CLOUD NATIVE COMPUTING FOUNDATION

Project Harbor Introduction

Open source trusted cloud native registry

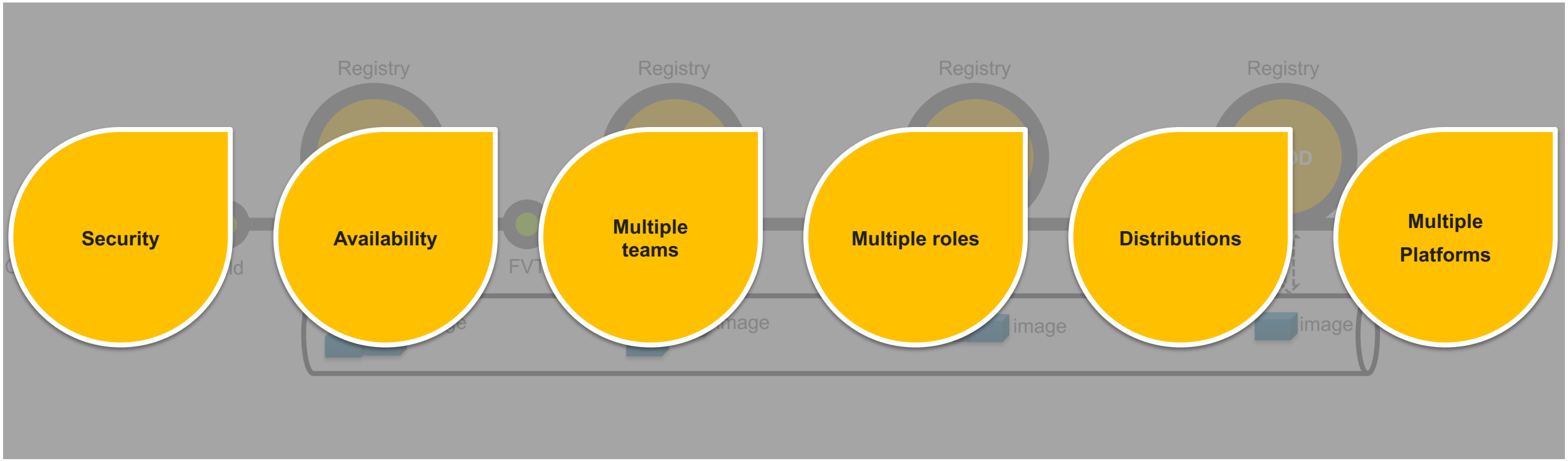
Henry Zhang, Chief Architect, VMware R&D China

Steven Zou, Staff Engineer, VMware R&D China

Nov. 2018

vmware

Image Management through Pipeline



开源的可信云原生仓库项目

goharbor.io

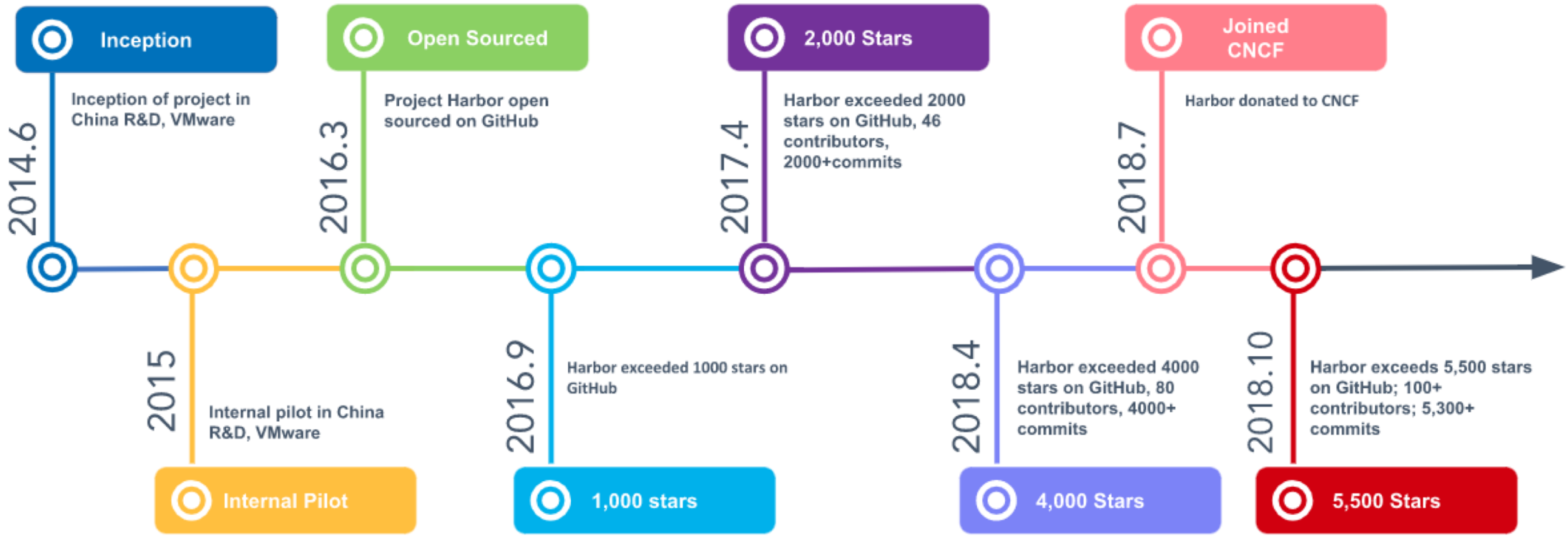
由 VMware 中国研发团队发起，社区共同维护

集成到多个企业级产品中:VIC和PKS

Apache 2.0 使用许可

GitHub Repo: https://github.com/goharbor/harbor/

Harbor项目简史



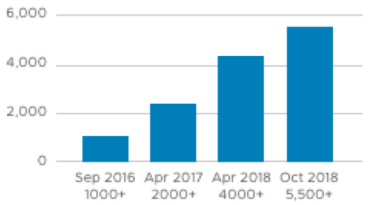
未来更多集成方向




Harbor社区概况

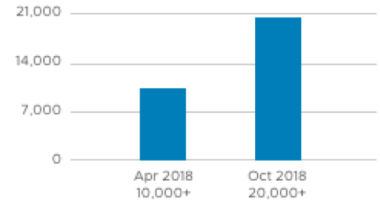
Stars

5,500+



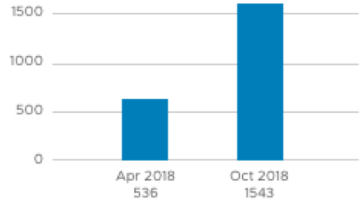
Downloads

20,000+



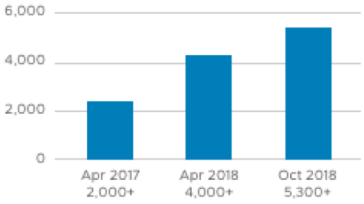
Forks

1,500+



Commits

5,300+

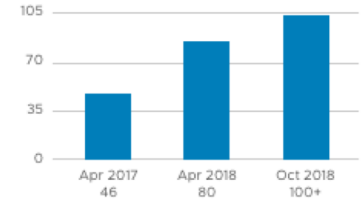


Users

1000+

Contributors

100+

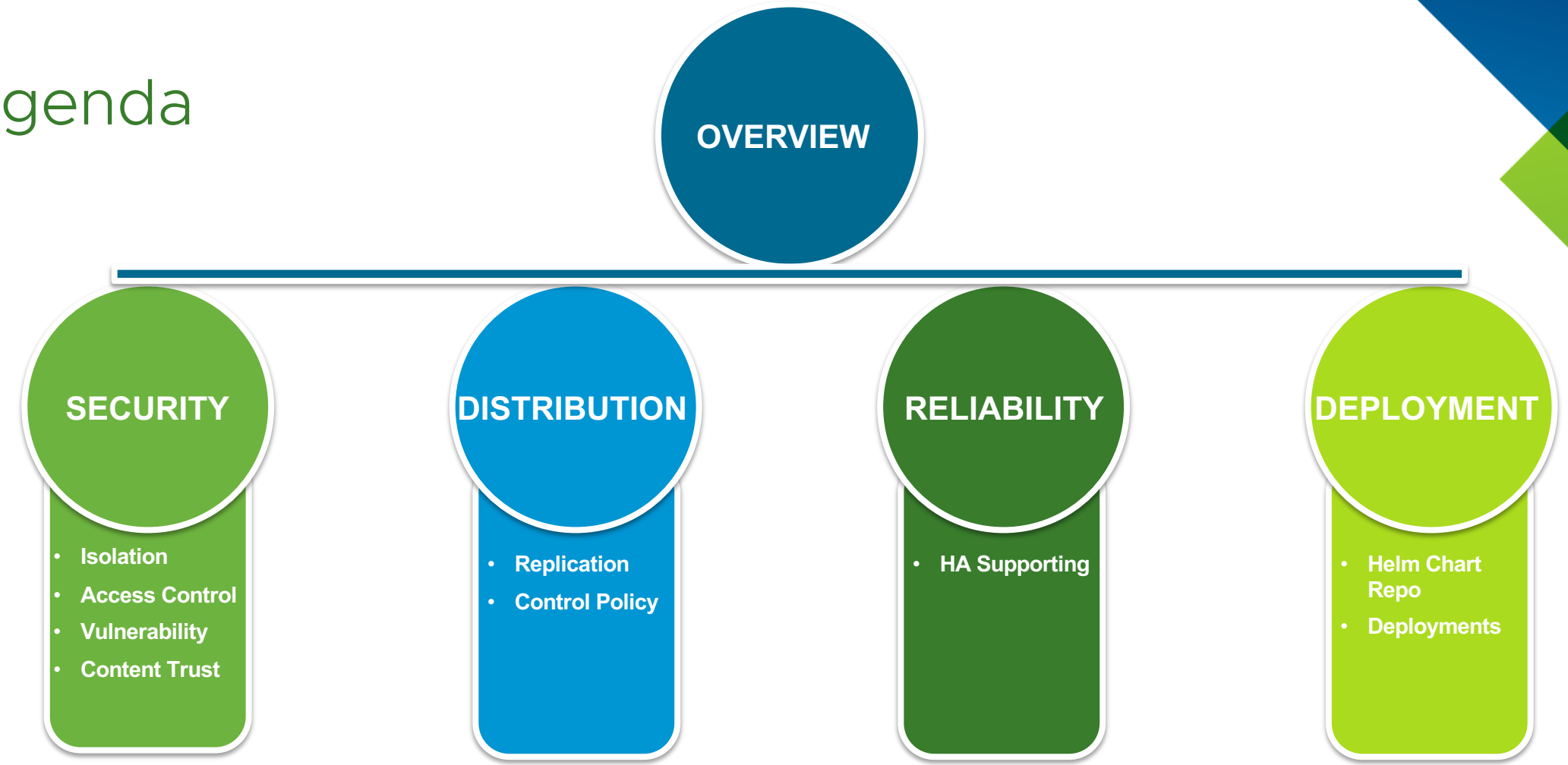


vmware

Harbor部分用户

vmware

Agenda


OVERVIEW
SECURITY
Isolation
Access Control
Vulnerability
Content Trust
DISTRIBUTION
Replication
Control Policy
RELIABILITY
HA Supporting
DEPLOYMENT
Helm Chart Repo
Deployments

