2017 China Kubernetes End User Conference
kubernetes 中国用户大会
KEUC 2017
2017.10.15 / 中国 · 杭州

Secure and Efficient Container Image Management for Kubernetes via Harbor

在Kubernetes上采用Harbor高效安全管理镜像

张海宁， VMware中国研发先进技术中心技术总监
杜　宁， Caicloud解决方案与交付副总裁

主办： CLOUD NATIVE COMPUTING FOUNDATION caicloud

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
- 多年全栈工程师
- 《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》

Agenda

1 Container Image Basics

2 Project Harbor Introduction

3 Consistency of Images

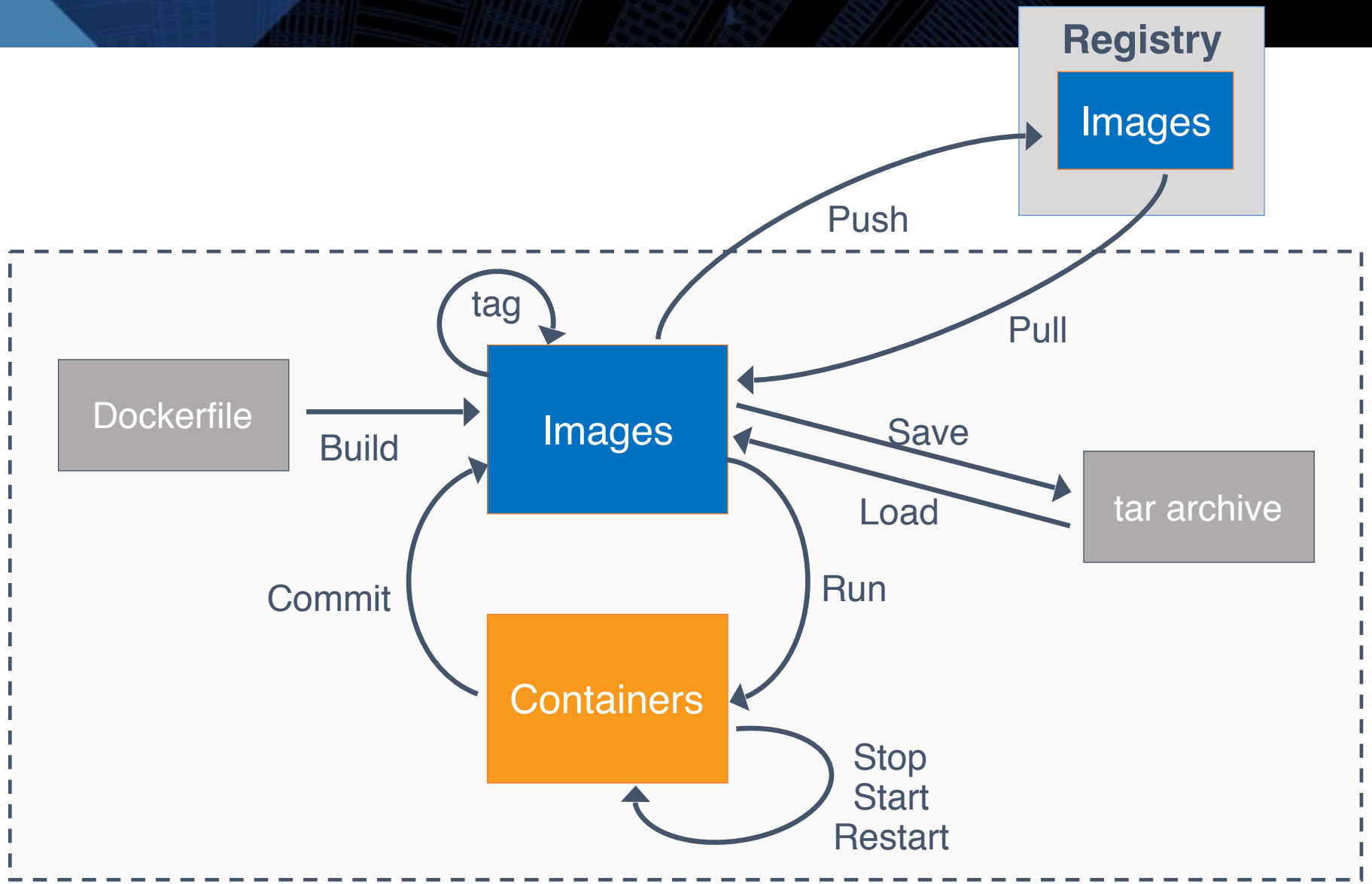
4 Security

5 Image Distribution

6 Integration with Kubernetes

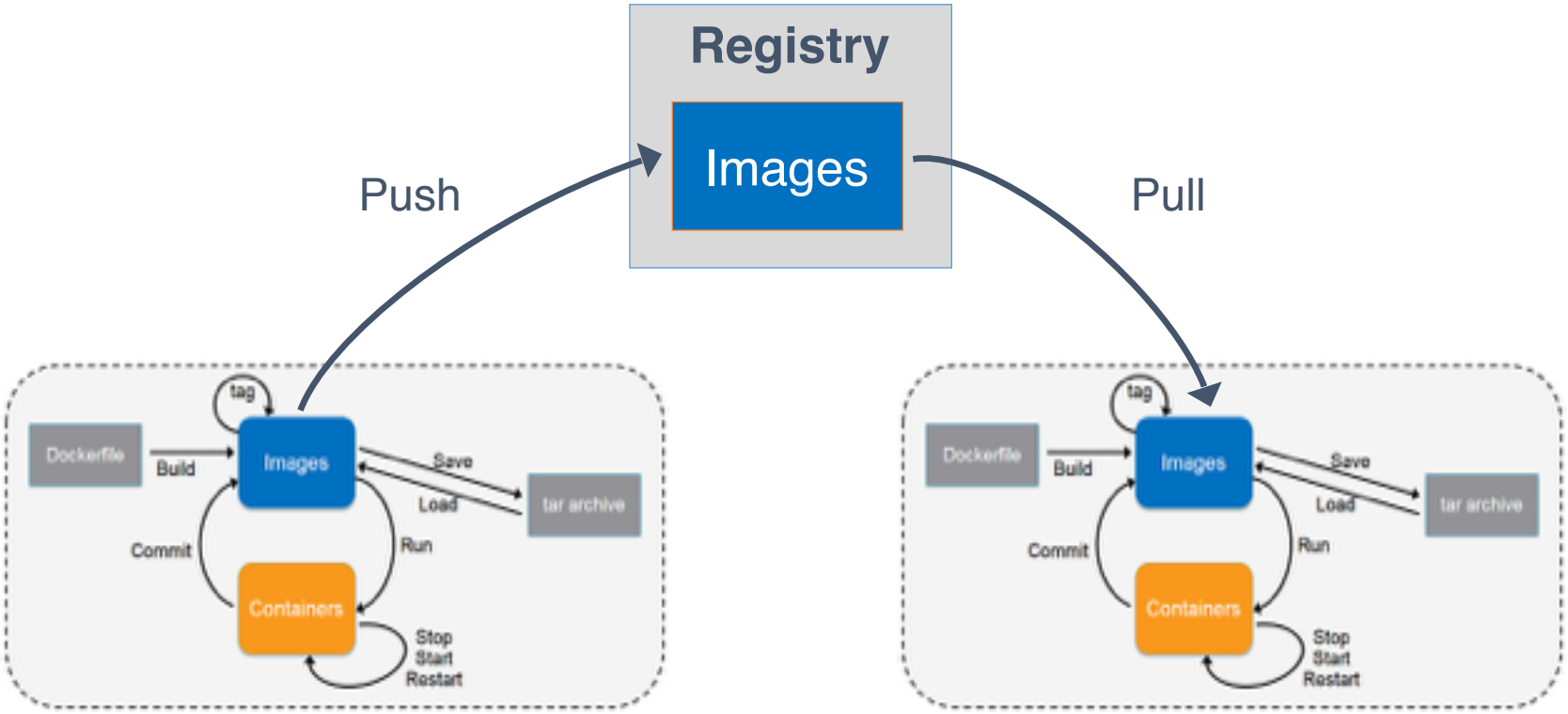
Agenda

Lifecycle of Containers and Images



Registry - Key Component to Manage Images

- Repository for storing images
