云原生应用升级

Kubernetes集群升级 - 邵欢庆

云原生应用升级 - 柴壮

磐基PaaS平台作为数智云原生技术底座，以容器化、微服务、DevOps为核心的云原生技术，具有快速、灵活、弹性、扩展性强等优势，可以助力行业企业在国家企业数字化转型战略大趋势下，支持大中型企业从“基础设施上云”迈入“应用和系统上云“，大幅降低企业IT开发和运维的成本，提升企业业务的创新效率和产业价值。

01 传统服务器时代

- 小型机或者X86服务器独立运行
- 当系统容量提升，需要扩容CPU、硬盘和内存
- **扩展能力差，资源无法共享**

02 云化时代

- IaaS层能力和上层应用松耦合
- 虚拟化技术重点解决资源利用率与复用度，实现计算、存储、网络等**基础设施资源共享**

03 云原生时代

- **权威机构将云原生技术评为未来十大技术之一，预计2023年75%的新应用由容器承载，2025年将达到95%**
- **应用：** “化整为零”，软件变为模块化的“积木”
- **容器：** 将“积木”和运行环境打包在单独的“集装箱”里，使搬运更容易
- **编排：** 以应用为中心，将“集装箱”组合装配，使调度更轻松，交付更迅速

磐基容器云平台通过云原生技术体系，打造架构先进、技术中立、运营高效、自主可控的统一技术底座，为各业务领域的运营支撑系统提供一站式、可插拔的平台级支撑能力，为深化企业数智化转型提供核心动能。

磐基 PaaS 平台历经 9 年发展历程，积累了大量的部署经验，拥有庞大的部署基数；每年发布两个版本以及多个 fixpack，存在较多的历史版本。

Kubernetes集群升级

邵欢庆

Kubernetes 集群使用广泛，并且部分集群使用时间较长，需要进行升级。

中移信息部署了大量的 Kubernetes集群
且每个集群的规模相对都比较大
集群版本主要分布在 1.14/1.15/1.18/1.19/1.23/1.28

安全修复

- Kubernetes 和其组件（如 Docker、etcd、kubelet 等）会定期发布安全更新，以修复已发现的安全漏洞。这些漏洞可能允许未授权访问、数据泄露或其他安全威胁。

功能增强

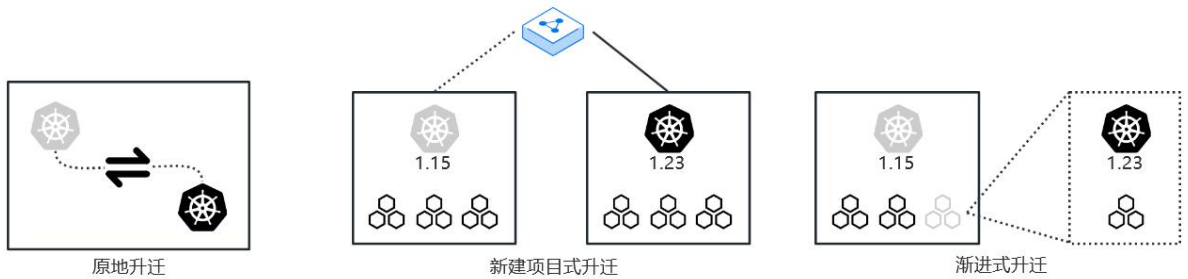
- 新版本的 Kubernetes 通常会引入新的特性和功能，这些功能可能包括改进的调度算法、增强的网络插件、更好的存储选项、新的 API 资源和改进的 CLI 工具等。
- 随着版本的更新，Kubernetes 的性能也会不断优化。这可能包括减少资源消耗、提高处理速度、改进错误处理和恢复能力等。

生态支持

- 社区对旧版本的 Kubernetes 不再提供支持。
- 许多新的有特色的第三方工具和服务（如监控、日志记录、CI/CD 管道等）不支持旧版本的 Kubernetes 集群。

Kubernetes 集群升迁方案：原地升迁、新建升迁、渐进式升迁。3种方案在资源开销、停机割接时长、实施难度、条件限制等方面各有不同。

原地升迁：在不新增资源的情况下，利用原有集群资源升级到新版本 K8S；
新建升迁：新增一套同等配置资源，部署新版本 K8S，并将应用迁移切换到新版本K8S；
渐进升迁：新增一套小规模配置的资源，部署新版本K8S，逐步迁移应用和节点到新版本K8S；



原地升迁

- **优势**
  - 资源开销小，基本不需要申请额外的资源；
- **劣势**
  - 停机割接时间较长；
  - 需要开发升迁回退脚本，实施难度较高；

新建升迁

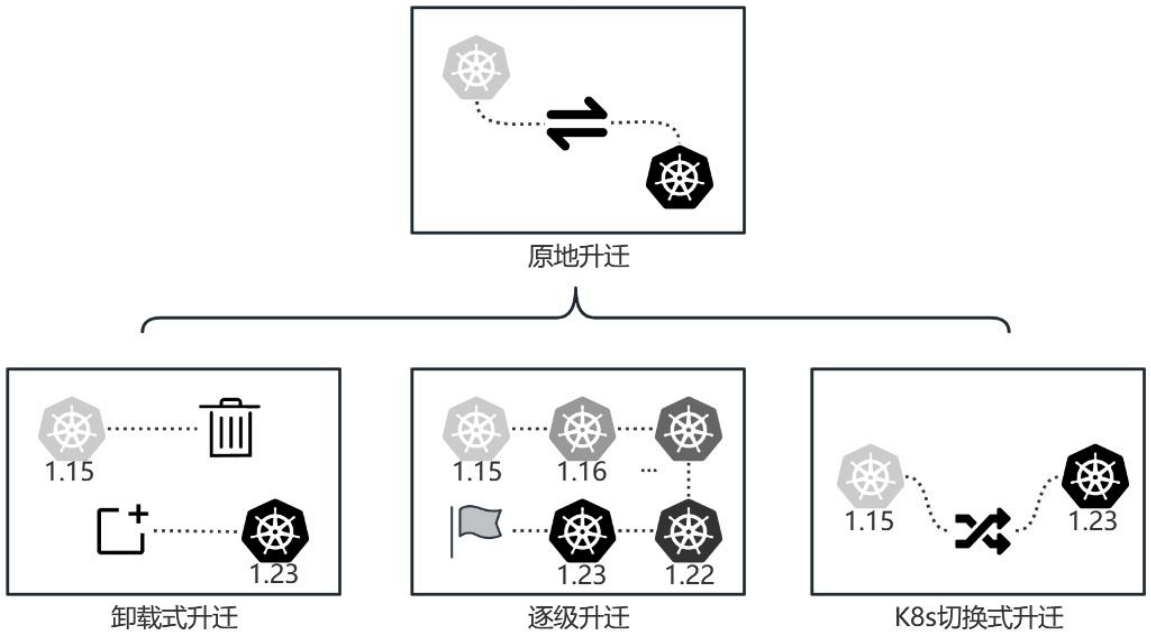
- **优势**
  - 无停机割接时间；
  - 实施难度较低；
- **劣势**
  - 需要较多额外资源；

