采用开源Harbor Registry实现高效安全的容器镜像运维

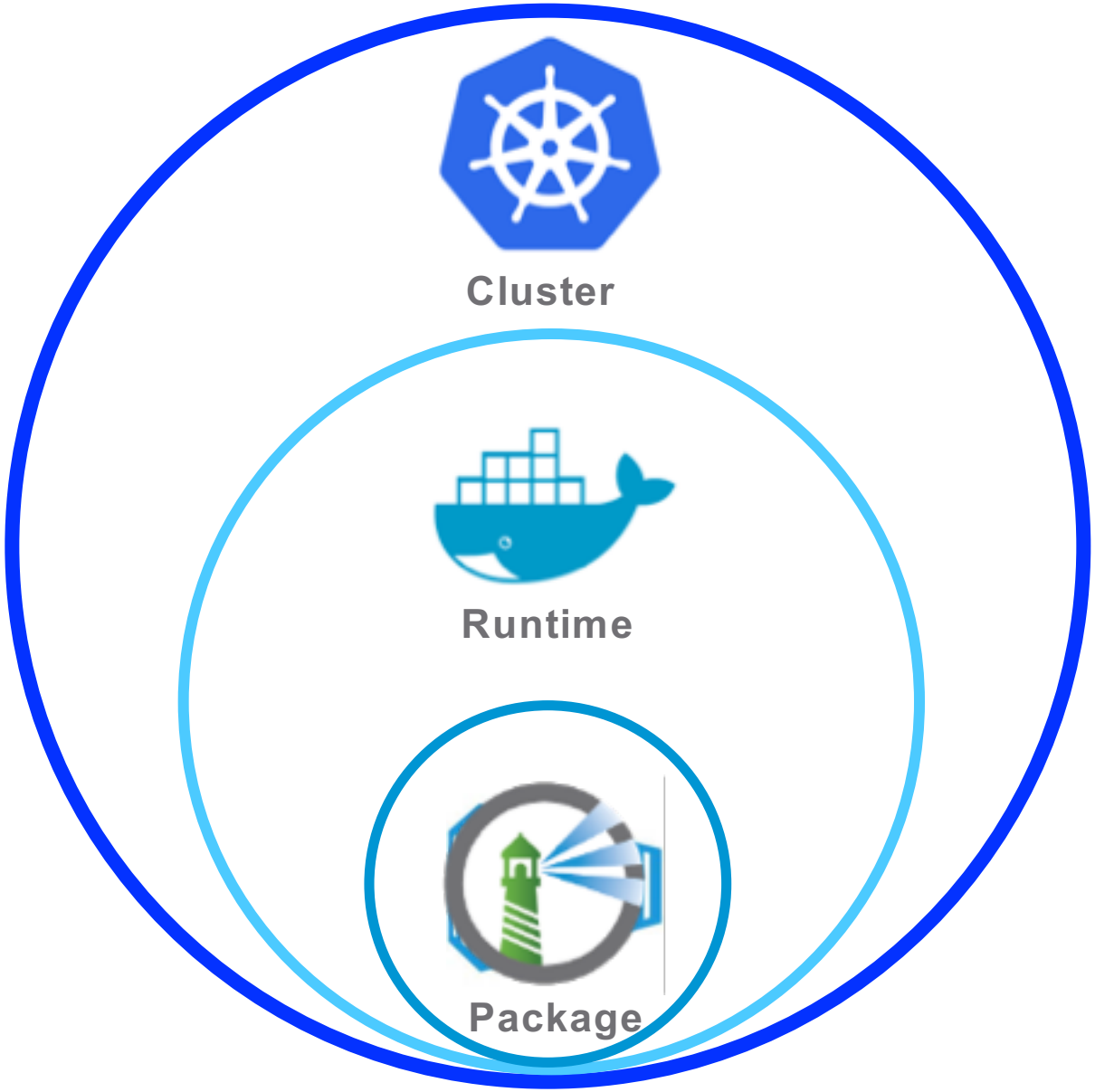
邹佳
VMware中国研发中心资深研发工程师

vmware

自我介绍

- VMware中国研发中心云原生应用部门资深研发工程师
- Harbor开源企业级容器Registry项目核心研发之一
- 曾在HPE,IBM等公司从事云计算，DevOps以及云原生应用等相关技术的研发工作
- 拥有多项全球专利
- PMP

