



Red Hat CodeReady Workspaces 2.8

Installation Guide

Installing Red Hat CodeReady Workspaces 2.8

Red Hat CodeReady Workspaces 2.8 Installation Guide

Installing Red Hat CodeReady Workspaces 2.8

Robert Kratky
rkratky@redhat.com

Michal Maléř
mmaler@redhat.com

Fabrice Flore-Thébault
ffloreth@redhat.com

Yana Hontyk
yhontyk@redhat.com

Legal Notice

Copyright © 2021 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

Information for administrators installing Red Hat CodeReady Workspaces.

Table of Contents

MAKING OPEN SOURCE MORE INCLUSIVE	5
CHAPTER 1. SUPPORTED PLATFORMS	6
CHAPTER 2. CONFIGURING THE CODEREADY WORKSPACES INSTALLATION	7
2.1. UNDERSTANDING THE CHECLUSTER CUSTOM RESOURCE	7
2.2. CHECLUSTER CUSTOM RESOURCE FIELDS REFERENCE	7
CHAPTER 3. INSTALLING CODEREADY WORKSPACES	20
3.1. INSTALLING CODEREADY WORKSPACES ON OPENSIFT 4 USING OPERATORHUB	20
3.1.1. Creating a project in OpenShift Web Console	20
3.1.2. Installing the Red Hat CodeReady Workspaces Operator	20
3.1.3. Creating an instance of the Red Hat CodeReady Workspaces Operator	21
3.2. INSTALLING CODEREADY WORKSPACES ON OPENSIFT 4 USING THE CLI	22
3.3. INSTALLING CODEREADY WORKSPACES ON OPENSIFT CONTAINER PLATFORM 3.11	23
3.3.1. Installing the crwctl CLI management tool	23
3.3.2. Installing CodeReady Workspaces on OpenShift 3 using the Operator	23
3.4. INSTALLING CODEREADY WORKSPACES IN A RESTRICTED ENVIRONMENT	25
3.4.1. Installing CodeReady Workspaces in a restricted environment using OperatorHub	25
3.4.2. Installing CodeReady Workspaces in a restricted environment using CLI management tool	26
3.4.2.1. Preparing an private registry	26
3.4.2.2. Preparing CodeReady Workspaces Custom Resource for restricted environment	33
3.4.2.2.1. Downloading the default CheCluster Custom Resource	33
3.4.2.2.2. Customizing the CheCluster Custom Resource for restricted environment	33
3.4.2.3. Starting CodeReady Workspaces installation in a restricted environment using CodeReady Workspaces CLI management tool	34
3.4.3. Preparing CodeReady Workspaces Custom Resource for installing behind a proxy	34
CHAPTER 4. CONFIGURING CODEREADY WORKSPACES	36
4.1. ADVANCED CONFIGURATION OPTIONS FOR THE CODEREADY WORKSPACES SERVER COMPONENT	36
4.1.1. Understanding CodeReady Workspaces server advanced configuration using the Operator	36
4.1.2. CodeReady Workspaces server component system properties reference	37
4.1.2.1. Che server	37
4.1.2.2. Authentication parameters	43
4.1.2.3. Internal	45
4.1.2.4. OpenShift Infra parameters	46
4.1.2.5. OpenShift Infra parameters	59
4.1.2.6. Experimental properties	60
4.1.2.7. Configuration of major "/websocket" endpoint	64
4.1.2.8. CORS settings	65
4.1.2.9. Factory defaults	65
4.1.2.10. Devfile defaults	66
4.1.2.11. Che system	68
4.1.2.12. Workspace limits	69
4.1.2.13. Users workspace limits	70
4.1.2.14. Organizations workspace limits	71
4.1.2.15. Organizations notifications settings	72
4.1.2.16. Multi-user-specific OpenShift infrastructure configuration	72
4.1.2.17. Keycloak configuration	73
4.2. CONFIGURING PROJECT STRATEGIES	76
4.2.1. One project per user strategy	78

4.2.2. One project per workspace strategy	78
4.2.3. One project for all workspaces strategy	78
4.2.4. Allowing user-defined workspace projects	79
4.2.5. Handling incompatible usernames or user IDs	79
4.2.6. Pre-creating projects for users	79
4.2.7. Labeling the namespaces	80
4.3. CONFIGURING STORAGE STRATEGIES	81
4.3.1. Storage strategies for codeready-workspaces workspaces	81
4.3.1.1. The common PVC strategy	82
4.3.1.2. The per-workspace PVC strategy	83
4.3.1.3. The unique PVC strategy	83
4.3.1.4. How subpaths are used in PVCs	83
4.3.2. Configuring a CodeReady Workspaces workspace with a persistent volume strategy	84
4.3.2.1. Configuring a PVC strategy using the Operator	84
4.4. CONFIGURING STORAGE TYPES	85
4.4.1. Persistent storage	85
4.4.2. Ephemeral storage	86
4.4.3. Asynchronous storage	86
4.4.4. Configuring storage type defaults for CodeReady Workspaces dashboard	87
4.4.5. Idling asynchronous storage Pods	87
4.5. RUNNING MORE THAN ONE WORKSPACE AT A TIME	88
4.6. CONFIGURING WORKSPACE EXPOSURE STRATEGIES	88
4.6.1. Configuring workspace exposure strategies using an Operator	89
4.6.2. Workspace exposure strategies	90
4.6.2.1. Multi-host strategy	90
4.6.2.2. Single-host strategy	90
4.6.2.2.1. devfile endpoints: single-host	91
4.6.2.2.2. devfile endpoints: multi-host	91
4.6.3. Security considerations	91
4.6.3.1. JSON web token (JWT) proxy	92
4.6.3.2. Secured plug-ins and editors	92
4.6.3.3. Secured container-image components	92
4.6.3.4. Cross-site request forgery attacks	92
4.6.3.5. Phishing attacks	92
4.7. CONFIGURING WORKSPACES NODESELECTOR	93
4.8. CONFIGURING RED HAT CODEREADY WORKSPACES SERVER HOSTNAME	93
4.9. CONFIGURING LABELS FOR OPENSIFT ROUTE	94
4.10. CONFIGURING LABELS AND DOMAINS FOR OPENSIFT ROUTE TO WORK WITH ROUTER SHARDING	95
4.11. DEPLOYING CODEREADY WORKSPACES WITH SUPPORT FOR GIT REPOSITORIES WITH SELF-SIGNED CERTIFICATES	97
4.12. INSTALLING CODEREADY WORKSPACES USING STORAGE CLASSES	98
4.13. IMPORTING UNTRUSTED TLS CERTIFICATES TO CODEREADY WORKSPACES	102
4.13.1. Adding new CA certificates into CodeReady Workspaces	103
4.13.2. Verification at the CodeReady Workspaces installation level	104
4.13.3. Verification at the workspace level	105
4.14. SWITCHING BETWEEN EXTERNAL AND INTERNAL DNS NAMES IN INTER-COMPONENT COMMUNICATION	106
4.15. SETTING UP THE RH-SSO CODEREADY-WORKSPACES-USERNAME-READONLY THEME FOR THE RED HAT CODEREADY WORKSPACES LOGIN PAGE	107
4.15.1. Logging in to RH-SSO	107
4.15.2. Setting up the RH-SSO codeready-workspaces-username-readonly theme	107
4.16. MOUNTING A SECRET AS A FILE OR AN ENVIRONMENT VARIABLE INTO A RED HAT CODEREADY	

WORKSPACES CONTAINER	108
4.16.1. Mounting a secret as a file into a Red Hat CodeReady Workspaces container	108
4.16.2. Mounting a secret as an environment variable into a Red Hat CodeReady Workspaces container	110
4.17. ENABLING DEV WORKSPACE ENGINE	111
CHAPTER 5. UPGRADING CODEREADY WORKSPACES	113
5.1. UPGRADING CODEREADY WORKSPACES USING OPERATORHUB	113
5.1.1. Specifying the approval strategy of CodeReady Workspaces in OperatorHub	113
5.1.2. Manually upgrading CodeReady Workspaces in OperatorHub	114
5.2. UPGRADING CODEREADY WORKSPACES USING THE CLI MANAGEMENT TOOL	115
5.3. UPGRADING CODEREADY WORKSPACES USING THE CLI MANAGEMENT TOOL IN RESTRICTED ENVIRONMENT	115
5.3.1. Understanding network connectivity in restricted environments	116
5.3.2. Building offline registry images	116
5.3.2.1. Building an offline devfile registry image	116
5.3.2.2. Building an offline plug-in registry image	117
5.3.3. Preparing an private registry	117
5.3.4. Upgrading CodeReady Workspaces using the CLI management tool in restricted environment	124
CHAPTER 6. UNINSTALLING CODEREADY WORKSPACES	126
6.1. UNINSTALLING CODEREADY WORKSPACES AFTER OPERATORHUB INSTALLATION USING THE OPENSIFT WEB CONSOLE	126
6.2. UNINSTALLING CODEREADY WORKSPACES AFTER OPERATORHUB INSTALLATION USING OPENSIFT CLI	127
6.3. UNINSTALLING CODEREADY WORKSPACES AFTER CRWCTL INSTALLATION	128

MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see [our CTO Chris Wright's message](#).

CHAPTER 1. SUPPORTED PLATFORMS

This section describes the availability and the supported installation methods of CodeReady Workspaces 2.8 on OpenShift Container Platform 4.6, 3.11, and OpenShift Dedicated.

Table 1.1. Supported deployment environments for CodeReady Workspaces 2.8 on OpenShift Container Platform and OpenShift Dedicated

Platform	Architecture	Deployment method
OpenShift Container Platform 3.11	AMD64 and Intel 64 (x86_64)	crwctl
OpenShift Container Platform 4.6	AMD64 and Intel 64 (x86_64)	OperatorHub, crwctl
OpenShift Container Platform 4.6	IBM Z (s390x)	OperatorHub, crwctl
OpenShift Container Platform 4.6	IBM Power Systems (ppc64le)	OperatorHub, crwctl
OpenShift Container Platform 4.7	AMD64 and Intel 64 (x86_64)	OperatorHub, crwctl
OpenShift Container Platform 4.7	IBM Z (s390x)	OperatorHub, crwctl
OpenShift Container Platform 4.7	IBM Power Systems (ppc64le)	OperatorHub, crwctl
OpenShift Dedicated 4.7	AMD64 and Intel 64 (x86_64)	Add-On



NOTE

Support for deploying CodeReady Workspaces on OpenShift Container Platform on IBM Z (s390x) and IBM Power Systems (ppc64le) is currently only available as a Technology Preview feature. Technology Preview features are not supported with Red Hat production service level agreements (SLAs) and might not be functionally complete. Red Hat does not recommend using them in production. These features provide early access to upcoming product features, enabling customers to test functionality and provide feedback during the development process. For details about the level of support for Technology Preview features, see Technology Preview Features Support Scope.

CHAPTER 2. CONFIGURING THE CODEREADY WORKSPACES INSTALLATION

The following section describes configuration options to install Red Hat CodeReady Workspaces using the Operator.

2.1. UNDERSTANDING THE CHECLUSTER CUSTOM RESOURCE

A default deployment of CodeReady Workspaces consist in the application of a parametrized **CheCluster** Custom Resource by the Red Hat CodeReady Workspaces Operator.

CheCluster Custom Resource

- A YAML document describing the configuration of the overall CodeReady Workspaces installation.
- Contains sections to configure each component: **auth**, **database**, **server**, **storage**.

Role of the Red Hat CodeReady Workspaces Operator

- To translate the **CheCluster** Custom Resource into configuration (ConfigMap) usable by each component of the CodeReady Workspaces installation.

Role of the OpenShift platform

- To apply the configuration (ConfigMap) for each component.
- To create the necessary Pods.
- When OpenShift detects a change in the configuration of a component, it restarts the Pods accordingly.

Example 2.1. Configuring the main properties of the CodeReady Workspaces server component

1. The user applies a **CheCluster** Custom Resource containing some configuration related to the **server**.
2. The Operator generates a necessary ConfigMap, called **che**.
3. OpenShift detects change in the ConfigMap and triggers a restart of the CodeReady Workspaces Pod.

Additional resources

- [Understanding Operators](#).
- [Understanding Custom Resources](#).
- To learn how to modify the **CheCluster** Custom Resource, see the chosen installation procedure.

2.2. CHECLUSTER CUSTOM RESOURCE FIELDS REFERENCE

This section describes all fields available to customize the **CheCluster** Custom Resource.

- [Example 2.2, “A minimal **CheCluster** Custom Resource example.”](#)
- [Table 2.1, “**CheCluster** Custom Resource **server** settings, related to the CodeReady Workspaces server component.”](#)
- [Table 2.2, “**CheCluster** Custom Resource **database** configuration settings related to the database used by CodeReady Workspaces.”](#)
- [Table 2.3, “Custom Resource **auth** configuration settings related to authentication used by CodeReady Workspaces.”](#)
- [Table 2.4, “**CheCluster** Custom Resource **storage** configuration settings related to persistent storage used by CodeReady Workspaces.”](#)
- [Table 2.5, “**CheCluster** Custom Resource **k8s** configuration settings specific to CodeReady Workspaces installations on OpenShift.”](#)
- [Table 2.6, “**CheCluster** Custom Resource **metrics** settings, related to the CodeReady Workspaces metrics collection used by CodeReady Workspaces.”](#)
- [Table 2.7, “**CheCluster** Custom Resource **status** defines the observed state of CodeReady Workspaces installation”](#)

Example 2.2. A minimal **CheCluster** Custom Resource example.

```
apiVersion: org.eclipse.che/v1
kind: CheCluster
metadata:
  name: codeready-workspaces
spec:
  auth:
    externalIdentityProvider: false
  database:
    externalDb: false
  server:
    selfSignedCert: false
    gitSelfSignedCert: false
    tlsSupport: true
  storage:
    pvcStrategy: 'common'
    pvcClaimSize: '1Gi'
```

Table 2.1. **CheCluster Custom Resource **server** settings, related to the CodeReady Workspaces server component.**

Property	Description
airGapContainerRegistryHostname	Optional host name, or URL, to an alternate container registry to pull images from. This value overrides the container registry host name defined in all the default container images involved in a Che deployment. This is particularly useful to install Che in a restricted environment.

Property	Description
airGapContainerRegistryOrganization	Optional repository name of an alternate container registry to pull images from. This value overrides the container registry organization defined in all the default container images involved in a Che deployment. This is particularly useful to install CodeReady Workspaces in a restricted environment.
allowUserDefinedWorkspaceNamespaces	Defines that a user is allowed to specify a OpenShift project, or an OpenShift project, which differs from the default. It's NOT RECOMMENDED to set to true without OpenShift OAuth configured. The OpenShift infrastructure also uses this property.
cheClusterRoles	A comma-separated list of ClusterRoles that will be assigned to Che ServiceAccount. Be aware that the Che Operator has to already have all permissions in these ClusterRoles to grant them.
cheDebug	Enables the debug mode for Che server. Defaults to false .
cheFlavor	Specifies a variation of the installation. The options are che for upstream Che installations, or codeready for CodeReady Workspaces installation. Override the default value only on necessary occasions.
cheHost	Public host name of the installed Che server. When value is omitted, the value it will be automatically set by the Operator. See the cheHostTLSSecret field.
cheHostTLSSecret	Name of a secret containing certificates to secure ingress or route for the custom host name of the installed Che server. See the cheHost field.
cheImage	Overrides the container image used in Che deployment. This does NOT include the container image tag. Omit it or leave it empty to use the default container image provided by the Operator.
cheImagePullPolicy	Overrides the image pull policy used in Che deployment. Default value is Always for nightly or latest images, and IfNotPresent in other cases.
cheImageTag	Overrides the tag of the container image used in Che deployment. Omit it or leave it empty to use the default image tag provided by the Operator.
cheLogLevel	Log level for the Che server: INFO or DEBUG . Defaults to INFO .
cheServerIngress	The Che server ingress custom settings.
cheServerRoute	The Che server route custom settings.
cheWorkspaceClusterRole	Custom cluster role bound to the user for the Che workspaces. The default roles are used when omitted or left blank.

Property	Description
customCheProperties	Map of additional environment variables that will be applied in the generated che ConfigMap to be used by the Che server, in addition to the values already generated from other fields of the CheCluster custom resource (CR). When customCheProperties contains a property that would be normally generated in che ConfigMap from other CR fields, the value defined in the customCheProperties is used instead.
devfileRegistryCpuLimit	Overrides the CPU limit used in the devfile registry deployment. In cores. (500m = .5 cores). Default to 500m.
devfileRegistryCpuRequest	Overrides the CPU request used in the devfile registry deployment. In cores. (500m = .5 cores). Default to 100m.
devfileRegistryImage	Overrides the container image used in the devfile registry deployment. This includes the image tag. Omit it or leave it empty to use the default container image provided by the Operator.
devfileRegistryIngress	The devfile registry ingress custom settings.
devfileRegistryMemoryLimit	Overrides the memory limit used in the devfile registry deployment. Defaults to 256Mi.
devfileRegistryMemoryRequest	Overrides the memory request used in the devfile registry deployment. Defaults to 16Mi.
devfileRegistryPullPolicy	Overrides the image pull policy used in the devfile registry deployment. Default value is Always for nightly or latest images, and IfNotPresent in other cases.
devfileRegistryRoute	The devfile registry route custom settings.
devfileRegistryUrl	Public URL of the devfile registry, that serves sample, ready-to-use devfiles. Set this ONLY when a use of an external devfile registry is needed. See the externalDevfileRegistry field. By default, this will be automatically calculated by the Operator.
externalDevfileRegistry	Instructs the Operator on whether to deploy a dedicated devfile registry server. By default, a dedicated devfile registry server is started. When externalDevfileRegistry is true , no such dedicated server will be started by the Operator and you will have to manually set the devfileRegistryUrl field
externalPluginRegistry	Instructs the Operator on whether to deploy a dedicated plugin registry server. By default, a dedicated plugin registry server is started. When externalPluginRegistry is true , no such dedicated server will be started by the Operator and you will have to manually set the pluginRegistryUrl field.

Property	Description
gitSelfSignedCert	When enabled, the certificate from che-git-self-signed-cert ConfigMap will be propagated to the Che components and provide particular configuration for Git.
nonProxyHosts	List of hosts that will be reached directly, bypassing the proxy. Specify wild card domain use the following form .<DOMAIN> and as delimiter, for example: localhost .my.host.com 123.42.12.32 Only use when configuring a proxy is required. Operator respects OpenShift cluster wide proxy configuration and no additional configuration is required, but defining nonProxyHosts in a custom resource leads to merging non proxy hosts lists from the cluster proxy configuration and ones defined in the custom resources. See the doc https://docs.openshift.com/container-platform/4.4/networking/enable-cluster-wide-proxy.html). See also the proxyURL fields.
pluginRegistryCpuLimit	Overrides the CPU limit used in the plugin registry deployment. In cores. (500m = .5 cores). Default to 500m.
pluginRegistryCpuRequest	Overrides the CPU request used in the plugin registry deployment. In cores. (500m = .5 cores). Default to 100m.
pluginRegistryImage	Overrides the container image used in the plugin registry deployment. This includes the image tag. Omit it or leave it empty to use the default container image provided by the Operator.
pluginRegistryIngress	Plugin registry ingress custom settings.
pluginRegistryMemoryLimit	Overrides the memory limit used in the plugin registry deployment. Defaults to 256Mi.
pluginRegistryMemoryRequest	Overrides the memory request used in the plugin registry deployment. Defaults to 16Mi.
pluginRegistryPullPolicy	Overrides the image pull policy used in the plugin registry deployment. Default value is Always for nightly or latest images, and IfNotPresent in other cases.
pluginRegistryRoute	Plugin registry route custom settings.
pluginRegistryUrl	Public URL of the plugin registry that serves sample ready-to-use devfiles. Set this ONLY when a use of an external devfile registry is needed. See the externalPluginRegistry field. By default, this will be automatically calculated by the Operator.
proxyPassword	Password of the proxy server. Only use when proxy configuration is required. See the proxyURL , proxyUser and proxySecret fields.

Property	Description
proxyPort	Port of the proxy server. Only use when configuring a proxy is required. See also the proxyURL and nonProxyHosts fields.
proxySecret	The secret that contains user and password for a proxy server. When the secret is defined, the proxyUser and proxyPassword are ignored.
proxyURL	URL (protocol+host name) of the proxy server. This drives the appropriate changes in the JAVA_OPTS and https(s)_proxy variables in the Che server and workspaces containers. Only use when configuring a proxy is required. Operator respects OpenShift cluster wide proxy configuration and no additional configuration is required, but defining proxyUrl in a custom resource leads to overrides the cluster proxy configuration with fields proxyUrl , proxyPort , proxyUser and proxyPassword from the custom resource. See the doc https://docs.openshift.com/container-platform/4.4/networking/enable-cluster-wide-proxy.html). See also the proxyPort and nonProxyHosts fields.
proxyUser	User name of the proxy server. Only use when configuring a proxy is required. See also the proxyURL , proxyPassword and proxySecret fields.
selfSignedCert	Deprecated. The value of this flag is ignored. The Che Operator will automatically detect whether the router certificate is self-signed and propagate it to other components, such as the Che server.
serverCpuLimit	Overrides the CPU limit used in the Che server deployment In cores. (500m = .5 cores). Default to 1.
serverCpuRequest	Overrides the CPU request used in the Che server deployment In cores. (500m = .5 cores). Default to 100m.
serverExposureStrategy	Sets the server and workspaces exposure type. Possible values are multi-host , single-host , default-host . Defaults to multi-host , which creates a separate ingress, or OpenShift routes, for every required endpoint. single-host makes Che exposed on a single host name with workspaces exposed on subpaths. Read the docs to learn about the limitations of this approach. Also consult the singleHostExposureType property to further configure how the Operator and the Che server make that happen on Kubernetes. default-host exposes the Che server on the host of the cluster. Read the docs to learn about the limitations of this approach.
serverMemoryLimit	Overrides the memory limit used in the Che server deployment. Defaults to 1Gi.
serverMemoryRequest	Overrides the memory request used in the Che server deployment. Defaults to 512Mi.

Property	Description
serverTrustStoreConfigMap Name	Name of the ConfigMap with public certificates to add to Java trust store of the Che server. This is often required when adding the OpenShift OAuth provider, which has HTTPS endpoint signed with self-signed cert. The Che server must be aware of its CA cert to be able to request it. This is disabled by default.
singleHostGatewayConfigMapLabels	The labels that need to be present in the ConfigMaps representing the gateway configuration.
singleHostGatewayConfigSidecarImage	The image used for the gateway sidecar that provides configuration to the gateway. Omit it or leave it empty to use the default container image provided by the Operator.
singleHostGatewayImage	The image used for the gateway in the single host mode. Omit it or leave it empty to use the default container image provided by the Operator.
tlsSupport	Deprecated. Instructs the Operator to deploy Che in TLS mode. This is enabled by default. Disabling TLS sometimes cause malfunction of some Che components.
useInternalClusterSVCNames	Use internal cluster SVC names to communicate between components to speed up the traffic and avoid proxy issues. The default value is true .
workspaceNamespaceDefault	Defines default OpenShift project in which user's workspaces are created for a case when a user does not override it. It's possible to use <username> , <userid> and <workspaceid> placeholders, such as che-workspace- <username> . In that case, a new namespace will be created for each user or workspace.

