



GOps 2021
Shanghai

GOps

全球运维大会

2021
-XOps 风向标



上海站

指导单位：



主办单位：

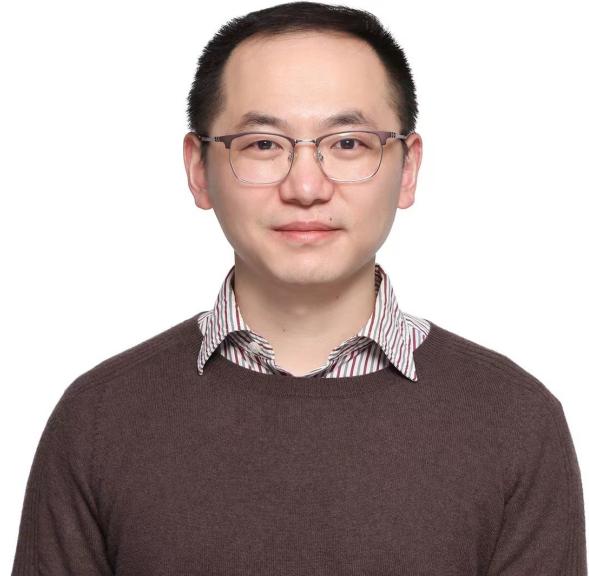


大会时间：2021年11月18日-19日

大会地点：上海中庚聚龙酒店

新一代开源多集群管理与应用治理项目 - Clusternet

徐迪 腾讯云技术专家



徐迪

技术专家

腾讯云技术专家，Clusternet 项目发起人。在云原生领域有着丰富的经验，也是国内较早参与 Kubernetes 社区的开发者，代码贡献量全球 Top 50。热爱开源，拥抱开源，并多次在 KubeCon 各大峰会上发表演讲。目前在腾讯负责分布式云的开发工作。

目录

contents

- ① 背景
- ② Clusternet 开源
- ③ Clusternet – 多集群管理
- ④ Clusternet – 应用分发



PART 1

背景

分布式云是未来

- 成本优化 (Cost Effective)
- 更好的弹性及灵活性 (Elasticity & Flexibility)
- 避免厂商锁定 (Avoid Vendor Lock-in)
- 第一时间获取云上的新功能 (Innovation)
- 容灾 (Resilience & Recovery)
- 数据保护及风险管理 (Data Protection & Risk Management)
- 提升响应速度 (Network Performance Improvements)

分布式云的挑战

- Kubernetes 单集群承载能力有限
- 异构的基础设施
- 存量资源接入
- 配置变更及下发
- 跨地域、跨机房应用部署及管理
- 容灾与隔离性，异地多活
- 弹性调度及自动伸缩
- 监控告警

如何应对

- 通过 Kubernetes 屏蔽底层基础设施，提供统一的接入层
- 多云架构
 - 多集群 ≠ 多云
 - 多集群管控
- 统一的管控面
- 方便接入，降低使用门槛



PART 2

Clusternet 开源

Clusternet 开源

- 11月4日，腾讯联合6家合作伙伴一起开源了 Kubernetes 多集群管理与应用治理项目 Clusternet
- Clusternet 目标是让管理多云、多集群就像上网一样简单

