dockercon EU
BARCELONA • 16-17 NOVEMBER 2015

- Mathieu Buffenoir
  @MBuffenoir
- Sebastien Goasguen
  @sebgoa

A bitcoin broker on Docker

dockercon EU

Mathieu Buffenoir

CTO Bity.com

VP of Swiss Bitcoin Association

@MBuffenoir

Sebastien Goasguen

VP Apache CloudStack

Author of O'Reilly Docker cookbook

@sebgoa

dockercon EU

Outline

What is Bity ?

From nothing to Docker

Docker-compose in dev env

Ansible for cloud providers

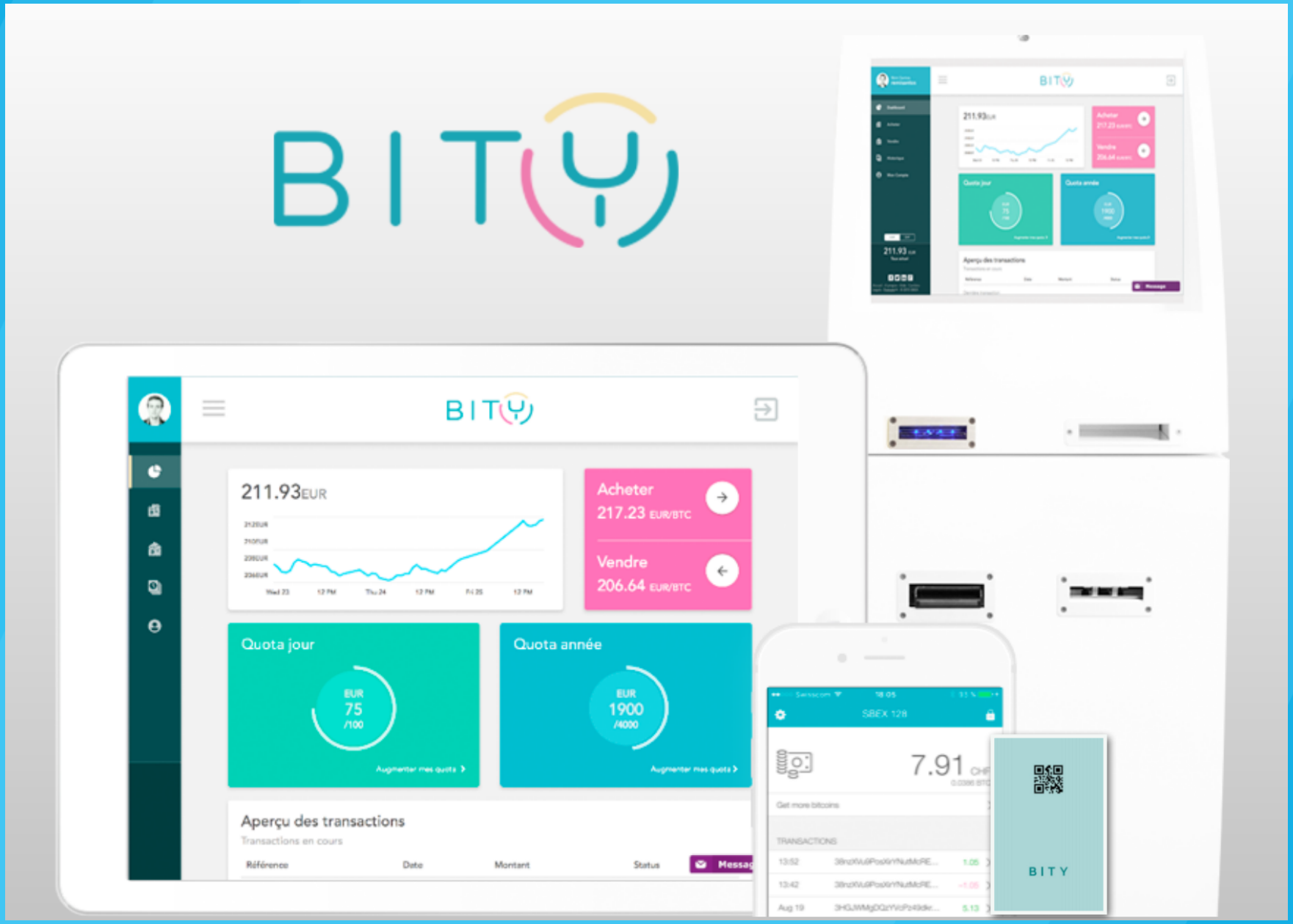
Ansible for docker orchestration

Lessons learned

Future

What is Bity.com ?

