Harbor 101

Henry Zhang, Chief Architect, VMware China

Steven Ren, Sr. Manager, VMware China

KubeCon | CloudNativeCon

Europe 2019

About Us

Haining Henry Zhang

- Founder and evangelist of Project Harbor
- Chief Architect, VMware China R&D
- Former evangelist of Cloud Foundry China community
- Hyperledger Cello Contributor
- Coauthor of best selling blockchain book - Blockchain Technical Guide (in Chinese)
- Current interest: cloud computing, AI, blockchain etc.

Steven Ren

- R&D engineering manager, VMware
- Delivered several open source products: VMware integrated OpenStack, VMware integrated containers, Harbor.
- Current interest: cloud computing, networking, cloud native apps, etc.

Mission
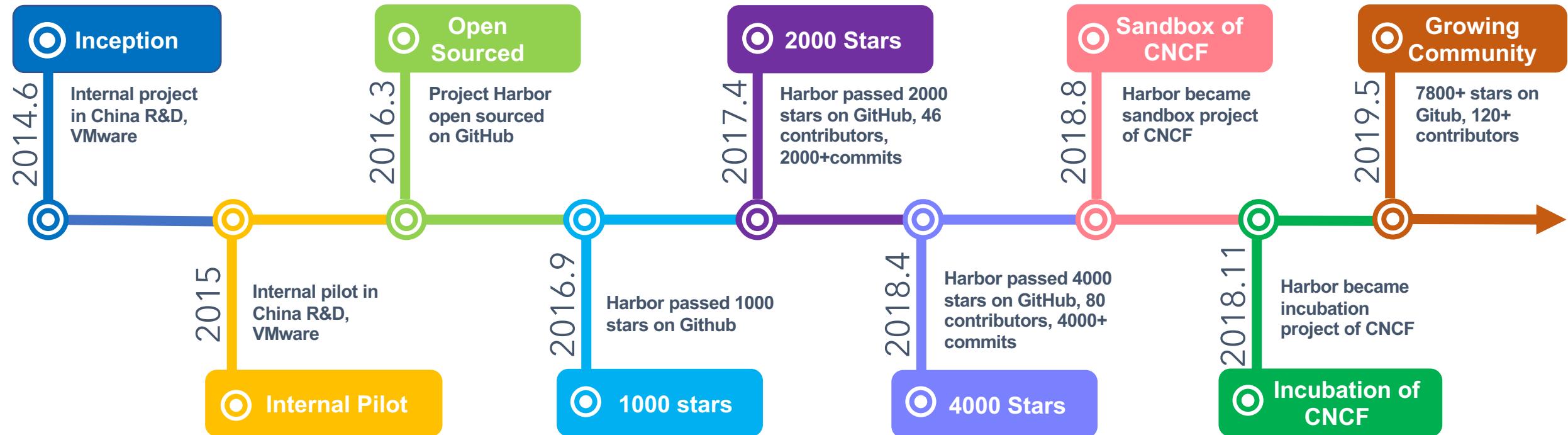
Harbor is a <u>trusted cloud native registry</u> that stores, signs, and scans content. The mission is to provide cloud native environments the ability to confidently manage and serve container images and related artifacts.

Harbor Timeline

KubeCon | CloudNativeCon
Europe 2019

Inception
2014.6
Internal project in China R&D, VMware

2015
Internal Pilot
Internal pilot in China R&D, VMware

Open Sourced
2016.3
Project Harbor open sourced on GitHub

2016.9
1000 stars
Harbor passed 1000 stars on Github

2000 Stars
2017.4
Harbor passed 2000 stars on GitHub, 46 contributors, 2000+commits

2018.4
4000 Stars
Harbor passed 4000 stars on GitHub, 80 contributors, 4000+ commits

Sandbox of CNCF
2018.8
Harbor became sandbox project of CNCF

2018.11
Incubation of CNCF
Harbor became incubation project of CNCF

Growing Community
2019.5
7800+ stars on Gitub, 120+ contributors

Harbor Community

Stars	Forks	Commits	Contributors	Members
7800+	**2100+**	**6600+**	**120+**	**1500+**