- Intermediary for shipping and distributing images
- Ideal for access control and other image management



Agenda

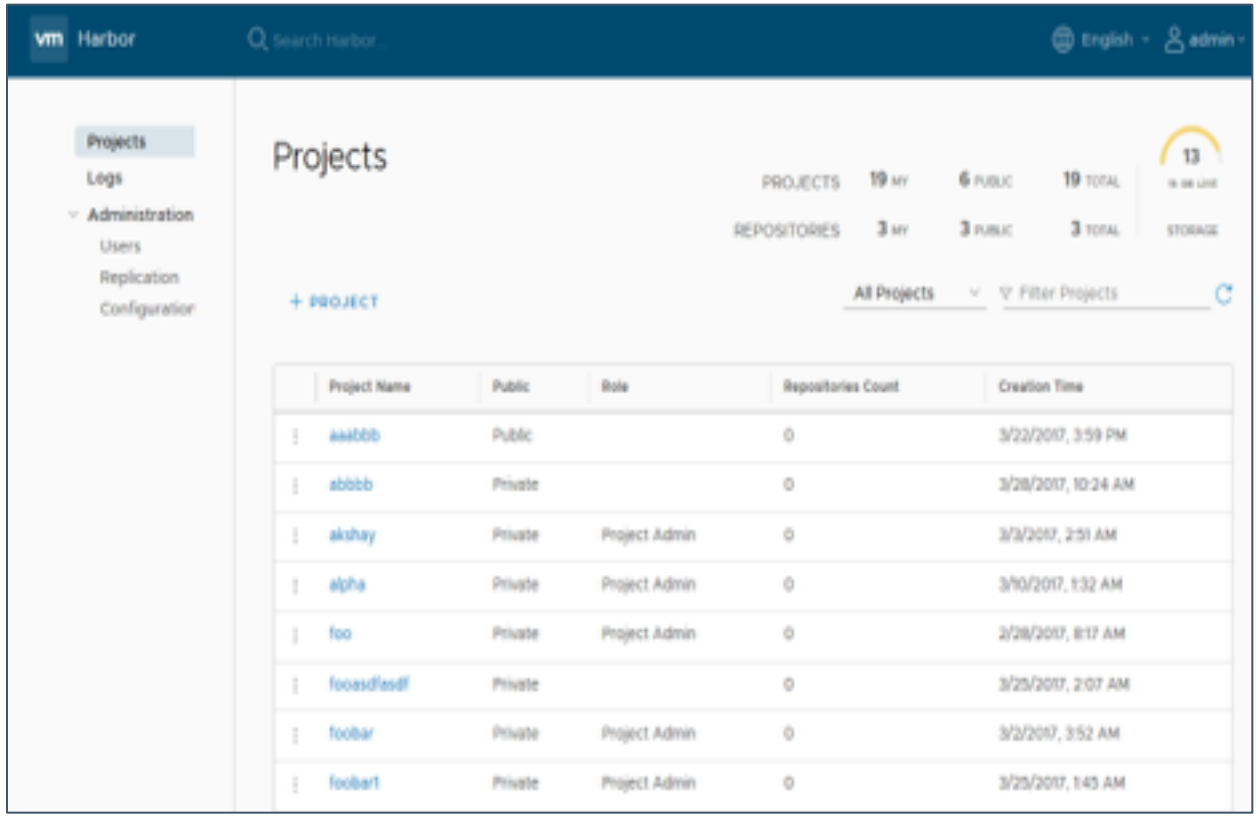
Project Harbor

HARBOR™

- An open source enterprise-class registry server.
- Initiated by VMware China, adopted by users worldwide.
- Apache 2 license.
- https://github.com/vmware/harbor/

Key Features

- User management & access control
  - RBAC: admin, developer, guest
  - AD/LDAP integration
- Policy based image replication
- Vulnerability Scanning
- Notary
- Integrated with Kubernetes
- Web UI
- Audit and logs
- Restful API for integration
- Lightweight and easy deployment



HARBOR™

Harbor Momentum

20K+	2800+	1000+
Downloads	**Stars**	**Users**
800+	58	6
Forks	**Contributors**	**Partners**

