OKD 4.4 on Azure

Josef Meier

Cloud Architect

Working at **Rohde & Schwarz** in Munich, Germany (https://www.rohde-schwarz.com/)

Working with **OKD** since version 3

Waiting for OKD 4 since October 2018 ☺

OKD 4 – Why do we wait eagerly ?

- **Modern Kubernetes version**

- **Great Ops features** (automatic updates of **OKD and** the underlying **OS**)

- Great integration of tools: Monitoring, OperatorHub, Tekton, …

- The **Web UI looks absolutely fantastic** and is **great** for **experienced Kubernetes Devs and Beginners !**

- The **roadmap** also looks very **promising**

OKD 4 on Azure: Installation

There **was a problem with networking in Fedora CoreOS on Azure**:

- A **few reboots were required** to get it running.
- All VMs were affected by this bug (bootstrap, masters, workers).
- Since a few days a **test version of FCOS** is available where this **bug seems to be fixed**.

FCOS image still not available on Azure Marketplace:

- Image must be **downloaded**, **extracted** and **uploaded** to an Azure Blob container.
  A few weeks ago it also was necessary to convert the vhd image with qemu for Azure.
  Because the image is rather big (8GByte) at least with my internet connection my **OKD installation** always **timed out**.

I coded a **workaround** for this problem, because I wanted to test OKD on Azure.

It's **not necessary anymore** if FCOS **is available** on the **Azure Marketplace** !

Fedora CoreOS image and Azure

If FCOS is on Azure Marketplace

2020-03-29: FCOS is not on Azure Marketplace

> „Hacky" workaround:
> Create helper VM on Azure with the installer that downloads, extracts and uploads it to Storage Account.
>
> **Installer must be modified for that.**

```
openshift-install create cluster
```

```
openshift-install create cluster
```

Core commands executed in the Hack

The hack creates a **helper VM** with Terraform on Azure and executes this code:

```bash
#!/bin/bash

wget https://aka.ms/downloadazcopy-v10-linux -O azcopy.tar
tar xvf azcopy.tar --strip-components 1
chmod +x azcopy

wget ${vhd_url} -O fcos.vhd.xz
xz -d fcos.vhd.xz

# Upload decompressed VHD file to Azure blob storage.
./azcopy copy ./fcos.vhd ${primary_blob_endpoint}${container_name}/fcos.vhd${sas_token}'
```

HACK

Install Go

```
cd ~
wget https://dl.google.com/go/go1.14.1.linux-amd64.tar.gz
tar xvf go1.14.1.linux-amd64.tar.gz
sudo mv go /usr/local/bin/
echo 'export PATH=$PATH:/usr/local/bin/go/bin' >> ~/.bashrc
echo 'export GOPATH=~/go' >> ~/.bashrc
source ~/.bashrc
```

Clone and patch openshift installer

```
mkdir -p ~/go/src/github.com/openshift
cd ~/go/src/github.com/openshift

git clone https://github.com/openshift/installer.git
cd installer
git checkout fcos

# At the time of this demo there isn't a version 4.5 available.
sed -i 's/origin\/release:4.5/origin\/release:4.4/g' \
  pkg/asset/releaseimage/default.go

git remote add jomeier https://github.com/jomeier/installer.git
git fetch jomeier
git cherry-pick 8ea156f372ce2ab22acf51d1bddbc649c326e63d
git cherry-pick 62ef1042ead3deb7585a53b7fdfe2a0ddb76ac72
git cherry-pick 05a7dff57a68134a54573e98864e62783221a5aa
go mod tidy
go mod vendor

./hack/build.sh

sudo cp bin/openshift-install /usr/bin
```

Prepare installation of OKD 4

Create Azure Service Principal for OKD4:
https://docs.openshift.com/container-platform/4.3/installing/installing_azure/installing-azure-account.html

```
ssh-keygen      # <enter>,<enter>, …

openshift-install create install-config

# The installer deletes this file. Don't know why ☺. Save it for later.
cp install-config.yaml ~

# This fcos image has a fix for a severe network bug that occurs on Azure:
export OPENSHIFT_INSTALL_OS_IMAGE_OVERRIDE=\
https://builds.coreos.fedoraproject.org/prod/streams/testing-
devel/builds/31.20200323.20.0/x86_64/fedora-coreos-31.20200323.20.0-
azure.x86_64.vhd.xz
```

Install OKD 4

```
openshift-install create cluster
```

- It takes ~ 10 minutes until the bootstrap VM starts
- After the master VMs show up in the Azure portal you can start watching OKD 4 coming to life
- All **Azure resources** are **created completely automatic** by the installer !