渐进升迁

- **优势**
  - 无停机割接时间；
  - 实施难度适中；
  - 资源开销适中；
- **劣势**
  - 需要的割接时间较长；

Kubernetes 集群原地升迁：在不增加新机器的情况下，实现 Kubernetes 的版本升级，有多种可选方案：卸载式升迁，逐级式升迁，切换式升迁。

卸载式升迁：先卸载旧版本 K8S，再部署新版本 K8S；
逐级式升迁：依据 K8S 官方升级方式，逐版本升级；
切换式升迁：在环境中同时部署新旧两个 K8S 版本，并切换到新版本；



卸载式升迁

- **优势**
  - 方案简单，实现便捷；
- **劣势**
  - 割接时间长，导致较长时间的业务停机；
  - 回退困难；

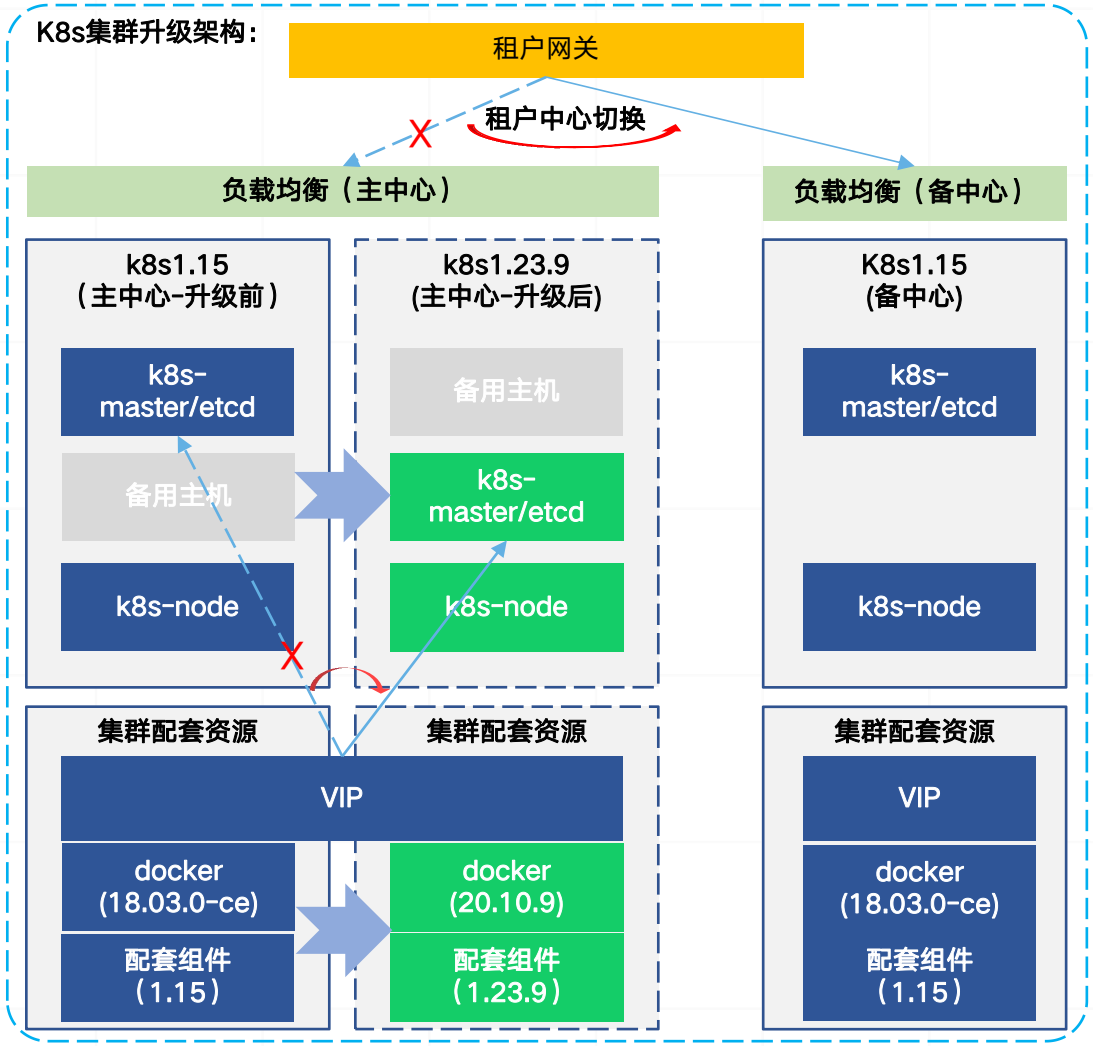
逐级式升迁

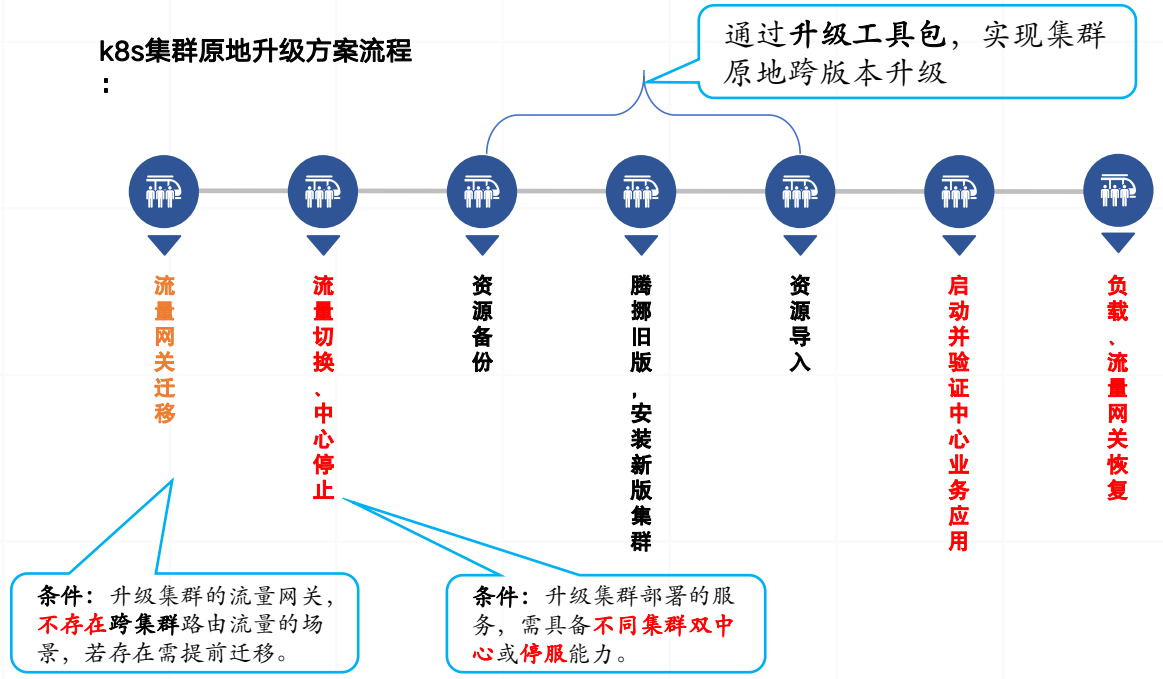
- **优势**
  - Kubernetes 社区官方支持的升级方式
- **劣势**
  - 需要多次割接，每个版本割接一次；
  - 升级周期长；
  - 回退困难；

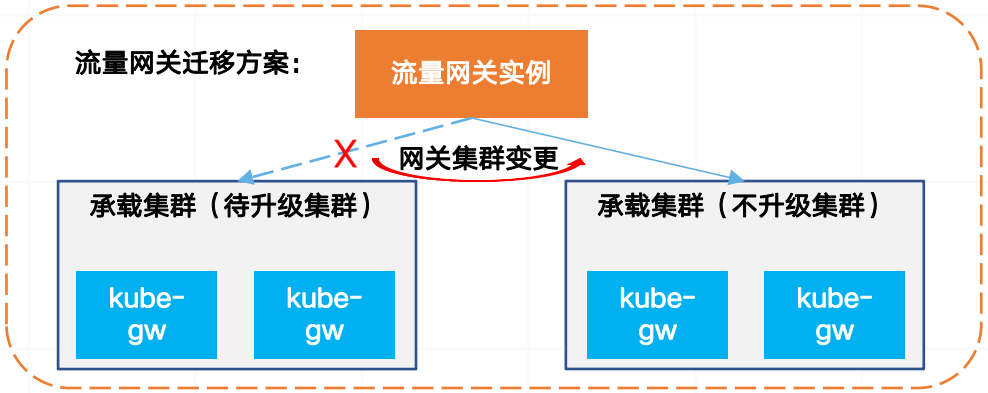
切换式升迁

- **优势**
  - 割接快速；
  - 回退便捷；
- **劣势**
  - 需提前开发切换升级工具，并进行多次测试验证；

