

Using BOSH to Deploy the Open Source Harbor Docker Registry

Jesse Hu 胡 辉
Staff Engineer - huh@vmware.com

DaoJun Zhang 张道军
Staff Engineer - daojunz@vmware.com

2018.11



Harbor is an open source cloud native docker registry that stores, signs, and scans container images for vulnerabilities.

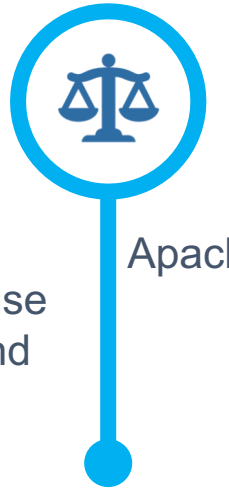
Harbor is a CNCF project https://github.com/goharbor/harbor/



Initiated by VMware China, maintained by the Harbor community



Integrated into VMware enterprise products: VIC and PKS



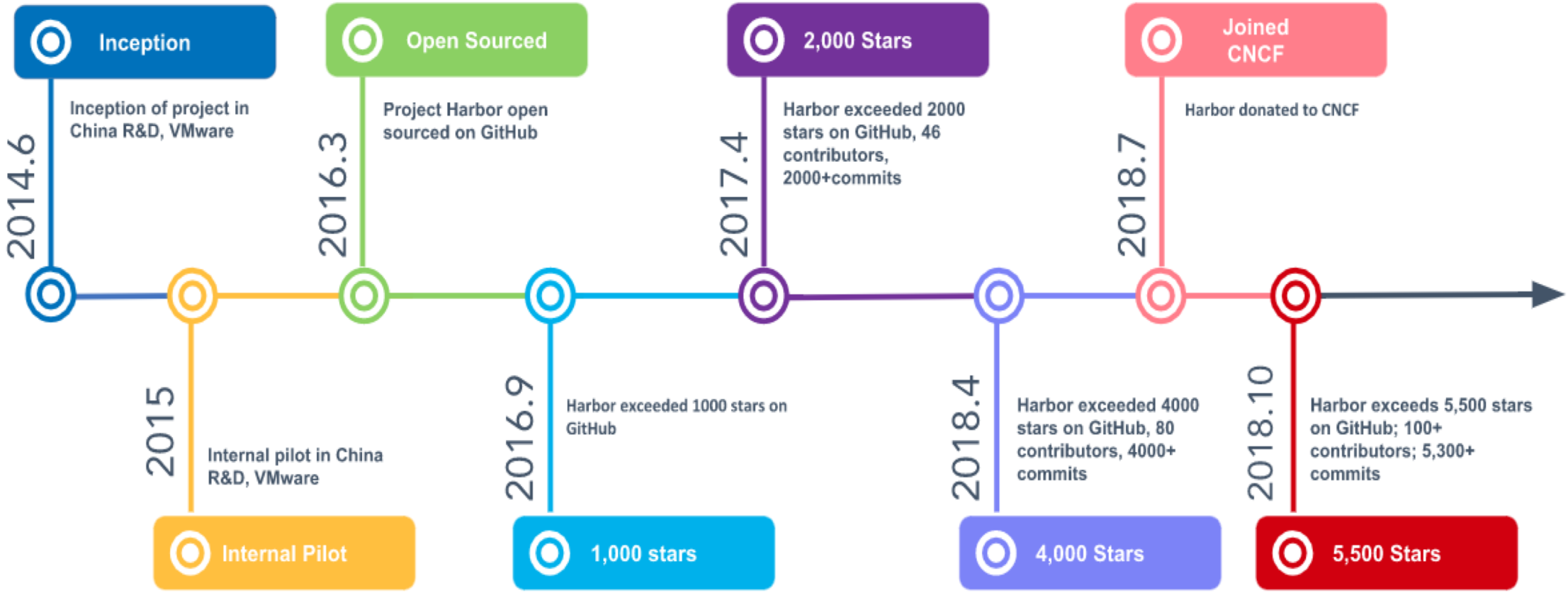
Apache 2.0 license



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

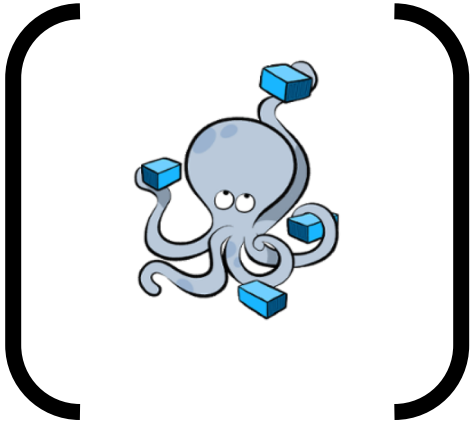
CLOUD FOUNDRY DAYS

History of Project Harbor



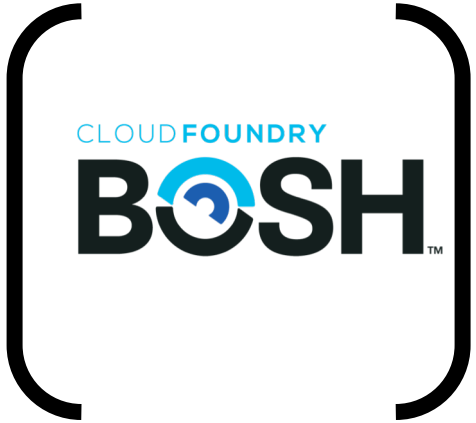
CLOUD FOUNDRY DAYS

Harbor Deployment Approaches



DOCKER COMPOSE

on single host



BOSH RELEASE

or PCF TILE

on Cloud Foundry Bosh Director



HELM CHART

on Kubernetes

What is Cloud Foundry BOSH



