OSC 源创会 Opensource Innovation Meetup | IT大咖说 知识共享平台

# 2017源创会年终盛典

## 与电子标准院共建开源标准

12月23日　北京万豪酒店

主办方 开源中国 oschina.net　ESI

# 采用开源 Harbor Registry 实现高效安全的容器镜像运维

张海宁
VMware 中国研发中心技术总监

主办方 开源中国 oschina.net ESI

# 自我介绍

- VMware 中国研发先进技术中心首席架构师、技术总监
- Harbor 开源企业级容器 Registry 项目创始人
- Cloud Foundry 中国社区最早技术布道师之一
- 《区块链技术指南》、《软件定义存储》作者之一

公众号：亨利笔记


《区块链技术指南》


《软件定义存储》

# 议程

1 容器镜像基础

2 Harbor开源镜像仓库简介

3 镜像的一致性

4 安全性

5 镜像分发

6 总结

# 议程

1 容器镜像基础

2 Harbor开源镜像仓库简介

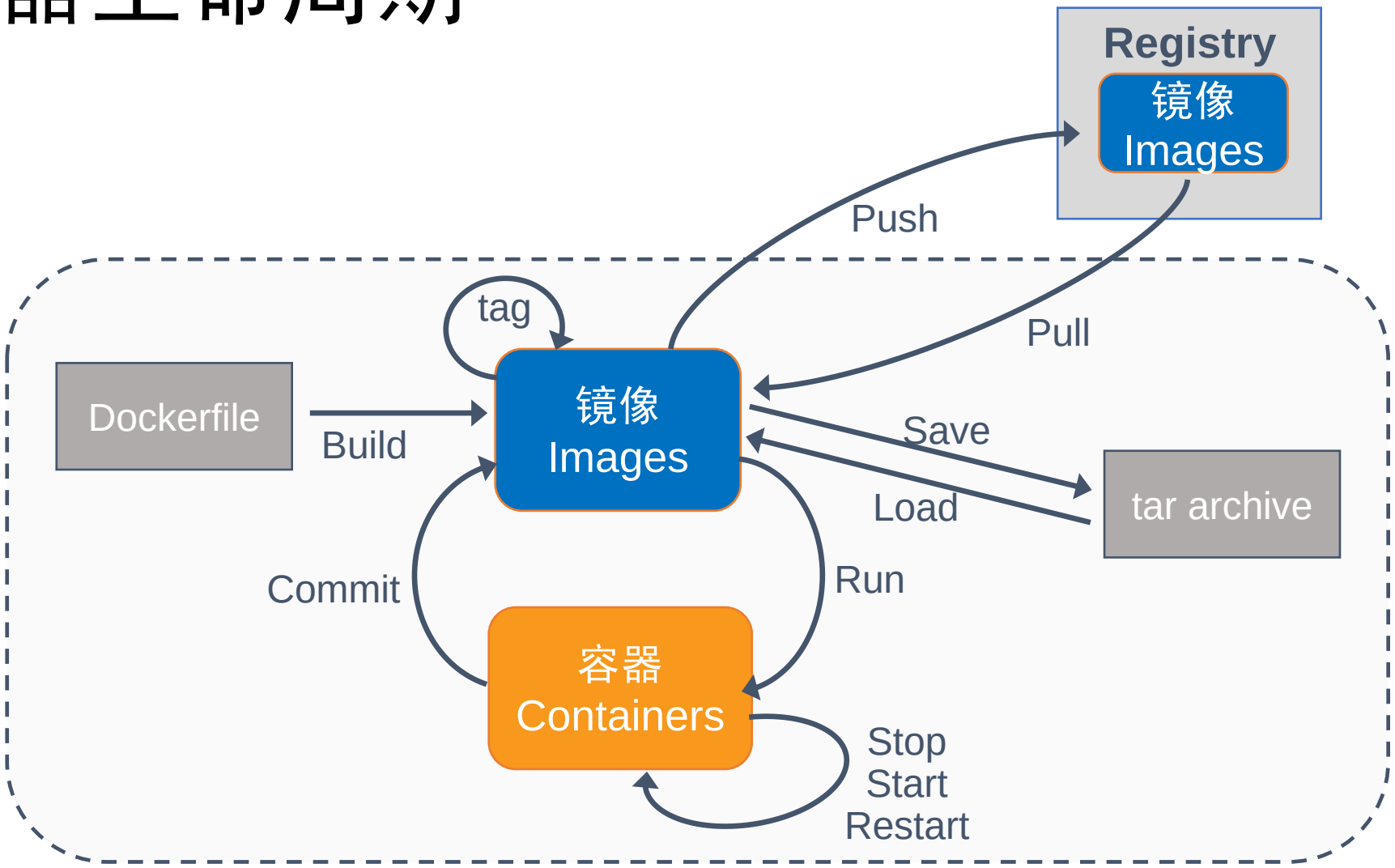
3 镜像的一致性

4 安全性

5 镜像分发

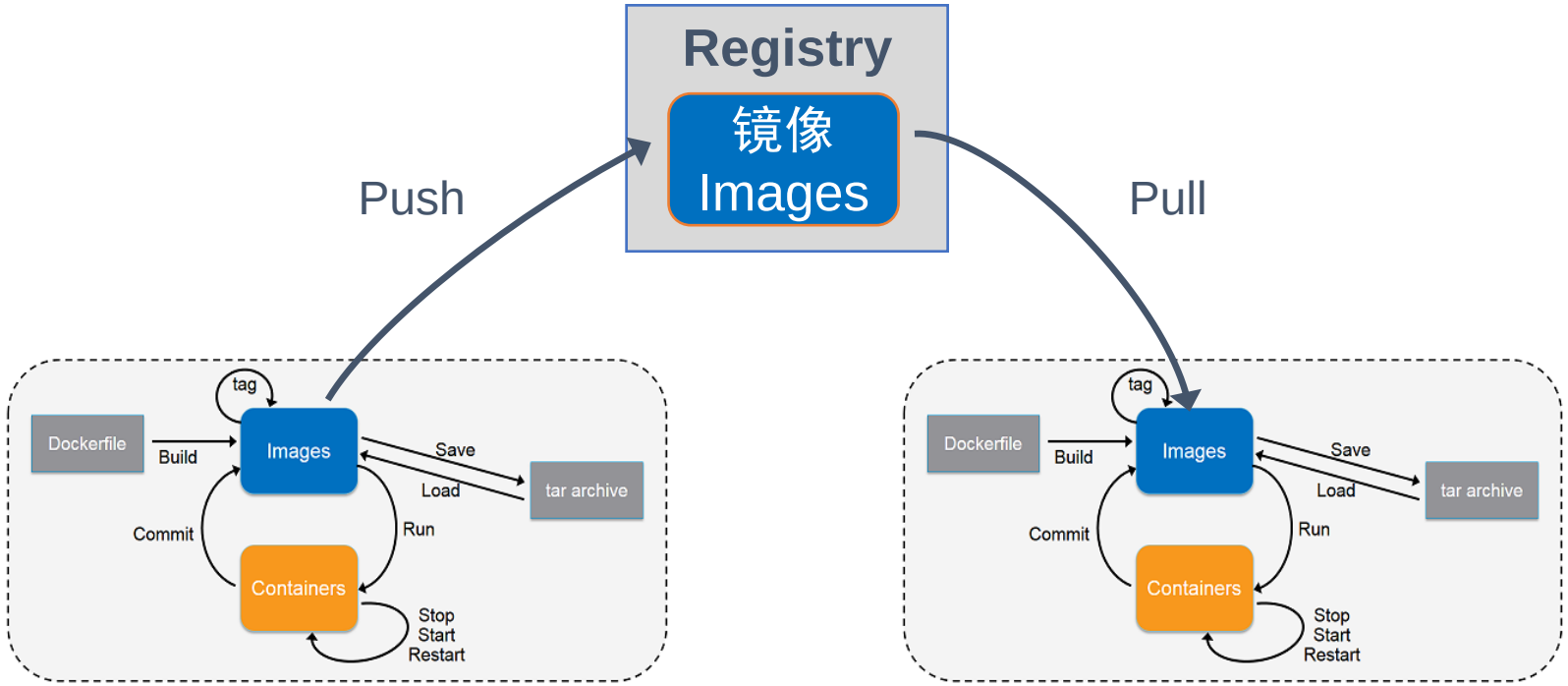
6 总结

# 容器生命周期


Registry
镜像
Images
Push
Pull
tag
Dockerfile
Build
镜像
Images
Save
Load
tar archive
Commit
Run
容器
Containers
Stop
Start
Restart