Contributors & Maintainers

Canada

USA

Nicaragua

Brazil

Sweden

UK

Germany

France

Spain

Italy

Belarus

Ukraine

Russia

China

Korea

Japan

India

Vietnam

Singapore

South Africa

Australia

New Zealand

14 Maintainers

126 Contributors

65+ Companies

36+ Countries

Source: https://harbor.devstats.cncf.io

Harbor Users and Partners (selected)
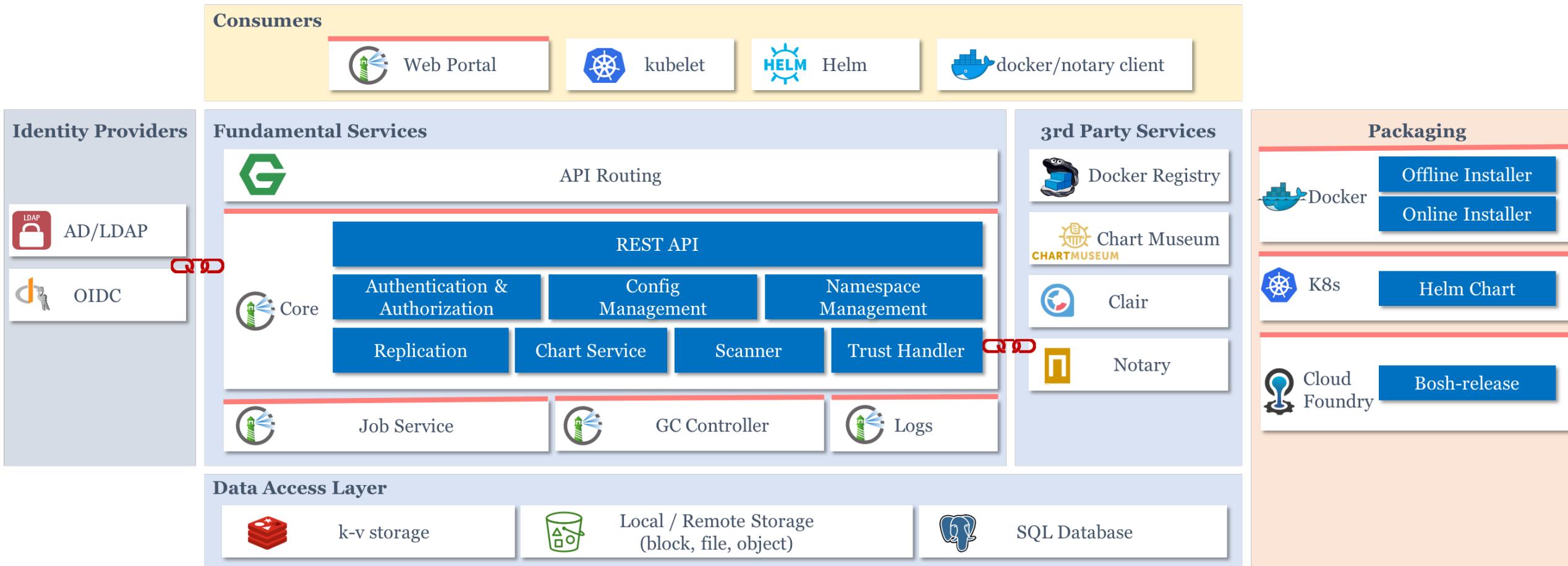
Overall Architecture

