Configuring registries for OpenShift Container Platform
OpenShift Container Platform 4.4 Registry

Configuring registries for OpenShift Container Platform
Abstract

This document provides instructions for configuring and managing the internal registry for OpenShift Container Platform. It also provides a general overview of registries associated with OpenShift Container Platform.
Table of Contents

CHAPTER 1. IMAGE REGISTRY ................................................................. 4
  1.1. INTEGRATED OPENSİFT CONTAINER PLATFORİ PLATFORM REGISTRY  4

CHAPTER 2. IMAGE REGISTRY OPERATOR İN OPENSİFT CONTAINER PLATFORM .......... 5
  2.1. IMAGE REGISTRY ON CLOUD PLATFORMS AND OPENSTACK  5
  2.2. IMAGE REGISTRY ON BARE METAL AND VSİHERE  5
    2.2.1. Image registry removed during installation  5
  2.3. IMAGE REGISTRY OPERATOR CONFIGURATION PARAMETERS  6
  2.4. ENABLE THE IMAGE REGISTRY DEFAULT ROUTE WITH THE CUSTOM RESOURCE DEFINITION 6
  2.5. CONFIGURING ADDİONAL TRUST STORES FOR IMAGE REGISTRY ACCESS  7
  2.6. CONFIGURING STORAGE CREDENTİALS FOR THE IMAGE REGISTRY OPERATOR  8
  2.7. ADDİONAL RESOURCES  8

CHAPTER 3. SETİNG UP AND CONFIGURING THE REGİSTERY ............................... 9
  3.1. CONFIGURING THE REGİSTERY FOR AWS USER-PROVISIONED INFRASTRUCTURE  9
    3.1.1. Configuring a secret for the Image Registry Operator  9
    3.1.2. Configuring registry storage for AWS with user-provisioned infrastructure  9
    3.1.3. Image Registry Operator configuration parameters for AWS S3  10
  3.2. CONFIGURING THE REGİSTERY FOR GCP USER-PROVISIONED INFRASTRUCTURE  10
    3.2.1. Configuring a secret for the Image Registry Operator  10
    3.2.2. Registry storage for GCP with user-provisioned infrastructure  11
    3.2.3. Image Registry Operator configuration parameters for GCP GCS  11
  3.3. CONFIGURING THE REGİSTERY FOR AZURE USER-PROVISIONED INFRASTRUCTURE  12
    3.3.1. Configuring a secret for the Image Registry Operator  12
    3.3.2. Configuring registry storage for Azure  12
  3.4. CONFIGURING THE REGİSTERY FOR BARE METAL  13
    3.4.1. Image registry removed during installation  13
    3.4.2. Changing the image registry’s management state  13
    3.4.3. Image registry storage configuration  13
    3.4.4. Configuring registry storage for bare metal  13
    3.4.5. Configuring storage for the image registry in non-production clusters  14
    3.4.6. Configuring block registry storage for bare metal  15
    3.4.7. Additional resources  15
  3.5. CONFIGURING THE REGİSTERY FOR VSİHERE  15
    3.5.1. Image registry removed during installation  16
    3.5.2. Changing the image registry’s management state  16
      3.5.2.1. Image registry storage configuration  16
    3.5.3. Configuring registry storage for VMware vSphere  16
    3.5.4. Configuring storage for the image registry in non-production clusters  18
    3.5.5. Configuring block registry storage for VMware vSphere  18
    3.5.6. Additional resources  19

CHAPTER 4. REGİSTERY OPTIONS ......................................................... 20
  4.1. INTEGRATED OPENSİFT CONTAINER PLATFORİ PLATFORM REGİSTERY  20
  4.2. THIRD PARTY REGİSTRIES  20
    4.2.1. Authentication  20
  4.3. RED HAT QUAY REGİSTRIES  20
  4.4. AUTHENTICATION ENABLED RED HAT REGİSTERY  21

CHAPTER 5. ACCESSİNG THE REGİSTERY .................................................. 22
  5.1. PREREGUISTİES  22
  5.2. ACCESSİNG REGİSTERY DIRECTLY FROM THE CLUSTER  22
CHAPTER 1. IMAGE REGISTRY

1.1. INTEGRATED OPENSSHIFT CONTAINER PLATFORM REGISTRY

OpenShift Container Platform provides a built-in container image registry which runs as a standard workload on the cluster. The registry is configured and managed by an infrastructure operator. It provides an out of the box solution for users to manage the images that run their workloads, and runs on top of the existing cluster infrastructure. This registry can be scaled up or down like any other cluster workload and does not require specific infrastructure provisioning. In addition, it is integrated into the cluster user authentication and authorization system which means that access to create and retrieve images is controlled by defining user permissions on the image resources.

The registry is typically used as a publication target for images built on the cluster as well as a source of images for workloads running on the cluster. When a new image is pushed to the registry, the cluster is notified of the new image and other components can react to and consume the updated image.

Image data is stored in two locations. The actual image data is stored in a configurable storage location such as cloud storage or a filesystem volume. The image metadata, which is exposed by the standard cluster APIs and is used to perform access control, is stored as standard API resources, specifically images and imagestreams.

Additional resources

- Image Registry Operator in OpenShift Container Platform
CHAPTER 2. IMAGE REGISTRY OPERATOR IN OPENSHIFT CONTAINER PLATFORM

2.1. IMAGE REGISTRY ON CLOUD PLATFORMS AND OPENSTACK

The Image Registry Operator installs a single instance of the OpenShift Container Platform registry, and manages all registry configuration, including setting up registry storage.