- Buy, sell and store bitcoins
- Regulated
- Hosted in Switzerland
- Small team
- Fast-moving space

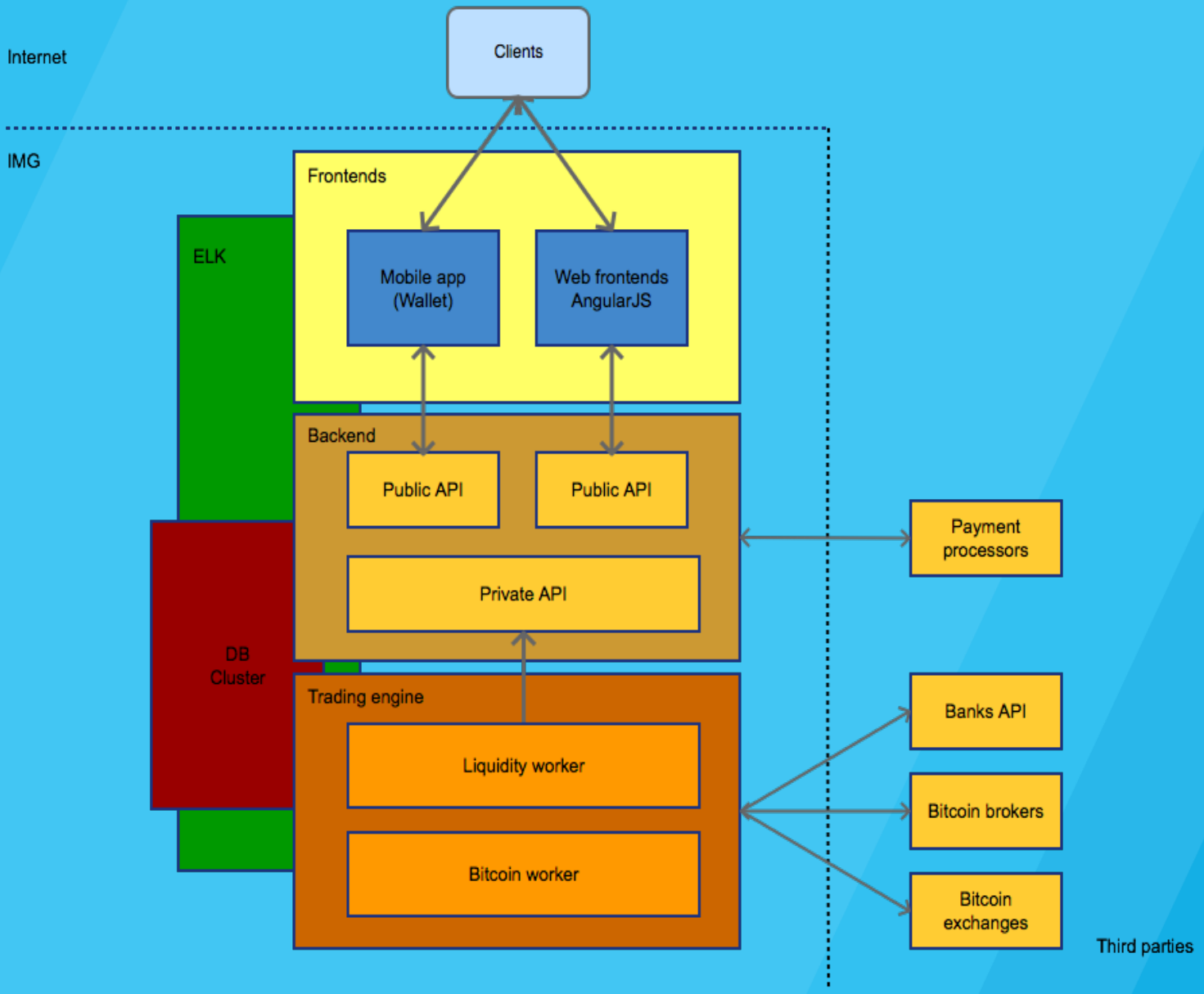

BITY
211.93EUR
Acheter
217.23 EUR/BTC
Vendre
206.64 EUR/BTC
Quota jour
EUR
75
/100
Augmenter mes quota
Quota année
EUR
1900
/4000
Augmenter mes quota
Aperçu des transactions
Transactions en cours
Référence
Date
Montant
Status
7.91
BITY

