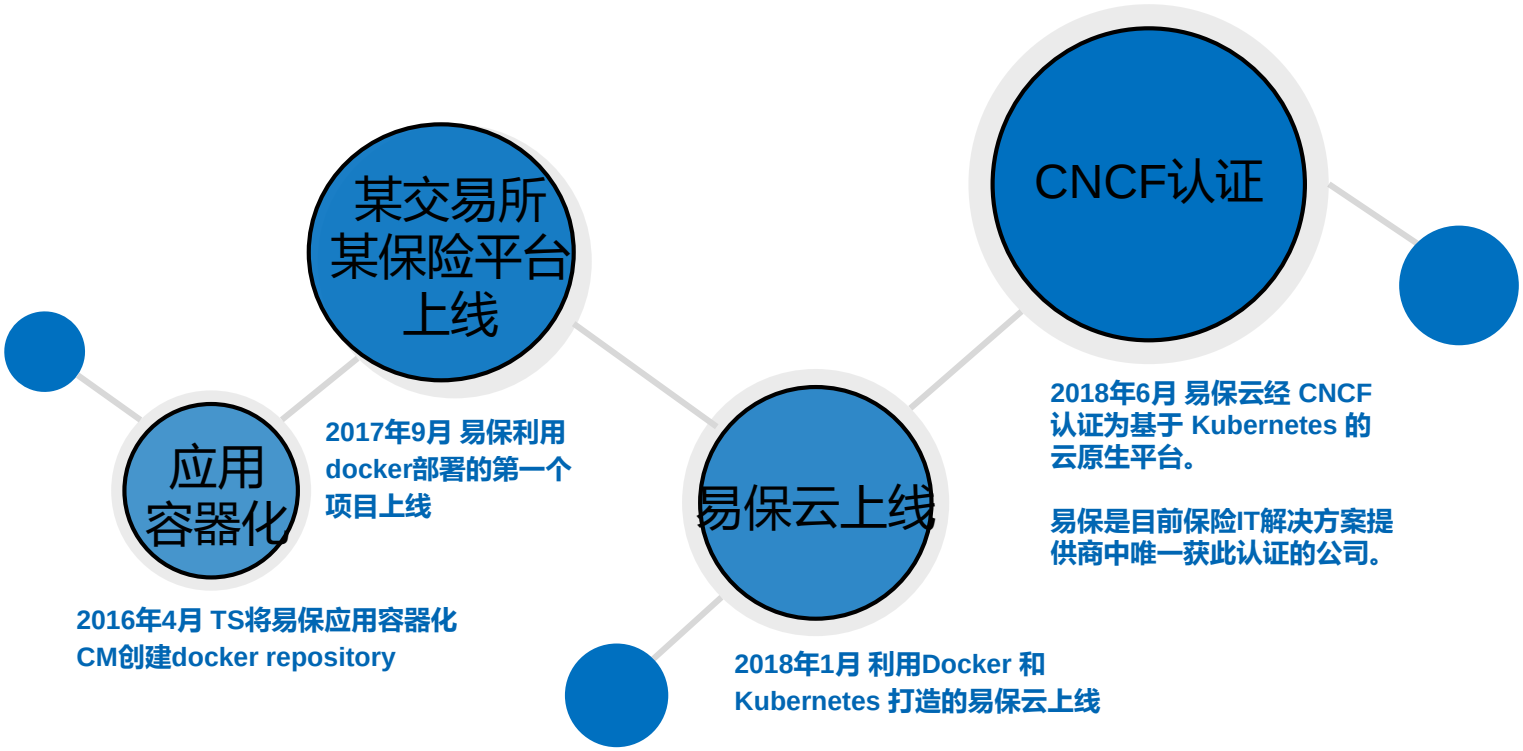
易保容器化之路

xiaojun.wu@ebaotech.com
吴小军(github/wechat：nhwuxiaojun)
July, 2018

里程碑

里程碑



Company Confidential. Copyright 2016 eBaoTech Corporation. All rights reserved.

易保为什么选择docker

我们的痛点：

- 越来越多的机器，过保的机器用的心惊胆战
- 环境对机器的依赖性很高，服务器维护，影响面大
- 多种不同版本操作系统的升级麻烦
- 服务无法实现弹性水平扩展，资源的调整会导致环境的不可用
- 无法动态调整资源，资源的使用率低。
- 环境配置不一致，导致问题排查困难

Company Confidential. Copyright 2016 eBaoTech Corporation. All rights reserved.

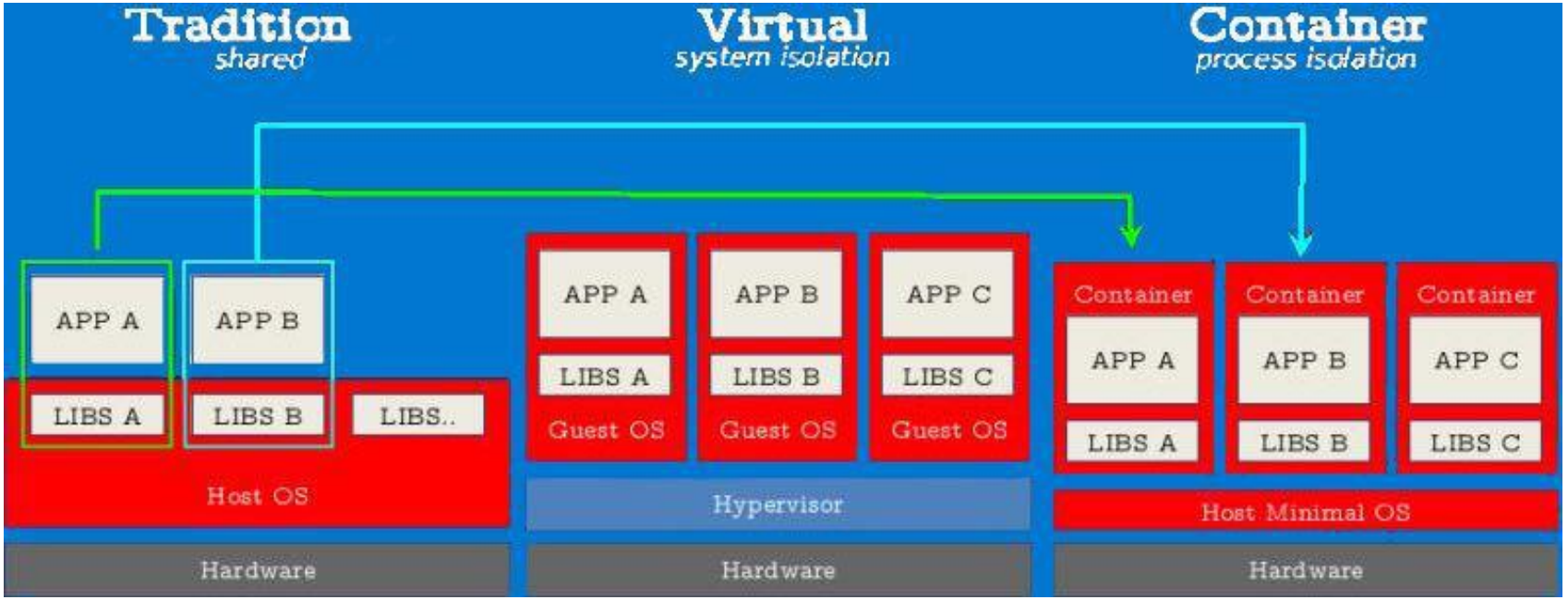
我们的需求：

- NS虚拟化 → 提升性能节约成本
- 启动速度快 → 快速部署环境
- 镜像分层技术 → 更快的部署扩容
- CI环境构建 → 测试生产环境统一

Company Confidential. Copyright 2016 eBaoTech Corporation. All rights reserved.

Docker 应用于基础架构

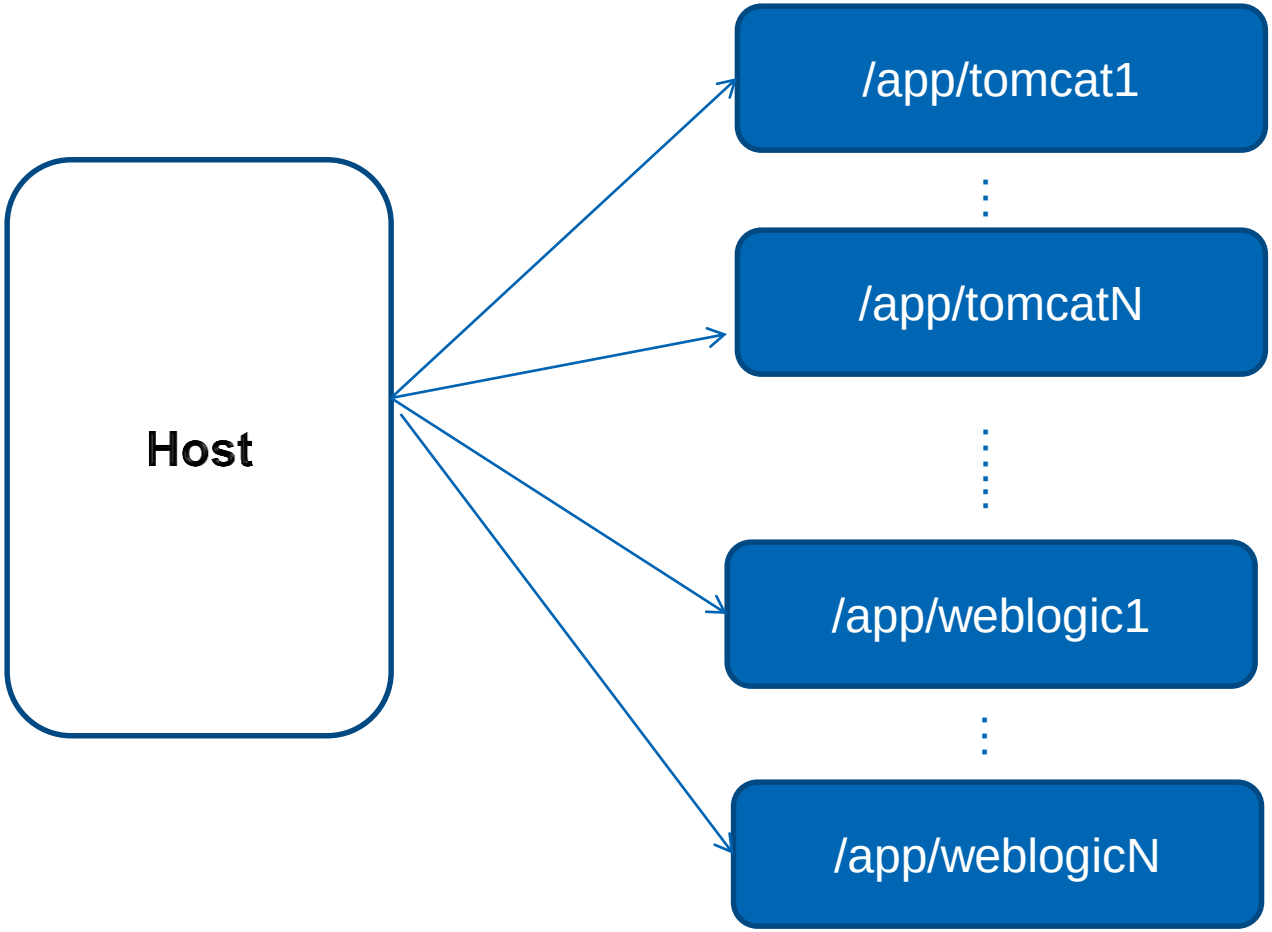
基础架构的变迁



Buy Less Server, Run More Environments

Company Confidential. Copyright 2016 eBaoTech Corporation. All rights reserved.