Key Features

Access Control

- **RBAC**
- **AD/LDAP integration**
- **OIDC**
- **Robot account**

Access Control
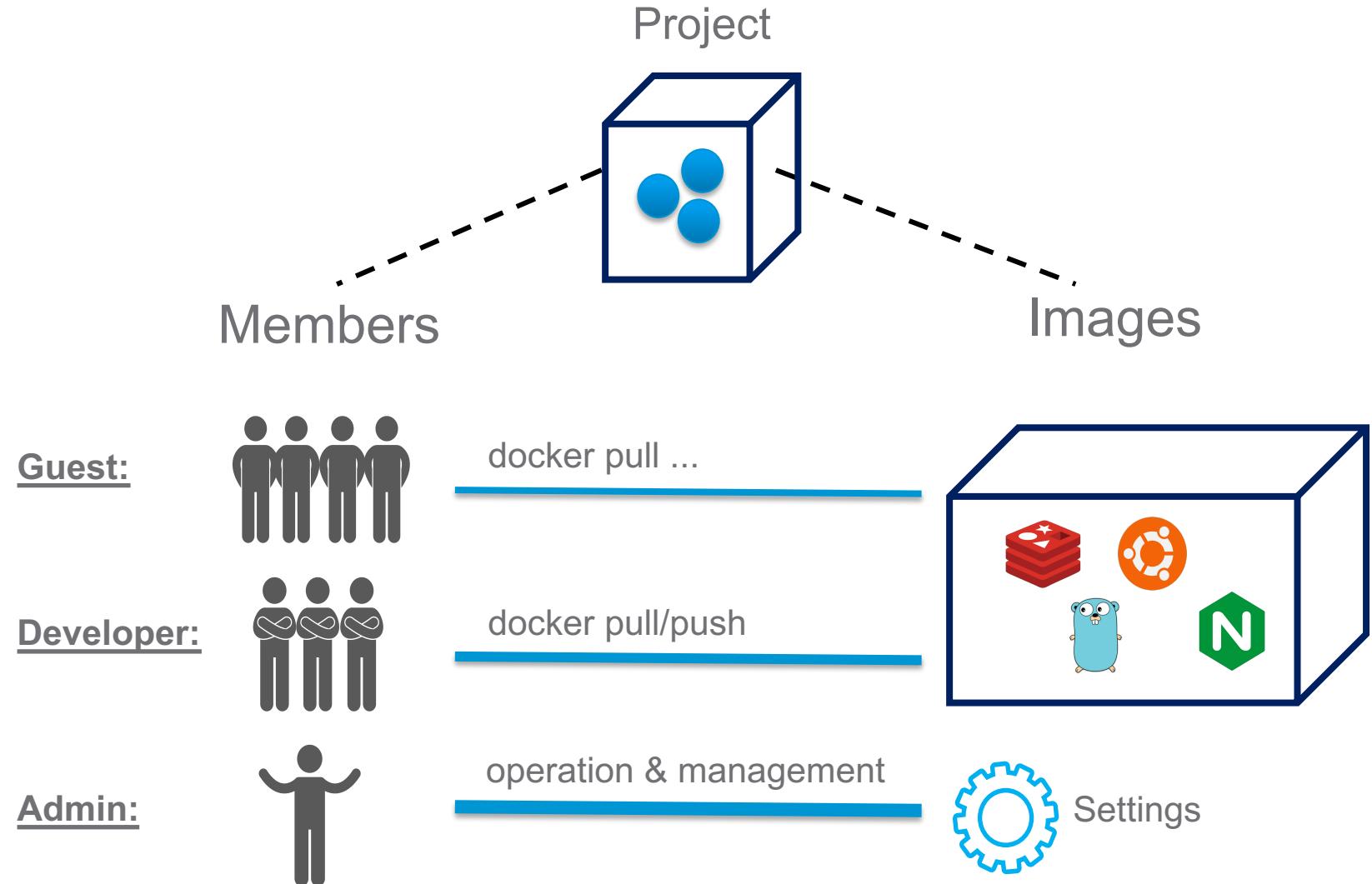
- Access managed by project
- RBAC - Role based access control
- Identity providers:
  - AD/LDAP
  - OIDC
- Robot account (for systems such as CI/CD)

Project

Members

Images

Guest: docker pull ...

Developer: docker pull/push

Admin: operation & management

Settings

Key Features

Access Control

- RBAC
- AD/LDAP integration
- OIDC
- Robot account
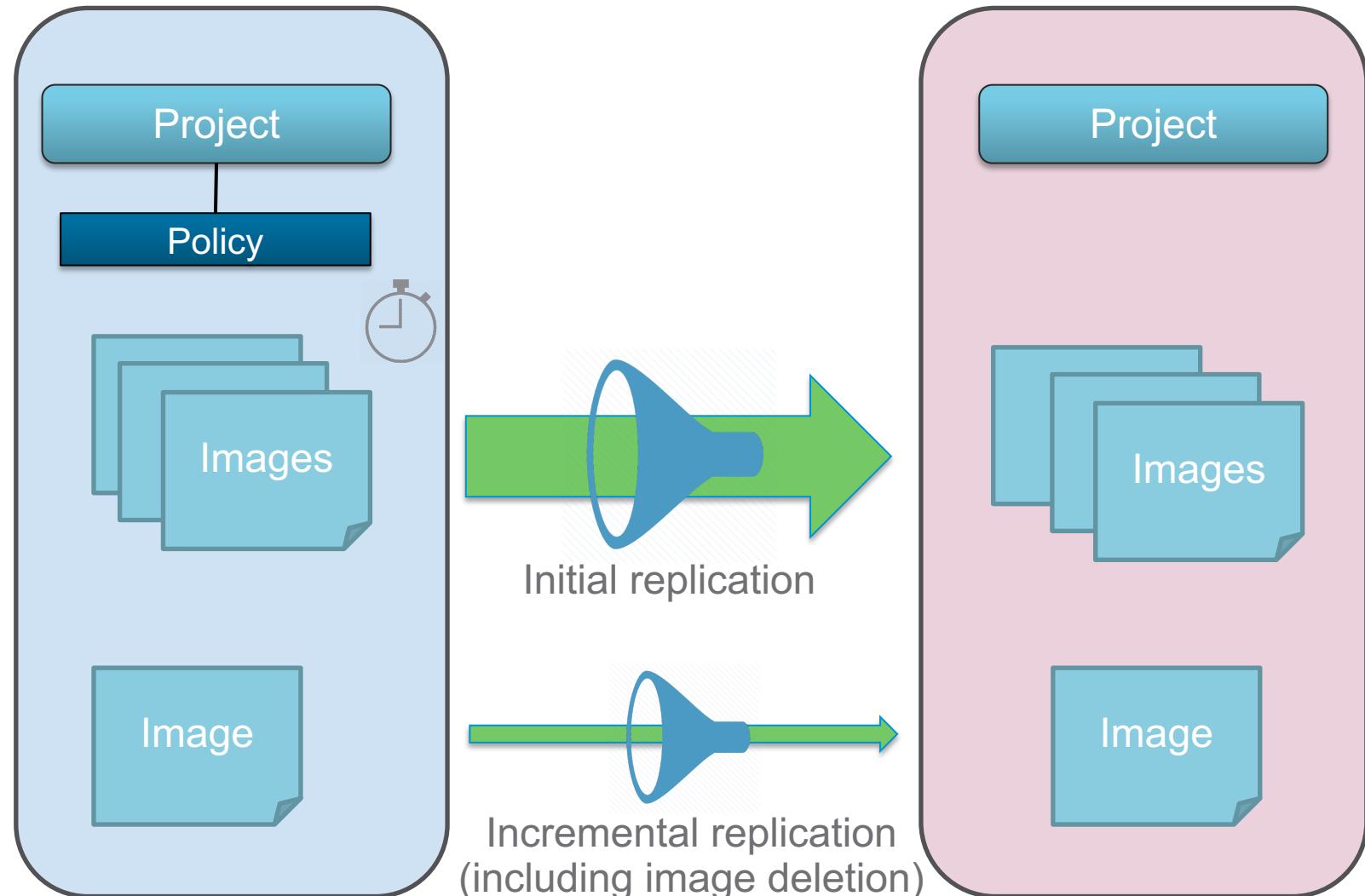
Replication