OVERVIEW

Main Features

Architecture

主要特性

GUI支持

基于开源Clarity构建
完备镜像运管能力批处理操作支持

Restful API

完善的API支持集成
Swagger API 文档

远程复制

多种过滤器支持
定时,即时和手动触发

访问控制

基于角色的访问控制
AD/LDAP 用户集成

审计日志

操作日志记录以审计

分发控制

基于内容信任
基于漏洞扫描
基于RBAC

主要特性（续）

漏洞扫描

多种漏洞扫描策略
详尽的漏洞扫描报告

内容信任

数字签名镜像

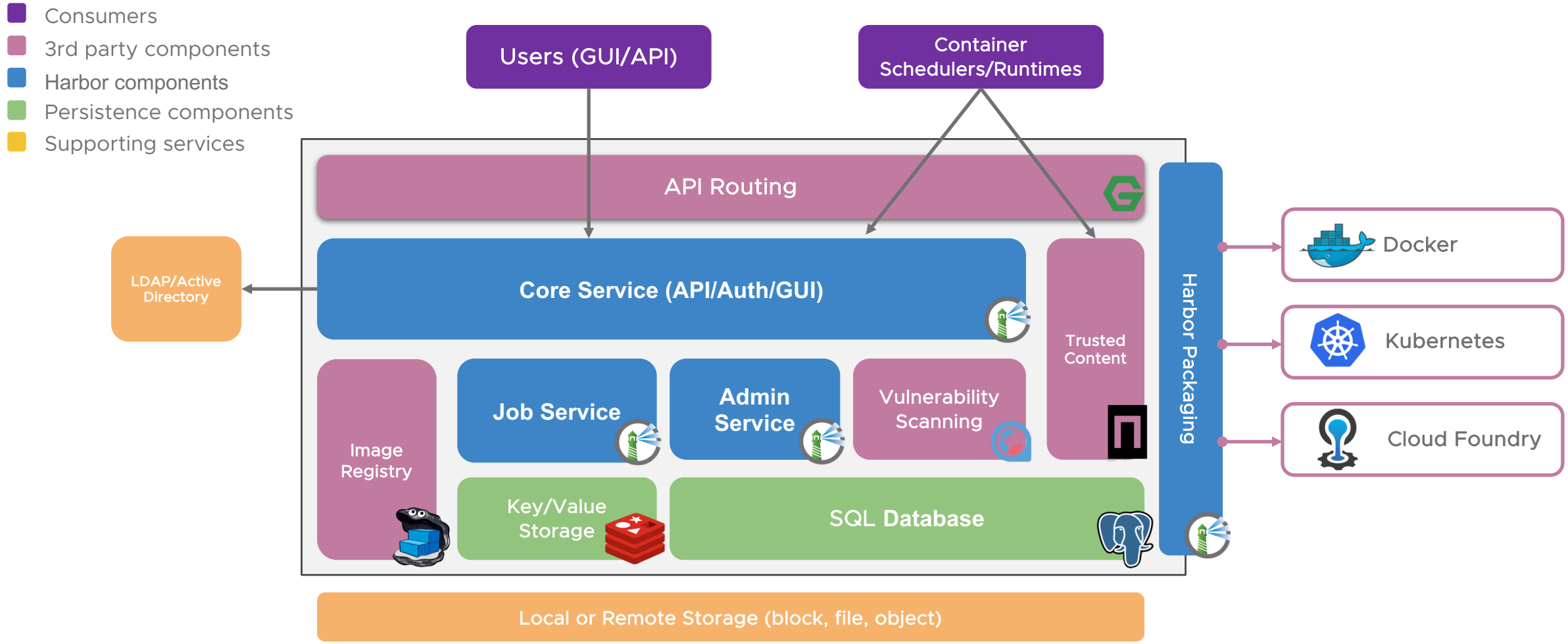
HA高可用

高可用性支持

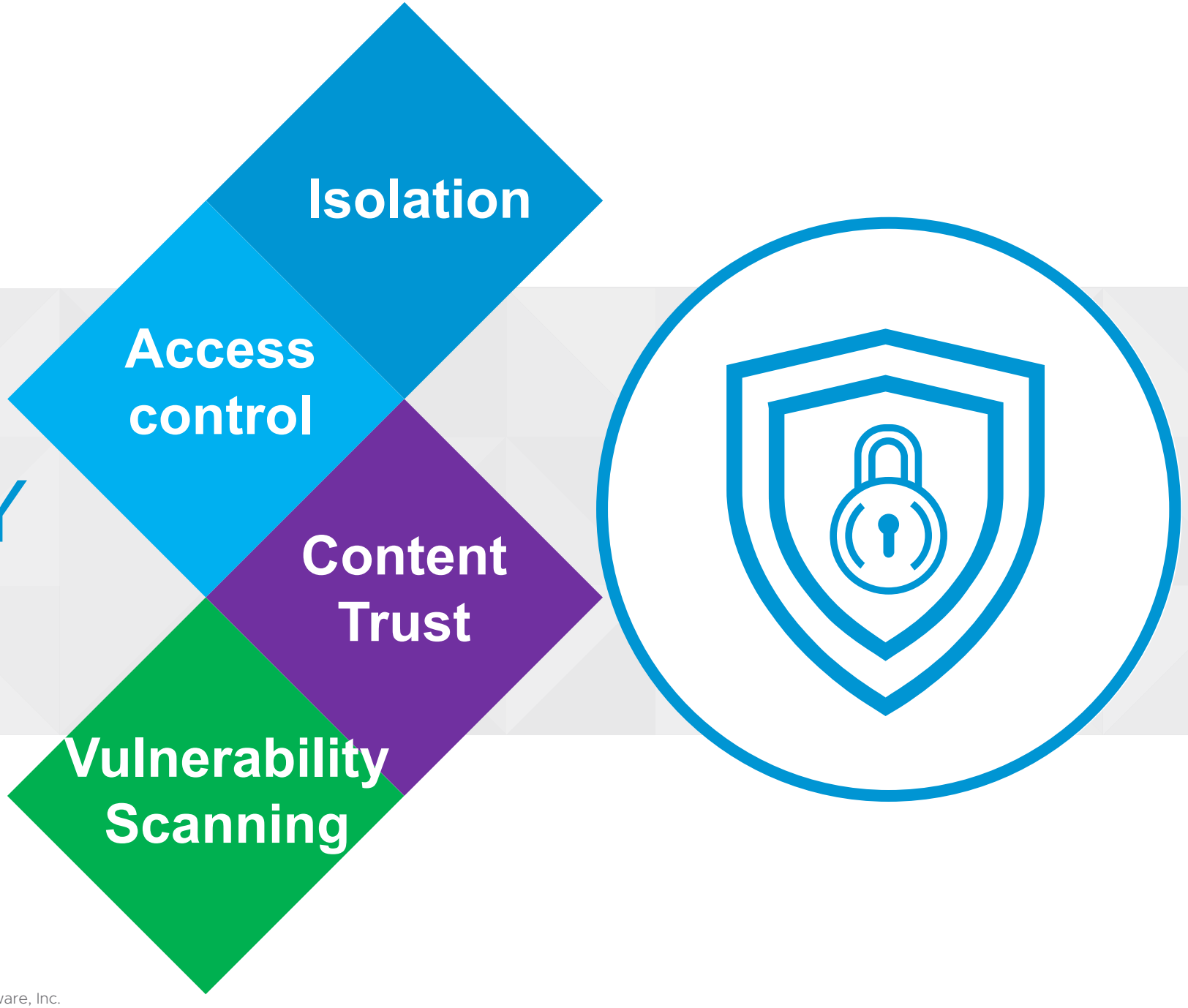
Helm Chart支持

Helm Chart仓库
与镜像相同的管理机制和体验

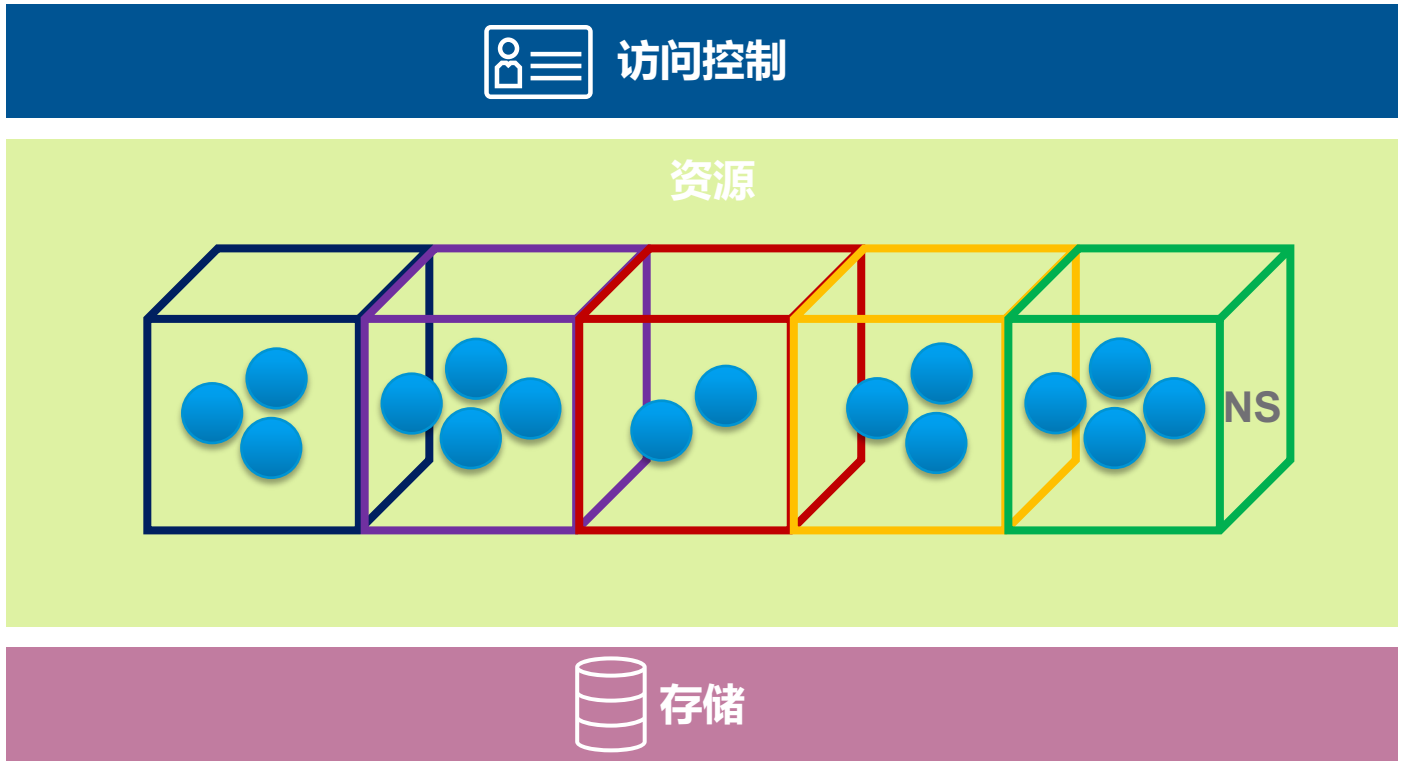
Harbor架构


Consumers
3rd party components
Harbor components
Persistence components
Supporting services
Users (GUI/API)
Container Schedulers/Runtimes
API Routing
LDAP/Active Directory
Core Service (API/Auth/GUI)
Trusted Content
Harbor Packaging
Image Registry
Job Service
Admin Service
Vulnerability Scanning
Key/Value Storage
SQL Database
Docker
Kubernetes
Cloud Foundry
Local or Remote Storage (block, file, object)

