China · Shenzhen

小米生态云的应用引擎实践

李波

资深研发工程师

北京　伦敦　纽约　旧金山　圣保罗　上海　东京

QCon 全球软件开发大会

[上海站]

信息安全　机器学习　人工智能　黑产　互联网金融（FinTech）　团队管理　基础设施　云计算　软件性能　硅谷　微服务　互联网架构

主办方 Geekbang 极客邦科技　InfoQ

2017年10月17-19日
上海·宝华万豪酒店

扫描二维码
开启软件开发新思路

SPEAKER

INTRODUCE

李 波 资深研发工程师

- 小米生态云团队资深研发工程师，负责小米生态云及小米应用引擎的设计开发和线上业务运维。
- 曾就职于IBM中国开发中心，参与了BPM，Bluemix等产品的开发工作。

TABLE OF
CONTENTS 大纲

小米生态云

- 为小米生态企业提供一站式云服务及解决方案

整体解决方案/技术咨询/技术支持

用户管理控制台

认证与授权（集成小米账号）

用户权限管理（用户/组/角色）

计量计费

Event Log
Audit Log

应用引擎

v1: CF + Docker

v2: Kubernetes

自动扩容

日志采集

日志分析

计划任务

域名及证书

监控

短信邮件报警

安全扫描

SDS
FDS
EMQ
Talos

数据分析

RPC

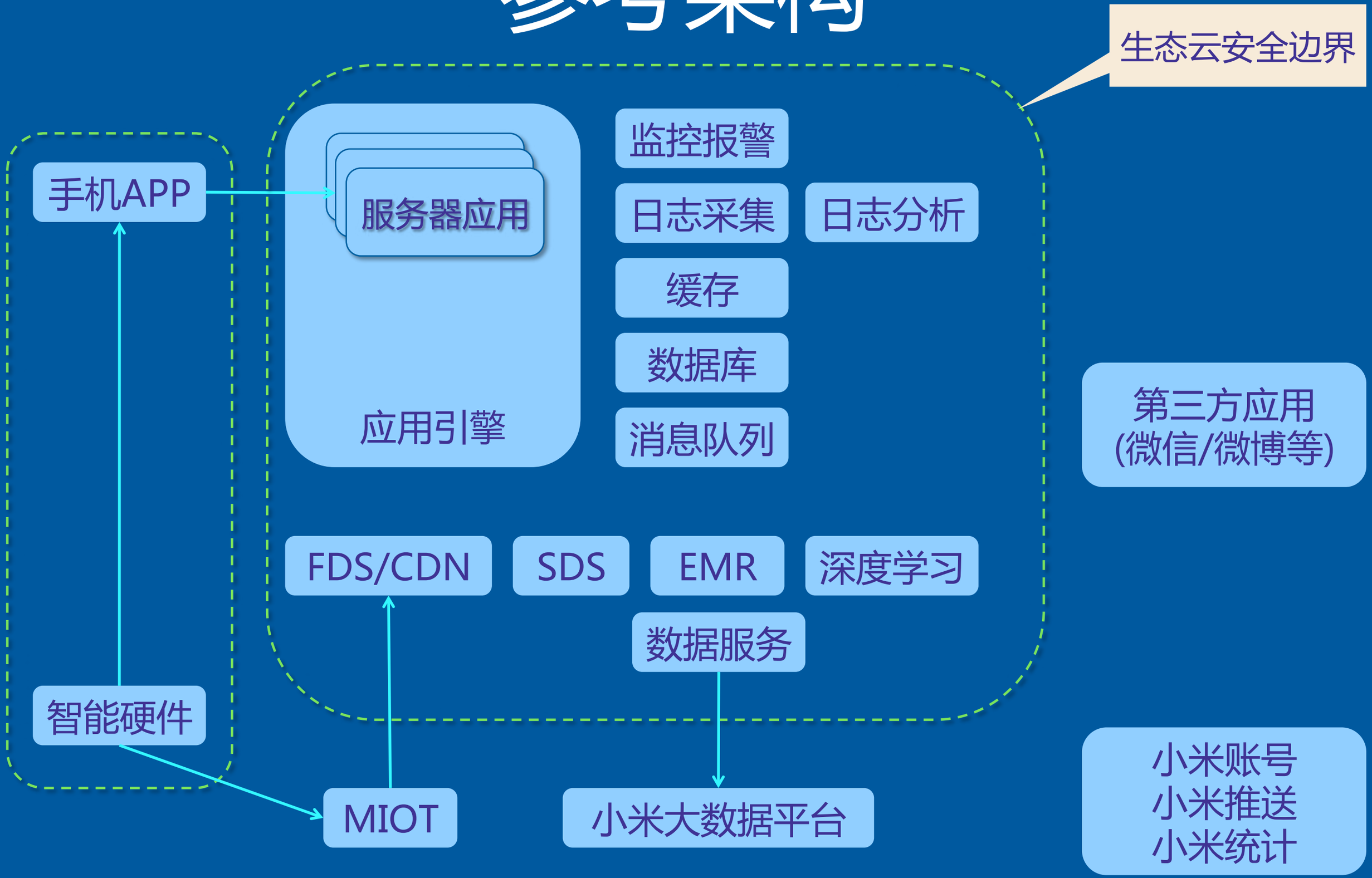
深度学习

无服务器计算

用户画像
推送推广
特征分析
数据工厂
数据通道

虚机
缓存
数据库
网络带宽
CDN

参考架构


生态云安全边界
手机APP
服务器应用
应用引擎
监控报警
日志采集
日志分析
缓存
数据库
消息队列
第三方应用
(微信/微博等)
FDS/CDN
SDS
EMR
深度学习
数据服务
智能硬件
MIOT
小米大数据平台
小米账号
小米推送
小米统计