开场



vmware

议程

1 镜像运维

2 开源企业级镜像仓库-Harbor

3 集成Harbor

4 总结

议程

1 **镜像运维**

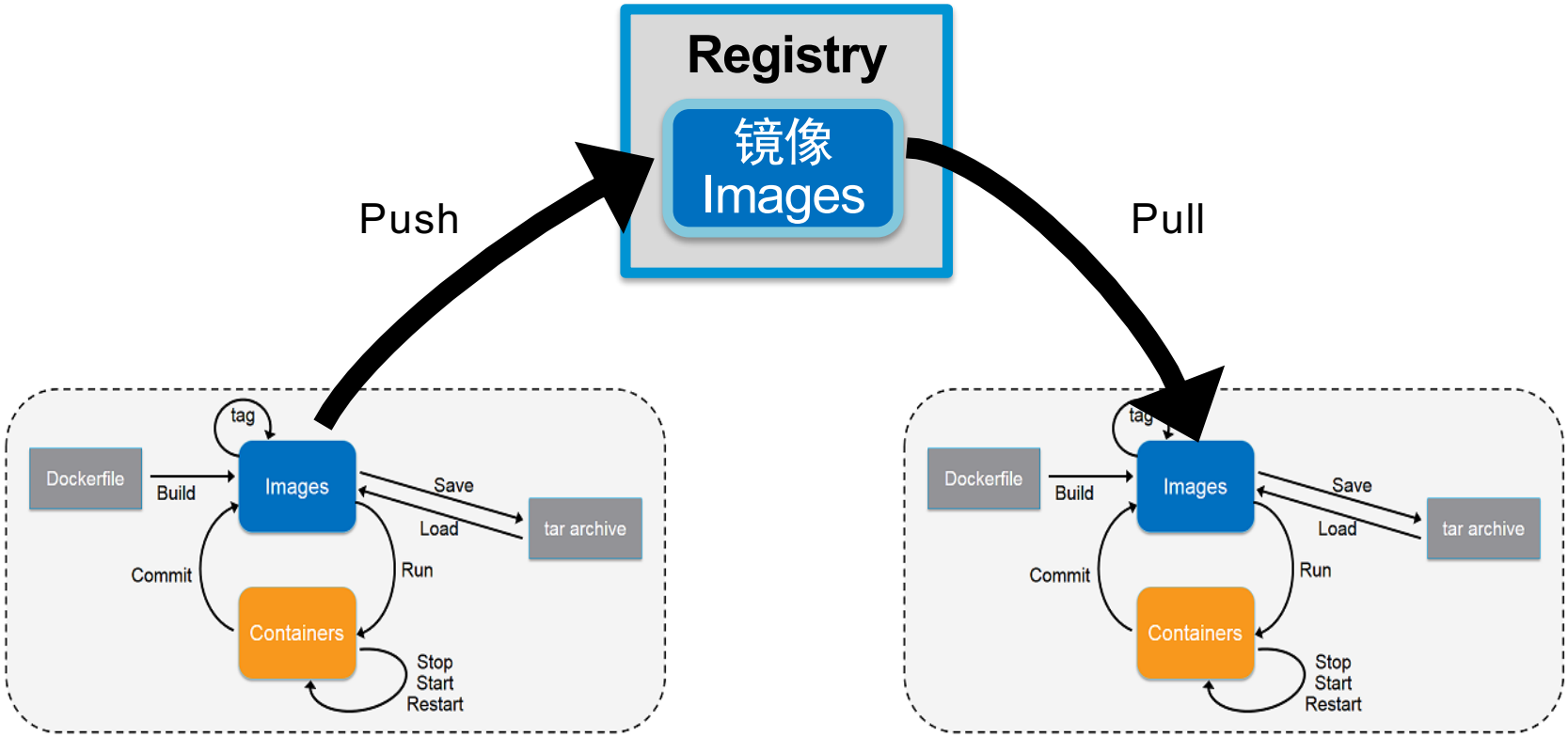
2 开源企业级镜像仓库-Harbor

3 集成Harbor

4 总结

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



一致性：同一个 Dockerfile 始终生成同一个镜像?