传统的环境分配方式

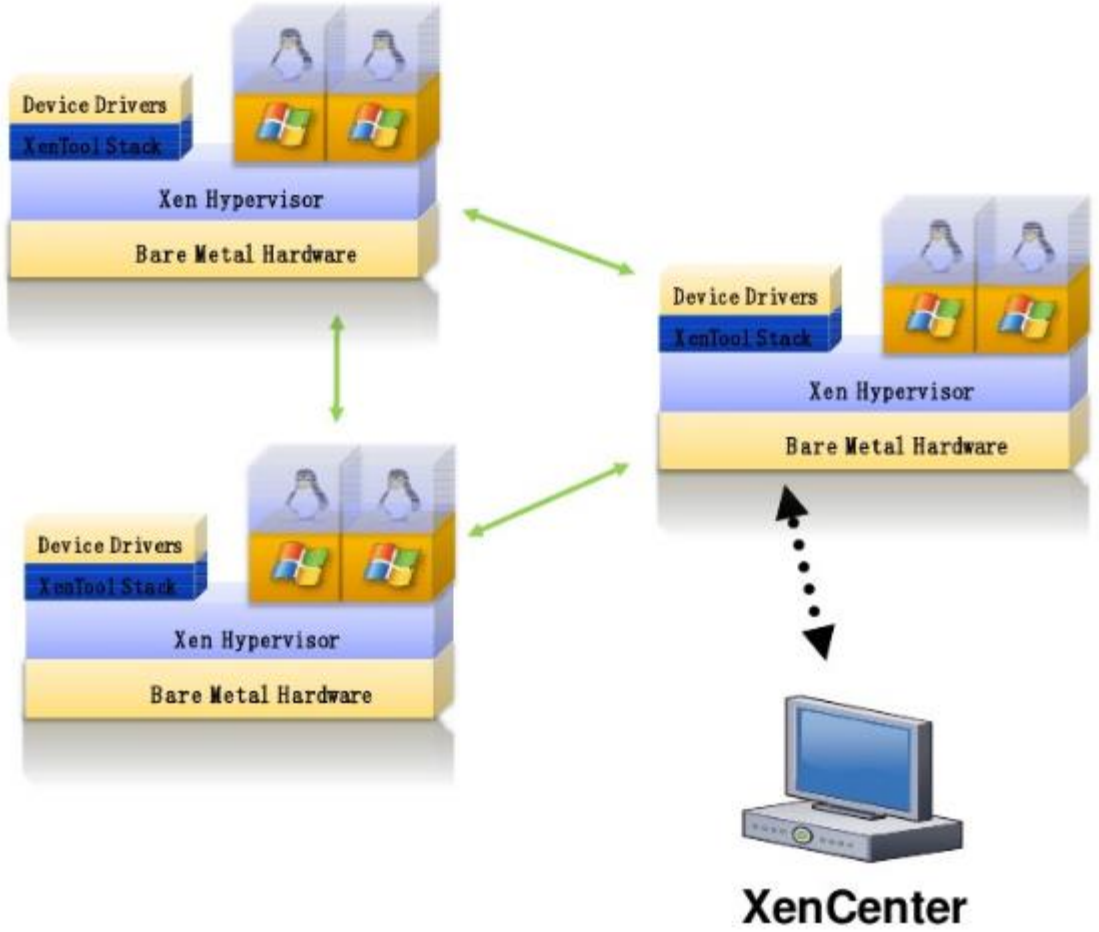


Every Instanace have one virtual IP

Company Confidential. Copyright 2016 eBaoTech Corporation. All rights reserved.

虚拟化

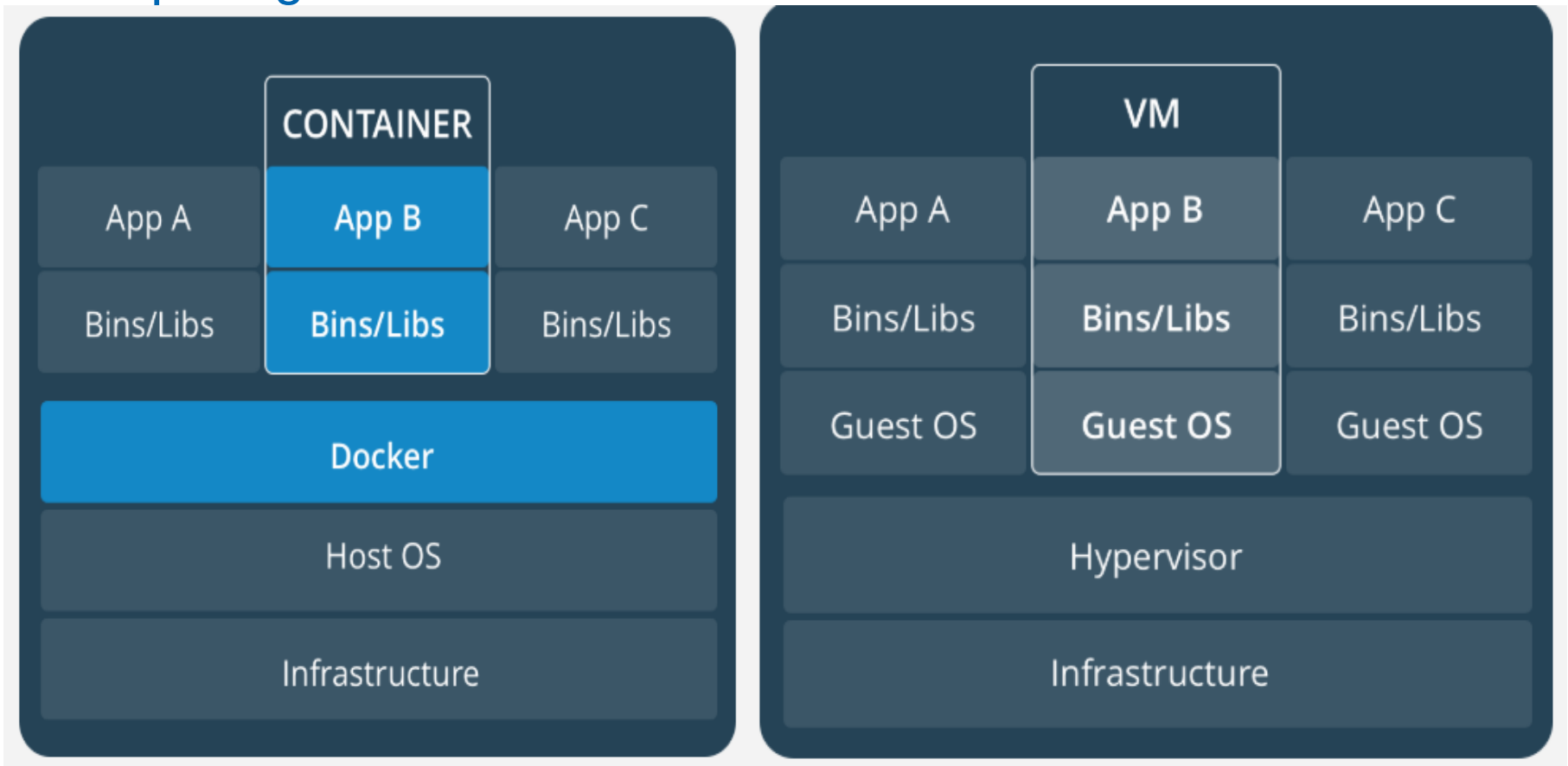
Xenserver



Company Confidential. Copyright 2016 eBaoTech Corporation. All rights reserved.

容器

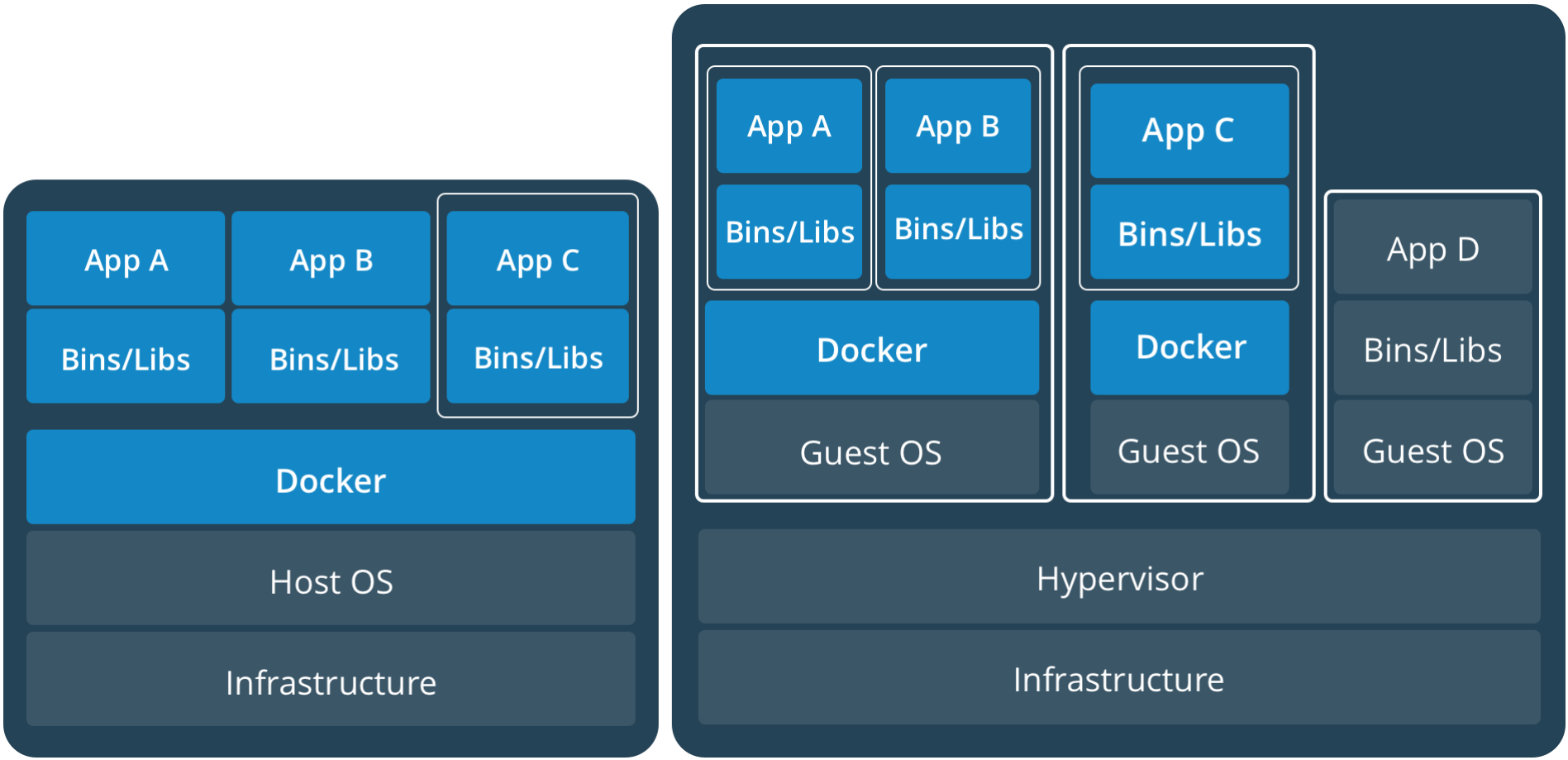
Comparing Containers and Virtual Machines



Company Confidential. Copyright 2016 eBaoTech Corporation. All rights reserved.