生态云区域分布

法兰克福

北京

北京&上海

俄勒冈

东京

新加坡

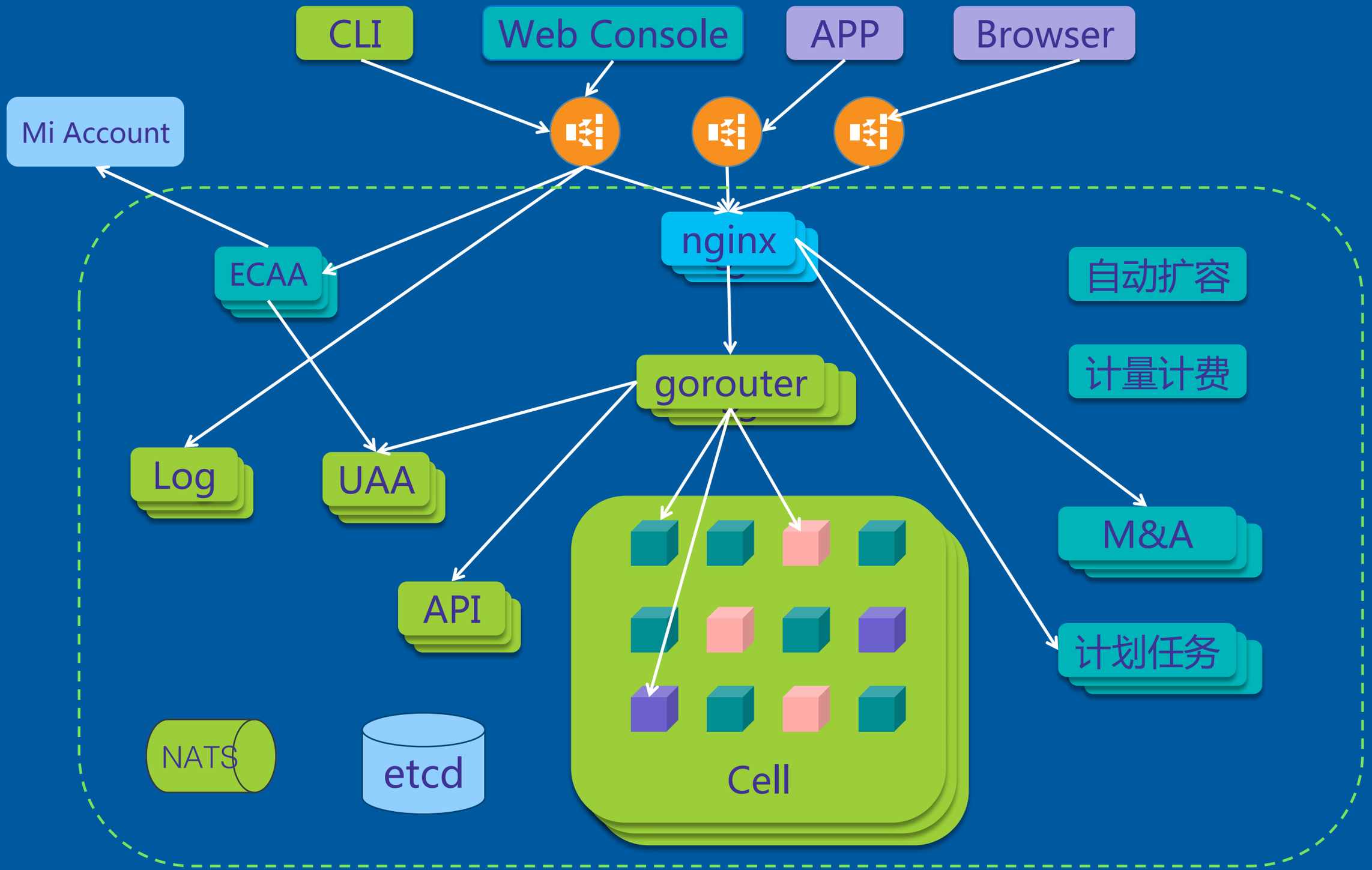
TABLE OF
CONTENTS 大纲

- 小米生态云简介
- 小米生态云应用引擎演进
- 未来展望

应用引擎v1

- 基于Cloud Foundry
- 集成小米账号，支持公司及部门隔离，用户和角色管理
- 支持主流开发语言以及静态页面和二进制文件（ Heroku Buildpack ）
- 支持Docker应用
- 域名及证书

v1 架构


CLI
Web Console
APP
Browser
Mi Account
ECAA
nginx
自动扩容
计量计费
gorouter
Log
UAA
API
M&A
计划任务
NATS
etcd
Cell

优点和缺点

- 优点
  - 开箱即用的PaaS平台
  - 完整的权限和授权体系
  - 成熟稳定，非常适用于无状态Web应用
- 缺点
  - 自有体系，组件繁多，部署运维复杂
  - 无法限制应用的CPU绝对用量
  - 不支持cluster应用、UDP应用
  - Docker支持不完整，非原生体验
  - 社区参与度和活跃度下降