Our needs

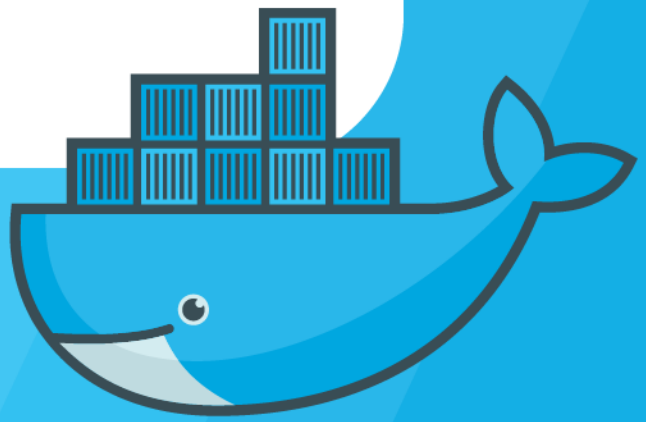
- Follow the "Twelve factor" app recommendations.
- Scalable, CI/CD -> Docker
- Cloud (Paas) + Hosted in Switzerland -> Exoscale

Our tech stack

Infrastructure design



Zero to Prod in 8 months ?



"It works on my machine" syndrome

- Gain velocity
- Increased team collaboration

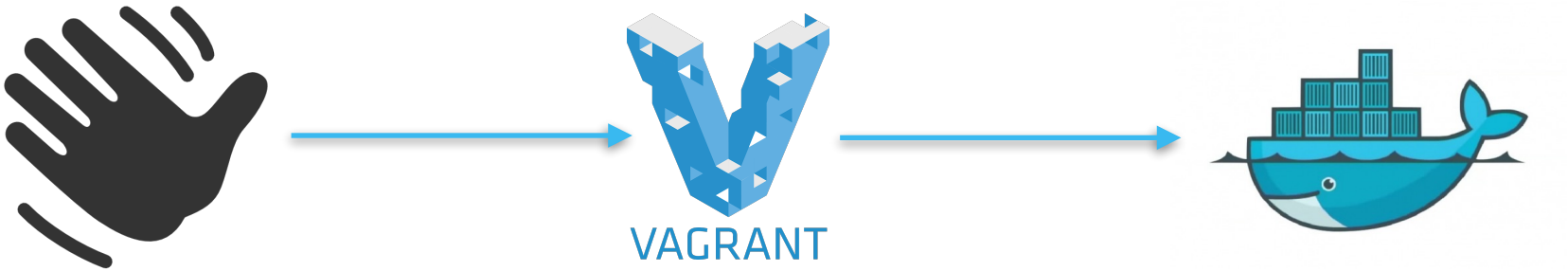
Thanks to :

- Increased reproducibility
- Easy portability

Challenges to gain velocity

- Difficulty on-boarding developers
- Difficulty developing across team due to time to setup environment
- Teams working on different part of the infrastructure

Steps



Nothing to Docker

Code on developer laptop with custom environment

- Zero portability (i.e /source/tree)

Use of Vagrant box

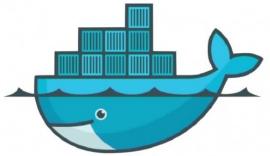
- Reproducibility of development environment (i.e /source/tree/Vagrantfile)

Use of Vagrant box and Docker

- Build image for applications and publish for collaboration (i.e /source/tree/Dockerfile +Vagrantfile)