Harbor Users and Partners

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

主办： CLOUD NATIVE COMPUTING FOUNDATION caicloud 才云

Harbor Architecture

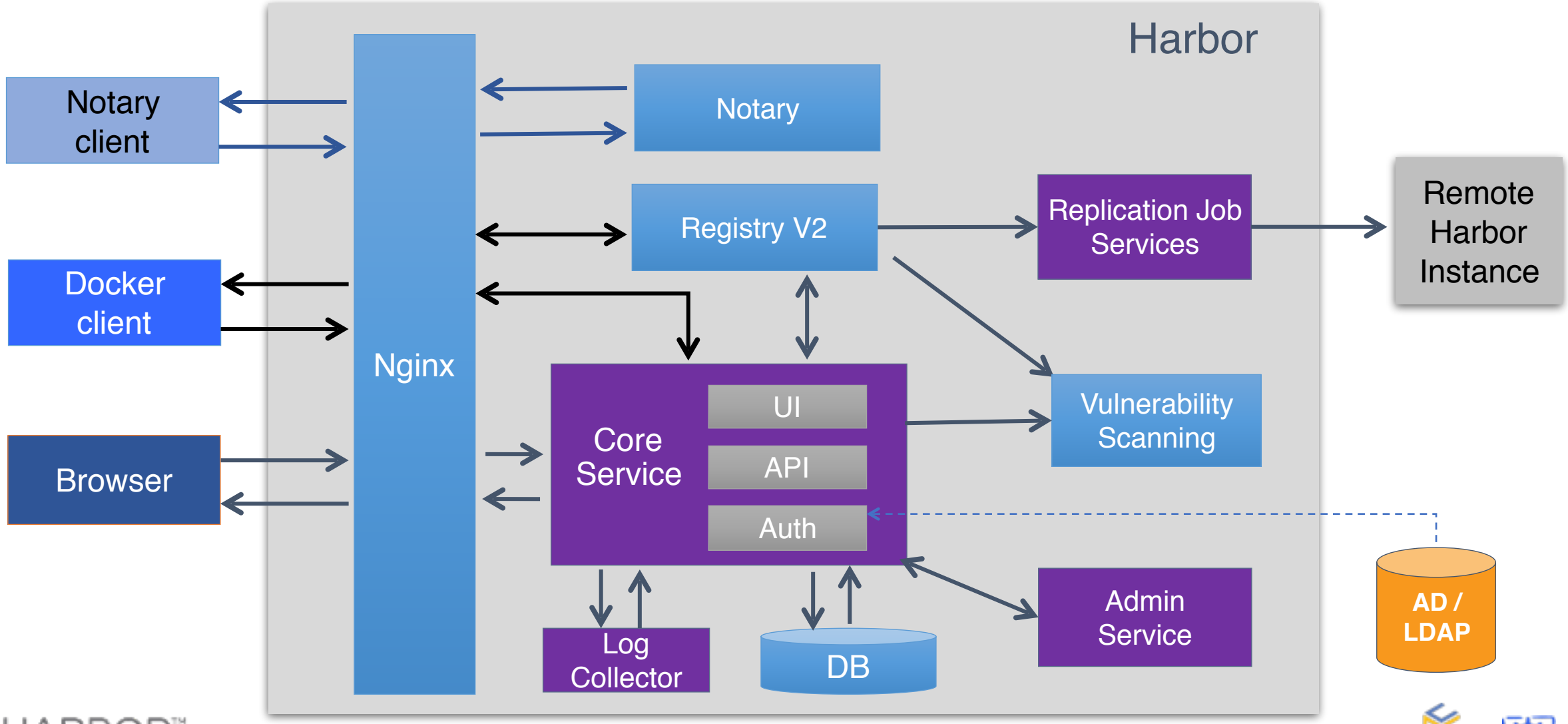
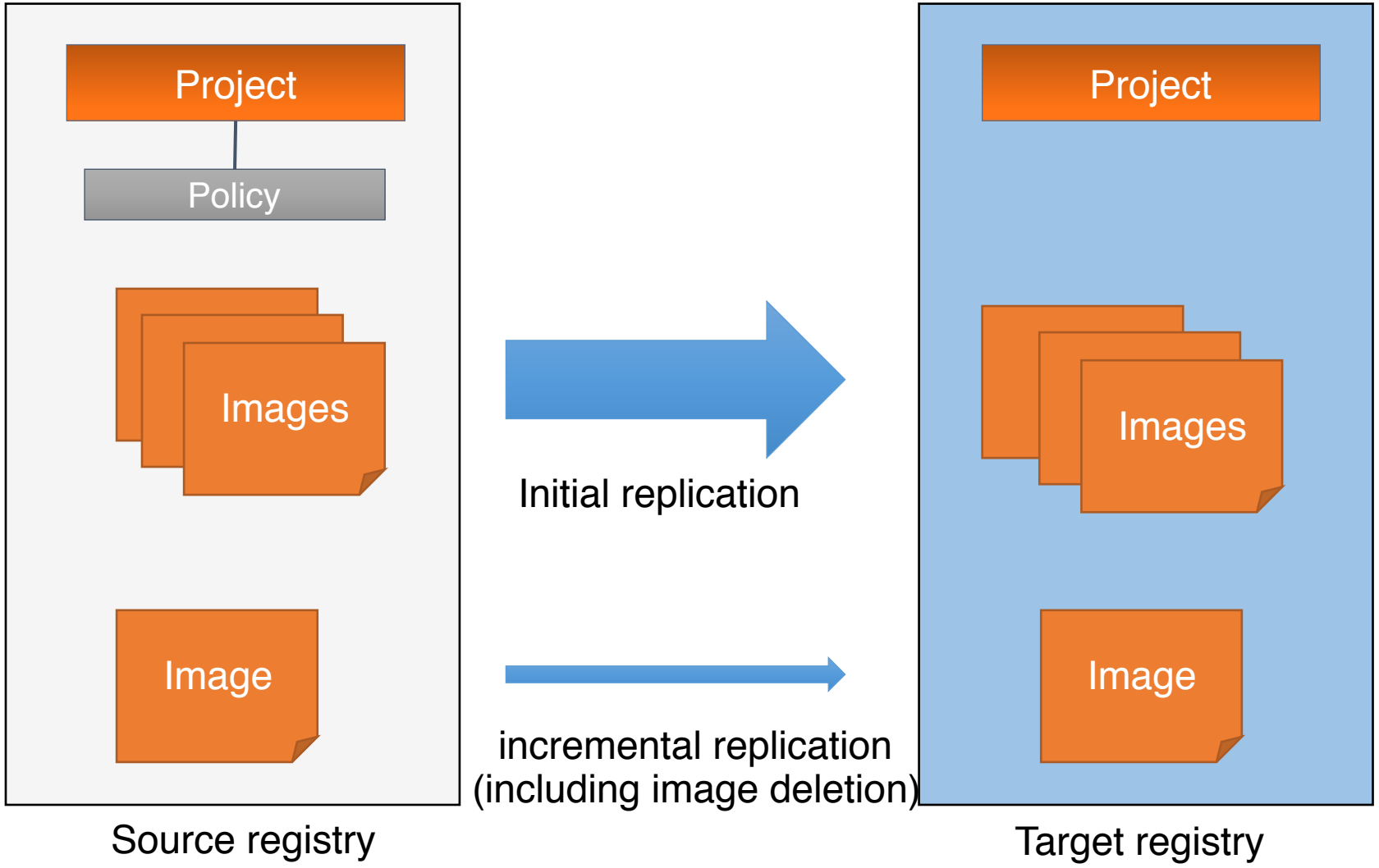


Image Replication (Synchronization)



Agenda

Consistency of Container Images

- Container images are used throughout the life cycle of software development
  - Dev
  - Test
  - Staging
  - Production
- Consistency must be maintained
  - Version control
  - Issue tracking
  - Troubleshooting
  - Auditing