# Registry – 镜像管理的重要部件

- 镜像存储仓库
- 分发镜像的媒介
- 访问控制和镜像管理较佳节点



# 议程

# Harbor开源项目


- 开源企业级容器镜像仓库
- 由 VMware 中国团队设计和开发
- 集成到多个企业级产品中
- Apache 2 使用许可
- https://github.com/vmware/harbor/

# 主要特性

HARBOR™

- 用户管理和访问控制
  - 基于角色的访问控制（RBAC）
  - AD/LDAP 用户身份集成
- 镜像远程复制
- 镜像安全漏洞扫描
- 镜像来源公证（content trust）
- 图形化管理界面
- 审计和日志
- Restful API

# 用户和开发者情况


3200+
Stars
20K+
Downloads
800+
Users
66
Contributors
900+
Forks
6
Partners

# Harbor部分用户

caicloud 才云

RANCHER

数人云 shurenyun.com

品高云 BingoCloud

时速云 tenxcloud.com

安吉星 OnStar

TREND MICRO

AXA 安盛天平

TalkingData

通联数据 DATAYES

iFRE

亿阳信通 BOCO Inter-Telecom

wise2c TECHNOLOGY

慧博云通 HYDSOFT

SLAMTEC

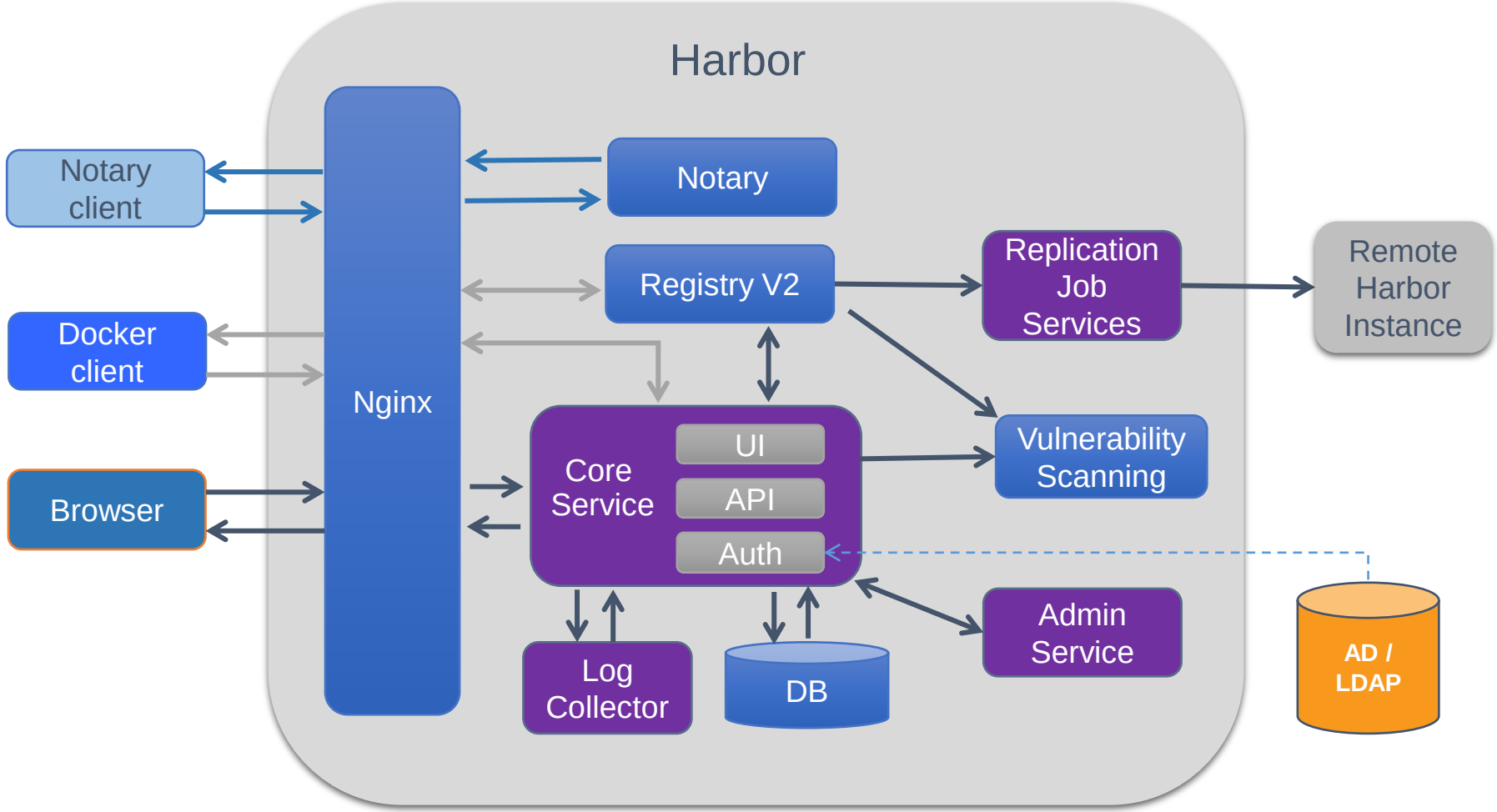