**NOTE**

Storage is only automatically configured when you install an installer-provisioned infrastructure cluster on AWS, GCP, Azure, or OpenStack.

After the control plane deploys, the Operator will create a default configs.imageregistry.operator.openshift.io resource instance based on configuration detected in the cluster.

If insufficient information is available to define a complete configs.imageregistry.operator.openshift.io resource, the incomplete resource will be defined and the Operator will update the resource status with information about what is missing.

The Image Registry Operator runs in the openshift-image-registry namespace, and manages the registry instance in that location as well. All configuration and workload resources for the registry reside in that namespace.

**IMPORTANT**

The Image Registry Operator’s behavior for managing the pruner is orthogonal to the managementState specified on the ClusterOperator object for the Image Registry Operator. If the Image Registry Operator is not in the Managed state, the image pruner can still be configured and managed by the Pruning custom resource.

However, the managementState of the Image Registry Operator alters the behavior of the deployed image pruner job:

- Managed: the --prune-registry flag for the image pruner is set to true.
- Removed: the --prune-registry flag for the image pruner is set to false, meaning it only prunes image metadata in etcd.
- Unmanaged: the --prune-registry flag for the image pruner is set to false.

2.2. IMAGE REGISTRY ON BARE METAL AND VSPHERE

2.2.1. Image registry removed during installation

On platforms that do not provide shareable object storage, the OpenShift Image Registry Operator bootstraps itself as Removed. This allows openshift-installer to complete installations on these platform types.

After installation, you must edit the Image Registry Operator configuration to switch the managementState from Removed to Managed.
NOTE

The Prometheus console provides an ImageRegistryRemoved alert, for example:

"Image Registry has been removed. ImageStreamTags, BuildConfigs and DeploymentConfigs which reference ImageStreamTags may not work as expected. Please configure storage and update the config to Managed state by editing configs.imageregistry.operator.openshift.io."

2.3. IMAGE REGISTRY OPERATOR CONFIGURATION PARAMETERS

The configs.imageregistry.operator.openshift.io resource offers the following configuration parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>managementState</td>
<td><strong>Managed</strong>: The Operator updates the registry as configuration resources are updated.</td>
</tr>
<tr>
<td></td>
<td><strong>Unmanaged</strong>: The Operator ignores changes to the configuration resources.</td>
</tr>
<tr>
<td></td>
<td><strong>Removed</strong>: The Operator removes the registry instance and tear down any storage that the Operator provisioned.</td>
</tr>
<tr>
<td>logging</td>
<td>Sets loglevel of the registry instance.</td>
</tr>
<tr>
<td>httpSecret</td>
<td>Value needed by the registry to secure uploads, generated by default.</td>
</tr>
<tr>
<td>proxy</td>
<td>Defines the Proxy to be used when calling master API and upstream registries.</td>
</tr>
<tr>
<td>storage</td>
<td><strong>Storagetype</strong>: Details for configuring registry storage, for example S3 bucket coordinates. Normally configured by default.</td>
</tr>
<tr>
<td>readOnly</td>
<td>Indicates whether the registry instance should reject attempts to push new images or delete existing ones.</td>
</tr>
<tr>
<td>requests</td>
<td>API Request Limit details. Controls how many parallel requests a given registry instance will handle before queuing additional requests.</td>
</tr>
<tr>
<td>defaultRoute</td>
<td>Determines whether or not an external route is defined using the default hostname. If enabled, the route uses re-encrypt encryption. Defaults to false.</td>
</tr>
<tr>
<td>routes</td>
<td>Array of additional routes to create. You provide the hostname and certificate for the route.</td>
</tr>
<tr>
<td>replicas</td>
<td>Replica count for the registry.</td>
</tr>
</tbody>
</table>

2.4. ENABLE THE IMAGE REGISTRY DEFAULT ROUTE WITH THE CUSTOM RESOURCE DEFINITION
In OpenShift Container Platform, the Registry Operator controls the registry feature. The Operator is defined by the `configs.imageregistry.operator.openshift.io` Custom Resource Definition (CRD).

If you need to automatically enable the Image Registry default route, patch the Image Registry Operator CRD.

**Procedure**

- Patch the Image Registry Operator CRD:

  ```
  $ oc patch configs.imageregistry.operator.openshift.io/cluster --type merge -p "{"spec":
  {"defaultRoute":true}}"
  ```

### 2.5. CONFIGURING ADDITIONAL TRUST STORES FOR IMAGE REGISTRY ACCESS

The `image.config.openshift.io/cluster` custom resource can contain a reference to a ConfigMap that contains additional certificate authorities to be trusted during image registry access.

**Prerequisites**

- The CAs must be PEM-encoded.

**Procedure**

You can create a ConfigMap in the `openshift-config` namespace and use its name in `AdditionalTrustedCA` in the `image.config.openshift.io` custom resource to provide additional CAs that should be trusted when contacting external registries.

The ConfigMap key is the host name of a registry with the port for which this CA is to be trusted, and the base64-encoded certificate is the value, for each additional registry CA to trust.