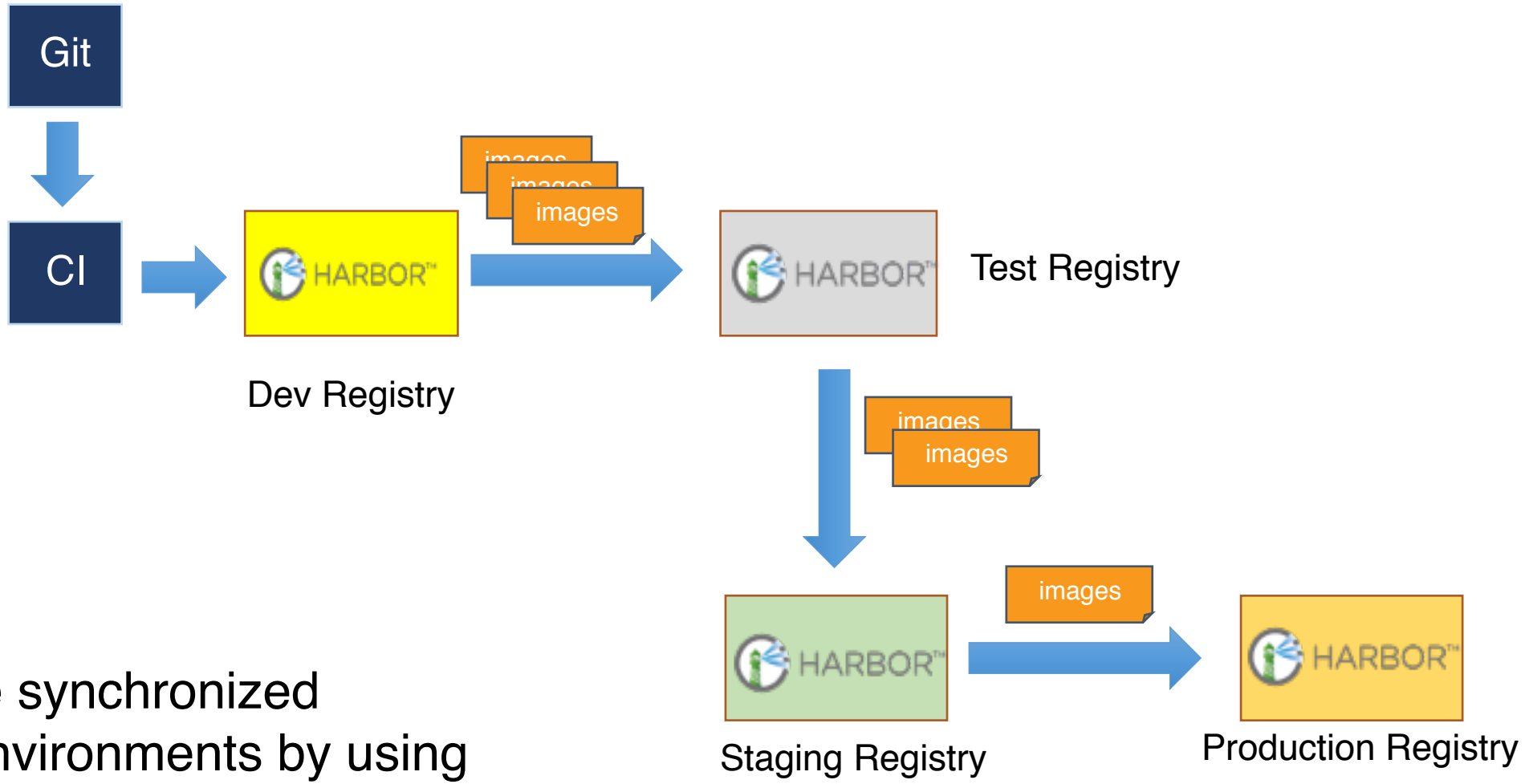
Same Dockerfile Always Builds Same Image?

Example:

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

- Base image `ubuntu:latest` could be changed between builds
- `ubuntu:16.04` could also be changed due to patching
- `apt-get` (`curl`, `wget`..) cannot guarantee always to install the same packages
- ADD depends on the build time environment to add files

Shipping Images in Binary Format for Consistency



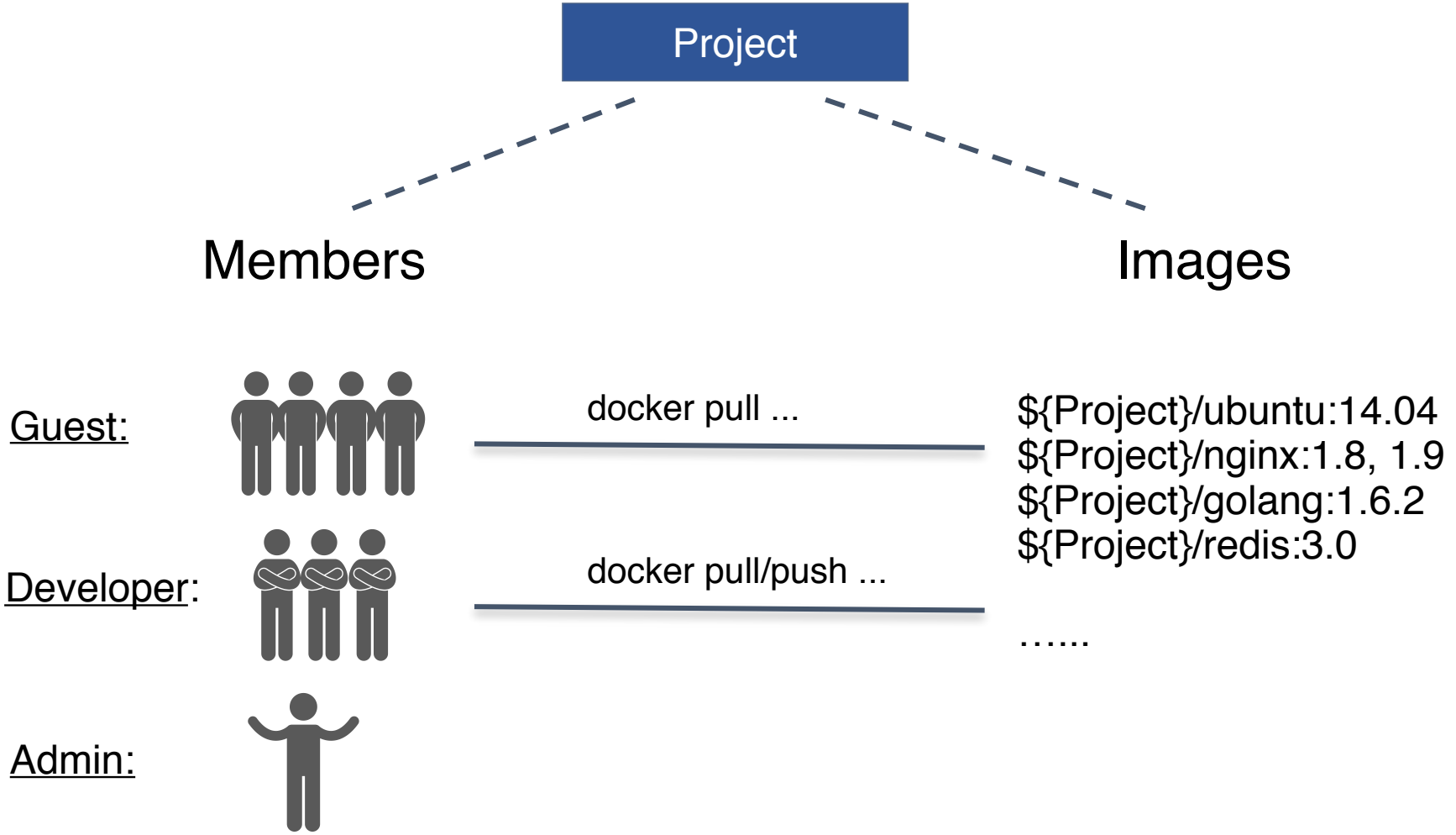
Images are synchronized between environments by using Harbor registry.