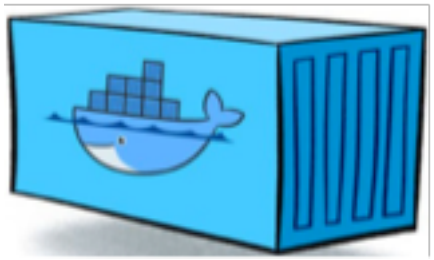
例子:

```
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

镜像一致性

- 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



二进制格式

安全：访问控制

- 企业用户通常把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
- 可与已有内部用户系统集成
  - LDAP/Active Directory

其它安全考量

- **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）

- **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

议程

1 镜像运维

2 **开源企业级镜像仓库-Harbor**

3 集成Harbor

4 总结

Harbor开源项目

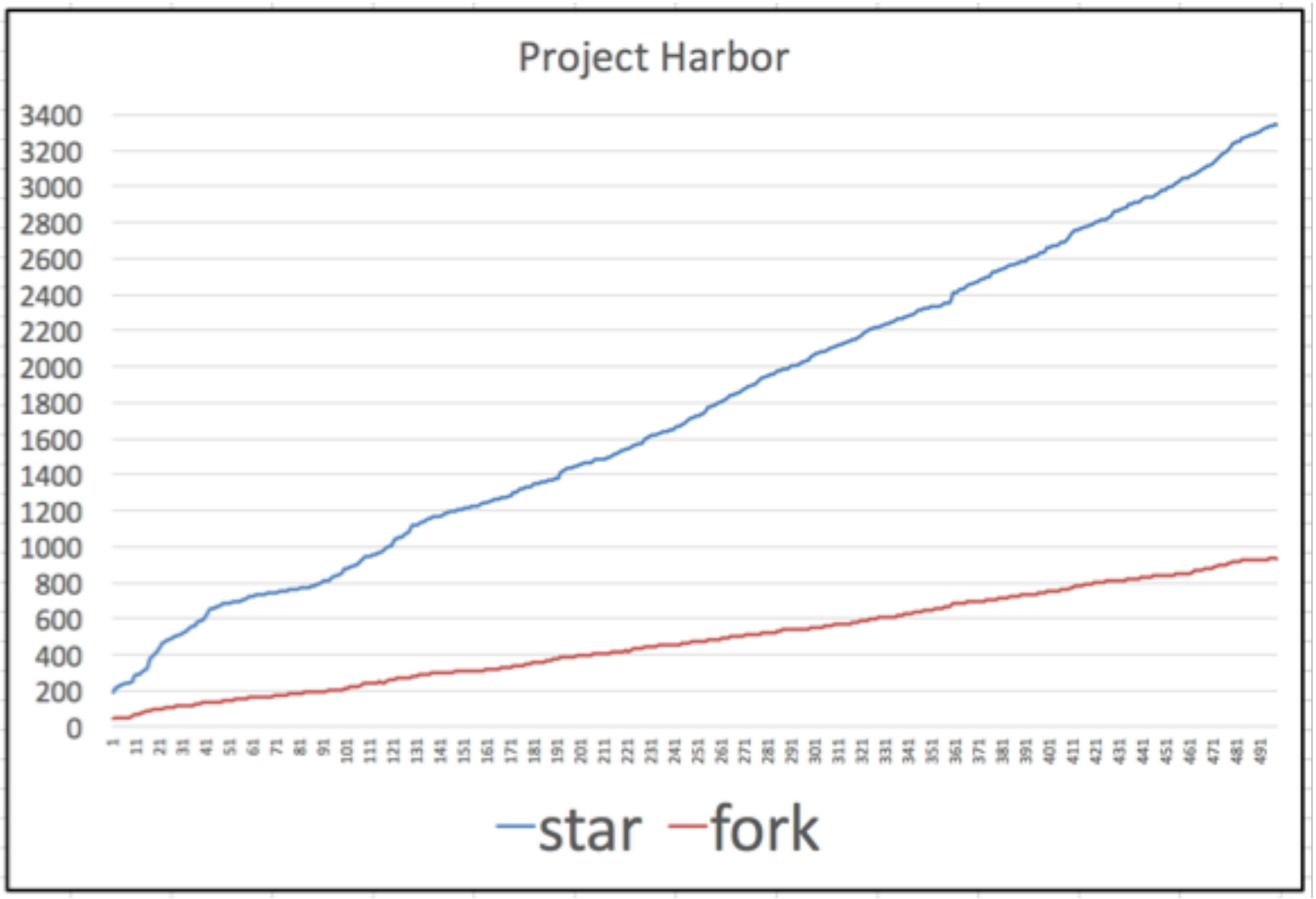
- 开源企业级容器镜像仓库
- 由 VMware 中国团队设计和开发
- 集成到多个企业级产品中:VIC和PKS
- Apache 2 使用许可
- https://github.com/vmware/harbor/

HARBOR™

用户和开发者情况

vmware®

Harbor社区的增长



vmware

Harbor部分用户


caicloud 才云
RANCHER
数人云
shurenyun.com
品高云
BingoCloud
时速云
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
EDUTAINMENT
奥鹏教育
BOER
博耳智能
BOER SMART
云星数据
BEYONDSOFT
beyond your expectations