Kubernetes 集群切换式升级：在不增加新机器的情况下，使用切换的方式实现 Kubernetes 集群的原地跨版本升级。







Kubernetes 集群切换式升级（有备用中心）： 在不增加新机器的情况下，使用切换的方式实现 Kubernetes 集群的原地跨版本升级。

准备阶段，升级评估；
割接阶段，先停止旧版本 K8S，腾挪、部署新版本 K8S，并将所有工作负载导入到新版本 K8S 集群；
回退阶段，停止新版本 K8S，启动旧版本 K8S。

支持的版本

- **原K8S版本**
  v1.15.2、v1.18.8、v1.19.12
- **目标K8S版本**
  v1.23.6、v1.28.6

优势

准备快速，前期只需做集群的升迁评估工作
割接快速，可在12小时内完成大规模集群的割接；
风险降低，保留了旧版本 K8S 集群的所有文件，可轻松回退，降低风险；
回退便捷，可在0.5小时内完成大规模集群的回退；

劣势

需提前开发切换升级工具，并进行多次测试验证；
对于非标准化安装的 K8S 集群，需要对升级工具做适当调整；

Kubernetes 集群切换式升级（无备用中心）： 在不增加新机器的情况下，使用切换的方式实现 Kubernetes 集群的原地跨版本升级。

准备阶段，将 K8S 各节点上所有相关组件移动到指定路径；
割接阶段，先停止旧版本 K8S，再部署新版本 K8S，并将所有工作负载导入到新版本 K8S 集群；
回退阶段，停止新版本 K8S，启动旧版本 K8S。