BOSH is a project that unifies release engineering, deployment, and lifecycle management of small and large-scale cloud software. BOSH can provision and deploy software over hundreds of VMs. It also performs monitoring, failure recovery, and software updates with zero-to-minimal downtime.

While BOSH was developed to deploy **Cloud Foundry PaaS**, it can also be used to deploy almost any other software. BOSH is particularly well-suited for large distributed systems.

In addition, BOSH supports multiple Infrastructure as a Service (**IaaS**) providers like

- VMware vSphere,
- Google Cloud Platform,
- Amazon Web Services EC2,
- Microsoft Azure,
- and OpenStack.

https://bosh.io/

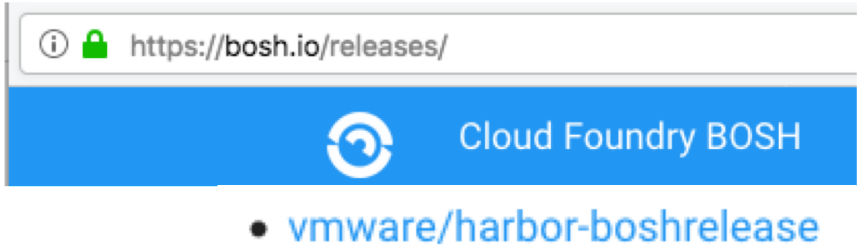
What is BOSH Release for Harbor

The BOSH Release for Harbor is used to deploy Harbor Docker Registry Server on Bosh Director.

- Open sourced on GitHub under Apache License v2 on Mar 2018.
- Source code https://github.com/vmware/harbor-boshrelease/
- Can be seamlessly integrated with container applications running in Cloud Foundry.

- Use Docker Compose to launch Harbor services on a VM created by BOSH Director.
- Monitor healthy status of Harbor services via monit