Install OKD 4

- After the FCOS image conversion the storage account should contain a page blob file.
- Type ‚Page blob' or Azure will complain, if it converts the file to an Azure VM image later.

Watch the installation

```
wget \
https://mirror.openshift.com/pub/openshift-v4/clients/oc/latest/linux/oc.tar.gz

tar xvf oc.tar.gz

export KUBECONFIG=auth/kubeconfig

watch -n 1 ./oc get pods --all-namespaces
```

- It can take around **15-20 minutes** after *openshift-install create cluster* was called, until *oc get pods --all-namespaces* shows pods
- If all pods in the namespace **openshift-machine-api** are ready, three worker VMs should be created

Enjoy the web console

```
./oc get routes -n openshift-console
…
console console-openshift-console.apps.c2.okd4.<your domain>  console  https  reencrypt/Redirect None
…
```

User: kubeadmin
Password: <cat auth/kubeadmin-password>
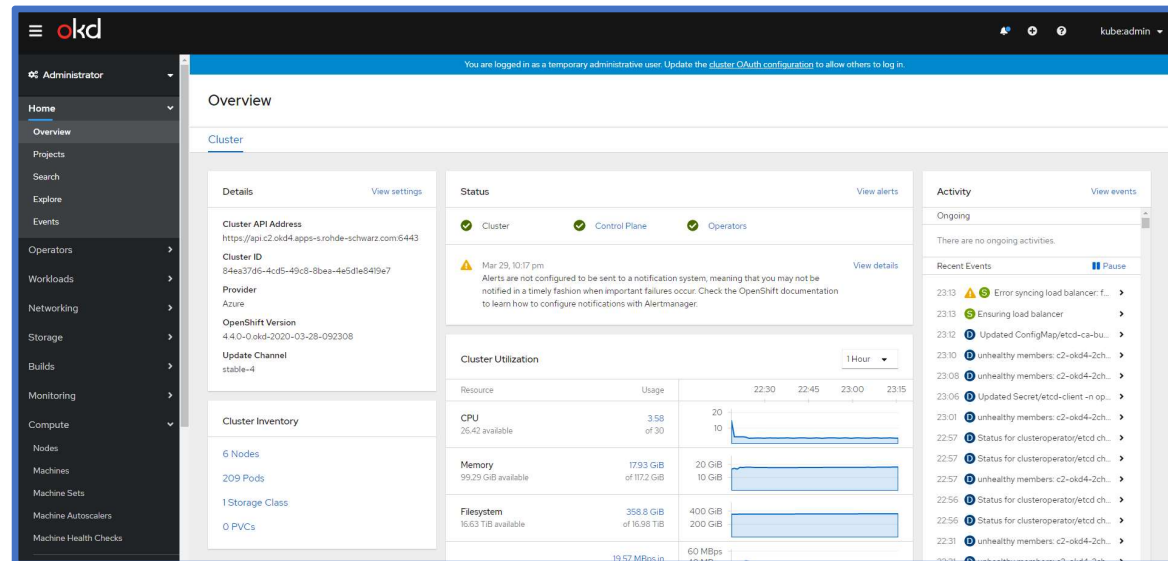
If something goes wrong #1

```
ssh core@<IP of bootstrap VM>
curl google.de        # You should have Internet access
sudo podman images    # < after a short time there should be images listed
sudo journalctl -f --no-pager  # watch for errors
sudo crictl logs <containerID>
```

- **If it takes forever** until the **control plane** comes up
  - give each master VM a public IPs, enable port 22 in their NSGs
  - ssh into VM and do the same as described above (*ssh core@<IP master VM>, curl google.de, sudo podman images, …*)
- Check if all masters are listed with *oc get csr* and their certs are approved:

```
./oc get csr

NAME        AGE    REQUESTOR                                    CONDITION
…
csr-bjszt   40m    system:node:c2-okd4-2chsr-master-0           Approved,Issued
csr-jt65q   40m    system:node:c2-okd4-2chsr-master-1           Approved,Issued
csr-qkn48   40m    system:node:c2-okd4-2chsr-master-2           Approved,Issued
```

- If not all masters show up after a reasonable waiting time you have bad luck <- destroy and recreate cluster !