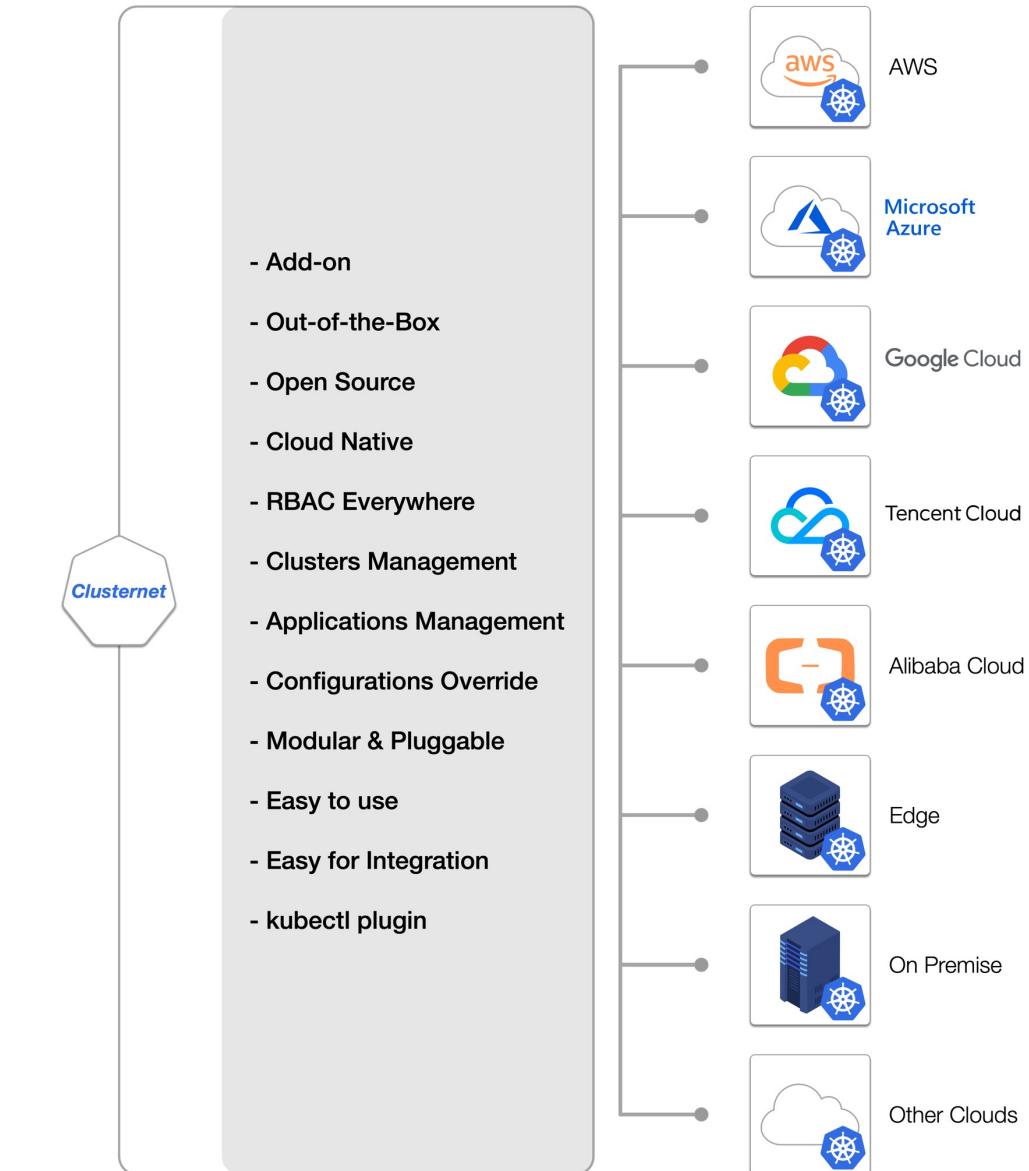


Clusternet 简介

- Clusternet (*Cluster Internet*)是一个兼具多集群管理和跨集群应用编排的开源云原生管控平台，打通了跨 VPC、跨地域、跨云的集群管理。
- Clusternet 面向未来混合云、分布式云和边缘计算场景设计，支持海量集群的接入和管理。
- Clusternet 在保证无侵入且轻量化的基础之上，创建了一张集群网络，对子集群进行纳管，并支持多集群的应用编排与治理。
- 开源项目地址：<https://github.com/clusternet/clusternet>
 - 最新版本 v0.6.0
 - 多平台支持：linux/amd64, linux/arm64, linux/ppc64le, linux/s390x, linux/386, linux/arm

Clusternet 能力一览

- 统一管控各类 Kubernetes 集群
- 集群管理 Pull / Push 模式
- 轻量化，开箱即用，易于部署和维护
- 跨集群的服务发现及服务互访
- Kubernetes 原生，没有额外的学习成本
- 完善的 RBAC 能力，访问任一子集群
- 完善的接入能力：kubectl plugin / client-go
- 支持分发各类原生应用 / CRD / HelmChart