Agenda

Access Control to Images

- Organizations often keep images within their own organizations
  - Intellectual property stays in organization
  - Efficiency: LAN vs WAN
- People with different roles should have different access
  - Developer – Read/Write
  - Tester – Read Only
- Different rules should be enforced in different environments
  - Dev/test env – many people can access
  - Production – a limited number of people can access
- Can be integrated with internal user management system
  - LDAP/Active Directory

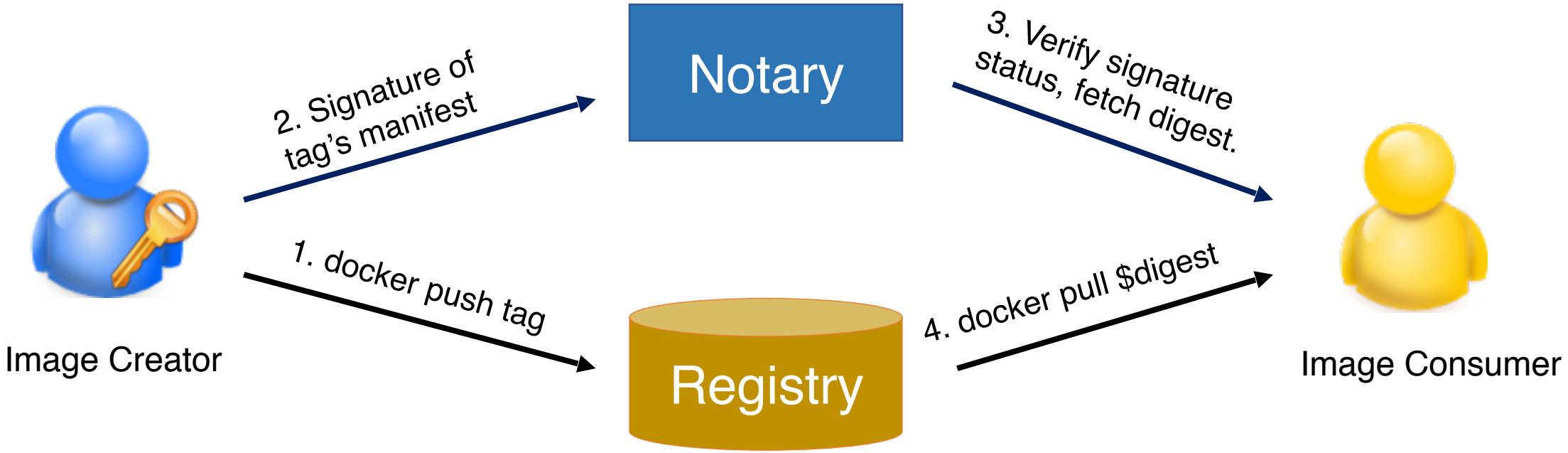
Example: Role Based Access Control in Harbor



Other Security Considerations

- Enable content trust by installing Notary service
  - Image is signed by publisher's private key during pushing
  - Image is pulled using digest
- Perform vulnerability scanning
  - Prevent images with vulnerabilities from being pulled
  - Regular scanning based on updated vulnerability database

Content Trust for Image Provenance

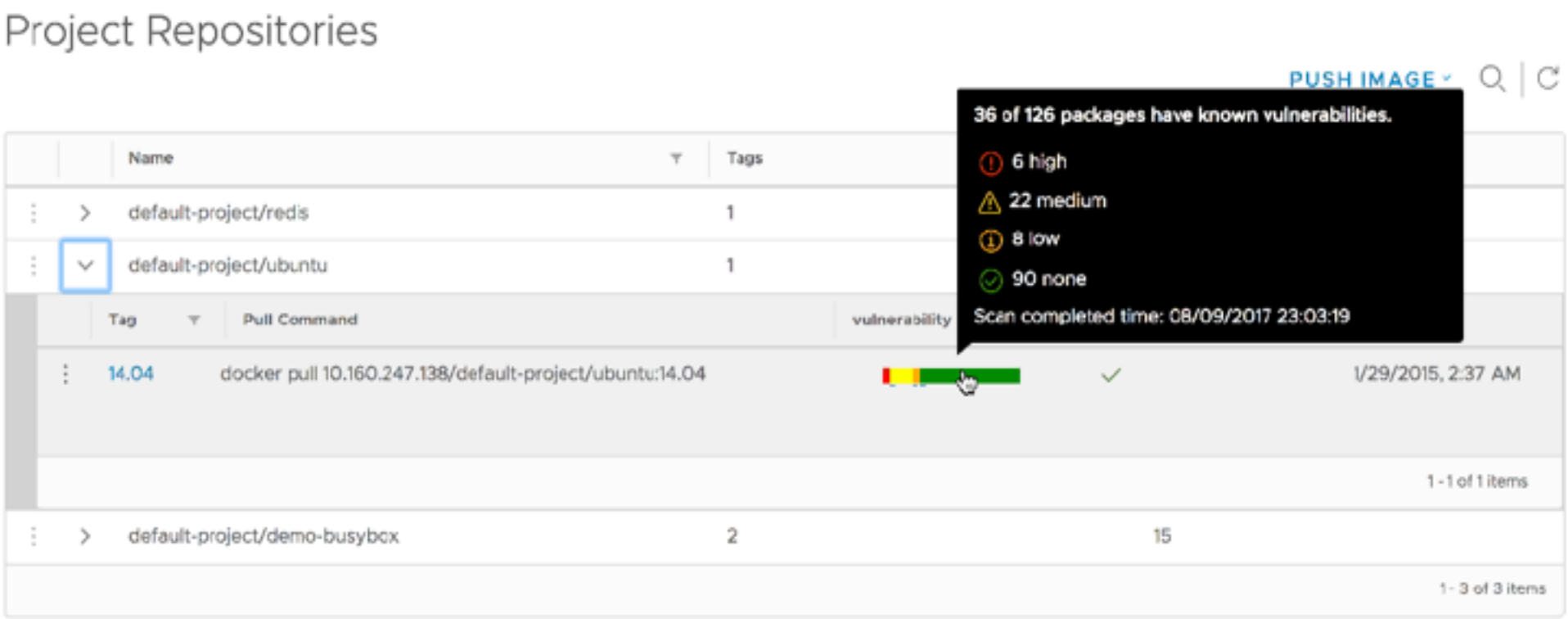


Vulnerability Scanning

- **Static analysis** of vulnerability by inspecting filesystem of container image and indexing features in database.
- **Rescanning** is needed only and only if new detectors are added.
- Update vulnerability data regularly
  - Debian Security Bug Tracker
  - Ubuntu CVE Tracker
  - Red Hat Security Data
  - Oracle Linux Security Data
  - Alpine SecDB

