

容器镜像服务产品介绍

-云原生资产托管及分发管理

目录

云原生定义

容器镜像服务产品

典型场景

演示

云原生定义

- CNCF 云原生定义 V1.0
云原生技术有利于各组织在公有云、私有云和混合云等新型动态环境中，构建和运行可弹性扩展的应用。
- 云原生应用 Cloud-Native Applications
应用原生被设计在云上运行，充分发挥云平台的优势和能力。



云原生代表技术

容器

Container



微服务

Micro Services



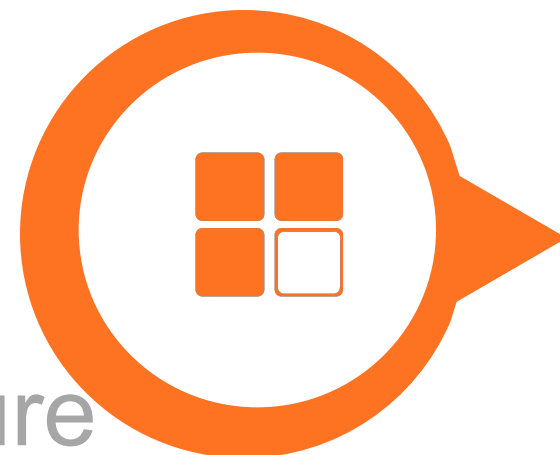
服务网格

Service Meshes



不可变基础设施

Immutable infrastructure



云原生

Cloud-Native



声明式 API

Declarative APIs





弹性

降低 50% 计算成本



易用

10 X 研发效率提升



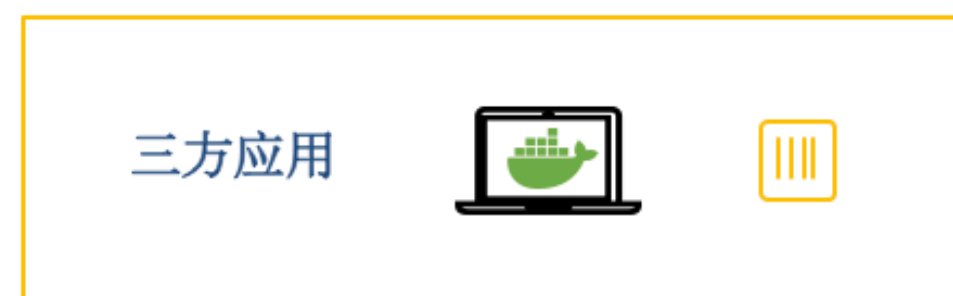
可移植

开放、标准、一致性认证

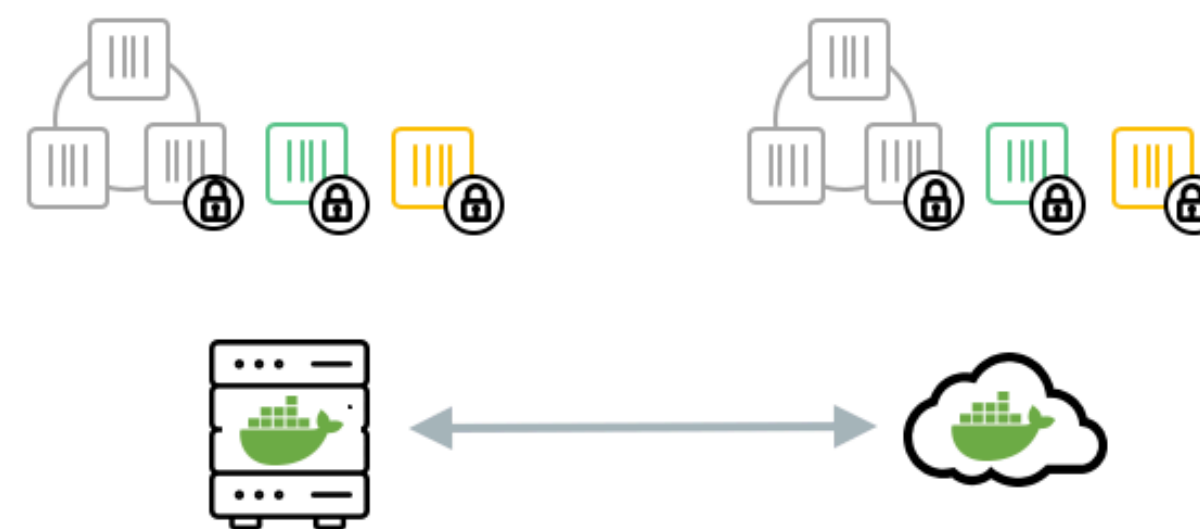
云原生代表技术

- 容器定义了**标准化**的交付方式：**容器镜像**
- 容器推动软件供应链的变革

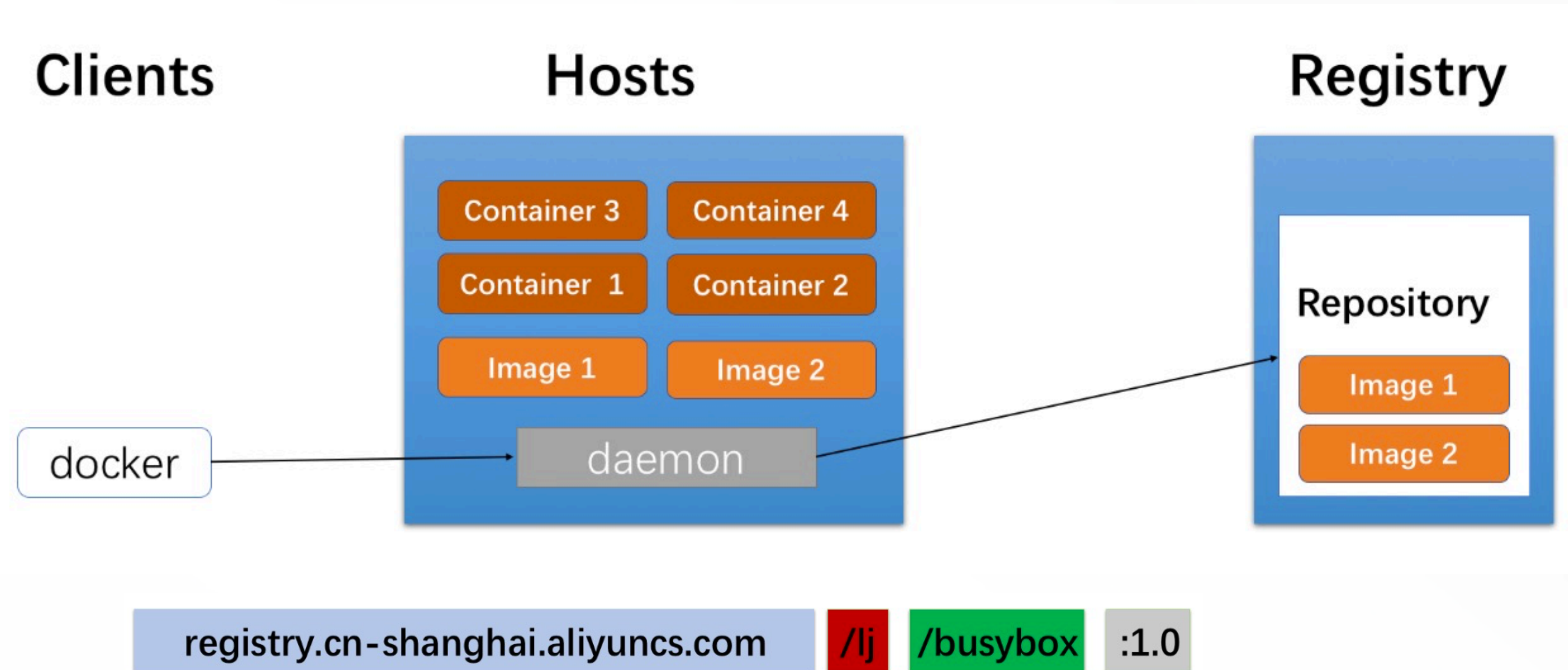
开发团队



IT 运维团队



容器镜像简介



```
docker login registry.cn-shanghai.aliyuncs.com
```

```
docker tag busybox registry.cn-shanghai.aliyuncs.com/lj/busybox:1.0
```

```
docker push registry.cn-shanghai.aliyuncs.com/lj/busybox:1.0
```

目录

云原生定义

容器镜像服务产品

典型场景

演示

容器镜像服务

云原生时代的重要基础设施，托管和分发客户容器应用资产

- 公共云

- 容器镜像服务-默认实例

- 6 w+ 容器开发者，月均镜像下载量 1亿+次

- 容器镜像服务-企业版

- GC5及以上的企业级客户

- 上海、北京、深圳、伦敦已开服

- 集团内部

- 阿里经济体（阿里经济体应用发布、扩容关键路径）

- 支撑双十一，实现10分钟万台服务器的容器因公部署

- 专有云



容器镜像服务

云原生时代的重要基础设施，托管和分发客户容器应用资产

	企业版	默认实例版
客户画像	GC5及以上企业级客户 安全需求高、大规模节点、全球多地域业务部署	容器开发者
SLA	管控及服务平面 99.95%	不对外承诺
云原生应用资产托管	客户自己 OSS Bucket，企业版实例独享 能达到总 40Gbps 下载带宽	OSS Bucket 共享 镜像拉取及推送流控，单Bucket 10Gbps带宽
公共云/VPC/内网访问	支持+网络访问控制	
大规模分发	支持千节点的并发拉取	
全球镜像同步	全球地域+自动同步	仅国内地域+手动触发
云原生交付链	支持 全链路可观测、可追踪、可自主设置	
收费	基于SKU 收费	免费

容器镜像服务企业版 ACR (EE)

企业级解决方案

为企业客户提供安全、高性能的云原生资产托管服务，提供全球镜像同步及大规模分发能力，支撑容器服务等云产品上对安全要求高、业务多地域大规模部署的企业级客户。

- 江苏唱游 (已在生产系统大规模使用)

依赖企业版提供的网络访问控制，避免公网及其他VPC 的访问；使用企业版独享管控及存储，提升镜像生产使用性能和安全性

- 迪士尼 (全球多地域同步)、流利说 (镜像大规模分发)

云原生资产分发底座

被多个云产品集成封装，作为云原生资产托管及分发的基础设施。

- 云市场：支撑容器应用市场的容器商品托管及商业化分发，构建云上云原生生态闭环
- Cloud Native App Hub：支撑 Helm Chart 的全生命周期托管，帮助国内的云原生开发者更便捷稳定使用官方 Chart。

容器镜像服务企业版 ACR (EE)