- **Multiple filters**
- **Flexible scheduling**
- **Heterogeneous registries**
- **Helm Chart replication**

Replication

- Heterogenous registries
  - Harbor
  - Docker Hub
  - Docker Distribution
  - Huawei Container Registry
  - More can be added …
- Flexible policy:
  - Filters
  - Cron-based scheduling
  - Pull / push mode
- Helm Chart supported
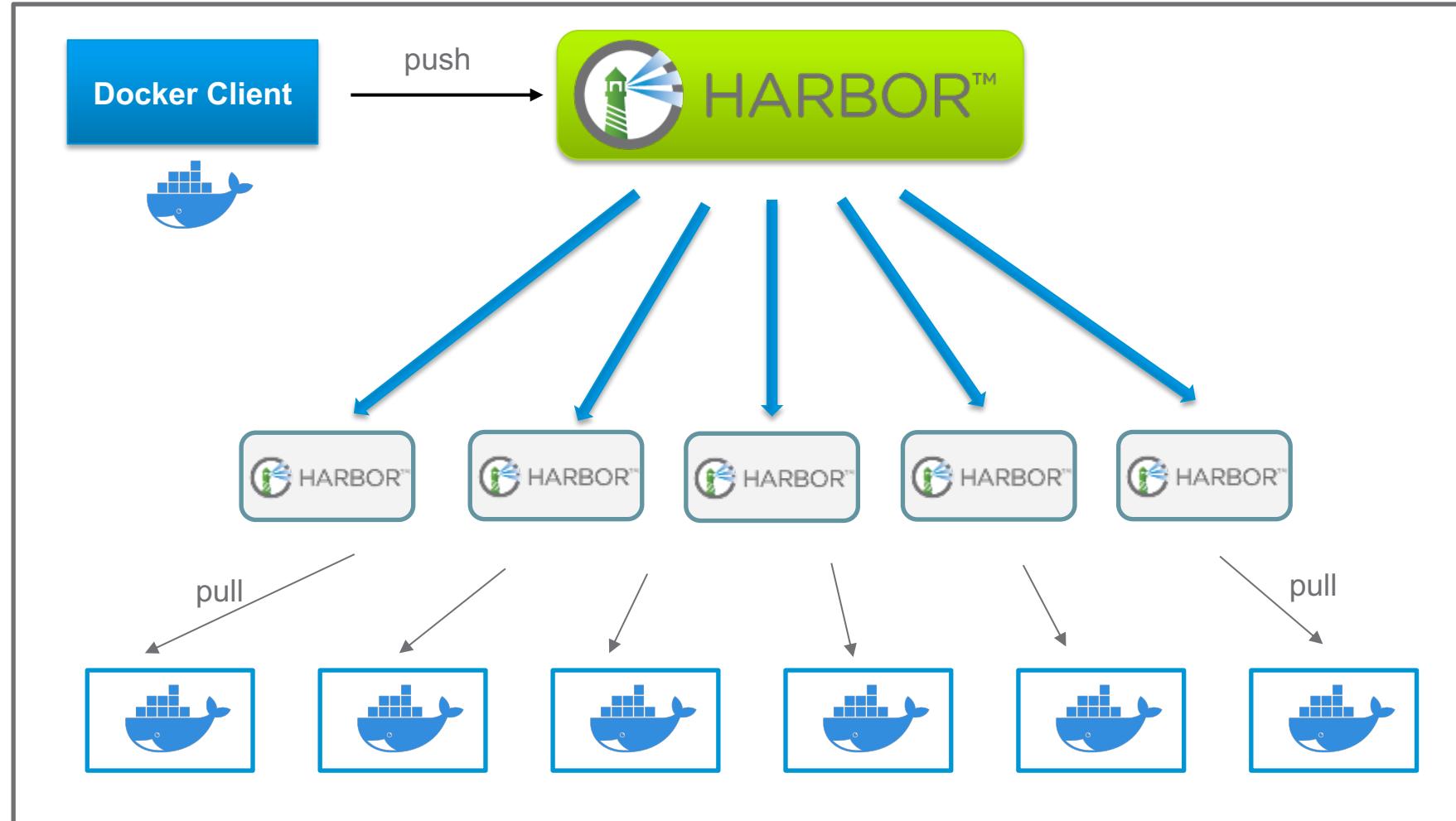
Project

