Standard Operating Procedure

*OSE Cert Upgrades*

## PURPOSE

The purpose of this standard operating procedure (SOP) is to provide a detailed step-by-step procedure to upgrade certs (except DTR cert, which is on a separate SOP).

## PROCEDURE

All Certs:

ansible-playbook -i /etc/ansible/hosts /usr/share/ansible/openshift-ansible/playbooks/byo/openshift-cluster/redeploy-openshift-ca.yml (this is also CA Cert)

ansible-playbook -i /etc/ansible/hosts /usr/share/ansible/openshift-ansible/playbooks/byo/openshift-cluster/redeploy-certificates.yml

ETCD Cert:

ansible-playbook -i /etc/ansible/hosts /usr/share/ansible/openshift-ansible/playbooks/byo/openshift-cluster/redeploy-etcd-ca.yml

ansible-playbook -i /etc/ansible/hosts /usr/share/ansible/openshift-ansible/playbooks/byo/openshift-cluster/redeploy-etcd-certificates.yml

Master Cert:

ansible-playbook -i /etc/ansible/hosts /usr/share/ansible/openshift-ansible/playbooks/byo/openshift-cluster/redeploy-master-certificates.yml

Node Cert:

ansible-playbook -i /etc/ansible/hosts /usr/share/ansible/openshift-ansible/playbooks/byo/openshift-cluster/redeploy-node-certificates.yml

Metrics Cert:

Metrics deployer creates hawkular certs and link them to hawkular secrets and hawkular cassandra secrets, so metrics must be redeployed:

1. Go to openshift-infra project:

oc project openshift-infra

1. Delete the following:

oc delete all --selector="metrics-infra"  
 oc delete sa --selector="metrics-infra"  
 oc delete templates --selector="metrics-infra"  
 oc delete secrets --selector="metrics-infra"  
 oc delete pvc --selector="metrics-infra"  
 oc delete sa metrics-deployer  
 oc delete secret metrics-deployer

1. Create metrics-deployer service account (SA):

echo "Creating Service Account..."  
 oc create -f - <<API  
 apiVersion: v1  
 kind: ServiceAccount  
 metadata:  
 name: metrics-deployer  
 secrets:  
 - name: metrics-deployer  
 API

1. Grant edit permissions to SA:

oadm policy add-role-to-user edit system:serviceaccount:openshift-infra:metrics-deployer

1. Add cluster-reader to heapster:

oadm policy add-cluster-role-to-user cluster-reader system:serviceaccount:openshift-infra:heapster

1. Create metrics-deployer secret without cert:

oc secrets new metrics-deployer nothing=/dev/null

1. Go to the directory where metrics-deployer.yaml resides (i.e. /home/svc-vxby-ose/OpenShift/environments/perf2-vxbyr/artifacts/metrics in CR Perf Red) and deploy metrics:

cd <path where metrics-deployer.yaml resides>

oc new-app -f metrics-deployer.yaml -p HAWKULAR\_METRICS\_HOSTNAME=hawkular-metrics.openshift-infra.ose-perf2-vxbyr.marriott.com -p USE\_PERSISTENT\_STORAGE=false

1. After all metrics pods come up, add pvc to Cassandra rc:

oc volume rc/hawkular-cassandra-1 --add --overwrite --name=cassandra-data -t pvc --claim-name=openshift-infra-metrics-pvc1

1. Delete all NFS data and restart metrics pods in sequential manner (Also in ‘Metrics Pods Not Restarting’ SOP):
   1. Try deleting Metrics pods which are crashed. Pods should come up.

oc project openshift-infra

oc get pods

oc delete pods <pod name>

Check the logs to see the issue:

oc logs -f <pod name>

If still pods are not coming up try delete pods one by one:

* + 1. Delete Hawkular Cassandra pods. This also takes a while to start up again due to the Cassandra DB volume:

oc delete pods <hawkular cassandra pod name>

* + 1. Delete heapster pods:

oc delete pods <heapster pod name>

* + 1. Delete Hawkular Metrics pods:

oc delete pods <hawkular metrics pod name>

* 1. If pods do not come up locate the nfs server metrics is using. **This is only applicable in Cloud Red (not in AWS).** AWS has EmptyDir listed in PV as it uses EFS instead of NFS. Deleting pods should be sufficient for AWS.

List all rc of openshift-infra project:

oc project openshift-infra

oc get rc

NAME                   DESIRED   CURRENT   AGE

hawkular-cassandra-1   1         1         1y

hawkular-metrics       1         1         1y

heapster               1         1         1y

Locate pvc that is used openshift-infra project

oc describe rc/hawkular-cassandra-1

Check under Volumes section for cassandra-data volume is using which pvc:

Volumes:

cassandra-data:

Type:  PersistentVolumeClaim (a reference to a PersistentVolumeClaim in the same namespace)

ClaimName:  <pvc name>

Read-only:  false

Describe pvc:

oc describe pvc/<pvc name>

Check under volume parameter for pv name:

Volume:         <pv name>

Describe pv:

oc describe pv/<pv name>

Find server IP and path:

i.e.