云原生资产托管及分发的企业级解决方案

云原生 资产托管

- 支持容器镜像全生命周期管理
- 支持 Helm 云原生应用格式

全球化 镜像分发

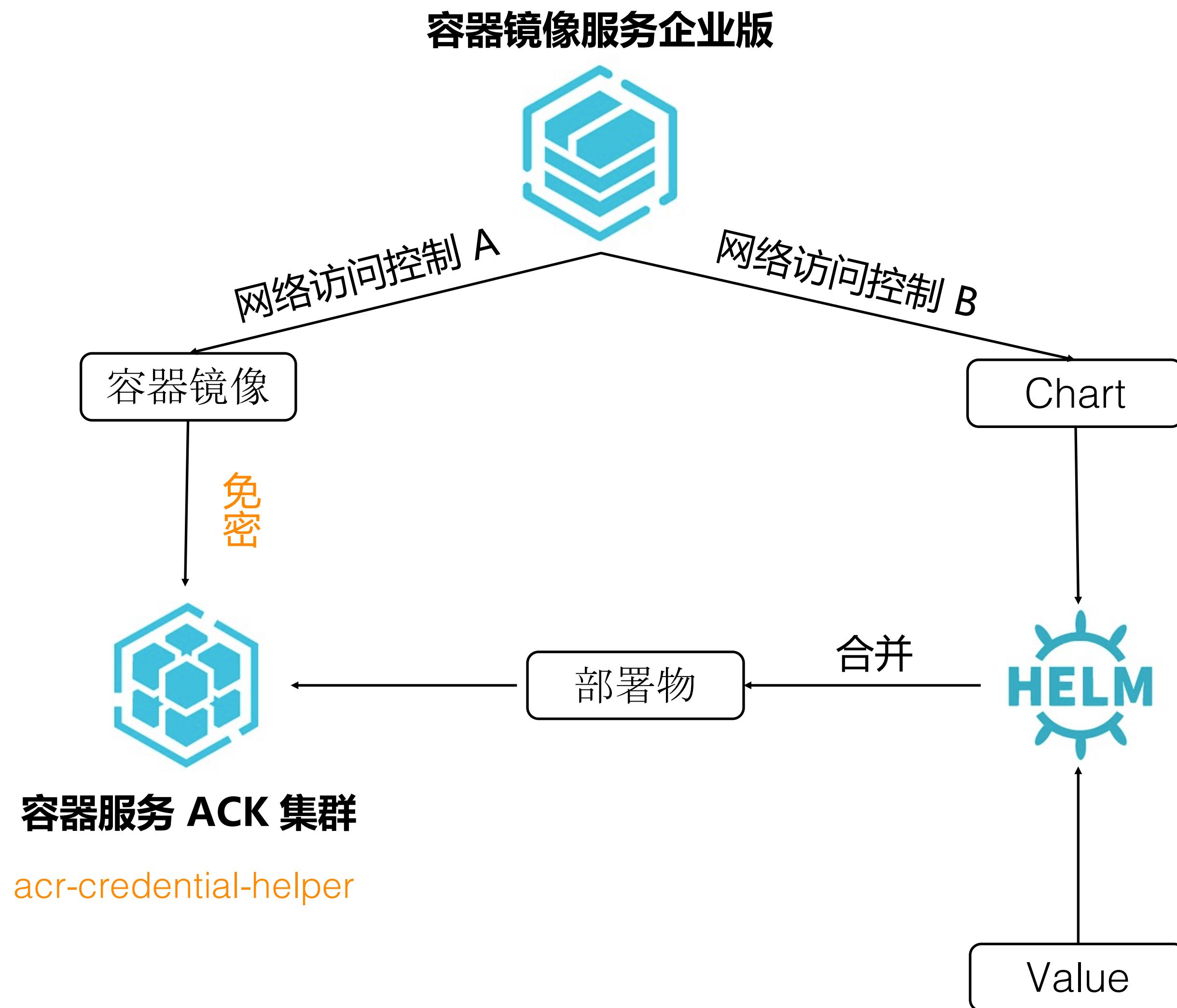
- 全球主要地域覆盖
- 多种同步策略和网络链路优化
- 镜像全球同步效率提升7倍