主要特性

访问控制

基于角色的访问控制（RBAC）
AD/LDAP 用户身份集成
直接添加LDAP用户为成员

远程复制

支持过滤器
支持**定时**,即时和手动策略

漏洞扫描

多种漏洞扫描策略
配置策略阻止漏洞镜像分发

内容信任

签名镜像
配置策略阻止未签名镜像分发

审计和日志

记录操作日志以便审计

Restful API

完善的API以支持集成

主要特性

图形化管理界面

基于开源UI库Clarity构建
提供完备的镜像管理运维能力

增加批处理操作
为镜像库添加描述信息

高可用性

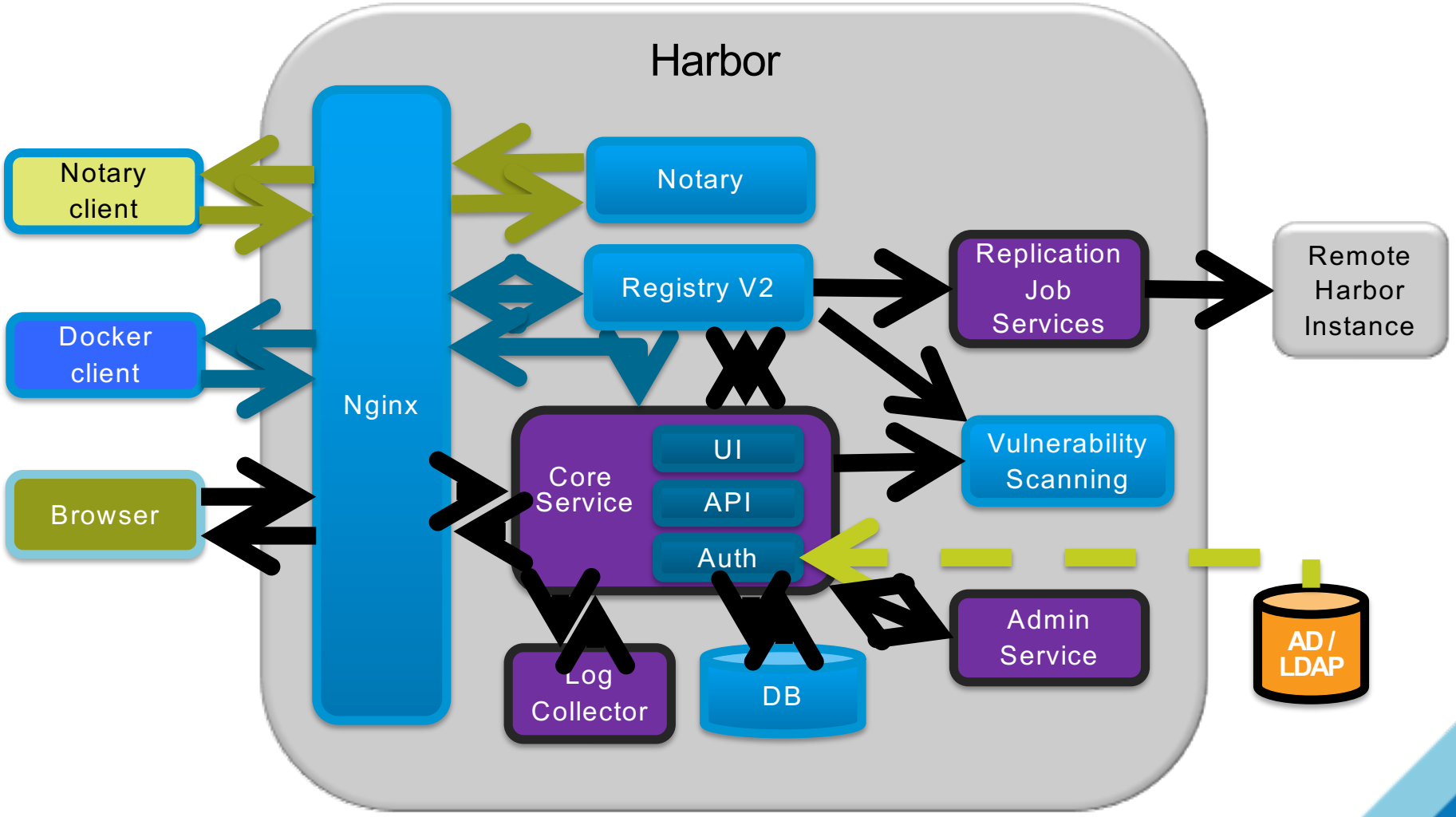
高可用性支持

ova@vSphere

ova的虚拟机，直接部署在vSphere上

vmware

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

基于角色的访问控制

项目 Project

< 项目

library