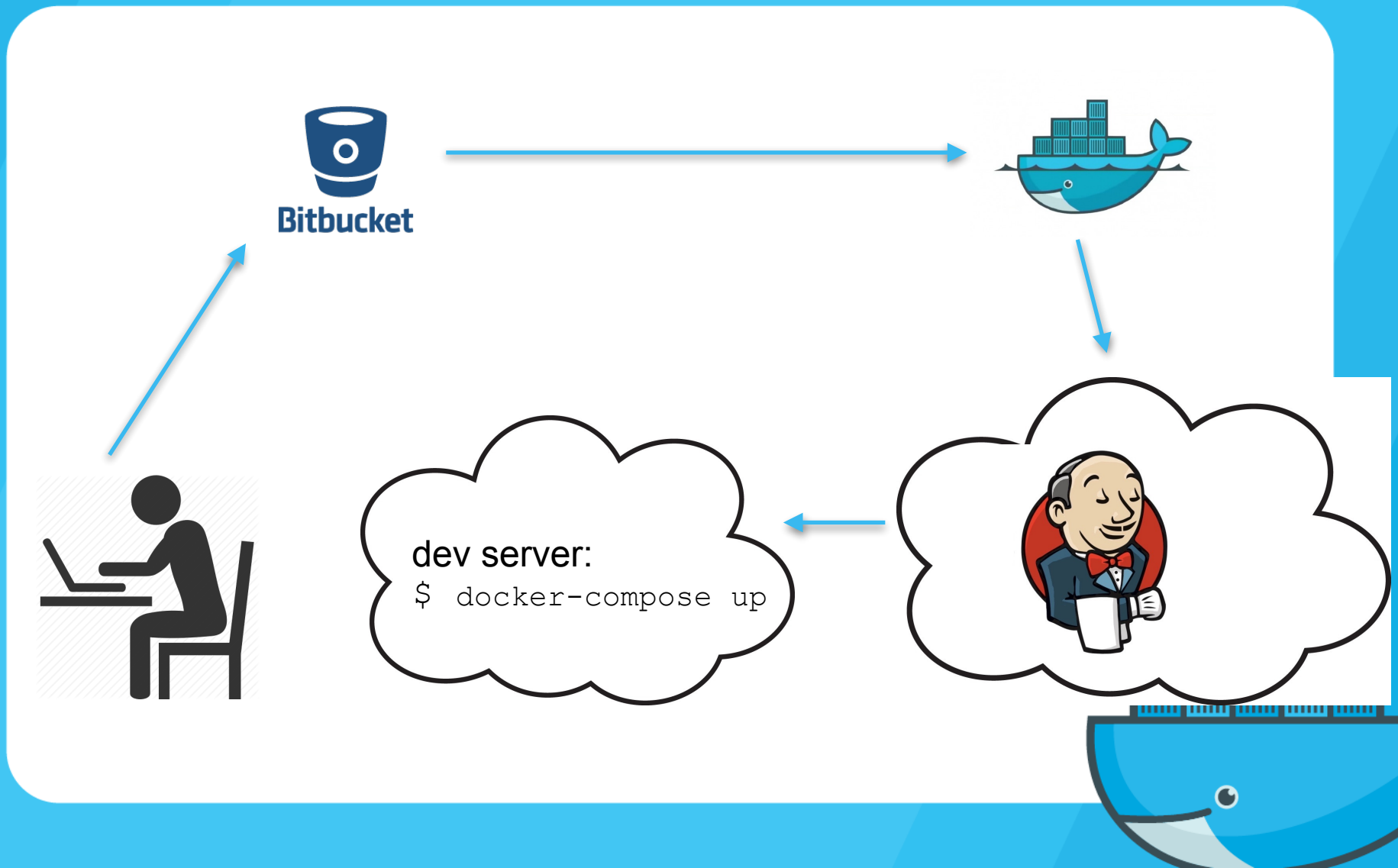
```
$ docker build -t sbex/bity .
$ docker run -d -p 80:80 sbex/bity
```

Docker Hub



Private repositories on Bitbucket
Private repositories on Docker Hub
Automated builds
Web Hooks from Bitbucket to Docker hub
Web Hooks from DockerHub to Jenkins