应用 大规模分发

- 千节点镜像规模化分发
- 分发效率提升4倍

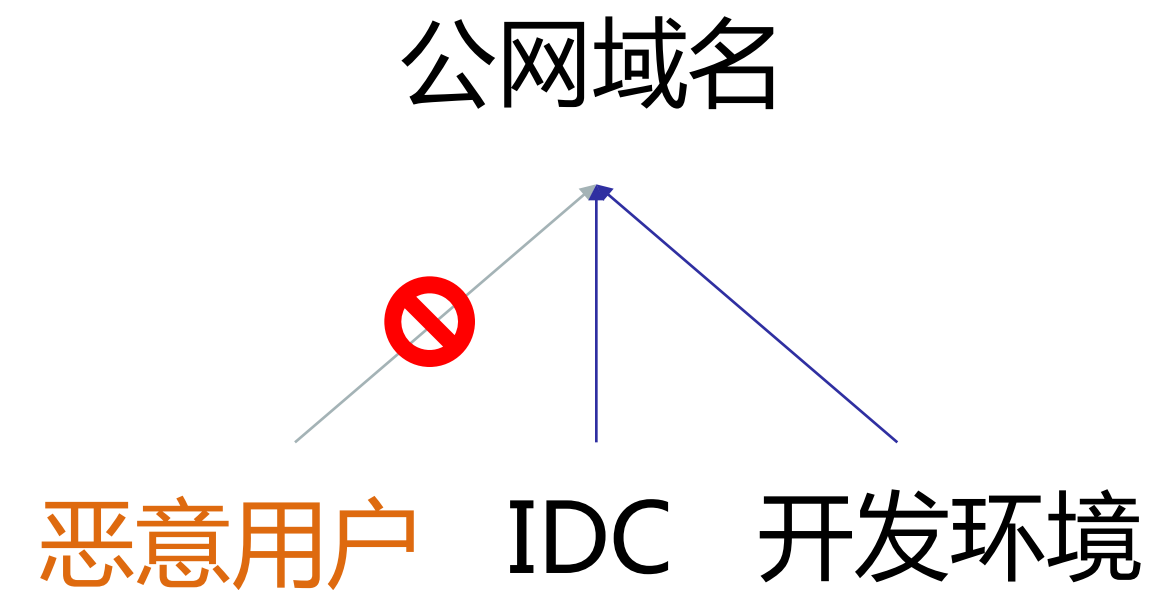
云原生 应用交付链

- Dockerfile 智能优化，构建加速
- 镜像安全扫描，高风险阻断部署
- 镜像加密存储和细粒度权限管理



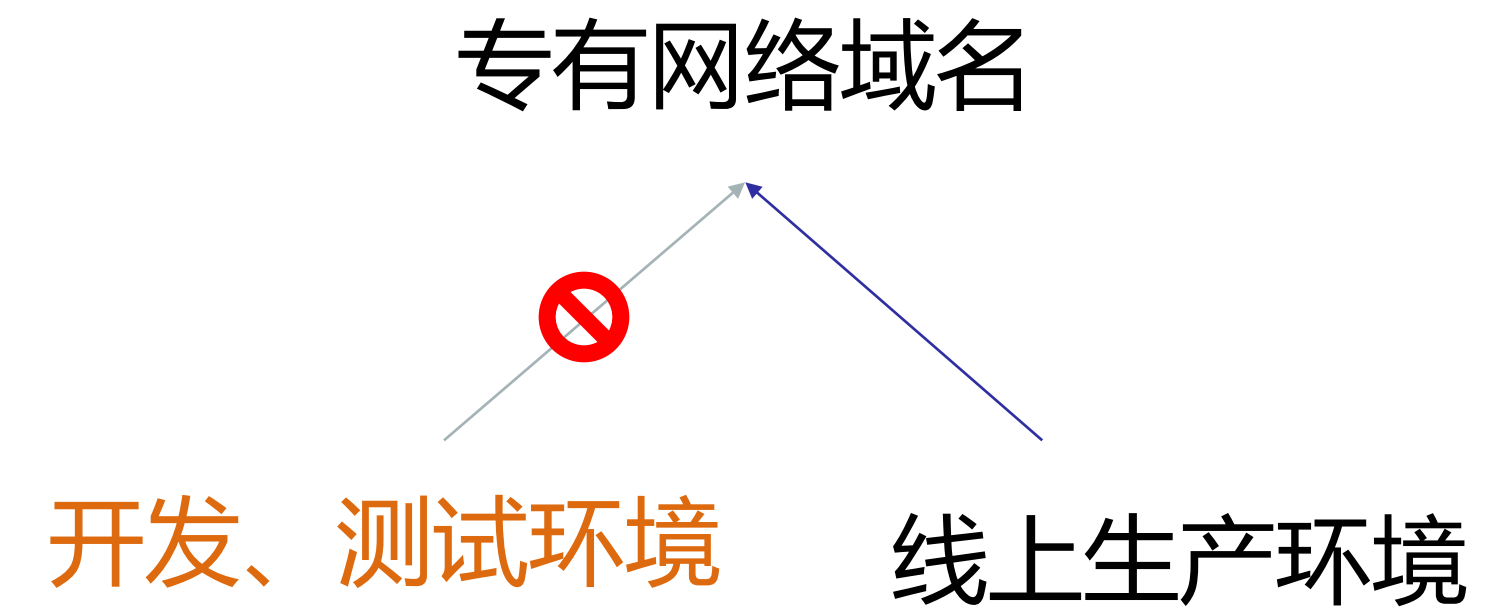
云原生资产托管

网络访问控制



hello-cr-registry.cn-
hangzhou.cr.aliyuncs.com

开关公网入口
自定义 ACL 规则



hello-cr-registry-vpc.cn-
hangzhou.cr.aliyuncs.com

自定义 ACL 规则

云原生资产托管

容器镜像安全扫描



nginx

华东2（上海） | 私有 | 自动构建仓库 | ● 正常

部署应用

安全扫描

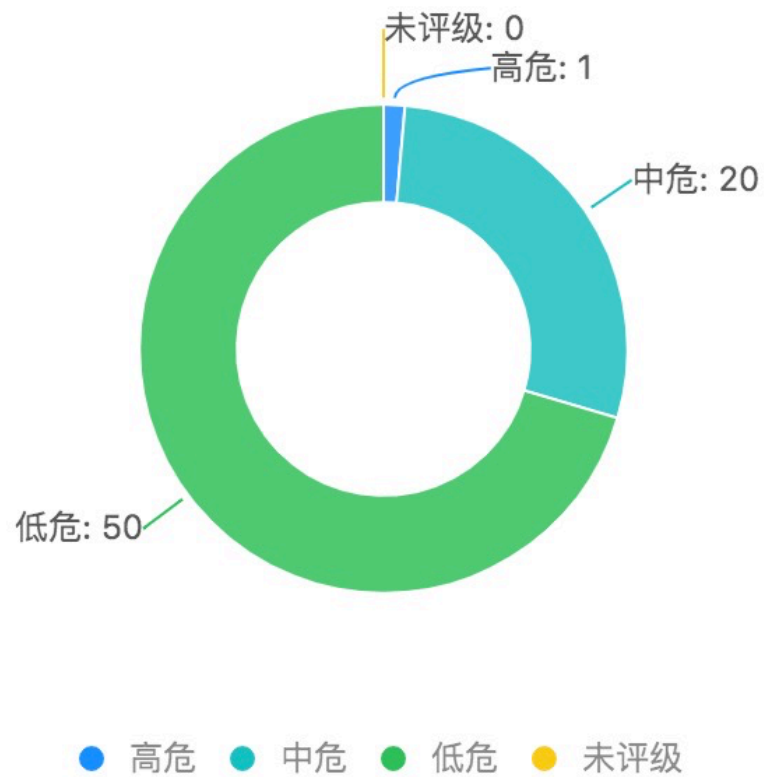
镜像层信息

安全扫描

本次扫描共发现 71 个安全漏洞

镜像缺陷

- 1 高危
- 50 低危
- 20 中危
- 0 未评级



漏洞编号	漏洞等级	软件包	当前版本	修复版本	漏洞位置
CVE-2019-5094	中危	e2fsprogs	1.44.5-1+deb10u1	1.44.5-1+deb10u2	sha256:b8f262c62ec6...
CVE-2019-3844	中危	systemd	241-7~deb10u1		sha256:b8f262c62ec6...
CVE-2019-3843	中危	systemd	241-7~deb10u1		sha256:b8f262c62ec6...
CVE-2019-17371	中危	libpng1.6	1.6.36-6		sha256:e9218e8f93b1...
CVE-2019-15847	中危	gcc-8	8.3.0-6		sha256:b8f262c62ec6...



云原生资产托管

容器镜像安全扫描



安全扫描

镜像层信息

```
trusted=yes ] file://$tempDir ./" > /etc/apt/sources.list.d/temp.list && apt-get -o Acquire::GzipIndexes=false update ;; esac && apt-get install --no-install-recommends --no-install-suggests -y $nginxPackages gettext-base && apt-get remove --purge --auto-remove -y ca-certificates && rm -rf /var/lib/apt/lists/* /etc/apt/sources.list.d/nginx.list && if [ -n "$tempDir" ]; then apt-get purge -y --auto-remove && rm -rf "$tempDir" /etc/apt/sources.list.d/temp.list; fi
```

> sha256:a3ed95caeb02...

32 Bytes

ENV

PKG_RELEASE=1~buster

> sha256:a3ed95caeb02...

32 Bytes

ENV

NJS_VERSION=0.3.5

> sha256:a3ed95caeb02...

32 Bytes

ENV

NGINX_VERSION=1.17.4

> sha256:a3ed95caeb02...

32 Bytes

LABEL

maintainer=NGINX Docker Maintainers <docker-maint@nginx.com>

> sha256:a3ed95caeb02...

32 Bytes

CMD

["bash"]

> sha256:b8f262c62ec6...