SECURITY


Isolation
Access control
Content Trust
Vulnerability Scanning

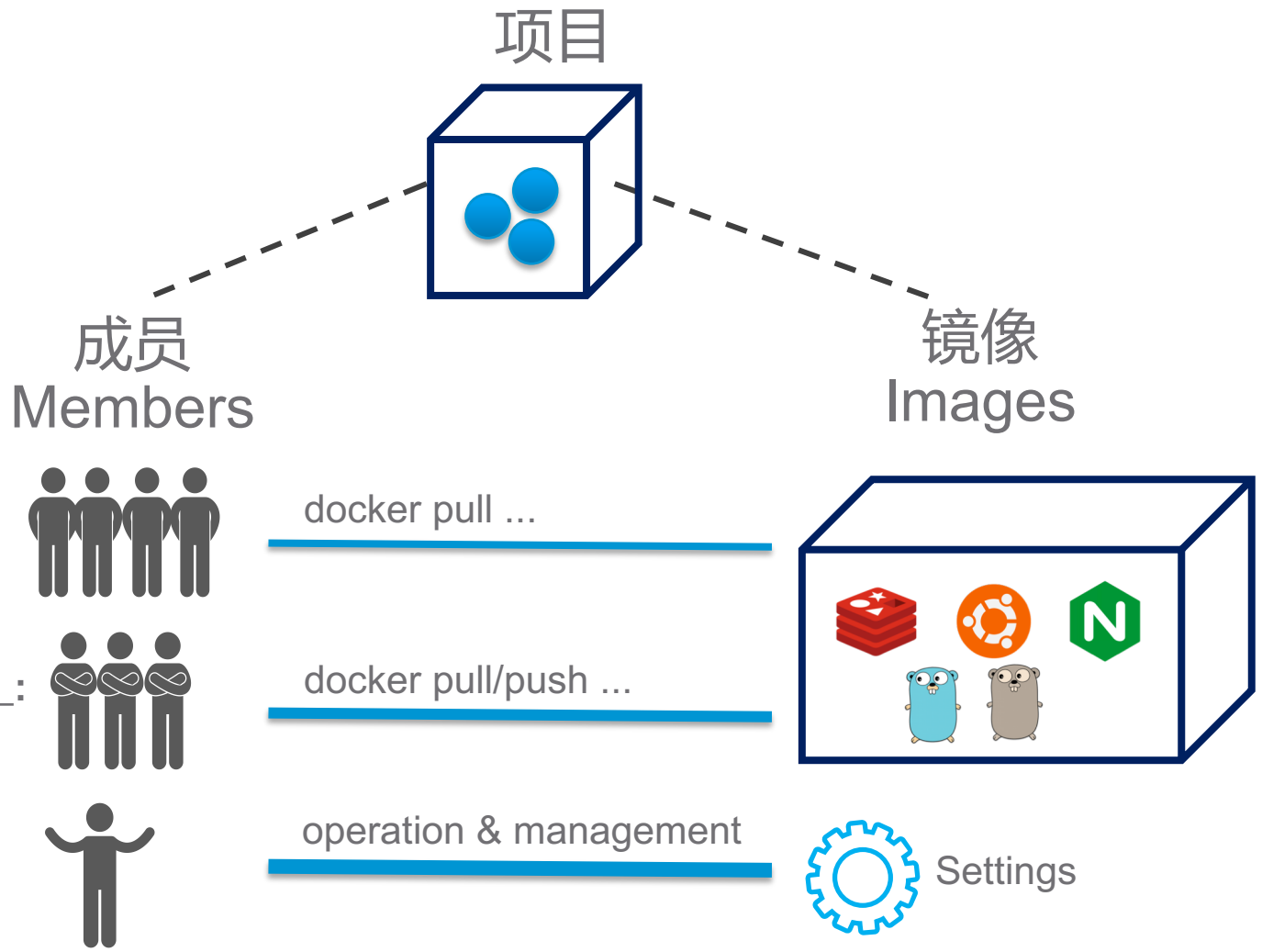
资源隔离



资源隔离

- 基于项目提供独立的NS
- 逻辑隔离，存储共享
- 访问控制的基础
- 为多租户提供可能

访问控制



访问控制

- 企业用户通常把镜像存放在组织内部
- 不同角色人员应有不同的访问权限
- 不同环境人员的角色不同
- 与已有的LDAP/AD用户系统集成

vmware

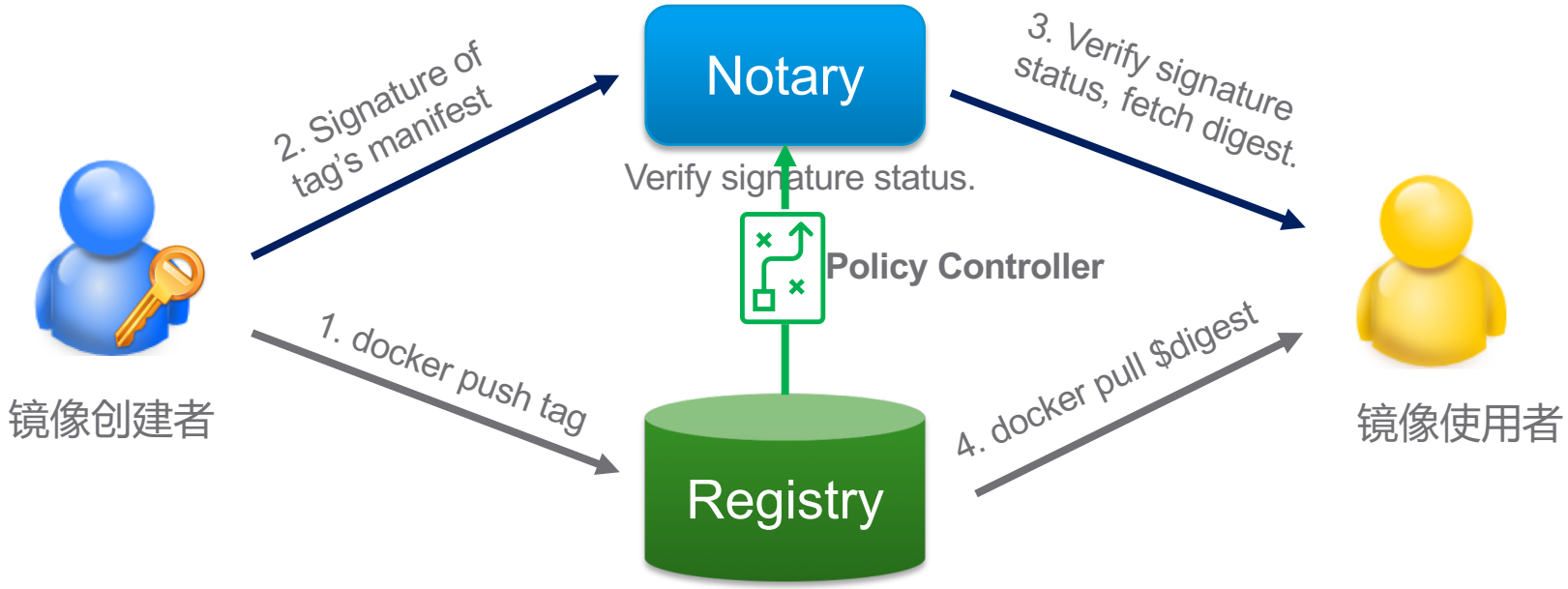
访问控制

访问控制

- 企业用户通常把镜像存放在组织内部
- 不同角色人员应有不同的访问权限
- 不同环境人员的角色不同
- 与已有的LDAP/AD用户系统集成

vmware

内容信任



内容信任

- 发布者对镜像签名
- 下载镜像时使用签名摘要（Digest）

vmware

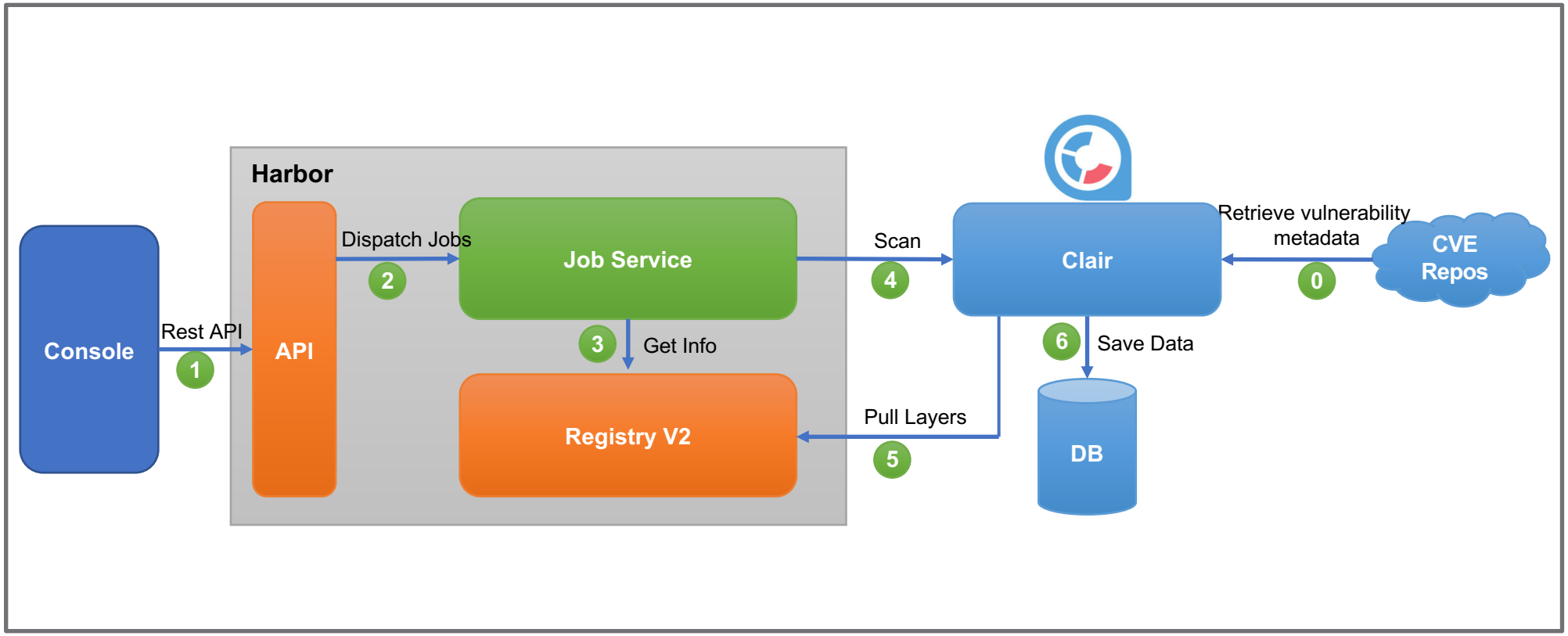
内容信任

内容信任

- 发布者对镜像签名
- 下载镜像时使用签名摘要（Digest）

vmware

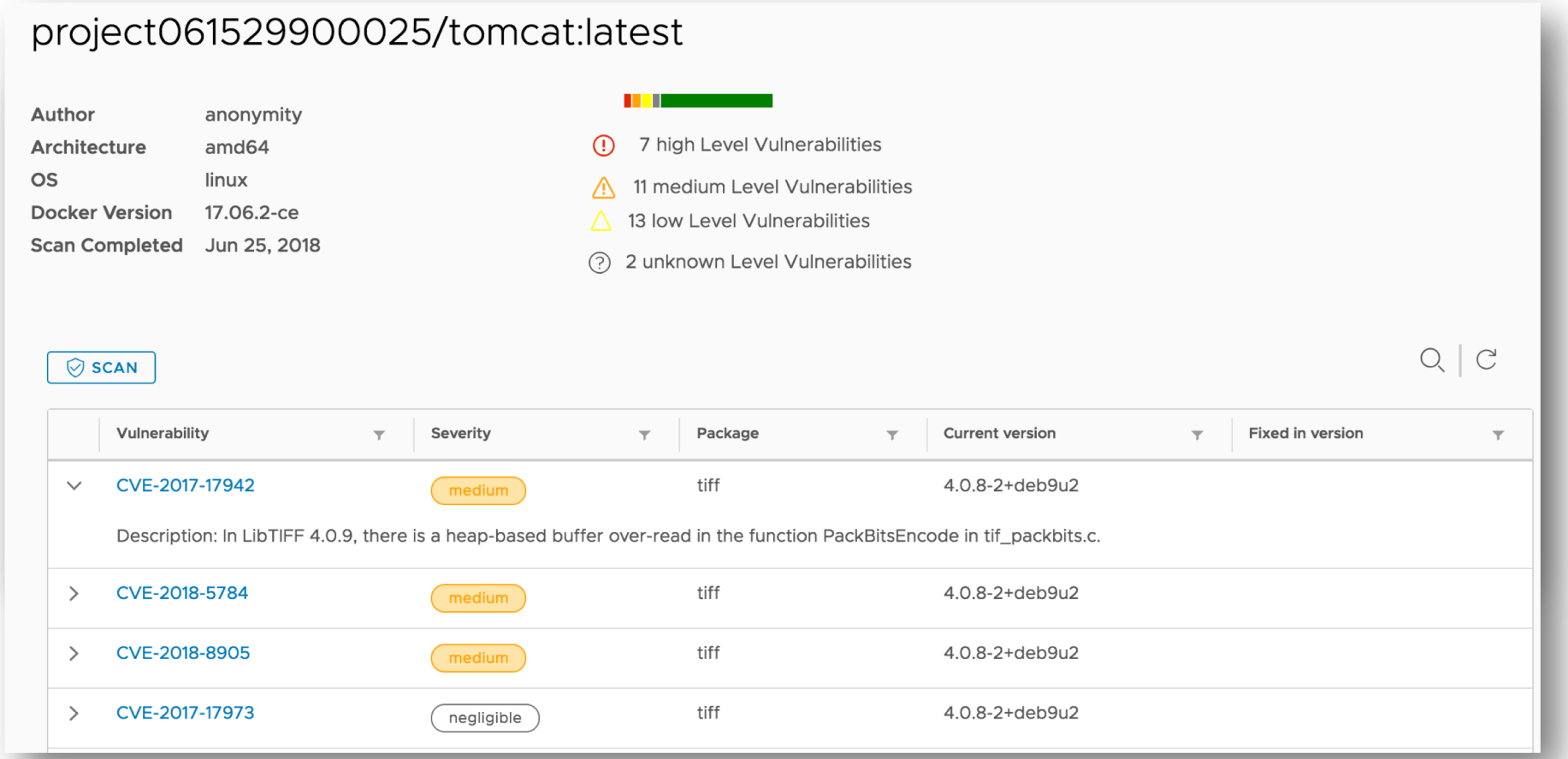
漏洞扫描



漏洞扫描

- 对镜像文件做静态分析
- 多种扫描模式支持
  - 定时
  - 事件
  - 手动
- 漏洞数据库定期更新
- 多重漏洞数据来源
  - Debian Security Bug Tracker
  - Ubuntu CVE Tracker
  - Red Hat Security Data
  - Oracle Linux Security Data
  - Alpine SecDB