Table 2.2. CheCluster Custom Resource database configuration settings related to the database used by CodeReady Workspaces.

Property	Description
chePostgresContainerResources	PostgreSQL container custom settings
chePostgresDb	PostgreSQL database name that the Che server uses to connect to the DB. Defaults to dbche .
chePostgresHostName	PostgreSQL Database host name that the Che server uses to connect to. Defaults is postgres . Override this value ONLY when using an external database. See field externalDb . In the default case it will be automatically set by the Operator.
chePostgresPassword	PostgreSQL password that the Che server uses to connect to the DB. When omitted or left blank, it will be set to an automatically generated value.

Property	Description
chePostgresPort	PostgreSQL Database port that the Che server uses to connect to. Defaults to 5432. Override this value ONLY when using an external database. See field externalDb . In the default case it will be automatically set by the Operator.
chePostgresSecret	The secret that contains PostgreSQL `user` and password that the Che server uses to connect to the DB. When the secret is defined, the chePostgresUser and chePostgresPassword are ignored. When the value is omitted or left blank, the one of following scenarios applies: 1. chePostgresUser and chePostgresPassword are defined, then they will be used to connect to the DB. 2. chePostgresUser or chePostgresPassword are not defined, then a new secret with the name che-postgres-secret will be created with default value of pgche for user and with an auto-generated value for password .
chePostgresUser	PostgreSQL user that the Che server uses to connect to the DB. Defaults to pgche .
externalDb	Instructs the Operator on whether to deploy a dedicated database. By default, a dedicated PostgreSQL database is deployed as part of the Che installation. When externalDb is true , no dedicated database will be deployed by the Operator and you will need to provide connection details to the external DB you are about to use. See also all the fields starting with: chePostgres .
postgresImage	Overrides the container image used in the PostgreSQL database deployment. This includes the image tag. Omit it or leave it empty to use the default container image provided by the Operator.
postgresImagePullPolicy	Overrides the image pull policy used in the PostgreSQL database deployment. Default value is Always for nightly or latest images, and IfNotPresent in other cases.

Table 2.3. Custom Resourceauth configuration settings related to authentication used by CodeReady Workspaces.

Property	Description
externalIdentityProvider	Instructs the Operator on whether to deploy a dedicated Identity Provider (Keycloak or RH-SSO instance). By default, a dedicated Identity Provider server is deployed as part of the Che installation. When externalIdentityProvider is true , no dedicated identity provider will be deployed by the Operator and you will need to provide details about the external identity provider you are about to use. See also all the other fields starting with: identityProvider .
identityProviderAdminUserName	Overrides the name of the Identity Provider administrator user. Defaults to admin .

Property	Description
identityProviderClientId	Name of a Identity provider, Keycloak or RH-SSO, client-id that is used for Che. Override this when an external Identity Provider is in use. See the externalIdentityProvider field. When omitted or left blank, it is set to the value of the flavour field suffixed with -public .
identityProviderContainerResources	Identity provider container custom settings.
identityProviderImage	Overrides the container image used in the Identity Provider, Keycloak or RH-SSO, deployment. This includes the image tag. Omit it or leave it empty to use the default container image provided by the Operator.
identityProviderImagePullPolicy	Overrides the image pull policy used in the Identity Provider, Keycloak or RH-SSO, deployment. Default value is Always for nightly or latest images, and IfNotPresent in other cases.
identityProviderIngress	Ingress custom settings.
identityProviderPassword	Overrides the password of Keycloak administrator user. Override this when an external Identity Provider is in use. See the externalIdentityProvider field. When omitted or left blank, it is set to an auto-generated password.
identityProviderPostgresPassword	Password for a Identity Provider, Keycloak or RH-SSO, to connect to the database. Override this when an external Identity Provider is in use. See the externalIdentityProvider field. When omitted or left blank, it is set to an auto-generated password.
identityProviderPostgresSecret	The secret that contains password for the Identity Provider, Keycloak or RH-SSO, to connect to the database. When the secret is defined, the identityProviderPostgresPassword is ignored. When the value is omitted or left blank, the one of following scenarios applies: 1. identityProviderPostgresPassword is defined, then it will be used to connect to the database. 2. identityProviderPostgresPassword is not defined, then a new secret with the name che-identity-postgres-secret will be created with an auto-generated value for password .
identityProviderRealm	Name of a Identity provider, Keycloak or RH-SSO, realm that is used for Che. Override this when an external Identity Provider is in use. See the externalIdentityProvider field. When omitted or left blank, it is set to the value of the flavour field.
identityProviderRoute	Route custom settings.

Property	Description
identityProviderSecret	The secret that contains user and password for Identity Provider. When the secret is defined, the identityProviderAdminUserName and identityProviderPassword are ignored. When the value is omitted or left blank, the one of following scenarios applies: 1. identityProviderAdminUserName and identityProviderPassword are defined, then they will be used. 2. identityProviderAdminUserName or identityProviderPassword are not defined, then a new secret with the name che-identity-secret will be created with default value admin for user and with an auto-generated value for password .
identityProviderURL	Public URL of the Identity Provider server (Keycloak / RH-SSO server). Set this ONLY when a use of an external Identity Provider is needed. See the externalIdentityProvider field. By default, this will be automatically calculated and set by the Operator.
oAuthClientName	Name of the OpenShift OAuthClient resource used to setup identity federation on the OpenShift side. Auto-generated when left blank. See also the OpenShiftoAuth field.
oAuthSecret	Name of the secret set in the OpenShift OAuthClient resource used to setup identity federation on the OpenShift side. Auto-generated when left blank. See also the OAuthClientName field.
openShiftoAuth	Enables the integration of the identity provider (Keycloak / RHSSO) with OpenShift OAuth. Empty value on OpenShift by default. This will allow users to directly login with their OpenShift user through the OpenShift login, and have their workspaces created under personal OpenShift namespaces. WARNING: the kubeadmin user is NOT supported, and logging through it will NOT allow accessing the Che Dashboard.
updateAdminPassword	Forces the default admin Che user to update password on first login. Defaults to false .

Table 2.4. CheCluster Custom Resourcestorage configuration settings related to persistent storage used by CodeReady Workspaces.

Property	Description
postgresPVCStorageClassName	Storage class for the Persistent Volume Claim dedicated to the PostgreSQL database. When omitted or left blank, a default storage class is used.
preCreateSubPaths	Instructs the Che server to start a special Pod to pre-create a sub-path in the Persistent Volumes. Defaults to false , however it will need to enable it according to the configuration of your OpenShift cluster.
pvcClaimSize	Size of the persistent volume claim for workspaces. Defaults to 1Gi .

Property	Description
pvcJobsImage	Overrides the container image used to create sub-paths in the Persistent Volumes. This includes the image tag. Omit it or leave it empty to use the default container image provided by the Operator. See also the preCreateSubPaths field.
pvcStrategy	Persistent volume claim strategy for the Che server. This Can be: <code>common</code> (all workspaces PVCs in one volume), per-workspace (one PVC per workspace for all declared volumes) and unique (one PVC per declared volume). Defaults to common .
workspacePVCStorageClass Name	Storage class for the Persistent Volume Claims dedicated to the Che workspaces. When omitted or left blank, a default storage class is used.

Table 2.5. CheCluster Custom ResourceK8s configuration settings specific to CodeReady Workspaces installations on OpenShift.

Property	Description
ingressClass	Ingress class that will define the which controller will manage ingresses. Defaults to nginx . NB: This drives the kubernetes.io/ingress.class annotation on Che-related ingresses.
ingressDomain	Global ingress domain for an OpenShift cluster. This MUST be explicitly specified: there are no defaults.
ingressStrategy	Strategy for ingress creation. Options are: multi-host (host is explicitly provided in ingress), single-host (host is provided, path-based rules) and default-host (no host is provided, path-based rules). Defaults to multi-host Deprecated in favor of serverExposureStrategy in the server section, which defines this regardless of the cluster type. When both are defined, the serverExposureStrategy option takes precedence.
securityContextFsGroup	The FSGroup in which the Che Pod and workspace Pods containers runs in. Default value is 1724 .
securityContextRunAsUser	ID of the user the Che Pod and workspace Pods containers run as. Default value is 1724 .
singleHostExposureType	When the serverExposureStrategy is set to single-host , the way the server, registries and workspaces are exposed is further configured by this property. The possible values are native , which means that the server and workspaces are exposed using ingresses on Kubernetes or gateway where the server and workspaces are exposed using a custom gateway based on Traefik . All the endpoints whether backed by the ingress or gateway route always point to the subpaths on the same domain. Defaults to native .

Property	Description
tlsSecretName	Name of a secret that will be used to setup ingress TLS termination when TLS is enabled. When the field is empty string, the default cluster certificate will be used. See also the tlsSupport field.

Table 2.6. CheCluster Custom Resource metrics settings, related to the CodeReady Workspaces metrics collection used by CodeReady Workspaces.

Property	Description
enable	Enables metrics the Che server endpoint. Default to true .

Table 2.7. CheCluster Custom Resource status defines the observed state of CodeReady Workspaces installation

Property	Description
cheClusterRunning	Status of a Che installation. Can be Available , Unavailable , or Available, Rolling Update in Progress .
cheURL	Public URL to the Che server.
cheVersion	Current installed Che version.
dbProvisioned	Indicates that a PostgreSQL instance has been correctly provisioned or not.
devfileRegistryURL	Public URL to the devfile registry.
gitHubOAuthProvisioned	Indicates whether an Identity Provider instance, Keycloak or RH-SSO, has been configured to integrate with the GitHub OAuth.
helpLink	A URL that points to some URL where to find help related to the current Operator status.
keycloakProvisioned	Indicates whether an Identity Provider instance, Keycloak or RH-SSO, has been provisioned with realm, client and user.
keycloakURL	Public URL to the Identity Provider server, Keycloak or RH-SSO,.
message	A human readable message indicating details about why the Pod is in this condition.
openShifttoAuthProvisioned	Indicates whether an Identity Provider instance, Keycloak or RH-SSO, has been configured to integrate with the OpenShift OAuth.
pluginRegistryURL	Public URL to the plugin registry.

Property	Description
reason	A brief CamelCase message indicating details about why the Pod is in this state.

CHAPTER 3. INSTALLING CODEREADY WORKSPACES

This section contains instructions to install Red Hat CodeReady Workspaces. The installation method depends on the target platform and the environment restrictions.

3.1. INSTALLING CODEREADY WORKSPACES ON OPENSIFT 4 USING OPERATORHUB

This section describes how to install CodeReady Workspaces using the CodeReady Workspaces Operator available in OpenShift 4 web console.

Operators are a method of packaging, deploying, and managing an OpenShift application which also provide the following:

- Repeatability of installation and upgrade.
- Constant health checks of every system component.
- Over-the-air (OTA) updates for OpenShift components and independent software vendor (ISV) content.
- A place to encapsulate knowledge from field engineers and spread it to all users.

Prerequisites

- An administrator account on a running instance of OpenShift 4.

3.1.1. Creating a project in OpenShift Web Console

A project allows to organize and manage different resources on the cluster in an isolated unit. Create a project first to host the Red Hat CodeReady Workspaces Operator.

Procedure

1. Open the OpenShift web console, in the left panel navigate to the **Home → Projects** section.
2. Click **Create Project**.
3. Specify the project details:
 - **Name: openshift-workspaces**
 - **Display Name: Red Hat CodeReady Workspaces**
 - **Description: Red Hat CodeReady Workspaces**

3.1.2. Installing the Red Hat CodeReady Workspaces Operator

Red Hat CodeReady Workspaces Operator provides all the resources for running CodeReady Workspaces, such as PostgreSQL, RH-SSO, image registries, and the CodeReady Workspaces server, and also configures all these services.

Prerequisites

- Access to the Web Console on the cluster.

Procedure

1. To install the Red Hat CodeReady Workspaces Operator, in the left panel, navigate to the **Operators** → **OperatorHub** section.
2. In the **Filter by keyword** field, type **Red Hat CodeReady Workspaces** and click the **Red Hat CodeReady Workspaces** tile.
3. In the **Red Hat CodeReady Workspaces** pop-up window, click the **Install** button.
4. On the **Install Operator** screen, specify the following options:
 - **Installation mode: A specific project on the cluster**
 - **Installed Namespace:** *Pick an existing project → **openshift-workspaces**

Verification steps

1. To verify the Red Hat CodeReady Workspaces Operator has installed correctly, in the left panel navigate to the **Operators** → **Installed Operators** section.
2. In the **Installed Operators** screen, click the **Red Hat CodeReady Workspaces** name and navigate to the **Details** tab.
3. In the **ClusterServiceVersion Details** section at the bottom of the page, wait for these messages:
 - **Status: Succeeded**
 - **Status Reason: install strategy completed with no errors**
4. Navigate to the **Events** tab and wait for this message: **install strategy completed with no errors**.

3.1.3. Creating an instance of the Red Hat CodeReady Workspaces Operator

Follow this procedure to install Red Hat CodeReady Workspaces with the default configuration. To modify the configuration, see [Chapter 2, Configuring the CodeReady Workspaces installation](#).

Procedure

1. To create an instance of the Red Hat CodeReady Workspaces Operator, in the left panel, navigate to the **Operators** → **Installed Operators** section.
2. In the **Installed Operators** screen, click the **Red Hat CodeReady Workspaces** name.
3. In the **Operator Details** screen, in the **Details** tab, inside of the **Provided APIs** section, click the **Create Instance** link.
4. The **Create CheCluster** page contains the configuration of the overall CodeReady Workspaces instance to create. It is the **CheCluster** Custom Resource. Keep the default values.
5. To create the **codeready-workspaces** cluster, click the **Create** button in the lower left corner of the window.

6. On the **Operator Details** screen, in the **Red Hat CodeReady Workspaces Cluster** tab, click on the **codeready-workspaces** link.
7. To navigate to the **codeready-workspaces** instance, click the link under **Red Hat CodeReady Workspaces URL**.



NOTE

The installation might take more than 5 minutes. The URL appears after the Red Hat CodeReady Workspaces installation finishes.

Verification steps

1. To verify that the Red Hat CodeReady Workspaces instance has installed correctly, navigate to the **CodeReady Workspaces Cluster** tab. The **CheClusters** screen displays the list of Red Hat CodeReady Workspaces instances and their status.
2. Click **codeready-workspaces CheCluster** in the table and navigate to the **Details** tab.
3. See the content of following fields:
 - **Message**: the field contains error messages, if any. The expected content is **None**.
 - **Red Hat CodeReady Workspaces URL**: displays the URL of the Red Hat CodeReady Workspaces instance, once the deployment is successful.
4. Navigate to the **Resources** tab. The screen displays the list of the resources assigned to the CodeReady Workspaces deployment.
5. To see more details about the state of a resource, click its name and inspect the content of the available tabs.

Additional resources

- [Navigating CodeReady Workspaces using the Dashboard](#).
- [Viewing the state of the CodeReady Workspaces cluster deployment using OpenShift 4 CLI tools](#).

3.2. INSTALLING CODEREADY WORKSPACES ON OPENSIFT 4 USING THE CLI

This section describes how to install CodeReady Workspaces on OpenShift 4 with the **crwctl** CLI management tool.

Prerequisites

- An OpenShift cluster with an administrator account.
- **oc** is available. See [Getting started with the OpenShift CLI](#). **oc** version must match the OpenShift cluster version.
- You have logged in to OpenShift. See [Logging in to the CLI](#).
- **crwctl** is available. See [Section 3.3.1, "Installing the crwctl CLI management tool"](#).

Procedure

- Run the **server:deploy** command to create the CodeReady Workspaces instance:

```
$ crwctl server:deploy -n openshift-workspaces
```

Verification steps

1. The output of the **server:deploy** command ends with:

```
Command server:deploy has completed successfully.
```

2. Navigate to the CodeReady Workspaces cluster instance: **https://codeready-
<openshift_deployment_name>.<domain_name>**.

3.3. INSTALLING CODEREADY WORKSPACES ON OPENSIFT CONTAINER PLATFORM 3.11

3.3.1. Installing the crwctl CLI management tool

This section describes how to install `crwctl`, the CodeReady Workspaces CLI management tool.

Procedure

1. Navigate to <https://developers.redhat.com/products/codeready-workspaces/download>.
2. Download the CodeReady Workspaces CLI management tool archive for version 2.8.
3. Extract the archive to a folder, such as **`\${HOME}/crwctl`** or **`/opt/crwctl`**.
4. Run the **crwctl** executable from the extracted folder. In this example, **`\${HOME}/crwctl/bin/crwctl version`**.
5. Optionally, add the **bin** folder to your **`\${PATH}`**, for example, **`\${PATH}=\${PATH}:\${HOME}/crwctl/bin`** to enable running **crwctl** without the full path specification.

Verification step

Running **crwctl version** displays the current version of the tool.

3.3.2. Installing CodeReady Workspaces on OpenShift 3 using the Operator

This section describes how to install CodeReady Workspaces on OpenShift 3 with the **crwctl** CLI management tool. The method of installation is using the Operator and enable TLS (HTTPS).



NOTE

Methods for updating from a previous CodeReady Workspaces installation and enabling multiple instances in the same OpenShift Container Platform 3.11 cluster are provided below the installation procedure.

Operators are a method of packaging, deploying, and managing a OpenShift application which also provide the following:

- Repeatability of installation and upgrade.
- Constant health checks of every system component.
- Over-the-air (OTA) updates for OpenShift components and independent software vendor (ISV) content.
- A place to encapsulate knowledge from field engineers and spread it to all users.



NOTE

This approach is only supported for use with OpenShift Container Platform and OpenShift Dedicated version 3.11, but also work for newer versions of OpenShift Container Platform and OpenShift Dedicated, and serves as a backup installation method for situations when the installation method using OperatorHub is not available.

Prerequisites

- Administrator rights on a running instance of OpenShift 3.11.
- An installation of the **oc** OpenShift 3.11 CLI management tool. See [Installing the OpenShift 3.11 CLI](#).
- An installation of the **crwctl** management tool. See [Section 3.3.1, "Installing the crwctl CLI management tool"](#).
- To apply settings that the main crwctl command-line parameters cannot set, prepare a configuration file **operator-cr-patch.yaml** that will override the default values in the **CheCluster** Custom Resource used by the Operator. See [Chapter 2, Configuring the CodeReady Workspaces installation](#).
- `<namespace>` represents the project of the target installation.

Procedure

1. Log in to OpenShift. See [Basic Setup and Login](#).

```
$ oc login
```

2. Run the following command to verify that the version of the **oc** OpenShift CLI management tool is 3.11:

```
$ oc version
oc v3.11.0+0cbc58b
```

3. Run the following command to create the CodeReady Workspaces instance

- In the openshift-workspaces project:

```
$ crwctl server:deploy -n openshift-workspaces -p openshift
```

- In the default project called openshift-workspaces:

```
$ crwctl server:deploy -p openshift
```

Verification steps

1. The output of the previous command ends with:

```
Command server:deploy has completed successfully.
```

2. Navigate to the CodeReady Workspaces cluster instance: `https://codeready-
<openshift_deployment_name>.<domain_name>`.

3.4. INSTALLING CODEREADY WORKSPACES IN A RESTRICTED ENVIRONMENT

By default, Red Hat CodeReady Workspaces uses various external resources, mainly container images available in public registries.

To deploy CodeReady Workspaces in an environment where these external resources are not available (for example, on a cluster that is not exposed to the public Internet):

1. Identify the image registry used by the OpenShift cluster, and ensure you can push to it.
2. Push all the images needed for running CodeReady Workspaces to this registry.
3. Configure CodeReady Workspaces to use the images that have been pushed to the registry.
4. Proceed to the CodeReady Workspaces installation.

The procedure for installing CodeReady Workspaces in restricted environments is different based on the installation method you use:

- [Installation using OperatorHub on Openshift 4.3](#) and above
- [Installation using the crwctl management tool on both OpenShift 3.11 or 4.x](#)

Notes on network connectivity in restricted environments

Restricted network environments range from a private subnet in a cloud provider to a separate network owned by a company, disconnected from the public Internet. Regardless of the network configuration, CodeReady Workspaces works **provided that the Routes that are created for CodeReady Workspaces components (codeready-workspaces-server, identity provider, devfile and plugin registries) are accessible from inside the OpenShift cluster.**

Take into account the network topology of the environment to determine how best to accomplish this. For example, on a network owned by a company or an organization, the network administrators must ensure that traffic bound from the cluster can be routed to Route hostnames. In other cases, for example, on AWS, create a proxy configuration allowing the traffic to leave the node to reach an external-facing Load Balancer.

When the restricted network involves a proxy, follow the instructions provided in [Section 3.4.3, "Preparing CodeReady Workspaces Custom Resource for installing behind a proxy"](#).

3.4.1. Installing CodeReady Workspaces in a restricted environment using OperatorHub

Prerequisites

- A running OpenShift cluster. See the [OpenShift Container Platform 4.3 documentation](#) for instructions on how to install an OpenShift cluster on a restricted network.
- Access to the mirror registry used to installed the OpenShift disconnected cluster in restricted network. See the [Related OpenShift Container Platform 4.3 documentation about creating a mirror registry for installation in a restricted network](#).

On disconnected OpenShift 4 clusters running on restricted networks, an Operator can be successfully installed from OperatorHub only if it meets the additional requirements defined in [Enabling your Operator for restricted network environments](#).

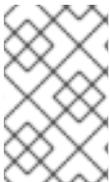
The CodeReady Workspaces operator meets these requirements and is therefore compatible with the [official documentation about OLM on a restricted network](#) .

Procedure

To install CodeReady Workspaces from OperatorHub:

1. Build a **redhat-operators** catalog image. See [Building an Operator catalog image](#) .
2. Configure OperatorHub to use this catalog image for operator installations. See [Configuring OperatorHub for restricted networks](#).
3. Proceed to the CodeReady Workspaces installation as usual as described in [Section 3.1, "Installing CodeReady Workspaces on OpenShift 4 using OperatorHub"](#).

3.4.2. Installing CodeReady Workspaces in a restricted environment using CLI management tool



NOTE

Use CodeReady Workspaces CLI management tool to install CodeReady Workspaces on restricted networks if installation through OperatorHub is not available. This method is supported for OpenShift Container Platform 3.11.

Prerequisites

- A running OpenShift cluster. See the [OpenShift Container Platform 3.11 documentation](#) for instructions on how to install an OpenShift cluster.

3.4.2.1. Preparing an private registry

Prerequisites

- The **oc** tool is available.
- The **skopeo** tool, version 0.1.40 or later, is available.
- The **podman** tool is available.
- An image registry accessible from the OpenShift cluster and supporting the format of the V2 image manifest, schema version 2. Ensure you can push to it from a location having, at least temporarily, access to the internet.

Table 3.1. Placeholders used in examples

<source-image>	Full coordinates of the source image, including registry, organization, and digest.
<target-registry>	Host name and port of the target container-image registry.
<target-organization>	Organization in the target container-image registry
<target-image>	Image name and digest in the target container-image registry.
<target-user>	User name in the target container-image registry.
<target-password>	User password in the target container-image registry.

