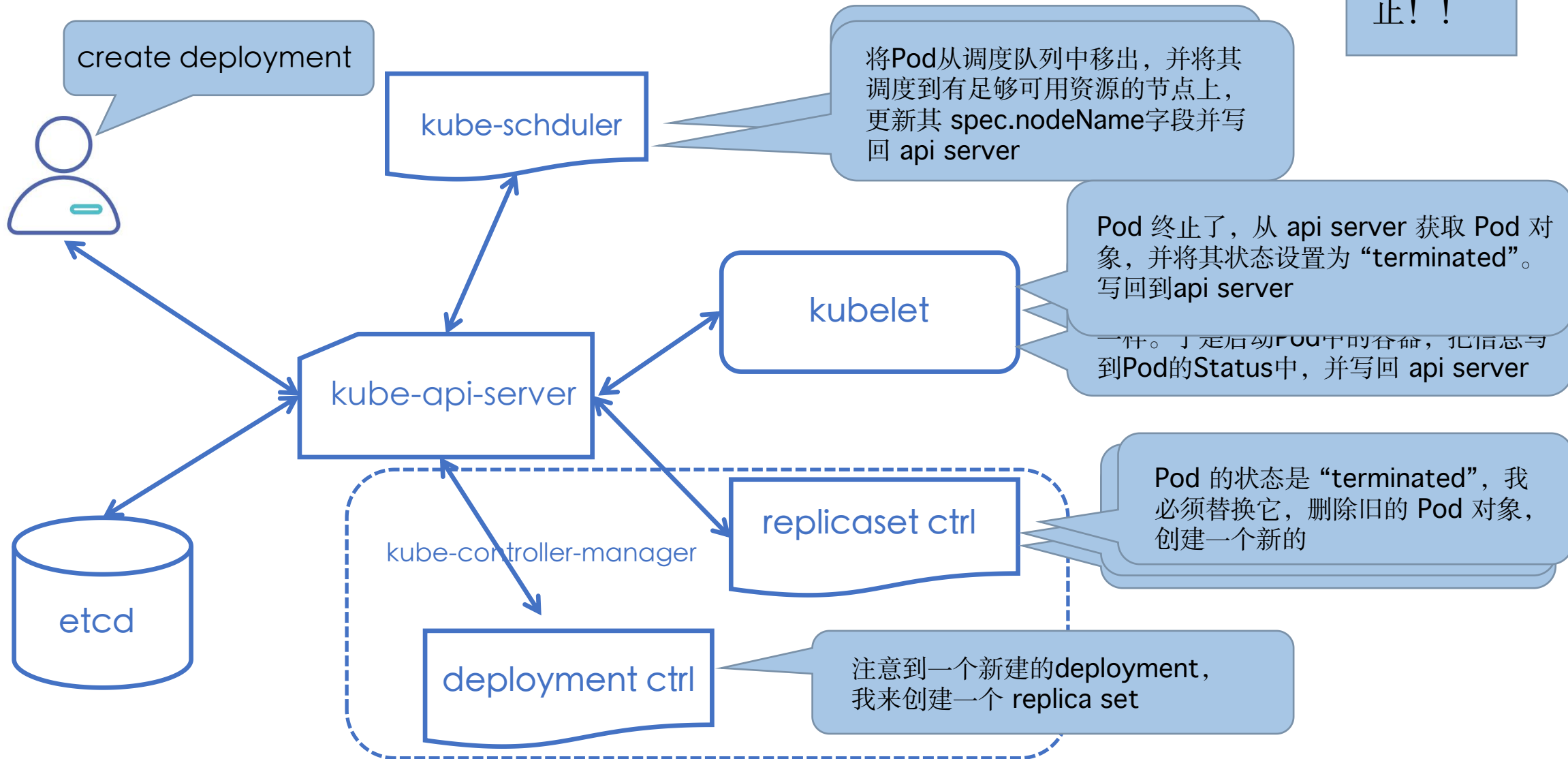
02

Pod 与虚拟机

- 部署Pod
- 部署虚拟机
- Controller and CR

部署 Pod

在 Kubernetes 中，通过 Deployment 部署一个 Pod 时，发生了什么？



部署 虚拟机

如何通过 K8S, 在 云联壹云 中部署一台虚拟机

```
apiVersion: onecloud.yunion.io/v1
kind: VirtualMachine
  name: test
  namespace: onecloud
spec:
  description: Test VM
  projectConfig:
    project: system
  vmConfig:
    hypervisor: kvm
    networks:
      - network: test-net
    rootDisk:
      image: CentOS-7.6.1810-
20190430.qcow2
      sizeGB: 30
      storageConfig:
        backend: local
    vcpuCount: 1
    vmemSizeGB: 1
```

