Docker BDay - Retour d’ expérience avec Docker

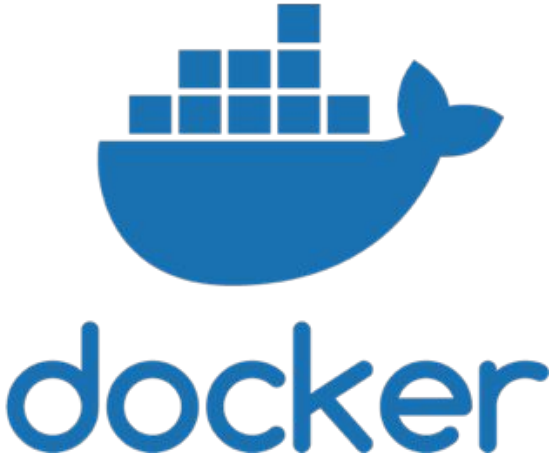
Maxime Coquerel - MVP Azure


6 years!!!
#DockerBday

Disclaimer

“*Tous les posts de cette présentation ne reflètent que mon opinion et non celle de mes employeurs et clients.*“

Remerciements



LE CAMP

Incubateur • Accélérateur

Ainsi qu’à la communauté Docker Québec !

Speaker

Maxime Coquerel

Cloud Architect Lead

Email : max.coquerel@live.fr

Blog : zigmax.net (Since 2012)

Github : https://github.com/zigmax

Twitter : @zig_max

Open Source Contributor (Kubernetes / OpenStack).

Mon expérience avec Docker (Timeline)

Sur demande uniquement.

Robust global operations

1.6+ billion
data requests processed per day

525+ million
travel agency bookings processed in 2014

695+ million
Passengers Boarded (PBs) in 2014

95%
of the world's scheduled network airline seats

amadeus

Amadeus Constraints

High volume

December 2014 (customer + internal traffic):

- At peak: **~210 000 queries per second**
- Average: **~145 000 queries per second**

Thousands (and thousands) of application servers

100+ TB of compressed data logged every day

amadeus

Amadeus System

Where we are

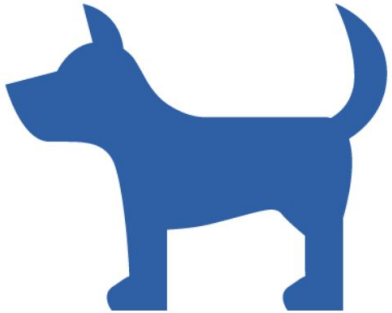
- Large distributed system (SOA)
  - 5000+ “micro” services
- One data-center + disaster-recovery sites
- Thousands of servers
  - x86-64 Linux servers
  - Pre-configured upfront for specific tasks
  - N+x model as servers can’t be replaced quickly
  - Roles cannot be changed

Amadeus System

Where we were

- Larg
  - 5
- One
- Thou
  - x8
  - Pr
  - N
  - R

Despite the number of servers largely managed as pets



Application Centric Deployment

- Deploy the application **as a whole**
  With **all** its dependencies

- Reproducibility
- Homogeneity
- Technology agnostic
- Simplify operations

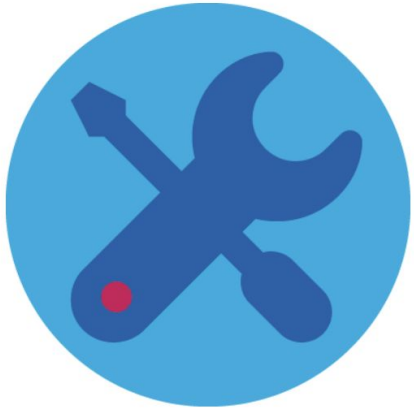
amadeus

Technological Stack: **OPEN**SHIFT

Docker + Kubernetes

- Linux Container Technology
- Container image format
- Easy deployment

- Orchestration of Linux containers
- “Manage a cluster of Linux containers as a single system”
- Automatic placement, self-healing