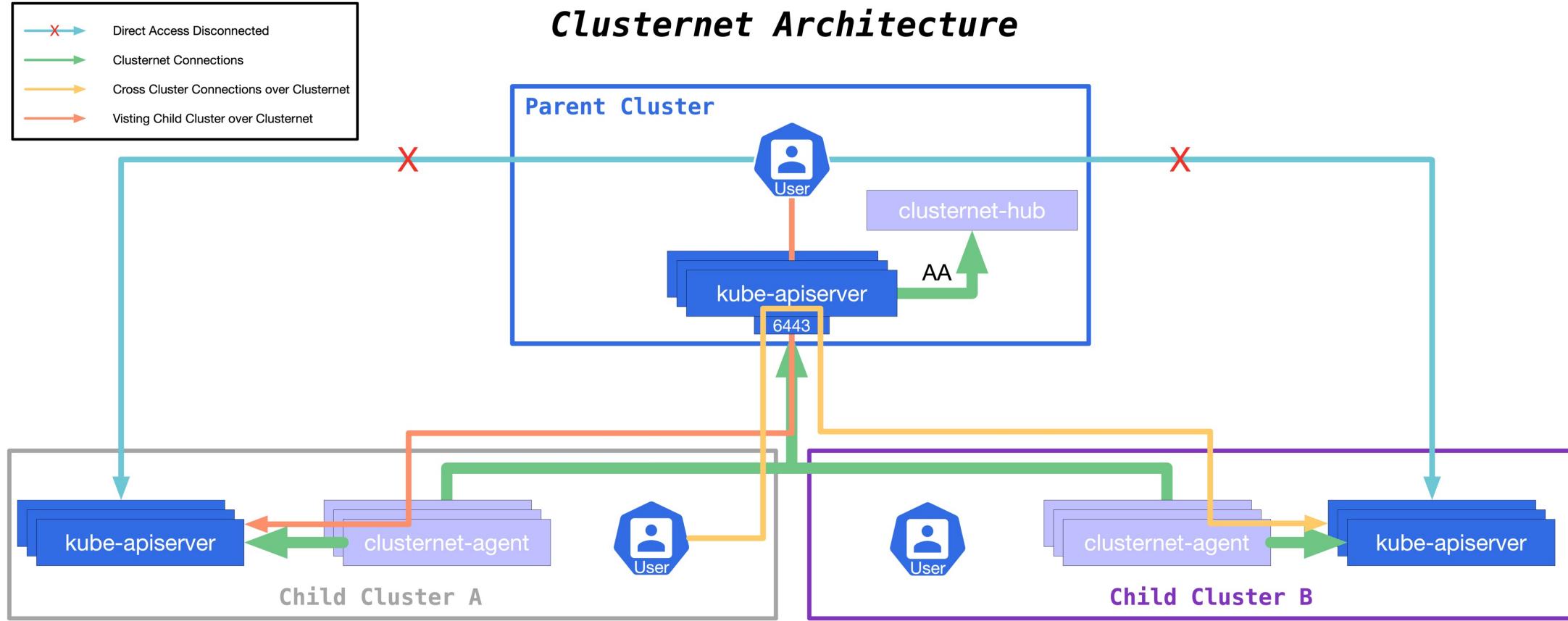
PART 3

Clusternet – 多 集群管理

多集群管理的挑战

- 集群无处不在
 - 公有云、私有云、混合云、边缘、裸金属
- 提供一致的纳管能力
 - 集群一键注册能力
 - 一致性的集群访问体验，比如 exec, logs
 - 权限管控 RBAC
- 架构要足够轻量化，方便一键接入