现在的基础架构

虚拟机+容器



Company Confidential. Copyright 2016 eBaoTech Corporation. All rights reserved.

CI/CD

发布方式的改变

更轻，更快，更稳定

SSH

Jenkins 从svn或git取包后SSH到应用服务器

Salt

Jenkins调用利用Salt master来传输发布包，再到minion上执行发布

Kubelet

Jenkins 调用Master kubelet 来执行发布， Node会根据版本更新下载新的镜像

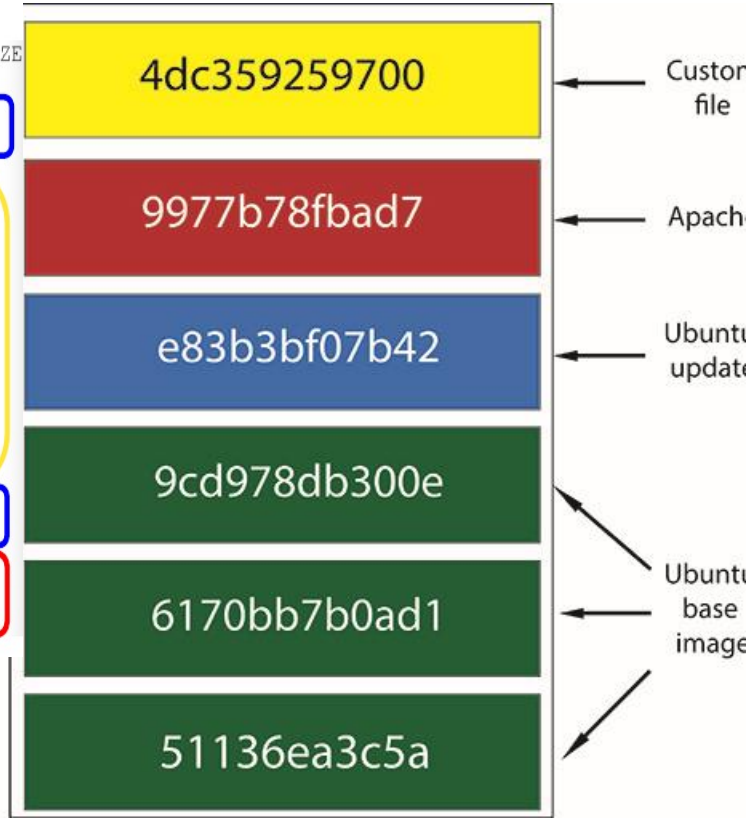
Jenkins

Company Confidential. Copyright 2016 eBaoTech Corporation. All rights reserved.

发布的镜像

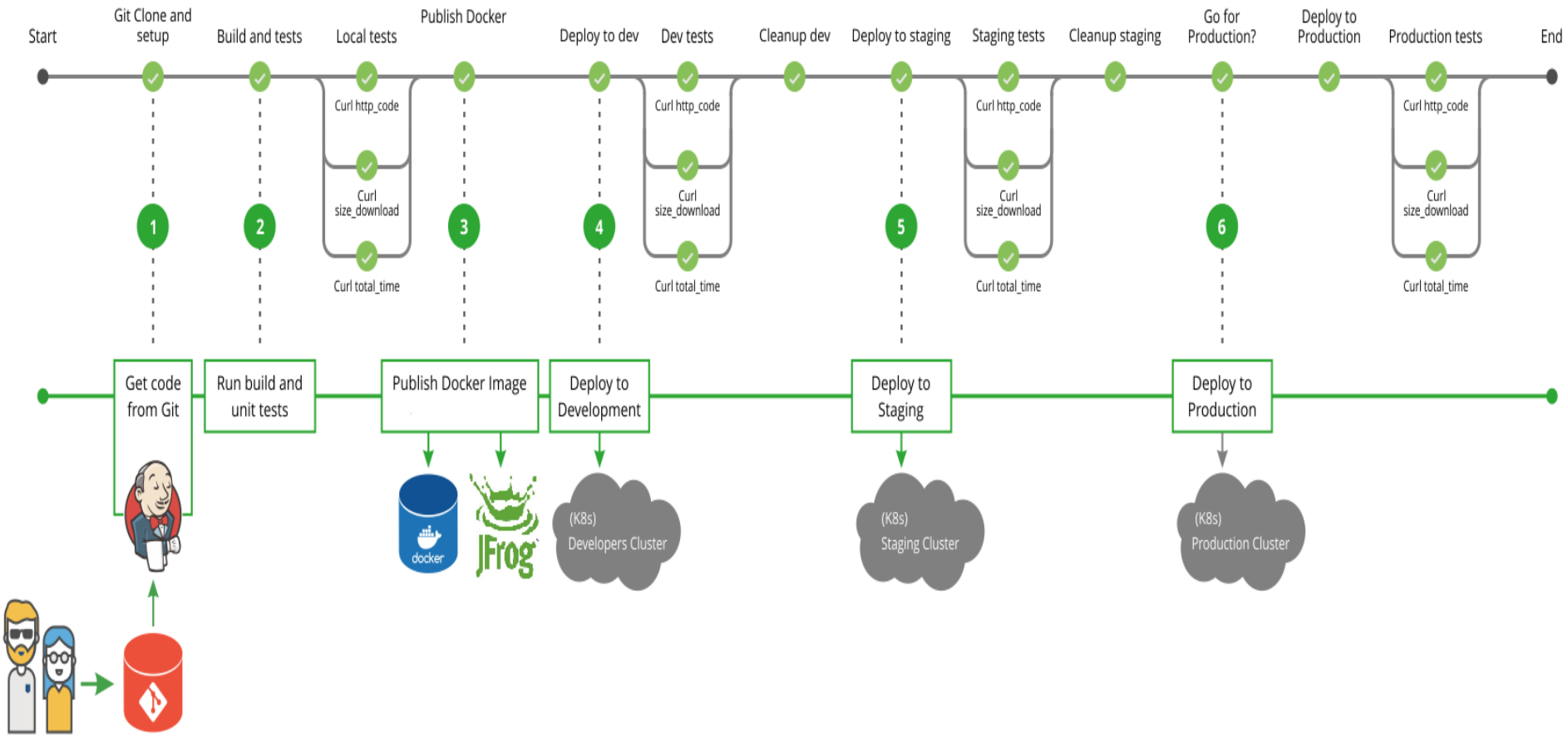
version control for environment

	REPOSITORY	TAG	IMAGE ID	CREATED	VIRTUAL SIZE
服务镜像	root/ssh	centos7	d9bc1aa19308	13 minutes ago	248.9 MB
	root/registry.v2	centos7	32f3a32ff36c	14 minutes ago	261.6 MB
	root/registry	centos7	52a0614bc222	14 minutes ago	325 MB
	root/redis	centos7	ba455f28fcfa	17 minutes ago	281.6 MB
应用镜像	root/rabbitmq	centos7	f4a99ff0bc9b	18 minutes ago	321.2 MB
	root/python	centos7	5cf4e9e2f3c4	19 minutes ago	290.1 MB
	root/pys3qlfs	centos7	b8e1d7cc48f4	21 minutes ago	514.9 MB
	root/postgres	centos7	e99ea4e190d7	22 minutes ago	358.7 MB
	root/owncloud	centos7	f2fa562864e8	25 minutes ago	465.3 MB
	root/nginx	centos7	c42b889f6114	27 minutes ago	340.6 MB
	root/mongodb	centos7	13015d8d52d9	30 minutes ago	315.5 MB
	root/memcached	centos7	ff5a78746657	31 minutes ago	320.3 MB
	root/lighttpd	centos7	907407b160a2	33 minutes ago	286.9 MB
	root/hadoop	centos7	f4e86ee66aba	36 minutes ago	1.068 GB
	root/bind	centos7	5c0576170acf	49 minutes ago	293.3 MB
系统镜像	root/kube2sky	busybox	53362966aeca	About an hour ago	24.9 MB
	root/skydns	busybox	86b3868a11c5	About an hour ago	13.99 MB
基础镜像	wanda/centos7	latest	d94236583afc	About an hour ago	245.2 MB
	wanda/ubuntu	14.04	933b7553ece8	About an hour ago	228.3 MB
	wanda/busybox	latest	545487ff61fe	About an hour ago	973.2 kB



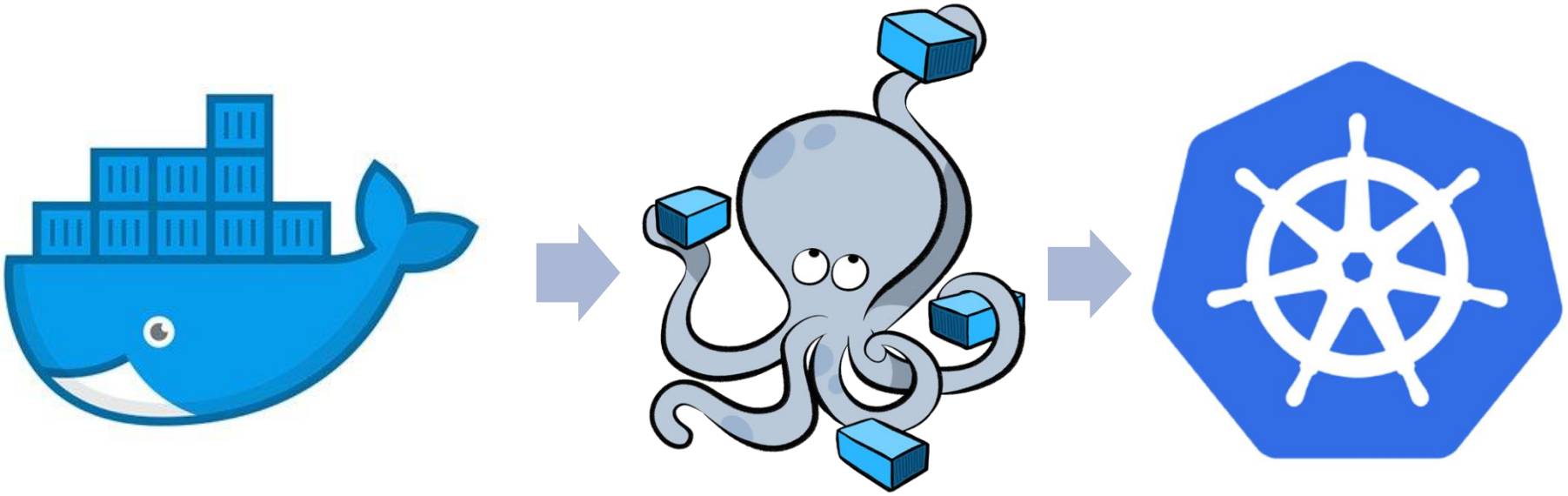
Company Confidential. Copyright 2016 eBaoTech Corporation. All rights reserved.