Open EDUTAINMENT 奥鹏教育

BOER 博耳智能 BOER SMART

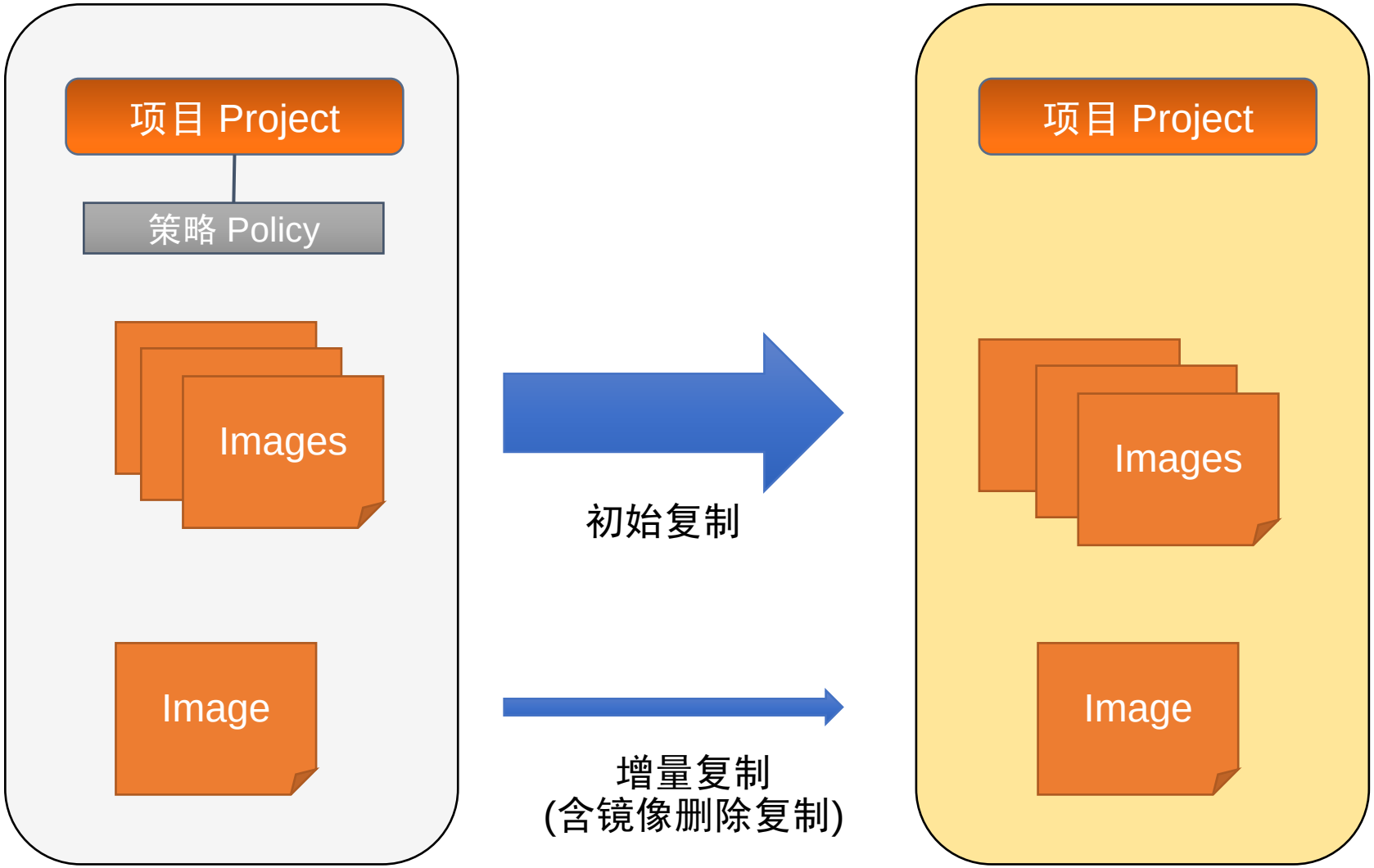
云星数据

BEYONDSOFT beyond your expectations

# Harbor 架构


Harbor
Notary client
Docker client
Browser
Nginx
Notary
Registry V2
Core Service
UI
API
Auth
Log Collector
DB
Replication Job Services
Vulnerability Scanning
Admin Service
Remote Harbor Instance
AD / LDAP