支持的版本

- **原K8S版本**
  v1.15.2、v1.18.8、v1.19.12
- **目标K8S版本**
  v1.23.6、v1.28.6

优势

准备充分，升级前进行充分的升级评估，并且在不影响生产环境的情况下，逐节点准备好 K8S 集群的各个机器；

割接快速，可在3小时内完成大规模集群的割接；

风险降低，保留了旧版本 K8S 集群的所有文件，可轻松回退，降低风险；

回退便捷，可在0.5小时内完成大规模集群的回退；

劣势

需提前开发切换升级工具，并进行多次测试验证；

对于非标准化安装的 K8S 集群，需要对升级工具做适当调整；

逐节点腾挪，周期较长

Kubernetes 集群切换式升级 - 实施效果

NO.	集群名称	集群规模	原版本	新版本	总耗时	各环节耗时			
						初始化	备份	清理	升级安装
1	...	45	1.15.2	1.23.6	103分钟	18分钟	23分钟	7分钟	55分钟
2	...	16	1.18.8	1.23.6	17分钟	1分钟	1分钟	1分钟	14分钟
3	...	64	1.15.12	1.28.6	72分钟	3分钟	6分钟	9分钟	54分钟
4	...								

云原生应用升级

柴壮

5G时代运营云原生业务分析一

到了5G时代，随着DCC量的增长，实时计费、实时控制提升了可用性和稳定性的核心需求

中国工信部已经对**实时消费提醒**等进行了**明文要求**；**海外**电信市场在5G时代虽然普遍采用**大流量套餐**，但**政府/行业监管部门**仍然要求运营商进行**流量/费用达限提醒**。

国内

2012年1月21日，**工信部**发布《**关于进一步加强电信服务用户消费提醒工作的通知**》，要求运营商对业务办理、套餐消费、余额不足、国际漫游等消费行为进行**消费提醒**，且消费提醒服务应**免费**。

- 其中对于套餐消费，运营商要对超出套餐后的收费标准予以明确，用户实际使用量接近套餐限量前和达到套餐限量时，电信业务经营者均应通过短信、语音、页面窗口等方式，提醒用户，并告知用户超出套餐外继续使用该业务的收费标准、收费查询方式。

国外

美国：免费发送超量预警短信 （FCC+CTIA）

加拿大：运营商每月收取的额外数据收费上限为50加元，国际漫游数据收费上限定为100加元等（CRTC）

英国：允许用户设定漫游费上限（Ofcom）

澳大利亚：多次预警（政府立法）

	流量/月	费用/月	费用/年
S	1G	$25	$300
M	5G	$35	$420
L	8G	$50	$600
XL	15G	$95	$1140

《电信消费者保护法案》

- 数据流量分别达到订购值的50%、85%及100%时将收到邮件/短信提醒
- 用户套餐使用率已达100%的提醒中必须包括费用超出部分的消费明细
- 如果消费者订购了某项避免出现“天价账单”的业务，将不会收到消费提醒

政策管控

客户体验

实时计费

收入保障

月因为对高使用费的恐惧及误读，网络疯狂谣传“**一晚忘关连接，房子就得归移动**”

5G速率高，离线计费模式下（以30分钟的分割单位为例）在速率为1Gbps的情况下， 两次计费间隔中用户可以消费约5G流量相当于套餐外约**3000**元(按3元/G计算)