Policy

Images

Image

Initial replication

Incremental replication
(including image deletion)

Project

Images

Image

Scaling Horizontally
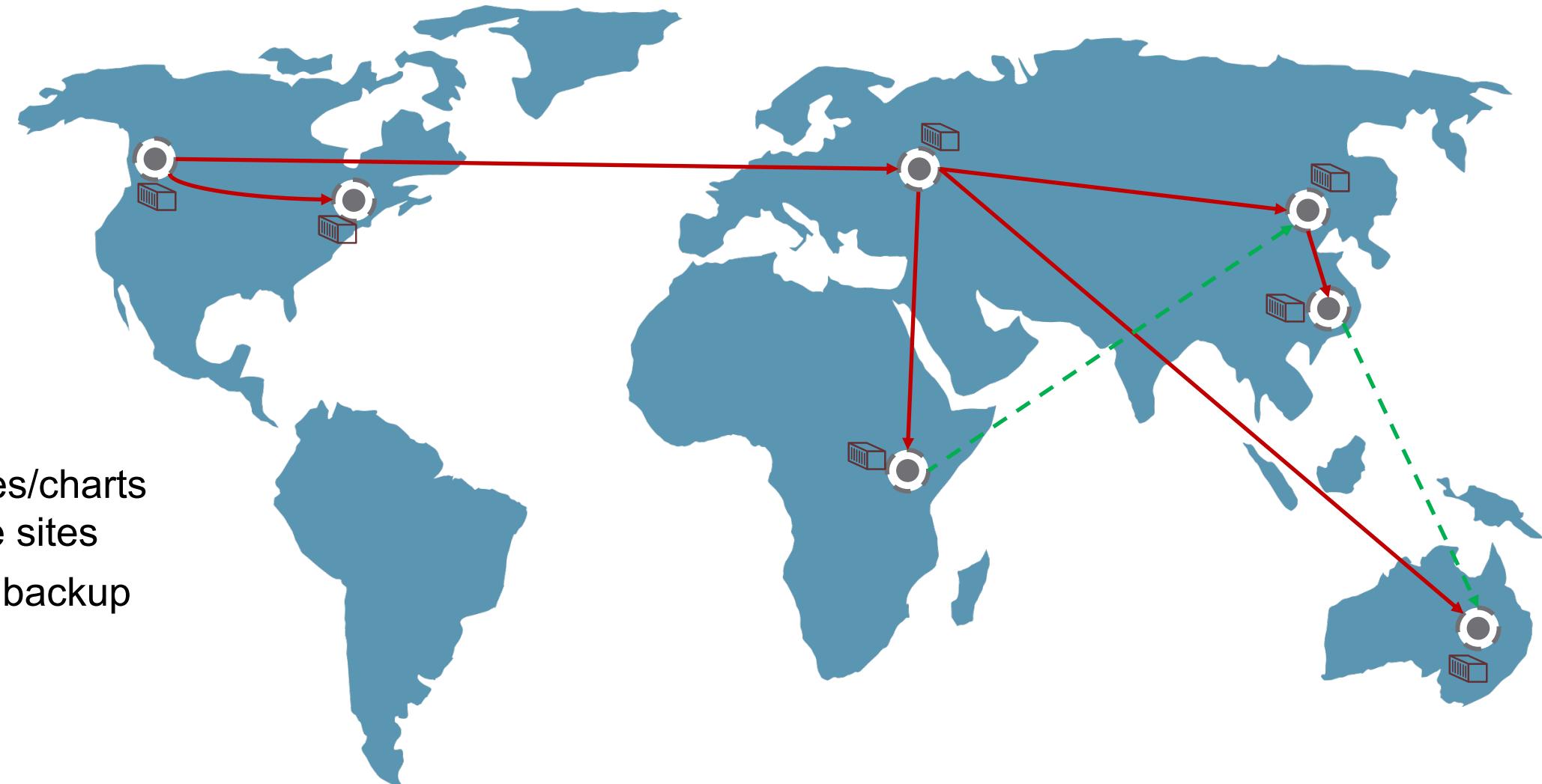
Global Replication

- Identical images/charts across multiple sites
- Image / charts backup
- Local access

Key Features

Access Control

- RBAC
- AD/LDAP integration
- OIDC
- Robot account

Replication

- Multiple filters
- Flexible scheduling
- Heterogeneous registries
- Helm Chart replication

Vulnerability Scanning

- **Flexible scanning policies**
- **Elaborated scanning report**

Vulnerability Scanning

- Leverage Red Hat Clair (née CoreOS)

- Static analysis of vulnerability

- Severity threshold of vulnerability to block `pulls` if exceeded

- Vulnerability data pulled from vendor DBs

  - Debian + Ubuntu {Bug,CVE} tracker

  - Red Hat security data

  - Oracle Linux security data

  - Alpine SecDB

  - NIST

project061529900025/tomcat:latest