Clusternet 架构



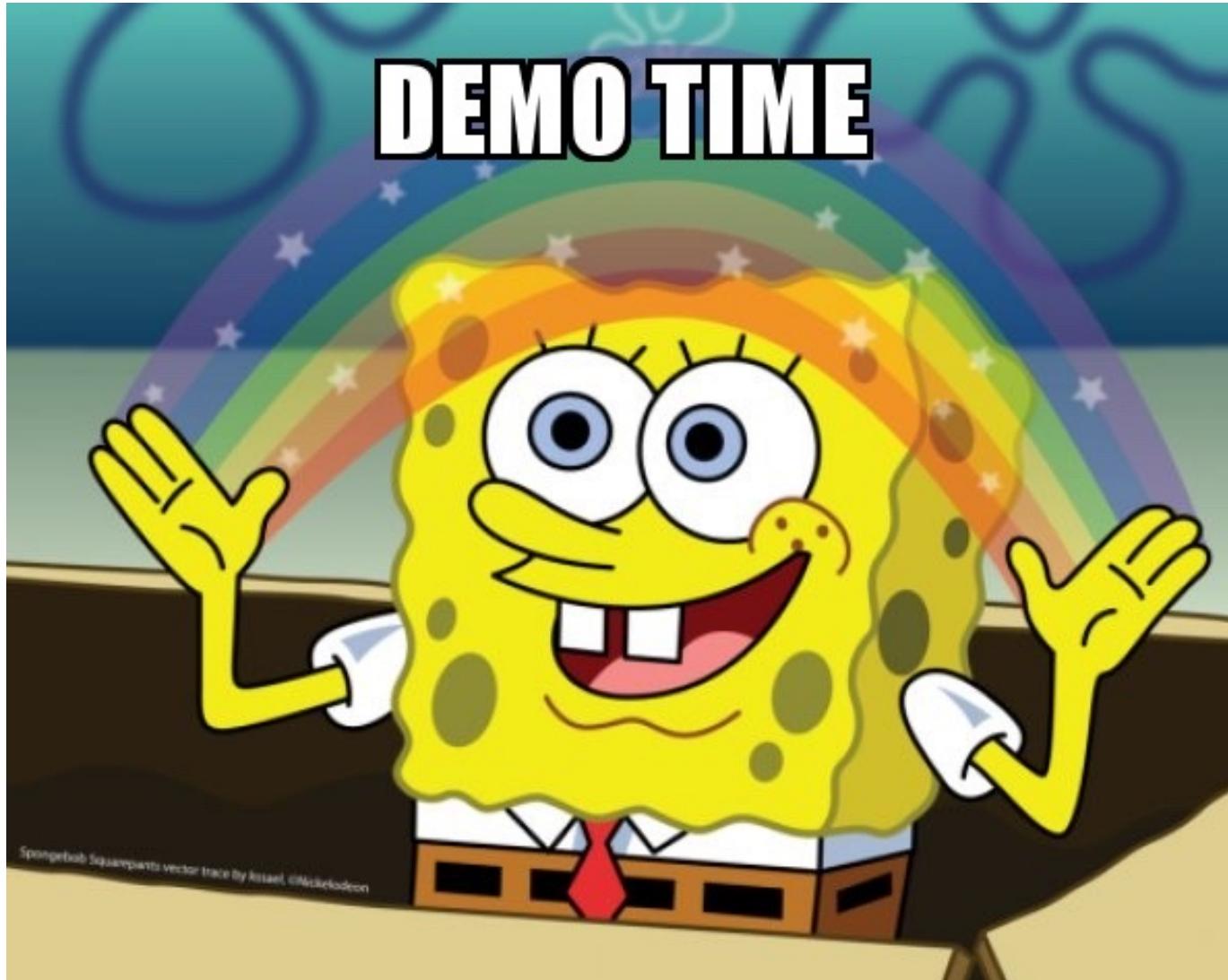
Clusternet 架构

- 最轻量化的架构
- 一站式连接各类集群
- 支持 Pull 和 Push 模式
- 跨集群路由访问
- 支持子集群 RBAC 访问
- 提供一致的集群访问体验，比如 exec, logs
- 原生 Kubernetes API
- 接入成本低，kubectl plugin / client-go