生态链用户需求

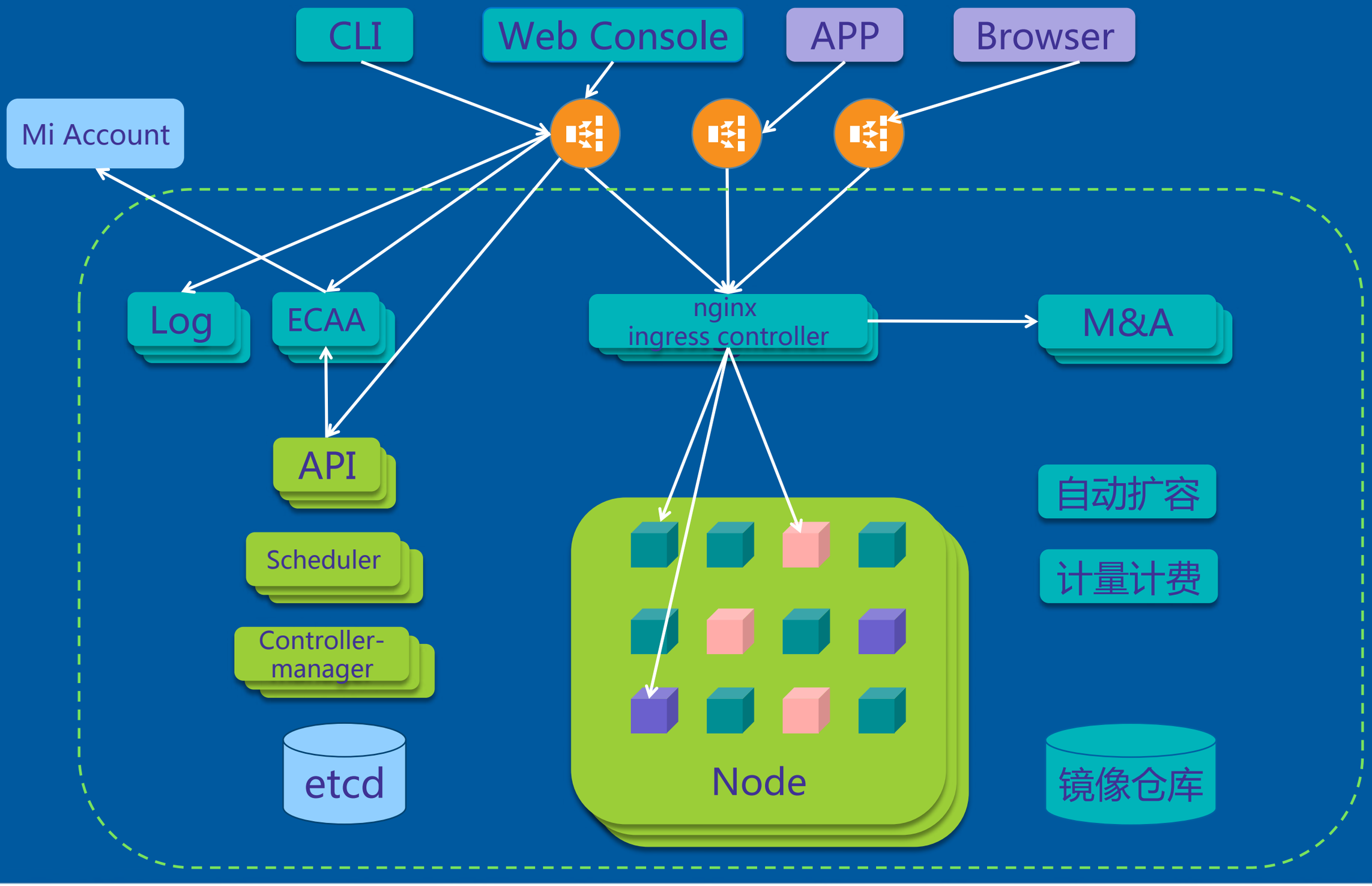
- Buildpack机制和基础文件系统不灵活，定制难度大
- 开发测试逐步迁移到Docker平台，与生产环境不一致
- 部分应用需要支持TCP/UDP
- 部分应用需要作为cluster部署
- 现有计划任务功能单一，不灵活
- 部分应用需要Windows平台的.Net支持

应用引擎v2

- 基于Kubernetes
- 原生Docker体验
- 支持TCP/UDP应用
- 原生计划任务支持
- 配置和敏感信息管理
- CPU的绝对用量限制
- 支持cluster应用
- 支持Windows平台