镜像仓库 成员 日志 复制 配置管理

+ 新建成员 设置角色 移除成员

姓名	角色
admin@harbor.local	开发人员
wangyan01	访客

0 条记录

Admin:

镜像漏洞扫描

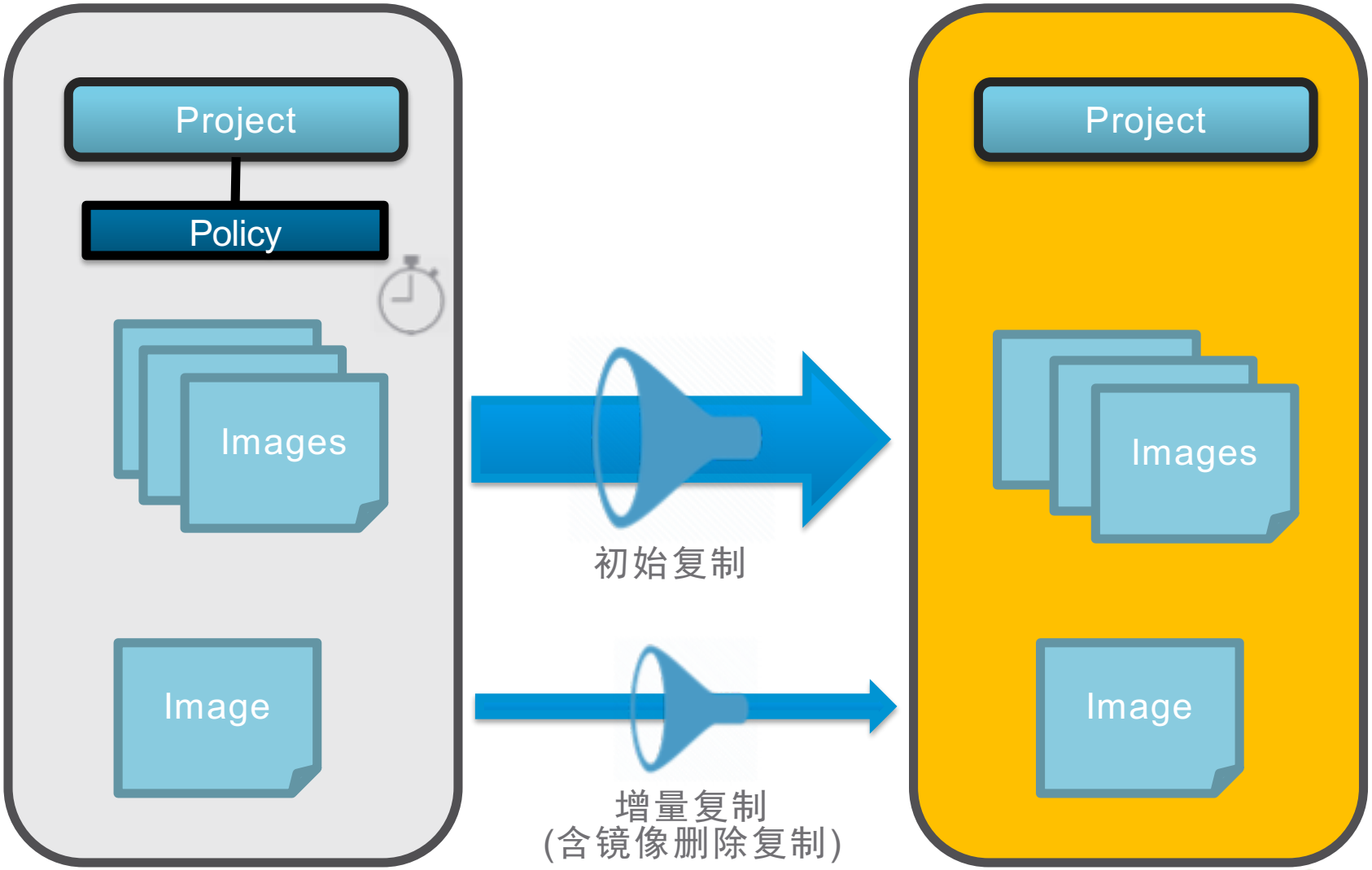
- 漏洞扫描是对镜像的文件做静态分析 (Clair)
- 漏洞数据来源
  - Debian Security Bug Tracker
  - Ubuntu CVE Tracker
  - Red Hat Security Data
  - Oracle Linux Security Data
  - Alpine SecDB

控制策略

- 设置自动扫描：上传即扫描
- 设置漏洞级别阈值；超过阈值的镜像无法下载
- 设置内容信任

vmware

镜像复制


Project
Policy
Images
Image
初始复制
增量复制
(含镜像删除复制)
Project
Images
Image