# 镜像复制




复制过程可自动
故障恢复

# 议程

# 容器镜像的一致性

- 容器镜像贯穿软件生命周期各个阶段
  - 开发
  - 测试
  - 准生产
  - 产线

- 镜像一致性重要性
  - 版本控制
  - 问题追踪
  - 审计

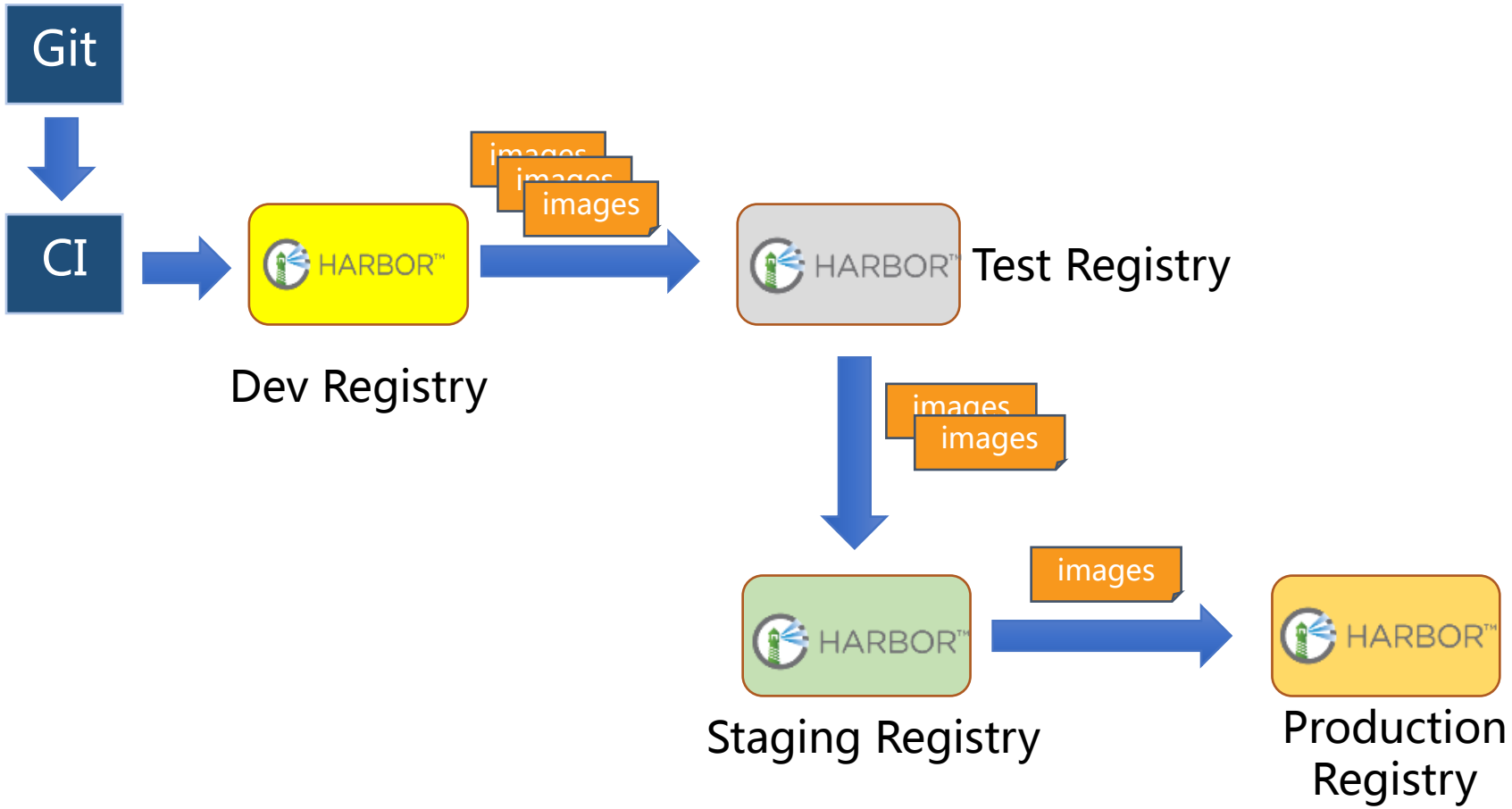
# 同一个 Dockerfile 始终生成同一个镜像?

例子:

```
FROM ubuntu
RUN apt-get install –y python
ADD app.jar /myapp/app.jar
```

- 基础镜像 ubuntu:latest 可能在不同构建时间会有差别
- 即使 ubuntu:14.04 也可能会有改变(补丁不同)
- apt-get (curl, wget..) 无法保证安装同样的软件包
- ADD 依赖构建时候的文件