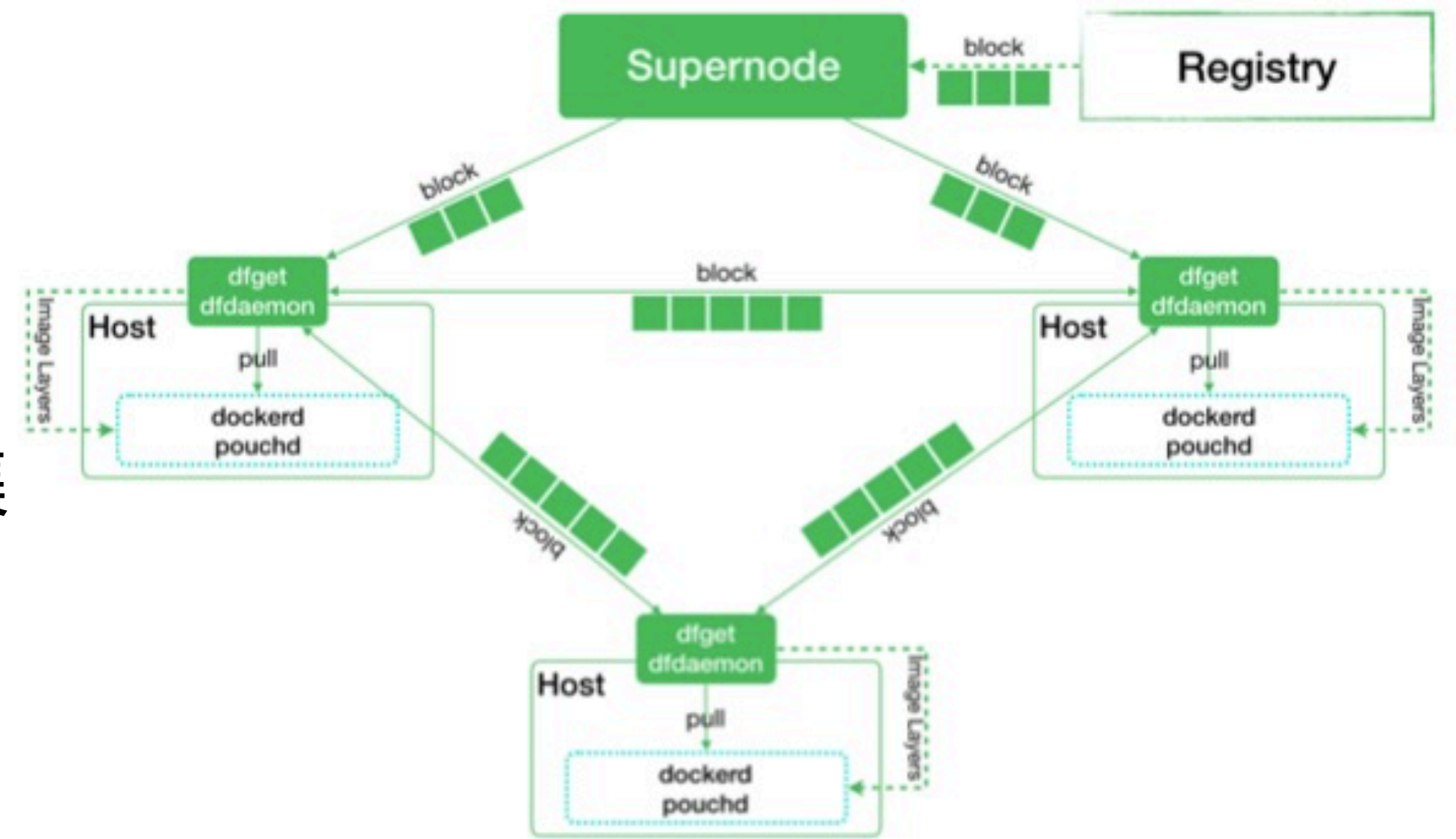
25.839 MB

RUN

ln -sf /dev/stdout /var/log/nginx/access.log && ln -sf /dev/stderr /var/log/nginx/error.log

云原生应用规模化分发

- 阿里集团在多年业务极速扩张及双十一大促场景，打磨出蜻蜓 Dragonfly（为 CNCF 的 SandBox 项目）工具，可以将镜像高速分发到全世界的各个机房。
- 容器镜像服务企业版基于 Dragonfly 加速用户大规模集群节点并发拉取镜像场景。



