OpenShift @ Proximus
From classical web applications to more real time services

RedHat Forum Brussels - 08/10/2019

nicolas.kaczmarek@proximus.com
• Introduction & context
• Overview of all OpenShift clusters
• Key figures
• IT clusters vs Telco clusters
  • Major differences
• Challenges
  • Capacity Management
  • Monitoring
  • Security
• What’s next ?
• Largest telco operator in Belgium providing fixed lines, mobile, internet & TV services.
• **Telindus** (ICT Services) and **BICS** (international connectivity) are also part of the Proximus group

• > 12 000 employees

• 5,8 Billion € revenue in 2018

• Still primarily owned by belgium government
  (>50% market shares)
IT Evolution requires strong enablers
Overview of all OpenShift clusters

- **OSS Fabric**
  - OCP Cluster
  - OSS – external facing
  - 4 compute nodes
  - 3.11
  - Delayed to late 2019

- **Telco Fabric**
  - « Old » OCP Cluster
  - Telco – external facing
  - 12 compute nodes
  - 3.9
  - Ready
  - To be removed

- **Service Zone**
  - OCP Cluster used for Enterprise Registry
  - Corp IT – external facing
  - 8 compute nodes
  - 3.11
  - Ready
  - Ready – to move to OSS

- **ConnectIT Zone**
  - OCP Cluster
  - Corp IT – internal facing
  - 5 compute nodes
  - 3.11
  - Ready

- **For OSS applications**
  - SDN Network

- **For Telco/IDTV applications**
  - SDN Network

- **For external facing IT applications**

- **For internal facing IT applications**

- Inline upgrade planned to 3.11
Key figures: 6 main OpenShift clusters

- OpenShift Cluster
- OpenShift Cluster
- OpenShift Cluster
- OpenShift Cluster
- OpenShift Cluster
- OpenShift Cluster
- Enterprise Registry Cluster
Key figures: 240 Nodes (RHEL 7 Linux VMs)
Key figures: > 10 000 containers
Key figures: 28 “applications” deployed

8 live in PROD
Detailed setup of OpenShift IT clusters

Single entry point for all env with wildcard DNS (ex: *.opbc)
Routing is done to correct pods by HA Proxy based on URL requested
Detailed setup of OpenShift Telco clusters

OpenStack Virtualization Layer (RedHat 7 Linux VMs)

- **Master Node**
  - 8 vCPU – 32GB vRAM
- **Infra Node**
  - 4 vCPU – 32GB vRAM
- **Compute Node**
  - 16vCPU – 128GB vRAM
- **DNS Node**
  - 2vCPU – 4GB vRAM
- **Audit Node**
  - 2vCPU – 4GB vRAM
- **Bastion Node**
  - 2vCPU – 4GB vRAM

OpenShift Virtualization Layer (docker containers)

- **Pod**
  - Application Containers
- **HA Proxy**
  - AVI VIP
  - NON-PROD
  - PROD

Physical Servers dedicated for OpenShift workloads

- **HP DL360**
  - 24 cores
  - 768 GB RAM

Sensitivity: Unrestricted
Multi-clusters challenges – Access & Synchronization

WAM Portal → API calls to change DC in use

3 DNS – GTM (F5)
Specific URL per application
Ex: app.global.com

Custom health check for every URL

LTM (F5)
Generic VIP
Ex: app.ocp-dc1.local

External Registry

Image Streams

LTM (F5)
Generic VIP
Ex: app.ocp-dc2.local

OpenShift cluster DC1

Name Space Applier POD

HA Proxy

Internal Registry

App POD

OpenShift cluster DC2

Name Space Applier POD

HA Proxy

HA Proxy

HA Proxy

Internal Registry

App POD

App POD

App POD

App POD

Git

Sensitivity: Unrestricted
Major differences between Telco and ITS setup

1. **Networking requirements**:
   - More future proof load-balancer solution
   - QoS/better segregation for incoming traffic
   - Support for multiple external networks
   - Better split Management traffic vs Application traffic

2. **Capacity Management requirement**:
   - More efficient usage of resources

3. **Automation requirement**:
   - More automated installation

4. **Multi-clusters requirements**:
   - Active/Active application
Resource quota’s implemented for all projects along with limitranges (request & limits)
Capacity Management : script to query OCP API & excel today -> Prometheus/Grafana tomorrow
Monitoring

To avoid this:

You need to know how your application containers are behaving and also get a view on the OpenShift control plane!
Monitoring setup for OpenShift IT clusters

Dynatrace

Dynatrace NON-PROD tenant

Dynatrace PROD tenant

ZenOSS

Infra Only Agents

Full Stack Agents

Infra Only Agents

Physical Servers dedicated for OpenShift workloads
Dynatrace Monitoring Dashboard
Proximus Control Plane Monitoring Dashboard

- Specific container running in each monitored cluster querying OCP API
- Data collected is send back to Prometheus in the central Enterprise Registry cluster
- Visualization via Grafana dashboards
Security

Current usage:
- Image vulnerability and compliance
- Host OS vulnerability and compliance
- CIS compliance of Docker/Kubernetes

Future usage:
- Central console to get the unified view and also define policies and apply everywhere
- Scanning during build
- How to handle false positive from RedHat images
- Namespace based access for developers
What’s next?

- OpenShift 4.x
- Telco core services
- Cluster Federation
- BlockChain
- GPU
- ServerLess
- AI
Questions?

RedHat Forum Brussels - 08/10/2019

nicolas.kaczmarek@proximus.com