漏洞扫描

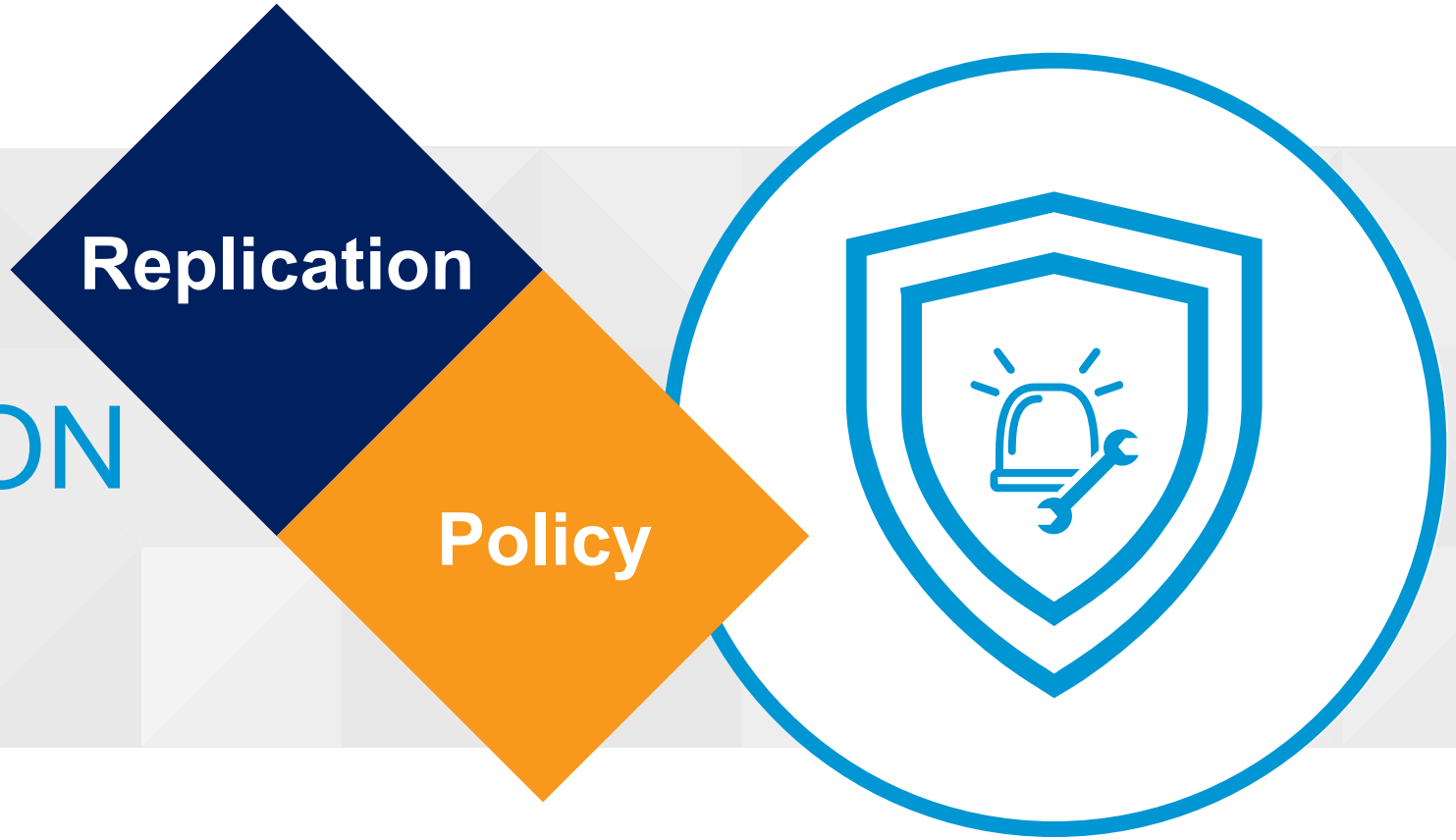


漏洞扫描

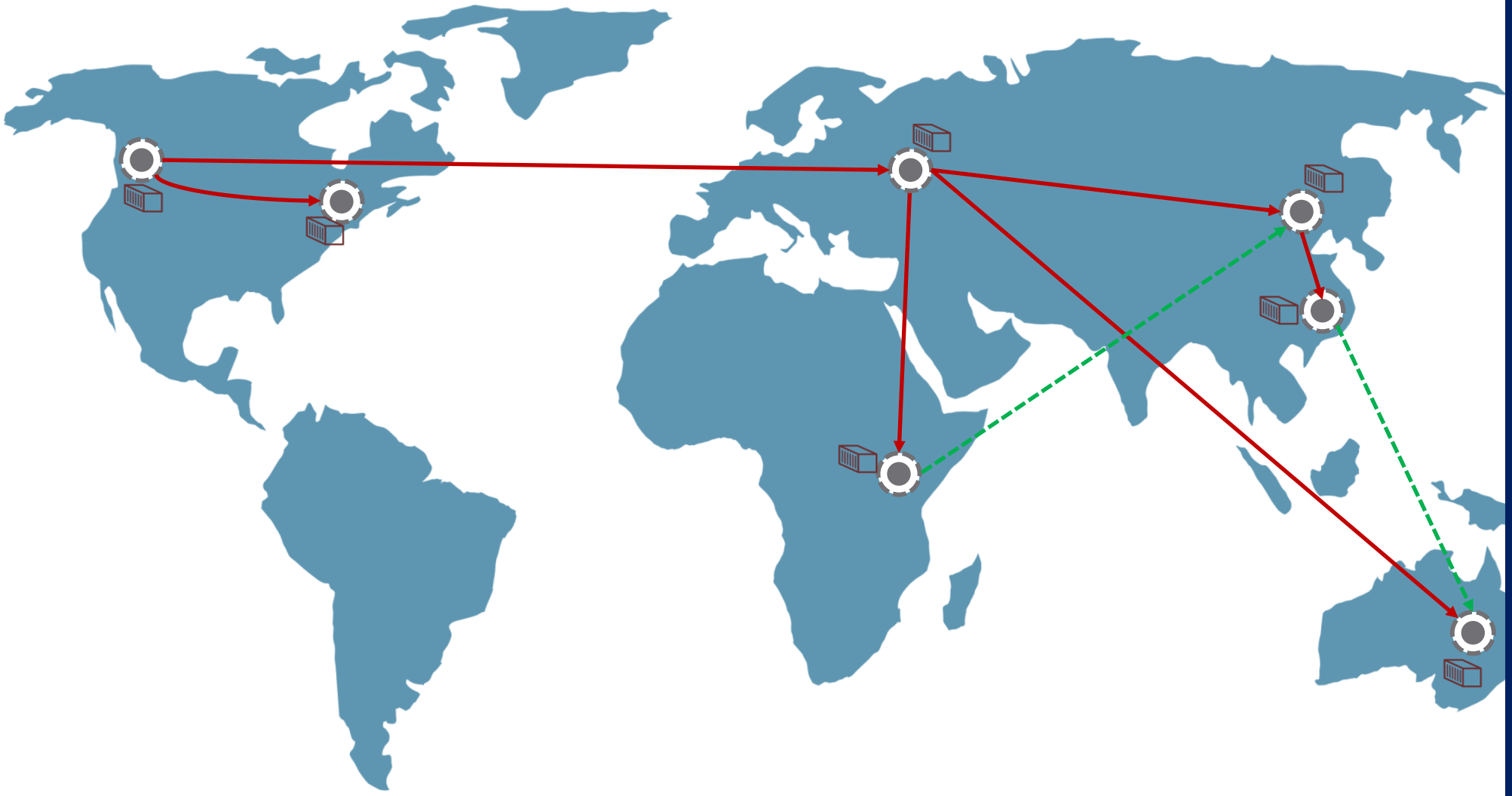
- 对镜像文件做静态分析
- 多种扫描模式支持
  - 定时
  - 事件
  - 手动
- 漏洞数据库定期更新
- 多重漏洞数据来源
  - Debian Security Bug Tracker
  - Ubuntu CVE Tracker
  - Red Hat Security Data
  - Oracle Linux Security Data
  - Alpine SecDB