**Image registry CA ConfigMap example**

```yaml
apiVersion: v1
kind: ConfigMap
metadata:
  name: my-registry-ca
data:
  registry.example.com: |
    -----BEGIN CERTIFICATE-----
    ...
    -----END CERTIFICATE-----
  registry-with-port.example.com:5000: |
    -----BEGIN CERTIFICATE-----
    ...
    -----END CERTIFICATE-----
```

1. If the registry has the port, such as `registry-with-port.example.com:5000`, the colon should be replaced with `:`.

You can configure additional CAs with the following procedure.
1. To configure an additional CA:

```bash
$ oc create configmap registry-config --from-file=<external_registry_address>=ca.crt -n openshift-config
$ oc edit image.config.openshift.io cluster
spec:
  additionalTrustedCA:
    name: registry-config
```

### 2.6. CONFIGURING STORAGE CREDENTIALS FOR THE IMAGE REGISTRY OPERATOR

In addition to the `configs.imageregistry.operator.openshift.io` and ConfigMap resources, storage credential configuration is provided to the Operator by a separate secret resource located within the `openshift-image-registry` namespace.

The `image-registry-private-configuration-user` secret provides credentials needed for storage access and management. It overrides the default credentials used by the Operator, if default credentials were found.

**Procedure**

- Create an OpenShift Container Platform secret that contains the required keys.

```bash
$ oc create secret generic image-registry-private-configuration-user --from-file=KEY1=value1 --from-literal=KEY2=value2 --namespace openshift-image-registry
```

### 2.7. ADDITIONAL RESOURCES

- Configuring the registry for AWS user-provisioned infrastructure
- Configuring the registry for GCP user-provisioned infrastructure
- Configuring the registry for Azure user-provisioned infrastructure
- Configuring the registry for bare metal
- Configuring the registry for vSphere
CHAPTER 3. SETTING UP AND CONFIGURING THE REGISTRY

3.1. CONFIGURING THE REGISTRY FOR AWS USER-PROVISIONED INFRASTRUCTURE

3.1.1. Configuring a secret for the Image Registry Operator

In addition to the configs.imageregistry.operator.openshift.io and ConfigMap resources, configuration is provided to the Operator by a separate secret resource located within the openshift-image-registry namespace.

The image-registry-private-configuration-user secret provides credentials needed for storage access and management. It overrides the default credentials used by the Operator, if default credentials were found.

For S3 on AWS storage the secret is expected to contain two keys:

- REGISTRY_STORAGE_S3_ACCESSKEY
- REGISTRY_STORAGE_S3_SECRETKEY

Procedure

- Create an OpenShift Container Platform secret that contains the required keys.

  $ oc create secret generic image-registry-private-configuration-user --from-literal=REGISTRY_STORAGE_S3_ACCESSKEY=myaccesskey --from-literal=REGISTRY_STORAGE_S3_SECRETKEY=mysecretkey --namespace openshift-image-registry

3.1.2. Configuring registry storage for AWS with user-provisioned infrastructure

During installation, your cloud credentials are sufficient to create an S3 bucket and the Registry Operator will automatically configure storage.

If the Registry Operator cannot create an S3 bucket and automatically configure storage, you can create an S3 bucket and configure storage with the following procedure.

Prerequisites

- A cluster on AWS with user-provisioned infrastructure.
- For S3 on AWS storage the secret is expected to contain two keys:
  - REGISTRY_STORAGE_S3_ACCESSKEY
  - REGISTRY_STORAGE_S3_SECRETKEY

Procedure

Use the following procedure if the Registry Operator cannot create an S3 bucket and automatically configure storage.

1. Set up a Bucket Lifecycle Policy to abort incomplete multipart uploads that are one day old.
2. Fill in the storage configuration in `configs.imageregistry.operator.openshift.io/cluster`:

```bash
$ oc edit configs.imageregistry.operator.openshift.io/cluster
```

```yaml
storage:
  s3:
    bucket: <bucket-name>
    region: <region-name>
```

**WARNING**

To secure your registry images in AWS, block public access to the S3 bucket.

### 3.1.3. Image Registry Operator configuration parameters for AWS S3

The following configuration parameters are available for AWS S3 registry storage.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bucket</td>
<td>Bucket is the bucket name in which you want to store the registry's data. It is optional and is generated if not provided.</td>
</tr>
<tr>
<td>region</td>
<td>Region is the AWS region in which your bucket exists. It is optional and is set based on the installed AWS Region.</td>
</tr>
<tr>
<td>regionEndpoint</td>
<td>RegionEndpoint is the endpoint for S3 compatible storage services. It is optional and defaults based on the Region that is provided.</td>
</tr>
<tr>
<td>encrypt</td>
<td>Encrypt specifies whether or not the registry stores the image in encrypted format. It is optional and defaults to false.</td>
</tr>
<tr>
<td>keyID</td>
<td>KeyID is the KMS key ID to use for encryption. It is optional. Encrypt must be true, or this parameter is ignored.</td>
</tr>
<tr>
<td>ImageRegistryConfigStorageS3CloudFront</td>
<td>CloudFront configures Amazon Cloudfront as the storage middleware in a registry. It is optional.</td>
</tr>
</tbody>
</table>

### 3.2. CONFIGURING THE REGISTRY FOR GCP USER-PROVISIONED INFRASTRUCTURE

#### 3.2.1. Configuring a secret for the Image Registry Operator

In addition to the `configs.imageregistry.operator.openshift.io` and ConfigMap resources, configuration is provided to the Operator by a separate secret resource located within the `openshift-image-registry` namespace.
The `image-registry-private-configuration-user` secret provides credentials needed for storage access and management. It overrides the default credentials used by the Operator, if default credentials were found.