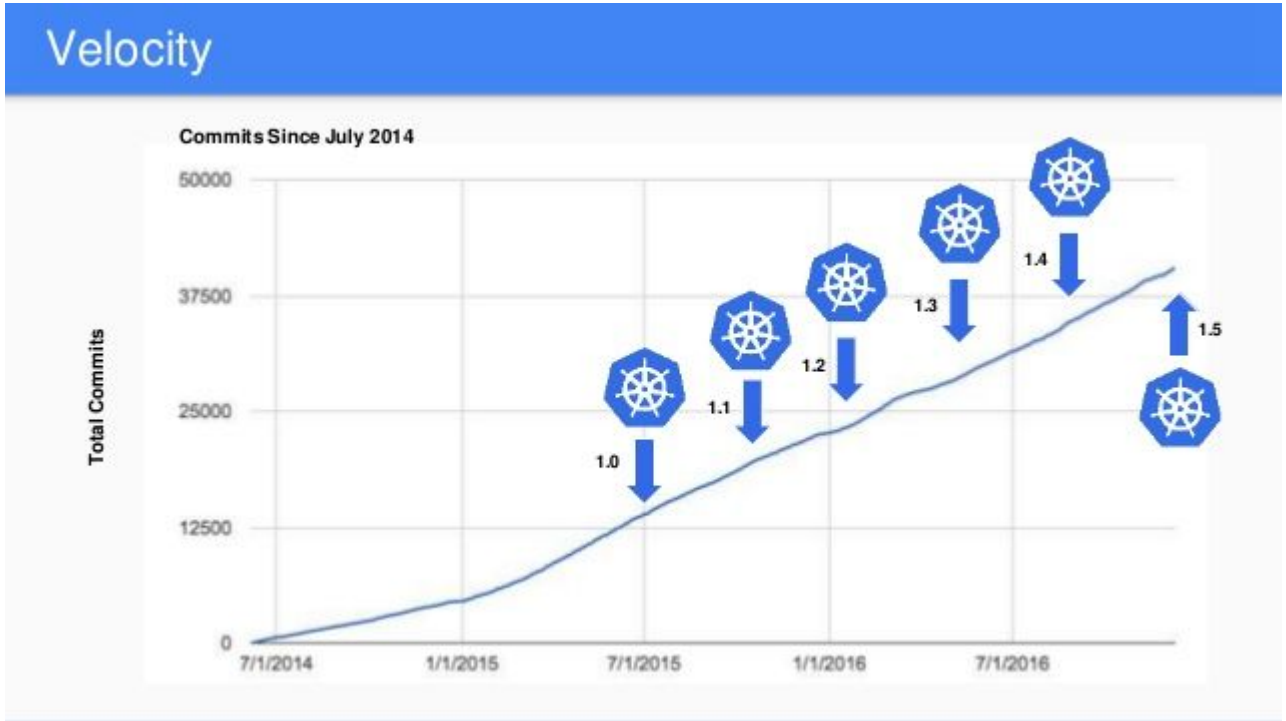


amadeus

Partnership

redhat

Je découvre Kubernetes en version 1.4



Kubernetes en version 1.4

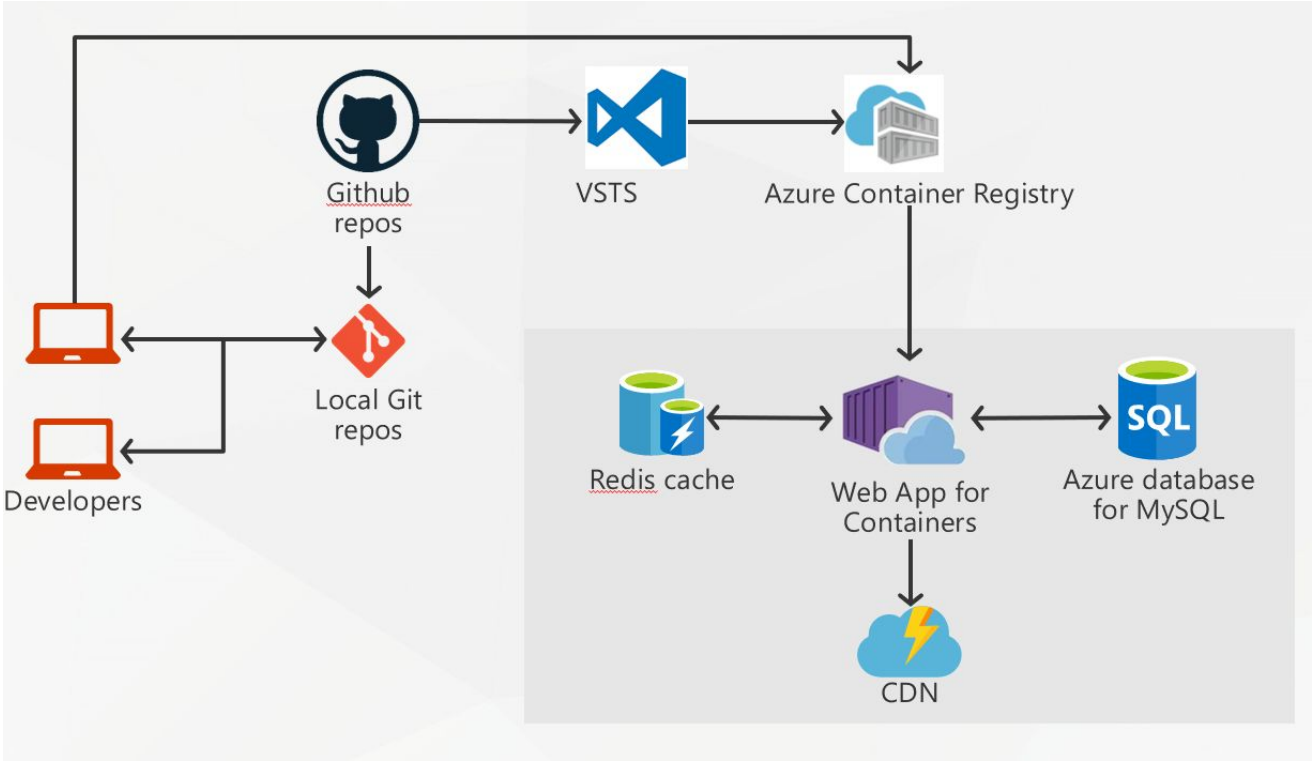
- Sécu .... What ????
  - Pas RBAC
  - ETCD by default pas d'authentification
  - Secret en base64 dans le cluster ETCD (Youhou !!!)
  - Kubelet (RCE vers API Server) (Youhouou !!!)
  - Pas de segmentation réseau entre les Pods (Tu en pwn un et tu deviens root du cluster !)
  - ....

- Not Ready pour notre prod, on attendra la version 1.6 (RBAC)

Ma vie avec Docker et Kubernetes (Now)