Procedure

1. Log into the internal image registry:

```
$ podman login --username <user> --password <password> <target-registry>
```



NOTE

If you encounter an error, like **x509: certificate signed by unknown authority**, when attempting to push to the internal registry, try one of these workarounds:

- add the OpenShift cluster's certificate to **/etc/containers/certs.d/<target-registry>**
- add the registry as an insecure registry by adding the following lines to the Podman configuration file located at **/etc/containers/registries.conf**:

```
[registries.insecure]
registries = ['<target-registry>']
```

2. Copy images without changing their digest. Repeat this step for every image in the following table:

```
$ skopeo copy --all docker://<source-image> docker://<target-registry>/<target-organization>/<target-image>
```

**NOTE**

Table 3.2. Understanding the usage of the container-images from the prefix or keyword they include in their name

Usage	Prefix or keyword
Essential	not stacks- , plugin- , or -openj9-
Workspaces	stacks- , plugin-
IBM Z and IBM Power Systems	-openj9-

Table 3.3. Images to copy in the private registry

<source-image>	<target-image>
registry.redhat.io/codeready-workspaces/configbump-rhel8@sha256:db34b20374d99c2055612663a669a06f6dd0fc1fc19603761e993fd0870eddf	configbump-rhel8@sha256:db34b20374d99c2055612663a669a06f6dd0fc1fc19603761e993fd0870eddf
registry.redhat.io/codeready-workspaces/crw-2-rhel8-operator@sha256:a24dc83d8cdd8af715f0c4f235dcba0736bf395b7029ceaed0b8a683da5f74e0	crw-2-rhel8-operator@sha256:a24dc83d8cdd8af715f0c4f235dcba0736bf395b7029ceaed0b8a683da5f74e0
registry.redhat.io/codeready-workspaces/crw-2-rhel8-operator@sha256:a24dc83d8cdd8af715f0c4f235dcba0736bf395b7029ceaed0b8a683da5f74e0	crw-2-rhel8-operator@sha256:a24dc83d8cdd8af715f0c4f235dcba0736bf395b7029ceaed0b8a683da5f74e0
registry.redhat.io/codeready-workspaces/devfileregistry-rhel8@sha256:e3c360c031d8e68b62d1a28a4d736f41c5bfb17c23999b9e1f1e5820858bf1d	devfileregistry-rhel8@sha256:e3c360c031d8e68b62d1a28a4d736f41c5bfb17c23999b9e1f1e5820858bf1d
registry.redhat.io/codeready-workspaces/jwtproxy-rhel8@sha256:3f40bb8a2022545ac06a0b41cdb0239fdacfc34b37faffb21348a2041e96d0f2	jwtproxy-rhel8@sha256:3f40bb8a2022545ac06a0b41cdb0239fdacfc34b37faffb21348a2041e96d0f2

<source-image>	<target-image>
<p>registry.redhat.io/codeready-workspaces/machineexec-rhel8@sha256:19a8daf7f9adde981dcd588b0526fa7682111097849f60a9b0e81137bdd e8f6c</p>	<p>machineexec-rhel8@sha256:19a8daf7f9adde981dcd588b0526fa7682111097849f60a9b0e81137bdd e8f6c</p>
<p>registry.redhat.io/codeready-workspaces/plugin-java11-openj9-rhel8@sha256:ee7c41053b4c8615886745566fc306dbf5bd1b1d367e525266477ae17a26673e</p>	<p>plugin-java11-openj9-rhel8@sha256:ee7c41053b4c8615886745566fc306dbf5bd1b1d367e525266477ae17a26673e</p>
<p>registry.redhat.io/codeready-workspaces/plugin-java11-openj9-rhel8@sha256:ee7c41053b4c8615886745566fc306dbf5bd1b1d367e525266477ae17a26673e</p>	<p>plugin-java11-openj9-rhel8@sha256:ee7c41053b4c8615886745566fc306dbf5bd1b1d367e525266477ae17a26673e</p>
<p>registry.redhat.io/codeready-workspaces/plugin-java11-openj9-rhel8@sha256:ee7c41053b4c8615886745566fc306dbf5bd1b1d367e525266477ae17a26673e</p>	<p>plugin-java11-openj9-rhel8@sha256:ee7c41053b4c8615886745566fc306dbf5bd1b1d367e525266477ae17a26673e</p>
<p>registry.redhat.io/codeready-workspaces/plugin-java11-rhel8@sha256:d93195134cef6351b1f9e3165fecc09f464dc99ab33d11b68fadd613d04d1636</p>	<p>plugin-java11-rhel8@sha256:d93195134cef6351b1f9e3165fecc09f464dc99ab33d11b68fadd613d04d1636</p>
<p>registry.redhat.io/codeready-workspaces/plugin-java8-openj9-rhel8@sha256:8d8948134405e45bdd895932afa85b6cf0fbfe4e9bb58ae9753d233ddf74672b</p>	<p>plugin-java8-openj9-rhel8@sha256:8d8948134405e45bdd895932afa85b6cf0fbfe4e9bb58ae9753d233ddf74672b</p>
<p>registry.redhat.io/codeready-workspaces/plugin-java8-openj9-rhel8@sha256:8d8948134405e45bdd895932afa85b6cf0fbfe4e9bb58ae9753d233ddf74672b</p>	<p>plugin-java8-openj9-rhel8@sha256:8d8948134405e45bdd895932afa85b6cf0fbfe4e9bb58ae9753d233ddf74672b</p>
<p>registry.redhat.io/codeready-workspaces/plugin-java8-openj9-rhel8@sha256:8d8948134405e45bdd895932afa85b6cf0fbfe4e9bb58ae9753d233ddf74672b</p>	<p>plugin-java8-openj9-rhel8@sha256:8d8948134405e45bdd895932afa85b6cf0fbfe4e9bb58ae9753d233ddf74672b</p>

<source-image>	<target-image>
registry.redhat.io/codeready-workspaces/plugin-java8-rhel8@sha256:ecaa9ddef5ca8db9552f1b5e66f7aacb19d72e488d718d8135b1e1d9f66a1a7a	plugin-java8-rhel8@sha256:ecaa9ddef5ca8db9552f1b5e66f7aacb19d72e488d718d8135b1e1d9f66a1a7a
registry.redhat.io/codeready-workspaces/plugin-kubernetes-rhel8@sha256:cf1d0e24f8bae0f87cae0b1577dfd25e124437d78031d7076fabebb2dcf48d7f	plugin-kubernetes-rhel8@sha256:cf1d0e24f8bae0f87cae0b1577dfd25e124437d78031d7076fabebb2dcf48d7f
registry.redhat.io/codeready-workspaces/plugin-openshift-rhel8@sha256:13ce6d8fdeeea0cc5a220eb8abd2811c31bb2a424736759be9a6df15c8f77fd	plugin-openshift-rhel8@sha256:13ce6d8fdeeea0cc5a220eb8abd2811c31bb2a424736759be9a6df15c8f77fd
registry.redhat.io/codeready-workspaces/pluginbroker-artifacts-rhel8@sha256:cda306cb7e5c42faa6ab43218d39984d4955134b3ca9654968c28b05e0796c3a	pluginbroker-artifacts-rhel8@sha256:cda306cb7e5c42faa6ab43218d39984d4955134b3ca9654968c28b05e0796c3a
registry.redhat.io/codeready-workspaces/pluginbroker-metadata-rhel8@sha256:0143a80b869620af08a0d60165dc9d13357a79e7243502832326cf053c17ee38	pluginbroker-metadata-rhel8@sha256:0143a80b869620af08a0d60165dc9d13357a79e7243502832326cf053c17ee38
registry.redhat.io/codeready-workspaces/pluginregistry-rhel8@sha256:3f5163a2303de7f538eca2cc560403f38b920af1169821dfa06dbef695fb10c6	pluginregistry-rhel8@sha256:3f5163a2303de7f538eca2cc560403f38b920af1169821dfa06dbef695fb10c6
registry.redhat.io/codeready-workspaces/server-rhel8@sha256:6635e8c160c8c73c00c9b05eccab08a4ff23d344f102ef0097a3798bf108217a	server-rhel8@sha256:6635e8c160c8c73c00c9b05eccab08a4ff23d344f102ef0097a3798bf108217a
registry.redhat.io/codeready-workspaces/stacks-cpp-rhel8@sha256:06cd3600c3b6c3dca0451b10b46961fd0db4140c7dddc4f9637984022f5cfc09	stacks-cpp-rhel8@sha256:06cd3600c3b6c3dca0451b10b46961fd0db4140c7dddc4f9637984022f5cfc09

<source-image>	<target-image>
<p>registry.redhat.io/codeready-workspaces/stacks-dotnet-rhel8@sha256:ea77974b206c7d7abcd5cd32149f6bb669d3cf867135553af4d7dddd24ba9cf</p>	<p>stacks-dotnet-rhel8@sha256:ea77974b206c7d7abcd5cd32149f6bb669d3cf867135553af4d7dddd24ba9cf</p>
<p>registry.redhat.io/codeready-workspaces/stacks-golang-rhel8@sha256:e01d32e58a55a552f0d35b9a6210b7a2cc8ed444f8ae54a24113dcc85f4d80db</p>	<p>stacks-golang-rhel8@sha256:e01d32e58a55a552f0d35b9a6210b7a2cc8ed444f8ae54a24113dcc85f4d80db</p>
<p>registry.redhat.io/codeready-workspaces/stacks-php-rhel8@sha256:95c324ed660924bf76e10b461d75aa5be2a323f26e5033239f7cbfe1ec10b26e</p>	<p>stacks-php-rhel8@sha256:95c324ed660924bf76e10b461d75aa5be2a323f26e5033239f7cbfe1ec10b26e</p>
<p>registry.redhat.io/codeready-workspaces/theia-endpoint-rhel8@sha256:60c84fca55a997a6aab4ca07b8ff7d859948c1f525adeba2ae624c84fe059a56</p>	<p>theia-endpoint-rhel8@sha256:60c84fca55a997a6aab4ca07b8ff7d859948c1f525adeba2ae624c84fe059a56</p>
<p>registry.redhat.io/codeready-workspaces/theia-rhel8@sha256:de36fdf140ba6367e6edf577d6dbaffa270e5e5ecf0890e498f5907f8287858f</p>	<p>theia-rhel8@sha256:de36fdf140ba6367e6edf577d6dbaffa270e5e5ecf0890e498f5907f8287858f</p>
<p>registry.redhat.io/codeready-workspaces/traefik-rhel8@sha256:0698a776c6ae2f08238cf011d69ac2c67f934b1e25ec38701a9e360430fd10f7</p>	<p>traefik-rhel8@sha256:0698a776c6ae2f08238cf011d69ac2c67f934b1e25ec38701a9e360430fd10f7</p>
<p>registry.redhat.io/jboss-eap-7/eap-xp2-openj9-11-openshift-rhel8@sha256:95d2ce73a0759de5befdbec115514a555752e2f20070fbfe356801da6d0a2bd6</p>	<p>eap-xp2-openj9-11-openshift-rhel8@sha256:95d2ce73a0759de5befdbec115514a555752e2f20070fbfe356801da6d0a2bd6</p>
<p>registry.redhat.io/jboss-eap-7/eap-xp2-openj9-11-openshift-rhel8@sha256:95d2ce73a0759de5befdbec115514a555752e2f20070fbfe356801da6d0a2bd6</p>	<p>eap-xp2-openj9-11-openshift-rhel8@sha256:95d2ce73a0759de5befdbec115514a555752e2f20070fbfe356801da6d0a2bd6</p>

<source-image>	<target-image>
registry.redhat.io/jboss-eap-7/eap-xp2-openj9-11-openshift-rhel8@sha256:95d2ce73a0759de5befdbec115514a555752e2f20070fbfe356801da6d0a2bd6	eap-xp2-openj9-11-openshift-rhel8@sha256:95d2ce73a0759de5befdbec115514a555752e2f20070fbfe356801da6d0a2bd6
registry.redhat.io/jboss-eap-7/eap-xp2-openjdk11-openshift-rhel8@sha256:647d092383a760edc083eafb2d7bc3208d6409097281bedbd5eaccde360e7e39	eap-xp2-openjdk11-openshift-rhel8@sha256:647d092383a760edc083eafb2d7bc3208d6409097281bedbd5eaccde360e7e39
registry.redhat.io/jboss-eap-7/eap73-openjdk8-openshift-rhel7@sha256:d16cfe30eaf20a157cd5d5980a6c34f3fcbcf2fd225e670a0138d81007dd919	eap73-openjdk8-openshift-rhel7@sha256:d16cfe30eaf20a157cd5d5980a6c34f3fcbcf2fd225e670a0138d81007dd919
registry.redhat.io/rh-sso-7/sso74-openj9-openshift-rhel8@sha256:ed11770a85ca95fc9cbb2cade539a67ff0e127cff73a89a017415800e032bd5b	sso74-openj9-openshift-rhel8@sha256:ed11770a85ca95fc9cbb2cade539a67ff0e127cff73a89a017415800e032bd5b
registry.redhat.io/rh-sso-7/sso74-openj9-openshift-rhel8@sha256:ed11770a85ca95fc9cbb2cade539a67ff0e127cff73a89a017415800e032bd5b	sso74-openj9-openshift-rhel8@sha256:ed11770a85ca95fc9cbb2cade539a67ff0e127cff73a89a017415800e032bd5b
registry.redhat.io/rh-sso-7/sso74-openshift-rhel8@sha256:3154fd4f6ce080260de9d2b4c02930b67b57f1181f4e660f5ddfc9f6050420b1	sso74-openshift-rhel8@sha256:3154fd4f6ce080260de9d2b4c02930b67b57f1181f4e660f5ddfc9f6050420b1
registry.redhat.io/rhel8/postgresql-96@sha256:32d73d737acec3daabc3f5c8236588454c8f57f7a2656ac7a50cf3a04f520b9b	postgresql-96@sha256:32d73d737acec3daabc3f5c8236588454c8f57f7a2656ac7a50cf3a04f520b9b
registry.redhat.io/rhsc1/mongodb-36-rhel7@sha256:9f799d356d7d2e442bde9d401b720600fd9059a3d8eefea6f3b2ffa721c0dc73	mongodb-36-rhel7@sha256:9f799d356d7d2e442bde9d401b720600fd9059a3d8eefea6f3b2ffa721c0dc73

<source-image>	<target-image>
registry.redhat.io/ubi8/ubi-minimal@sha256:2f6b88c037c0503da7704bccd3fc73cb76324101af39ad28f16460e7bce98324	ubi8ubi-minimal@sha256:2f6b88c037c0503da7704bccd3fc73cb76324101af39ad28f16460e7bce98324

Verification steps

- Verify the images have the same digests:

```
$ skopeo inspect docker://<source-image>
$ skopeo inspect docker://<target-registry>/<target-organization>/<target-image>
```

Additional resources

- To find the sources of the images list, see the values of the **relatedImages** attribute in the [CodeReady Workspaces Operator ClusterServiceVersion sources](#).

3.4.2.2. Preparing CodeReady Workspaces Custom Resource for restricted environment

When installing CodeReady Workspaces in a restricted environment using **crwctl** or OperatorHub, provide a **CheCluster** custom resource with additional information.

3.4.2.2.1. Downloading the default **CheCluster** Custom Resource

Procedure

1. Download [the default custom resource YAML file](#).
2. Name the downloaded custom resource **org_v1_che_cr.yaml**. Keep it for further modification and usage.

3.4.2.2.2. Customizing the **CheCluster** Custom Resource for restricted environment

Prerequisites

- All required images available in an image registry that is visible to the OpenShift cluster where CodeReady Workspaces is to be deployed. This is described in [Section 3.4.2.1, "Preparing an private registry"](#), where the placeholders used in the following examples are also defined.

Procedure

1. In the **CheCluster** Custom Resource, which is managed by the CodeReady Workspaces Operator, add the fields used to facilitate deploying an instance of CodeReady Workspaces in a restricted environment:

```
# [...]
spec:
  server:
```

```
airGapContainerRegistryHostname: '<target-registry>'
airGapContainerRegistryOrganization: '<target-organization>'
# [...]
```

3.4.2.3. Starting CodeReady Workspaces installation in a restricted environment using CodeReady Workspaces CLI management tool

This section describes how to start the CodeReady Workspaces installation in a restricted environment using the CodeReady Workspaces CLI management tool.

Prerequisites

- CodeReady Workspaces CLI management tool is installed. See [Section 3.3.1, “Installing the crwctl CLI management tool”](#).
- The **oc** tool is installed.
- Access to an OpenShift instance.

Procedure

1. Log in to OpenShift Container Platform:

```
$ oc login ${OPENSIFT_API_URL} --username ${OPENSIFT_USERNAME} \
--password ${OPENSIFT_PASSWORD}
```

2. Install CodeReady Workspaces with a customized Custom Resource to add fields related to the restricted environment:

```
$ crwctl server:start \
--che-operator-image=<target-registry>/<target-organization>/crw-2-rhel8-operator:2.8 \
--che-operator-cr-yaml=org_v1_che_cr.yaml
```



NOTE

For slow systems or internet connections, add the **--k8spodwaittimeout=1800000** flag option to the **crwctl server:start** command to extend the Pod timeout period to 1800000 ms or longer.

3.4.3. Preparing CodeReady Workspaces Custom Resource for installing behind a proxy

This procedure describes how to provide necessary additional information to the **CheCluster** custom resource when installing CodeReady Workspaces behind a proxy.

Procedure

1. In the **CheCluster** Custom Resource, which is managed by the CodeReady Workspaces Operator, add the fields used to facilitate deploying an instance of CodeReady Workspaces in a restricted environment:

```
# [...]  
spec:
```

```
server:
  proxyURL: '<URL of the proxy, with the http protocol, and without the port>'
  proxyPort: '<Port of proxy, typically 3128>'
# [...]
```

- In addition to those basic settings, the proxy configuration usually requires adding the host of the external OpenShift cluster API URL in the list of the hosts to be accessed from CodeReady Workspaces without using the proxy.

To retrieve this cluster API host, run the following command against the OpenShift cluster:

```
$ oc whoami --show-server | sed 's#https://##' | sed 's#:.*$##'
```

The corresponding field of the **CheCluster** Custom Resource is **nonProxyHosts**. If a host already exists in this field, use `|` as a delimiter to add the cluster API host:

```
# [...]
spec:
  server:
    nonProxyHosts: 'anotherExistingHost|<cluster api host>'
# [...]
```

CHAPTER 4. CONFIGURING CODEREADY WORKSPACES

The following chapter describes configuration methods and options for Red Hat CodeReady Workspaces, with some user stories as example.

- [Section 4.1, “Advanced configuration options for the CodeReady Workspaces server component”](#) describes advanced configuration methods to use when the previous method is not applicable.

The next sections describe some specific user stories.

- [Section 4.2, “Configuring project strategies”](#)
- [Section 4.5, “Running more than one workspace at a time”](#)
- [Section 4.7, “Configuring workspaces nodeSelector”](#)
- [Section 4.8, “Configuring Red Hat CodeReady Workspaces server hostname”](#)
- [Section 4.9, “Configuring labels for OpenShift Route”](#)
- [Section 4.10, “Configuring labels and domains for OpenShift Route to work with Router Sharding”](#)
- [Section 4.11, “Deploying CodeReady Workspaces with support for Git repositories with self-signed certificates”](#)
- [Section 4.12, “Installing CodeReady Workspaces using storage classes”](#)
- [Section 4.4, “Configuring storage types”](#)
- [Section 4.13, “Importing untrusted TLS certificates to CodeReady Workspaces”](#)
- [Section 4.14, “Switching between external and internal DNS names in inter-component communication”](#)
- [Section 4.15, “Setting up the RH-SSO codeready-workspaces-username-readonly theme for the Red Hat CodeReady Workspaces login page”](#)
- [Section 4.16, “Mounting a secret as a file or an environment variable into a Red Hat CodeReady Workspaces container”](#)
- [Section 4.17, “Enabling Dev Workspace engine”](#)

4.1. ADVANCED CONFIGURATION OPTIONS FOR THE CODEREADY WORKSPACES SERVER COMPONENT

The following section describes advanced deployment and configuration methods for the CodeReady Workspaces server component.

4.1.1. Understanding CodeReady Workspaces server advanced configuration using the Operator

The following section describes the CodeReady Workspaces server component advanced configuration method for a deployment using the Operator.

Advanced configuration is necessary to:

- Add environment variables not automatically generated by the Operator from the standard **CheCluster** Custom Resource fields.
- Override the properties automatically generated by the Operator from the standard **CheCluster** Custom Resource fields.

The **customCheProperties** field, part of the **CheCluster** Custom Resource **server** settings, contains a map of additional environment variables to apply to the CodeReady Workspaces server component.

Example 4.1. Override the default memory limit for workspaces

- Add the **CHE_WORKSPACE_DEFAULT_MEMORY_LIMIT_MB** property to **customCheProperties**:

```
apiVersion: org.eclipse.che/v1
kind: CheCluster
# [...]
spec:
  server:
    # [...]
    customCheProperties:
      CHE_WORKSPACE_DEFAULT_MEMORY_LIMIT_MB: "2048"
# [...]
```



NOTE

Previous versions of the CodeReady Workspaces Operator had a ConfigMap named **custom** to fulfill this role. If the CodeReady Workspaces Operator finds a **configMap** with the name **custom**, it adds the data it contains into the **customCheProperties** field, redeploys CodeReady Workspaces, and deletes the **custom configMap**.

Additional resources

- For the list of all parameters available in the **CheCluster** Custom Resource, see [Chapter 2, *Configuring the CodeReady Workspaces installation*](#).
- For the list of all parameters available to configure **customCheProperties**, see [Section 4.1.2, *“CodeReady Workspaces server component system properties reference”*](#).

4.1.2. CodeReady Workspaces server component system properties reference

The following document describes all possible configuration properties of the CodeReady Workspaces server component.

4.1.2.1. Che server

Table 4.1. Che server

Environment Variable Name	Default value	Description
CHE_DATABASE	<code>\${che.home}/storage</code>	Folder where CodeReady Workspaces stores internal data objects.
CHE_API	<code>http://\${CHE_HOST}:\${CHE_PORT}/api</code>	API service. Browsers initiate REST communications to CodeReady Workspaces server with this URL.
CHE_API_INTERNAL	<code>http://\${CHE_HOST}:\${CHE_PORT}/api</code>	API service internal network url. Back-end services should initiate REST communications to CodeReady Workspaces server with this URL.
CHE_WEBSOCKET_ENDPOINT	<code>ws://\${CHE_HOST}:\${CHE_PORT}/api/websocket</code>	CodeReady Workspaces websocket major endpoint. Provides basic communication endpoint for major websocket interactions and messaging.
CHE_WORKSPACE_PROJECTS_STORAGE	<code>/projects</code>	Your projects are synchronized from the CodeReady Workspaces server into the machine running each workspace. This is the directory in the machine where your projects are placed.
CHE_WORKSPACE_PROJECTS_STORAGE_DEFAULT_SIZE	<code>1Gi</code>	Used when OpenShift-type components in a devfile request project PVC creation (Applied in case of 'unique' and 'per workspace' PVC strategy. In case of the 'common' PVC strategy, it is rewritten with the value of the <code>che.infra.kubernetes.pvc.quantity</code> property.)
CHE_WORKSPACE_LOGS_ROOT_DIR	<code>/workspace_logs</code>	Defines the directory inside the machine where all the workspace logs are placed. Provide this value into the machine, for example, as an environment variable. This is to ensure that agent developers can use this directory to back up agent logs.