For GCS on GCP storage the secret is expected to contain one key whose value is the contents of a credentials file provided by GCP:

- **REGISTRY_STORAGE_GCS_KEYFILE**

Procedure

- Create an OpenShift Container Platform secret that contains the required keys.

  ```bash
  $ oc create secret generic image-registry-private-configuration-user --from-file=REGISTRY_STORAGE_GCS_KEYFILE=<path_to_keyfile> --namespace openshift-image-registry
  ```

### 3.2.2. Registry storage for GCP with user-provisioned infrastructure

You must set up the storage medium manually and configure the settings in the registry CRD.

**Prerequisites**

- A cluster on GCP with user-provisioned infrastructure.
- To configure registry storage for GCP, you need to provide Registry Operator cloud credentials.
- For GCS on GCP storage the secret is expected to contain one key whose value is the contents of a credentials file provided by GCP:
  - **REGISTRY_STORAGE_GCS_KEYFILE**

### 3.2.3. Image Registry Operator configuration parameters for GCP GCS

**Procedure**

The following configuration parameters are available for GCP GCS registry storage.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bucket</td>
<td>Bucket is the bucket name in which you want to store the registry's data. It is optional and is generated if not provided.</td>
</tr>
<tr>
<td>region</td>
<td>Region is the GCS location in which your bucket exists. It is optional and is set based on the installed GCS Region.</td>
</tr>
<tr>
<td>projectID</td>
<td>ProjectID is the Project ID of the GCP project that this bucket should be associated with. It is optional.</td>
</tr>
<tr>
<td>keyID</td>
<td>KeyID is the KMS key ID to use for encryption. It is optional because buckets are encrypted by default on GCP. This allows for the use of a custom encryption key.</td>
</tr>
</tbody>
</table>
3.3. CONFIGURING THE REGISTRY FOR AZURE USER-PROVISIONED INFRASTRUCTURE

3.3.1. Configuring a secret for the Image Registry Operator

In addition to the `configs.imageregistry.operator.openshift.io` and ConfigMap resources, configuration is provided to the Operator by a separate secret resource located within the `openshift-image-registry` namespace.

The `image-registry-private-configuration-user` secret provides credentials needed for storage access and management. It overrides the default credentials used by the Operator, if default credentials were found.

For Azure registry storage the secret is expected to contain one key whose value is the contents of a credentials file provided by Azure:

- `REGISTRY_STORAGE_AZURE_ACCOUNTKEY`

**Procedure**

- Create an OpenShift Container Platform secret that contains the required key.

  ```
  $ oc create secret generic image-registry-private-configuration-user --from-literal=REGISTRY_STORAGE_AZURE_ACCOUNTKEY=<accountkey> --namespace openshift-image-registry
  ```

3.3.2. Configuring registry storage for Azure

During installation, your cloud credentials are sufficient to create Azure Blob Storage, and the Registry Operator automatically configures storage.

**Prerequisites**

- A cluster on Azure with user-provisioned infrastructure.

- To configure registry storage for Azure, provide Registry Operator cloud credentials.

- For Azure storage the secret is expected to contain one key:

  - `REGISTRY_STORAGE_AZURE_ACCOUNTKEY`

**Procedure**

1. Create an Azure storage container.

2. Fill in the storage configuration in `configs.imageregistry.operator.openshift.io/cluster`:

   ```
   $ oc edit configs.imageregistry.operator.openshift.io/cluster
   
   storage:
   azure:
     accountName: <storage-account-name>
     container: <container-name>
   ```
3.4. CONFIGURING THE REGISTRY FOR BARE METAL

3.4.1. Image registry removed during installation

On platforms that do not provide shareable object storage, the OpenShift Image Registry Operator bootstraps itself as **Removed**. This allows **openshift-installer** to complete installations on these platform types.

After installation, you must edit the Image Registry Operator configuration to switch the **managementState** from **Removed** to **Managed**.

**NOTE**

The Prometheus console provides an **ImageRegistryRemoved** alert, for example:

"Image Registry has been removed. **ImageStreamTags**, **BuildConfigs** and **DeploymentConfigs** which reference **ImageStreamTags** may not work as expected. Please configure storage and update the config to **Managed** state by editing configs.imageregistry.operator.openshift.io."

3.4.2. Changing the image registry’s management state

To start the image registry, you must change the Image Registry Operator configuration’s **managementState** from **Removed** to **Managed**.

**Procedure**

- Change **managementState** Image Registry Operator configuration from **Removed** to **Managed**. For example:

  ```
  $ oc patch configs.imageregistry.operator.openshift.io cluster --type merge --patch '{"spec": {
  "managementState": "Managed"
  }}'
  ```

3.4.3. Image registry storage configuration

The Image Registry Operator is not initially available for platforms that do not provide default storage. After installation, you must configure your registry to use storage so the Registry Operator is made available.

Instructions for both configuring a persistent volume, which is required for production clusters, and for configuring an empty directory as the storage location, which is available for only non-production clusters, are shown.

3.4.4. Configuring registry storage for bare metal

As a cluster administrator, following installation you must configure your registry to use storage.

**Prerequisites**

- Cluster administrator permissions.
- A cluster on bare metal.
- Persistent storage provisioned for your cluster, such as Red Hat OpenShift Container Storage.

**IMPORTANT**

OpenShift Container Platform supports **ReadWriteOnce** access for image registry storage when you have only one replica. To deploy an image registry that supports high availability with two or more replicas, **ReadWriteMany** access is required.

- Must have 100Gi capacity.

**Procedure**

1. To configure your registry to use storage, change the `spec.storage.pvc` in the `configs.imageregistry/cluster` resource.

   **NOTE**

   When using shared storage, review your security settings to prevent outside access.