Image Vulnerability Scanning

- **Set vulnerability threshold**
- **Prevent images from being pulled** if they exceed threshold
- **Periodic scanning** based on updated vulnerability database

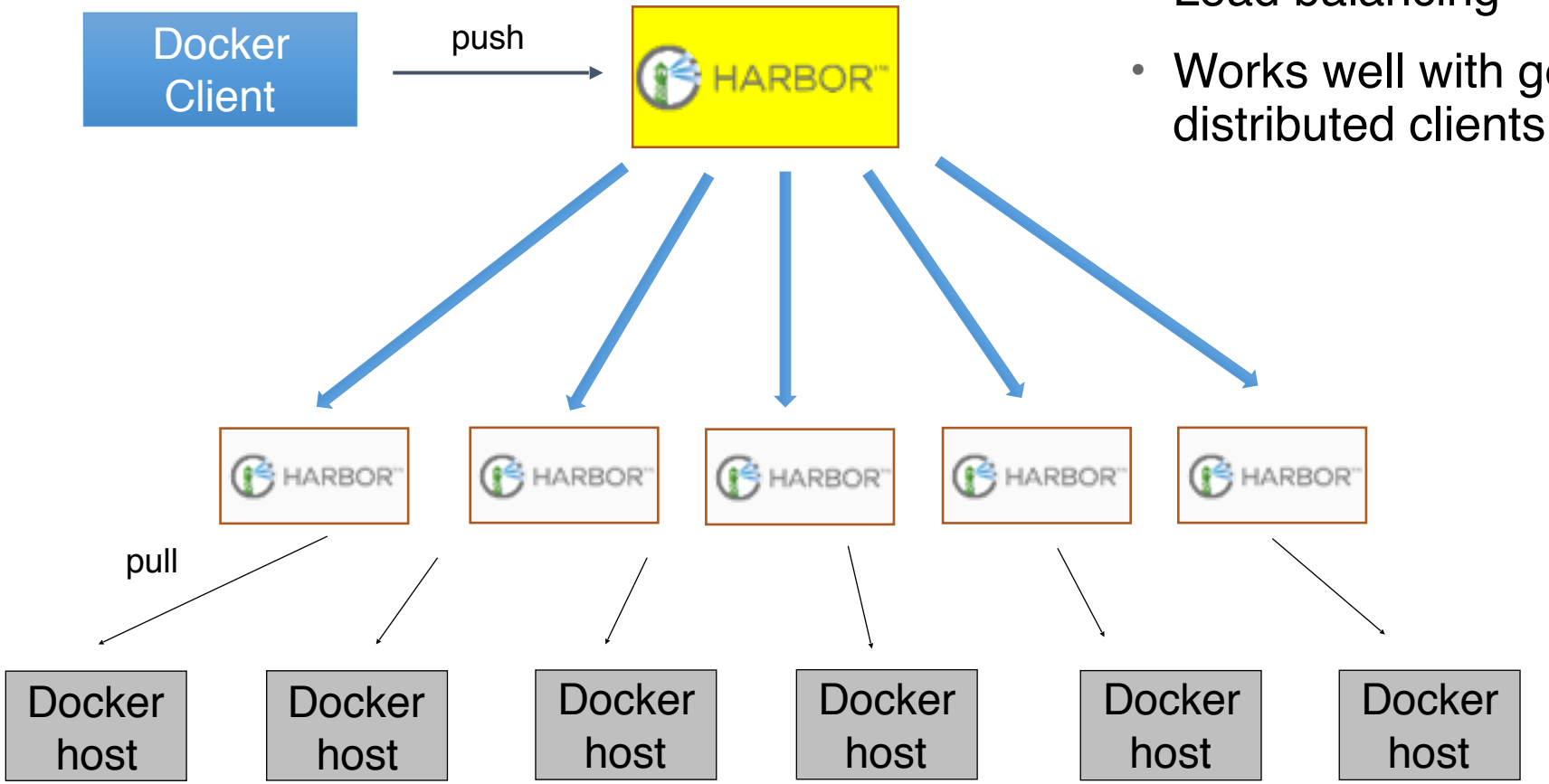


Agenda

Image Distribution

- Container images are usually distributed from a registry.
- Registry becomes the bottleneck for a large cluster of nodes
  - I/O
  - Network
- Scaling out an registry server
  - Multiple instances of registry sharing same storage
  - Multiple instances of independent registry sharing no storage