Author	anonymity
Architecture	amd64
OS	linux
Docker Version	17.06.2-ce
Scan Completed	Jun 25, 2018

- 7 high Level Vulnerabilities
- 11 medium Level Vulnerabilities
- 13 low Level Vulnerabilities
- 2 unknown Level Vulnerabilities

🛡 SCAN

Vulnerability	Severity	Package	Current version	Fixed in version
∨ CVE-2017-17942	medium	tiff	4.0.8-2+deb9u2	
Description: In LibTIFF 4.0.9, there is a heap-based buffer over-read in the function PackBitsEncode in tif_packbits.c.				
› CVE-2018-5784	medium	tiff	4.0.8-2+deb9u2	
› CVE-2018-8905	medium	tiff	4.0.8-2+deb9u2	
› CVE-2017-17973	negligible	tiff	4.0.8-2+deb9u2	

Key Features

Access Control

- RBAC
- AD/LDAP integration
- OIDC
- Robot account

Replication

- Multiple filters
- Flexible scheduling
- Heterogeneous registries
- Helm Chart replication

Vulnerability Scanning

- Flexible scanning policies
- Elaborated scanning report
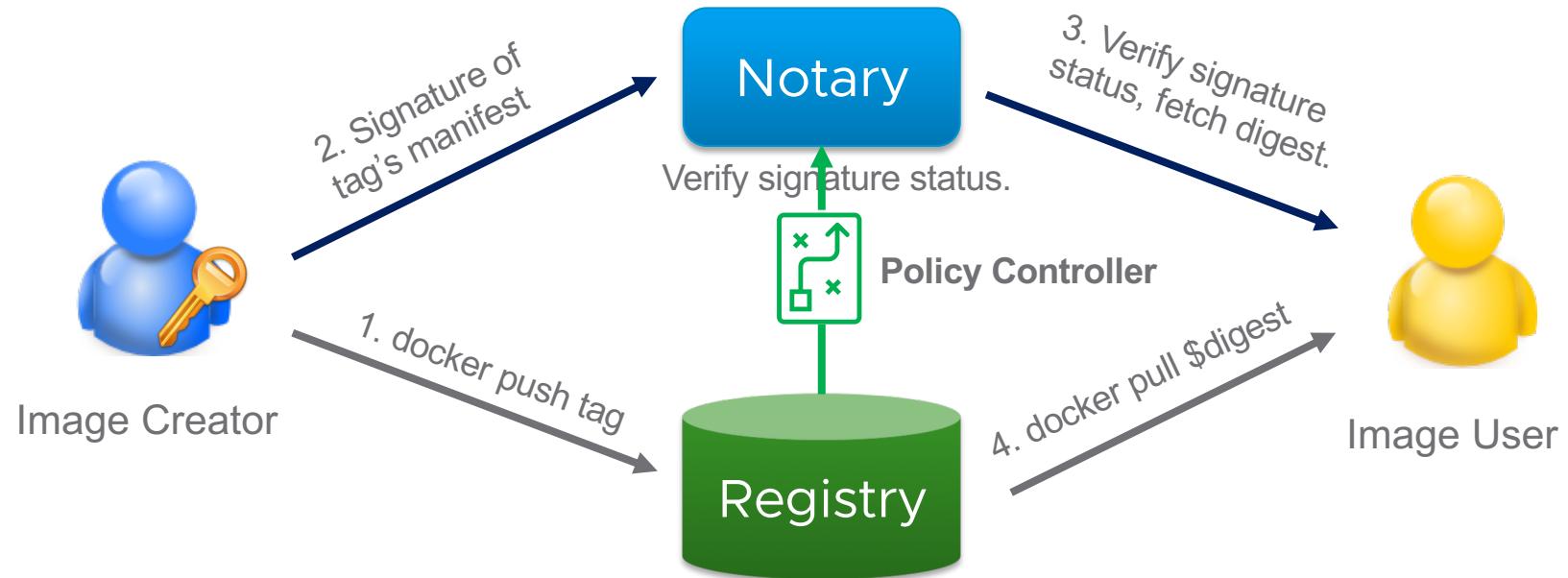
Content Trust

