



Creating Private Image Registries: Red Hat OpenShift with NetApp

NetApp Solutions

Alan V Cowles, Nikhil M Kulkarni
August 05, 2021

Table of Contents

Creating Private Image Registries: Red Hat OpenShift with NetApp	1
Creating A Private Image Registry	1

Creating Private Image Registries: Red Hat OpenShift with NetApp

For most deployments of Red Hat OpenShift, using a public registry like [Quay.io](#) or [DockerHub](#) meets most customer's needs. However there are times when a customer may want to host their own private or customized images.

This procedure documents creating a private image registry which is backed by a persistent volume provided by Astra Trident and NetApp ONTAP.



Astra Control Center requires a registry to host the images the Astra containers require. The following section describes the steps to setup a private registry on Red Hat OpenShift cluster and pushing the images required to support the installation of Astra Control Center.

Creating A Private Image Registry

1. Edit the imageregistry operator, enter the below storage parameters to `spec` section

```
[netapp-user@rhel7 ~]$ oc edit
configs.imageregistry.operator.openshift.io

storage:
  pvc:
    claim:
```

2. Then enter the following parameters to `spec` section for creating a OpenShift route with a custom hostname, save and exit

```
routes:
- hostname: astra-registry.apps.ocp-vmw.cie.netapp.com
  name: netapp-astra-route
```



The above route config is used when you want a custom hostname for your route. If you want OpenShift to create a route with default hostname, you can just add the following parameters to `spec` section – `defaultRoute: true`

Custom TLS Certificates

When you are using custom hostname for the route, by default, it uses the default TLS configuration of OpenShift Ingress operator. However, you can add a custom TLS configuration to the route. To do so, following the below steps –

- a. Create a secret with the route's TLS certificates and key –

```
[netapp-user@rhel7 ~]$ oc create secret tls astra-route-tls -n openshift-image-registry --cert=/home/admin/netapp-astra/tls.crt --key=/home/admin/netapp-astra/tls.key
```

- b. Edit the imageregistry operator and add the following parameters to the `spec` section –

```
[netapp-user@rhel7 ~]$ oc edit configs.imageregistry.operator.openshift.io

routes:
  - hostname: astra-registry.apps.ocp-vmw.cie.netapp.com
    name: netapp-astra-route
    secretName: astra-route-tls
```

3. Next step is to edit the imageregistry operator again and change the management state of the operator to `Managed` state, save and exit –

```
oc edit configs.imageregistry/cluster

managementState: Managed
```

4. If all the pre-requisites are satisfied, it should start creating PVCs, pods and services for the private image registry. In a few minutes, the registry should be up.

```
[netapp-user@rhel7 ~]$ oc get all -n openshift-image-registry
```

NAME	READY	STATUS
RESTARTS AGE		
pod/cluster-image-registry-operator-74f6d954b6-rb7zr	1/1	Running
3 90d		
pod/image-pruner-1627257600-f5cpj	0/1	Completed
0 2d9h		
pod/image-pruner-1627344000-swqx9	0/1	Completed
0 33h		

pod/image-pruner-1627430400-rv5nt	0/1	Completed
0 9h		
pod/image-registry-6758b547f-6pnj8	1/1	Running
0 76m		
pod/node-ca-bwb5r	1/1	Running
0 90d		
pod/node-ca-f8w54	1/1	Running
0 90d		
pod/node-ca-gjx7h	1/1	Running
0 90d		
pod/node-ca-lcx4k	1/1	Running
0 33d		
pod/node-ca-v7zmx	1/1	Running
0 7d21h		
pod/node-ca-xpppp	1/1	Running
0 89d		

NAME	TYPE	CLUSTER-IP	EXTERNAL-
IP PORT(S) AGE			
service/image-registry	ClusterIP	172.30.196.167	<none>
5000/TCP 15h			
service/image-registry-operator	ClusterIP	None	<none>
60000/TCP 90d			

NAME	DESIRED	CURRENT	READY	UP-TO-DATE
AVAILABLE NODE SELECTOR AGE				
daemonset.apps/node-ca	6	6	6	6
kubernetes.io/os=linux 90d				

NAME	READY	UP-TO-DATE
AVAILABLE AGE		
deployment.apps/cluster-image-registry-operator	1/1	1
90d		
deployment.apps/image-registry	1/1	1
15h		

