M by Orange

How to build a telco operator from scratch in less than 1 year

David Sastre - Senior Architect, EMEA
Ignacio Verona - Senior Solution Architect, EMEA Telco Technology Office (TTO)

May 8th, 2019
EMEA Architects Team (Consulting)

#RHEL

#OCP

#automation

#security_padawan

EMEA Telco Technology Office (TTO)

#NFV

#automation

#geek

#maker
WHAT IS X by Orange?
It's an MVNO Reseller NO!
It’s an Over The Top operator!

Orange Spain (Mobile and Fixed)
Zero-Hardware (Uber model)
UX focused (Customer 1st)
100% DevOps (Full automation)
Which services do they offer?

Connectivity
XFiber

Privacy
XPrivacy
XSecurity
XProtection

Digitalization
XMusic

Collaboration
XUCom
WE CANNOT SOLVE OUR PROBLEMS WITH THE SAME THINKING WE USED WHEN WE CREATED THEM

-Albert Einstein
What makes them different?

- Modular Offering
- UX focus
- Fully Automated platform
- Full visibility platform
- Subscription based model
- Cloud Centric model
- Market success through ecosystem (not going alone)
What makes them different?

5 KPIs:

1. 30 days from “idea to sellable feature”
2. Scalable, zero touch provisioning
3. Max time to provision a new client: 3 days
4. Max time to provision a new feature: 15mins
5. 99.95% e2e availability
How many RFX’s?

ZERO.
A bit of history

Vision Paper received and answered

PoCs
Ansible, CloudForms, OpenShift, Gluster

Contract signed, engagement start

Project About to be canceled!

X by Orange goes LIVE
What have they built?
What have they built?
Orange wants Red...

How do we start?
SERVICES/DELIVERY PART
OBJECTIVES

● Infrastructure as Code
● Immutability
● Automation
● Built-in Security
INFRASTRUCTURE AS CODE
RHEL 7

- GitLab
- Packer
- Terraform
- Ansible
OCP 3.x

- GitLab
- Terraform
- Ansible
- Red Hat Atomic OS
OCP 4.x

- GitLab CI (WIP)
- New OCP installer
- Red Hat CoreOS Linux
IMMUTABILITY
OVERCOME LIMITATIONS WHEN POSSIBLE

- Subscription Handling BYOL
- Cloud-init not enough
- Workaround possible
- SystemD unit
KNOWN LIMITATIONS

- Installers
- Datastores are mutable by design
- No workaround possible
- Orchestration
AUTOMATION
NETWORK AUTOMATION

- Check Point Software
- Nuage Networks
- Cisco
- Ansible Networking
PaaS AUTOMATION, ONE EXAMPLE

Atomic OS upgrade, version 1

- Cordon
- Drain
- Download new OSTree for each node
- Reboot
PaaS AUTOMATION, ONE EXAMPLE

Atomic OS upgrade, version 2

- Terraform to deploy updated AMIs
- AWS autoscaling groups
- Ansible to scale up the cluster
- Cordon, drain and delete old nodes
BUILT-IN SECURITY
AMI GENERATION

Starting point:

- Single filesystem CentOS image
- Lightweight hardening
- No corporate approved AMI
- GitLab CI pipeline orchestration
AMI GENERATION

Public AWS RHEL 7 AMI as base

- Packer generates an LVM2 partitioned AMI
- Ansible to apply hardening baseline
- Resulting AMI is new corporate baseline
- GitLab CI pipeline orchestration
USE CASES

Jump Hosts/Bastion Hosts

- LVM2 partitioned EBS
- Mount point hardening (even RO!)
- No interactive shell
- Polyinstantiation of /home, /tmp
- Exhaustive auditing (via auditd)
USE CASES

Jump Hosts/Bastion Hosts

- Intrusion Detection System
- Intrusion Prevention System
- Firewalld
- Logging
- Monitoring
USE CASES

Jump Hosts/Bastion Hosts

- GRUB2 options
- Sysctl settings
- Main service hardening (SSHD)
USE CASES

Jump Hosts/Bastion Hosts

- No sudo rules
- SELinux
- Secure mode
USE CASES
USE CASES

IdM, centralised identity management

- LDAP Directory
- Kerberos
- Public Key Infrastructure
- DNS (replaced with Route53)
- NTP (AWS’ own NTP servers)
- KRA (replaced with Hashicorp Vault)
USE CASES

IdM, centralised identity management

- Role Based Access Control
- Host Based Access Control
- SELinux user mapping
- Sudo policies
IDENTITY MANAGEMENT

Starting point:

- Local users created in each CentOS
- SSH public key deployment automated but cumbersome
- No corporate approved JML process
- GitLab as OIDC provider for OCP
IDENTITY MANAGEMENT

IdM provides centralised single source of truth for identity and access policy

- No local users on EC2 instances
- SSH public key distribution process not required anymore
- Corporate approved JML process
- GitLab consumes OIDC provided by RHSSO using IdM as backend
IDENTITY MANAGEMENT

IdM provides centralised single source of truth for identity and access policy

● Other services integrated with IdM
  ○ SDLC tools (Nexus, Sonarqube, ...)
  ○ RHSSO
  ○ FreeRADIUS WPA2 Enterprise and 802.1x
  ○ Staff VPN authentication
NEXT STEPS

● RHEL 8
● OCP 4.x + ISTIO
● Engineering to visit XbyOrange
● Improve and extend collaboration
CONCLUSIONS
AND
LESSONS LEARNED
CONSULTING SERVICES ADD VALUE

Engaging with us allowed XbyOrange to

● Identify weaknesses early
● Improve on Automation and Security
● Enhance processes and integrations
● Come talk to us!
LESSONS LEARNED

- Apply Red Hat core values: be transparent, honest, do team work
- Telco IS special, but that is changing
- Red Hat services bring extreme value to the customer teams
- Cooperation between technology, culture and vision is needed
- Will XbyOrange be the model for new operators, focused on VAS?
THANK YOU

linkedin.com/company/Red-Hat
youtube.com/user/RedHatVideos
facebook.com/RedHatinc
twitter.com/RedHat