# 用二进制格式确保镜像一致性




不同环境中的镜像同步使用Harbor registry来实现

# 议程

1 容器镜像基础

2 Harbor开源镜像仓库简介

3 镜像的一致性

4 安全性

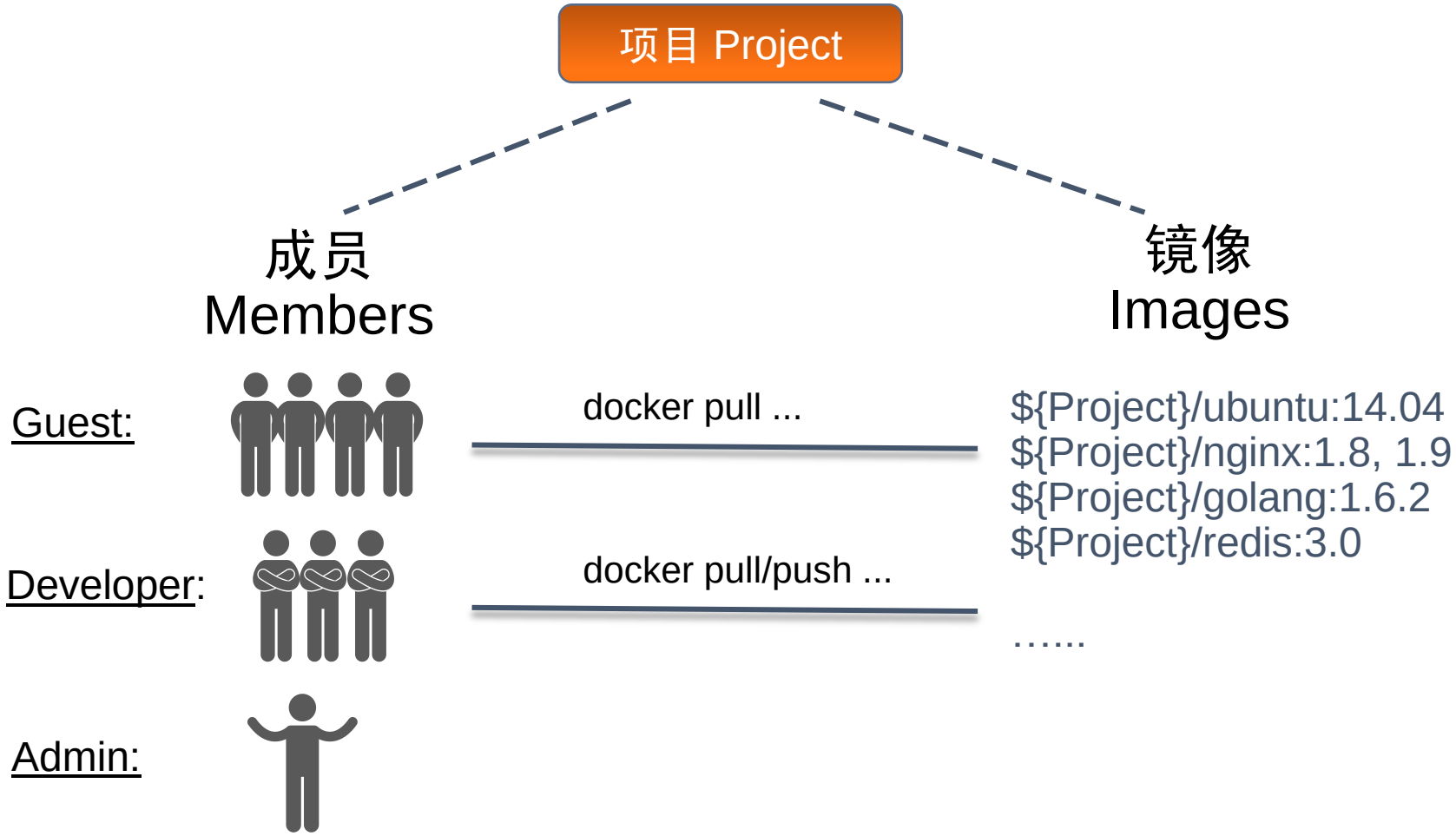
5 镜像分发

6 总结

# 镜像访问控制

- 企业用户通常报镜像存放在组织内部
  - 知识产权不泄漏
  - 高效率: LAN vs WAN
- 不同角色人员应有不同的访问权限
  - 开发人员– Read/Write
  - 测试人员– Read Only
- 不同环境人员的角色不同
  - 开发测试环境 – 许多人可访问
  - 生产系统– 少数人可以接触

# 例子: Harbor中基于角色的访问控制



# 其他安全考虑

- 使用内容信任（ content trust）
  - 发布者对镜像签名
  - 下载镜像时使用签名摘要（Digest）

- 进行漏洞扫描
  - 阻止有漏洞对镜像被拉取
  - 定期更新漏洞数据库

# 镜像漏洞扫描

- 漏洞扫描是对镜像的文件做静态分析
- 漏洞数据来源
  - Debian Security Bug Tracker
  - Ubuntu CVE Tracker
  - Red Hat Security Data
  - Oracle Linux Security Data
  - Alpine SecDB