Server:  10.224.211.95

Path:  /u20

* 1. Delete nfs metrics data and try deleting pods again. Pods should come up now.

ssh nfs server IP:

ssh root@serverip

Go to path (i.e. u20)

If space is there on server, move metrics data to some other place for prod.

For devtest and perf delete metrics data directly.

Again, delete pods in sequence mentioned in step 1.

Hawkular-metrics pods should come up now.

1. Validate (see validations under ‘Metrics Cert’)

## VALIDATION

All Certs:

Look through expiration date of all certs:

for i in /etc/origin/master/\*.crt; do echo $i; openssl x509 -in $i -noout -enddate; done

i.e.

[root@master01-perf2-vxbyb ~]# for i in /etc/origin/master/\*.crt; do echo $i; openssl x509 -in $i -noout -enddate; done

/etc/origin/master/admin.crt

notAfter=Feb 17 15:21:28 2021 GMT

/etc/origin/master/ca-bundle.crt

notAfter=Feb 17 14:56:40 2024 GMT

/etc/origin/master/ca.crt

notAfter=Feb 17 14:56:40 2024 GMT

/etc/origin/master/etcd.server.crt

notAfter=Feb 17 15:21:29 2021 GMT

/etc/origin/master/master.etcd-ca.crt

notAfter=Feb 15 01:36:49 2022 GMT

…

Metrics Cert:

1. Go to openshift-infra project:

oc project openshift-infra

i.e.

[svc-vxby-ose@master01-devtest-vxbyr ~]$ oc project openshift-infra

Now using project "openshift-infra" on server "<https://ose-devtest-vxbyr.marriott.com:8443>".

1. Check for services:

oc get svc

i.e.

[svc-vxby-ose@master01-devtest-vxbyr ~]$ oc get svc

NAME CLUSTER-IP EXTERNAL-IP PORT(S) AGE

hawkular-cassandra 172.30.243.63 <none> 9042/TCP,9160/TCP,7000/TCP,7001/TCP 9h

hawkular-cassandra-nodes None <none> 9042/TCP,9160/TCP,7000/TCP,7001/TCP 9h

hawkular-metrics 172.30.190.136 <none> 443/TCP 9h

heapster 172.30.251.188 <none> 80/TCP 9h

1. Hit the service directly by curling hawkular-metrics IP and check for the hawkular expiration date:

curl -kv https://< hawkular-metrics IP>:443/hawkular/metrics/gauges/pod%2F6e29b312-4f49-11e9-a261-00505684f1ca%2Fcpu%2Frequest/tags

i.e.

[svc-vxby-ose@master01-devtest-vxbyr ~]$ curl -kv <https://172.30.190.136:443/hawkular/metrics/gauges/pod%2F6e29b312-4f49-11e9-a261-00505684f1ca%2Fcpu%2Frequest/tags>

\* About to connect() to 172.30.190.136 port 443 (#0)

\* Trying 172.30.190.136...

\* Connected to 172.30.190.136 (172.30.190.136) port 443 (#0)

\* Initializing NSS with certpath: sql:/etc/pki/nssdb

\* skipping SSL peer certificate verification

\* SSL connection using TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

\* Server certificate:

\* subject: CN=hawkular-metrics

\* start date: Mar 27 09:57:29 2019 GMT

\* expire date: Mar 26 09:57:30 2021 GMT

\* common name: hawkular-metrics

\* issuer: CN=metrics-signer@1553680649

> GET /hawkular/metrics/gauges/pod%2F6e29b312-4f49-11e9-a261-00505684f1ca%2Fcpu%2Frequest/tags HTTP/1.1

> User-Agent: curl/7.29.0

> Host: 172.30.190.136

> Accept: \*/\*

>

< HTTP/1.1 403 Forbidden

< Connection: keep-alive

< X-Powered-By: Undertow/1

< Server: WildFly/10

< Content-Length: 74

< Content-Type: text/html

< Date: Wed, 27 Mar 2019 19:32:00 GMT

<

\* Connection #0 to host 172.30.190.136 left intact

<html><head><title>Error</title></head><body>403 - Forbidden</body></html>

1. Check if metrics data started flowing on the console.

Router Cert:

1. Check if router-certs secrets are updated:

oc get secrets -n default | grep -i router

i.e.

[root@master01-perf2-vxbyb master]# oc get secrets -n default | grep -i router

ha-router-black-certs kubernetes.io/tls 2 1y

router-certs Opaque 1 40s

1. Use curl commands to see if routers are working fine:

curl -kv http://<infra node>/default.mi -H ‘Host:<host name>’

There should not be a 503 error.

i.e.

[root@master01-perf2-vxbyb master]# curl -kv http://infra01-perf2-vxbyb.marriott.com/default.mi -H 'Host:reservation-black-app-ram-preprodengage1.ose-perf2-vxbyb.marriott.com'

\* About to connect() to infra01-perf2-vxbyb.marriott.com port 80 (#0)

\* Trying 172.23.97.52...