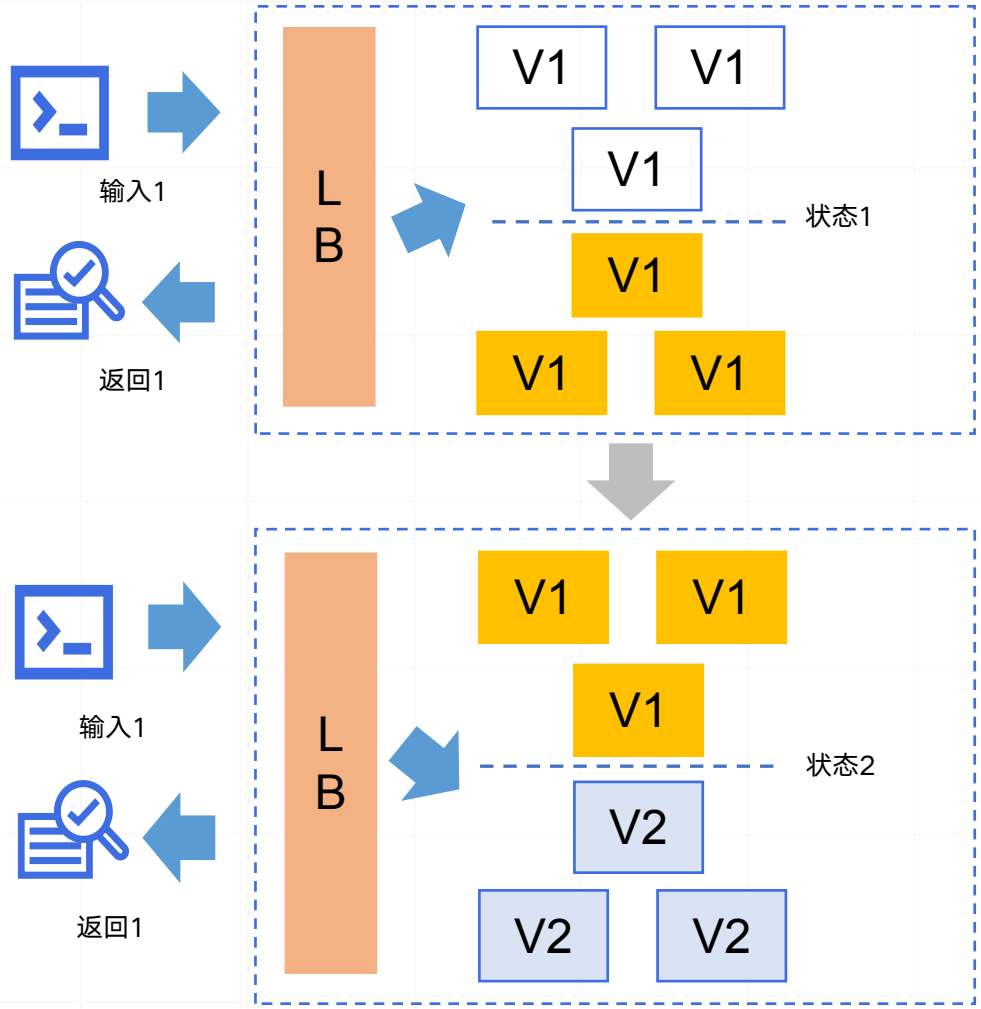
5G时代下，**用户更加需要实时计费**、实时提醒以实现**放心使用**

在高带宽、高速率的背景下，离线计费的计费及控制模式会带来**高欠费风险**。

在高速带宽使用场景下，离线计费的可控阈值远超“双封顶”的限额。对超高流量的异常使用行为缺乏合理的管控手段，将导致的客户投诉，以至**退费**。

所以在5G时代下， **中国移动更需要实时计费、实时管控**以控制风险降低收入流失。

实现稳定的完成升级的目标， 核心任务选择蓝绿发布



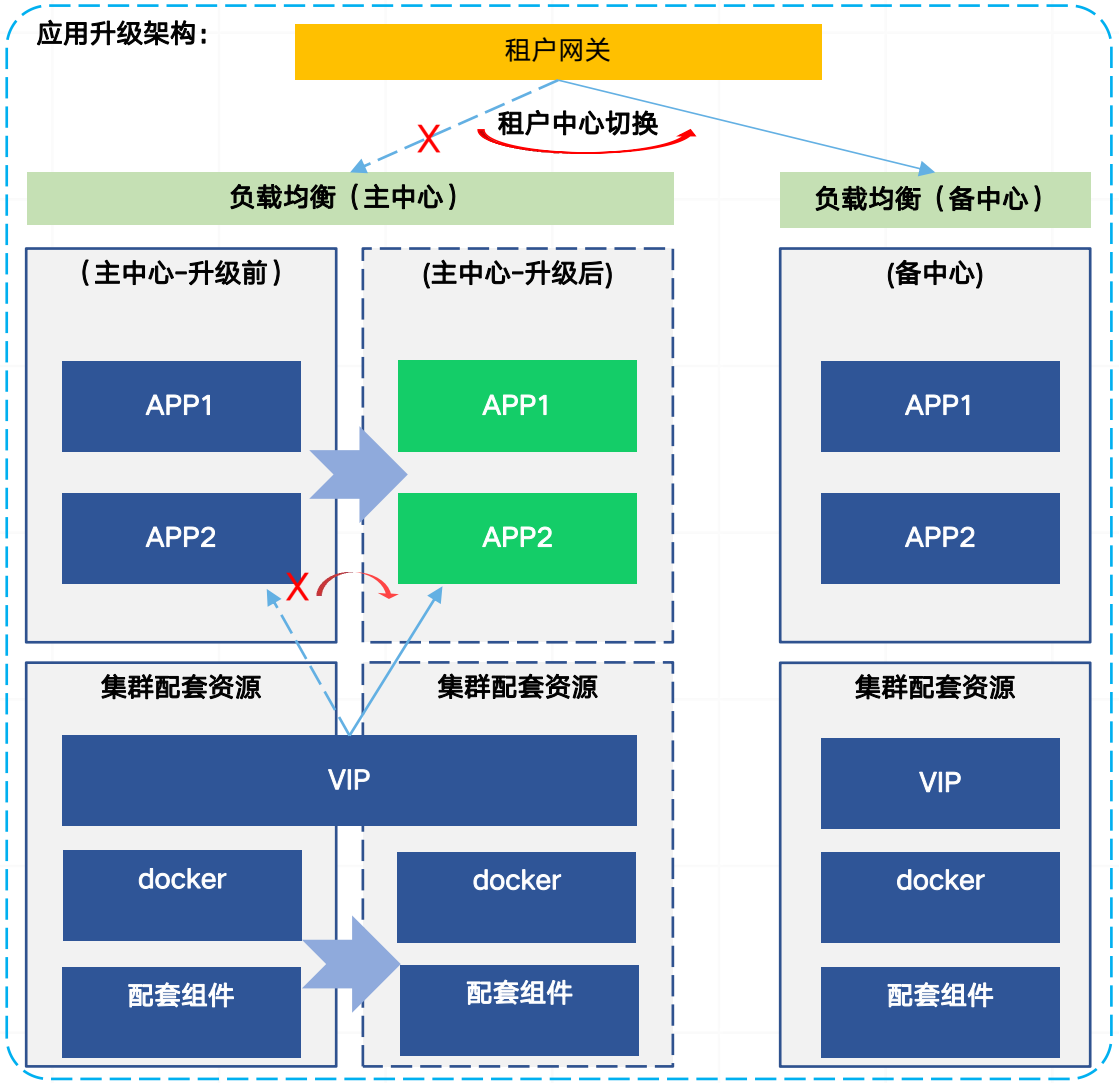
技术特征

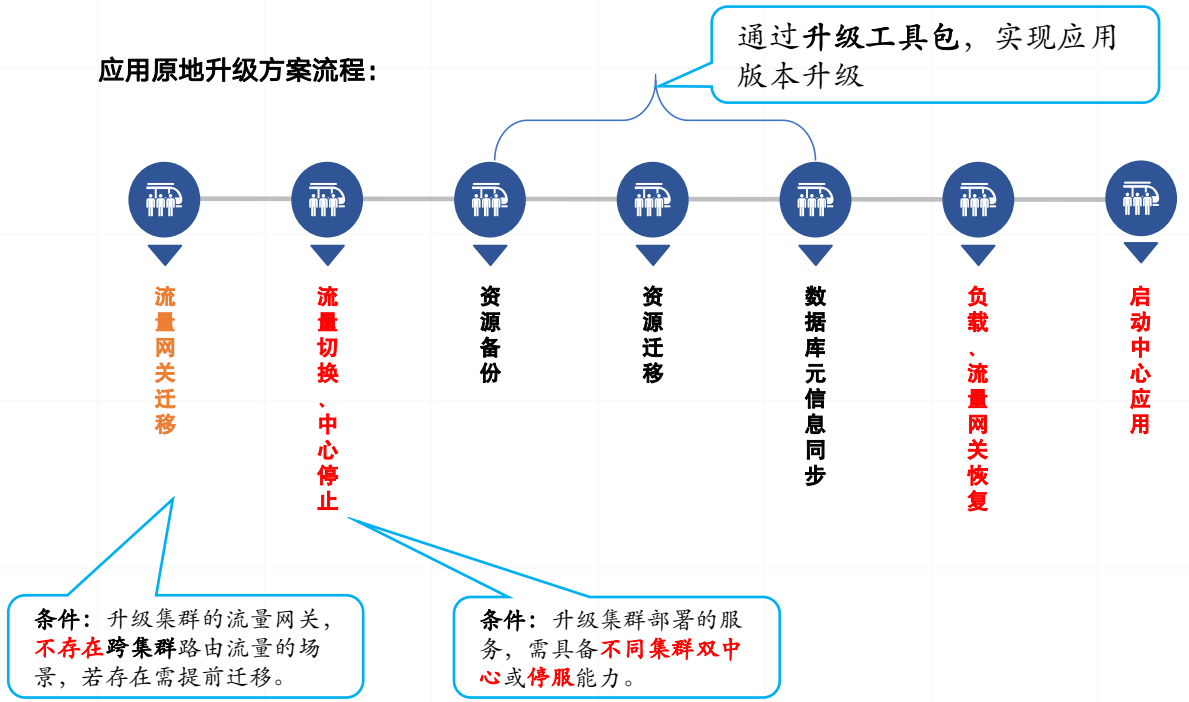