CI/CD for dev

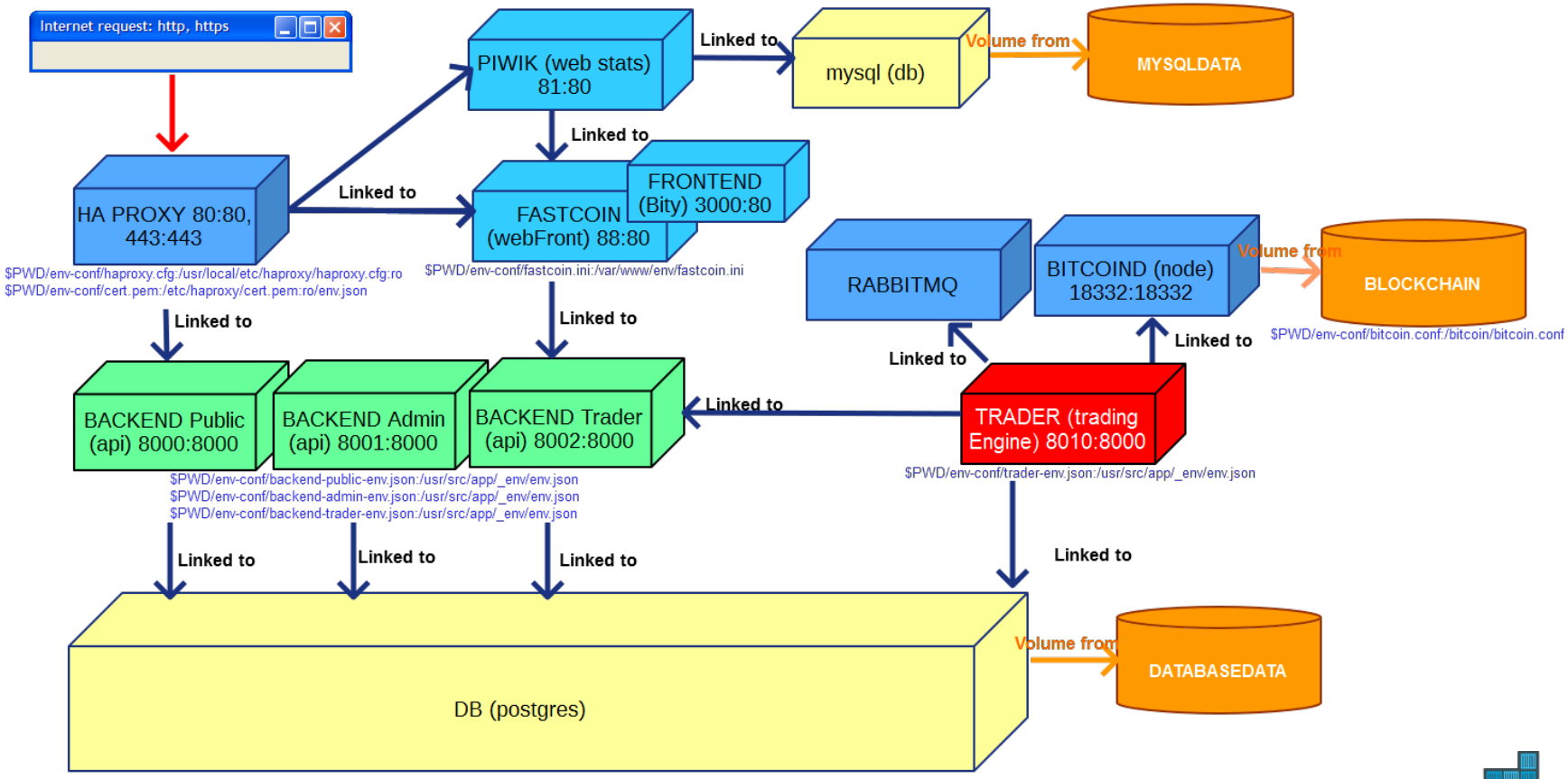


Docker-compose for dev env

- One docker-compose file to deploy entire infra
- Great for developers and testing
- Used to test parts of applications with latest image from repo
- Used prior to merging in staging

One compose file to run all infra in dev

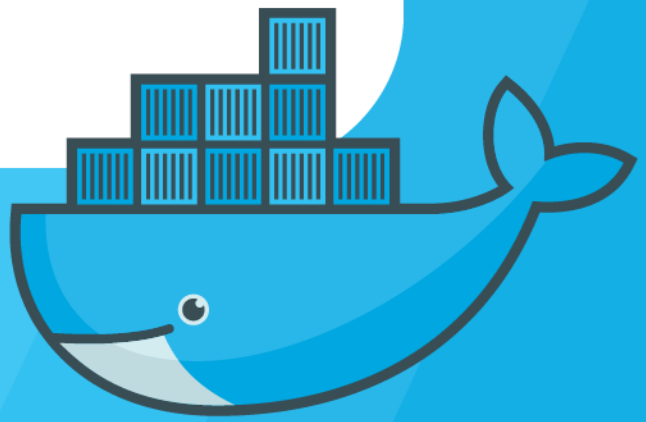
Docker view : Infra Sbex on one box



Limitations of compose

- Impossible to run command inside containers
- How to deal with secrets ?
- At the time, no Swarm so compose was a single host dev tool

Going to production in the cloud



Choosing a Cloud and "config" tool

- Need a Swiss sovereign cloud
- Need a tool to configure:
  - security groups
  - key pairs
  - manage instances
- Not a configuration management tool to deploy apps.