Image Distribution via Master-Slave Replication



- Load balancing
- Works well with geographically distributed clients

Master – Slave model

Agenda

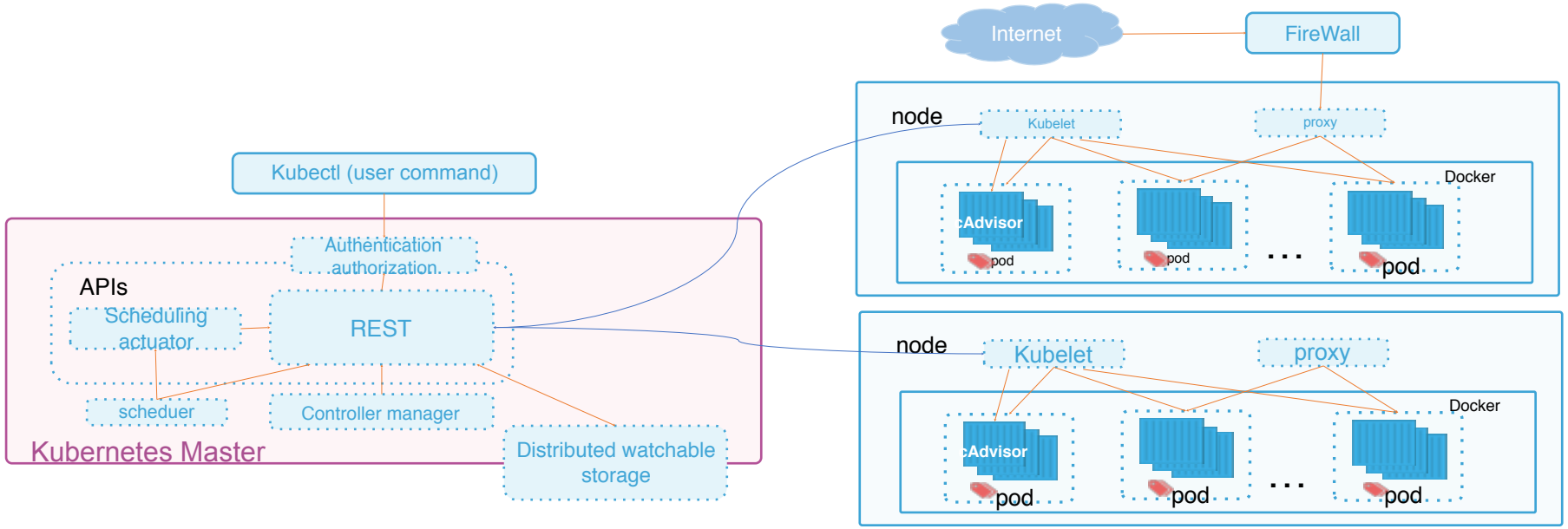
自我介绍

杜　宁

- 才云科技首席解决方案架构师
- Email：tony@caicloud.io
- Cell：18610255655

Harbor Integration with Kubernetes

- Harbor作为Kubernetes集群的镜像仓库

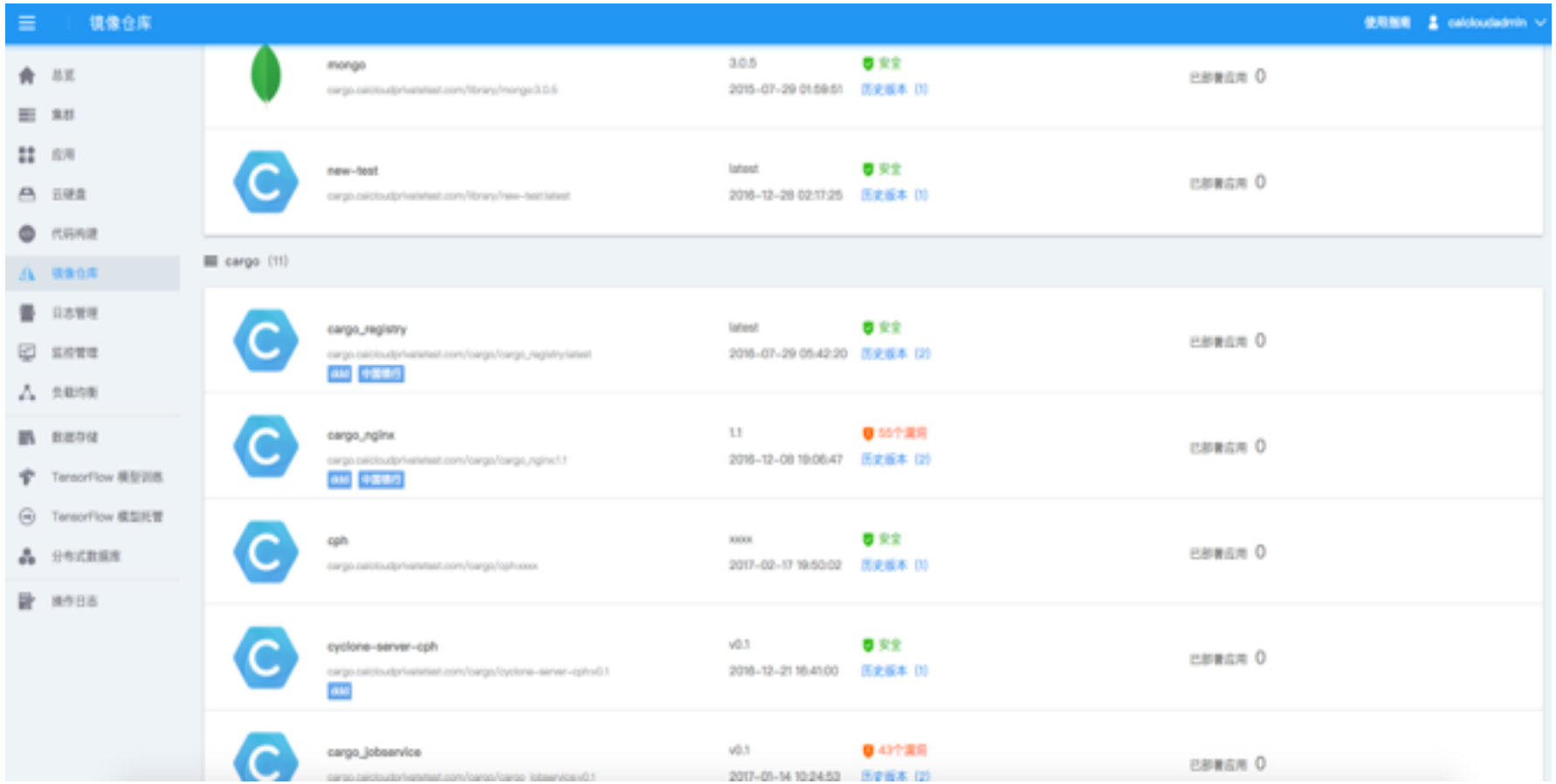


HARBOR™

主办：

Harbor Integration with Kubernetes

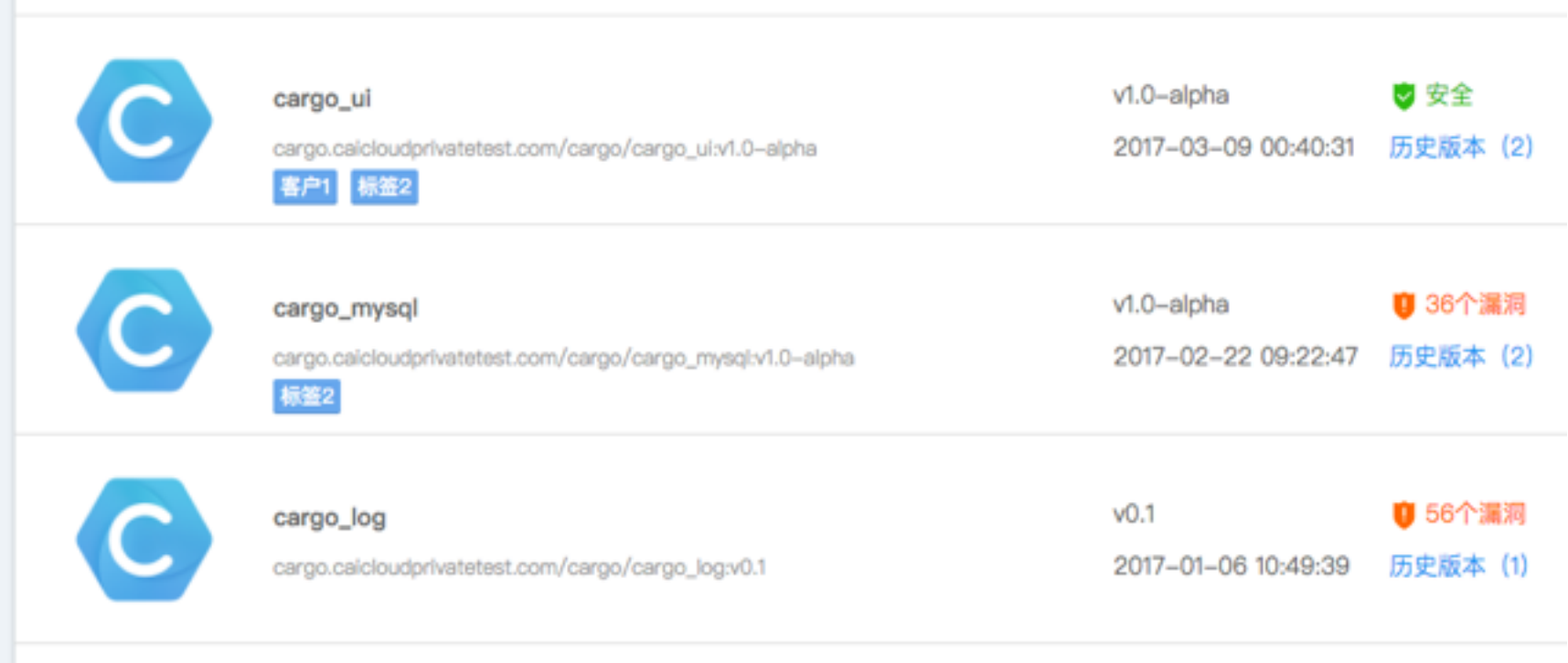