将左边的文本保存为 `vm.yaml`, 然后使用:

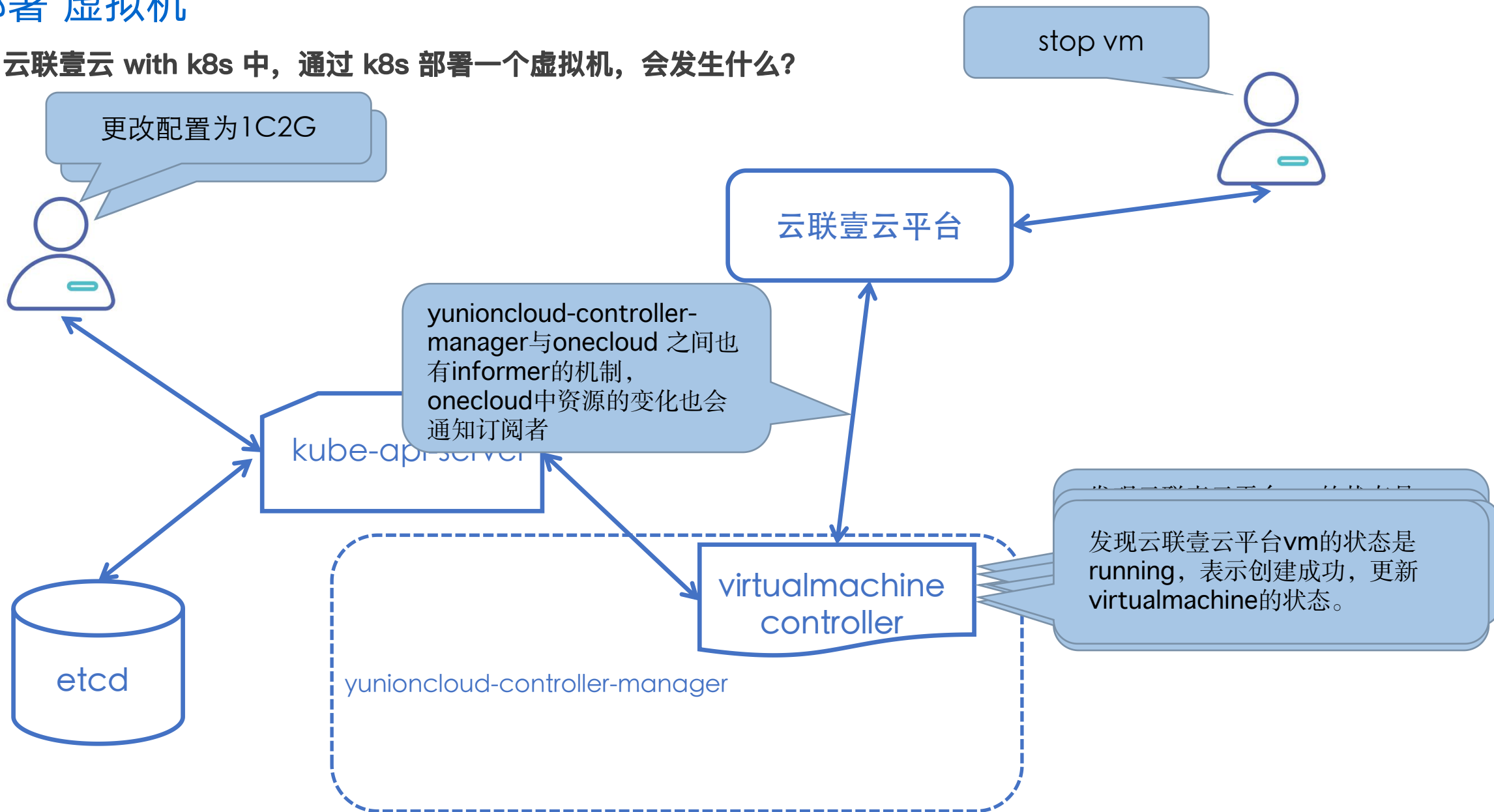
```
kubectl create -f vm.yaml
```

就可以创建一台KVM虚拟机, 其项目为**system**, 具体配置为:

cpu: 1核; **内存:** 1G; **存储:** 30G;
镜像: CentOS-7.6.1810-20190430.qcow2;
网络: test-net;