ANSIBLE

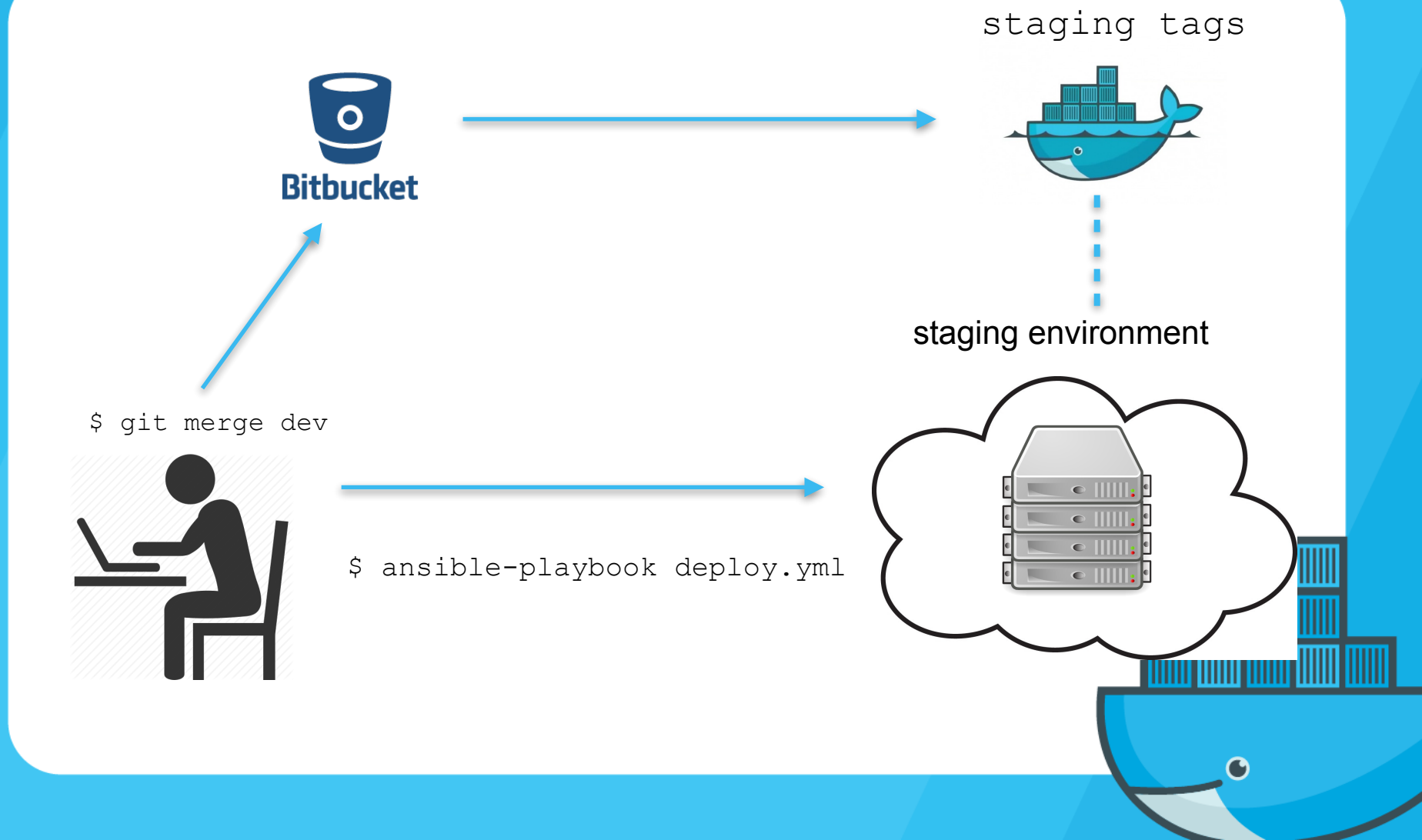
exoscale

Environments

- Dev (server or laptop + docker-compose) on bitcoin-testnet
- Staging (cloudstack + ansible) on bitcoin-testnet
- Prod (cloudstack + ansible) on bitcoin-mainnet