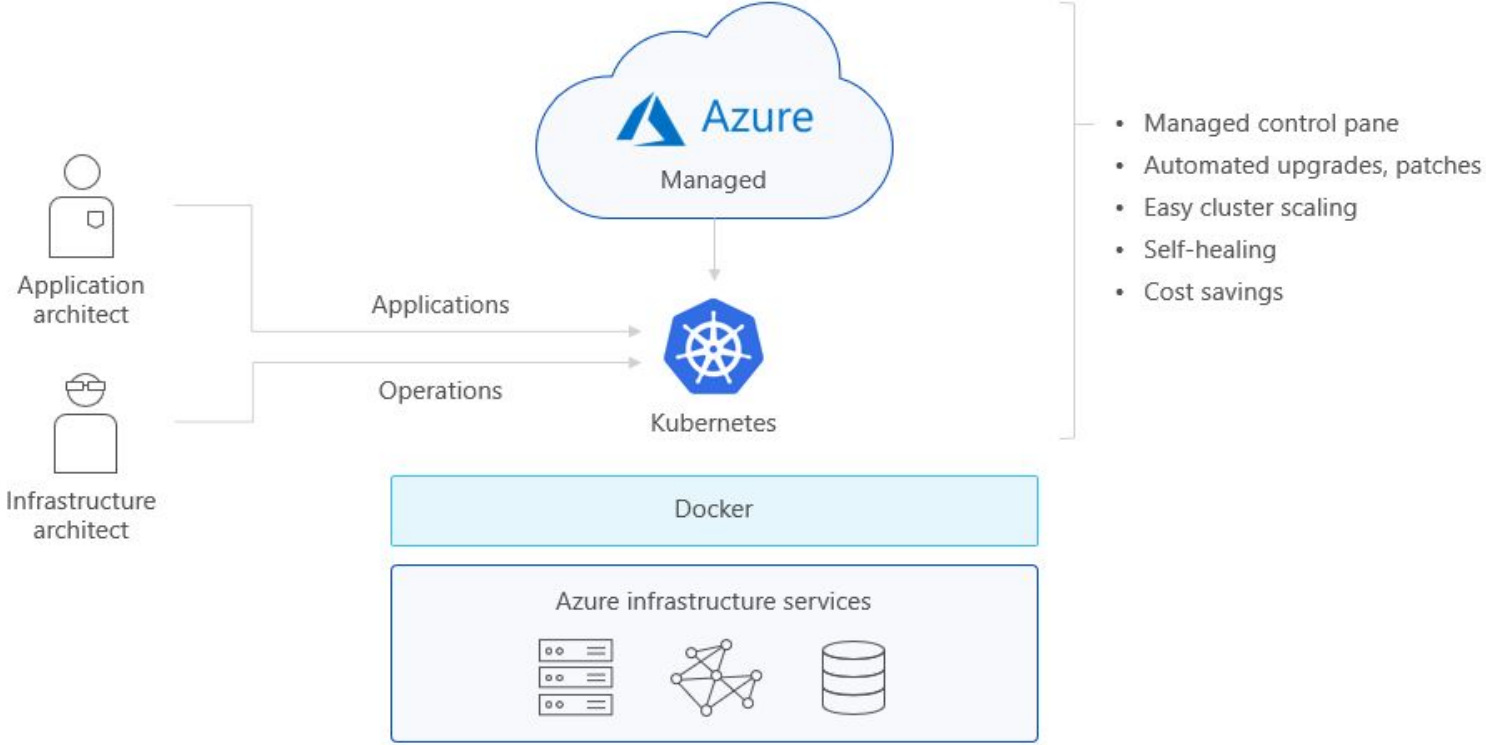
- 3 Clusters AKS (2 Dev + 1 Prod)
- CI / CD avec Azure DevOps
- Scan des images + Pentests
- Orientation PaaS à 200% !

Docker - Web App for Container



Azure Kubernetes Service (AKS)

A fully managed Kubernetes cluster



Kubernetes Master And Node Attacks

by Maxime Coquerel

The objective of this article is to present an introduction of Kubernetes penetration testing.

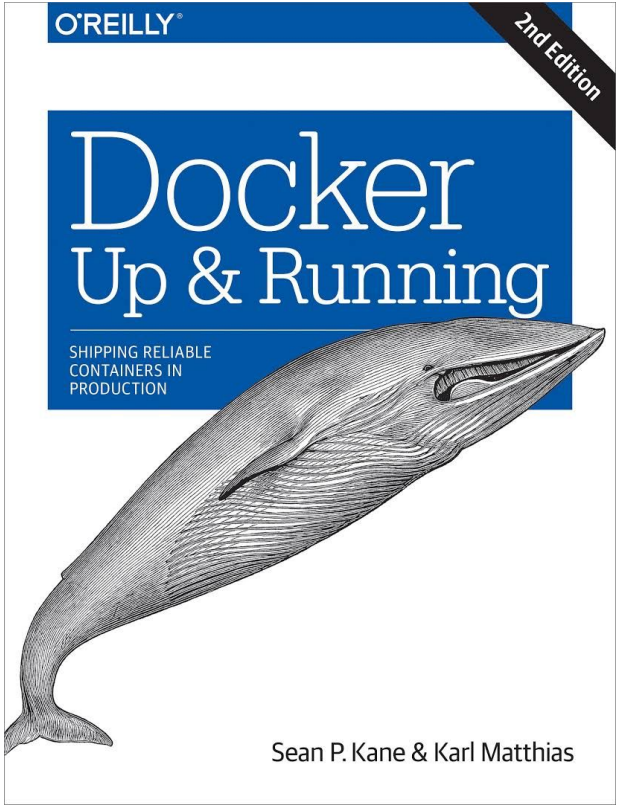
The first goal of a Kubernetes penetration test is to increase the security of the Kubernetes resources and of your company.