Automate CI/CD Pipeline With Jenkins,Gitlab, JFrog and Kubernetes



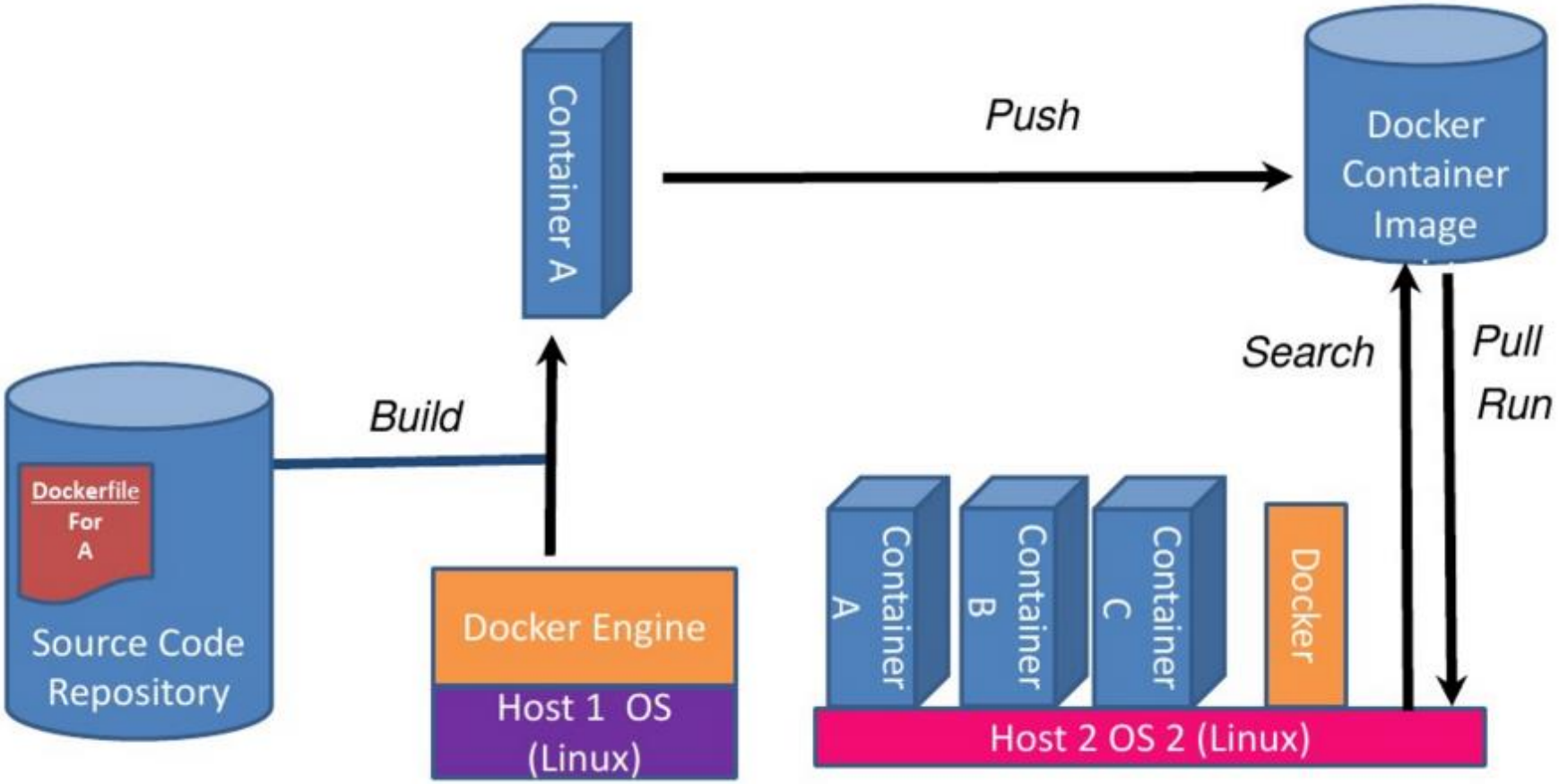
Docker，Docker Compose，Kubernetes

K8S之路



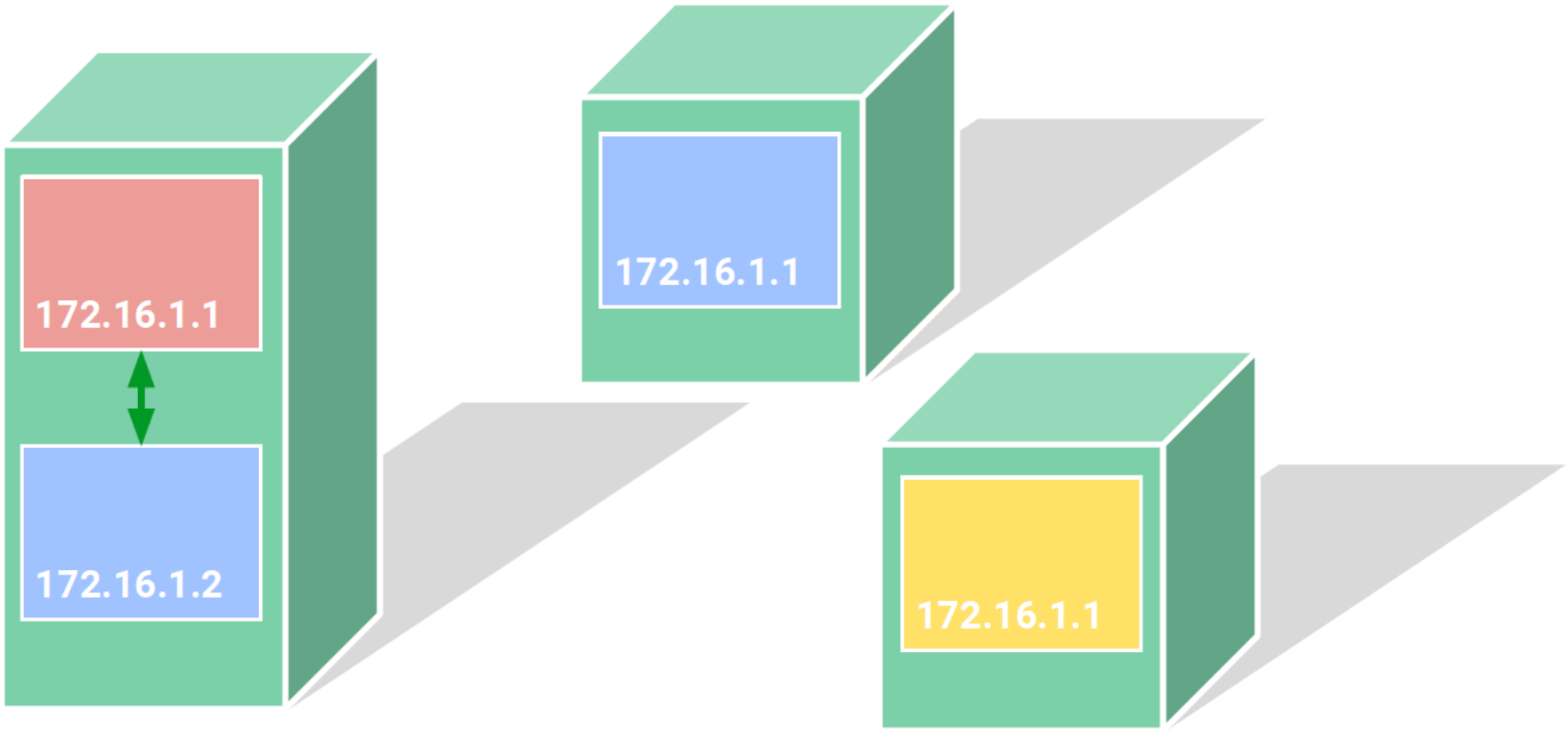
Company Confidential. Copyright 2016 eBaoTech Corporation. All rights reserved.