separate branches for code and different image tags

Deploying on staging env

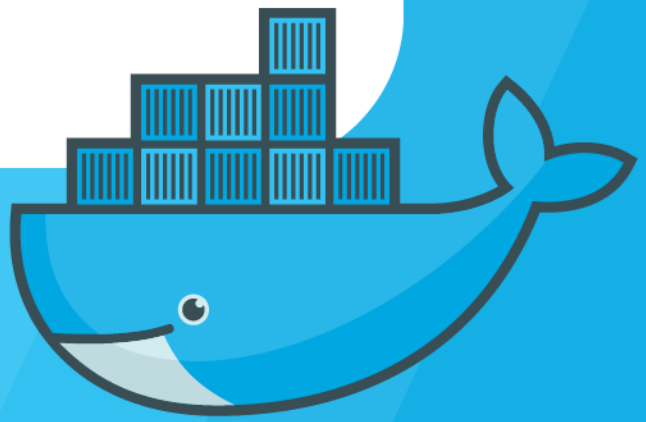


Create Cloud Infrastructure at Will

ANSIBLE

exoscale

cloudstack
open source cloud computing



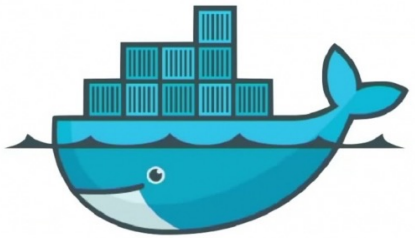
Ansible CloudStack module

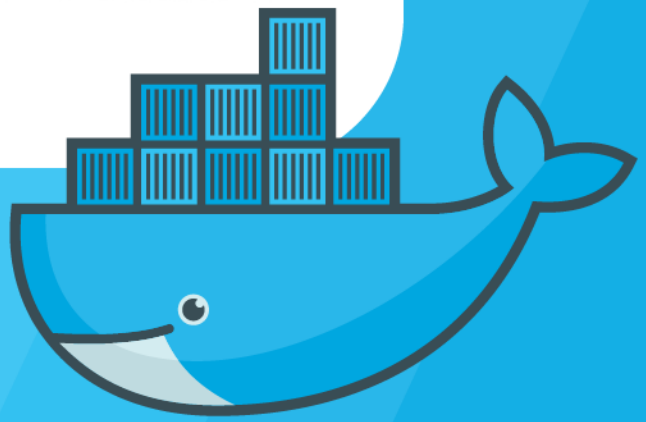
```
- name: Start Backend VM
  local_action:
    module: cloudstack_vm
    name: backendpublic
    template: "{{ template }}"
    service_offering: "{{ instance_type }}"
    security_groups: [ 'backend_public' ]
    ssh_key: "{{ ssh_key }}"
    user_data: "{{ lookup('file', '../files/backend_userdata.yml') }}"
  register: backend_public
  tags: create_vm
```

```
- name: backend SecGroup
  local_action:
    module: cloudstack_sg
    name: database
    description: Backend public
  tags: secgroup
```

Deploying/Managing containers with Ansible

Ansible Docker module in Ansible core





Ansible docker module

```
- name: Set Docker login credentials
  command: docker login -u foobar -e {{hub_email}} --password={{hub_password}}

- name: Docker pull sbex/angular-frontend
  command: docker pull sbex/angular-frontend

- name: Start bity
  docker:
    image: sbex/angular-frontend
    detach: true
    restart_policy: always
    name: bity
    ports: 80:80
  tags: start_container
```

Ansible and logdriver

```
- name: Start backend public
   docker:
     name: backend
     image: sbex/backend
     restart_policy: always
     volumes:
       - /app/_env:/usr/src/app/_env:ro
     detach: true
     ports: 8000:8000
     log_driver: syslog
     log_opt:
       syslog-address: udp://{{hostvars['logserver'].ansible_ssh_host}}:5000
       syslog-facility: local0
       syslog-tag: backendpublic
```

Ansible to configure containers

```
  - name: Create directory for settings
    file: path=/app/_env state=directory

  - name: Create json settings from template
    template: src=env.j2 dest=/app/_env/env.json

...

  - name: Create tables
    command: docker exec -ti backend ./manage.py migrate
```

Dealing with secrets

No secrets in container images

Use Ansible vault to encrypt all secrets in playbooks stored in bitbucket

```
$ ansible-vault create /path/to/file.yml
$ ansible-vault encrypt /path/to/file.yml
$ ansible-vault decrypt /path/to/file.yml
$ ansible-vault rekey /path/to/file.yml
```

Container “Orchestration”

Every application has its role

Several playbooks

```
$ ansible-playbook deploy.yml
$ ansible-playbook upgrade.yml
$ ansible-playbook stop.yml
$ ansible-playbook start.yml
```

Logging

Early on:

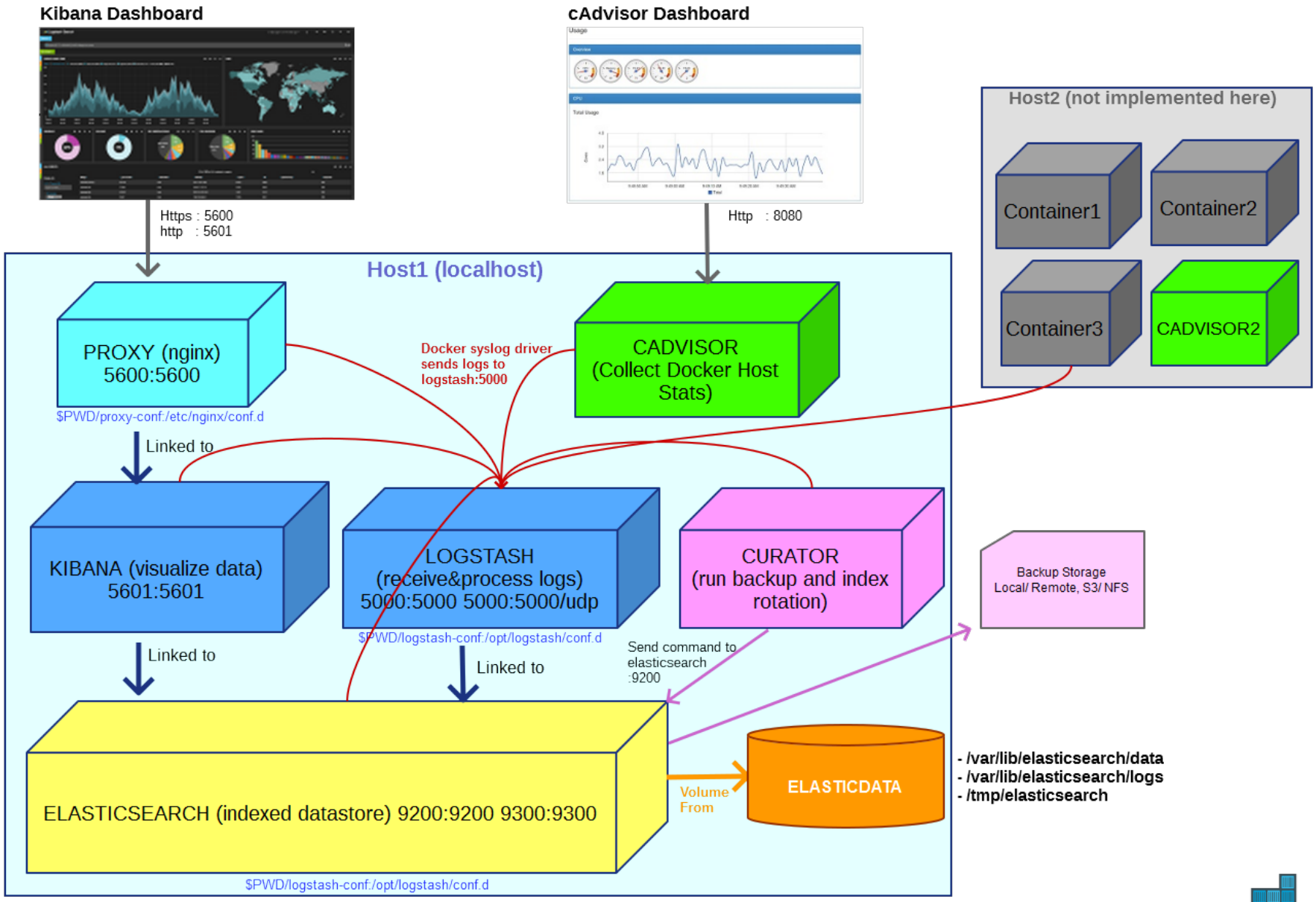
- Logspout to ELK

Now:

- Logdriver (ansible 2.0) syslog driver to logstash with ELK
- Test/deploy monitoring with docker-compose.

One docker-compose runs

- ElasticSearch 1.7 (+data container)
- Logstash 1.5.3 (+conf for elk logs)
- Kibana 4 (+Dashboard for elk logs)
- cAdvisor (Collect & View containers performance)
- Ngnix Proxy 1.9.3 (for SSL + password access).


Kibana Dashboard
cAdvisor Dashboard
Https : 5600
http : 5601
Http : 8080
Host2 (not implemented here)
Container1
Container2
Container3
CADVISOR2
Host1 (localhost)
PROXY (nginx)
5600:5600
$PWD/proxy-conf:/etc/nginx/conf.d
Docker syslog driver
sends logs to
logstash:5000
CADVISOR
(Collect Docker Host
Stats)
Linked to
KIBANA (visualize data)
5601:5601
LOGSTASH
(receive&process logs)
5000:5000 5000:5000/udp
$PWD/logstash-conf:/opt/logstash/conf.d
CURATOR
(run backup and index
rotation)
Backup Storage
Local/ Remote, S3/ NFS
Linked to
Linked to
Send command to
elasticsearch
:9200
ELASTICSEARCH (indexed datastore) 9200:9200 9300:9300
Volume
From
ELASTICDATA
- /var/lib/elasticsearch/data
- /var/lib/elasticsearch/logs
- /tmp/elasticsearch
$PWD/logstash-conf:/opt/logstash/conf.d

Lessons Learned

- Container restart -> thanks to restart policy (docker > 1.6)
- Weird Ansible docker behavior at times
- Config as volume mounts (Too many env variables to handle)
- Cannot use compose in prod yet (vault, execute commands inside containers)

Future

- Currently using Ubuntu
- Investigate the use of Docker optimized OS (e.g coreOS, Atomic, RancherOS)
- Need Easy upgrade of Docker versions
- With new versions every 2 months, and possible change of recommended storage driver, we need an easy way to cleanly upgrade production systems
- Investigate the use of a Docker orchestrator, possible replacing Ansible docker module
  - (e.g Swarm, Kubernetes, tutum...)

dockercon EU
BARCELONA • 16-17 NOVEMBER 2015

Thank you!

MATHIEU BUFFENOIR

@MBuffenoir
mathieu@bity.com

SEBASTIEN GOASGUEN

@sebgoa
runseb@gmail.com