13

If something goes wrong #2

Sometimes the VMs are in a state **where no images are pulled** by podman. **The VMs have an internet connection**.

- If the masters are affected, **I recreate the cluster**.
- If a worker is affected: **delete it** and **create a new one** by duplicating the Machine CR of an existing worker. The missing worker will be created afterwards by the machine-api operator and joins the cluster afterwards.

This effect **should be observed**.

Recap

Installation of OKD 4 currently is possible on Azure even if it takes sometimes a few attempts.

My **hack is not necessary anymore** if the FCOS image is **available** on the **Azure Marketplace**.

Sometimes there still are **effects during installation,** that must be observed. But if OKD **is installed**, it **seems to run stable**.

It's **lots of fun** to work with **OKD**: congrats to Red Hat and the community !

Thanks to Vadim, Christian, Dusty and many others for your support !

(Thanks to my wife that she always supports her engineer)

What should be improved?

- **Fedora CoreOS** should get on the Azure Marketplace <- my **hack** **would be not necessary** anymore

- **Biggest pain point** in OKD 3**:**
  Image Scanners were **reporting vulnerabilities** every few weeks in OKD 3 images. Must **patch the OKD images on our own** because some official OKD images **were rather old** -> OKD v4 images should be rebuilt **regularly**, not only if there are code commits. During rebuild of the images a **yum update** should **update all rpm packages in the image** at least **for getting hotfixes**.

- **GlusterFS** was very **unstable** in OKD 3

- **LDAP Sync creates lots of traffic** on our Active Directory servers in OKD (nested groups query). It should provide better caching algorithms of Users and Groups to reduce the load on the AD servers.

- **Update logging stack** (as example ElasticSearch is rather **outdated**)

- Docs about OpenShift's **internal architecture** (purpose of operators, diagrams, …)

- More **debugging features** (private keys for masters and workers in the bootstrap VM so we can ssh into them because they are all in the same private network, …)

Valuable information sources

- **Slack** channel #openshift-dev in Kubernetes Workspace
- https://github.com/openshift/okd   <- Open your **OKD issues** here. Docs are growing.
- https://origin-release.svc.ci.openshift.org/   <- **new versions**, changelogs
- https://github.com/openshift/community/projects/1 <- **OKD working group** boards
  - YouTube: OKD working group **videos** (meetings are bi weekly)
  - iCal **calendar**: https://apps.fedoraproject.org/calendar/ical/okd/
- https://docs.openshift.com/container-platform/4.3/welcome/index.html

- Main differences between OpenShift and OKD currently are here:
- https://github.com/openshift/installer
- https://github.com/openshift/machine-config-operator

Thank's for your attention !

Addendum

- In the recording of the video I describe a problem that has happened to me sometimes with **master/worker VMs not joining the Kubernetes cluster** and that caused me concern.
The root cause of that was that after the first boot of a VM a systemd service called „ machine-config-daemon-firstboot" tried to pull the initial docker image from OKDs CI registry once.

   In the last weeks the registry sometimes was overloaded, an image pull was not always possible. In this case the service tried to download the initial image, failed and with that the init of the VM failed. I opened an issue on openshift/okd for that today:
https://github.com/openshift/okd/issues/124, Vadim was already working on a fix for a simliar issue.
That one will pretty sure also fix „my" problem -> **the power of the community** ☺ !

- I installed a new cluster one day after the recording of this video: the **openshift-console** worked as expected. The root cause of that one could also be related to the mentioned one above (speculation) but it will be observed, because it happens rather rarely.