2. Verify that you do not have a registry pod:

   ```bash
   $ oc get pod -n openshift-image-registry
   ```

   **NOTE**

   If the storage type is **emptyDIR**, the replica number cannot be greater than 1.

3. Check the registry configuration:

   ```bash
   $ oc edit configs.imageregistry.operator.openshift.io
   ```

   **Example output**

   ```yaml
   storage:
   pvc:
   claim:
   ```

   Leave the `claim` field blank to allow the automatic creation of an `image-registry-storage` PVC.

4. Check the `clusteroperator` status:

   ```bash
   $ oc get clusteroperator image-registry
   ```

### 3.4.5. Configuring storage for the image registry in non-production clusters

You must configure storage for the Image Registry Operator. For non-production clusters, you can set the image registry to an empty directory. If you do so, all images are lost if you restart the registry.

**Procedure**
### 3.4.6. Configuring block registry storage for bare metal

To allow the image registry to use block storage types during upgrades as a cluster administrator, you can use the **Recreate** rollout strategy.

**IMPORTANT**

Block storage volumes are supported but not recommended for use with the image registry on production clusters. An installation where the registry is configured on block storage is not highly available because the registry cannot have more than one replica.

**Procedure**

1. To set the image registry storage as a block storage type, patch the registry so that it uses the **Recreate** rollout strategy and runs with only one (1) replica:

   ```
   $ oc patch config.imageregistry.operator.openshift.io/cluster --type=merge -p ' htonspec":
   {"rolloutStrategy":"Recreate","replicas":1})'
   ```

2. Provision the PV for the block storage device, and create a PVC for that volume. The requested block volume uses the ReadWriteOnce (RWO) access mode.

3. Edit the registry configuration so that it references the correct PVC.

### 3.4.7. Additional resources

For more details about configuring registry storage for bare metal, see [Recommended configurable storage technology](#).

### 3.5. CONFIGURING THE REGISTRY FOR VSPHERE
3.5.1. Image registry removed during installation

On platforms that do not provide shareable object storage, the OpenShift Image Registry Operator boots itself as Removed. This allows openshift-installer to complete installations on these platform types.

After installation, you must edit the Image Registry Operator configuration to switch the managementState from Removed to Managed.

NOTE
The Prometheus console provides an ImageRegistryRemoved alert, for example:

"Image Registry has been removed. ImageStreamTags, BuildConfigs and DeploymentConfigs which reference ImageStreamTags may not work as expected. Please configure storage and update the config to Managed state by editing configs.imageregistry.operator.openshift.io."

3.5.2. Changing the image registry’s management state

To start the image registry, you must change the Image Registry Operator configuration’s managementState from Removed to Managed.

Procedure

- Change managementState Image Registry Operator configuration from Removed to Managed. For example:

  $ oc patch configs.imageregistry.operator.openshift.io cluster --type merge --patch '{"spec": {"managementState":"Managed"}}'

3.5.2.1. Image registry storage configuration

The Image Registry Operator is not initially available for platforms that do not provide default storage. After installation, you must configure your registry to use storage so the Registry Operator is made available.

Instructions for both configuring a persistent volume, which is required for production clusters, and for configuring an empty directory as the storage location, which is available for only non-production clusters, are shown.

3.5.3. Configuring registry storage for VMware vSphere

As a cluster administrator, following installation you must configure your registry to use storage.

Prerequisites

- Cluster administrator permissions.
- A cluster on VMware vSphere.
- Persistent storage provisioned for your cluster, such as Red Hat OpenShift Container Storage.
IMPORTANT

OpenShift Container Platform supports **ReadWriteOnce** access for image registry storage when you have only one replica. To deploy an image registry that supports high availability with two or more replicas, **ReadWriteMany** access is required.

- Must have "100Gi" capacity.

IMPORTANT

Testing shows issues with using the NFS server on RHEL as storage backend for core services. This includes the OpenShift Container Registry and Quay, Prometheus for monitoring storage, and Elasticsearch for logging storage. Therefore, using RHEL NFS to back PVs used by core services is not recommended.

Other NFS implementations on the marketplace might not have these issues. Contact the individual NFS implementation vendor for more information on any testing that was possibly completed against these OpenShift Container Platform core components.

Procedure

1. To configure your registry to use storage, change the `spec.storage.pvc` in the `configs.imageregistry/cluster` resource.

   **NOTE**
   
   When using shared storage, review your security settings to prevent outside access.

2. Verify that you do not have a registry pod:

   ```
   $ oc get pod -n openshift-image-registry
   ```

   **NOTE**
   
   If the storage type is **emptyDir**, the replica number cannot be greater than 1.

3. Check the registry configuration:

   ```
   $ oc edit configs.imageregistry.operator.openshift.io
   ```

   **Example output**

   ```
   storage:
   pvc:
     claim: 1
   ```

   Leave the `claim` field blank to allow the automatic creation of an `image-registry-storage` PVC.
3.5.4. Configuring storage for the image registry in non-production clusters

You must configure storage for the Image Registry Operator. For non-production clusters, you can set the image registry to an empty directory. If you do so, all images are lost if you restart the registry.

Procedure

- To set the image registry storage to an empty directory:

  ```bash
  $ oc patch configs.imageregistry.operator.openshift.io cluster --type merge --patch '{"spec":
  {"storage":{"emptyDir":{}}}}'
  ```

**WARNING**

Configure this option for only non-production clusters.

If you run this command before the Image Registry Operator initializes its components, the `oc patch` command fails with the following error:

```
Error from server (NotFound): configs.imageregistry.operator.openshift.io "cluster" not found
```

Wait a few minutes and run the command again.