- 界面集成
- 租户
- 权限



主办：

Harbor Integration with Kubernetes

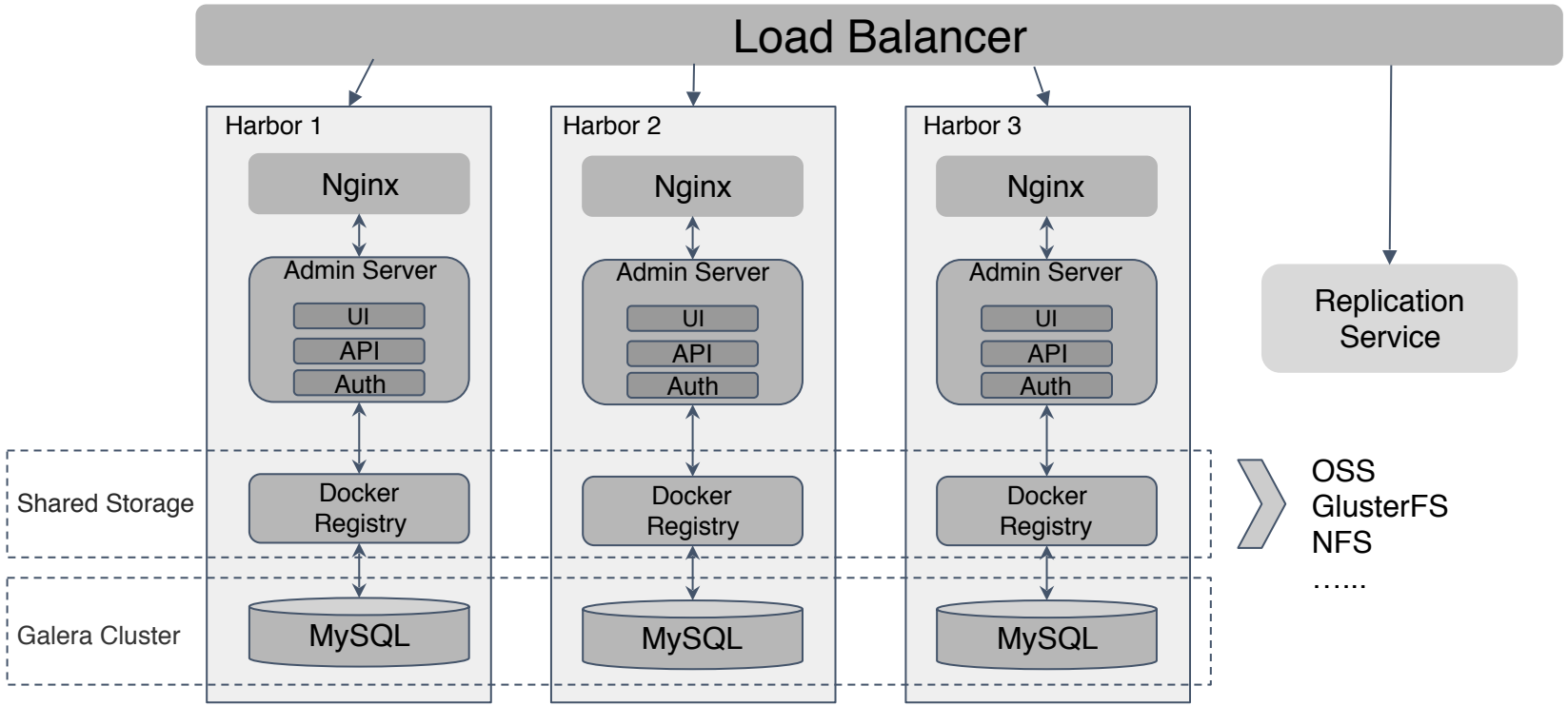
- 漏洞检测



主办：

Harbor Integration with Kubernetes

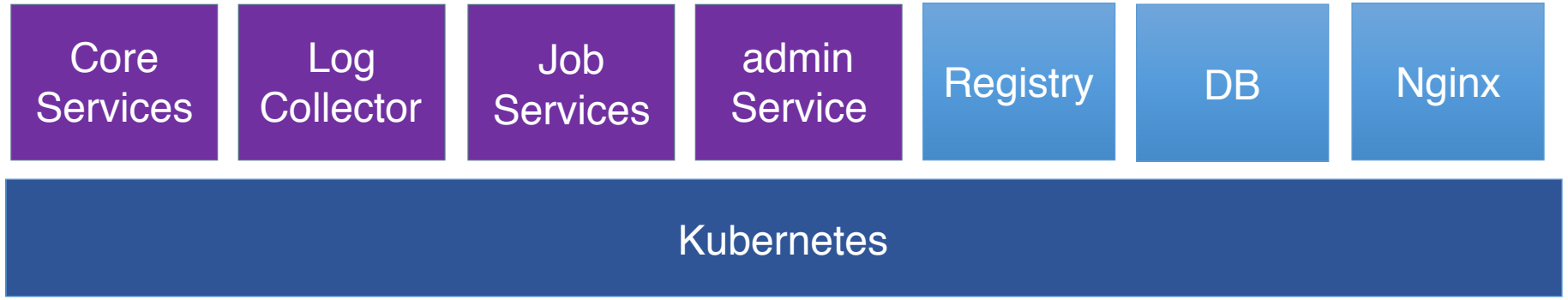
- 高可用性



主办：

Harbor Integration with Kubernetes

- 以Pod的形式部署到Kubernetes上



2017
China Kubernetes
End User Conference
kubernetes 中国用户大会

KEUC 2017

2017.10.15 / 中国 · 杭州

Harbor用户微信群

Thank you for your time

主办：

CLOUD NATIVE COMPUTING FOUNDATION

caicloud 才云

中国社区