云原生应用规模化分发

容器镜像服务企业版提供分发域名

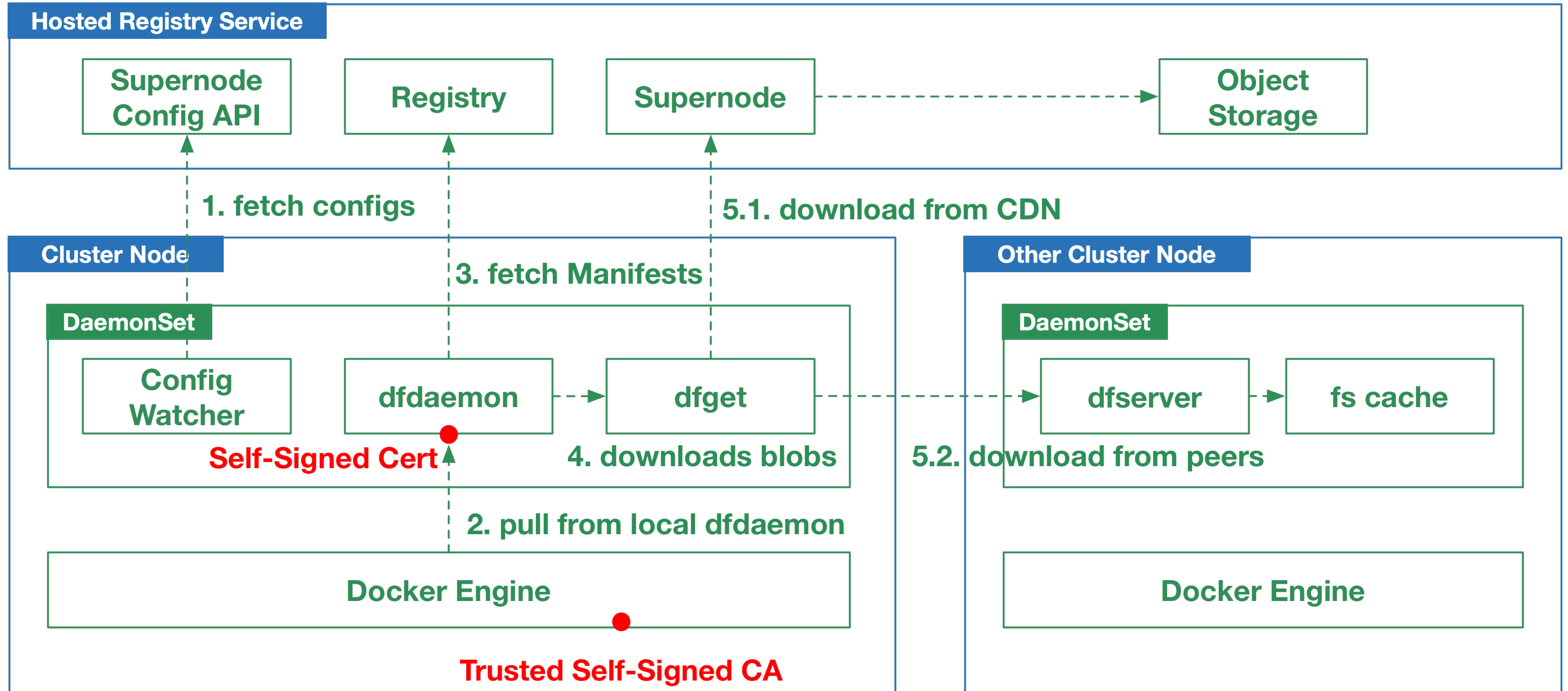
P2P 加速域名

hello-cr-registry-vpc.distributed.cn-hangzhou.cr.aliyuncs.com
-> 解析至本地

容器镜像服务提供 installer :