3.5.5. Configuring block registry storage for VMware vSphere

To allow the image registry to use block storage types such as vSphere Virtual Machine Disk (VMDK) during upgrades as a cluster administrator, you can use the `Recreate` rollout strategy.

**IMPORTANT**

Block storage volumes are supported but not recommended for use with image registry on production clusters. An installation where the registry is configured on block storage is not highly available because the registry cannot have more than one replica.

Procedure

1. To set the image registry storage as a block storage type, patch the registry so that it uses the `Recreate` rollout strategy and runs with only 1 replica:

  ```bash
  $ oc patch config.imageregistry.operator.openshift.io/cluster --type=merge -p '{"spec":
  {"rolloutStrategy":"Recreate","replicas":1}}'
  ```
2. Provision the PV for the block storage device, and create a PVC for that volume. The requested block volume uses the ReadWriteOnce (RWO) access mode.

   a. Create a `pvc.yaml` file with the following contents to define a VMware vSphere PersistentVolumeClaim object:

   ```yaml
   kind: PersistentVolumeClaim
   apiVersion: v1
   metadata:
     name: image-registry-storage
   spec:
     accessModes:
     - ReadWriteOnce
     resources:
       requests:
         storage: 100Gi
   ```

   1. A unique name that represents the PersistentVolumeClaim object.
   2. The access mode of the PersistentVolumeClaim. With ReadWriteOnce, the volume can be mounted with read and write permissions by a single node.
   3. The size of the PersistentVolumeClaim.

   b. Create the PersistentVolumeClaim object from the file:

   ```sh
   $ oc create -f pvc.yaml
   ```

3. Edit the registry configuration so that it references the correct PVC:

   ```sh
   $ oc edit config.imageregistry.operator.openshift.io -o yaml
   ```

   **Example output**

   ```yaml
   storage:
   pvc:
     claim: image-registry-storage
   ```

   1. Creating a custom PVC allows you to leave the claim field blank for the default automatic creation of an image-registry-storage PVC.

For instructions about configuring registry storage so that it references the correct PVC, see Configuring the registry for vSphere.

### 3.5.6. Additional resources

For more details about configuring registry storage for vSphere, see Recommended configurable storage technology.
CHAPTER 4. REGISTRY OPTIONS

OpenShift Container Platform can build images from your source code, deploy them, and manage their lifecycle. To enable this, OpenShift Container Platform provides an internal, integrated container image registry that can be deployed in your OpenShift Container Platform environment to locally manage images.

4.1. INTEGRATED OPENSHEIFT CONTAINER PLATFORM REGISTRY

OpenShift Container Platform provides a built-in container image registry which runs as a standard workload on the cluster. The registry is configured and managed by an infrastructure operator. It provides an out-of-the-box solution for users to manage the images that run their workloads, and runs on top of the existing cluster infrastructure. This registry can be scaled up or down like any other cluster workload and does not require specific infrastructure provisioning. In addition, it is integrated into the cluster user authentication and authorization system which means that access to create and retrieve images is controlled by defining user permissions on the image resources.

The registry is typically used as a publication target for images built on the cluster as well as a source of images for workloads running on the cluster. When a new image is pushed to the registry, the cluster is notified of the new image and other components can react to and consume the updated image.

Image data is stored in two locations. The actual image data is stored in a configurable storage location such as cloud storage or a filesystem volume. The image metadata, which is exposed by the standard cluster APIs and is used to perform access control, is stored as standard API resources, specifically images and imagestreams.

4.2. THIRD PARTY REGISTRIES

OpenShift Container Platform can create containers using images from third party registries, but it is unlikely that these registries offer the same image notification support as the integrated OpenShift Container Platform registry. In this situation OpenShift Container Platform will fetch tags from the remote registry upon imagestream creation.

Refreshing the fetched tags is as simple as running `oc import-image <stream>`. When new images are detected, the previously-described build and deployment reactions occur.

4.2.1. Authentication

OpenShift Container Platform can communicate with registries to access private image repositories using credentials supplied by the user. This allows OpenShift Container Platform to push and pull images to and from private repositories.

4.3. RED HAT QUAY REGISTRIES

If you need an enterprise-quality container image registry, Red Hat Quay is available both as a hosted service and as software you can install in your own data center or cloud environment. Advanced registry features in Red Hat Quay include geo-replication, image scanning, and the ability to roll back images.

Visit the Quay.io site to set up your own hosted Quay registry account. After that, follow the Quay Tutorial to log in to the Quay registry and start managing your images.

You can access your Red Hat Quay registry from OpenShift Container Platform like any remote container image registry.
4.4. AUTHENTICATION ENABLED RED HAT REGISTRY

All container images available through the Red Hat Container Catalog are hosted on an image registry, registry.redhat.io.

The registry, registry.redhat.io, requires authentication for access to images and hosted content on OpenShift Container Platform. Following the move to the new registry, the existing registry will be available for a period of time.

NOTE

OpenShift Container Platform pulls images from registry.redhat.io, so you must configure your cluster to use it.

The new registry uses standard OAuth mechanisms for authentication, with the following methods:

- **Authentication token.** Tokens, which are generated by administrators, are service accounts that give systems the ability to authenticate against the container image registry. Service accounts are not affected by changes in user accounts, so the token authentication method is reliable and resilient. This is the only supported authentication option for production clusters.

- **Web username and password.** This is the standard set of credentials you use to log in to resources such as access.redhat.com. While it is possible to use this authentication method with OpenShift Container Platform, it is not supported for production deployments. Restrict this authentication method to stand-alone projects outside OpenShift Container Platform.