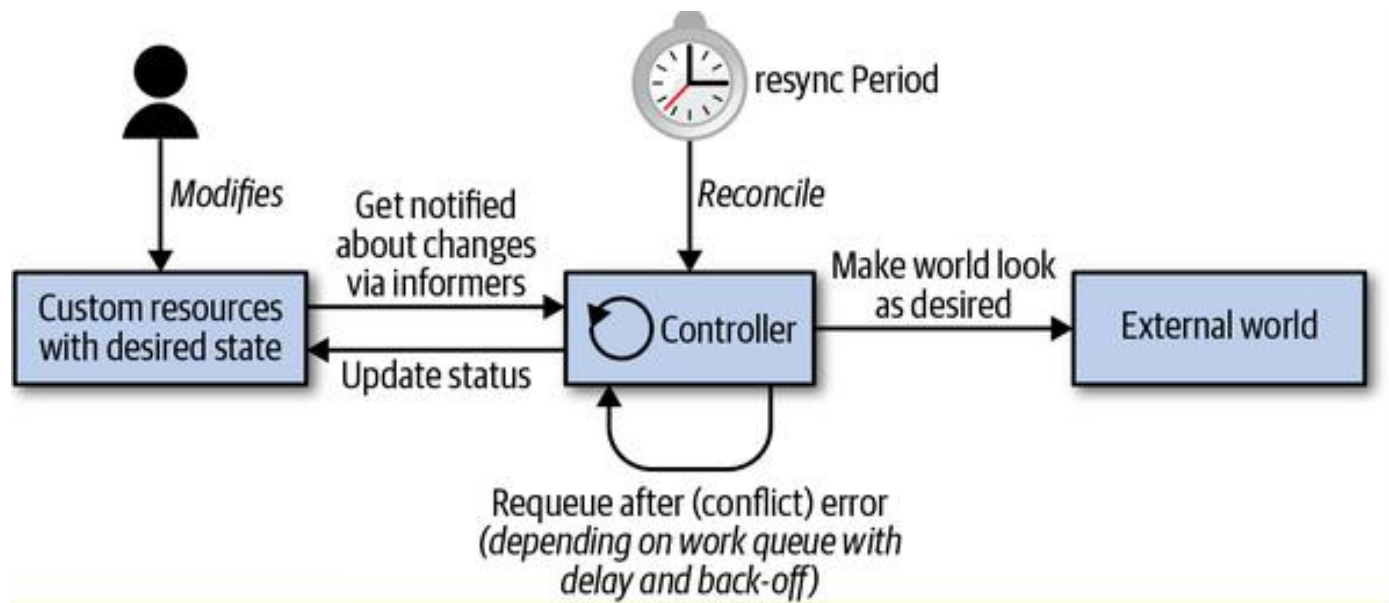
部署 虚拟机

在 云联壹云 with k8s 中，通过 k8s 部署一个虚拟机，会发生什么？



Controller

Controller 监视资源，并不断尝试使资源达到期望的状态



Informer

Work queues

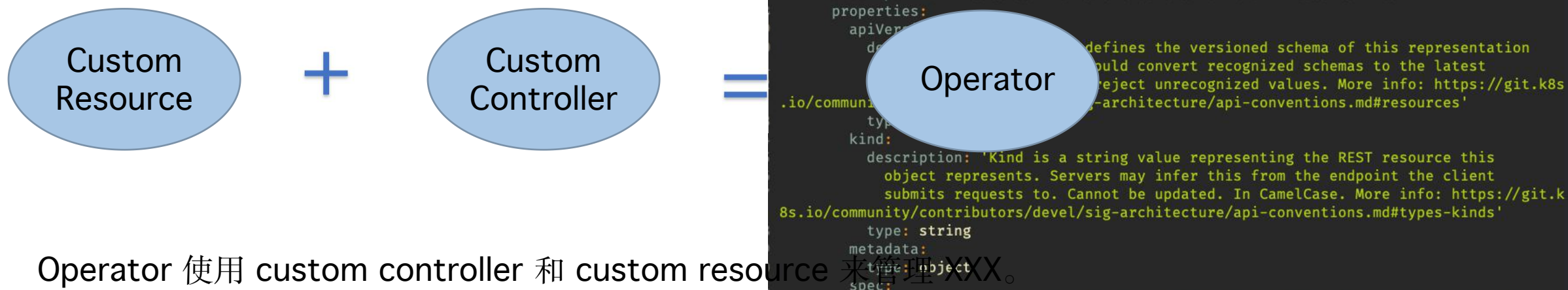
1. 读取资源的状态，往往是通过事件驱动
2. 根据资源的Spec，改变集群内对象或者集群外对象的状态。比如，部署Pod，创建一个网络或者请求云提供商的api。

3. 通过 api server 向 etcd 更新资源的状态
4. 重复循环

CR and Operator

CR(custom resource) 是Kubernetes API的扩展机制。

通过 k8s 提供的 custom resource definition (CRD) 可以定义我们自己的 k8s 资源。



Operator 使用 custom controller 和 custom resource 来管理 XXX。

```
apiVersion: apiextensions.k8s.io/v1beta1
kind: CustomResourceDefinition
metadata:
  annotations:
    controller-gen.kubebuilder.io/version: v0.2.5
  creationTimestamp: null
  name: virtualmachines.onecloud.yunion.io
spec:
  group: onecloud.yunion.io
  names:
    kind: VirtualMachine
    listKind: VirtualMachineList
    plural: virtualmachines
    singular: virtualmachine
  scope: Namespaced
  subresources:
    status: {}
  validation:
    openAPIV3Schema:
      description: VirtualMachine is the Schema for the virtualmachines API
      properties:
        apiVersion:
          description: defines the versioned schema of this representation
          type: string
        kind:
          description: Kind is a string value representing the REST resource this
            object represents. Servers may infer this from the endpoint the client
            submits requests to. Cannot be updated. In CamelCase. More info: https://git.k
            8s.io/community/contributors/devel/sig-architecture/api-conventions.md#types-kinds'
          type: string
        metadata:
          type: object
        spec:
          description: VirtualMachineSpec defines the desired state of VirtualMachine
          properties:
            autoRenew:
              description: AutoRenew indicates whether to automatically renewal.
              type: boolean
            billDuration:
              description: BillDuration describes the duration of the annual and monthly
                billing type. That length of BillDuration represents the billing type
                is 'prepaid'.
              type: string
```

03

部署应用

- Ansible Playbook
- Helm and Charts
- 部署应用
- 前端使用

Ansible Playbook

Ansible playbook 是一种简单的配置管理系统与多机器部署系统的基础。

```
- hosts: jenkins
  become: true

  vars:
    jenkins_hostname:
jenkins.example.com
    java_packages:
      - openjdk-8-jdk

  roles:
    - role: geerlingguy.java
    - role: geerlingguy.jenkins
```

安装role:

```
ansible-galaxy install -r requirements.yml
```

执行:

```
ansible-playbook --inventory inventory.yml
playbook.yml
```

AnsiblePlaybook(Template)