- **蓝绿发布**：两个完全相同的、互相独立的生产环境，一个叫做“蓝环境”，一个叫做“绿环境”。其中，绿环境是用户正在使用的生产环境。当要部署一个新版本的时候，先把这个新版本部署到蓝环境中，然后在蓝环境中运行冒烟测试，以检查新版本是否正常工作。如果测试通过，发布系统更新路由配置，将用户流量从绿环境导向蓝环境，蓝环境就变成了生产环境。这种切换通常在一秒钟之内就能搞定。如果出了问题，把路由切回到绿环境上，再在蓝环境中调试，找到问题的原因。因此，蓝绿部署可以做到仅仅一次切换，立刻就向所有用户推出新版本，新功能对所有用户立刻生效可见。

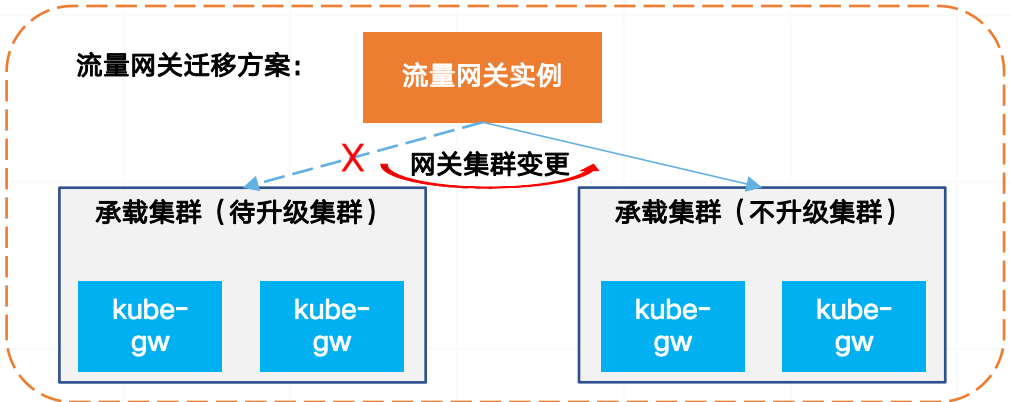
能力分析

- **优势：** 升级切换和回退速度非常快
  零停机时间
- **不足：** 一次性的全量切换, 如果发布出现问题, 会对用户产生比较大的影响
  需要两倍的机器资源
  需要中间件和应用自身支持热备集群的流量切换
- **适用场景：** 机器资源比较富余或者按需分配