vmware

DISTRIBUTION



镜像分发

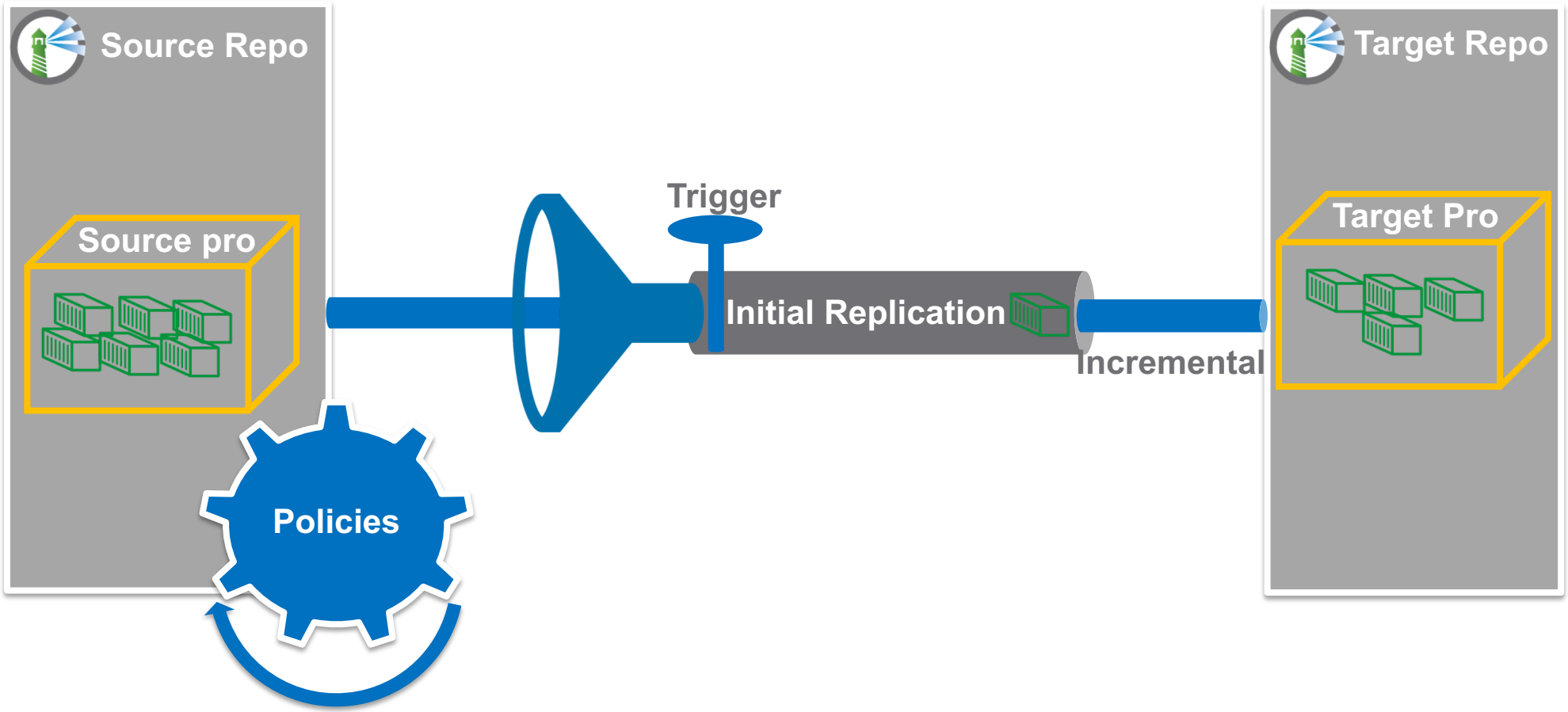


镜像分发

- 多点保持镜像一致
- 镜像备份与恢复
- 就近访问与下载
- 负载分担

vmware

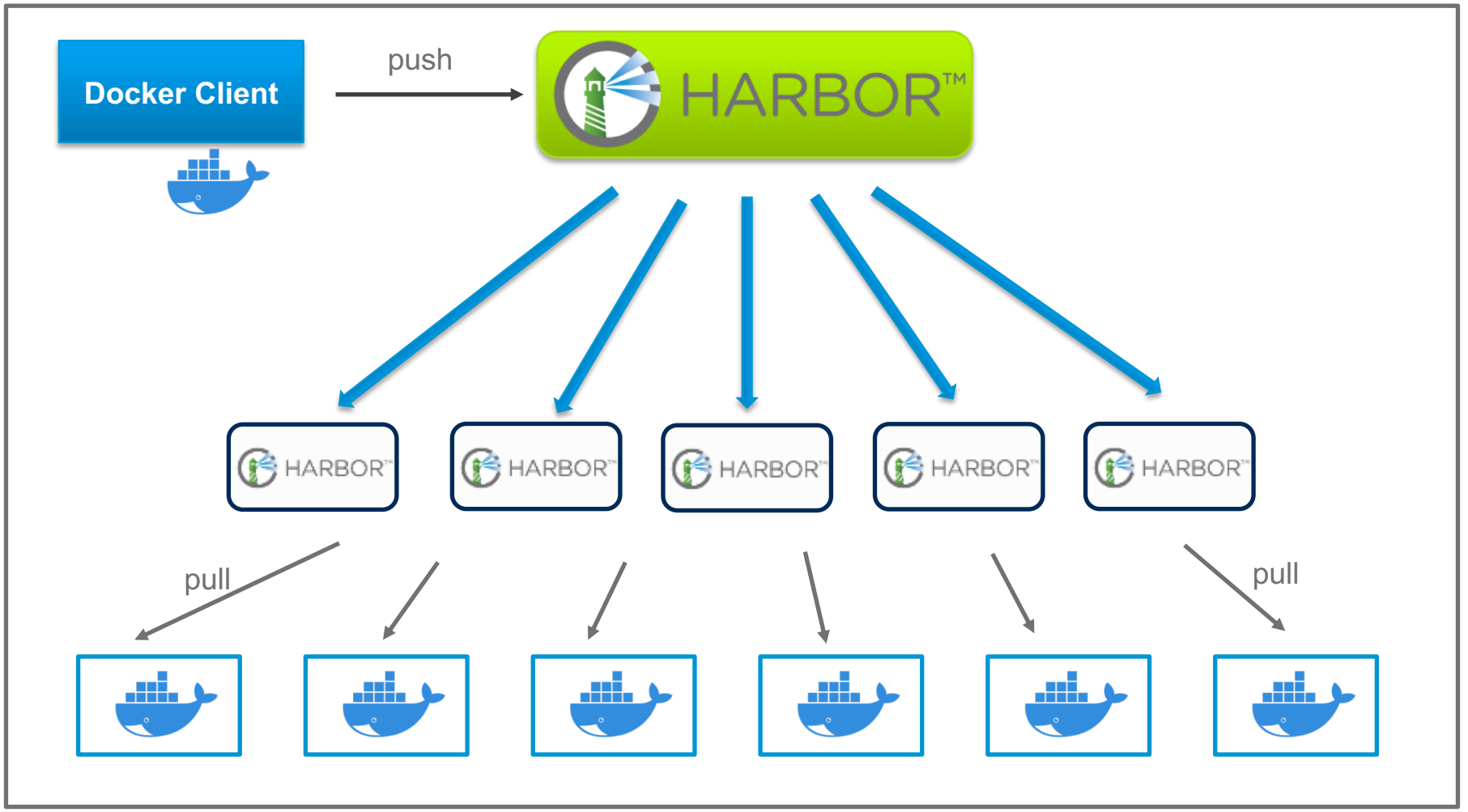
Image Replication



镜像复制

- 基于策略
- 面向项目
- 增量复制
- 支持过滤器
- 多种触发策略

镜像分发-负载分担



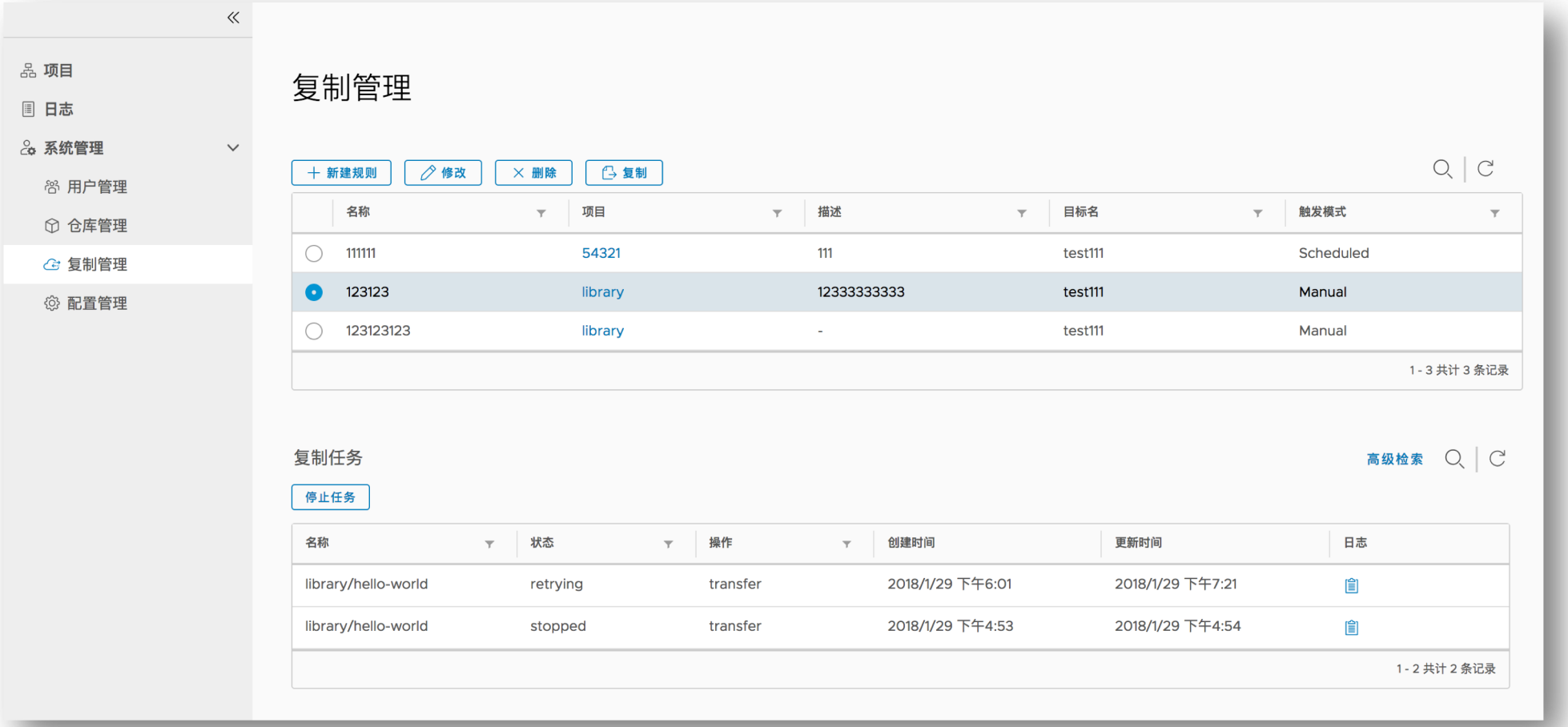
Master – Slave 模式

负载分担

- 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
- 扩展 registry 服务