AnsiblePlaybook 和 AnsiblePlaybookTemplate 是 k8s 中

```
apiVersion: onecloud.yunion.io/v1
kind: AnsiblePlaybook
metadata:
  name: jk-test-pk-master
spec:
  playbookTemplateRef:
    name: jk-test-pktem-master
  inventory:
    - virtualMachine:
        name: jk-test-master
  vars:
    jenkins_hostname:
      value: localhost
    jenkins_http_port:
      value: 8080
    jenkins_admin_username:
      value: admin
    jenkins_admin_password:
      value: admin
    onecloud_vm_id:
      reference:
        kind: VirtualMachine
        namespace: onecloud
        name: jk-test-master
        fieldPath: Status.ExternalInfo.Id
    maxRetryTimes: 2
```

```
apiVersion: onecloud.yunion.io/v1
kind: AnsiblePlaybookTemplate
metadata:
  name: jk-test-pktem-master
spec:
  playbook: |
    - hosts: all
      become: true

    vars:
      jenkins_plugins:
        - swarm
      jenkins_version: "2.204"
      telegraf_agent_hostname: jk-test-master
      telegraf_global_tags:
        - tag_name: release_name
          tag_value: test
      telegraf_agent_output:
        - type: influxdb
          config:
            - urls = [""]
            - database = "telegraf"
            - insecure_skip_verify = true
      telegraf_plugins_default:
        - plugin: jenkins
          config:
            - url = "http://localhost:8080"
            - username = "admin"
            - password = "admin"
            - response_timeout = "5s"

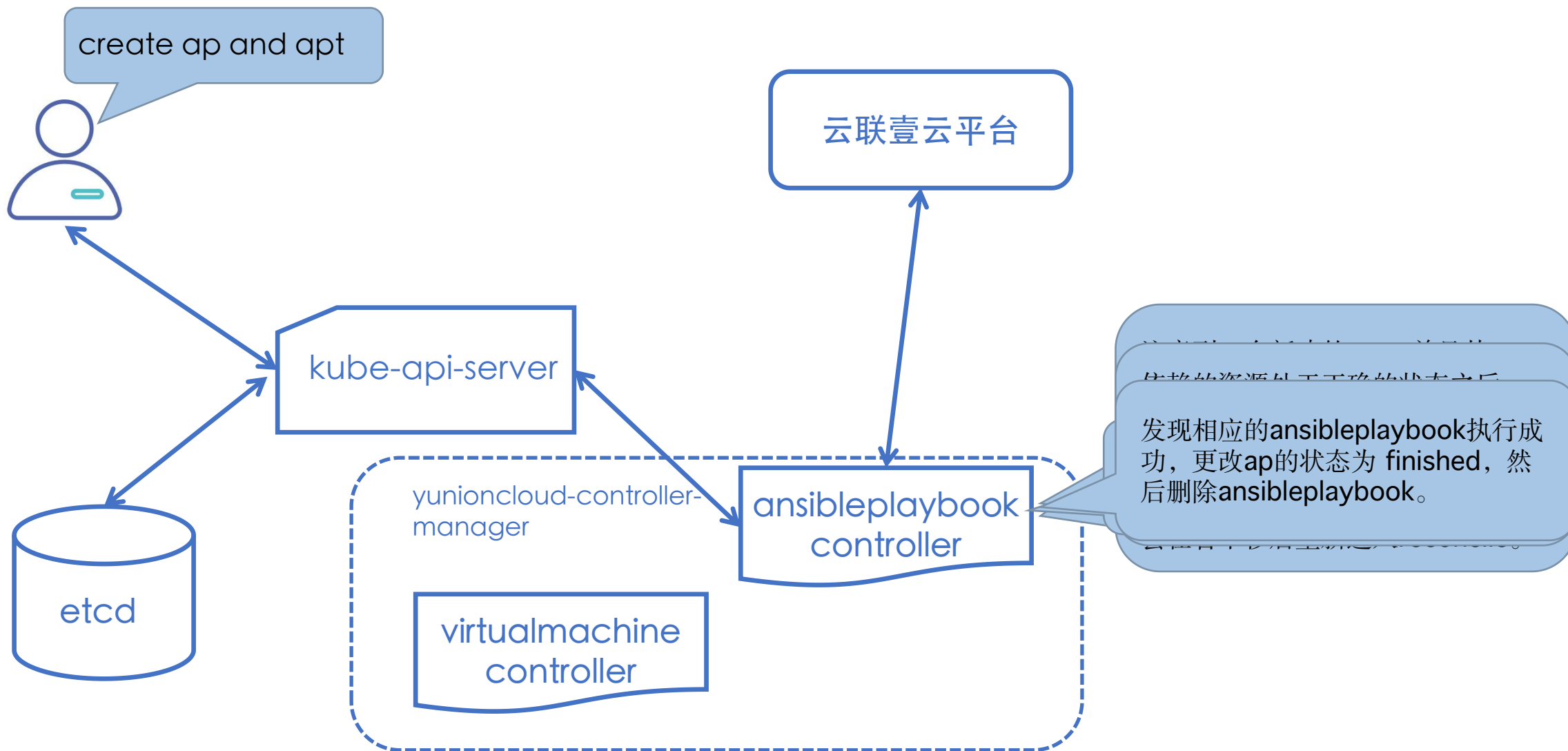
    roles:
      - role: geerlingguy.jenkins
      - role: ansible-telegraf
    requirements: |
      - src: geerlingguy.jenkins
      - src: https://github.com/ansible/ansible-telegraf
      - src: https://github.com/ansible/ansible-telegraf

    vars:
      - name: jenkins_hostname
        default: localhost
      - name: jenkins_http_port
        default: 8080
      - name: jenkins_admin_username
        default: admin
      - name: jenkins_admin_password
        default: admin
      - name: onecloud_vm_id
        required: true
```