- 在集群中安装 DaemonSet
- 生成一张自签发证书，分发到所有 Docker Engine 目录中

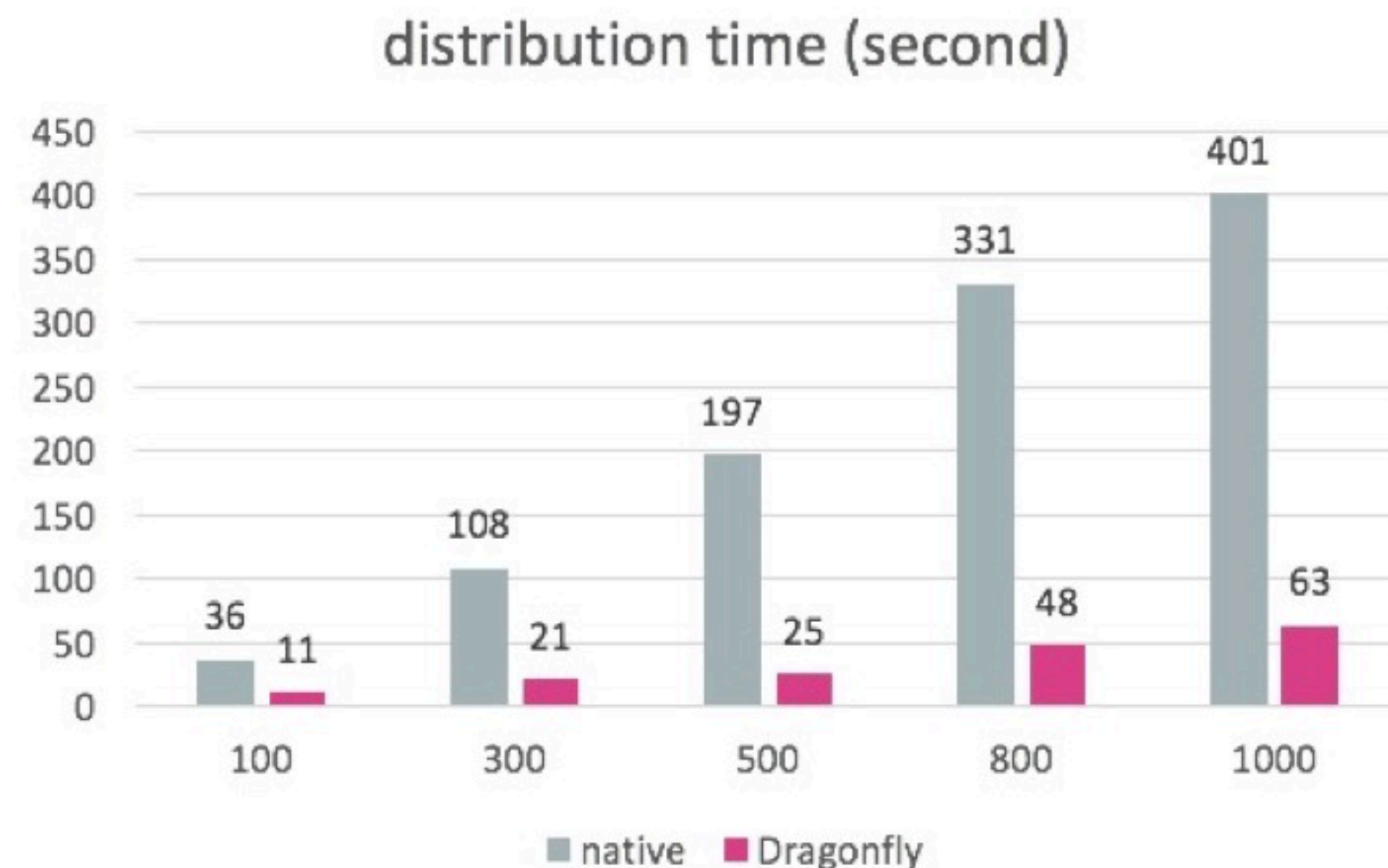
云原生应用规模化分发



云原生应用规模化分发



分发 512MB 镜像到 800 节点集群



分发 512MB 镜像到不同大小的集群

节约 80%的时间，分发效率提升 4倍

目录

云原生定义

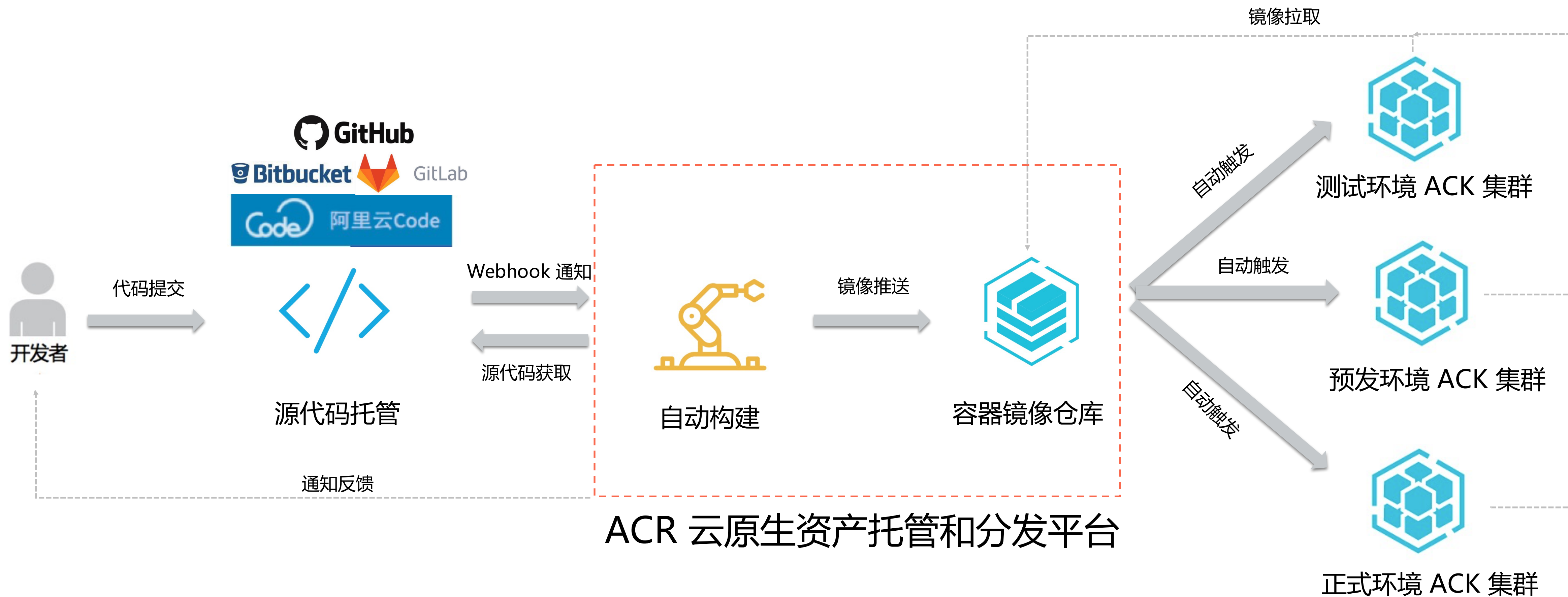
容器镜像服务产品

典型场景

演示

典型场景一

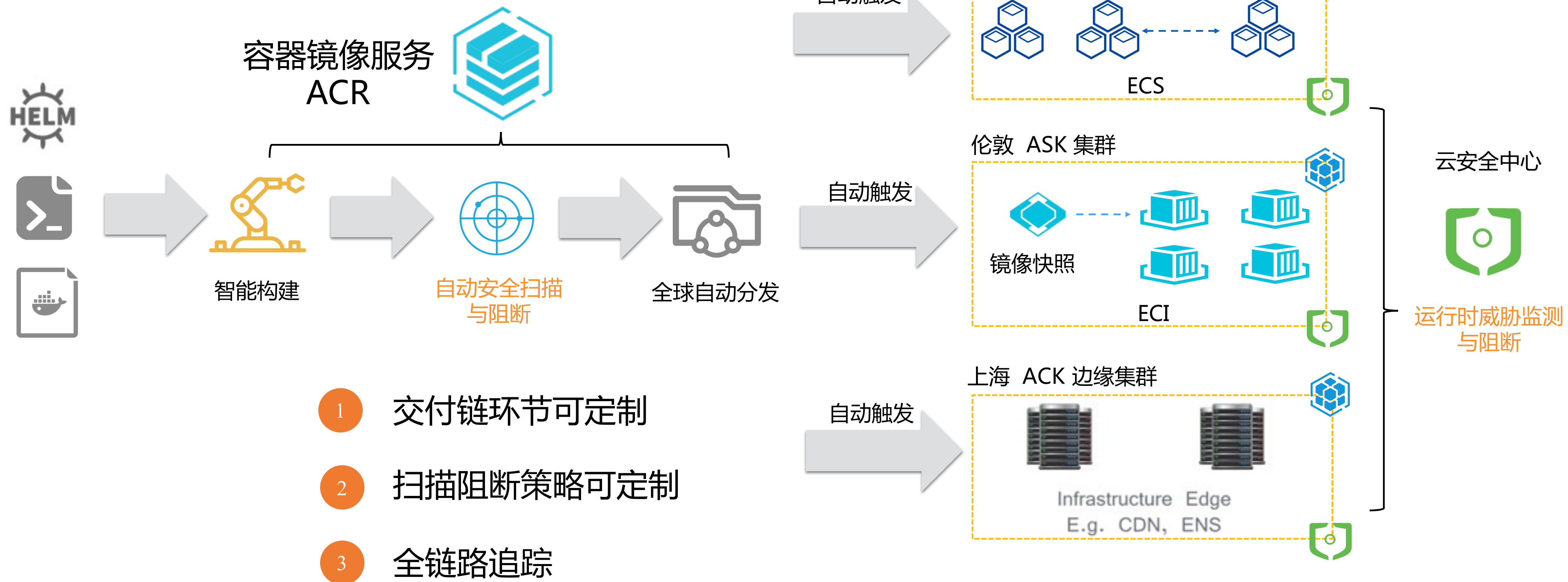
容器化 DevOps 最佳实践



典型场景 二

云原生应用交付链

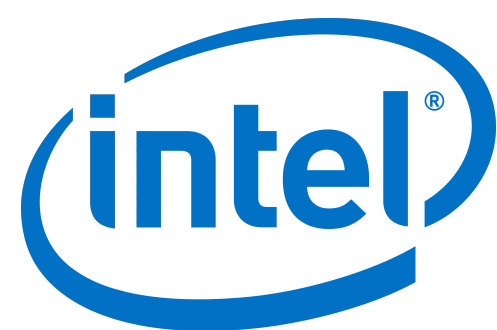
一次提交，全球多样场景自动交付



典型场景 三

容器应用市场

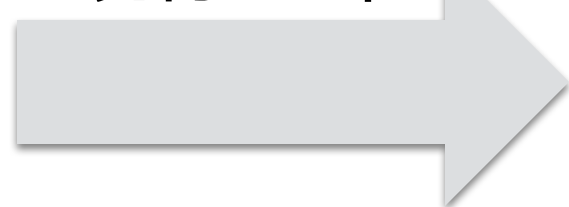
全球生态伙伴



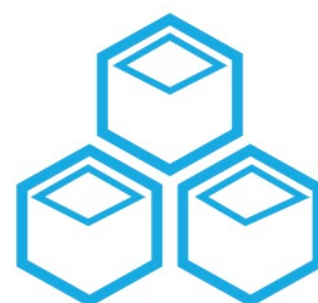
FORTINET

ATHINE 奥哲

镜像上架

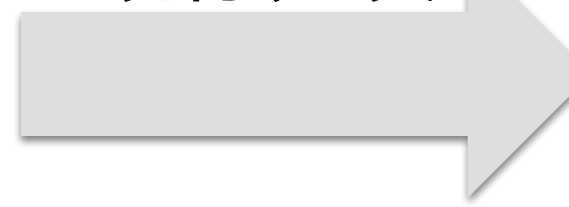


容器应用市场