  - 多实例共享存储
  - 多实例不共享存储

vmware

复制策略管理

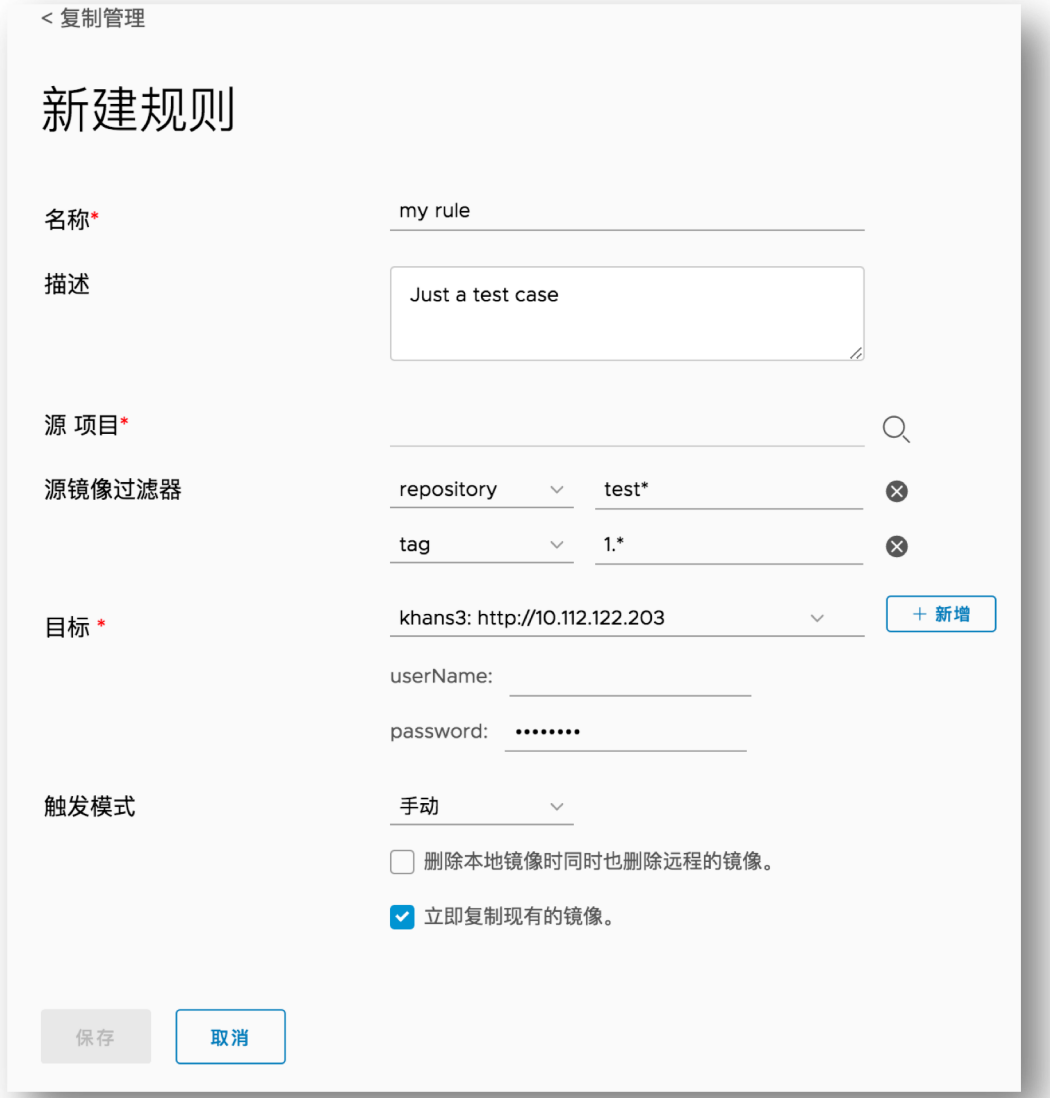


复制管理

- 可在系统与项目级别管理复制策略
- 查看复制历史
- 查看复制日志

vmware

复制策略构建



复制管理

- 支持Repo过滤
- 支持Tag过滤
- 多种触发模式
  - 手动
  - 定期
  - 事件

vmware

控制策略

公开项目

私有项目

漏洞级别<阈值

漏洞级别>=阈值

已签名

未签名（阻止）

vmware

控制策略

- 设置项目访问级别：公有/私有
- 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：未认证镜像无法下载
- 设置自动扫描：上传即扫描