实现稳定的完成升级的目标

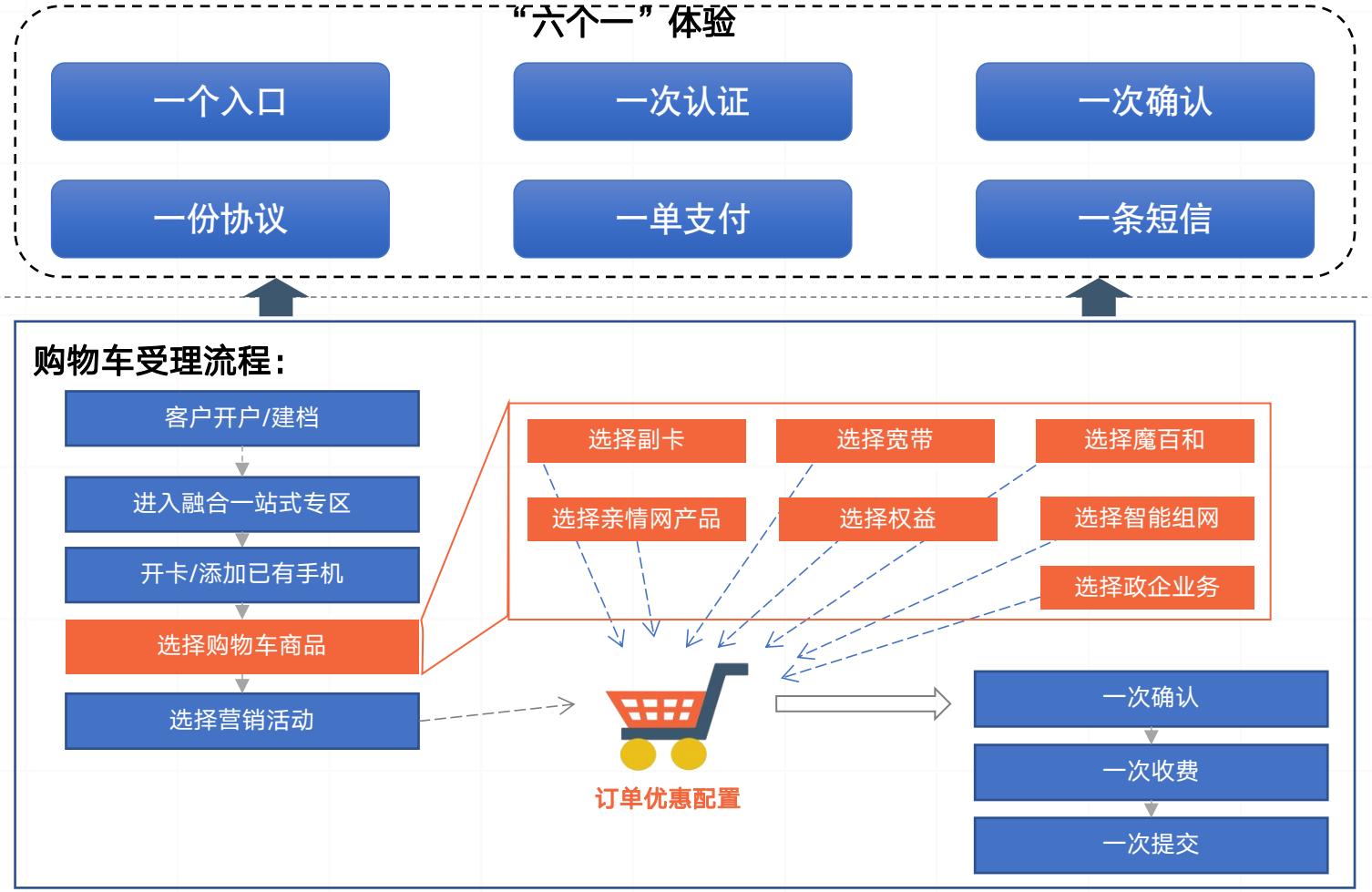






5G时代运营云原生业务分析二

为缩短原地升级应用耗时，需对集群升级过程进行工具化改造，实现割接时间范围内完成升级的目标



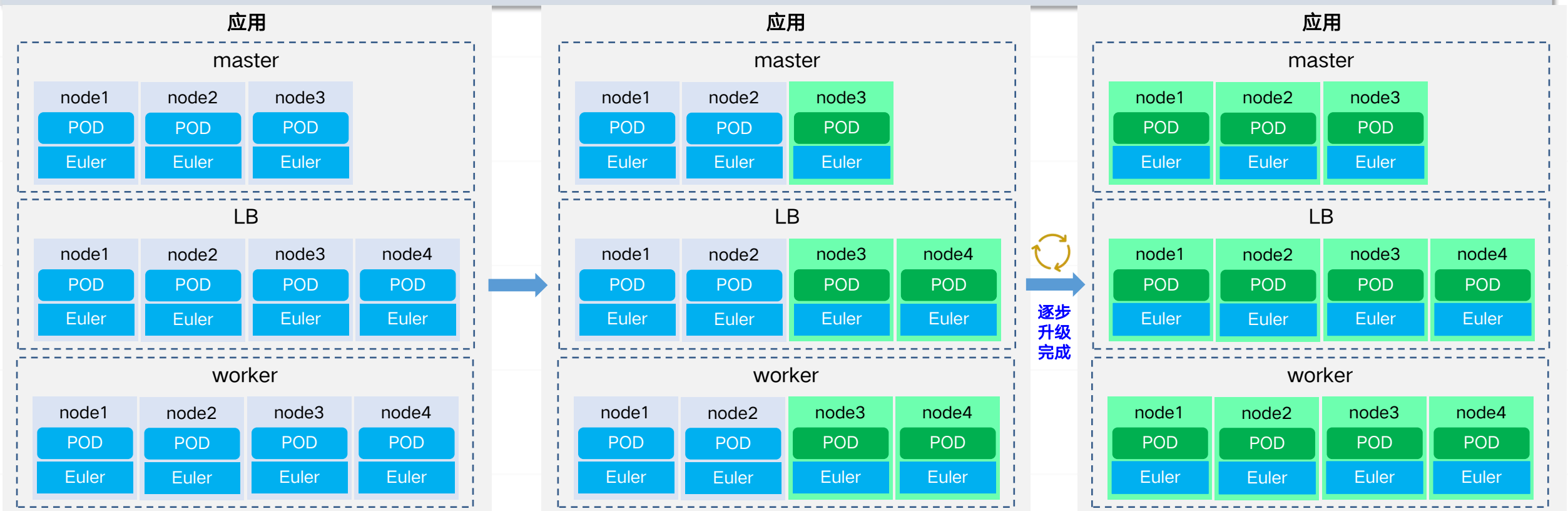
升级系能力支撑

建设内容：

- 对 K8s 自身的应用部署能力（比如工作负载）进行扩展；
- 提供原地升级能力，给应用带来了更快的发布速度，以及避免对其他 Scheduler、 CNI、CSI 等组件的负面影响；
- 提供容器按顺序加载能力，保证应用依赖稳定性；
- 通过旁路管理应用内的 sidecar 容器，Pod 创建时特定 sidecar 注入和管理；
- 提供镜像预热拉取能力