AP

部署 应用

在 云联壹云 with k8s 中，部署一个应用会发生什么？



Helm and Charts

在k8s中的helm和charts, 可以类比于在centos中的yum和rpm。

```
project: "system"
preferManager: ""
preferRegion: ""
preferZone: ""
hypervisor: "kvm"
vpc: ""
network: ""
virtualMachines:
  masterNode:
    preferHost: ""
    instanceType: ""
    vcpuCount: 1
    vmemSizeGB: 1
    # 系统盘镜像大小
    diskSizeGB: 30
    # 系统镜像
    image: ""
    # 存储后端类型
    storageBackend: "local"
    ansiblePlaybook:
      jenkins:
        hostname: localhost
        httpPort: 8080
        adminUsername: admin
        adminPassword: admin
      telegraf:
        # required
        influxdbUrl: ""
        influxdbName: telegraf
  slaveNode:
    # slave节点的数量, 可以指定为 0
    count: 1
    preferHost: ""
    # 系统盘镜像大小
    diskSizeGB: 30
    # 系统镜像
    image: ""
    # 主机的套餐, 不能和 vcpuCount或者vmemSize 同时指定
    instanceType: ""
    # 不能和instanceType同时指定, 否则instanceType优先生效
    vcpuCount: 1
    vmemSizeGB: 1
    # 存储后端类型
    storageBackend: "local"
```

执行命令:

```
helm install test forvm/jenkins -f
values.yaml
```


就可以新建一个两个节点的jenkins应用

使用Helm的两个好处:

1. 将复杂的, 众多k8s yaml文件整合起来, 封装成一个整体。
2. 对外提供自定义的参数, 可以修改, 复用。

前端展示

运维工具 ==> 应用市场 ==> 部署



onecloud-jenkins

虚拟机应用

A Helm chart for Jenkins on Onecloud

* 名称:

请输入名称

* 商店-模板版本:

OneCloud - 0.1.0

资源归属项目:

域: Default

项目: lizexi

表单配置

* 平台:

阿里云

请选择平台

* 区域:

阿里云 华北2 (北京)

请选择区域

* 可用区:

阿里云 华北 2 可用区 A

请选择可用区

VPC:

ali-vpc

请选择VPC

* 网络:

请选择

vsw-2zei5rju3x04pk8y7fkmu (172.17.128.1 - 172.17.143.252, vlan=1)

test1qaz (192.168.0.1 - 192.168.255.252, vlan=1)

aliyunv1 (192.168.100.1 - 192.168.100.252, vlan=1)

环境信息

项目ID:

域ID:

* 虚拟机配置

* 主节点

04

问题与改进

- 问题

- 改进

问题

- CR较少，目前只有VirtualMachine, Image, AnsiblePlaybookTemplate, AnsiblePlaybook
- 应用的helm模板不支持自定义
- 使用方式比较原始，还是表单的方式

改进

- 增加较多的CR，下一步要支持包括：Network, VPC, Storage, LB, ScalingGroup 等等
- 将Ansible Playbook加入到运维工具中，使用户可以自己创建并且绑定虚拟机。
- 基础设施模板和应用模板分开，应用模板由上一点生成。
- 基础设施的模板创建：
 - 支持拖拽，以拓扑图的形式展现。
 - 拓扑图中的每一个节点，可以点击并修改详细的配置。
- 使用基础设施的模板后，展示拓扑图中的每一个vm节点，可以绑定相应的应用模板，以部署应用。

2020 THANK YOU

云联壹云核心产品融合云 云联壹云 秉承：简单、开放、融合、智能的产品理念，能够帮助企业实现异构IT基础设施的全面云化、统一管理及成本优化，提高运维效率的同时，降低企业运营成本。

郑雨 工程师 2020-09-23



扫码进技术交流群



更多资讯关注我