容器的构建流程



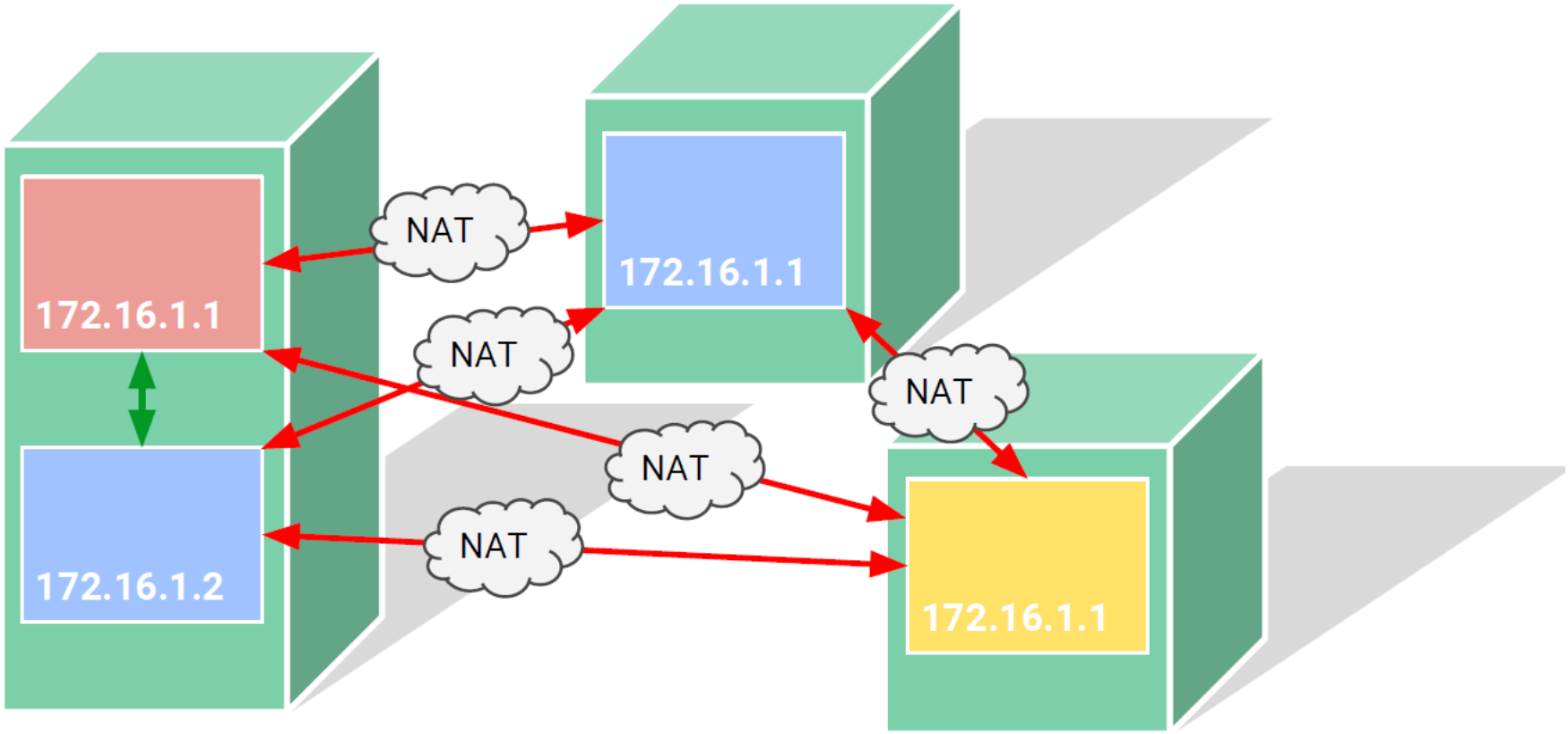
Company Confidential. Copyright 2016 eBaoTech Corporation. All rights reserved.

Docker 网络：bridge



Company Confidential. Copyright 2016 eBaoTech Corporation. All rights reserved.

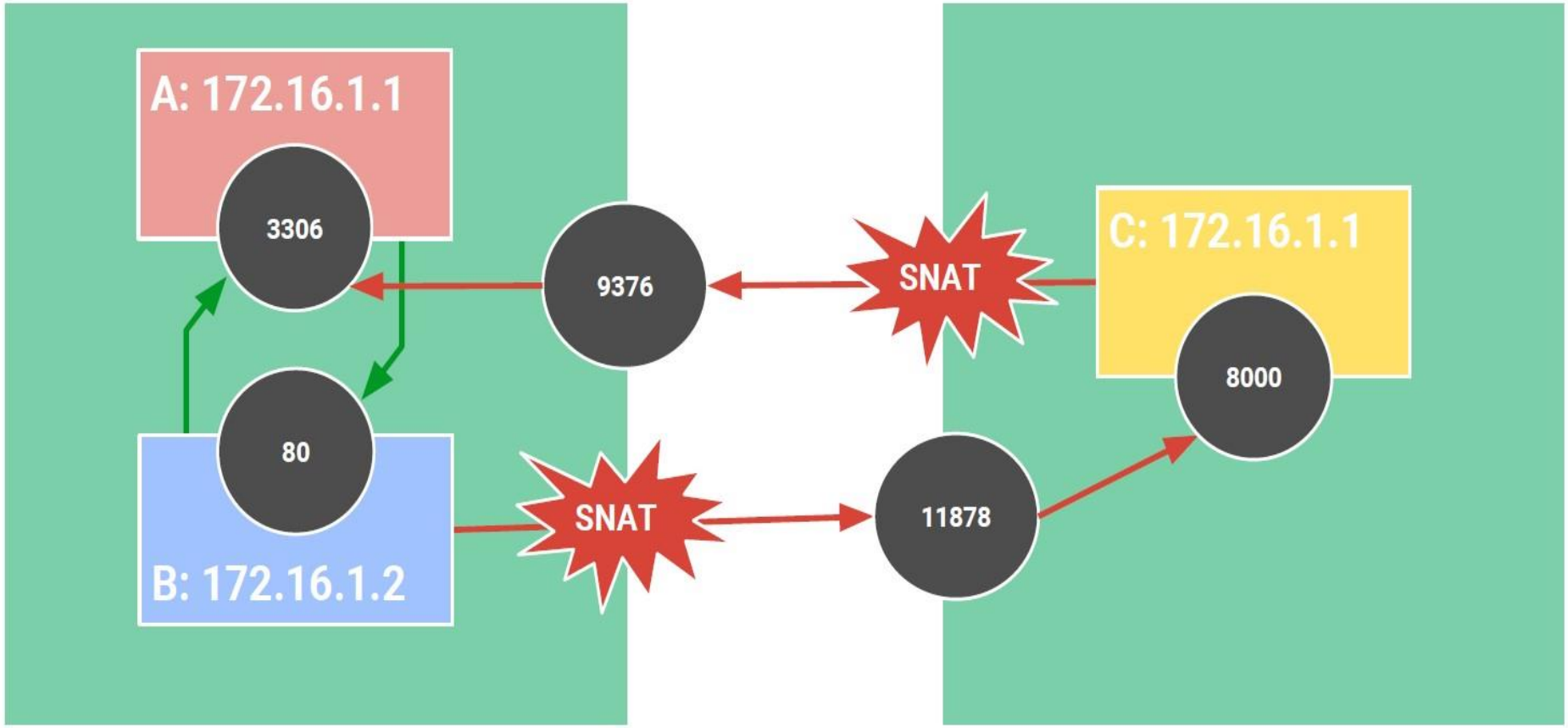
Docker 网络： Nat



eBaoTech
make insurance easy

Company Confidential. Copyright 2016 eBaoTech Corporation. All rights reserved.

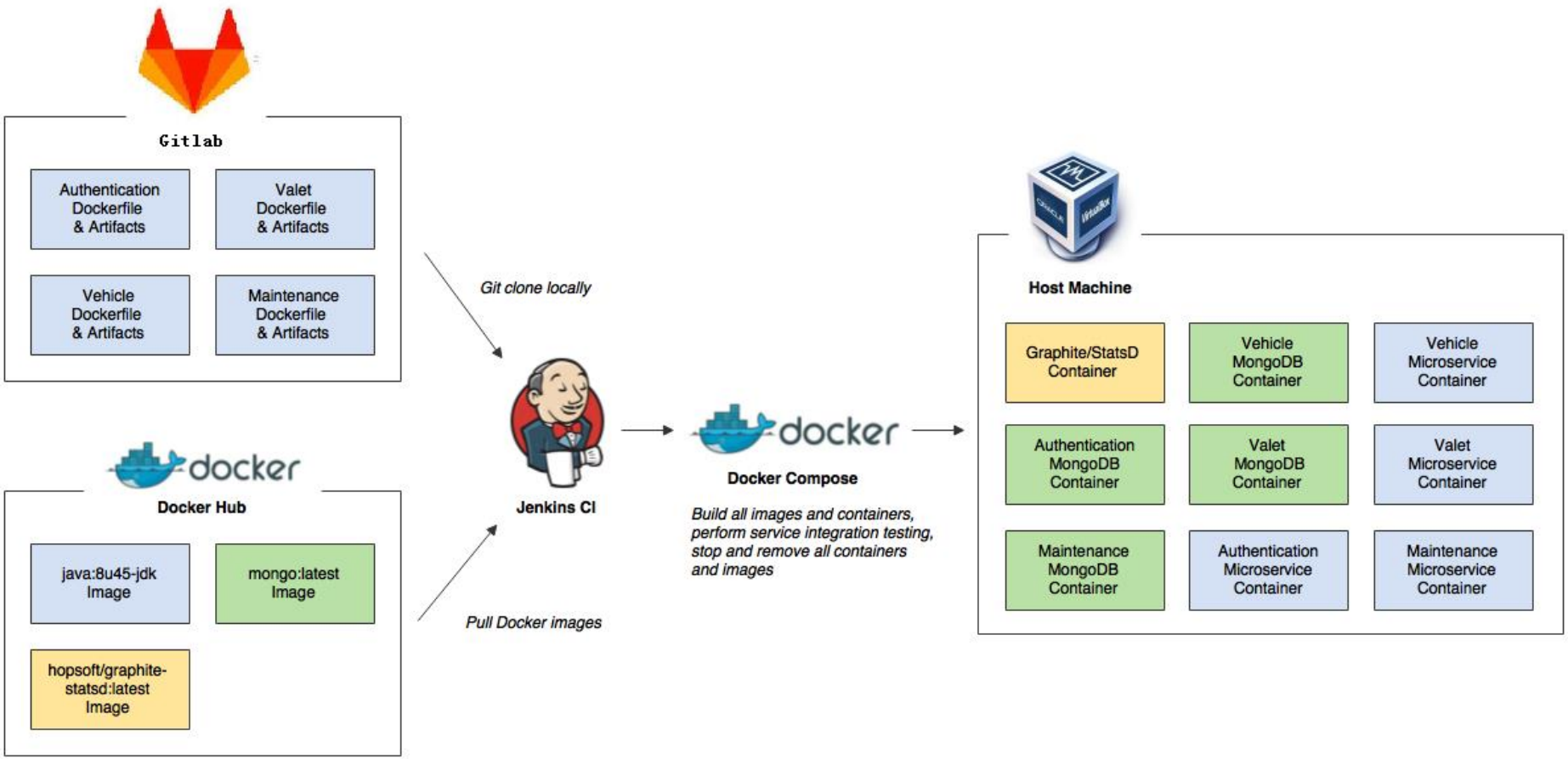
Docker 网络：端口映射



eBaoTech
make insurance easy

Company Confidential. Copyright 2016 eBaoTech Corporation. All rights reserved.