# Registry 的镜像扫描

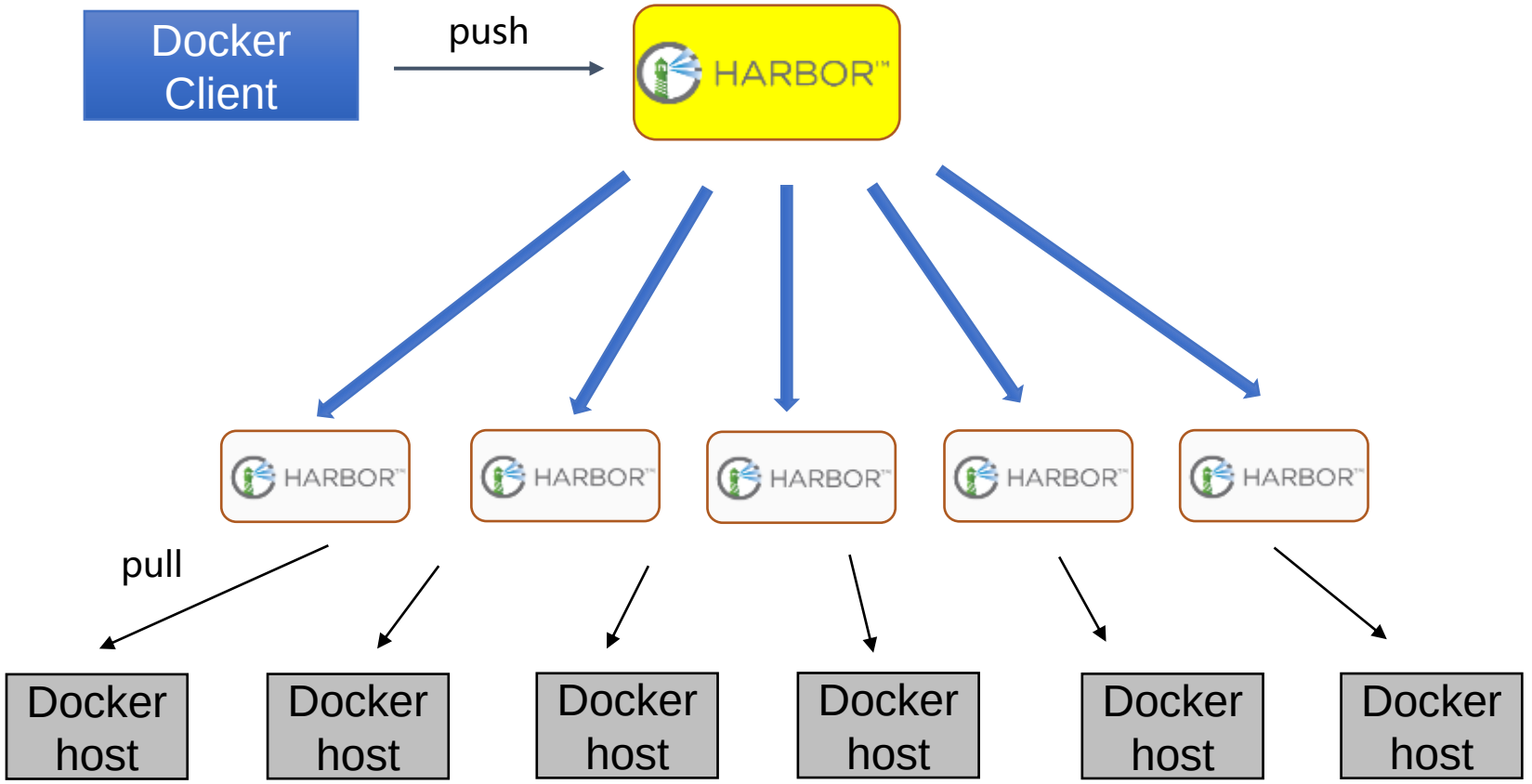
- 设置漏洞级别阀值
- 超过阀值的镜像无法下载
- 定期更新漏洞数据库

# 议程

# 镜像分发

- 容器镜像通常从registry分发
- 在大规模集群场景下，Registry 是镜像分发瓶颈
  - I/O
  - 网络带宽
- 扩展 registry 服务
  - 多实例 registry 共享存储
  - 多实例 registry 不共享存储

# 复制技术在镜像分发中应用




Master – Slave 模式

# 总结

- 镜像运维是容器运维中重要部分
- Registry 是镜像运维最重要的部件
- Harbor 可帮助企业用户运维容器镜像