如何通过 Clusternet 访问任一子集群

- Clusternet 支持通过 Bootstrap Token, Service Token, TLS 证书等 RBAC 的方式访问子集群;
 - 子集群的 credential 信息不需要存在父集群中！！！
- 也支持通过 kubectl 命令行的方式对子集群进行 create/get/list/watch/patch/exec 等操作;

如何通过 Clusternet 访问任一子集群



如何通过 Clusternet 访问任一子集群

- 更详细步骤及功能可以参照

<https://github.com/clusternet/clusternet/blob/main/docs/tutorials/visiting-child-clusters-with-rbac.md>

- 使用 curl 进行访问
- 通过 kubectl 进行访问

PART 4



Clusternet - 应 用分发

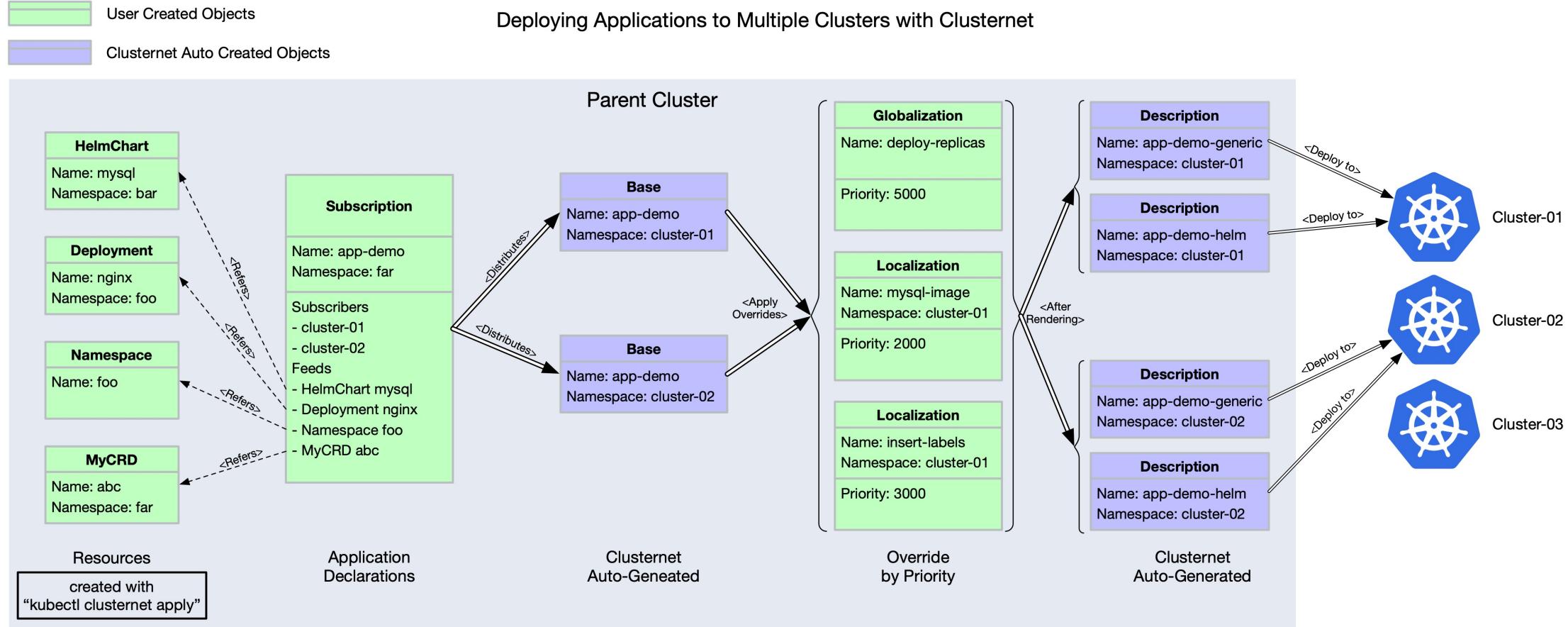
Clusternet 应用分发设计

- 完全兼容 Kubernetes 的内置 API
- 支持 Helm Charts
- 支持 CRD
- 丰富灵活的分发策略配置、差异化策略

应用分发的差异化痛点

1. 在分发的资源上全部打上统一的标签，比如 `apps.my.company/deployed-by: my-platform`；
2. 在分发到子集群的资源上标记集群的信息，比如 `apps.my.company/running-in: cluster-01`；
3. 调整应用在每个集群中的副本数目、镜像名称等
4. 在分发到某集群前，调整应用在该集群中的一些配置，比如注入一个 `Sidecar` 容器等；
5. 灰度升级，变更可控，方便回滚；
6. 重复定义怎么办？冲突吗？
7. ...

Clusternet 应用分发模型



如何创建一个资源

1. kubectl 插件 kubectl-clusternet

```
$ kubectl krew update
$ kubectl krew install clusternet
# check plugin version
$ kubectl clusternet version
```

- Live demo

2. 通过 client-go wrapper

- 一键接入，无需改造
- 兼容 client-go 各个版本
- 示例：

<https://github.com/clusternet/clusternet/blob/main/examples/clientgo/README.md>

示例：声明多集群应用 Subscription

```
apiVersion: apps.clusternet.io/v1alpha1
kind: Subscription
metadata:
  name: app-demo
  namespace: default
spec:
  subscribers: # defines the clusters to be distributed to
  - clusterAffinity:
    matchLabels:
      clusters.clusternet.io/cluster-id: dc91021d-2361-4f6d-a404-7c33b9e01118
  feeds: # defines all the resources to be deployed with
  - apiVersion: apps.clusternet.io/v1alpha1
    kind: HelmChart
    name: mysql
    namespace: default
  - apiVersion: v1
    kind: Namespace
    name: foo
  - apiVersion: apps/v1
    kind: Service
    name: my-nginx-svc
    namespace: foo
  - apiVersion: apps/v1
    kind: Deployment
    name: my-nginx
    namespace: foo
```

示例：差异化策略 Localization/Globalization

```