- **Digital signature**
- **Provenance of images**

Image signing

- Leverage CNCF's Notary
    - Sign image when pushing
    - Enforce signing policy and block pulls of unsigned images

Key Features

Access Control

- RBAC
- AD/LDAP integration
- OIDC
- Robot account

Replication

- Multiple filters
- Flexible scheduling
- Heterogeneous registries
- Helm Chart replication

Vulnerability Scanning

- Flexible scanning policies
- Elaborated scanning report

Content Trust

- Digital signature
- Provenance of images

Helm Chart Mgmt

- **Helm Chart repository**
- **Same user experiences as image management**

Helm Chart Management

- Unified image and Helm Chart management
  - Access Control
  - Replication
  - Upload / download charts via UI
  - Helm CLI support

Key Features

Access Control
- RBAC
- AD/LDAP integration
- OIDC
- Robot account

Replication
- Multiple filters
- Flexible scheduling
- Heterogeneous registries
- Helm Chart replication

Vulnerability Scanning
- Flexible scanning policies
- Elaborated scanning report

Content Trust
- Digital signature
- Provenance of images

Helm Chart Mgmt
- Helm Chart repository
- Same user experiences as image management

Web Portal
- Ease of use
- Batch operations

Restful API
- API for integration
- Nested Swagger UI

Multi Deployments
- Docker Compose
- Helm Chart
- BOSH

What's New in Harbor 1.8 ?

- OIDC (Open ID Connect)

- Robot account for system integration (e.g. CI/CD)

- Replication advancements

  - Heterogenous registries: Docker Hub, Docker Distribution, Huawei Registry

  - Pull / push mode

- Health check API

- Swagger UI for exploring and triggering Harbor API

- Cron-based scheduling tasks: scan, garbage collection and replication

- Bug fixes

DEMO 1
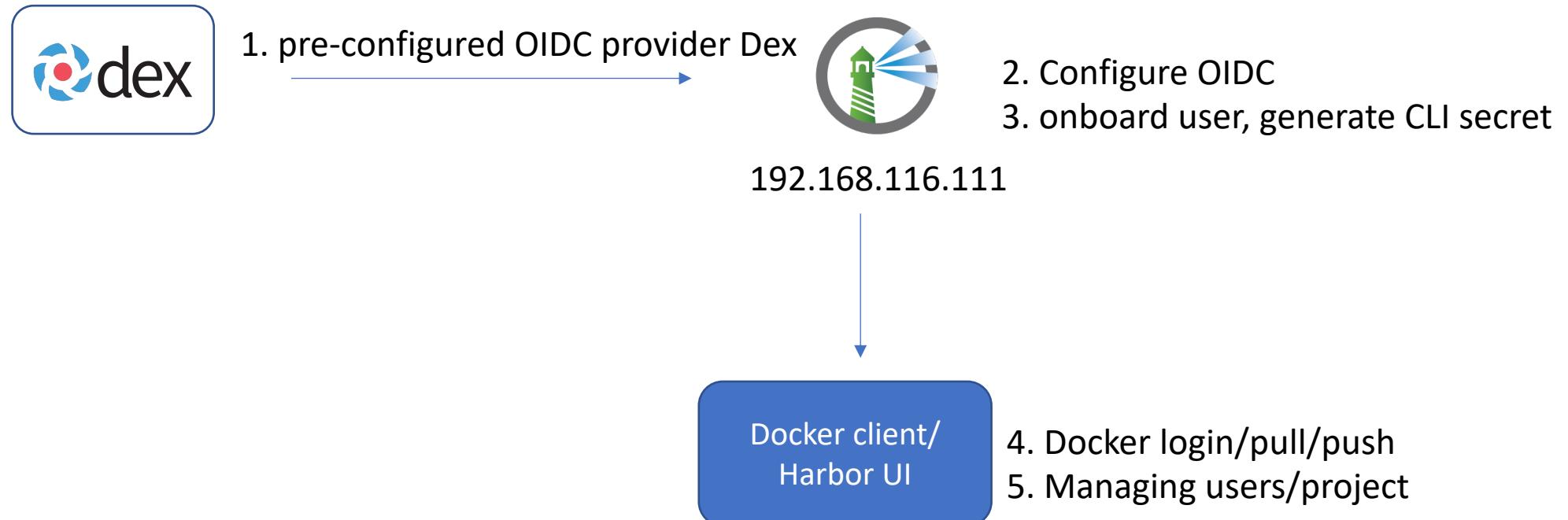
- ## OIDC (Open ID Connect)