复制策略管理

< 复制管理

新建规则

名称*

my rule

描述

Just a test case

源 项目*

源镜像过滤器

repository

test*

tag

1.*

目标 *

khans3: http://10.112.122.203

+ 新增

userName:

password:

触发模式

手动

删除本地镜像时同时也删除远程的镜像。

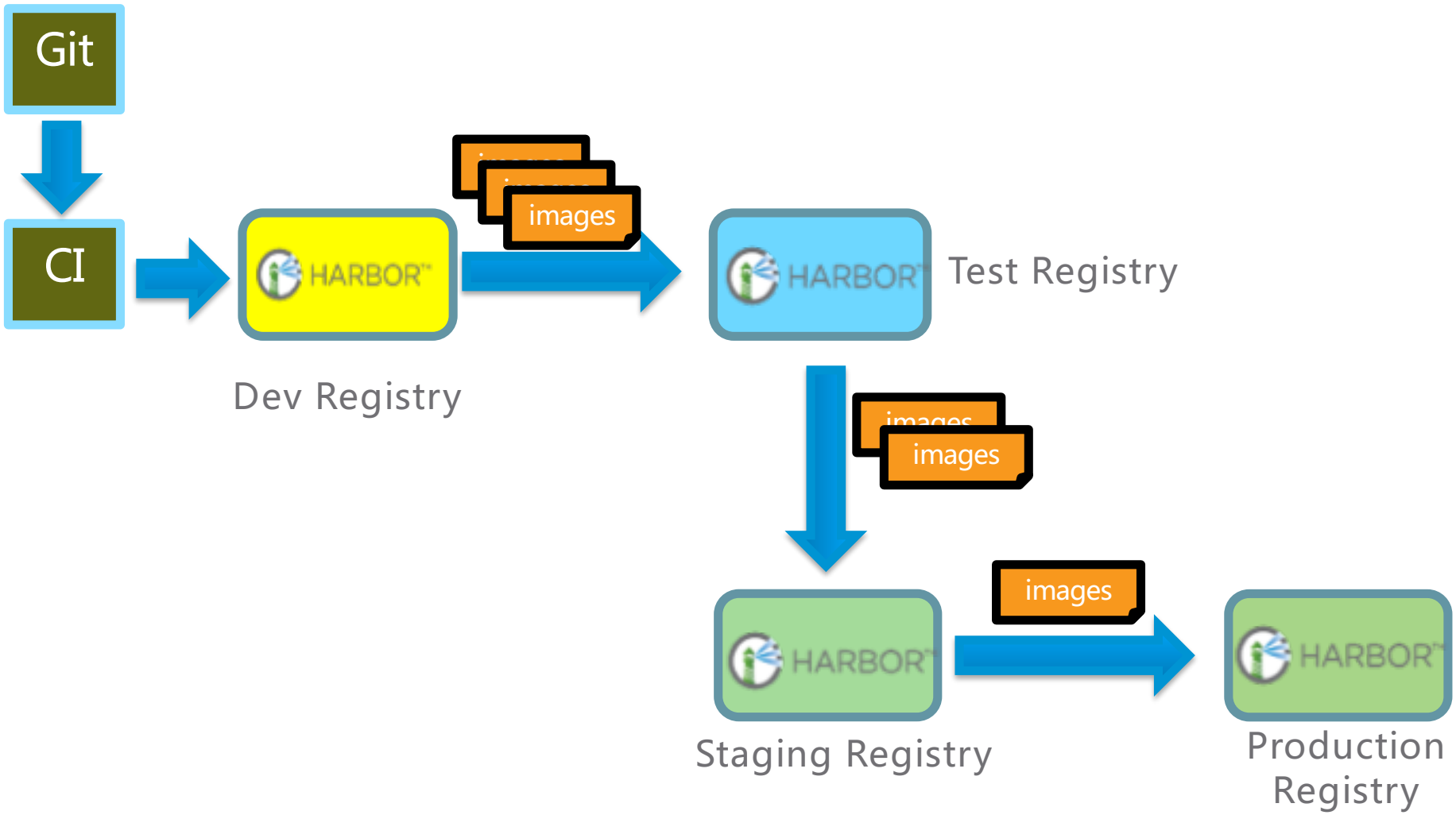
立即复制现有的镜像。

保存

取消

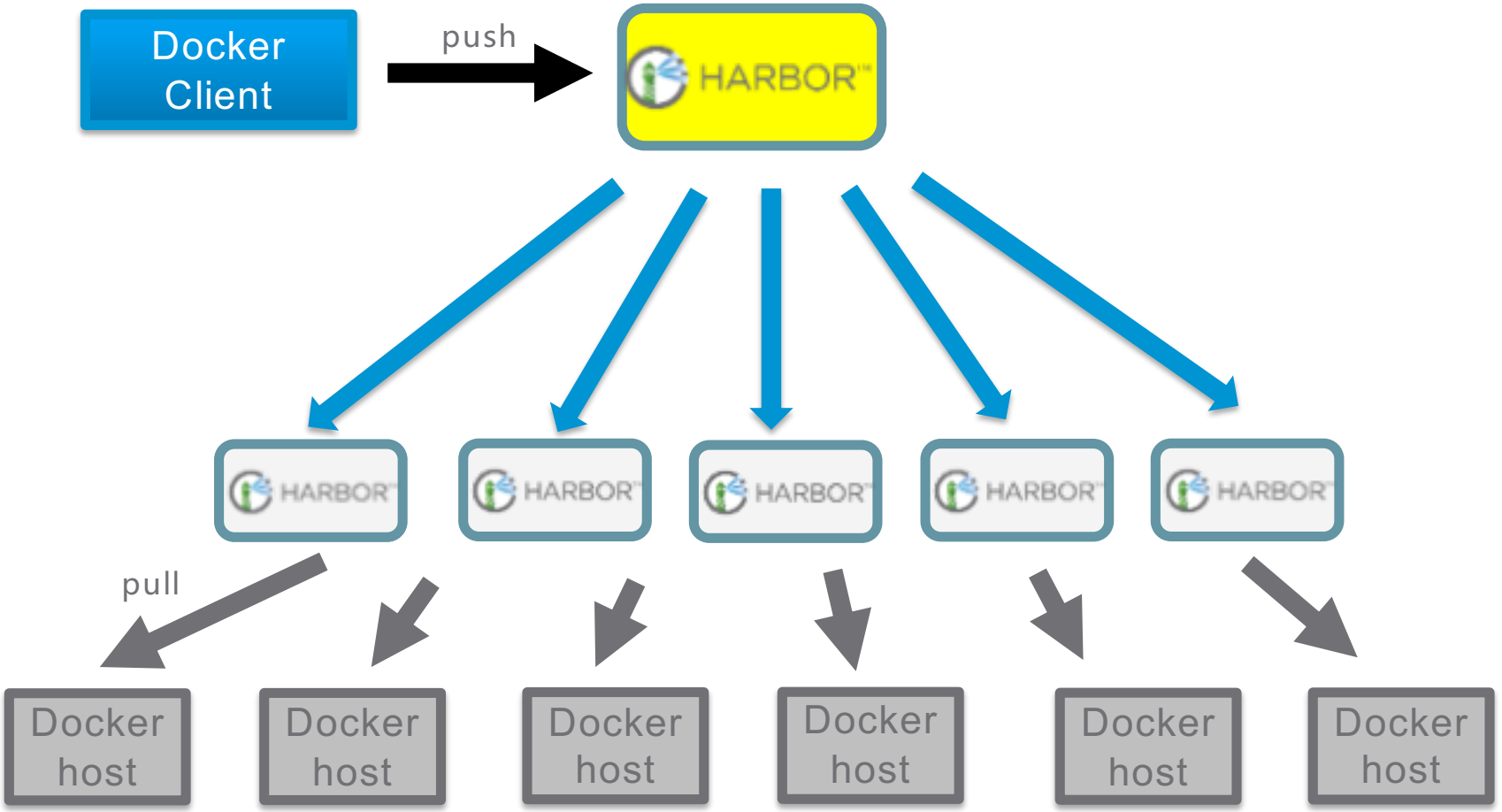
vmware

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

复制技术在镜像分发中应用



Master – Slave 模式

议程

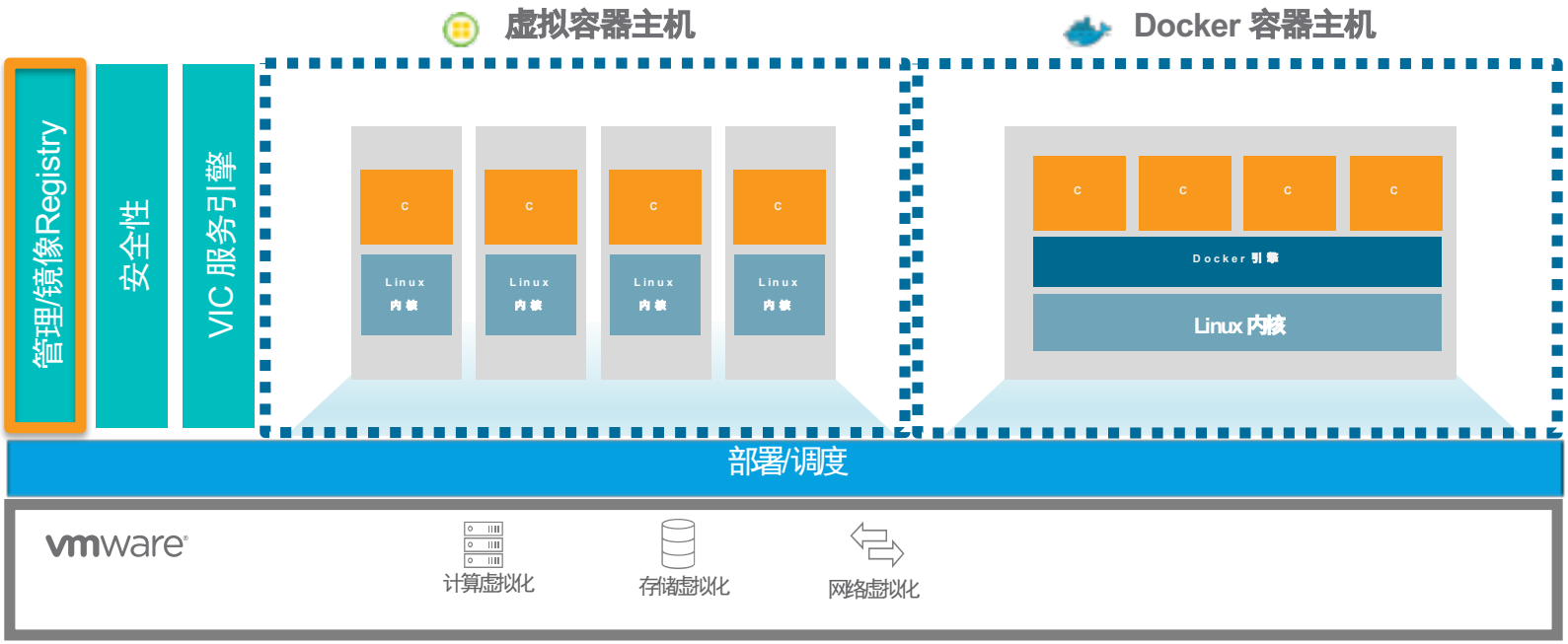