Environment Variable Name	Default value	Description
CHE_WORKSPACE_HTTP__PROXY		Configures environment variable HTTP_PROXY to a specified value in containers powering workspaces.
CHE_WORKSPACE_HTTPS__PROXY		Configures environment variable HTTPS_PROXY to a specified value in containers powering workspaces.
CHE_WORKSPACE_NO__PROXY		Configures environment variable NO_PROXY to a specified value in containers powering workspaces.
CHE_WORKSPACE_AUTO__START	true	By default, when users access a workspace with its URL, the workspace automatically starts (if currently stopped). Set this to false to disable this behavior.
CHE_WORKSPACE_POOL_TTYPE	fixed	Workspace threads pool configuration. This pool is used for workspace-related operations that require asynchronous execution, for example, starting and stopping. Possible values are fixed and cached .
CHE_WORKSPACE_POOL_EXACT_SIZE	30	This property is ignored when pool type is different from fixed . It configures the exact size of the pool. When set, the multiplier property is ignored. If this property is not set (0 , <0 , NULL), then the pool size equals the number of cores. See also che.workspace.pool.cores_multiplier .
CHE_WORKSPACE_POOL_CORES_MULTIPLIER	2	This property is ignored when pool type is not set to fixed , che.workspace.pool.exact_size is set. When set, the pool size is N_CORES * multiplier .
CHE_WORKSPACE_PROBE_POOL_SIZE	10	This property specifies how many threads to use for workspace server liveness probes.

Environment Variable Name	Default value	Description
CHE_WORKSPACE_HTTP_PROXY_JAVA_OPTIONS	NULL	HTTP proxy setting for workspace JVM.
CHE_WORKSPACE_JAVA_OPTIONS	-XX:MaxRAM=150m - XX:MaxRAMFraction=2 - XX:+UseParallelGC - XX:MinHeapFreeRatio=10 - XX:MaxHeapFreeRatio=20 - XX:GCTimeRatio=4 - XX:AdaptiveSizePolicyWeight=90 - Dsun.zip.disableMemoryMapping=true -Xms20m - Djava.security.egd=file:/dev/. /urandom	Java command-line options added to JVMs running in workspaces.
CHE_WORKSPACE_MAVEN_OPTIONS	-XX:MaxRAM=150m - XX:MaxRAMFraction=2 - XX:+UseParallelGC - XX:MinHeapFreeRatio=10 - XX:MaxHeapFreeRatio=20 - XX:GCTimeRatio=4 - XX:AdaptiveSizePolicyWeight=90 - Dsun.zip.disableMemoryMapping=true -Xms20m - Djava.security.egd=file:/dev/. /urandom	Maven command-line options added to JVMs running agents in workspaces.
CHE_WORKSPACE_DEFAULT_MEMORY_LIMIT_MB	1024	RAM limit default for each machine that has no RAM settings in its environment. Value less or equal to 0 is interpreted as disabling the limit.
CHE_WORKSPACE_DEFAULT_MEMORY_REQUEST_MB	200	RAM request for each container that has no explicit RAM settings in its environment. This amount is allocated when the workspace container is created. This property may not be supported by all infrastructure implementations. Currently it is supported by OpenShift. A memory request exceeding the memory limit is ignored, and only the limit size is used. Value less or equal to 0 is interpreted as disabling the limit.

Environment Variable Name	Default value	Description
CHE_WORKSPACE_DEFAULT_CPU_LIMIT_CORES	-1	CPU limit for each container that has no CPU settings in its environment. Specify either in floating point cores number, for example, 0.125 , or using the OpenShift format, integer millicores, for example, 125m . Value less or equal to 0 is interpreted as disabling the limit.
CHE_WORKSPACE_DEFAULT_CPU_REQUEST_CORES	-1	CPU request for each container that has no CPU settings in environment. A CPU request exceeding the CPU limit is ignored, and only limit number is used. Value less or equal to 0 is interpreted as disabling the limit.
CHE_WORKSPACE_SIDECAR_DEFAULT_MEMORY_LIMIT_MB	128	RAM limit for each sidecar that has no RAM settings in the CodeReady Workspaces plug-in configuration. Value less or equal to 0 is interpreted as disabling the limit.
CHE_WORKSPACE_SIDECAR_DEFAULT_MEMORY_REQUEST_MB	64	RAM request for each sidecar that has no RAM settings in the CodeReady Workspaces plug-in configuration.
CHE_WORKSPACE_SIDECAR_DEFAULT_CPU_LIMIT_CORES	-1	CPU limit default for each sidecar that has no CPU settings in the CodeReady Workspaces plug-in configuration. Specify either in floating point cores number, for example, 0.125 , or using the OpenShift format, integer millicores, for example, 125m . Value less or equal to 0 is interpreted as disabling the limit.
CHE_WORKSPACE_SIDECAR_DEFAULT_CPU_REQUEST_CORES	-1	CPU request default for each sidecar that has no CPU settings in the CodeReady Workspaces plug-in configuration. Specify either in floating point cores number, for example, 0.125 , or using the OpenShift format, integer millicores, for example, 125m .

Environment Variable Name	Default value	Description
CHE_WORKSPACE_SIDECA R_IMAGE_PULL_POLICY	Always	Defines image-pulling strategy for sidecars. Possible values are: Always, Never, IfNotPresent . For any other value, Always is assumed for images with the :latest tag, or IfNotPresent for all other cases.
CHE_WORKSPACE_ACTIVIT Y_CHECK_SCHEDULER_ PERIOD__S	60	Period of inactive workspaces suspend job execution.
CHE_WORKSPACE_ACTIVIT Y_CLEANUP_SCHEDULER __PERIOD__S	3600	The period of the cleanup of the activity table. The activity table can contain invalid or stale data if some unforeseen errors happen, like a server crash at a peculiar point in time. The default is to run the cleanup job every hour.
CHE_WORKSPACE_ACTIVIT Y_CLEANUP_SCHEDULER __INITIAL_DELAY__S	60	The delay after server startup to start the first activity clean up job.
CHE_WORKSPACE_ACTIVIT Y_CHECK_SCHEDULER_ DELAY__S	180	Delay before first workspace idleness check job started to avoid mass suspend if ws master was unavailable for period close to inactivity timeout.
CHE_WORKSPACE_CLEANU P_TEMPORARY_INITIAL_ DELAY__MIN	5	Time period to delay the first execution of temporary workspaces cleanup job.
CHE_WORKSPACE_CLEANU P_TEMPORARY_PERIOD_ __MIN	180	Time period delay between the termination of one execution and the commencement of the next execution of temporary workspaces cleanup job
CHE_WORKSPACE_SERVER _PING_SUCCESS_THRES HOLD	1	Number of sequential successful pings to server after which it is treated as available. Note: the property is common for all servers e.g. workspace agent, terminal, exec etc.

Environment Variable Name	Default value	Description
CHE_WORKSPACE_SERVER_PING_INTERVAL_MILLISECONDS	3000	Interval, in milliseconds, between successive pings to workspace server.
CHE_WORKSPACE_SERVER_LIVENESS_PROBES	wsagent/http,exec-agent/http,terminal,theia,jupyter,dirigible,cloud-shell,intellij	List of servers names which require liveness probes
CHE_WORKSPACE_STARTUP_DEBUG_LOG_LIMIT_BYTES	10485760	Limit size of the logs collected from single container that can be observed by che-server when debugging workspace startup. default 10MB=10485760
CHE_WORKSPACE_STOP_ROLE_ENABLED	true	If true, 'stop-workspace' role with the edit privileges will be granted to the 'che' ServiceAccount if OpenShift OAuth is enabled. This configuration is mainly required for workspace idling when the OpenShift OAuth is enabled.
CHE_DEVWORKSPACES_ENABLED	false	Specifies whether che is deployed with DevWorkspaces enabled. This property is set by the CodeReady Workspaces operator if it also installed the support for DevWorkspaces. This property is used to advertise this fact to the CodeReady Workspaces dashboard. It does not make sense to change the value of this property manually.

4.1.2.2. Authentication parameters

Table 4.2. Authentication parameters

Environment Variable Name	Default value	Description
CHE_AUTH_USER_SELF_CREATION	false	CodeReady Workspaces has a single identity implementation, so this does not change the user experience. If true, enables user creation at API level
CHE_AUTH_ACCESS_DENIED_ERROR_PAGE	/error-oauth	Authentication error page address

Environment Variable Name	Default value	Description
CHE_AUTH_RESERVED_USER_NAMES		Reserved user names
CHE_OAUTH_GITHUB_CLIENTID	NULL	Configuration of GitHub OAuth client. You can setup GitHub OAuth to automate authentication to remote repositories. You need to first register this application with GitHub OAuth. GitHub OAuth client ID.
CHE_OAUTH_GITHUB_CLIENTSECRET	NULL	GitHub OAuth client secret.
CHE_OAUTH_GITHUB_AUTH_URI	https://github.com/login/oauth/authorize	GitHub OAuth authorization URI.
CHE_OAUTH_GITHUB_TOKEN_URI	https://github.com/login/oauth/access_token	GitHub OAuth token URI.
CHE_OAUTH_GITHUB_REDIRECTURIS	http://localhost:\${CHE_PORT}/api/oauth/callback	GitHub OAuth redirect URIs. Separate multiple values with comma, for example: URI,URI,URI
CHE_OAUTH_OPENSHIFT_CLIENTID	NULL	Configuration of OpenShift OAuth client. Used to obtain OpenShift OAuth token. OpenShift OAuth client ID.
CHE_OAUTH_OPENSHIFT_CLIENTSECRET	NULL	Configuration of OpenShift OAuth client. Used to obtain OpenShift OAuth token. OpenShift OAuth client ID. OpenShift OAuth client secret.
CHE_OAUTH_OPENSHIFT_AUTH_ENDPOINT	NULL	Configuration of OpenShift OAuth client. Used to obtain OpenShift OAuth token. OpenShift OAuth client ID. OpenShift OAuth client secret. OpenShift OAuth endpoint.

Environment Variable Name	Default value	Description
CHE_OAUTH_OPENSIFT_VERIFY__TOKEN__URL	NULL	Configuration of OpenShift OAuth client. Used to obtain OpenShift OAuth token. OpenShift OAuth client ID. OpenShift OAuth client secret. OpenShift OAuth endpoint. OpenShift OAuth verification token URL.
CHE_OAUTH1_BITBUCKET_CONSUMERKEYPATH	NULL	Configuration of Bitbucket Server OAuth1 client. Used to obtain Personal access tokens. Location of the file with Bitbucket Server application consumer key (equivalent to a username).
CHE_OAUTH1_BITBUCKET_PRIVATEKEYPATH	NULL	Configuration of Bitbucket Server OAuth1 client. Used to obtain Personal access tokens. Location of the file with Bitbucket Server application consumer key (equivalent to a username). Location of the file with Bitbucket Server application private key
CHE_OAUTH1_BITBUCKET_ENDPOINT	NULL	Configuration of Bitbucket Server OAuth1 client. Used to obtain Personal access tokens. Location of the file with Bitbucket Server application consumer key (equivalent to a username). Location of the file with Bitbucket Server application private key Bitbucket Server URL. To work correctly with factories the same URL has to be part of che.integration.bitbucket.server_endpoints too.

4.1.2.3. Internal

Table 4.3. Internal

Environment Variable Name	Default value	Description
---------------------------	---------------	-------------

Environment Variable Name	Default value	Description
SCHEDULE_CORE__POOL__SIZE	10	CodeReady Workspaces extensions can be scheduled executions on a time basis. This configures the size of the thread pool allocated to extensions that are launched on a recurring schedule.
DB_SCHEMA_FLYWAY_BASELINE_ENABLED	true	DB initialization and migration configuration. If true, ignore scripts up to the version configured by baseline.version.
DB_SCHEMA_FLYWAY_BASELINE_VERSION	5.0.0.8.1	Scripts with version up to this are ignored. Note that scripts with version equal to baseline version are also ignored.
DB_SCHEMA_FLYWAY_SCRIPTS_PREFIX		Prefix of migration scripts.
DB_SCHEMA_FLYWAY_SCRIPTS_SUFFIX	.sql	Suffix of migration scripts.
DB_SCHEMA_FLYWAY_SCRIPTS_VERSION_SEPARATOR	—	Separator of version from the other part of script name.
DB_SCHEMA_FLYWAY_SCRIPTS_LOCATIONS	classpath:che-schema	Locations where to search migration scripts.

4.1.2.4. OpenShift Infra parameters

Table 4.4. OpenShift Infra parameters

Environment Variable Name	Default value	Description
CHE_INFRA_KUBERNETES_MASTER_URL		Configuration of OpenShift client master URL that Infra will use.
CHE_INFRA_KUBERNETES_TRUST_CERTS	false	Boolean to configure OpenShift client in order to use trusted certificates.

Environment Variable Name	Default value	Description
CHE_INFRA_KUBERNETES_SERVER_STRATEGY	multi-host	Defines the way how servers are exposed to the world in OpenShift infra. List of strategies implemented in CodeReady Workspaces: default-host, multi-host, single-host
CHE_INFRA_KUBERNETES_SINGLEHOST_WORKSPACE_EXPOSURE	native	Defines the way in which the workspace plugins and editors are exposed in the single-host mode. Supported exposures: - 'native': Exposes servers using OpenShift Ingresses. Works only on Kubernetes. - 'gateway': Exposes servers using reverse-proxy gateway.
CHE_INFRA_KUBERNETES_SINGLEHOST_WORKSPACE_DEVFILE_ENDPOINT_EXPOSURE	multi-host	Defines the way how to expose devfile endpoints, thus end-user's applications, in single-host server strategy. They can either follow the single-host strategy and be exposed on subpaths, or they can be exposed on subdomains. - 'multi-host': expose on subdomains - 'single-host': expose on subpaths
CHE_INFRA_KUBERNETES_SINGLEHOST_GATEWAY_CONFIGMAP_LABELS	app=che,component=che-gateway-config	Defines labels which will be set to ConfigMaps configuring single-host gateway.
CHE_INFRA_KUBERNETES_INGRESS_DOMAIN		Used to generate domain for a server in a workspace in case property che.infra.kubernetes.server_strategy is set to multi-host

Environment Variable Name	Default value	Description
CHE_INFRA_KUBERNETES_NAMESPACE		DEPRECATED - please do not change the value of this property otherwise the existing workspaces will loose data. Do not set it on new installations. Defines OpenShift project in which all workspaces will be created. If not set, every workspace will be created in a new namespace, where namespace = workspace id. It's possible to use <username> and <userid> placeholders (e.g.: che-workspace-<username>). In that case, new namespace will be created for each user. Service account with permission to create new namespace must be used. Ignored for OpenShift infra. Use che.infra.openshift.project instead. If the namespace pointed to by this property exists, it will be used for all workspaces. If it does not exist, the namespace specified by the che.infra.kubernetes.namespace.default will be created and used.
CHE_INFRA_KUBERNETES_NAMESPACE_CREATION_ALLOWED	true	Indicates whether CodeReady Workspaces server is allowed to create namespaces/projects for user workspaces, or they're intended to be created manually by cluster administrator. This property is also used by the OpenShift infra.
CHE_INFRA_KUBERNETES_NAMESPACE_DEFAULT	<username>-che	Defines default OpenShift project in which user's workspaces are created if user does not override it. It's possible to use <username>, <userid> and <workspaceid> placeholders (e.g.: che-workspace-<username>). In that case, new namespace will be created for each user (or workspace). Is used by OpenShift infra as well to specify Project
CHE_INFRA_KUBERNETES_NAMESPACE_LABEL	true	Defines whether che-server should try to label the workspace namespaces.

Environment Variable Name	Default value	Description
CHE_INFRA_KUBERNETES_NAMESPACE_LABELS	app.kubernetes.io/part-of=che.eclipse.org,app.kubernetes.io/component=workspaces-namespace	List of labels to find Namespaces/Projects that are used for CodeReady Workspaces Workspaces. They are used to: - find prepared Namespaces/Projects for users in combination with che.infra.kubernetes.namespace.annotations . - actively label namespaces with any workspace.
CHE_INFRA_KUBERNETES_NAMESPACE_ANNOTATIONS	che.eclipse.org/username=<username>	List of annotations to find Namespaces/Projects prepared for CodeReady Workspaces users workspaces. Only Namespaces/Projects matching the che.infra.kubernetes.namespace.labels will be matched against these annotations. Namespaces/Projects that matches both che.infra.kubernetes.namespace.labels and che.infra.kubernetes.namespace.annotations will be preferentially used for User's workspaces. It's possible to use <username> placeholder to specify the Namespace/Project to concrete user.
CHE_INFRA_KUBERNETES_NAMESPACE_ALLOW_USER_DEFINED	false	Defines if a user is able to specify OpenShift project (or OpenShift project) different from the default. It's NOT RECOMMENDED to configured true without OAuth configured. This property is also used by the OpenShift infra.

Environment Variable Name	Default value	Description
CHE_INFRA_KUBERNETES_SERVICE_ACCOUNT_NAME	NULL	Defines Kubernetes Service Account name which should be specified to be bound to all workspaces pods. Note that OpenShift Infrastructure won't create the service account and it should exist. OpenShift infrastructure will check if project is predefined(if che.infra.openshift.project is not empty): - if it is predefined then service account must exist there - if it is 'NULL' or empty string then infrastructure will create new OpenShift project per workspace and prepare workspace service account with needed roles there
CHE_INFRA_KUBERNETES_WORKSPACE_SA_CLUSTER_ROLES	NULL	Specifies optional, additional cluster roles to use with the workspace service account. Note that the cluster role names must already exist, and the CodeReady Workspaces service account needs to be able to create a Role Binding to associate these cluster roles with the workspace service account. The names are comma separated. This property deprecates 'che.infra.kubernetes.cluster_role_name'.
CHE_INFRA_KUBERNETES_WORKSPACE_START_TIMEOUT_MIN	8	Defines time frame that limits the Kubernetes workspace start time
CHE_INFRA_KUBERNETES_INGRESS_START_TIMEOUT_MIN	5	Defines the timeout in minutes that limits the period for which OpenShift Route become ready

Environment Variable Name	Default value	Description
CHE_INFRA_KUBERNETES_WORKSPACE__UNRECOVERABLE__EVENTS	FailedMount,FailedScheduling,MountVolume.SetUpfailed,Failed to pull image,FailedCreate,ReplicaSetCreateError	If during workspace startup an unrecoverable event defined in the property occurs, terminate workspace immediately instead of waiting until timeout Note that this SHOULD NOT include a mere 'Failed' reason, because that might catch events that are not unrecoverable. A failed container startup is handled explicitly by CodeReady Workspaces server.
CHE_INFRA_KUBERNETES_PVC_ENABLED	true	Defines whether use the Persistent Volume Claim for the workspace needs e.g backup projects, logs etc or disable it.
CHE_INFRA_KUBERNETES_PVC_STRATEGY	common	Defined which strategy will be used while choosing PVC for workspaces. Supported strategies: - 'common' All workspaces in the same Kubernetes Namespace will reuse the same PVC. Name of PVC may be configured with 'che.infra.kubernetes.pvc.name'. Existing PVC will be used or new one will be created if it doesn't exist. - 'unique' Separate PVC for each workspace's volume will be used. Name of PVC is evaluated as '{che.infra.kubernetes.pvc.name} + '-' + {generated_8_chars}'. Existing PVC will be used or a new one will be created if it doesn't exist. - 'per-workspace' Separate PVC for each workspace will be used. Name of PVC is evaluated as '{che.infra.kubernetes.pvc.name} + '-' + {WORKSPACE_ID}'. Existing PVC will be used or a new one will be created if it doesn't exist.

Environment Variable Name	Default value	Description
CHE_INFRA_KUBERNETES_PVC_PRECREATE__SUBPATHS	true	Defines whether to run a job that creates workspace's subpath directories in persistent volume for the 'common' strategy before launching a workspace. Necessary in some versions of OpenShift as workspace subpath volume mounts are created with root permissions, and thus cannot be modified by workspaces running as a user (presents an error importing projects into a workspace in CodeReady Workspaces). The default is 'true', but should be set to false if the version of Openshift/Kubernetes creates subdirectories with user permissions. Relevant issue: https://github.com/kubernetes/kubernetes/issues/41638 Note that this property has effect only if the 'common' PVC strategy used.
CHE_INFRA_KUBERNETES_PVC_NAME	claim-che-workspace	Defines the settings of PVC name for che workspaces. Each PVC strategy supplies this value differently. See doc for <code>che.infra.kubernetes.pvc.strategy</code> property
CHE_INFRA_KUBERNETES_PVC_STORAGE__CLASS__NAME		Defines the storage class of Persistent Volume Claim for the workspaces. Empty strings means 'use default'.
CHE_INFRA_KUBERNETES_PVC_QUANTITY	10Gi	Defines the size of Persistent Volume Claim of che workspace. Format described here: https://docs.openshift.com/container-platform/4.4/storage/understanding-persistent-storage.html
CHE_INFRA_KUBERNETES_PVC_JOBS_IMAGE	centos:centos7	Pod that is launched when performing persistent volume claim maintenance jobs on OpenShift

Environment Variable Name	Default value	Description
CHE_INFRA_KUBERNETES_PVC_JOBS_IMAGE_PULL_POLICY	IfNotPresent	Image pull policy of container that used for the maintenance jobs on Kubernetes/OpenShift cluster
CHE_INFRA_KUBERNETES_PVC_JOBS_MEMORYLIMIT	250Mi	Defines pod memory limit for persistent volume claim maintenance jobs
CHE_INFRA_KUBERNETES_PVC_ACCESS_MODE	ReadWriteOnce	Defines Persistent Volume Claim access mode. Note that for common PVC strategy changing of access mode affects the number of simultaneously running workspaces. If OpenShift flavor where che running is using PVs with RWX access mode then a limit of running workspaces at the same time bounded only by che limits configuration like(RAM, CPU etc). Detailed information about access mode is described here: https://docs.openshift.com/container-platform/4.4/storage/understanding-persistent-storage.html
CHE_INFRA_KUBERNETES_PVC_WAIT_BOUND	true	Defines whether CodeReady Workspaces Server should wait workspaces PVCs to become bound after creating. It's used by all PVC strategies. It should be set to false in case if volumeBindingMode is configured to WaitForFirstConsumer otherwise workspace starts will hangs up on phase of waiting PVCs. Default value is true (means that PVCs should be waited to be bound)

Environment Variable Name	Default value	Description
CHE_INFRA_KUBERNETES_INSTALLER_SERVER_MIN_PORT	10000	Defined range of ports for installers servers By default, installer will use own port, but if it conflicts with another installer servers then OpenShift infrastructure will reconfigure installer to use first available from this range Unused, will be removed.
CHE_INFRA_KUBERNETES_INSTALLER_SERVER_MAX_PORT	20000	Unused, will be removed.