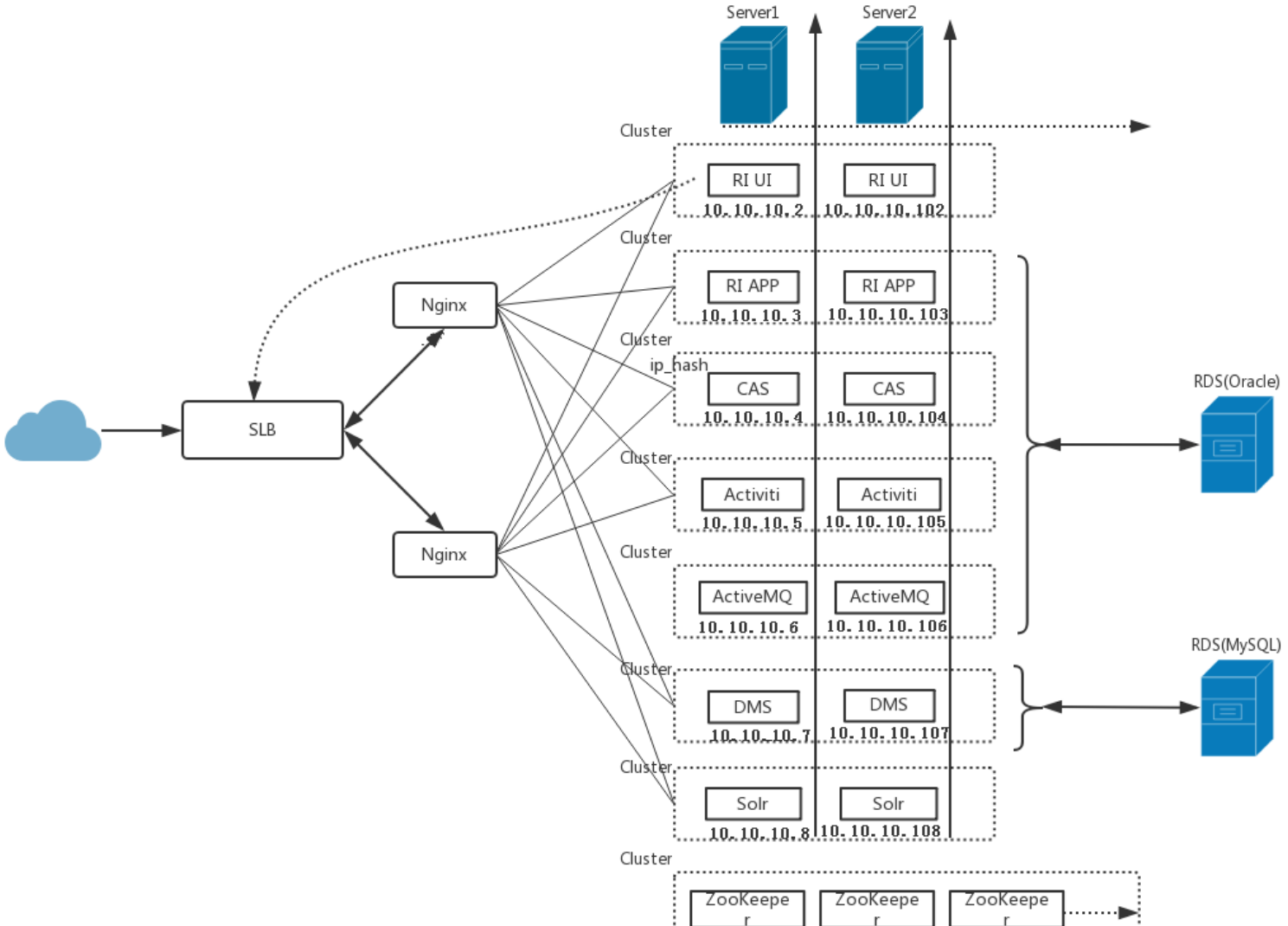
Docker-compose



Company Confidential. Copyright 2016 eBaoTech Corporation. All rights reserved.

Docker-compose的应用

Docker as VM



Docker-compose的应用

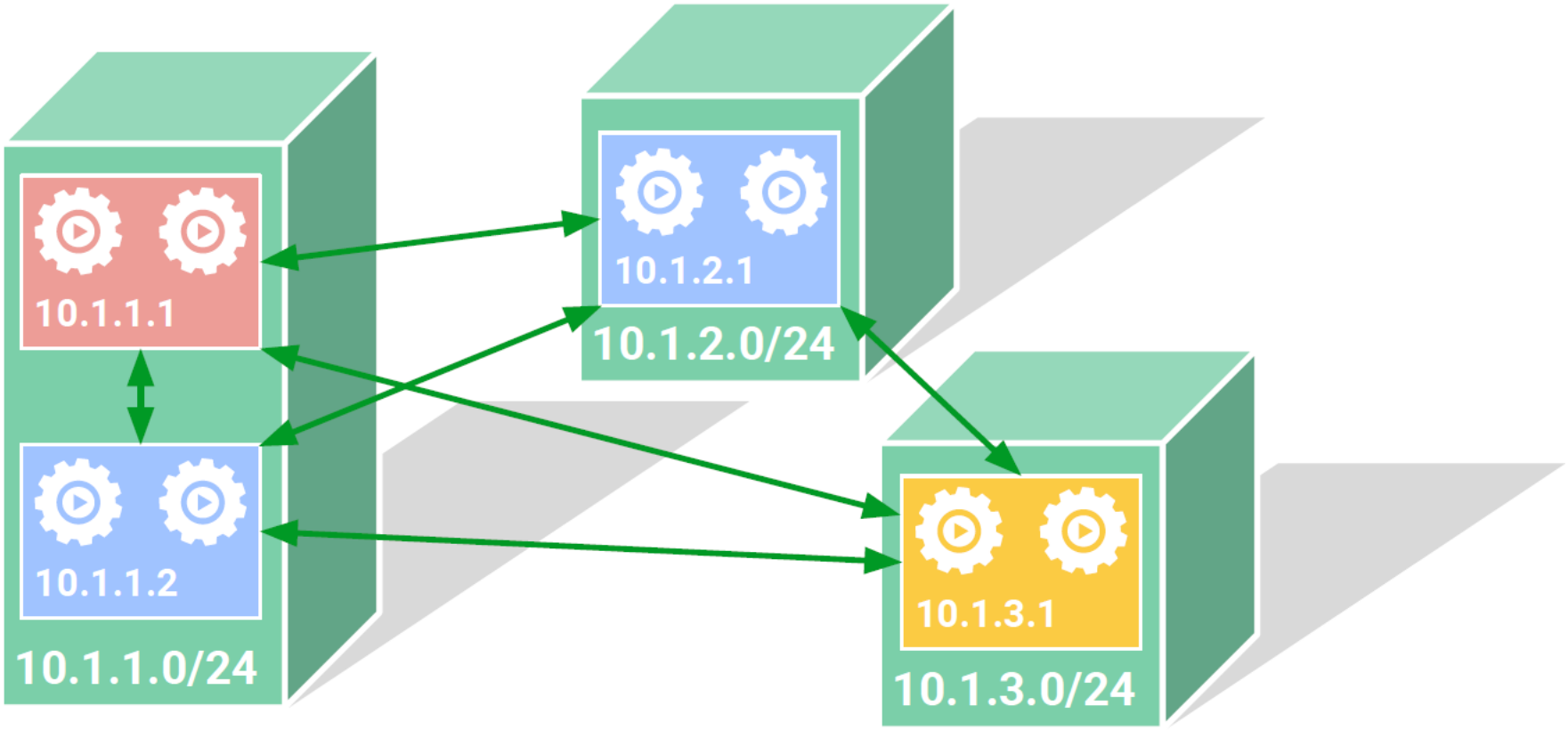
Docker as VM

```
version: '3'
services:
  cas:
    container_name: cas
    image: dockerhub.ebaotech.com/cas:v1.6.8
    networks:
      testing_net:
        ipv4_address: 10.10.10.4
  activemq:
    container_name: activemq
    image: dockerhub.ebaotech.com/activemq:v1.6.8
    networks:
      testing_net:
        ipv4_address: 10.10.10.6
  solr:
    container_name: dockerhub.ebaotech.com/solr:v1.6.8
    image: some:image
    networks:
      testing_net:
        ipv4_address: 10.10.10.8

networks:
  prod_net:
    ipam:
      driver: default
      config:
        - subnet: 10.10.10.0/24
```

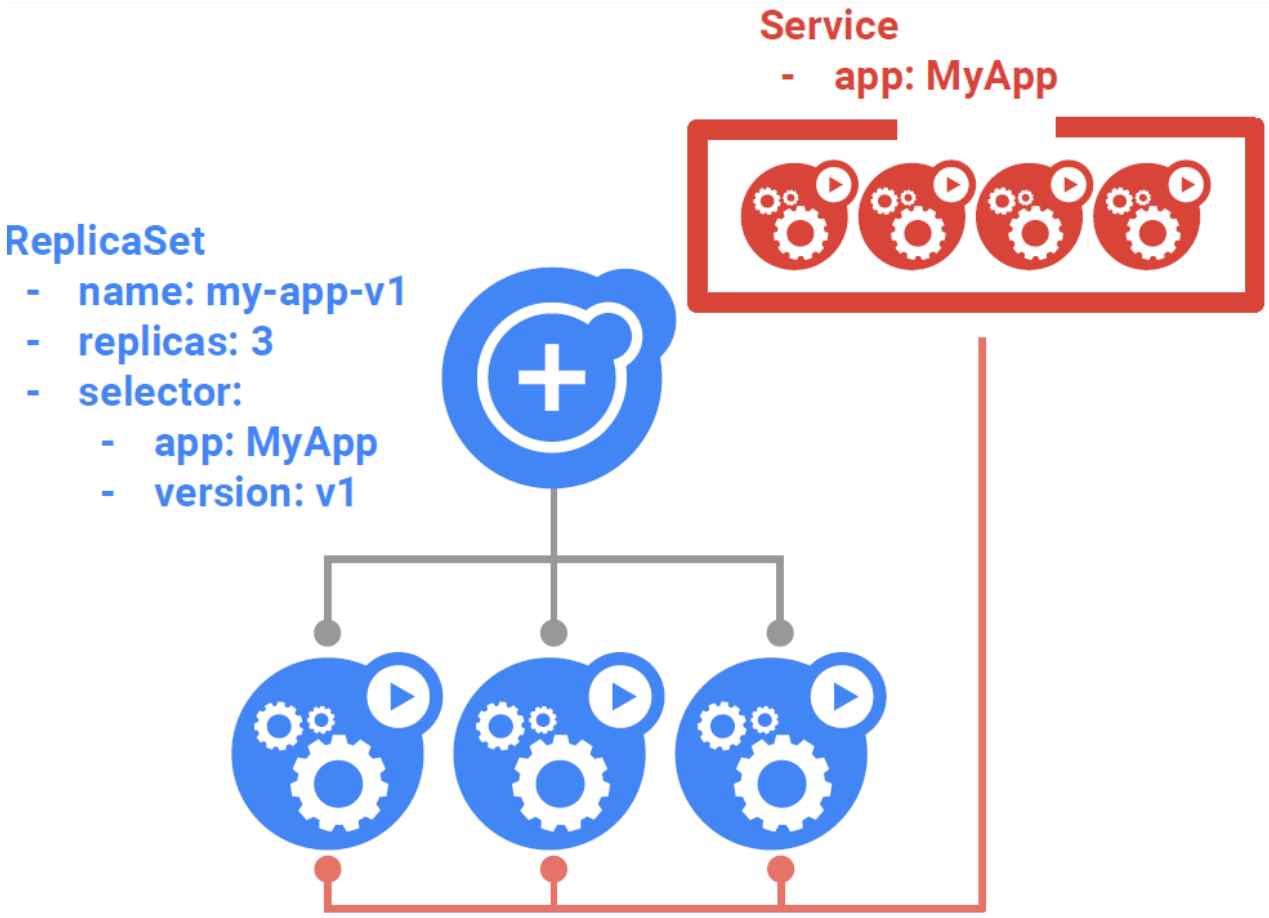

Company Confidential. Copyright 2016 eBaoTech Corporation. All rights reserved.