- 多租户与安全隔离
  - 权限体系： 组织，开发空间，角色，用户
  - 网络隔离
  - 安全策略
  - 流量隔离
- 应用抽象和封装
- 命令行工具

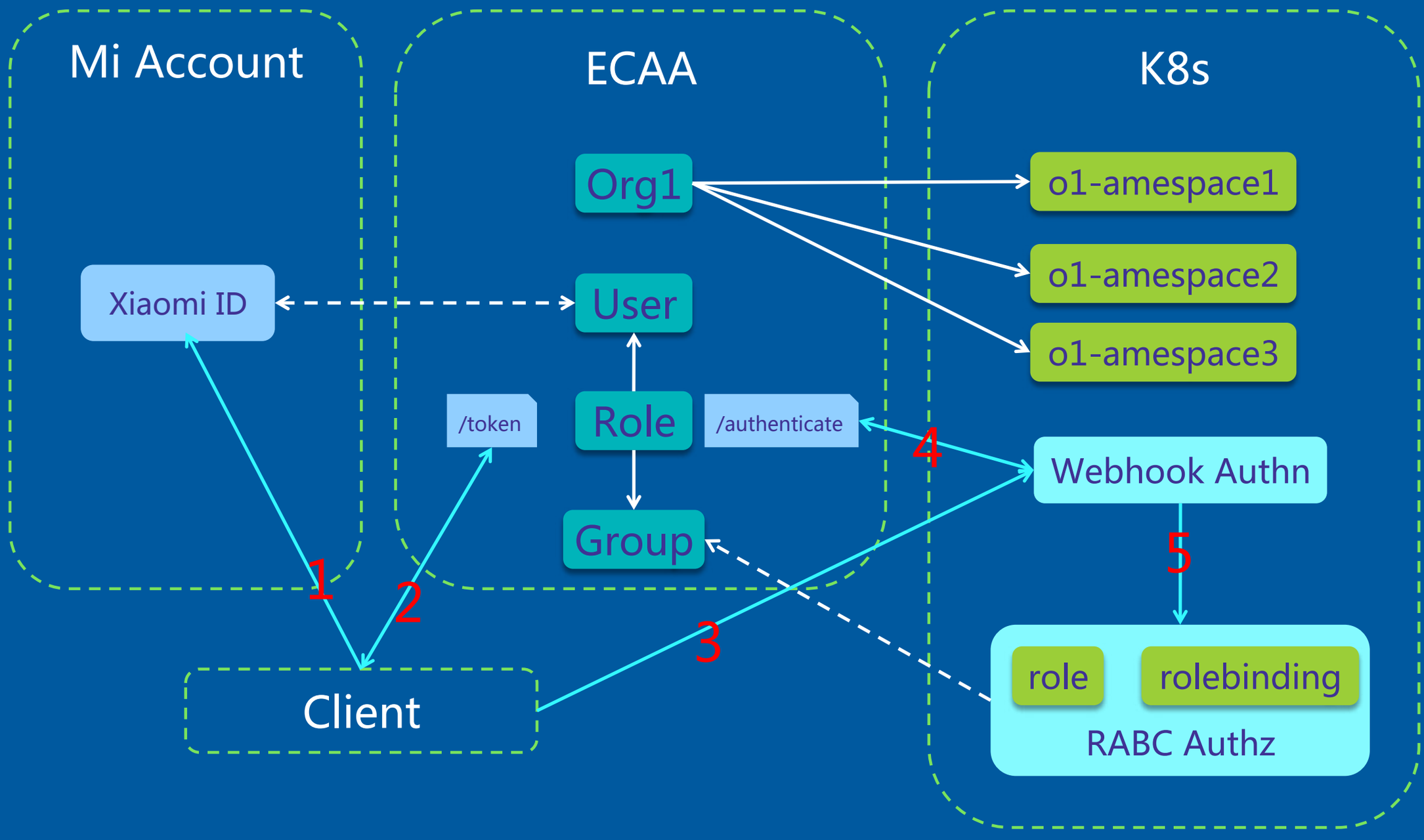
v2 架构


CLI
Web Console
APP
Browser
Mi Account
Log
ECAA
nginx
ingress controller
M&A
API
Scheduler
Controller-
manager
etcd
Node
自动扩容
计量计费
镜像仓库