You can use podman login with your credentials, either username and password or authentication token, to access content on the new registry.

All imagestreams point to the new registry. Because the registry requires authentication for access, the Samples Operator creates the samples-registry-credentials secret.

You must place your credentials in two places:

- **openshift namespace.** Your credentials must exist in the OpenShift namespace so that the imagestreams in the openshift namespace can import.

- **Your host.** Your credentials must exist on your host because Kubernetes uses the credentials from your host when it goes to pull images.
CHAPTER 5. ACCESSING THE REGISTRY

Use the following sections for instructions on accessing the registry, including viewing logs and metrics, as well as securing and exposing the registry.

You can access the registry directly to invoke podman commands. This allows you to push images to or pull them from the integrated registry directly using operations like podman push or podman pull. To do so, you must be logged in to the registry using the oc login command. The operations you can perform depend on your user permissions, as described in the following sections.

5.1. PREREQUISITES

- You must have configured an identity provider (IDP).

- For pulling images, for example when using the podman pull command, the user must have the registry-viewer role. To add this role:

  ```
  $ oc policy add-role-to-user registry-viewer <user_name>
  ```

- For writing or pushing images, for example when using the podman push command, the user must have the registry-editor role. To add this role:

  ```
  $ oc policy add-role-to-user registry-editor <user_name>
  ```

5.2. ACCESSING REGISTRY DIRECTLY FROM THE CLUSTER

You can access the registry from inside the cluster.

Procedure

Access the registry from the cluster by using internal routes:

1. Access the node by getting the node’s address:

   ```
   $ oc get nodes
   $ oc debug nodes/<node_address>
   ```

2. In order to have access to tools such as oc and podman on the node, run the following command:

   ```
   sh-4.2# chroot /host
   ```

3. Log in to the container image registry by using your access token:

   ```
   sh-4.2# oc login -u kubeadmin -p <password_from_install_log> https://api-int.<cluster_name>.<base_domain>:6443
   sh-4.2# podman login -u kubeadmin -p $(oc whoami -t) image-registry.openshift-image-registry.svc:5000
   ```

   You should see a message confirming login, such as:

   ```
   Login Succeeded!
   ```
NOTE
You can pass any value for the user name; the token contains all necessary information. Passing a user name that contains colons will result in a login failure.

Since the Image Registry Operator creates the route, it will likely be similar to `default-route-openshift-image-registry.<cluster_name>`.

4. Perform `podman pull` and `podman push` operations against your registry:

IMPORTANT
You can pull arbitrary images, but if you have the `system:registry` role added, you can only push images to the registry in your project.

In the following examples, use:

<table>
<thead>
<tr>
<th>Component</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;registry_ip&gt;</code></td>
<td>172.30.124.220</td>
</tr>
<tr>
<td><code>&lt;port&gt;</code></td>
<td>5000</td>
</tr>
<tr>
<td><code>&lt;project&gt;</code></td>
<td>openshift</td>
</tr>
<tr>
<td><code>&lt;image&gt;</code></td>
<td>image</td>
</tr>
<tr>
<td><code>&lt;tag&gt;</code></td>
<td>omitted (defaults to latest)</td>
</tr>
</tbody>
</table>

a. Pull an arbitrary image:

```
$ podman pull name.io/image
```

b. Tag the new image with the form `<registry_ip>:<port>/<project>/<image>`. The project name must appear in this pull specification for OpenShift Container Platform to correctly place and later access the image in the registry:

```
$ podman tag name.io/image image-registry.openshift-image-registry.svc:5000/openshift/image
```

NOTE
You must have the `system:image-builder` role for the specified project, which allows the user to write or push an image. Otherwise, the `podman push` in the next step will fail. To test, you can create a new project to push the image.

c. Push the newly-tagged image to your registry:

```
$ podman push image-registry.openshift-image-registry.svc:5000/openshift/image
```
5.3. CHECKING THE STATUS OF THE REGISTRY PODS

As a cluster administrator, you can list the image registry pods running in the openshift-image-registry project and check their status.

Prerequisites

- You have access to the cluster as a user with the cluster-admin role.
- You have installed the OpenShift CLI (oc).

Procedure

1. List the pods in the openshift-image-registry project and view their status:

   $ oc get pods -n openshift-image-registry

Example output

<table>
<thead>
<tr>
<th>NAME</th>
<th>READY</th>
<th>STATUS</th>
<th>RESTARTS</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster-image-registry-operator-764bd7f846-qqtpb</td>
<td>1/1</td>
<td>Running</td>
<td>0</td>
<td>78m</td>
</tr>
<tr>
<td>image-registry-79fb4469f6-llrln</td>
<td>1/1</td>
<td>Running</td>
<td>0</td>
<td>77m</td>
</tr>
<tr>
<td>node-ca-hjksc</td>
<td>1/1</td>
<td>Running</td>
<td>0</td>
<td>73m</td>
</tr>
<tr>
<td>node-ca-tftj6</td>
<td>1/1</td>
<td>Running</td>
<td>0</td>
<td>77m</td>
</tr>
<tr>
<td>node-ca-wb6ht</td>
<td>1/1</td>
<td>Running</td>
<td>0</td>
<td>77m</td>
</tr>
<tr>
<td>node-ca-zvt9q</td>
<td>1/1</td>
<td>Running</td>
<td>0</td>
<td>74m</td>
</tr>
</tbody>
</table>

5.4. VIEWING REGISTRY LOGS

You can view the logs for the registry by using the oc logs command.