\* Connected to infra01-perf2-vxbyb.marriott.com (172.23.97.52) port 80 (#0)

> GET /default.mi HTTP/1.1

> User-Agent: curl/7.29.0

> Accept: \*/\*

> Host:reservation-black-app-ram-preprodengage1.ose-perf2-vxbyb.marriott.com

>

< HTTP/1.1 404 Not Found

< Content-Type: text/plain; charset=utf-8

< Content-Length: 34

< Set-Cookie: 71c53c91d71adb5afa28bac44f223ce4=857c2319a523cb8a378b3f4015f4bcbe; path=/; HttpOnly

<

\* Connection #0 to host infra01-perf2-vxbyb.marriott.com left intact

Request URI: /default.mi not found[root@master01-perf2-vxbyb master]#

curl -kv https://foo.<environment>

i.e.

[root@master01-perf2-vxbyb master]# curl -kv https://foo.ose-perf2-vxbyb.marriott.com

\* About to connect() to foo.ose-perf2-vxbyb.marriott.com port 443 (#0)

\* Trying 172.23.96.14...

\* Connected to foo.ose-perf2-vxbyb.marriott.com (172.23.96.14) port 443 (#0)

\* Initializing NSS with certpath: sql:/etc/pki/nssdb

\* skipping SSL peer certificate verification

\* SSL connection using TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

\* Server certificate:

\* subject: OU=Example,O=Example,E=example@example.com,C=US,ST=SC,CN=www.example.com

\* start date: Jan 13 19:40:57 2016 GMT

\* expire date: Jan 10 19:40:57 2026 GMT

\* common name: www.example.com

\* issuer: E=example@example.com,CN=www.exampleca.com,OU=Test CA,O=Default Company Ltd,L=Default City,ST=SC,C=US

> GET / HTTP/1.1

> User-Agent: curl/7.29.0

ETCD Cert:

1. To check ETCD cluster health, run the following command in /etc/origin/master on a master node:

cd /etc/origin/master

etcdctl --endpoint=https://<master node IP>:2379 --cert-file=master.etcd-client.crt --key-file=master.etcd-client.key --ca-file=master.etcd-ca.crt cluster-health

i.e.

[root@master01-perf2-vxbyr ~]# cd /etc/origin/master

[root@master01-perf2-vxbyr master]# etcdctl --endpoint=https://172.23.116.14:2379 --cert-file=master.etcd-client.crt --key-file=master.etcd-client.key --ca-file=master.etcd-ca.crt cluster-health

member 98f791ffcdb18a6c is healthy: got healthy result from https://172.23.116.16:2379

member aed059c94589e4ae is healthy: got healthy result from https://172.23.116.15:2379

member d4039d8cff915118 is healthy: got healthy result from https://172.23.116.14:2379

cluster is healthy

UPDATE ROUTER CERTS:

1. cd /root# mkdir cert ; cd cert# CA=/etc/origin/master# oadm ca create-server-cert --signer-cert=$CA/ca.crt --signer-key=$CA/ca.key --signer-serial=$CA/ca.serial.txt --hostnames='\*.hostnames.for.the.certificate' --cert=router.crt --key=router.key

* # cat router.crt $CA/ca.crt router.key > router.pem

1. Backup the old certificate: (router-certs is the default name of the secret, as it's the name used by oadm router's --default-cert option)
2. # oc export secret router-certs > ~/old-router-certs-secret.yaml
3. Create a new Secret to hold the new certificate and key and replace the contents of the existing Secret: (router.pem is the file from step 1 containing the new certificate and its signing CA)
4. Oc project default
5. # oc secrets new router-certs tls.crt=router.pem tls.key=router.key \ -o json --type='kubernetes.io/tls' --confirm | \ oc replace -f -

* Re-deploy the component so that the new secret is mounted:
  + Prior to 3.4:
* [**Raw**](https://access.redhat.com/solutions/2650171#)
* # oc deploy dc/router --latest
  + From 3.4 onwards:
* [**Raw**](https://access.redhat.com/solutions/2650171#)
* # oc rollout latest router
* If you need to roll back to the previous secrets you can delete the new ones, re-create them from the backup taken in step 2 and re-deploy:

[**Raw**](https://access.redhat.com/solutions/2650171#)

# oc delete secret router-certs# oc create -f ~/old-router-certs-secret.yaml# oc deploy dc/router --latest // Prior to 3.4# oc rollout latest router

**Document Version Control**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Effective Date | Reviewed by | Approved by |
| 1.0 | 2/15/2019 | KyungIn Kim | Yashi Kumar |
|  |  |  |  |

Document Modification History & Revision Log

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Version | Date Modified | Revised by | Role | Section Affected | Reference | Remarks |
| 1.0 |  |  |  |  |  |  |
| 1.1 |  |  |  |  |  |  |