1 镜像运维

2 开源企业级镜像仓库-Harbor

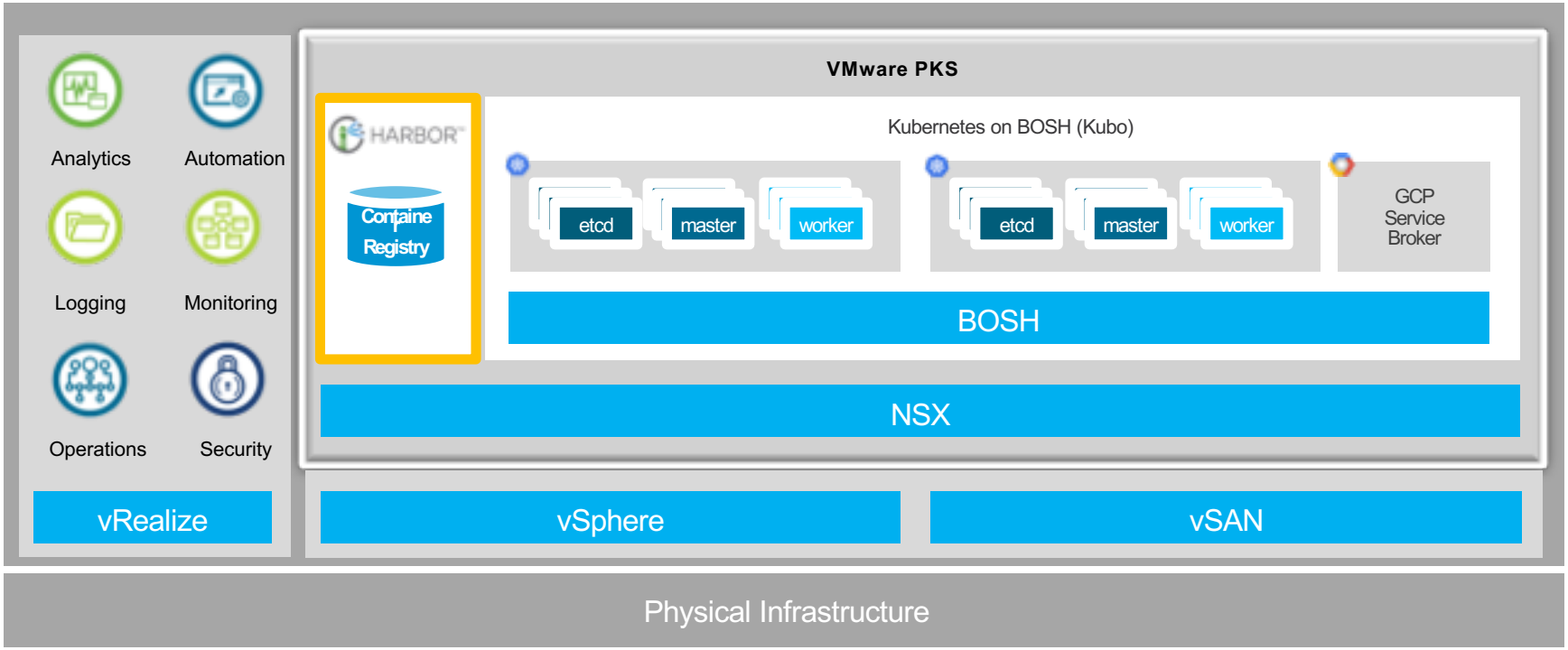
3 **集成Harbor**

4 总结

Harbor与VIC


虚拟容器主机
Docker 容器主机
管理/镜像Registry
安全性
VIC 服务引擎
C
Linux 内核
Docker 引擎
Linux 内核
部署/调度
vmware
计算虚拟化
存储虚拟化
网络虚拟化

Harbor与Kubernetes



vmware

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

网站：https://github.com/vmware/harbor

Twitter: @Project_harbor

Email组：（加入方式参见GitHub）

harbor-users@googlegroups.com
harbor-dev@googlegroups.com

云原生沙龙现场群