apiVersion: apps.clusternet.io/v1alpha1
kind: Localization
metadata:
  name: nginx-local-overrides-demo-lower-priority
  namespace: clusternet-5l82l # PLEASE UPDATE THIS TO YOUR ManagedCluster NAMESPACE!!!
spec:
  # Priority is an integer defining the relative importance of this Localization compared to others.
  # Lower numbers are considered lower priority.
  # Override values in lower Localization will be overridden by those in higher Localization.
  # (Optional) Default priority is 500.
  priority: 300
  feed:
    apiVersion: apps/v1
    kind: Deployment
    name: my-nginx
    namespace: foo
    overrides: # defines all the overrides to be processed with
      - name: add-update-labels
        type: MergePatch
        # Value is a YAML/JSON format patch that provides MergePatch to current resource defined by feed.
        # This override adds or updates some labels.
        value: '{"metadata":{"labels":{"deployed-in-cluster":"clusternet-5l82l"}}}'
      - name: scale-replicas
        type: JSONPatch
        # Value is a YAML/JSON format patch that provides JSONPatch to current resource defined by feed.
        # This patch sets replicas to 1.
        # But due to lower priority, this value will be overridden by above "nginx-local-overrides-demo-higher-priority" eventually.
        value: |-
          [
            {
              "path": "/spec/replicas",
              "value": 1,
              "op": "replace"
            }
          ]
```

更多示例

- 注册一个集群
 - <https://github.com/clusternet/clusternet/blob/main/docs/tutorials/installing-clusternet-with-helm.md>
- 部署一个完整的多集群应用
 - <https://github.com/clusternet/clusternet/blob/main/docs/tutorials/deploying-applications-to-multiple-clusters.md>
- 如何使用 client-go 创建多集群应用
 - https://github.com/clusternet/clusternet/blob/main/examples/clientgo/README_E.md



扫码加入 Clusternet 技术交流群



扫码加入腾源会互动交流群



或扫码添加小助手「腾小源」为好友，拉你入群
(PS：申请时请备注 “**GOPS**”)

Thank You