NAME	DESIRED
CURRENT READY AGE	
replicaset.apps/cluster-image-registry-operator-74f6d954b6	1
1 90d	
replicaset.apps/image-registry-6758b547f	1
1 76m	
replicaset.apps/image-registry-78bfbd7f59	0
0 15h	
replicaset.apps/image-registry-7fcc8d6cc8	0
0 80m	

```

replicaset.apps/image-registry-864f88f5b      0      0
0      15h
replicaset.apps/image-registry-cb47fffb      0      0
0      10h

NAME                                COMPLETIONS   DURATION   AGE
job.batch/image-pruner-1627257600      1/1           10s        2d9h
job.batch/image-pruner-1627344000      1/1           6s         33h
job.batch/image-pruner-1627430400      1/1           5s         9h

NAME                                SCHEDULE      SUSPEND     ACTIVE     LAST
SCHEDULE      AGE
cronjob.batch/image-pruner      0 0 * * *      False       0          9h
90d

NAME                                HOST/PORT
PATH      SERVICES      PORT      TERMINATION  WILDCARD
route.route.openshift.io/public-routes  astra-registry.apps.ocp-
vmw.cie.netapp.com              image-registry  <all>      reencrypt    None

```

5. If you are using the default TLS certificates of Ingress operator OpenShift registry route, you can fetch the TLS certificates using the below command.

```

[netapp-user@rhel7 ~]$ oc extract secret/router-ca --keys=tls.crt -n
openshift-ingress-operator

```

6. To allow OpenShift nodes to access and pull the images from the registry, you need to add the certificates to the docker client on the OpenShift nodes. Create a configmap in `openshift-config` namespace using the TLS certificates and patch it to the cluster image config to make the certificate trusted.

```

[netapp-user@rhel7 ~]$ oc create configmap astra-ca -n openshift-config
--from-file=astra-registry.apps.ocp-vmw.cie.netapp.com=tls.crt

[netapp-user@rhel7 ~]$ oc patch image.config.openshift.io/cluster
--patch '{"spec":{"additionalTrustedCA":{"name":"astra-ca"}}}'
--type=merge

```

7. OpenShift internal registry is controlled by authentication. All the OpenShift users can access the OpenShift registry, but the operations that the logged in user can perform depends on the user permissions.
- To allow a user/group of users to pull images from the registry, the user/s must have registry-viewer role assigned.

```
[netapp-user@rhel7 ~]$ oc policy add-role-to-user registry-viewer  
ocp-user
```

```
[netapp-user@rhel7 ~]$ oc policy add-role-to-group registry-viewer  
ocp-user-group
```

- b. To allow a user/group of users to write or push images, the user/s must have registry-editor role assigned.

```
[netapp-user@rhel7 ~]$ oc policy add-role-to-user registry-editor  
ocp-user
```

```
[netapp-user@rhel7 ~]$ oc policy add-role-to-group registry-editor  
ocp-user-group
```

8. For OpenShift nodes to access the registry and push/pull the images, you will need to configure a pull secret.

```
[netapp-user@rhel7 ~]$ oc create secret docker-registry astra-registry-  
credentials --docker-server= astra-registry.apps.ocp-vmw.cie.netapp.com  
--docker-username=ocp-user --docker-password=password
```

9. This pull secret can then be patched to serviceaccounts or be referenced in the corresponding pod definition.

- a. To patch it to service accounts

```
[netapp-user@rhel7 ~]$ oc secrets link <service_account_name> astra-  
registry-credentials --for=pull
```

- b. To reference the pull secret in Pod definition, add the following parameter to the 'spec' section.

```
imagePullSecrets:  
  - name: astra-registry-credentials
```

10. To push/pull an image from workstations apart from OpenShift node.

- a. Add the TLS certificates to the docker client.

```
[netapp-user@rhel7 ~]$ sudo mkdir /etc/docker/certs.d/astra-registry.apps.ocp-vmw.cie.netapp.com

[netapp-user@rhel7 ~]$ sudo cp /path/to/tls.crt
/etc/docker/certs.d/astra-registry.apps.ocp-vmw.cie.netapp.com
```

b. Log into OpenShift using oc login command.

```
[netapp-user@rhel7 ~]$ oc login --token=sha256~D49SpB_lesSrJYwrM0LIO-VRcjWHu0a27vKa0 --server=https://api.ocp-vmw.cie.netapp.com:6443
```

c. Log into the registry using OpenShift user credentials via podman/docker command.

podman

```
[netapp-user@rhel7 ~]$ podman login astra-registry.apps.ocp-vmw.cie.netapp.com -u kubeadmin -p $(oc whoami -t)
```

docker

```
[netapp-user@rhel7 ~]$ docker login astra-registry.apps.ocp-vmw.cie.netapp.com -u kubeadmin -p $(oc whoami -t)
```

d. Push/pull the images.

podman

```
[netapp-user@rhel7 ~]$ podman push astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra/vault-controller:latest
[netapp-user@rhel7 ~]$ podman pull astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra/vault-controller:latest
```

docker

```
[netapp-user@rhel7 ~]$ docker push astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra/vault-controller:latest
[netapp-user@rhel7 ~]$ docker pull astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra/vault-controller:latest
```

Next: [Solution Validation/Use Cases: Red Hat OpenShift with NetApp.](#)

Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.