1. pre-configured OIDC provider Dex

192.168.116.111

2. Configure OIDC
3. onboard user, generate CLI secret

Docker client/
Harbor UI

4. Docker login/pull/push
5. Managing users/project

DEMO 2
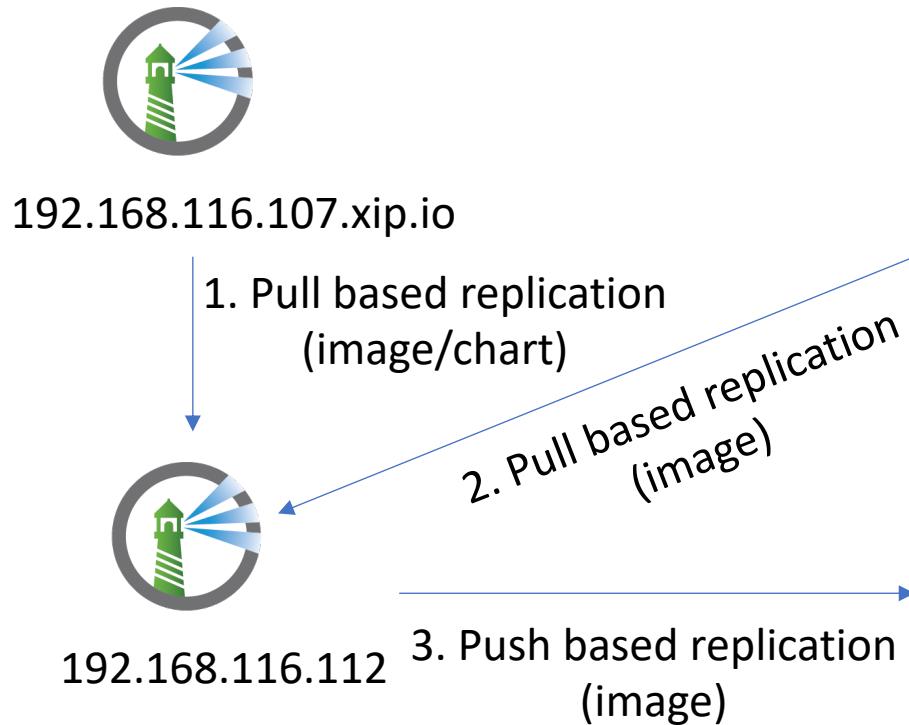
- Replication between heterogenous registries with push/pull mode

192.168.116.107.xip.io

1. Pull based replication (image/chart)

2. Pull based replication (image)

https://hub.docker.com

192.168.116.112

3. Push based replication (image)

Native registry – 10.155.21.231:5000

Harbor Sessions at KubeCon EU

- Harbor Intro Session:
  - Tuesday, May 21, 2019 14:50-15:25 in **Hall 8.0 E5**
- Harbor Deep-Dive Session:
  - Wednesday, May 22, 2019 14:50-15:25 in **Hall 8.0 E5**

- Find us @CNCF Answer Bar

Maintainer	Day	Time
Steven Zou	Tuesday & Wednesday (May 21 & 22)	4:00pm - 4:30pm
Steven Ren	Wednesday & Thursday (May 22 & 23)	12:00pm - 12:30pm

Join the fun!

Web: https://www.goharbor.io

Github: https://github.com/goharbor

Slack: slack.cncf.io (#habor and #harbor-dev)

Twitter: @Project_harbor

By-weekly Community Meetings: https://zoom.us/j/734959521

Email groups:

harbor-users@lists.cncf.io

harbor-dev@lists.cncf.io