Harbor Bosh Release is officially published on https://bosh.io/releases/

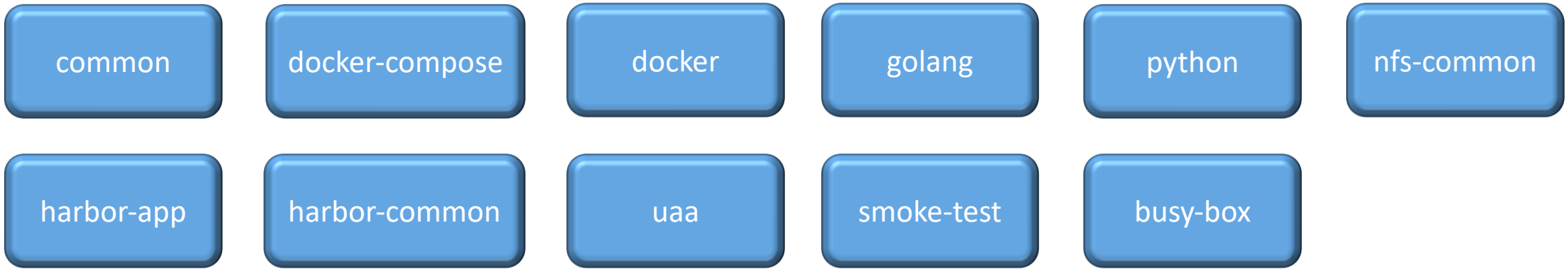


You can easily deploy Harbor in Cloud Foundry with the published Harbor Bosh Release:

```
bosh -n -d harbor-deployment deploy manifests/harbor.yml -v hostname=harbor.my.local
```

CLOUD FOUNDRY DAYS

Packages in Harbor BOSH Release

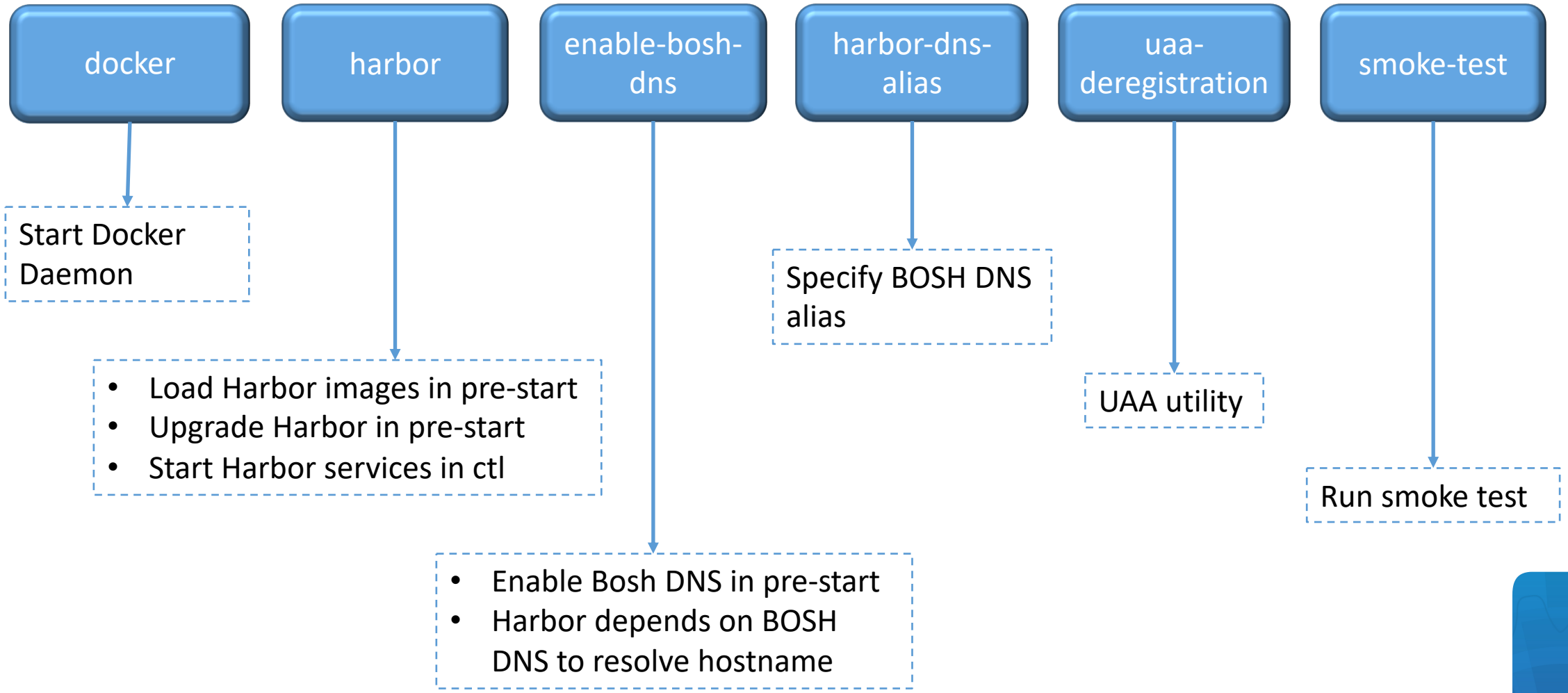


Using **bosh vendor-package** to easily vendor final version of a package from another release.
BOSH team has also created bosh-packages Github organization for tracking official commonly used packages: golang-release, ruby-release, java-release, python-release and nginx-release.