Environment Variable Name	Default value	Description
CHE_INFRA_KUBERNETES_INGRESS_ANNOTATIONS_JSON	NULL	<p>Defines annotations for ingresses which are used for servers exposing. Value depends on the kind of ingress controller. OpenShift infrastructure ignores this property because it uses Routes instead of ingresses. Note that for a single-host deployment strategy to work, a controller supporting URL rewriting has to be used (so that URLs can point to different servers while the servers don't need to support changing the app root). The <code>che.infra.kubernetes.ingress.path.rewrite_transform</code> property defines how the path of the ingress should be transformed to support the URL rewriting and this property defines the set of annotations on the ingress itself that instruct the chosen ingress controller to actually do the URL rewriting, potentially building on the path transformation (if required by the chosen ingress controller). For example for nginx ingress controller 0.22.0 and later the following value is recommended:</p> <pre>{'ingress.kubernetes.io/rewrite-target': '/\$1','ingress.kubernetes.io/ssl-redirect': 'false',\ 'ingress.kubernetes.io/proxy-connect-timeout': '3600','ingress.kubernetes.io/proxy-read-timeout': '3600'}</pre> <p>and the <code>che.infra.kubernetes.ingress.path.rewrite_transform</code> should be set to <code>'%s(.*)'</code> For nginx ingress controller older than 0.22.0, the <code>rewrite-target</code> should be set to merely <code>'/'</code> and the path transform to <code>'%s'</code> (see the <code>che.infra.kubernetes.ingress.path.rewrite_transform</code> property). Please consult the nginx ingress controller documentation for the explanation of how the ingress controller uses the regular</p>

Environment Variable Name	Default value	Description
CHE_INFRA_KUBERNETES_INGRESS_PATH_TRANSFORM	NULL	expression present in the ingress path and how it achieves the URL rewriting. Defines a 'recipe' on how to declare the path of the ingress that should expose a server. The '%s' represents the base public URL of the server and is guaranteed to end with a forward slash. This property must be a valid input to the String.format() method and contain exactly one reference to '%s'. Please see the description of the che.infra.kubernetes.ingress.annotations.json property to see how these two properties interplay when specifying the ingress annotations and path. If not defined, this property defaults to '%s' (without the quotes) which means that the path is not transformed in any way for use with the ingress controller.
CHE_INFRA_KUBERNETES_INGRESS_LABELS	NULL	Additional labels to add into every Ingress created by CodeReady Workspaces server to allow clear identification.
CHE_INFRA_KUBERNETES_POD_SECURITY_CONTEXT_RUN_AS_USER	NULL	Defines security context for pods that will be created by OpenShift Infra. Specifies that for any Containers in the Pod, all processes run with given user ID. This is ignored by OpenShift infra
CHE_INFRA_KUBERNETES_POD_SECURITY_CONTEXT_FS_GROUP	NULL	Defines security context for pods that will be created by OpenShift Infra. A special supplemental group that applies to all containers in a pod. This is ignored by OpenShift infra.

Environment Variable Name	Default value	Description
CHE_INFRA_KUBERNETES_POD_TERMINATION_GRACE_PERIOD_SEC	0	Defines grace termination period for pods that will be created by Kubernetes / OpenShift infrastructures Grace termination period of Kubernetes / OpenShift workspace's pods defaults '0', which allows to terminate pods almost instantly and significantly decrease the time required for stopping a workspace. Note: if terminationGracePeriodSeconds have been explicitly set in Kubernetes / OpenShift recipe it will not be overridden.
CHE_INFRA_KUBERNETES_CLIENT_HTTP_ASYNC_REQUESTS_MAX	1000	Number of maximum concurrent async web requests (http requests or ongoing web socket calls) supported in the underlying shared http client of the KubernetesClient instances. Default values are 64, and 5 per-host, which doesn't seem correct for multi-user scenarios, knowing that CodeReady Workspaces keeps a number of connections opened (e.g. for command or ws-agent logs)
CHE_INFRA_KUBERNETES_CLIENT_HTTP_ASYNC_REQUESTS_MAX_PER_HOST	1000	Number of maximum concurrent async web requests per host.
CHE_INFRA_KUBERNETES_CLIENT_HTTP_CONNECTION_POOL_MAX_IDLE	5	Max number of idle connections in the connection pool of the Kubernetes-client shared http client
CHE_INFRA_KUBERNETES_CLIENT_HTTP_CONNECTION_POOL_KEEP_ALIVE_MIN	5	Keep-alive timeout of the connection pool of the Kubernetes-client shared http client in minutes
CHE_INFRA_KUBERNETES_TLS_ENABLED	false	Creates Ingresses with Transport Layer Security (TLS) enabled In OpenShift infrastructure, Routes will be TLS-enabled

Environment Variable Name	Default value	Description
CHE_INFRA_KUBERNETES_TLS__SECRET		Name of a secret that should be used when creating workspace ingresses with TLS Ignored by OpenShift infrastructure
CHE_INFRA_KUBERNETES_TLS__KEY	NULL	Key data for TLS Secret that should be used for workspaces Ingresses. Key should be encoded with Base64 algorithm. This property is ignored by OpenShift infrastructure.
CHE_INFRA_KUBERNETES_TLS__CERT	NULL	Certificate data for TLS Secret that should be used for workspaces Ingresses. Certificate should be encoded with Base64 algorithm. This property is ignored by OpenShift infrastructure.
CHE_INFRA_KUBERNETES_RUNTIMES__CONSISTENCY__CHECK__PERIOD__MIN	-1	Defines the period with which runtimes consistency checks will be performed. If runtime has inconsistent state then runtime will be stopped automatically. Value must be more than 0 or -1 , where -1 means that checks won't be performed at all. It is disabled by default because there is possible CodeReady Workspaces Server configuration when CodeReady Workspaces Server doesn't have an ability to interact with Kubernetes API when operation is not invoked by user. It DOES work on the following configurations: - workspaces objects are created in the same namespace where CodeReady Workspaces Server is located; - cluster-admin service account token is mount to CodeReady Workspaces Server pod; It DOES NOT work on the following configurations: - CodeReady Workspaces Server communicates with Kubernetes API using token from OAuth provider;

Environment Variable Name	Default value	Description
CHE_INFRA_KUBERNETES_TRUSTED__CA_SRC__CONFIGMAP	NULL	Name of config map in CodeReady Workspaces server namespace with additional CA TLS certificates to be propagated into all user's workspaces. If the property is set on OpenShift 4 infrastructure, and <code>che.infra.openshift.trusted_ca.dest_configmap_labels</code> includes <code>config.openshift.io/inject-trusted-cabundle=true</code> label, then cluster CA bundle will be propagated too.
CHE_INFRA_KUBERNETES_TRUSTED__CA_DEST__CONFIGMAP	ca-certs	Name of configmap in a workspace namespace with additional CA TLS certificates. Holds the copy of <code>che.infra.kubernetes.trusted_ca.src_configmap</code> but in a workspace namespace. Content of this config map is mounted into all workspace containers including plugin brokers. Do not change the config map name unless it conflicts with the already existing config map. Note that the resulting config map name can be adjusted eventually to make it unique in OpenShift namespace. The original name would be stored in che.original_name label.
CHE_INFRA_KUBERNETES_TRUSTED__CA_MOUNT__PATH	/public-certs	Configures path on workspace containers where the CA bundle should be mount. Content of config map specified by <code>che.infra.kubernetes.trusted_ca.dest_configmap</code> is mounted.
CHE_INFRA_KUBERNETES_TRUSTED__CA_DEST__CONFIGMAP__LABELS		Comma separated list of labels to add to the CA certificates config map in user workspace. See <code>che.infra.kubernetes.trusted_ca.dest_configmap</code> property.

4.1.2.5. OpenShift Infra parameters

Table 4.5. OpenShift Infra parameters

Environment Variable Name	Default value	Description
CHE_INFRA_OPENSIFT_PROJECT		DEPRECATED - please do not change the value of this property otherwise the existing workspaces will loose data. Do not set it on new installations. Defines OpenShift namespace in which all workspaces will be created. If not set, every workspace will be created in a new project, where project name = workspace id It's possible to use <username> and <userid> placeholders (e.g.: che-workspace-<username>). In that case, new project will be created for each user. OpenShift oauth or service account with permission to create new projects must be used. If the project pointed to by this property exists, it will be used for all workspaces. If it does not exist, the namespace specified by the che.infra.kubernetes.namespace.default will be created and used.
CHE_INFRA_OPENSIFT_TRUSTED_CA_DEST_CONFIGMAP_LABELS	config.openshift.io/inject-trusted-cabundle=true	Comma separated list of labels to add to the CA certificates config map in user workspace. See che.infra.kubernetes.trusted_ca_dest_configmap property. This default value is used for automatic cluster CA bundle injection in Openshift 4.
CHE_INFRA_OPENSIFT_ROUTE_LABELS	NULL	Additional labels to add into every Route created by CodeReady Workspaces server to allow clear identification.
CHE_INFRA_OPENSIFT_ROUTE_HOST_DOMAIN_SUFFIX	NULL	The hostname that should be used as a suffix for the workspace routes. For example host=open.che.org then the route will look like routed3qrtek.open.che.org It has to be a valid DNS name.

4.1.2.6. Experimental properties

Table 4.6. Experimental properties

Environment Variable Name	Default value	Description
CHE_WORKSPACE_PLUGIN_BROKER_METADATA_IMAGE	quay.io/eclipse/che-plugin-metadata-broker:v3.4.0	Docker image of plugin metadata broker. This broker must be run prior to starting the workspaces pod, as its job is to provision required containers, volumes, and environment variables for the workspace to be able to start with the installed plugins enabled. Note this image is overridden by the CodeReady Workspaces Operator by default; changing the image here will not have an effect if CodeReady Workspaces is installed via Operator.
CHE_WORKSPACE_PLUGIN_BROKER_ARTIFACTS_IMAGE	quay.io/eclipse/che-plugin-artifacts-broker:v3.4.0	Docker image of CodeReady Workspaces plugin artifacts broker. This broker runs as an init container on the workspace pod. Its job is to take in a list of plugin identifiers (either references to a plugin in the registry or a link to a plugin meta.yaml) and ensure that the correct .vsix and .theia extensions are downloaded into the /plugins directory, for each plugin requested for the workspace.
CHE_WORKSPACE_PLUGIN_BROKER_DEFAULT_MERGE_PLUGINS	false	Configures the default behavior of the plugin brokers when provisioning plugins into a workspace. If set to true, the plugin brokers will attempt to merge plugins when possible (i.e. they run in the same sidecar image and do not have conflicting settings). This value is the default setting used when the devfile does not specify otherwise, via the 'mergePlugins' attribute.
CHE_WORKSPACE_PLUGIN_BROKER_PULL_POLICY	Always	Docker image of CodeReady Workspaces plugin broker app that resolves workspace tooling configuration and copies plugins dependencies to a workspace
CHE_WORKSPACE_PLUGIN_BROKER_WAIT_TIMEOUT_MIN	3	Defines the timeout in minutes that limits the max period of result waiting for plugin broker.

Environment Variable Name	Default value	Description
CHE_WORKSPACE_PLUGIN__REGISTRY__URL	https://che-plugin-registry.prod-preview.openshift.io/v3	Workspace tooling plugins registry endpoint. Should be a valid HTTP URL. Example: http://che-plugin-registry-eclipse-che.192.168.65.2.nip.io In case CodeReady Workspaces plugins tooling is not needed value 'NULL' should be used
CHE_WORKSPACE_PLUGIN__REGISTRY__INTERNAL__URL	NULL	Workspace tooling plugins registry 'internal' endpoint. Should be a valid HTTP URL. Example: http://devfile-registry.che.svc.cluster.local:8080 In case CodeReady Workspaces plugins tooling is not needed value 'NULL' should be used
CHE_WORKSPACE_DEVFILE__REGISTRY__URL	https://che-devfile-registry.prod-preview.openshift.io/	Devfile Registry endpoint. Should be a valid HTTP URL. Example: http://che-devfile-registry-eclipse-che.192.168.65.2.nip.io In case CodeReady Workspaces plugins tooling is not needed value 'NULL' should be used
CHE_WORKSPACE_DEVFILE__REGISTRY__INTERNAL__URL	NULL	Devfile Registry 'internal' endpoint. Should be a valid HTTP URL. Example: http://plugin-registry.che.svc.cluster.local:8080 In case CodeReady Workspaces plugins tooling is not needed value 'NULL' should be used

Environment Variable Name	Default value	Description
CHE_WORKSPACE_STORAGE_AVAILABLE_TYPES	persistent,ephemeral,async	The configuration property that defines available values for storage types that clients like Dashboard should propose for users during workspace creation/update. Available values: <ul style="list-style-type: none"> - 'persistent': Persistent Storage slow I/O but persistent. - 'ephemeral': Ephemeral Storage allows for faster I/O but may have limited storage and is not persistent. - 'async': Experimental feature: Asynchronous storage is combination of Ephemeral and Persistent storage. Allows for faster I/O and keep your changes, will backup on stop and restore on start workspace. Will work only if: <ul style="list-style-type: none"> - che.infra.kubernetes.pvc.strategy='common' - che.limits.user.workspaces.run.count=1 - che.infra.kubernetes.namespace.allow_user_defined=false - che.infra.kubernetes.namespace.default contains <username> in other cases remove 'async' from the list.
CHE_WORKSPACE_STORAGE_PREFERRED_TYPE	persistent	The configuration property that defines a default value for storage type that clients like Dashboard should propose for users during workspace creation/update. The 'async' value not recommended as default type since it's experimental
CHE_SERVER_SECURE_EXPOSER	jwtproxy	Configures in which way secure servers will be protected with authentication. Suitable values: <ul style="list-style-type: none"> - 'default': jwtproxy is configured in a pass-through mode. So, servers should authenticate requests themselves. - 'jwtproxy': jwtproxy will authenticate requests. So, servers will receive only authenticated ones.

Environment Variable Name	Default value	Description
CHE_SERVER_SECURE_EX POSER_JWTPROXY_TOKEN _ISSUER	wsmaster	JWTProxy issuer string.
CHE_SERVER_SECURE_EX POSER_JWTPROXY_TOKEN _TTL	8800h	JWTProxy issuer token lifetime.
CHE_SERVER_SECURE_EX POSER_JWTPROXY_AUTH_ LOADER_PATH	/_app/loader.html	Optional authentication page path to route unsigned requests to.
CHE_SERVER_SECURE_EX POSER_JWTPROXY_IMAGE	quay.io/eclipse/che- jwtproxy:0.10.0	JWTProxy image.
CHE_SERVER_SECURE_EX POSER_JWTPROXY_MEMOR Y_REQUEST	15mb	JWTProxy memory request.
CHE_SERVER_SECURE_EX POSER_JWTPROXY_MEMOR Y_LIMIT	128mb	JWTProxy memory limit.
CHE_SERVER_SECURE_EX POSER_JWTPROXY_CPU_ REQUEST	0.03	JWTProxy CPU request.
CHE_SERVER_SECURE_EX POSER_JWTPROXY_CPU_ LIMIT	0.5	JWTProxy CPU limit.

4.1.2.7. Configuration of major "/websocket" endpoint

Table 4.7. Configuration of major "/websocket" endpoint

Environment Variable Name	Default value	Description
CHE_CORE_JSONRPC_PRO CESSOR_MAX_POOL_S IZE	50	Maximum size of the JSON RPC processing pool in case if pool size would be exceeded message execution will be rejected
CHE_CORE_JSONRPC_PRO CESSOR_CORE_POOL_S IZE	5	Initial json processing pool. Minimum number of threads that used to process major JSON RPC messages.

Environment Variable Name	Default value	Description
CHE_CORE_JSONRPC_PROCESSOR_QUEUE_CAPACITY	100000	Configuration of queue used to process Json RPC messages.
CHE_METRICS_PORT	8087	Port the the http server endpoint that would be exposed with Prometheus metrics

4.1.2.8. CORS settings

Table 4.8. CORS settings

Environment Variable Name	Default value	Description
CHE_CORS_ALLOWED_ORIGINS	*	CORS filter on WS Master is turned off by default. Use environment variable 'CHE_CORS_ENABLED=true' to turn it on 'cors.allowed.origins' indicates which request origins are allowed
CHE_CORS_ALLOW_CREDENTIALS	false	'cors.support.credentials' indicates if it allows processing of requests with credentials (in cookies, headers, TLS client certificates)

4.1.2.9. Factory defaults

Table 4.9. Factory defaults

Environment Variable Name	Default value	Description
CHE_FACTORY_DEFAULT_EDITOR	eclipse/che-theia/latest	Editor that will be used for factories which are created from remote git repository which doesn't contain any CodeReady Workspaces-specific workspace descriptor.

Environment Variable Name	Default value	Description
CHE_FACTORY_DEFAULT_PLUGINS	NULL	Plugins that will be used for factories which are created from remote git repository which doesn't contain any CodeReady Workspaces-specific workspace descriptor. Multiple plugins must be comma-separated, for example: pluginFooPublisher/pluginFooName/pluginFooVersion,pluginBarPublisher/pluginBarName/pluginBarVersion
CHE_FACTORY_DEFAULT_DEVFILE_FILENAMES	devfile.yaml, .devfile.yaml	Devfile filenames to look on repository-based factories (like GitHub etc). Factory will try to locate those files in the order they enumerated in the property.

4.1.2.10. Devfile defaults

Table 4.10. Devfile defaults

Environment Variable Name	Default value	Description
CHE_WORKSPACE_DEVFILE_DEFAULT_EDITOR	eclipse/che-theia/latest	Default Editor that should be provisioned into Devfile if there is no specified Editor Format is editorPublisher/editorName/editorVersion value. NULL or absence of value means that default editor should not be provisioned.

Environment Variable Name	Default value	Description
CHE_WORKSPACE_DEVFILE_DEFAULT_EDITOR_PLUGINS	NULL	Default Plugins which should be provisioned for Default Editor. All the plugins from this list that are not explicitly mentioned in the user-defined devfile will be provisioned but only when the default editor is used or if the user-defined editor is the same as the default one (even if in different version). Format is comma-separated pluginPublisher/pluginName/pluginVersion values, and URLs. For example: eclipse/che-theia-exec-plugin/0.0.1,eclipse/che-theia-terminal-plugin/0.0.1,https://cdn.pluginregistry.com/vi-mode/meta.yaml If the plugin is a URL, the plugin's meta.yaml is retrieved from that URL.
CHE_WORKSPACE_PROVISION_SECRET_LABELS	app.kubernetes.io/part-of=che.eclipse.org,app.kubernetes.io/component=workspace-secret	Defines comma-separated list of labels for selecting secrets from a user namespace, which will be mount into workspace containers as a files or env variables. Only secrets that match ALL given labels will be selected.
CHE_WORKSPACE_DEVFILE_ASYNC_STORAGE_PLUGIN	eclipse/che-async-pv-plugin/latest	Plugin is added in case async storage feature will be enabled in workspace config and supported by environment
CHE_INFRA_KUBERNETES_ASYNC_STORAGE_IMAGE	quay.io/eclipse/che-workspace-data-sync-storage:0.0.1	Docker image for the CodeReady Workspaces async storage
CHE_WORKSPACE_POD_NODE_SELECTOR	NULL	Optionally configures node selector for workspace pod. Format is comma-separated key=value pairs, e.g: disktype=ssd,cpu=xlarge,foo=bar

Environment Variable Name	Default value	Description
CHE_WORKSPACE_POD_TOLERATIONS_JSON	NULL	Optionally configures tolerations for workspace pod. Format is a string representing a JSON Array of taint tolerations, or NULL to disable it. The objects contained in the array have to follow this spec . Example: <pre>[{'effect':'NoExecute','key':'aNodeTaint','operator':'Equal','value':'aValue'}]</pre>
CHE_INFRA_KUBERNETES_ASYNC_STORAGE_SHUTDOWN_TIMEOUT_MIN	120	The timeout for the Asynchronous Storage Pod shutdown after stopping the last used workspace. Value less or equal to 0 interpreted as disabling shutdown ability.
CHE_INFRA_KUBERNETES_ASYNC_STORAGE_SHUTDOWN_CHECK_PERIOD_MIN	30	Defines the period with which the Asynchronous Storage Pod stopping ability will be performed (once in 30 minutes by default)
CHE_INTEGRATION_BITBUCKET_SERVER_ENDPOINTS	NULL	Bitbucket endpoints used for factory integrations. Comma separated list of bitbucket server URLs or NULL if no integration expected.
CHE_INTEGRATION_GITLAB_SERVER_ENDPOINTS	NULL#	Gitlab endpoints used for factory integrations. Comma separated list of Gitlab server URLs or NULL if no integration expected.

4.1.2.11. Che system

Table 4.11. Che system

Environment Variable Name	Default value	Description
---------------------------	---------------	-------------

Environment Variable Name	Default value	Description
CHE_SYSTEM_SUPER_PRIVILEGED_MODE	false	System Super Privileged Mode. Grants users with the manageSystem permission additional permissions for getByKey, getByNameSpace, stopWorkspaces, and getResourcesInformation. These are not given to admins by default and these permissions allow admins gain visibility to any workspace along with naming themselves with admin privileges to those workspaces.
CHE_SYSTEM_ADMIN_NAME	admin	Grant system permission for 'che.admin.name' user. If the user already exists it'll happen on component startup, if not - during the first login when user is persisted in the database.

4.1.2.12. Workspace limits

Table 4.12. Workspace limits

Environment Variable Name	Default value	Description
CHE_LIMITS_WORKSPACE_ENV_RAM	16gb	Workspaces are the fundamental runtime for users when doing development. You can set parameters that limit how workspaces are created and the resources that are consumed. The maximum amount of RAM that a user can allocate to a workspace when they create a new workspace. The RAM slider is adjusted to this maximum value.

Environment Variable Name	Default value	Description
CHE_LIMITS_WORKSPACE_IDLE_TIMEOUT	1800000	The length of time that a user is idle with their workspace when the system will suspend the workspace and then stopping it. Idleness is the length of time that the user has not interacted with the workspace, meaning that one of our agents has not received interaction. Leaving a browser window open counts toward idleness.
CHE_LIMITS_WORKSPACE_RUN_TIMEOUT	0	The length of time in milliseconds that a workspace will run, regardless of activity, before the system will suspend it. Set this property if you want to automatically stop workspaces after a period of time. The default is zero, meaning that there is no run timeout.

4.1.2.13. Users workspace limits

Table 4.13. Users workspace limits

Environment Variable Name	Default value	Description
CHE_LIMITS_USER_WORKSPACES_RAM	-1	The total amount of RAM that a single user is allowed to allocate to running workspaces. A user can allocate this RAM to a single workspace or spread it across multiple workspaces.
CHE_LIMITS_USER_WORKSPACES_COUNT	-1	The maximum number of workspaces that a user is allowed to create. The user will be presented with an error message if they try to create additional workspaces. This applies to the total number of both running and stopped workspaces.

Environment Variable Name	Default value	Description
CHE_LIMITS_USER_WORKSPACES_RUN_COUNT	1	The maximum number of running workspaces that a single user is allowed to have. If the user has reached this threshold and they try to start an additional workspace, they will be prompted with an error message. The user will need to stop a running workspace to activate another.