Kubernetes 网络



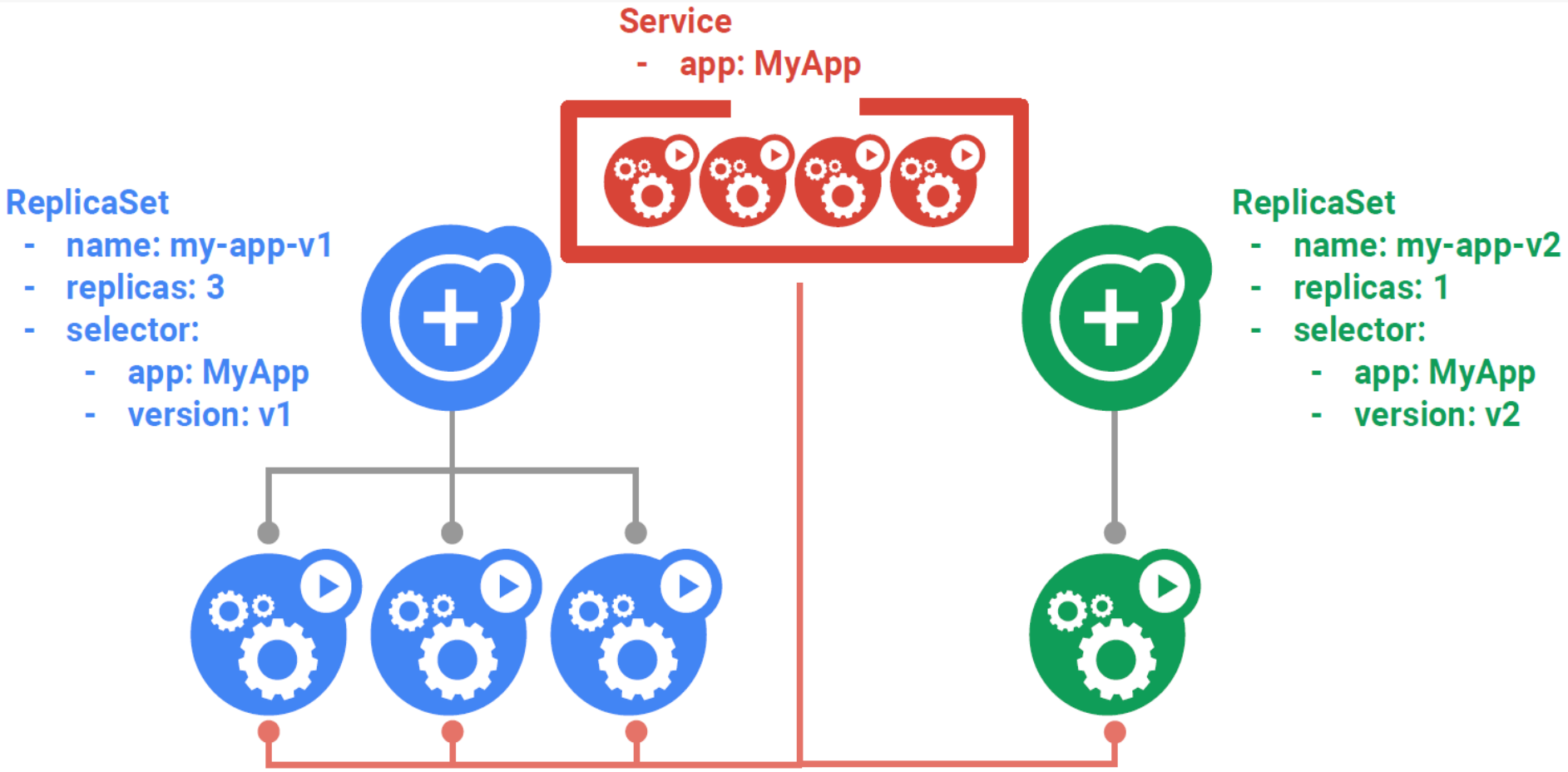
Company Confidential. Copyright 2016 eBaoTech Corporation. All rights reserved.

Kubernetes Rolling Update



Company Confidential. Copyright 2016 eBaoTech Corporation. All rights reserved.

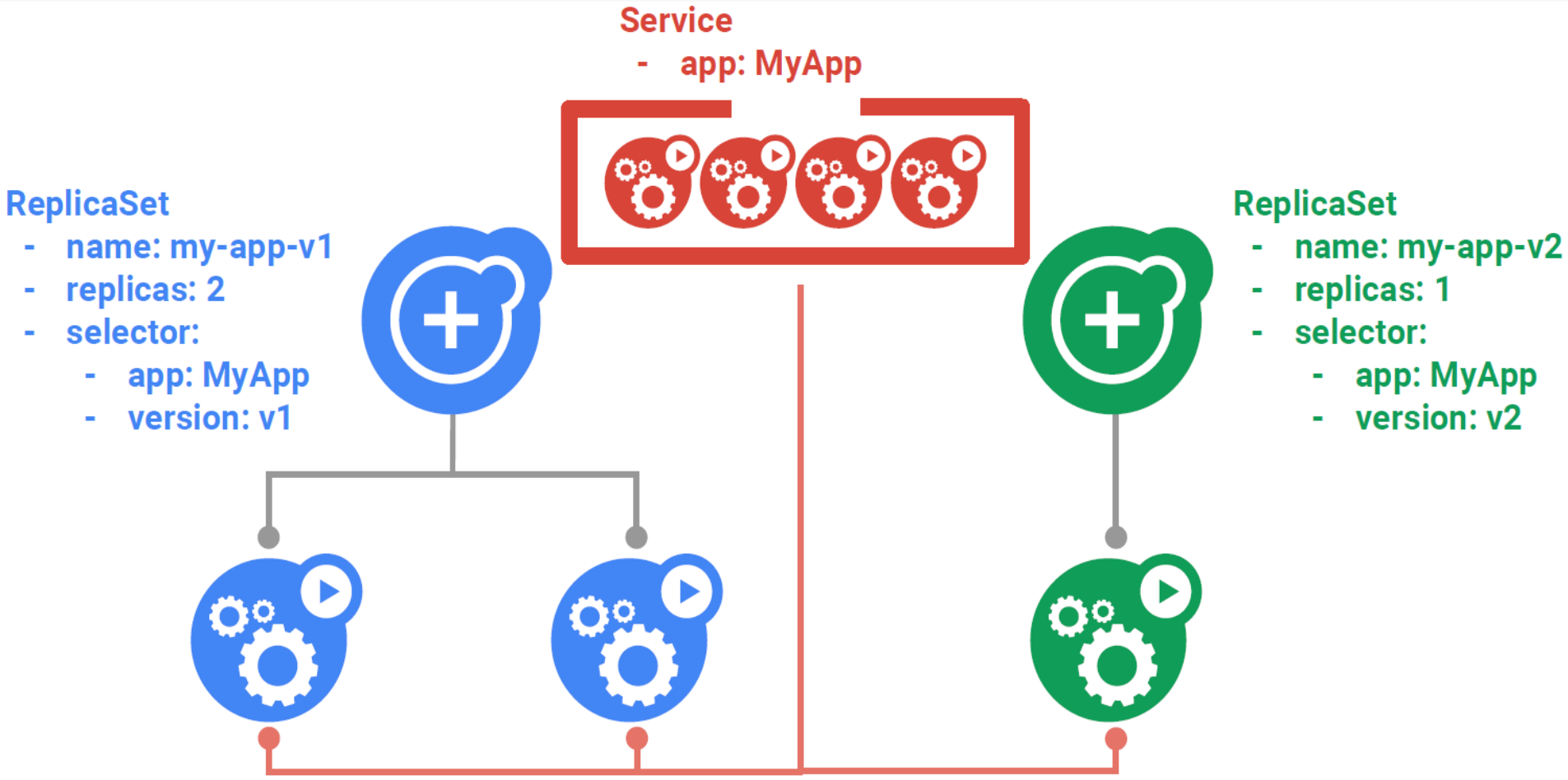
Kubernetes Rolling Update



eBaoTech®
make insurance easy

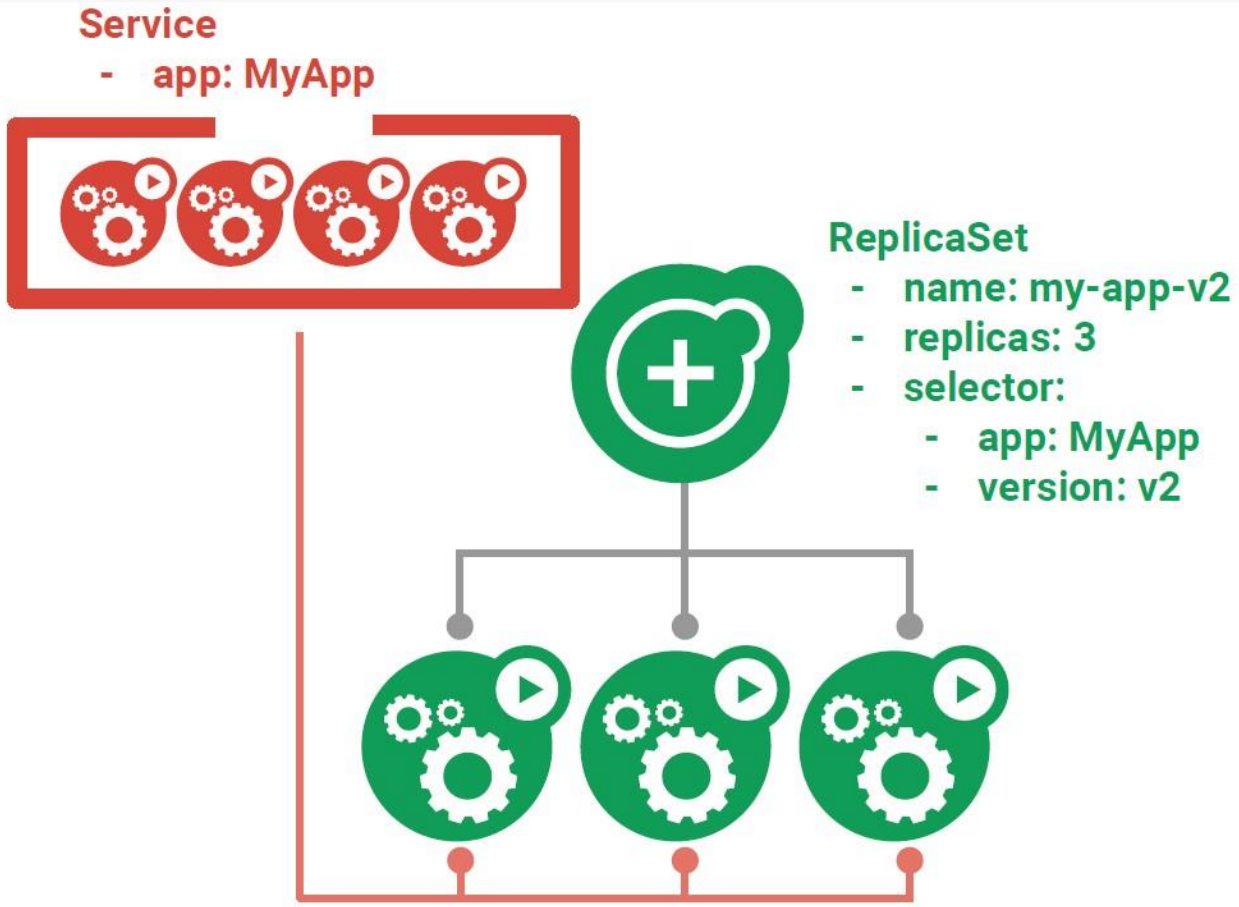
Company Confidential. Copyright 2016 eBaoTech Corporation. All rights reserved.

