OpenShift Dedicated 4

CI/CD

Contains information on builds, pipelines and GitOps for OpenShift Dedicated

Last Updated: 2023-12-15
OpenShift Dedicated 4 CI/CD

Contains information on builds, pipelines and GitOps for OpenShift Dedicated
Abstract

CI/CD for OpenShift Dedicated clusters.
# Table of Contents

CHAPTER 1. BUILDS ................................................................. 3
  1.1. SETTING UP ADDITIONAL TRUSTED CERTIFICATE AUTHORITIES FOR BUILDS 3
    1.1.1. Adding certificate authorities to the cluster 3
    1.1.2. Additional resources 3
CHAPTER 1. BUILDS

1.1. SETTING UP ADDITIONAL TRUSTED CERTIFICATE AUTHORITIES FOR BUILDS

Use the following sections to set up additional certificate authorities (CA) to be trusted by builds when pulling images from an image registry.

The procedure requires a cluster administrator to create a ConfigMap and add additional CAs as keys in the ConfigMap.

- The ConfigMap must be created in the openshift-config namespace.
- domain is the key in the ConfigMap and value is the PEM-encoded certificate.
  - Each CA must be associated with a domain. The domain format is hostname[.port].
- The ConfigMap name must be set in the image.config.openshift.io/cluster cluster scoped configuration resource’s spec.additionalTrustedCA field.

1.1.1. Adding certificate authorities to the cluster

You can add certificate authorities (CA) to the cluster for use when pushing and pulling images with the following procedure.

Prerequisites

- You must have at least dedicated administrator privileges.
- You must have access to the public certificates of the registry, usually a hostname/ca.crt file located in the /etc/docker/certs.d/ directory.

Procedure

1. Create a ConfigMap in the openshift-config namespace containing the trusted certificates for the registries that use self-signed certificates. For each CA file, ensure the key in the ConfigMap is the hostname of the registry in the hostname[.port] format:

   $ oc create configmap registry-cas -n openshift-config \
      --from-file=myregistry.corp.com..5000=/etc/docker/certs.d/myregistry.corp.com:5000/ca.crt \
      --from-file=otherregistry.com=/etc/docker/certs.d/otherregistry.com/ca.crt

2. Update the cluster image configuration:

   $ oc patch image.config.openshift.io/cluster --patch '{"spec":{"additionalTrustedCA": ["name":"registry-cas"]}}' --type=merge

1.1.2. Additional resources

- Create a ConfigMap
- Secrets and ConfigMaps