控制策略

控制策略

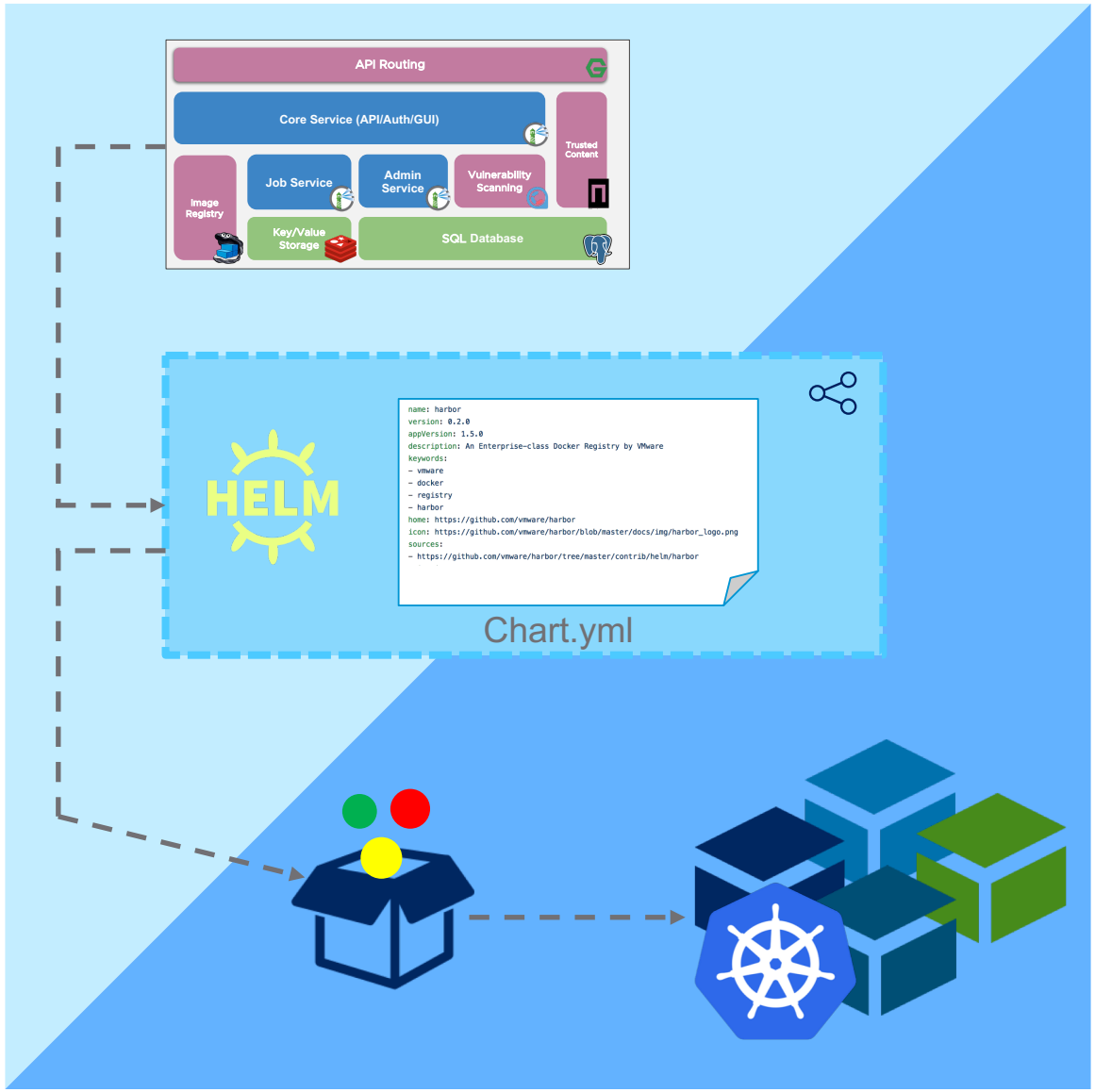
- 设置项目访问级别：公有/私有
- 设置漏洞级别阈值：超过阈值的镜像无法下载
- 设置内容信任：未认证镜像无法下载
- 设置自动扫描：上传即扫描

vmware

RELIABILITY

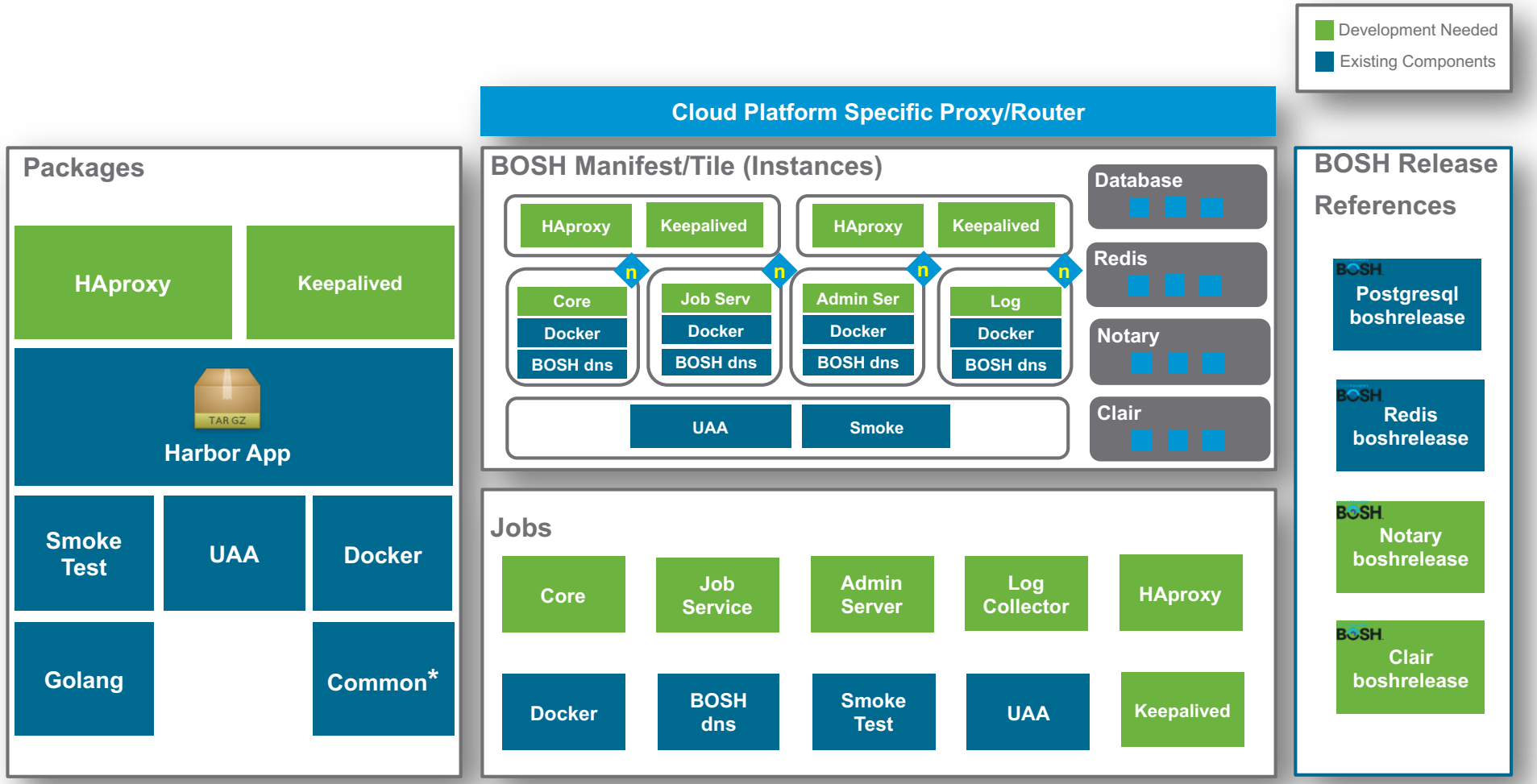
HA

Deploy Harbor HA via Harbor Helm chart



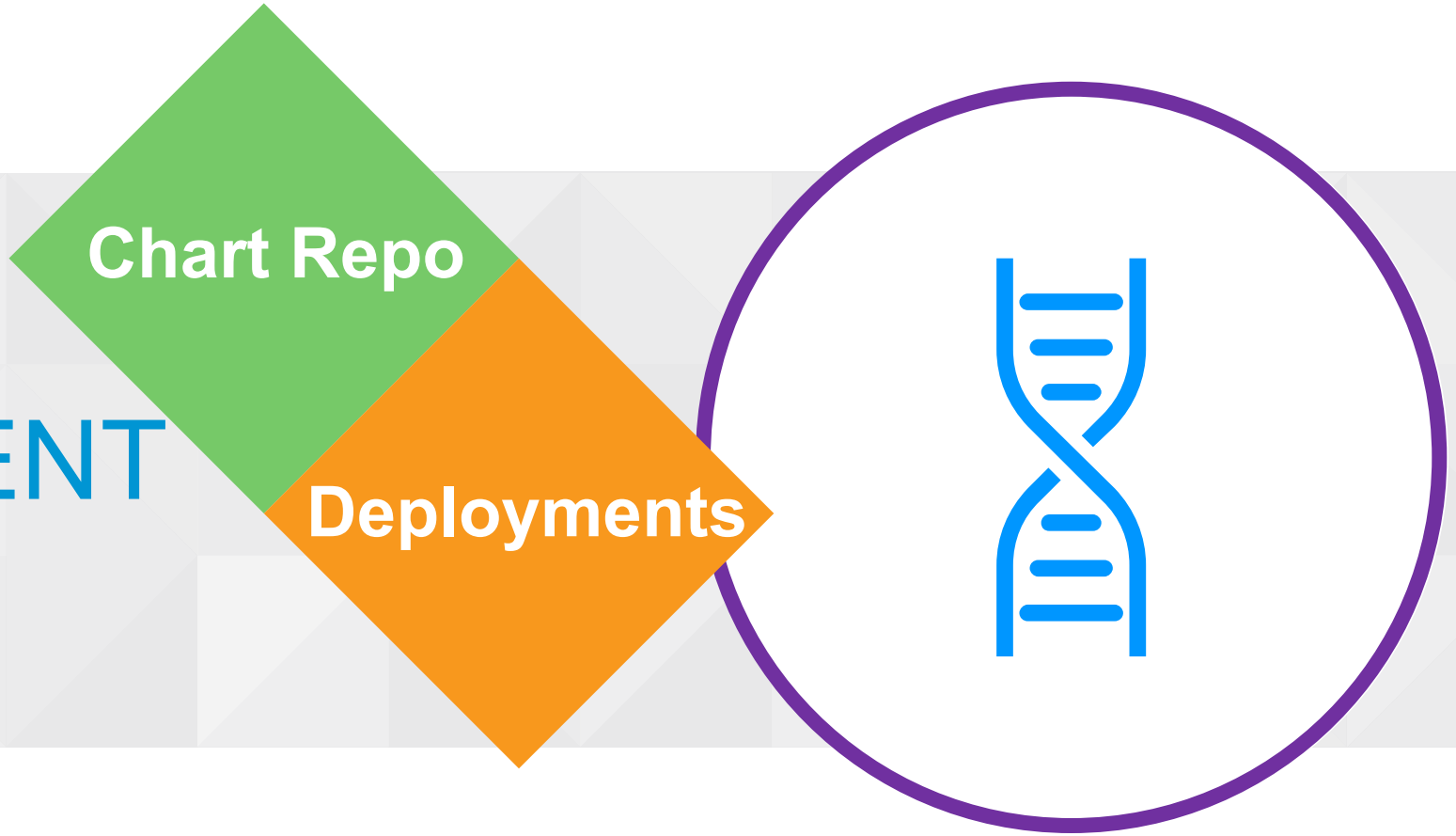
vmware®

Deploy Harbor HA via BOSH (Planning)