云市场
容器镜像服务
企业版实例

镜像分发



企业生产环境



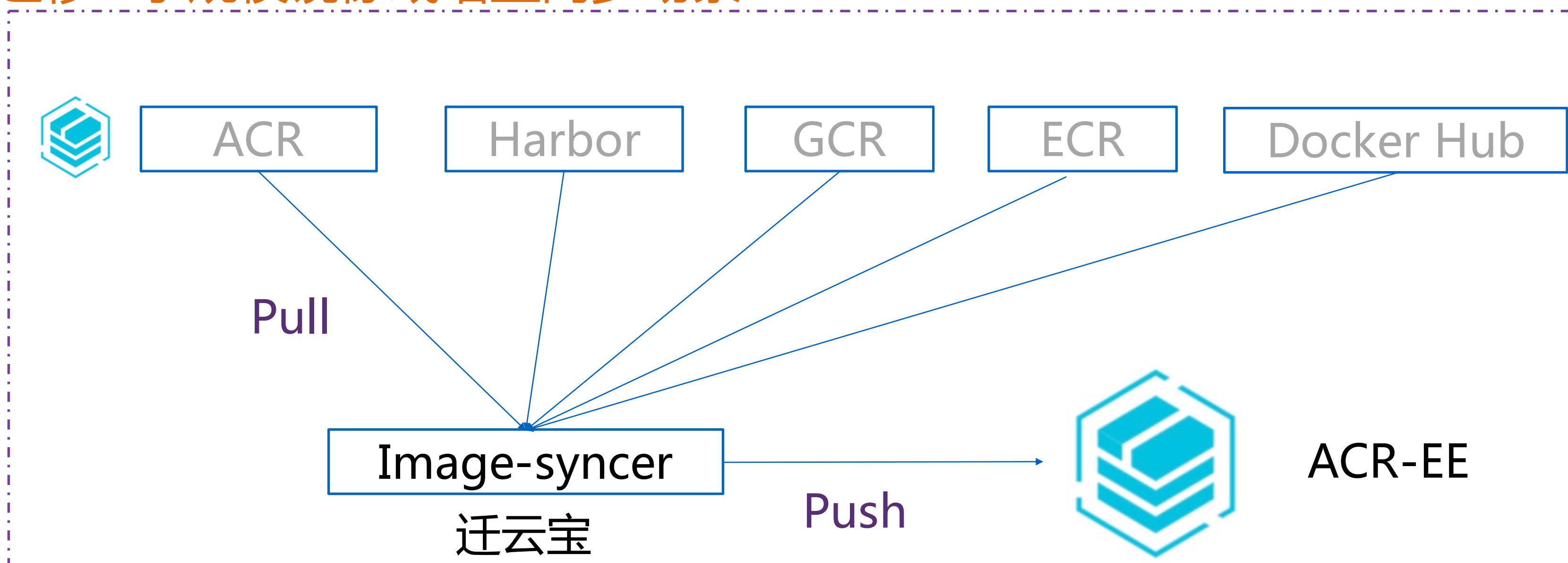
ACK 集群

- 1 基于容器镜像服务包装并向用户分发镜像
- 2 镜像上架安全审核及验证
- 3 阿里云提供安全的基础镜像

典型场景 四

迁云场景-容器镜像迁入

迁移1 小规模镜像或增量同步场景



迁移2 大规模镜像迁入



- 1 基于OSS 迁移及导入，迁云效率大幅提升
- 2 企业版实例的灾难恢复

目录

云原生定义

容器镜像服务产品

典型场景

演示

容器镜像服务企业版

概览页面



华东2（上海） | 标准版 | 运行中

概览

仓库管理

镜像仓库

命名空间

代码源

访问控制

Helm Chart

Chart 仓库

命名空间

访问控制

实例管理

访问凭证

监控信息

审计日志

分发管理

实例信息

实例名	付费类型	-	实例规格	标准版
实例ID	到期天数	-	并发拉取支持	500节点
地域	到期日期	-		
华东2（上海）				

仓库信息

仓库	命名空间	OSS Bucket	cri-50i5srla7...
2/1000	1/100	OSS 存储容量	42.725 MB
		OSS 存储数据	加密保护中 ✓

基本功能



Helm Chart NEW
支持独立访问控制的 Helm Chart 管理



实例同步 NEW
支持命名空间、仓库级别的镜像全球同步



P2P 加速
通过 P2P 加速器配置，保障大规模并发拉取镜像



触发器通知
配置镜像触发器，镜像推送完成后自动触发通知



安全扫描
可提供一键扫描镜像的安全漏洞



镜像部署
一键快速部署镜像到容器服务 Kubernetes/Swarm 集群

访问控制

专有网络 `o-registry-vpc.cn-shanghai.c`
`r.aliyuncs.com` [复制](#)

白名单 1个

公网

白名单 0个 [设置白名单](#)

组件设置

Charts

状态 运行中

联系我们

容器镜像服务企业版

云原生应用交付链

华东1 (杭州)

创建交付链

交付链名称: test

创建交付链

欢迎使用云原生交付链, 加速您的业务创新迭代。

1 基本信息

2 交付链

镜像构建 镜像推送 安全扫描 磁盘快照 分发触发器

触发同步 分发触发器

任务配置

构建规则设置

Branch/Tag	Dockerfile目录	Dockerfile文件名	镜像版本	操作
branches:release-v(?<tag>\d*)	/	Dockerfile	\${tag}	修改 删除

[添加规则](#)

上一步 确定 取消