4.1.2.14. Organizations workspace limits

Table 4.14. Organizations workspace limits

Environment Variable Name	Default value	Description
CHE_LIMITS_ORGANIZATION_WORKSPACES_RAM	-1	The total amount of RAM that a single organization (team) is allowed to allocate to running workspaces. An organization owner can allocate this RAM however they see fit across the team's workspaces.
CHE_LIMITS_ORGANIZATION_WORKSPACES_COUNT	-1	The maximum number of workspaces that a organization is allowed to own. The organization will be presented an error message if they try to create additional workspaces. This applies to the total number of both running and stopped workspaces.
CHE_LIMITS_ORGANIZATION_WORKSPACES_RUN_COUNT	-1	The maximum number of running workspaces that a single organization is allowed. If the organization has reached this threshold and they try to start an additional workspace, they will be prompted with an error message. The organization will need to stop a running workspace to activate another.
CHE_MAIL_FROM_EMAIL_ADDRESS	che@noreply.com	Address that will be used as from email for email notifications

4.1.2.15. Organizations notifications settings

Table 4.15. Organizations notifications settings

Environment Variable Name	Default value	Description
CHE_ORGANIZATION_EMAIL_MEMBER_ADDED_SUBJECT	You've been added to a Che Organization	You've been added to a CodeReady Workspaces Organization organization notification subject.
CHE_ORGANIZATION_EMAIL_MEMBER_ADDED_TEMPLATE	st-html-templates/user_added_to_organization	You've been added to a CodeReady Workspaces Organization organization notification template.
CHE_ORGANIZATION_EMAIL_MEMBER_REMOVED_SUBJECT	You've been removed from a Che Organization	You've been removed from a CodeReady Workspaces Organization organization notification subject.
CHE_ORGANIZATION_EMAIL_MEMBER_REMOVED_TEMPLATE	st-html-templates/user_removed_from_organization	You've been removed from a CodeReady Workspaces Organization organization notification template.
CHE_ORGANIZATION_EMAIL_ORG_REMOVED_SUBJECT	CheOrganization deleted	CodeReady Workspaces Organization deleted organization notification subject.
CHE_ORGANIZATION_EMAIL_ORG_REMOVED_TEMPLATE	st-html-templates/organization_deleted	CodeReady Workspaces Organization deleted organization notification template.
CHE_ORGANIZATION_EMAIL_ORG_RENAMED_SUBJECT	CheOrganization renamed	CodeReady Workspaces Organization renamed organization notification subject.
CHE_ORGANIZATION_EMAIL_ORG_RENAMED_TEMPLATE	st-html-templates/organization_renamed	CodeReady Workspaces Organization renamed organization notification template.

4.1.2.16. Multi-user-specific OpenShift infrastructure configuration

Table 4.16. Multi-user-specific OpenShift infrastructure configuration

Environment Variable Name	Default value	Description
CHE_INFRA_OPENSHIFT_OAUTH_IDENTITY_PROVIDER	NULL	Alias of the Openshift identity provider registered in Keycloak, that should be used to create workspace OpenShift resources in Openshift namespaces owned by the current CodeReady Workspaces user. Should be set to NULL if che.infra.openshift.project is set to a non-empty value. For more information see the following documentation: https://www.keycloak.org/docs/latest/server_admin/index.html#openshift-4

4.1.2.17. Keycloak configuration

Table 4.17. Keycloak configuration

Environment Variable Name	Default value	Description
CHE_KEYCLOAK_AUTH_SERVER_URL	http://\${CHE_HOST}:5050/auth	Url to keycloak identity provider server Can be set to NULL only if che.keycloak.oidcProvider is used
CHE_KEYCLOAK_AUTH_INTERNAL_SERVER_URL	NULL	Internal network service Url to keycloak identity provider server
CHE_KEYCLOAK_REALM	che	Keycloak realm is used to authenticate users Can be set to NULL only if che.keycloak.oidcProvider is used
CHE_KEYCLOAK_CLIENT_ID	che-public	Keycloak client id in che.keycloak.realm that is used by dashboard, ide and cli to authenticate users
CHE_KEYCLOAK_OSO_ENDPOINT	NULL	URL to access OSO oauth tokens
CHE_KEYCLOAK_GITHUB_ENDPOINT	NULL	URL to access Github oauth tokens

Environment Variable Name	Default value	Description
CHE_KEYCLOAK_ALLOWED_CLOCK_SKEW_SEC	3	The number of seconds to tolerate for clock skew when verifying exp or nbf claims.
CHE_KEYCLOAK_USE_NONCE	true	Use the OIDC optional nonce feature to increase security.
CHE_KEYCLOAK_JS_ADAPTER_URL	NULL	URL to the Keycloak Javascript adapter we want to use. if set to NULL, then the default used value is <code>#{che.keycloak.auth_server_url}/js/keycloak.js</code> , or <code><che-server>/api/keycloak/OIDCKeycloak.js</code> if an alternate oidc_provider is used
CHE_KEYCLOAK_OIDC_PROVIDER	NULL	Base URL of an alternate OIDC provider that provides a discovery endpoint as detailed in the following specification https://openid.net/specs/openid-connect-discovery-1_0.html#ProviderConfig
CHE_KEYCLOAK_USE_FIXED_REDIRECT_URLS	false	Set to true when using an alternate OIDC provider that only supports fixed redirect Urls This property is ignored when che.keycloak.oidc_provider is NULL
CHE_KEYCLOAK_USERNAME_CLAIM	NULL	Username claim to be used as user display name when parsing JWT token if not defined the fallback value is 'preferred_username'

Environment Variable Name	Default value	Description
CHE_OAUTH_SERVICE_MODE	delegated	Configuration of OAuth Authentication Service that can be used in 'embedded' or 'delegated' mode. If set to 'embedded', then the service work as a wrapper to CodeReady Workspaces's OAuthAuthenticator (as in Single User mode). If set to 'delegated', then the service will use Keycloak IdentityProvider mechanism. Runtime Exception wii be thrown, in case if this property is not set properly.
CHE_KEYCLOAK_CASCADE_USER_REMOVAL_ENABLED	false	Configuration for enabling removing user from Keycloak server on removing user from CodeReady Workspaces database. By default it's disabled. Can be enabled in some special cases when deleting a user in CodeReady Workspaces database should execute removing related-user from Keycloak. For correct work need to set admin username <code>#{che.keycloak.admin_username}</code> and password <code>#{che.keycloak.admin_password}</code> .
CHE_KEYCLOAK_ADMIN_USERNAME	NULL	Keycloak admin username. Will be used for deleting user from Keycloak on removing user from CodeReady Workspaces database. Make sense only in case <code>#{che.keycloak.cascade_user_removal_enabled}</code> set to 'true'
CHE_KEYCLOAK_ADMIN_PASSWORD	NULL	Keycloak admin password. Will be used for deleting user from Keycloak on removing user from CodeReady Workspaces database. Make sense only in case <code>#{che.keycloak.cascade_user_removal_enabled}</code> set to 'true'

Environment Variable Name	Default value	Description
CHE_KEYCLOAK_USERNAME_REPLACEMENT_PATTERNS	NULL	User name adjustment configuration. CodeReady Workspaces needs to use the usernames as part of K8s object names and labels and therefore has stricter requirements on their format than the identity providers usually allow (it needs them to be DNS-compliant). The adjustment is represented by comma-separated key-value pairs. These are sequentially used as arguments to the <code>String.replaceAll</code> function on the original username. The keys are regular expressions, values are replacement strings that replace the characters in the username that match the regular expression. The modified username will only be stored in the CodeReady Workspaces database and will not be advertised back to the identity provider. It is recommended to use DNS-compliant characters as replacement strings (values in the key-value pairs). Example: <code>\\=-, @=-at-</code> changes <code>\</code> to <code>-</code> and <code>@</code> to <code>-at-</code> so the username <code>org\user@com</code> becomes <code>org-user-at-com</code> .

Additional resources

- [Configuring Che to use an external Keycloak installation](#)

4.2. CONFIGURING PROJECT STRATEGIES

The OpenShift project where a new workspace Pod is deployed depends on the CodeReady Workspaces server configuration. By default, every workspace is deployed in a distinct OpenShift project, but the user can configure the CodeReady Workspaces server to deploy all workspaces in one specific OpenShift project. The name of a OpenShift project must be provided as a CodeReady Workspaces server configuration property and cannot be changed at runtime.

With **Operator** installer, OpenShift project strategies are configured using **server.workspaceNamespaceDefault** property.

Operator CheCluster CR patch

```
apiVersion: org.eclipse.che/v1
kind: CheCluster
```

```

metadata:
  name: <che-cluster-name>
spec:
  server:
    workspaceNamespaceDefault: <workspace-namespace> 1

```

- 1** - CodeReady Workspaces workspace namespace configuration



NOTE

The underlying environment variable that CodeReady Workspaces server uses is **CHE_INFRA_KUBERNETES_NAMESPACE_DEFAULT**.



WARNING

CHE_INFRA_KUBERNETES_NAMESPACE and **CHE_INFRA_OPENSHIFT_PROJECT** are legacy variables. Keep these variables unset for a new installations. Changing these variables during an update can lead to data loss.



WARNING

By default, only one workspace in the same project can be running at one time. See [Section 4.5, "Running more than one workspace at a time"](#) .



WARNING

Kubernetes limits the length of a namespace name to 63 characters (this includes the evaluated placeholders). Additionally, the names (after placeholder evaluation) must be valid DNS names.

On OpenShift with multi-host server exposure strategy, the length is further limited to 49 characters.

Be aware that the **<userid>** placeholder is evaluated into a 36 character long UUID string.

**WARNING**

For strategies where creating new project is needed, make sure that **che** ServiceAccount has enough permissions to do so. With OpenShift OAuth, the authenticated User must have privileges to create new project.

4.2.1. One project per user strategy

The strategy isolates each user in their own project.

To use the strategy, set the *CodeReady Workspaces workspace namespace configuration* value to contain one or more user identifiers. Currently supported identifiers are **<username>** and **<userid>**.

Example 4.2. One project per user

To assign project names composed of a ``codeready-ws`` prefix and individual usernames (**`codeready-ws-user1`**, **`codeready-ws-user2`**), set:

Operator installer (CheCluster CustomResource)

```
...
spec:
  server:
    workspaceNamespaceDefault: codeready-ws-<username>
...
```

4.2.2. One project per workspace strategy

The strategy creates a new project for each new workspace.

To use the strategy, set the *CodeReady Workspaces workspace namespace configuration* value to contain the **<workspaceID>** identifier. It can be used alone or combined with other identifiers or any string.

Example 4.3. One project per workspace

To assign project names composed of a ``codeready-ws`` prefix and workspace id, set:

Operator installer (CheCluster CustomResource)

```
...
spec:
  server:
    workspaceNamespaceDefault: codeready-ws-<workspaceID>
...
```

4.2.3. One project for all workspaces strategy

The strategy uses one predefined project for all workspaces.

To use the strategy, set the *CodeReady Workspaces workspace namespace configuration* value to the name of the desired project to use.

Example 4.4. One project for all workspaces

To have all workspaces created in `codeready-ws` project, set:`

Operator installer (CheCluster CustomResource)

```
...
spec:
  server:
    workspaceNamespaceDefault: codeready-ws
...
```

4.2.4. Allowing user-defined workspace projects

CodeReady Workspaces server can be configured to honor the user selection of a project when a workspace is created. This feature is disabled by default. To allow user-defined workspace projects:

- For Operator deployments, set the following field in the CheCluster Custom Resource:

```
...
server:
  allowUserDefinedWorkspaceNamespaces: true
...
```

4.2.5. Handling incompatible usernames or user IDs

CodeReady Workspaces server automatically checks usernames and IDs for compatibility with Kubernetes objects naming convention before creating a project from a template. Incompatible username or IDs are reduced to the nearest valid name by replacing groups of unsuitable symbols with the `-` symbol. To avoid collisions, a random 6-symbol suffix is added and the result is stored in preferences for reuse.

4.2.6. Pre-creating projects for users

To pre-create projects for users, use project labels and annotations. Such namespace is used in preference to **CHE_INFRA_KUBERNETES_NAMESPACE_DEFAULT** variable.

```
metadata:
  labels:
    app.kubernetes.io/part-of: che.eclipse.org
    app.kubernetes.io/component: workspaces-namespace
  annotations:
    che.eclipse.org/username: <username> 1
```

- 1 target user's username

To configure the labels, set the **CHE_INFRA_KUBERNETES_NAMESPACE_LABELS** to desired labels. To configure the annotations, set the **CHE_INFRA_KUBERNETES_NAMESPACE_ANNOTATIONS** to desired annotations. See the [CodeReady Workspaces server component system properties reference](#) for more details.



WARNING

Avoid creating multiple namespaces for single user. It may lead to undefined behavior.

IMPORTANT

On OpenShift with OAuth, target user must have **admin** role privileges in target namespace:

```
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: admin
  namespace: <namespace> 1
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: admin
subjects:
- apiGroup: rbac.authorization.k8s.io
  kind: User
  name: <username> 2
```

- 1 pre-created namespace
- 2 target user

On Kubernetes, **che** ServiceAccount must have a cluster-wide **list** and **get namespaces** permissions as well as an **admin** role in target namespace.

4.2.7. Labeling the namespaces

CodeReady Workspaces updates the workspace's namespace on workspace startup by adding the labels defined in **CHE_INFRA_KUBERNETES_NAMESPACE_LABELS**. To do so, **che** ServiceAccount has to have the following cluster-wide permissions to **update** and **get namespaces**:

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: <cluster-role-name> 1
rules:
- apiGroups:
  - ""
  resources:
```

```

- namespaces
verbs:
- update
- get

```

1 name of the cluster role

```

apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: <cluster-role-binding-name> 1
subjects:
  - kind: ServiceAccount
    name: <service-account-name> 2
    namespace: <service-account-namespace> 3
roleRef:
  kind: ClusterRole
  name: <cluster-role-name> 4
  apiGroup: rbac.authorization.k8s.io

```

1 name of the cluster role binding

2 name of the che service account

3 CodeReady Workspaces installation namespace

4 name of the cluster role created in previous step



NOTE

CodeReady Workspaces does not fail to start a workspace for lack of permissions, it only logs the warning. If you see the warnings in CodeReady Workspaces logs, consider disabling the feature with setting

CHE_INFRA_KUBERNETES_NAMESPACE_LABEL=false.

4.3. CONFIGURING STORAGE STRATEGIES

This section describes how to configure storage strategies for CodeReady Workspaces workspaces.

4.3.1. Storage strategies for codeready-workspaces workspaces

Workspace Pods use Persistent Volume Claims (PVCs), which are bound to the physical Persistent Volumes (PVs) with [ReadWriteOnce access mode](#). It is possible to configure how the CodeReady Workspaces server uses PVCs for workspaces. The individual methods for this configuration are called PVC strategies:

strategy	details	pros	cons
unique	One PVC per workspace volume or user-defined PVC	Storage isolation	An undefined number of PVs is required

strategy	details	pros	cons
per-workspace (default)	One PVC for one workspace	Easier to manage and control storage compared to unique strategy	PV count still is not known and depends on workspaces number
common	One PVC for all workspaces in one OpenShift namespace	Easy to manage and control storage	<p>If PV does not support ReadWriteMany (RWX) access mode then workspaces must be in a separate OpenShift namespaces</p> <p>Or there must not be more than 1 running workspace per namespace at the same time</p>

Red Hat CodeReady Workspaces uses the **common** PVC strategy in combination with the "one project per user" project strategy when all CodeReady Workspaces workspaces operate in the user's project, sharing one PVC.

4.3.1.1. The common PVC strategy

All workspaces inside a OpenShift project use the same Persistent Volume Claim (PVC) as the default data storage when storing data such as the following in their declared volumes:

- projects
- workspace logs
- additional Volumes defined by a use

When the **common** PVC strategy is in use, user-defined PVCs are ignored and volumes that relate to these user-defined PVCs are replaced with a volume that refers to the common PVC. In this strategy, all CodeReady Workspaces workspaces use the same PVC. When the user runs one workspace, it only binds to one node in the cluster at a time.

The corresponding containers volume mounts link to a common volume, and sub-paths are prefixed with **<workspace-ID>** or **<original-PVC-name>**. For more details, see [Section 4.3.1.4, "How subpaths are used in PVCs"](#).

The CodeReady Workspaces Volume name is identical to the name of the user-defined PVC. It means that if a machine is configured to use a CodeReady Workspaces volume with the same name as the user-defined PVC has, they will use the same shared folder in the common PVC.

When a workspace is deleted, a corresponding subdirectory (**/\${ws-id}**) is deleted in the PV directory.

Restrictions on using the common PVC strategy

When the **common** strategy is used and a workspace PVC access mode is ReadWriteOnce (RWO), only one node can simultaneously use the PVC.

If there are several nodes, you can use the **common** strategy, but:

- The workspace PVC access mode must be reconfigured to **ReadWriteMany** (RWM), so multiple nodes can use this PVC simultaneously.
- Only one workspace in the same project may be running. See [Section 4.5, “Running more than one workspace at a time”](#).

The **common** PVC strategy is not suitable for large multi-node clusters. Therefore, it is best to use it in single-node clusters. However, in combination with the **per-workspace** project strategy, the **common** PVC strategy is usable for clusters with not more than 75 nodes. The PVC used with this strategy must be large enough to accommodate all projects to prevent a situation in which one project depletes the resources of others.

4.3.1.2. The per-workspace PVC strategy

The **per-workspace** strategy is similar to the **common** PVC strategy. The only difference is that all workspace Volumes, but not all the workspaces, use the same PVC as the default data storage for:

- projects
- workspace logs
- additional Volumes defined by a user

With this strategy, CodeReady Workspaces keeps its workspace data in assigned PVs that are allocated by a single PVC.

The **per-workspace** PVC strategy is the most universal strategy out of the PVC strategies available and acts as a proper option for large multi-node clusters with a higher amount of users. Using the **per-workspace** PVC strategy, users can run multiple workspaces simultaneously, results in more PVCs being created.

4.3.1.3. The unique PVC strategy

When using the `unique` PVC strategy, every CodeReady Workspaces Volume of a workspace has its own PVC. This means that workspace PVCs are:

Created when a workspace starts for the first time. Deleted when a corresponding workspace is deleted.

User-defined PVCs are created with the following specifics:

- They are provisioned with generated names to prevent naming conflicts with other PVCs in a project.
- Subpaths of the mounted Physical persistent volumes that reference user-defined PVCs are prefixed with `<workspace-ID>` or `<PVC-name>`. This ensures that the same PV data structure is configured with different PVC strategies. For details, see [Section 4.3.1.4, “How subpaths are used in PVCs”](#).

The **unique** PVC strategy is suitable for larger multi-node clusters with a lesser amount of users. Since this strategy operates with separate PVCs for each volume in a workspace, vastly more PVCs are created.

4.3.1.4. How subpaths are used in PVCs

Subpaths illustrate the folder hierarchy in the Persistent Volumes (PV).

```

/pv0001
  /workspaceID1
  /workspaceID2
  /workspaceIDn
  /che-logs
  /projects
  /<volume1>
  /<volume2>
  /<User-defined PVC name 1 | volume 3>
  ...

```

When a user defines volumes for components in the devfile, all components that define the volume of the same name will be backed by the same directory in the PV as **<PV-name>**, **<workspace-ID>**, or **<original-PVC-name>**. Each component can have this location mounted on a different path in its containers.

Example

Using the **common** PVC strategy, user-defined PVCs are replaced with subpaths on the common PVC. When the user references a volume as **my-volume**, it is mounted in the common-pvc with the **/workspace-id/my-volume** subpath.

4.3.2. Configuring a CodeReady Workspaces workspace with a persistent volume strategy

A persistent volume (PV) acts as a virtual storage instance that adds a volume to a cluster.

A persistent volume claim (PVC) is a request to provision persistent storage of a specific type and configuration, available in the following CodeReady Workspaces storage configuration strategies:

- Common
- Per-workspace
- Unique

The mounted PVC is displayed as a folder in a container file system.

4.3.2.1. Configuring a PVC strategy using the Operator

The following section describes how to configure workspace persistent volume claim (PVC) strategies of a CodeReady Workspaces server using the Operator.



WARNING

It is not recommended to reconfigure PVC strategies on an existing CodeReady Workspaces cluster with existing workspaces. Doing so causes data loss.

Operators are software extensions to OpenShift that use [Custom Resources](#) to manage applications and their components.

When deploying CodeReady Workspaces using the Operator, configure the intended strategy by modifying the **spec.storage.pvcStrategy** property of the CheCluster Custom Resource object YAML file.

Prerequisites

- The **oc** tool is available.

Procedure

The following procedure steps are available for OpenShift command-line tool, `'oc'`.

To do changes to the CheCluster YAML file, choose one of the following:

- Create a new cluster by executing the **oc apply** command. For example:

```
$ oc apply -f <my-cluster.yaml>
```

- Update the YAML file properties of an already running cluster by executing the **oc patch** command. For example:

```
$ oc patch checluster codeready-workspaces --type=json \
-p '[{"op": "replace", "path": "/spec/storage/pvcStrategy", "value": "per-workspace"}]'
```

Depending on the strategy used, replace the **per-workspace** option in the above example with **unique** or **common**.

4.4. CONFIGURING STORAGE TYPES

Red Hat CodeReady Workspaces supports three types of storage with different capabilities:

- Persistent
- Ephemeral
- Asynchronous

4.4.1. Persistent storage

Persistent storage allows storing user changes directly in the mounted Persistent Volume. User changes are kept safe by the OpenShift infrastructure (storage backend) at the cost of slow I/O, especially with many small files. For example, Node.js projects tend to have many dependencies and the **node_modules/** directory is filled with thousands of small files.



NOTE

I/O speeds vary depending on the [Storage Classes](#) configured in the environment.

Persistent storage is the default mode for new workspaces. To make this setting visible in workspace configuration, add the following to the devfile:

```
attributes:
  persistVolumes: 'true'
```

4.4.2. Ephemeral storage

Ephemeral storage saves files to the **emptyDir** volume. This volume is initially empty. When a Pod is removed from a node, the data in the **emptyDir** volume is deleted forever. This means that all changes are lost on workspace stop or restart.



IMPORTANT

To save the changes, commit and push to the remote before stopping an ephemeral workspace.

Ephemeral mode provides faster I/O than persistent storage. To enable this storage type, add the following to workspace configuration:

```
attributes:
  persistVolumes: 'false'
```

Table 4.18. Comparison between I/O of ephemeral (**emptyDir**) and persistent modes on [AWS EBS](#)

Command	Ephemeral	Persistent
Clone Red Hat CodeReady Workspaces	0 m 19 s	1 m 26 s
Generate 1000 random files	1 m 12 s	44 m 53 s

4.4.3. Asynchronous storage



NOTE

Asynchronous storage is an experimental feature.

Asynchronous storage is a combination of persistent and ephemeral modes. The initial workspace container mounts the **emptyDir** volume. Then a backup is performed on workspace stop, and changes are restored on workspace start. Asynchronous storage provides fast I/O (similar to ephemeral mode), and workspace project changes are persisted.

Synchronization is performed by the **rsync** tool using the [SSH](#) protocol. When a workspace is configured with asynchronous storage, the **workspace-data-sync** plug-in is automatically added to the workspace configuration. The plug-in runs the **rsync** command on workspace start to restore changes. When a workspace is stopped, it sends changes to the permanent storage.

For relatively small projects, the restore procedure is fast, and project source files are immediately available after Che-Theia is initialized. In case **rsync** takes longer, the synchronization process is shown in the Che-Theia status-bar area. ([Extension in Che-Theia repository](#)).



NOTE

Asynchronous mode has the following limitations:

- Supports only the *common* PVC strategy
- Supports only the *per-user* project strategy
- Only one workspace can be running at a time

To configure asynchronous storage for a workspace, add the following to workspace configuration:

```
attributes:
  asyncPersist: 'true'
  persistVolumes: 'false'
```

4.4.4. Configuring storage type defaults for CodeReady Workspaces dashboard

Use the following two **che.properties** to configure the default client values in CodeReady Workspaces dashboard:

che.workspace.storage.available_types

Defines available values for storage types that clients like the dashboard propose for users during workspace creation or update. Available values: **persistent**, **ephemeral**, and **async**. Separate multiple values by commas. For example:

```
che.workspace.storage.available_types=persistent,ephemeral,async
```

che.workspace.storage.preferred_type

Defines the default value for storage type that clients like the dashboard propose for users during workspace creation. The **async** value is not recommended as the default type because it is experimental. For example:

```
che.workspace.storage.preferred_type=persistent
```

Then users are able to configure Storage Type on the **Create Custom Workspace** tab on CodeReady Workspaces dashboard during workspace creation. Storage type for existing workspace can be configured in on **Overview** tab of the workspace details.

4.4.5. Idling asynchronous storage Pods

CodeReady Workspaces can shut down the Asynchronous Storage Pod when not used for a configured period of time.

Use these configuration properties to adjust the behavior:

che.infra.kubernetes.async.storage.shutdown_timeout_min

Defines the idle time after which the asynchronous storage Pod is stopped following the stopping of the last active workspace. The default value is 120 minutes.

che.infra.kubernetes.async.storage.shutdown_check_period_min

Defines the frequency with which the asynchronous storage Pod is checked for idleness. The default value is 30 minutes.

4.5. RUNNING MORE THAN ONE WORKSPACE AT A TIME

This procedure describes how to run more than one workspace simultaneously. This makes it possible for multiple workspace contexts per user to run in parallel.

Prerequisites

- The `oc` tool is available.
- An instance of CodeReady Workspaces running in OpenShift.



NOTE

The following commands use the default OpenShift project, **openshift-workspaces**, as a user's example for the `-n` option.

Procedure

1. Set the **per-workspace** or **unique** PVC strategy if the underlying storage backend does not support or not configured to use the **ReadWriteMany** access mode. See [Section 4.3, "Configuring storage strategies"](#).



IMPORTANT

The default **common** PVC strategy, which uses a single PVC per user, supports running multiple workspaces simultaneously only if the persistent volumes on the cluster are configured to use the **ReadWriteMany** access mode. That way, any of the user's concurrent workspaces can read from and write to the common PVC. In some cases, configuring **ReadWriteMany** is not possible due to the storage limitations, for example, [EBS](#) only supports **ReadWriteOnce** access mode.

2. Change the default limit of **1** to **-1** to allow an unlimited number of concurrent workspaces, or to the precise value, for example, **10** to allow running **10** concurrent workspaces per user simultaneously:

```
$ oc patch checluster codeready-workspaces -n openshift-workspaces --type merge \
-p '{ "spec": { "server": {"customCheProperties":
{"CHE_LIMITS_USER_WORKSPACES_RUN_COUNT": "-1"} } } }
```

4.6. CONFIGURING WORKSPACE EXPOSURE STRATEGIES

The following section describes how to configure workspace exposure strategies of a CodeReady Workspaces server and ensure that applications running inside are not vulnerable to outside attacks.

4.6.1. Configuring workspace exposure strategies using an Operator

[Operators](#) are software extensions to OpenShift that use [Custom Resources](#) to manage applications and their components.

Prerequisites

- The **oc** tool is available.

Procedure

When deploying CodeReady Workspaces using the Operator, configure the intended strategy by modifying the **spec.server.serverExposureStrategy** property of the CheCluster Custom Resource object YAML file.

The supported values for **spec.server.serverExposureStrategy** are:

- **multi-host**
- **single-host**

See [Section 4.6.2, “Workspace exposure strategies”](#) for more detail about individual strategies.

To activate changes done to CheCluster YAML file, do one of the following:

- Create a new cluster by executing the **crwctl** command with applying a patch. For example:

```
$ crwctl server:deploy --installer=operator --platform=<platform> \
  --che-operator-cr-patch-yaml=patch.yaml
```



NOTE

For a list of available OpenShift deployment platforms, use **crwctl server:deploy --platform --help**.

- Use the following **patch.yaml** file:

```
apiVersion: org.eclipse.che/v1
kind: CheCluster
metadata:
  name: eclipse-che
spec:
  server:
    serverExposureStrategy: '<exposure-strategy>' 1
```

- 1** - used workspace exposure strategy

- Update the YAML file properties of an already running cluster by executing the **oc patch** command. For example:

```
$ oc patch checluster codeready-workspaces --type=json \
  -p '[{"op": "replace",
  "path": "/spec/server/serverExposureStrategy",
```

```
"value": "<exposure-strategy>"}] \ 1  
-n openshift-workspaces
```

1 - used workspace exposure strategy

4.6.2. Workspace exposure strategies

Specific components of workspaces need to be made accessible outside of the OpenShift cluster. This is typically the user interface of the workspace's IDE, but it can also be the web UI of the application being developed. This enables developers to interact with the application during the development process.

The supported way of making workspace components available to the users is referred to as a *strategy*. This strategy defines whether new subdomains are created for the workspace components and what hosts these components are available on.

CodeReady Workspaces supports:

- **multi-host** strategy
- **single-host** strategy
 - with the **gateway** subtype

4.6.2.1. Multi-host strategy

With multi-host strategy, each workspace component is assigned a new subdomain of the main domain configured for the CodeReady Workspaces server. This is the default strategy.

This strategy is the easiest to understand from the perspective of component deployment because any paths present in the URL to the component are received as they are by the component.

On a CodeReady Workspaces server secured using the Transport Layer Security (TLS) protocol, creating new subdomains for each component of each workspace requires a wildcard certificate to be available for all such subdomains for the CodeReady Workspaces deployment to be practical.

4.6.2.2. Single-host strategy

With single-host strategy, all workspaces are deployed to sub-paths of the main CodeReady Workspaces server domain.

This is convenient for TLS-secured CodeReady Workspaces servers because it is sufficient to have a single certificate for the CodeReady Workspaces server, which will cover all the workspace component deployments as well.

Single-host strategy have two subtypes with different implementation methods. First subtype is named **native**. This strategy is available and default on Kubernetes, but not on OpenShift, since it uses Ingresses for servers exposing. The second subtype named **gateway**, works both on OpenShift, and uses a special Pod with reverse-proxy running inside to route requests.



WARNING

With **gateway** single-host strategy, cluster network policies has to be configured so that workspace's services are reachable from reverse-proxy Pod (typically in CodeReady Workspaces project). These typically lives in different project.

To define how to expose the endpoints specified in the devfile, define the **CHE_INFRA_KUBERNETES_SINGLEHOST_WORKSPACE_DEVFILE__ENDPOINT__EXPOSURE** environment variable in the CodeReady Workspaces instance. This environment variable is only effective with the single-host server strategy and is applicable to all workspaces of all users.

4.6.2.2.1. devfile endpoints: single-host

CHE_INFRA_KUBERNETES_SINGLEHOST_WORKSPACE_DEVFILE__ENDPOINT__EXPOSURE: 'single-host'

This single-host configuration exposes the endpoints on subpaths, for example: **https://<che-host>/serverihzmuqqc/go-cli-server-8080**. This limits the exposed components and user applications. Any absolute URL generated on the server side that points back to the server does not work. This is because the server is hidden behind a path-rewriting reverse proxy that hides the unique URL path prefix from the component or user application.

For example, when the user accesses the hypothetical **https://codeready-<openshift_deployment_name>.<domain_name>/component-prefix-djh3d/app/index.php** URL, the application sees the request coming to **https://internal-host/app/index.php**. If the application used the host in the URL that it generates in its UI, it would not work because the internal host is different from the externally visible host. However, if the application used an absolute path as the URL (for the example above, this would be **/app/index.php**), such URL would still not work. This is because on the outside, such URL does not point to the application, because it is missing the component-specific prefix.

Therefore, only applications that use relative URLs in their UI work with the single-host workspace exposure strategy.

4.6.2.2.2. devfile endpoints: multi-host

CHE_INFRA_KUBERNETES_SINGLEHOST_WORKSPACE_DEVFILE__ENDPOINT__EXPOSURE: 'multi-host'

This single-host configuration exposes the endpoints on subdomains, for example: **http://serverihzmuqqc-go-cli-server-8080.<che-host>**. These endpoints are exposed on an unsecured HTTP port. A dedicated Ingress or Route is used for such endpoints, even with **gateway** single-host setup.

This configuration limits the usability of previews shown directly in the editor page when CodeReady Workspaces is configured with TLS. Since **https** pages allow communication only with secured endpoints, users must open their application previews in another browser tab.

4.6.3. Security considerations

This section explains the security impact of using different CodeReady Workspaces workspace exposure strategies.

All the security-related considerations in this section are only applicable to CodeReady Workspaces in multiuser mode. The single user mode does not impose any security restrictions.

4.6.3.1. JSON web token (JWT) proxy

All CodeReady Workspaces plug-ins, editors, and components can require authentication of the user accessing them. This authentication is performed using a JSON web token (JWT) proxy that functions as a reverse proxy of the corresponding component, based on its configuration, and performs the authentication on behalf of the component.

The authentication uses a redirect to a special page on the CodeReady Workspaces server that propagates the workspace and user-specific authentication token (workspace access token) back to the originally requested page.

The JWT proxy accepts the workspace access token from the following places in the incoming requests, in the following order:

1. The token query parameter
2. The Authorization header in the bearer-token format
3. The **access_token** cookie

4.6.3.2. Secured plug-ins and editors

CodeReady Workspaces users do not need to secure workspace plug-ins and workspace editors (such as Che-Theia). This is because the JWT proxy authentication is indiscernible to the user and is governed by the plug-in or editor definition in their **meta.yaml** descriptors.

4.6.3.3. Secured container-image components

Container-image components can define custom endpoints for which the devfile author can require CodeReady Workspaces-provided authentication, if needed. This authentication is configured using two optional attributes of the endpoint:

- **secure** - A boolean attribute that instructs the CodeReady Workspaces server to put the JWT proxy in front of the endpoint. Such endpoints have to be provided with the workspace access token in one of the several ways explained in [Section 4.6.3.1, "JSON web token \(JWT\) proxy"](#). The default value of the attribute is **false**.
- **cookiesAuthEnabled** - A boolean attribute that instructs the CodeReady Workspaces server to automatically redirect the unauthenticated requests for current user authentication as described in [Section 4.6.3.1, "JSON web token \(JWT\) proxy"](#). Setting this attribute to **true** has security consequences because it makes Cross-site request forgery (CSRF) attacks possible. The default value of the attribute is **false**.

4.6.3.4. Cross-site request forgery attacks

Cookie-based authentication can make an application secured by a JWT proxy prone to Cross-site request forgery (CSRF) attacks. See the [Cross-site request forgery](#) Wikipedia page and other resources to ensure your application is not vulnerable.

4.6.3.5. Phishing attacks

An attacker who is able to create an Ingress or route inside the cluster with the workspace that shares

the host with some services behind a JWT proxy, the attacker may be able to create a service and a specially forged Ingress object. When such a service or Ingress is accessed by a legitimate user that was previously authenticated with a workspace, it can lead to the attacker stealing the workspace access token from the cookies sent by the legitimate user's browser to the forged URL. To eliminate this attack vector, configure OpenShift to disallow setting the host of an Ingress.

4.7. CONFIGURING WORKSPACES NODESELECTOR

This section describes how to configure **nodeSelector** for Pods of CodeReady Workspaces workspaces.

Procedure

CodeReady Workspaces uses the **CHE_WORKSPACE_POD_NODE_SELECTOR** environment variable to configure **nodeSelector**. This variable may contain a set of comma-separated **key=value** pairs to form the nodeSelector rule, or **NULL** to disable it.

```
CHE_WORKSPACE_POD_NODE_SELECTOR=disktype=ssd,cpu=xlarge,[key=value]
```

IMPORTANT

nodeSelector must be configured during CodeReady Workspaces installation. This prevents existing workspaces from failing to run due to volumes affinity conflict caused by existing workspace PVC and Pod being scheduled in different zones.

To avoid Pods and PVCs to be scheduled in different zones on large, multi-zone clusters, create an additional **StorageClass** object (pay attention to the **allowedTopologies** field), which will coordinate the PVC creation process.

Pass the name of this newly created **StorageClass** to CodeReady Workspaces through the **CHE_INFRA_KUBERNETES_PVC_STORAGE_CLASS_NAME** environment variable. A default empty value of this variable instructs CodeReady Workspaces to use the cluster's default **StorageClass**.

4.8. CONFIGURING RED HAT CODEREADY WORKSPACES SERVER HOSTNAME

This procedure describes how to configure Red Hat CodeReady Workspaces to use custom hostname.

Prerequisites

- The **oc** tool is available.
- The certificate and the private key files are generated.

IMPORTANT

To generate the pair of private key and certificate the same CA must be used as for other Red Hat CodeReady Workspaces hosts.

IMPORTANT

Ask a DNS provider to point the custom hostname to the cluster ingress.

Procedure

1. Pre-create a project for CodeReady Workspaces:

```
$ oc create project openshift-workspaces
```

2. Create a TLS secret:

```
$ oc create secret TLS ${secret} \ 1
--key ${key_file} \ 2
--cert ${cert_file} \ 3
-n openshift-workspaces
```

- 1 The TLS secret name
- 2 A file with the private key
- 3 A file with the certificate

3. Set the following values in the Custom Resource:

```
spec:
  server:
    cheHost: <hostname> 1
    cheHostTLSecret: <secret> 2
```

- 1 Custom Red Hat CodeReady Workspaces server hostname
- 2 The TLS secret name

1. If CodeReady Workspaces has been already deployed and CodeReady Workspaces reconfiguring to use a new CodeReady Workspaces hostname is required, log in using RH-SSO and select the **codeready-public** client in the **CodeReady Workspaces** realm and update **Validate Redirect URIs** and **Web Origins** fields with the value of the CodeReady Workspaces hostname.

* Valid Redirect URIs ⓘ	https://<hostname>/*	-
	http://<hostname>/*	-
		+
Base URL ⓘ	<input type="text"/>	
Admin URL ⓘ	<input type="text"/>	
Web Origins ⓘ	https://<hostname>	-
	http://<hostname>	-
		+

For logging in to RH-SSO, follow the [Logging in to RH-SSO](#) procedure.

4.9. CONFIGURING LABELS FOR OPENSIFT ROUTE

This procedure describes how to configure labels for OpenShift Route to organize and categorize (scope and select) objects.

Prerequisites

- The **oc** tool is available.
- An instance of CodeReady Workspaces running in OpenShift.



IMPORTANT

Use comma to separate labels: **key1=value1,key2=value2**

Procedure

1. To configure labels for OpenShift Route, update the Custom Resource with the following commands:

```
$ oc patch checluster codeready-workspaces -n openshift-workspaces --type=json -p \
'{"op": "replace", "path": "/spec/server/cheServerIngress/labels", \
"value": "<labels for a codeready-workspaces server ingress>"}'
```

```
$ oc patch checluster codeready-workspaces -n openshift-workspaces --type=json -p \
'{"op": "replace", "path": "/spec/auth/identityProviderIngress/labels", \
"value": "<labels for a RH-SSO ingress>"}'
```

```
$ oc patch checluster codeready-workspaces -n openshift-workspaces --type=json -p \
'{"op": "replace", "path": "/spec/server/pluginRegistryIngress/labels", \
"value": "<labels for a plugin registry ingress>"}'
```

```
$ oc patch checluster codeready-workspaces -n openshift-workspaces --type=json -p \
'{"op": "replace", "path": "/spec/server/devfileRegistryIngress/labels", \
"value": "<labels for a devfile registry ingress>"}'
```

4.10. CONFIGURING LABELS AND DOMAINS FOR OPENSIFT ROUTE TO WORK WITH ROUTER SHARDING

This procedure describes how to configure labels and domains for OpenShift Route to work with [Router Sharding](#) and mentions how to do so on existing instances or those about to be installed.

Prerequisites

- The **oc** and **crwctl** tool is available.

Procedure

- For a new OperatorHub installation:
 1. Enter the Red Hat CodeReady Workspaces Cluster using OpenShift Container Platform and create CheCluster Custom Resource (CR). See, [Creating an instance of the Red Hat CodeReady Workspaces Operator](#)
 2. Set the following values in codeready-workspaces Custom Resource (CR):

```
spec:
  server:
    devfileRegistryRoute:
```

```

labels: <labels> 1
domain: <domain> 2
pluginRegistryRoute:
  labels: <labels> 3
  domain: <domain> 4
cheServerRoute:
  labels: <labels> 5
  domain: <domain> 6
customCheProperties:
  CHE_INFRA_OPENSHIFT_ROUTE_LABELS: <labels> 7
  CHE_INFRA_OPENSHIFT_ROUTE_HOST_DOMAIN_SUFFIX: <domain> 8
auth:
  identityProviderRoute:
    labels: <labels> 9
    domain: <domain> 10

```

1 3 5 7 9 comma separated list of labels that are used by the target ingress controller to filter the set of Routes to service

2 4 6 8 10 DNS name serviced by the target ingress controller

- For a new **crwctl** installation:

1. Configure the the **crwctl** installation using:

```
$ crwctl server:deploy --che-operator-cr-patch-yaml=patch.yaml ...
```

patch.yaml must contain the following:

```

spec:
  server:
    devfileRegistryRoute:
      labels: <labels> 1
      domain: <domain> 2
    pluginRegistryRoute:
      labels: <labels> 3
      domain: <domain> 4
    cheServerRoute:
      labels: <labels> 5
      domain: <domain> 6
    customCheProperties:
      CHE_INFRA_OPENSHIFT_ROUTE_LABELS: <labels> 7
      CHE_INFRA_OPENSHIFT_ROUTE_HOST_DOMAIN_SUFFIX: <domain> 8
  auth:
    identityProviderRoute:
      labels: <labels> 9
      domain: <domain> 10

```

1 3 5 7 9 comma separated list of labels that are used by the target ingress controller to filter the set of Routes to service

2 4 6 8 10 DNS name serviced by the target ingress controller

- For already existing CodeReady Workspaces installation:

1. Update **codeready-workspaces** CR using the **oc** tool:

```
$ oc patch checluster codeready-workspaces -n openshift-workspaces --type=json -p \
'{"op": "replace", "path": "/spec/server/cheServerRoute/labels", \
"value": "<labels for a codeready-workspaces server route>"}'
```

```
$ oc patch checluster codeready-workspaces -n openshift-workspaces --type=json -p \
'{"op": "replace", "path": "/spec/server/cheServerRoute/domain", \
"value": "<ingress domain>"}'
```

```
$ oc patch checluster codeready-workspaces -n openshift-workspaces --type=json -p \
'{"op": "replace", "path": "/spec/server/pluginRegistryRoute/labels", \
"value": "<labels for a plugin registry route>"}'
```

```
$ oc patch checluster codeready-workspaces -n openshift-workspaces --type=json -p \
'{"op": "replace", "path": "/spec/auth/identityProviderRoute/domain", \
"value": "<ingress domain>"}'
```

```
$ oc patch checluster codeready-workspaces -n openshift-workspaces --type=json -p \
'{"op": "replace", "path": "/spec/server/pluginRegistryRoute/domain", \
"value": "<ingress domain>"}'
```

```
$ oc patch checluster codeready-workspaces -n openshift-workspaces --type=json -p \
'{"op": "replace", "path": "/spec/server/devfileRegistryRoute/labels", \
"value": "<labels for a devfile registry route>"}'
```

```
$ oc patch checluster codeready-workspaces -n openshift-workspaces --type=json -p \
'{"op": "replace", "path": "/spec/server/devfileRegistryRoute/domain", \
"value": "<ingress domain>"}'
```

```
$ oc patch checluster codeready-workspaces -n openshift-workspaces --type=json -p \
'{"op": "replace", "path": \
"/spec/server/customCheProperties/CHE_INFRA_OPENSHIFT_ROUTE_LABELS", \
"value": "<labels for a workspace routes>"}'
```

```
$ oc patch checluster codeready-workspaces -n openshift-workspaces --type=json -p \
'{"op": "replace", "path": \
"/spec/server/customCheProperties/CHE_INFRA_OPENSHIFT_ROUTE_HOST_DOMAI \
N_SUFFIX", \
"value": "<ingress domain>"}'
```

4.11. DEPLOYING CODEREADY WORKSPACES WITH SUPPORT FOR GIT REPOSITORIES WITH SELF-SIGNED CERTIFICATES

This procedure describes how to configure CodeReady Workspaces for deployment with support for Git operations on repositories that use self-signed certificates.

Prerequisites

- Git version 2 or later

Procedure

Configuring support for self-signed Git repositories.

1. Create a new **ConfigMap** with details about the Git server:

```
$ oc create configmap che-git-self-signed-cert --from-file=ca.crt \
  --from-literal=githost=<host:port> -n {prod-namespace}
```

In the command, substitute **<host:port>** for the host and port of the HTTPS connection on the Git server (optional).



NOTE

- When **githost** is not specified, the given certificate is used for all HTTPS repositories.
- The certificate file must be named **ca.crt**.
- Certificate files are typically stored as Base64 ASCII files, such as **.pem**, **.crt**, **.ca-bundle**. Also, they can be encoded as binary data, for example, **.cer**. All **Secrets** that hold certificate files should use the Base64 ASCII certificate rather than the binary data certificate.

2. Configure the workspace exposure strategy:

Update the **gitSelfSignedCert** property. To do that, execute:

```
$ oc patch checluster codeready-workspaces -n openshift-workspaces --type=json \
  -p '[{"op": "replace", "path": "/spec/server/gitSelfSignedCert", "value": true}]'
```

3. Create and start a new workspace. Every container used by the workspace mounts a special volume that contains a file with the self-signed certificate. The repository's **.git/config** file contains information about the Git server host (its URL) and the path to the certificate in the **http** section (see Git documentation about [git-config](#)). For example:

```
[http "https://10.33.177.118:3000"]
  sslCAInfo = /etc/che/git/cert/ca.crt
```

4.12. INSTALLING CODEREADY WORKSPACES USING STORAGE CLASSES

To configure CodeReady Workspaces to use a configured infrastructure storage, install CodeReady Workspaces using storage classes. This is especially useful when a user wants to bind a persistent volume provided by a non-default provisioner. To do so, a user binds this storage for the CodeReady Workspaces data saving and sets the parameters for that storage. These parameters can determine the following:

- A special host path
- A storage capacity
- A volume mod

- Mount options
- A file system
- An access mode
- A storage type
- And many others

CodeReady Workspaces has two components that require persistent volumes to store data:

- A PostgreSQL database.
- A CodeReady Workspaces workspace. CodeReady Workspaces workspace stores source code using volumes, for example **/projects** volume.



NOTE

CodeReady Workspaces workspace source code is stored in the persistent volume only if a workspace is not ephemeral.

Persistent volume claims facts:

- CodeReady Workspaces does not create persistent volumes in the infrastructure.
- CodeReady Workspaces uses persistent volume claims (PVC) to mount persistent volumes.
- The CodeReady Workspaces server creates persistent volume claims.
A user defines a storage class name in the CodeReady Workspaces configuration to use the storage classes feature in the CodeReady Workspaces PVC. With storage classes, a user configures infrastructure storage in a flexible way with additional storage parameters. It is also possible to bind a static provisioned persistent volumes to the CodeReady Workspaces PVC using the class name.

Procedure

Use CheCluster Custom Resource definition to define storage classes:

1. Define storage class names

To do so, use one of the following methods:

- **Use arguments for the `server:deploy` command**
 - i. Provide the storage class name for the PostgreSQL PVC
Use the **`crwctl server:deploy`** command with the **`--postgres-pvc-storage-class-name=postgres-storage`** flag:

```
$ crwctl server:deploy -m -p minikube -a operator --postgres-pvc-storage-class-name=postgres-storage
```

- ii. Provide the storage class name for the CodeReady Workspaces workspace
Use the **`server:deploy`** command with the **`--workspace-pvc-storage-class-name`** flag:

```
$ crwctl server:deploy -m -p minikube -a operator --workspace-pvc-storage-class-name=workspace-storage
```

For CodeReady Workspaces workspaces, the storage class name has different behavior depending on the workspace PVC strategy.



NOTE

postgres-pvc-storage-class-name=postgres-storage and **workspace-pvc-storage-class-name** work for the Operator installer and the Helm installer.

- Define storage class names using a Custom Resources YAML file:
 - i. Create a YAML file with Custom Resources defined for the CodeReady Workspaces installation.
 - ii. Define fields: **spec#storage#postgresPVCStorageClassName** and **spec#storage#workspacePVCStorageClassName**.