Procedure

1. Use the oc logs command with deployments to view the logs for the container image registry:

   $ oc logs deployments/image-registry

Example output


5.5. ACCESSING REGISTRY METRICS

The OpenShift Container Registry provides an endpoint for Prometheus metrics. Prometheus is a stand-alone, open source systems monitoring and alerting toolkit.

The metrics are exposed at the /extensions/v2/metrics path of the registry endpoint.
Procedure

There are two ways in which you can access the metrics, running a metrics query or using the cluster role.

Metrics query

1. Run a metrics query, for example:

   ```bash
   $ curl --insecure -s -u <user>:<secret> \
       https://image-registry.openshift-image-registry.svc:5000/extensions/v2/metrics | grep imageregistry | head -n 20
   # HELP imageregistry_build_info A metric with a constant '1' value labeled by major, minor, git commit & git version from which the image registry was built.
   # TYPE imageregistry_build_info gauge
   imageregistry_build_info{gitCommit="9f72191",gitVersion="v3.11.0+9f72191-135-dirty",major="3",minor="11+"} 1
   # HELP imageregistry_digest_cache_requests_total Total number of requests without scope to the digest cache.
   # TYPE imageregistry_digest_cache_requests_total counter
   imageregistry_digest_cache_requests_total{type="Hit"} 5
   imageregistry_digest_cache_requests_total{type="Miss"} 24
   # HELP imageregistry_digest_cache_scoped_requests_total Total number of scoped requests to the digest cache.
   # TYPE imageregistry_digest_cache_scoped_requests_total counter
   imageregistry_digest_cache_scoped_requests_total{type="Hit"} 33
   imageregistry_digest_cache_scoped_requests_total{type="Miss"} 44
   # HELP imageregistry_http_in_flight_requests A gauge of requests currently being served by the registry.
   # TYPE imageregistry_http_in_flight_requests gauge
   imageregistry_http_in_flight_requests 1
   # HELP imageregistry_http_request_duration_seconds A histogram of latencies for requests to the registry.
   # TYPE imageregistry_http_request_duration_seconds summary
   imageregistry_http_request_duration_seconds{method="get",quantile="0.5"} 0.01296087
   imageregistry_http_request_duration_seconds{method="get",quantile="0.9"} 0.014847248
   imageregistry_http_request_duration_seconds{method="get",quantile="0.99"} 0.015981195
   imageregistry_http_request_duration_seconds_sum{method="get"} 12.260727916000022
   
   <user> can be arbitrary, but <secret> must match the value specified in the registry configuration.
   
   Cluster role

   1. Create a cluster role if you do not already have one to access the metrics:

      ```yaml
      $ cat <<EOF |
      apiVersion: rbac.authorization.k8s.io/v1
      kind: ClusterRole
      metadata:
        name: prometheus-scraper
      rules:
        - apiGroups:
          - image.openshift.io
          resources:
            - registry/metrics
      EOF
      ```
verbs:
- get
EOF

$ oc create -f -

2. Add this role to a user, run the following command:

$ oc adm policy add-cluster-role-to-user prometheus-scraper <username>

3. Access the metrics using cluster role. The part of the configuration file responsible for metrics should look like this:

```yaml
openshift:
  version: 1.0
  metrics:
    enabled: true
...```

Additional resources

- A `kubeadmin` can access the registry until deleted. See [Removing the kubeadmin user](#) for more information.

- For more information on configuring an identity provider, see [Understanding identity provider configuration](#).
CHAPTER 6. EXPOSING THE REGISTRY

By default, the OpenShift Container Platform registry is secured during cluster installation so that it serves traffic through TLS. Unlike previous versions of OpenShift Container Platform, the registry is not exposed outside of the cluster at the time of installation.

6.1. EXPOSING A SECURE REGISTRY MANUALLY

Instead of logging in to the OpenShift Container Platform registry from within the cluster, you can gain external access to it by exposing it with a route. This allows you to log in to the registry from outside the cluster using the route address, and to tag and push images using the route host.

Prerequisites:

- The following prerequisites are automatically performed:
  - Deploy the Registry Operator.
  - Deploy the Ingress Operator.

Procedure

You can expose the route by using DefaultRoute parameter in the configs.imageregistry.operator.openshift.io resource or by using custom routes.

To expose the registry using DefaultRoute:

1. Set DefaultRoute to True:

   ```bash
   $ oc patch configs.imageregistry.operator.openshift.io/cluster --patch '{"spec": {"defaultRoute":true}}' --type=merge
   ```

2. Log in with podman:

   ```bash
   $ HOST=$(oc get route default-route -n openshift-image-registry --template='{{ .spec.host }}')
   $ podman login -u $(oc whoami) -p $(oc whoami -t) --tls-verify=false $HOST
   ```

   `--tls-verify=false` is needed if the cluster’s default certificate for routes is untrusted. You can set a custom, trusted certificate as the default certificate with the Ingress Operator.

To expose the registry using custom routes:

1. Create a secret with your route’s TLS keys:

   ```bash
   $ oc create secret tls public-route-tls -n openshift-image-registry --cert=/path/to/tls.crt --key=/path/to/tls.key
   ```

   This step is optional. If you do not create a secret, the route uses the default TLS configuration from the Ingress Operator.

2. On the Registry Operator:
spec:
  routes:
    - name: public-routes
      hostname: myregistry.mycorp.organization
      secretName: public-route-tls

NOTE

Only set `secretName` if you are providing a custom TLS configuration for the registry's route.