Kubernetes Rolling Update



Company Confidential. Copyright 2016 eBaoTech Corporation. All rights reserved.

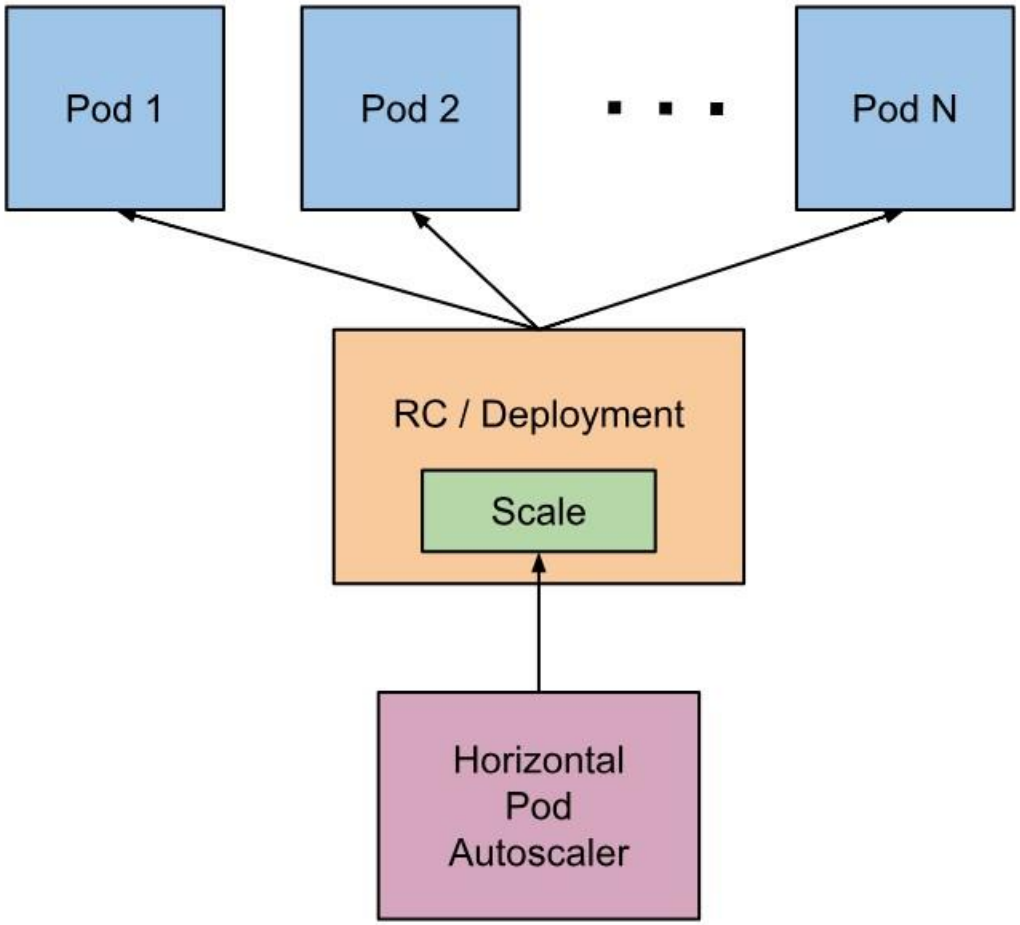
Kubernetes Rolling Update



Company Confidential. Copyright 2016 eBaoTech Corporation. All rights reserved.

Kubernetes Autoscale

HPA（Horizontal Pod Autoscaling）



#kubectl autoscale deploy ghost --min=1 --max=10 --cpu-percent=20 -n dev

#kubectl get hpa -n dev
NAME REFERENCE TARGETS MINPODS MAXPODS REPLICAS AGE
ghost Deployment/ghost <unknown> / 20% 1 10 4 5m

eBaoTech®
make insurance easy
Company Confidential. Copyright 2016 eBaoTech Corporation. All rights reserved.

遇到的坑

坑

- Docker 从1.12升级到1.13遇到的跨Node的Pod无法通信问题
  1.Node上执行iptables-P FORWARD ACCEPT
  2. docker启动参数设置ExecStartPost=/usr/sbin/iptables-P FORWARD ACCEPT

- kubernetes1.9以前的版本，kubelet的cgroup-driver与docker设置的不一致导致无法启动
  1.sed -i "s/cgroup-driver=systemd/cgroup-driver=cgroupfs/g" /etc/systemd/system/kubelet.service.d/10-kubeadm.conf

- Kubernetes 升级到1.8后，token过期问题
  1.Master初始化的时候 –token-ttl设置0
  2. kubeadm token create重新生成

- V1.11取消了Cadvisor 10255端口，导致监控获取不到数据
  1.V1.7-V1.10没有问题，建议不要升级

Company Confidential. Copyright 2017 eBaoTech Corporation. All rights reserved.

如何获取google镜像源

1. http proxy
2. RegistryMirror 来配置DaoCloud或者阿里云registry 镜像服务
3. docker hub 做中转
4. **将镜像压缩导入到本地**
5. k8s.gcr.io替换为registry.cn-hangzhou.aliyuncs.com/google_containers

Company Confidential. Copyright 2017 eBaoTech Corporation. All rights reserved.

需要注意的

应用中需要注意的

image	• 1.Do not use latest tag in production environment • 2.Do not build from latest image
Security	• Do not open external IP for kubernetes dashboard
Upgrade	• Test Test Test

Company Confidential. Copyright 2017 eBaoTech Corporation. All rights reserved.

CNCF认证

CNCF认证

eBaoCloud®
enable connected insurance

certified
kubernetes

CLOUD NATIVE
COMPUTING FOUNDATION

易保云经 CNCF 认证为基于 Kubernetes 的云原生平台

目前保险IT解决方案提供商中唯一获此认证的公司

https://www.ebaotech.com/cn/newsroom/newspages/%E6%98%93%E4%BF%9D%E4%BA%91%E7%BB%8F+CNCF+%E8%AE%A4%E8%AF%81%E4%B8%BA%E5%9F%BA%E4%BA%8E+Kubernetes+%E7%9A%84%E4%BA%91%E5%8E%9F%E7%94%9F%E5%B9%B3%E5%8F%B0

Company Confidential. Copyright 2017 eBaoTech Corporation. All rights reserved.

Demo Time

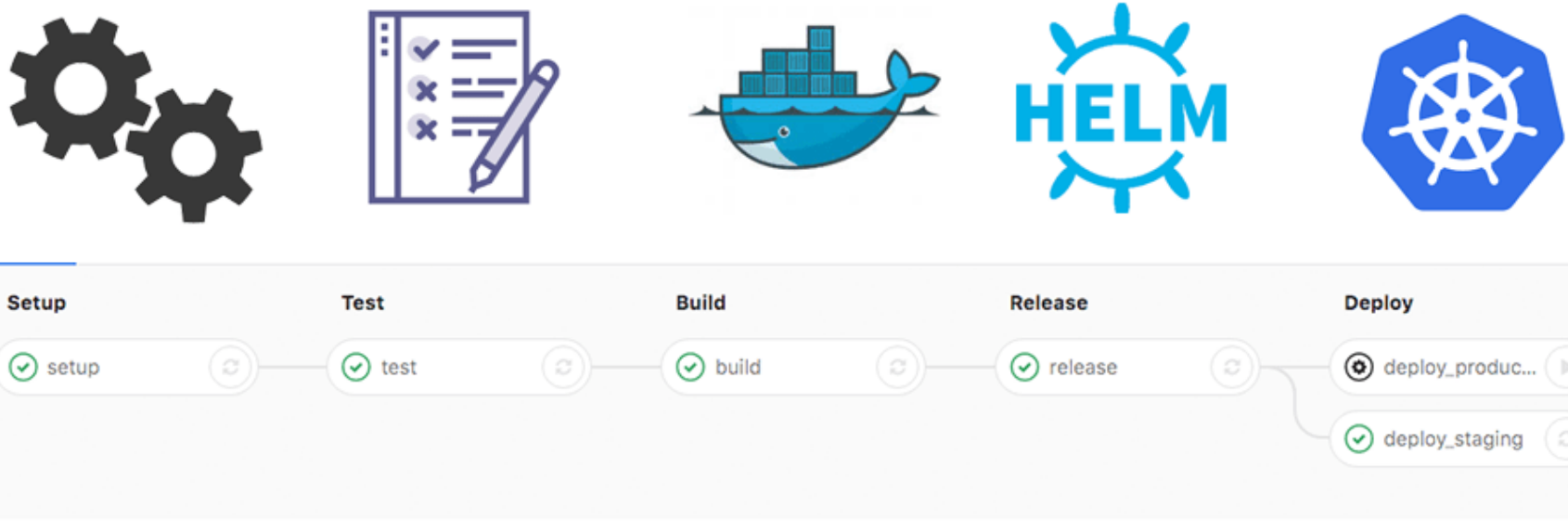
Demo for V1.9.3

Link： https://github.com/nhwuxiaojun/kubernetes-v1.9.3

Company Confidential. Copyright 2017 eBaoTech Corporation. All rights reserved.

Next

Helm



Company Confidential. Copyright 2017 eBaoTech Corporation. All rights reserved.

THANK YOU

eBaoTech®
make insurance easy

中国DevOpsDays社区

- 官方邮箱：organizer@ChinaDevOpsDays.org
- 官方网站：http://devopsdays.org
- 中文网站： http://chinadevopsdays.org

eBaoTech
make insurance easy

Company Confidential. Copyright 2017 eBaoTech Corporation. All rights reserved.