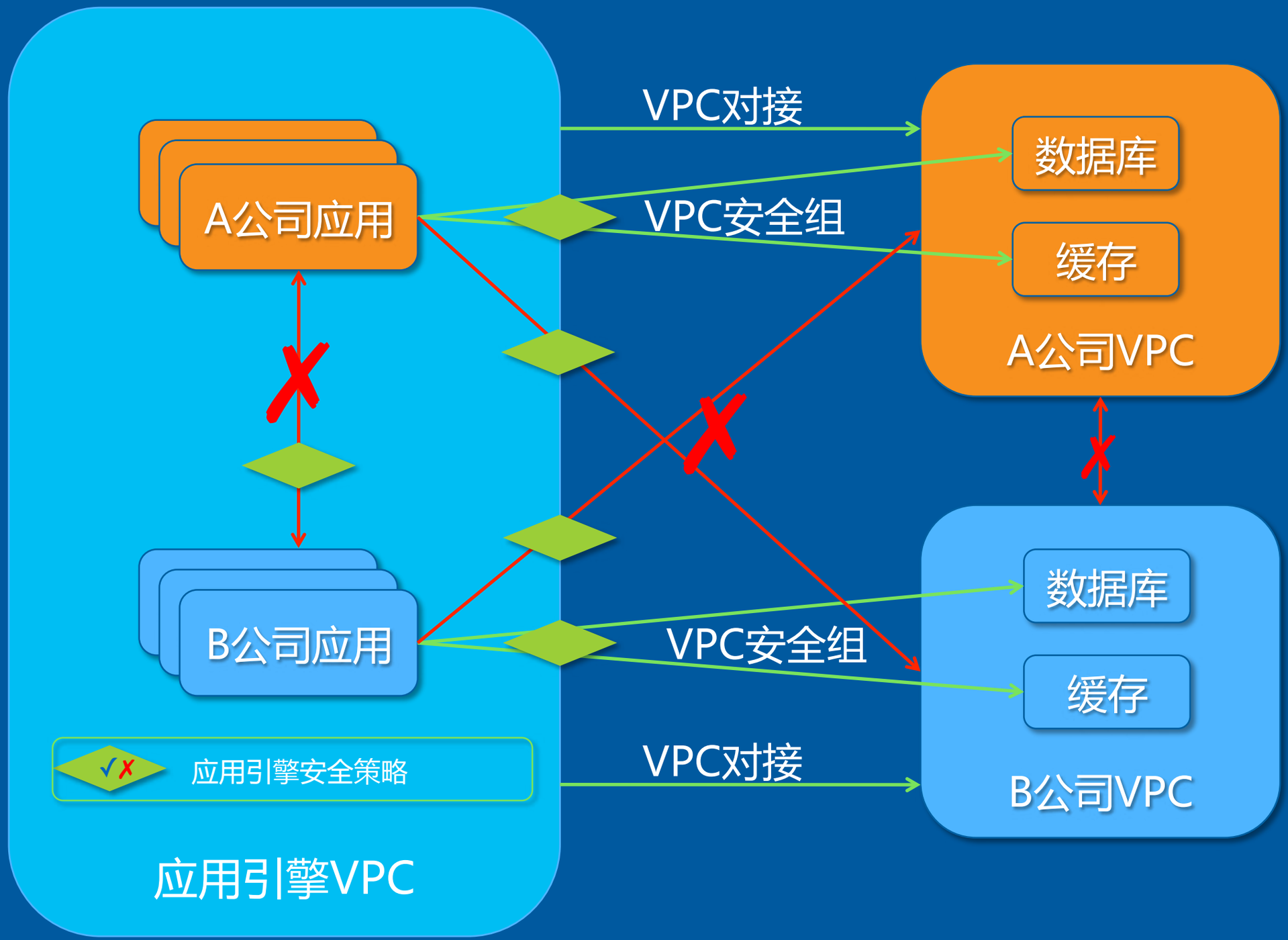
多租户环境

- 安全
- 安全
- 安全
- 流量隔离
- 资源公平分配

多租户与安全隔离： 权限体系



网络隔离


VPC对接
数据库
A公司应用
VPC安全组
缓存
A公司VPC
B公司应用
数据库
VPC安全组
缓存
应用引擎安全策略
VPC对接
B公司VPC
应用引擎VPC