5G时代运营云原生业务二升级方案

实现割接时间范围内完成升级的目标，需对集群升级过程进行分批次升级



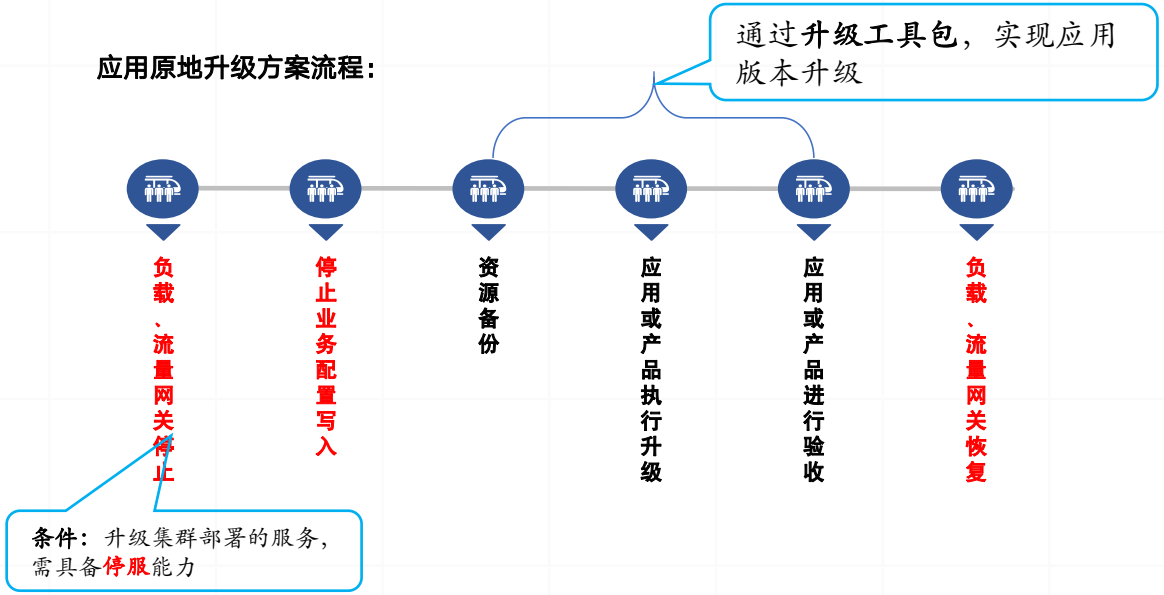
- 根据业务系统的情况，制定方案、场景进行原地升级验证
- 根据场景准备原地升级验证环境
- 制定原地升级策略：为了减少升级对业务的影响，建议采用主机节点逐步升级的方式，进行原地升级验证。

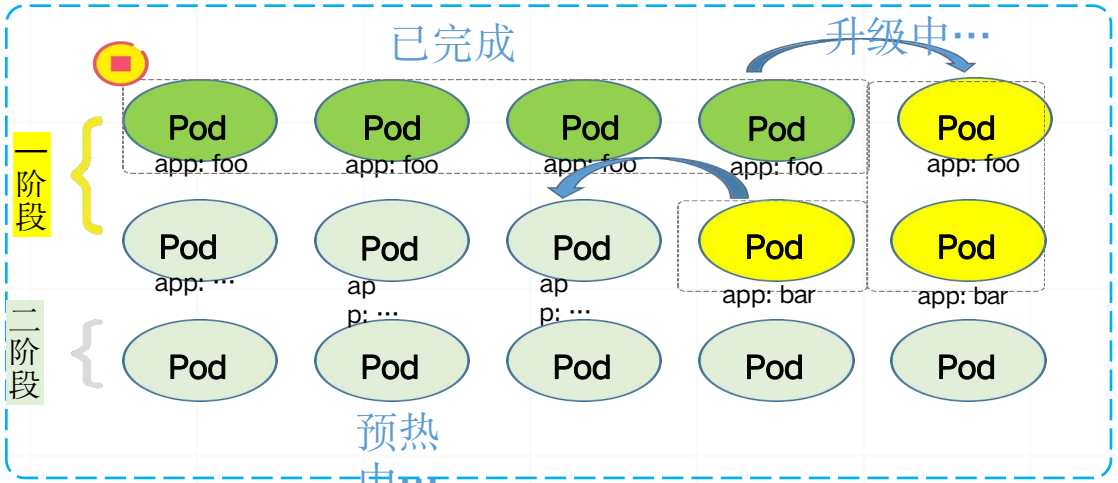
- 针对应用的master、lb、worker选取计划升级的节点。
- 将节点置为不可调度，并对应用POD进行驱逐，保证要升级的节点没有应用在运行。
- 对节点进行操作系统原地升级。
- 升级完成后，进行环境检查，恢复节点调度。
- 针对升级后的节点，进行场景、业务功能验证。

- 重复上一步骤，逐步的完成集群所有节点的升级操作、场景验证操作。
- 全部节点升级完成后，在对业务进行一次功能验证，保证原地升级后的业务不受影响。
- 对于业务验证中遇到的问题，需要有解决方案。

为缩短原地升级应用耗时，需对集群升级过程进行工具化改造，实现割接时间范围内完成升级的目标

应用原地升级方案流程：





建设内容

➢ 研发方案

- 对 K8s 自身的应用部署能力（比如工作负载）进行扩展；
- 控制升级过程，一次只升级指定 Pod 数量；
- 控制升级过程，允许升级发布暂停；
- 控制升级过程，允许快速回滚；
- 按指定顺序或优先级进行 Pod 升级；

➢ 预期效果

- 能够对升级过程进行管控，提供对升级定制化能力。
- 提供对大规模跨集群应用升级时，时间跨度大，分批分阶段灰度升级的弹性能力支撑。

感谢观看

云原生社区
Cloud Native Community