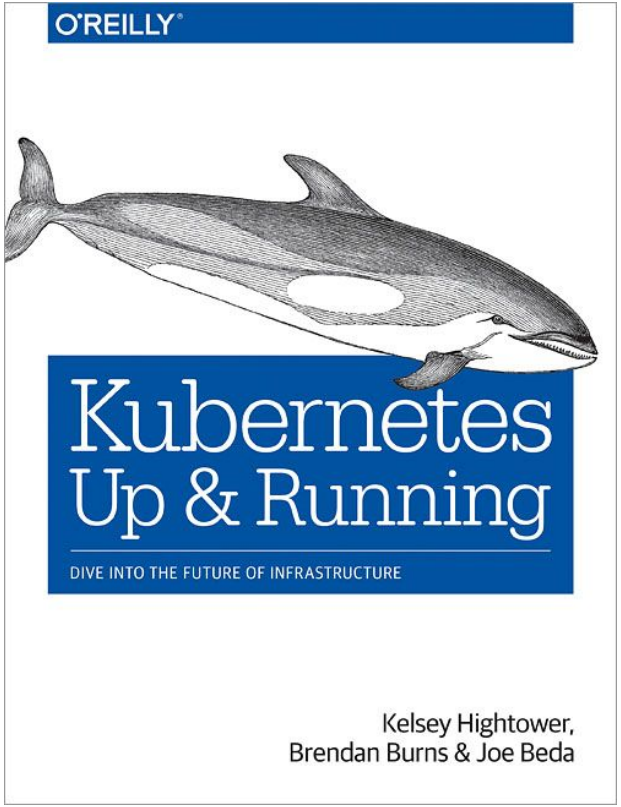
Security of Kubernetes Cluster is a large subject and pentesting of Kubernetes Cluster also. With a good comprehension of Kubernetes Architecture, everything is possible.

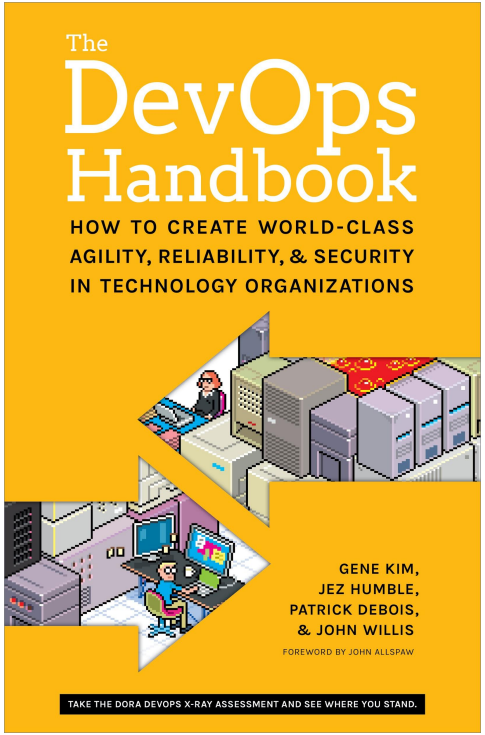
https://pentestmag.com/download/pentest-kubernetes-penetration-testing/

Questions / Talks

Books


O'REILLY
2nd Edition
Docker
Up & Running
SHIPPING RELIABLE CONTAINERS IN PRODUCTION
Sean P. Kane & Karl Matthias


O'REILLY
Kubernetes
Up & Running
DIVE INTO THE FUTURE OF INFRASTRUCTURE
Kelsey Hightower,
Brendan Burns & Joe Beda


The
DevOps
Handbook
HOW TO CREATE WORLD-CLASS AGILITY, RELIABILITY, & SECURITY IN TECHNOLOGY ORGANIZATIONS
GENE KIM,
JEZ HUMBLE,
PATRICK DEBOIS,
& JOHN WILLIS
FOREWORD BY JOHN ALLSPAW
TAKE THE DORA DEVOPS X-RAY ASSESSMENT AND SEE WHERE YOU STAND.

Technical Resources

App Service - Web App for Container - https://azure.microsoft.com/en-us/services/app-service/containers/

Azure Kubernetes Service (AKS) - https://docs.microsoft.com/en-us/azure/aks/

Azure Security Blog - https://azure.microsoft.com/en-us/blog/topics/security/

Maxime Blog - http://zigmax.net

Microsoft Ignite 2018 - https://myignite.techcommunity.microsoft.com/