网络安全

- VPC及子网：严格的安全组
- 对外服务
  - 只开放必要端口
  - 只允许生态链公司IP访问

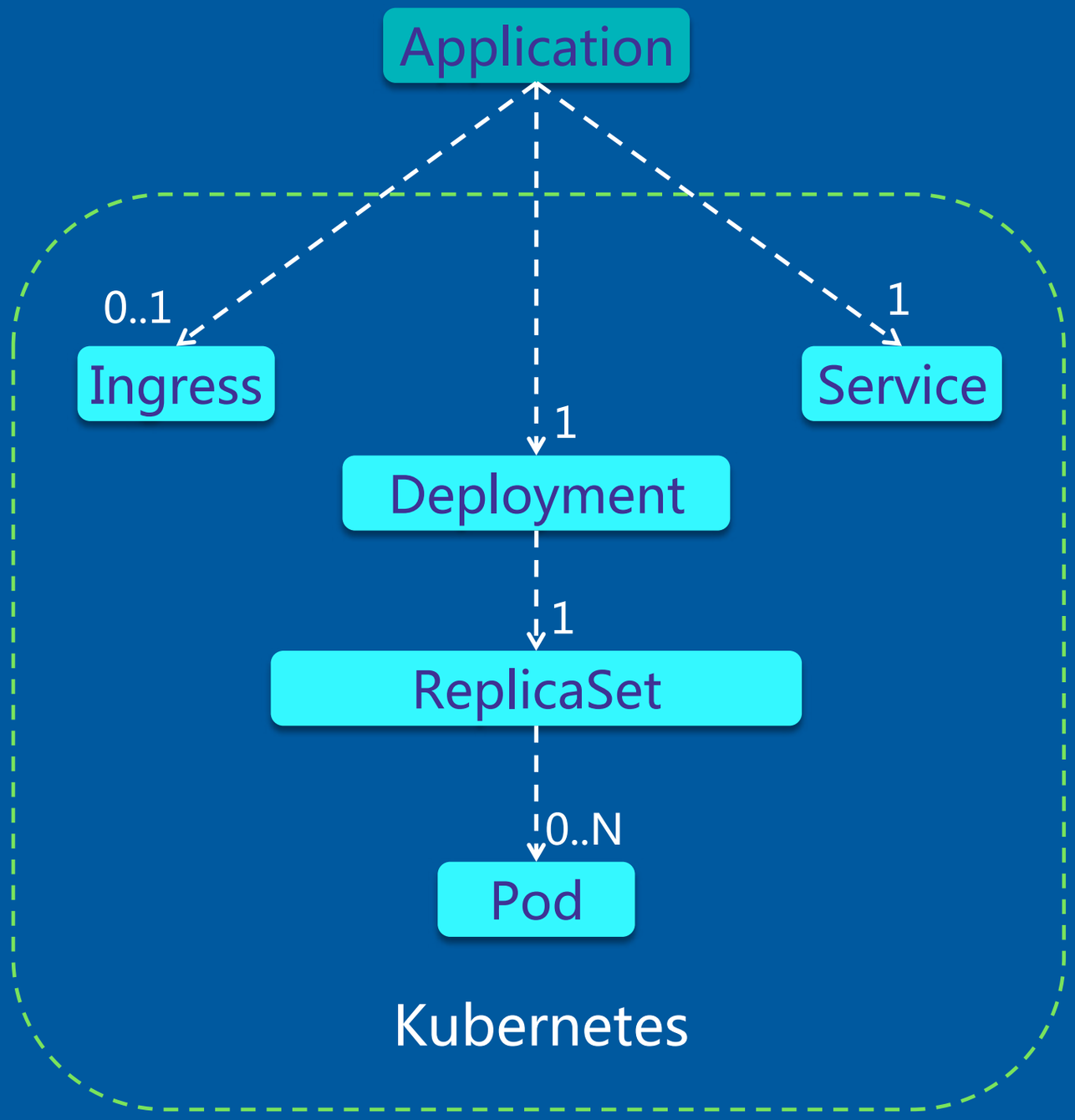
安全策略

- 容器网络：Calico
- 双向控制
  - ingress： Kubernetes网络策略
    - DefaultDeny
    - 允许同namespace应用访问
  - egress： Calico策略
    - 允许访问kube-dns
    - 允许访问用户VPC的内网地址
    - 拒绝访问私有地址

流量隔离

- 配置不同的SLB/ELB
  - 独立IP
  - 独立带宽
  - 独立的Nginx（如果需要）

应用抽象和封装


Application
0..1
Ingress
1
Service
1
Deployment
1
ReplicaSet
0..N
Pod
Kubernetes

命令行工具

- 不使用kubectl
  - 暴露过多细节
  - 认证不便
- 自研工具
  - ak/sk认证
  - 方便自动化的有限功能
    - 应用部署，更新，删除
    - 应用水平扩容

Lesson Learned

- 资源限制
  - ResourceQuota
  - LimitRange
- CronJob
  - successfulJobsHistoryLimit, failedJobsHistoryLimit
  - concurrencyPolicy: Forbid/Replace
  - activeDeadlineSeconds
- Events
  - 导出到外部存储
- Docker
  - log rotation: --log-driver json-file --log-opt max-size=100m --log-opt max-file=10
  - version >= docker 1.13

TABLE OF
CONTENTS 大纲

小米生态云的未来展望

- 应用引擎v2
  - 支持部署Cluster应用
  - TCP/UDP外部服务
  - 容器直连
  - 集群自动扩容
  - Windows平台
- 大数据服务
- 人工智能服务

THANKS!

让创新技术推动社会进步

HELP TO BUILD A BETTER SOCIETY WITH
INNOVATIVE TECHNOLOGIES

Geekbang.
极客邦科技

InfoQ

专注中高端技术人员的技术媒体

EGO EXTRA GEEKS' ORGANIZATION NETWORKS

高端技术人员学习型社交平台

StuQ 斯达克学院

实践驱动的 IT 教育平台

地址：北京市朝阳区洛娃大厦C座8层1801室　　网址：www.geekbang.org