vmware

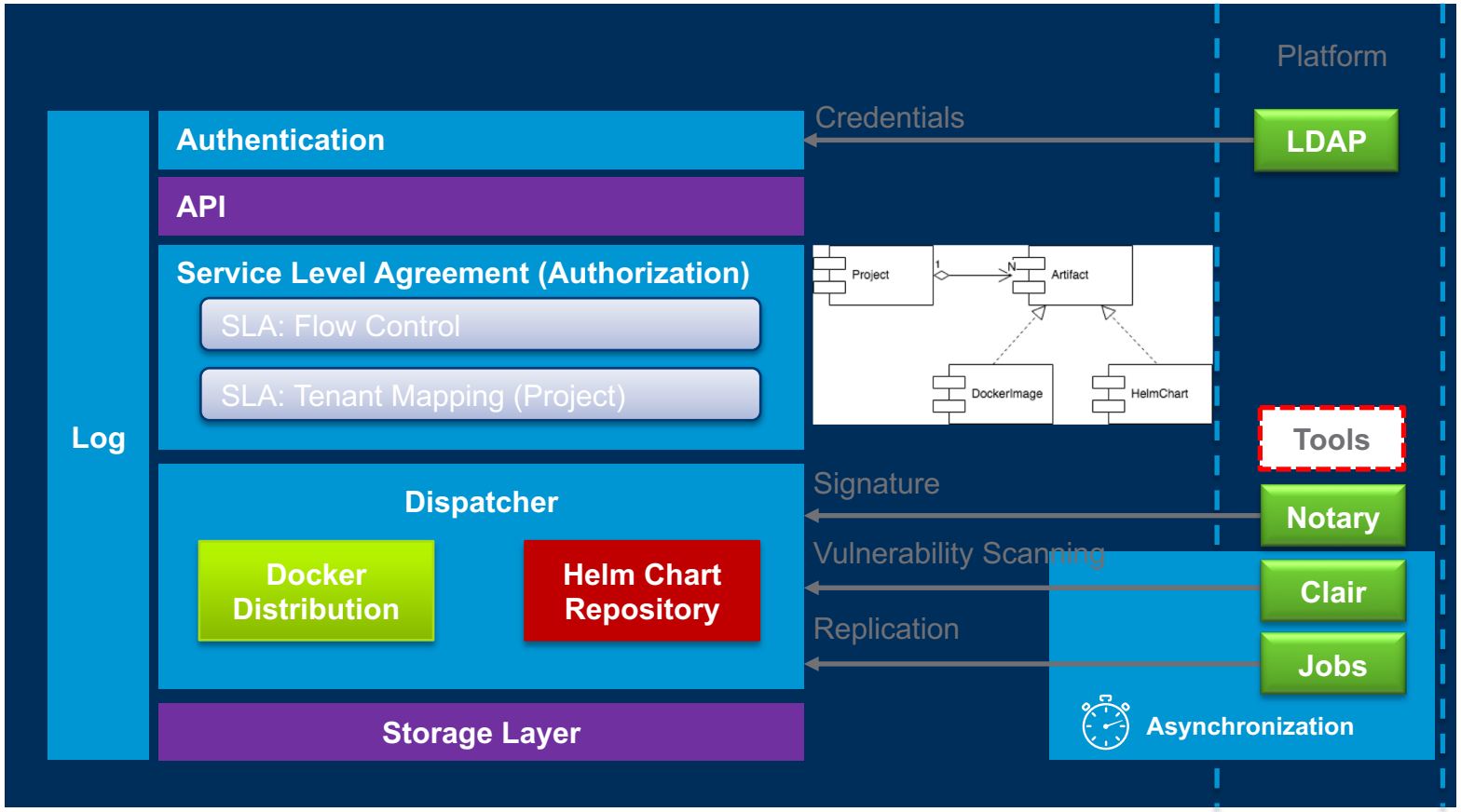
DEPLOYMENT



Helm Chart仓库支持

Updated Components

Planning Components



在容器镜像管理基础之上，Harbor将实现Helm Chart仓库的能力以支持对Chart的管理，并将通过创新方式打通Chart与镜像管理的通道。

- **Helm Chart事实上的Kubernetes包管理标准**
- **企业级应用与服务编排部署的有效模式**
- **简化难度，大幅提升生产效率**
- **与容器镜像紧密关联，利用Harbor优势**
- **拥抱云原生与Kubernetes**

vmware

Helm Chart仓库支持（续）

Supported

MANAGE

DOWNLOAD

UPLOAD

DELETE

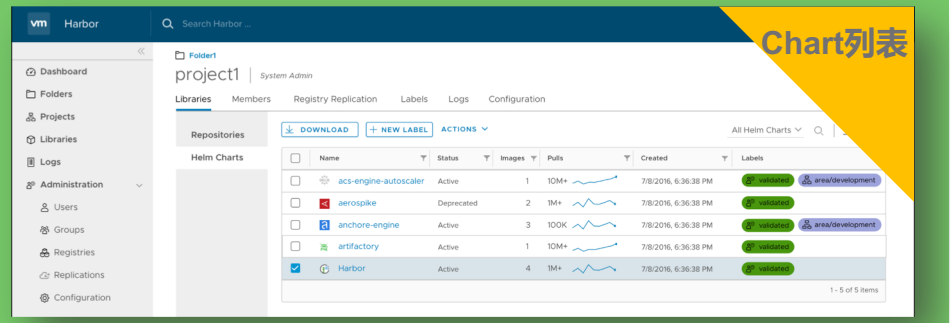
To be support

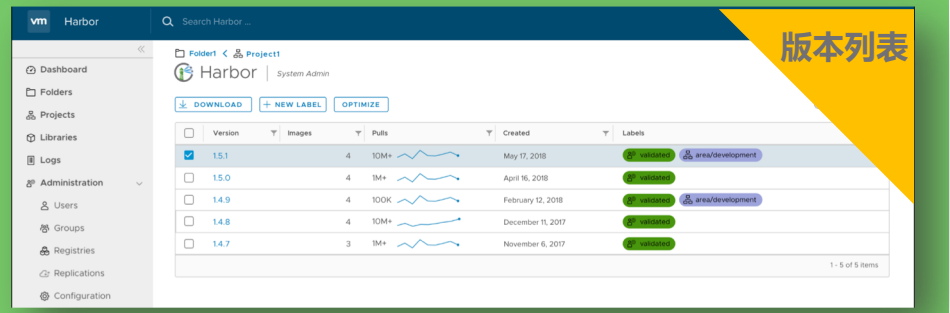
TRUST

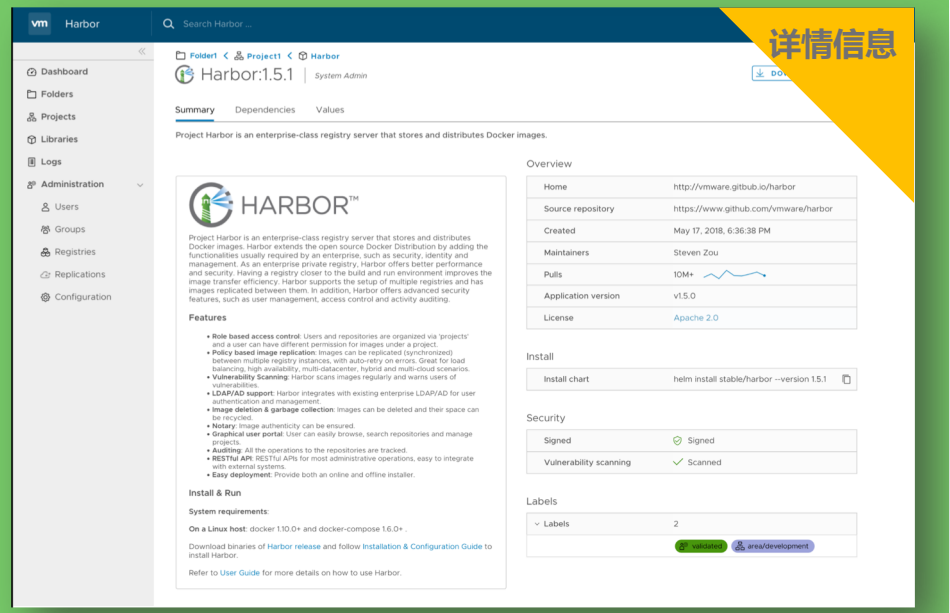
VERIFY&SCAN

REPLICATE

EXPORT/IMPORT



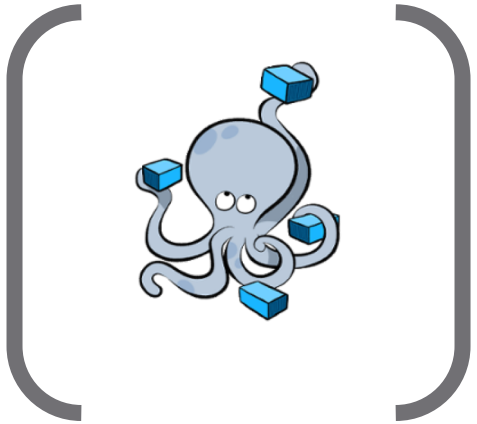




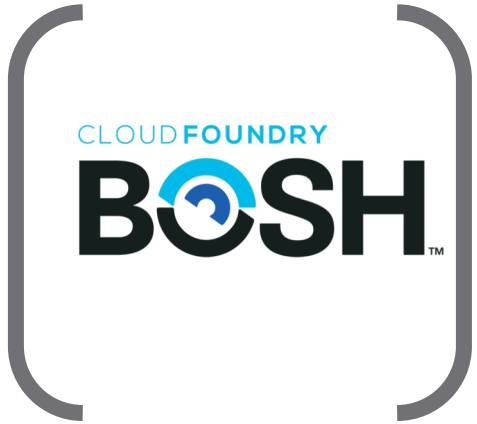
vmware

Deploy Harbor via various ways

Click to edit optional subtitle



DOCKER COMPOSE



BOSH RELEASE/TILE

HELM CHART*

NOTES: * HA deployment supported

Website：https://github.com/goharbor/harbor

Twitter: @Project_harbor

Slack: #harbor/#harbor-dev (register via slack.cncf.io)

Email group：（Refer README on GitHub for the subscription way ）

harbor-users@googlegroups.com

harbor-dev@googlegroups.com

WeChat group: Contact speakers

Thank You