https://bosh.io/docs/package-vendoring/

CLOUD FOUNDRY DAYS

Jobs in Harbor BOSH Release



CLOUD FOUNDRY DAYS

Techniques & Good Practice

Some techniques and good practice used in Harbor Bosh Release.

- Service Failure Recovery via monit
- Utilize Pre-start script for one-time tasks
- Utilize Bosh DNS for DNS resolution cross services

CLOUD FOUNDRY DAYS

Service Failure Recovery via monit

When starting harbor job, add a cron job to run the status check script every 2 seconds:

*/2 * * * * root /var/vcap/jobs/harbor/bin/status_check

If Harbor Service is not responding correctly, status_check script will delete the harbor.pid file.

As a result, bosh monit daemon (defined in monit spec for harbor job) detects harbor.pid is gone, then restart Harbor Service.

monit spec for harbor job:

```
check process harbor with pidfile /var/vcap/sys/run/harbor/harbor.pid
  group vcap
  start program "/var/vcap/jobs/harbor/bin/ctl start" with timeout 300 seconds
  stop program "/var/vcap/jobs/harbor/bin/ctl stop" with timeout 180 seconds
  depends on dockerd
  depends on harbor-enable-bosh-dns
```

CLOUD FOUNDRY DAYS

Utilize Pre-start script

A Bosh Release job can have a pre-start script that will run before the job is started by 'ctl start' script. This pre-start script allows the job to prepare machine and/or persistent data before starting its operation.

Bosh will run pre-start scripts of all Bosh jobs on the VM in parallel, then run 'ctl start' script of all Bosh jobs in the specific order.

The pre-start script will not run when running 'monit start', but only run when running 'bosh deploy'. So when monit detects job failure, it will run 'monit start', but not pre-start script.

We use pre-start script to perform the following tasks in Harbor Bosh Release:

- Configure Harbor service. This task is needed only once.
- Load Harbor docker images from a tar file. This task is time consuming and needed only once.
- Upgrade Harbor from old version to new version. This task is needed only once.
- UAA client registration. This task is needed only once.
- etc.

https://bosh.io/docs/pre-start/

Utilize Bosh DNS

Bosh DNS provides native DNS support for bosh jobs. It's similar to the DNS support in K8s and Docker Compose.

Bosh DNS job is usually configured as a Bosh add-on and runs on every Bosh nodes. The Bosh DNS service is started in its own pre-start script.

Harbor Bosh Release uses Bosh DNS to resolve:

- FQDN of Harbor Service
- FQDN of UAA Service

These services must be accessed via FQDN (not IP).

Installing a dns/aliases.json file in harbor bosh release job. By default, bosh-dns will glob local /var/vcap/jobs/*/dns/aliases.json files for bosh dns aliases.

The FQDN pattern matches the internal Bosh FQDN generated by Bosh for each bosh instance.
e.g. uaa.server.local will be resolved to the IP of the Bosh instance VM whose internal Bosh FQDN is <uuid>.uaa-app.deployment-network.uaa-deployment.bosh.

```
addons:
- name: harbor-bosh-dns
  jobs:
  - name: harbor-dns-aliases
    release: harbor-container-registry
    properties:
      aliases:
        ((hostname)):
        - "*.harbor-app.deployment-network.harbor-deployment.bosh"
        uaa.server.local:
        - "*.uaa-app.deployment-network.uaa-deployment.bosh"
- name: enable-bosh-dns
  jobs:
  - name: enable-bosh-dns
    release: harbor-container-registry
```

Thank You

Q&A



CLOUD
FOUNDRY
DAYS