```
apiVersion: org.eclipse.che/v1
kind: CheCluster
metadata:
  name: codeready-workspaces
spec:
  # ...
  storage:
    # ...
    # keep blank unless you need to use a non default storage class for PostgreSQL
    PVC
    postgresPVCStorageClassName: 'postgres-storage'
    # ...
    # keep blank unless you need to use a non default storage class for workspace
    PVC(s)
    workspacePVCStorageClassName: 'workspace-storage'
    # ...
```

- iii. Start the codeready-workspaces server with your Custom Resources:

```
$ crwctl server:deploy -m -p minikube -a operator --che-operator-cr-yaml=/path/to/custom/che/resource/org_v1_che_cr.yaml
```

2. Configure CodeReady Workspaces to store workspaces in one persistent volume and a PostgreSQL database in the second one:

- a. Modify your Custom Resources YAML file:

- Set **pvcStrategy** as **common**.
- Configure CodeReady Workspaces to start workspaces in a single project.
- Define storage class names for **postgresPVCStorageClassName** and **workspacePVCStorageClassName**.
- Example of the YAML file:

```
apiVersion: org.eclipse.che/v1
kind: CheCluster
```

```

metadata:
  name: codeready-workspaces
spec:
  server:
    # ...
    workspaceNamespaceDefault: 'che'
    # ...
  storage:
    # ...
    # Defaults to common
    pvcStrategy: 'common'
    # ...
    # keep blank unless you need to use a non default storage class for PostgreSQL
  PVC
    postgresPVCStorageClassName: 'postgres-storage'
    # ...
    # keep blank unless you need to use a non default storage class for workspace
  PVC(s)
    workspacePVCStorageClassName: 'workspace-storage'
    # ...

```

- b. Start the codeready-workspaces server with your Custom Resources:

```
$ crwctl server:deploy -m -p minikube -a operator --che-operator-cr-yaml=/path/to/custom/che/resource/org_v1_che_cr.yaml
```

3. Bind static provisioned volumes using class names:

- a. Define the persistent volume for a PostgreSQL database:

```

# che-postgres-pv.yaml
apiVersion: v1
kind: PersistentVolume
metadata:
  name: postgres-pv-volume
  labels:
    type: local
spec:
  storageClassName: postgres-storage
  capacity:
    storage: 1Gi
  accessModes:
    - ReadWriteOnce
  hostPath:
    path: "/data/che/postgres"

```

- b. Define the persistent volume for a CodeReady Workspaces workspace:

```

# che-workspace-pv.yaml
apiVersion: v1
kind: PersistentVolume
metadata:
  name: workspace-pv-volume
  labels:
    type: local

```

```
spec:
  storageClassName: workspace-storage
  capacity:
    storage: 10Gi
  accessModes:
    - ReadWriteOnce
  hostPath:
    path: "/data/che/workspace"
```

c. Bind the two persistent volumes:

```
$ oc apply -f che-workspace-pv.yaml -f che-postgres-pv.yaml
```



NOTE

You must provide valid file permissions for volumes. You can do it using storage class configuration or manually. To manually define permissions, define **storageClass#mountOptions uid** and **gid**. PostgreSQL volume requires **uid=26** and **gid=26**.

4.13. IMPORTING UNTRUSTED TLS CERTIFICATES TO CODEREADY WORKSPACES

External communications between CodeReady Workspaces components are, by default, encrypted with TLS. Communications of CodeReady Workspaces components with external services such as proxies, source code repositories, identity providers may require using of TLS. Those communications require the use of TLS certificates signed by trusted Certificate Authorities.

When the certificates used by CodeReady Workspaces components or by an external service are signed by an untrusted CA it can be necessary to import the CA certificate in the CodeReady Workspaces installation, so that every CodeReady Workspaces component will consider them as signed by a trusted CA.

Typical cases that may require this addition are:

- when the underlying OpenShift cluster uses TLS certificates signed by a CA that is not trusted,
- when CodeReady Workspaces server or workspace components connect to external services such as RH-SSO or a Git server that use TLS certificates signed by an untrusted CA.

CodeReady Workspaces uses labeled ConfigMaps in CodeReady Workspaces namespace as sources for TLS certificates. The ConfigMaps can have arbitrary number of keys with arbitrary number of certificates each.

**NOTE**

When the cluster contains cluster-wide trusted CA certificates added through the [cluster-wide-proxy configuration](#), CodeReady Workspaces Operator detects them and automatically injects them into this ConfigMap:

- CodeReady Workspaces automatically labels the ConfigMap with the **config.openshift.io/inject-trusted-ca-bundle="true"** label.
- Based on this annotation, OpenShift automatically injects the cluster-wide trusted CA certificates inside the **ca-bundle.crt** key of ConfigMap

**IMPORTANT**

Some CodeReady Workspaces components require to have full certificate chain to trust the endpoint. If the cluster is configured with an intermediate certificate, then the whole chain (including self-signed root) should be added to CodeReady Workspaces.

4.13.1. Adding new CA certificates into CodeReady Workspaces

This guide can be used before the installations of CodeReady Workspaces or when CodeReady Workspaces is already installed and running.

**NOTE**

If you are using CodeReady Workspaces version lower than 2.5.1 see [this guide](#) on how to apply additional TLS certificates.

Prerequisites

- The **oc** tool is available.
- Namespace for CodeReady Workspaces exists.

Procedure

1. Save the certificates you need to import, to a local file system.

CAUTION

- Certificate files are typically stored as Base64 ASCII files, such as **.pem**, **.crt**, **.ca-bundle**. But, they can also be binary-encoded, for example, as **.cer** files. All Secrets that hold certificate files should use the Base64 ASCII certificate rather than the binary-encoded certificate.
 - CodeReady Workspaces already uses some reserved file names to automatically inject certificates into the ConfigMap, so you should avoid using the following reserved file names to save your certificates:
 - **ca-bundle.crt**
 - **ca.crt**
2. Create a new ConfigMap with the required TLS certificates:
 -

```
$ oc create configmap custom-certs --from-file=<bundle-file-path> -n=openshift-workspaces
```

To apply more than one bundle, add another **--from-file=<bundle-file-path>** flag to the above command. Or you may create another ConfigMap.

- Label created ConfigMaps with both **app.kubernetes.io/part-of=che.eclipse.org** and **app.kubernetes.io/component=ca-bundle** labels:

```
$ oc label configmap custom-certs app.kubernetes.io/part-of=che.eclipse.org
app.kubernetes.io/component=ca-bundle -n <crw-namespace-name>
```

- Deploy CodeReady Workspaces if it has not been deployed before otherwise wait until rollout of CodeReady Workspaces components finishes. If there are running workspaces, they should be restarted in order the changes take effect.

4.13.2. Verification at the CodeReady Workspaces installation level

If after adding the certificates something does not work as expected, here is a list of things to verify:

- In case of a CodeReady Workspaces [Operator](#) deployment, namespace where **CheCluster** located contains labeled ConfigMaps with right content:

```
$ oc get cm --selector=app.kubernetes.io/component=ca-bundle,app.kubernetes.io/part-of=che.eclipse.org -n openshift-workspaces
```

And to check content of ConfigMap:

```
$ {orch-cli} get cm __<name>__ -n {prod-namespace} -o yaml
```

- CodeReady Workspaces Pod Volumes list contains a volume that uses **ca-certs-merged** ConfigMap as data-source. To get the list of Volumes of the CodeReady Workspaces Pod:

```
$ oc get pod -o json <codeready-workspaces-pod-name> -n openshift-workspaces | jq
.spec.volumes
```

- CodeReady Workspaces mounts certificates in folder **/public-certs/** of the CodeReady Workspaces server container. This command returns the list of files in that folder:

```
$ oc exec -t <codeready-workspaces-pod-name> -n openshift-workspaces -- ls /public-certs/
```

- In the CodeReady Workspaces server logs there is a line for every certificate added to the Java truststore, including configured CodeReady Workspaces certificates.

```
$ oc logs <codeready-workspaces-pod-name> -n openshift-workspaces
```

- CodeReady Workspaces server Java truststore contains the certificates. The certificates SHA1 fingerprints are among the list of the SHA1 of the certificates included in the truststore returned by the following command:

```
$ oc exec -t <codeready-workspaces-pod-name> -n openshift-workspaces -- keytool -list -
keystore /home/jboss/cacerts
Your keystore contains 141 entries
```

```
(...)
```

To get the SHA1 hash of a certificate on the local filesystem:

```
$ openssl x509 -in <certificate-file-path> -fingerprint -noout
SHA1 Fingerprint=3F:DA:BF:E7:A7:A7:90:62:CA:CF:C7:55:0E:1D:7D:05:16:7D:45:60
```

4.13.3. Verification at the workspace level

- Start a workspace, get the OpenShift project in which it has been created, and wait for it to be started
- Get the name of the workspace Pod with the following command:

```
$ oc get pods -o=jsonpath='{.items[0].metadata.name}' -n <workspace namespace> | grep
'^workspace.*'
```

- Get the name of the Theia IDE container in the workspace Pod with the following command:

```
$ oc get -o json pod <workspace pod name> -n <workspace namespace> | \
jq -r '.spec.containers[] | select(.name | startswith("theia-ide")).name'
```

- Look for a **ca-certs** ConfigMap that should have been created inside the workspace namespace:

```
$ oc get cm ca-certs <workspace namespace>
```

- Check that the entries in the **ca-certs** ConfigMap contain all the additional entries you added before. In addition it may contain **ca-bundle.crt** entry which is a reserved one:

```
$ oc get cm ca-certs -n <workspace namespace> -o json | jq -r '.data | keys[]'
ca-bundle.crt
source-config-map-name.data-key.crt
```

- Make sure that the **ca-certs** ConfigMap has been added as a volume in the workspace Pod:

```
$ oc get -o json pod <workspace pod name> -n <workspace namespace> | \
jq '.spec.volumes[] | select(.configMap.name == "ca-certs")'
{
  "configMap": {
    "defaultMode": 420,
    "name": "ca-certs"
  },
  "name": "che-self-signed-certs"
}
```

- Confirm that the volume has been mounted into containers, especially in the Theia IDE container:

```
$ oc get -o json pod <workspace pod name> -n <workspace namespace> | \
jq '.spec.containers[] | select(.name == "<theia ide container name>").volumeMounts[] | \
select(.name == "che-self-signed-certs")'
```

```
{
  "mountPath": "/public-certs",
  "name": "che-self-signed-certs",
  "readOnly": true
}
```

- Inspect **/public-certs** folder in the Theia IDE container and check that its contents match the list of entries in the **ca-certs** ConfigMap:

```
$ oc exec <workspace pod name> -c <theia ide container name> -n <workspace namespace> -- ls /public-certs
ca-bundle.crt
source-config-map-name.data-key.crt
```

4.14. SWITCHING BETWEEN EXTERNAL AND INTERNAL DNS NAMES IN INTER-COMPONENT COMMUNICATION

By default, new CodeReady Workspaces deployments use OpenShift services DNS names for communications between CodeReady Workspaces server, RH-SSO, registries, and helps with:

- Bypassing proxy, certificates, and firewalls issues
- Speeding up the traffic

This type of communication is an alternative to the external method of inter-component communication, which uses OpenShift Route cluster host names. In the situations described below, using OpenShift internal DNS names is not supported. By disabling the use of the internal cluster host name in inter-component communication, the communication using external OpenShift Route will come into effect.

Internal inter-component communication restrictions in OpenShift

- The CodeReady Workspaces components are deployed across multi-cluster OpenShift environments.
- The OpenShift NetworkPolicies restricts communication between namespaces.

The following section describes how to enable and disable the external inter-component communication for OpenShift Route.

Prerequisites

- The **oc** tool is available.
- An instance of CodeReady Workspaces running in OpenShift.

Procedure

Switching between external and internal inter-component communication method is reached through the update against Custom Resource (CR).

1. To use external OpenShift Route in inter-component communication:

```
$ oc patch checluster codeready-workspaces -n openshift-workspaces --type=json -p \
[{"op": "replace", "path": "/spec/server/useInternalClusterSVCNames", "value": false}]
```

- To use internal OpenShift DNS names in the inter-component communication:

```
$ oc patch checluster codeready-workspaces -n openshift-workspaces --type=json -p \
[{"op": "replace", "path": "/spec/server/useInternalClusterSVCNames", "value": true}]
```

4.15. SETTING UP THE RH-SSO CODEREADY-WORKSPACES-USERNAME-READONLY THEME FOR THE RED HAT CODEREADY WORKSPACES LOGIN PAGE

The following procedure is relevant for all CodeReady Workspaces instances with the OpenShift OAuth service enabled.

When a user with pre-created namespaces logs in to Red Hat CodeReady Workspaces Dashboard for the first time, a page allowing the user to update account information is displayed. It is possible to change the username, but choosing a username that doesn't match the OpenShift username, prevents the user's workspaces from running. This is caused by CodeReady Workspaces attempts to use a non-existing namespace, the name of which is derived from a user OpenShift username, to create a workspace. To prevent this, log in to RH-SSO and modify the theme settings.

4.15.1. Logging in to RH-SSO

The following procedure describes how to log in to RH-SSO, which acts as a route for OpenShift platforms. To log in to RH-SSO, a user has to obtain the RH-SSO URL and a user's credentials first.

Prerequisites

- The **oc** tool installed.
- Logged in to OpenShift cluster using the **oc** tool.

Procedure

- Obtain a user RH-SSO login:

```
oc get secret che-identity-secret -n openshift-workspaces -o json | jq -r '.data.user' | base64 -d
```

- Obtain a user RH-SSO password:

```
oc get secret che-identity-secret -n openshift-workspaces -o json | jq -r '.data.password' | base64 -d
```

- Obtain the RH-SSO URL:

```
oc get ingress -n openshift-workspaces -l app=che,component=keycloak -o 'custom-columns=URL:.spec.rules[0].host' --no-headers
```

- Open the URL in a browser and log in to RH-SSO using the obtained login and password.

4.15.2. Setting up the RH-SSO `codeready-workspaces-username-readonly` theme

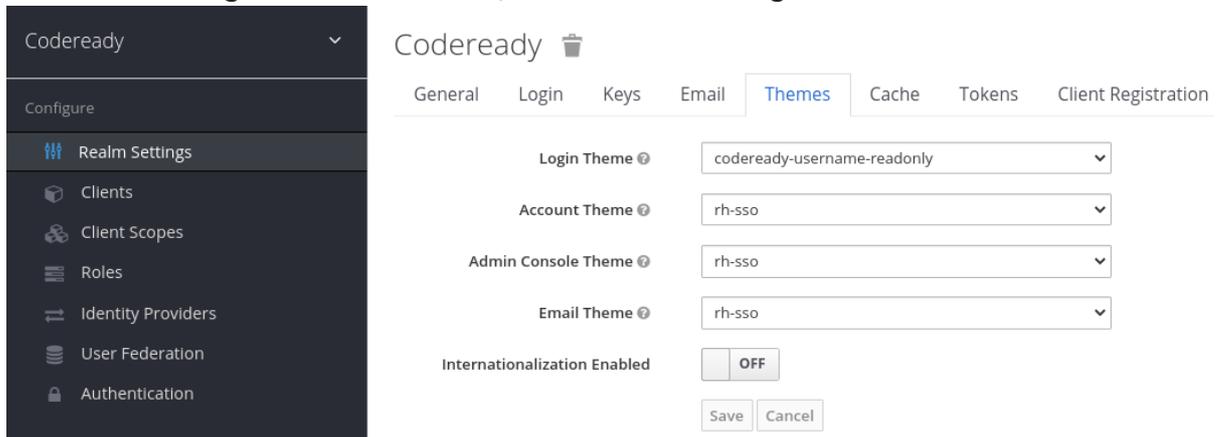
Prerequisites

- An instance of CodeReady Workspaces running in OpenShift.
- A user is logged in to the RH-SSO service.

Procedure

After changing a username, set the **Login Theme** option to **readonly**.

1. In the main **Configure** menu on the left, select **Realm Settings**:



2. Navigate to the **Themes** tab.
3. In the **Login Theme** field, select the **codeready-workspaces-username-readonly** option and click the **Save** button to apply the changes.

4.16. MOUNTING A SECRET AS A FILE OR AN ENVIRONMENT VARIABLE INTO A RED HAT CODEREADY WORKSPACES CONTAINER

Secrets are OpenShift objects that store sensitive data such as user names, passwords, authentication tokens, and configurations in an encrypted form.

Users can mount a OpenShift secret that contains sensitive data in a Red Hat CodeReady Workspaces container as:

- a file
- an environment variable

The mounting process uses the standard OpenShift mounting mechanism, but it requires additional annotations and labeling.

4.16.1. Mounting a secret as a file into a Red Hat CodeReady Workspaces container

Prerequisites

- A running instance of CodeReady Workspaces. To install an instance of CodeReady Workspaces, see [Installing CodeReady Workspaces](#).

Procedure

1. Create a new OpenShift secret in the OpenShift project where a CodeReady Workspaces is deployed. The labels of the secret that is about to be created must match the set of labels:

- **app.kubernetes.io/part-of: che.eclipse.org**
- **app.kubernetes.io/component: <DEPLOYMENT_NAME>-secret**

Where **<DEPLOYMENT_NAME>** is one of the following deployments: **postgres**, **keycloak**, **devfile-registry**, **plugin-registry** or **codeready**

Example 4.5. Example:

```
apiVersion: v1
kind: Secret
metadata:
  name: custom-certificate
labels:
  app.kubernetes.io/part-of: che.eclipse.org
  app.kubernetes.io/component: codeready-secret
...
```

Annotations must indicate that the given secret is mounted as a file. Configure the annotation values:

- **che.eclipse.org/mount-as: file** - to indicate that a secret is mounted as a file
- **che.eclipse.org/mount-path: <FOO_ENV>** - to provide a required mount path

```
apiVersion: v1
kind: Secret
metadata:
  name: custom-certificate
annotations:
  che.eclipse.org/mount-path: /custom-certificates
  che.eclipse.org/mount-as: file
labels:
...
```

The OpenShift secret may contain several items whose names must match the desired file name mounted into the container.

```
apiVersion: v1
kind: Secret
metadata:
  name: custom-certificate
labels:
  app.kubernetes.io/part-of: che.eclipse.org
  app.kubernetes.io/component: codeready-secret
annotations:
  che.eclipse.org/mount-path: /custom-certificates
  che.eclipse.org/mount-as: file
data:
  ca.crt: <base64 encoded data content here>
```

This results in a file named **ca.crt** being mounted at the **/custom-certificates** path of CodeReady Workspaces container.

4.16.2. Mounting a secret as an environment variable into a Red Hat CodeReady Workspaces container

Prerequisites

- A running instance of Red Hat CodeReady Workspaces. To install an instance of Red Hat CodeReady Workspaces, see [Installing CodeReady Workspaces](#).

Procedure

1. Create a new OpenShift secret in the OpenShift project where a CodeReady Workspaces is deployed. The labels of the secret that is about to be created must match the set of labels:
 - **app.kubernetes.io/part-of: che.eclipse.org**
 - **app.kubernetes.io/component: <DEPLOYMENT_NAME>-secret**

Where **<DEPLOYMENT_NAME>** is one of the following deployments: **postgres**, **keycloak**, **devfile-registry**, **plugin-registry** or **codeready**

Example 4.6. Example:

```
apiVersion: v1
kind: Secret
metadata:
  name: custom-settings
labels:
  app.kubernetes.io/part-of: che.eclipse.org
  app.kubernetes.io/component: codeready-secret
...
```

Annotations must indicate that the given secret is mounted as a environment variable. Configure the annotation values:

- **che.eclipse.org/mount-as: env** - to indicate that a secret is mounted as an environment variable
- **che.eclipse.org/env-name: <FOO_ENV>** - to provide an environment variable name, which is required to mount a secret key value

```
apiVersion: v1
kind: Secret
metadata:
  name: custom-settings
annotations:
  che.eclipse.org/env-name: FOO_ENV
  che.eclipse.org/mount-as: env
labels:
  ...
data:
  mykey: myvalue
```

This results in the environment variable named **FOO_ENV** and the value **myvalue** being provisioned into a CodeReady Workspaces container.

If the secret provides more than one data item, the environment variable name must be provided for each of the data keys as follows:

```
apiVersion: v1
kind: Secret
metadata:
  name: custom-settings
annotations:
  che.eclipse.org/mount-as: env
  che.eclipse.org/mykey_env-name: FOO_ENV
  che.eclipse.org/otherkey_env-name: OTHER_ENV
labels:
  ...
data:
  mykey: myvalue
  otherkey: othervalue
```

This results in two environment variables with names **FOO_ENV**, **OTHER_ENV**, and values **myvalue** and **othervalue**, being provisioned into a CodeReady Workspaces container.



NOTE

The maximum length of annotation names in a OpenShift secret is 63 characters, where 9 characters are reserved for a prefix that ends with /. This acts as a restriction for the maximum length of the key that can be used for the secret.

4.17. ENABLING DEV WORKSPACE ENGINE

This procedure describes how to enable the Dev Workspace engine to support the Devfile 2.0.0 file format and mentions how to do so on existing instances or those about to be installed.

Prerequisites

- The **oc** and **crwctl** tools are available.

Procedure

- For a new OperatorHub installation:
 1. Enter the Red Hat CodeReady Workspaces Cluster using OpenShift Container Platform and create CheCluster Custom Resource (CR). See, [Creating an instance of the Red Hat CodeReady Workspaces Operator](#)
 2. Set the following values in codeready-workspaces Custom Resource (CR):

```
spec:
  devWorkspace:
    enable: true
```

- For a new **crwctl** installation:

1. Configure the the **crwctl** installation using:

```
$ crwctl server:deploy --che-operator-cr-patch-yaml=patch.yaml ...
```

patch.yaml must contain the following:

```
spec:  
  devWorkspace:  
    enable: true
```

- For already existing CodeReady Workspaces installation:

1. Update **codeready-workspaces** CR using the **oc** tool:

```
$ oc patch checluster codeready-workspaces -n openshift-workspaces --type=json -p \  
' [{"op": "replace", "path": "/spec/devWorkspace/enable", "value": true}]'
```

Additional resources

For information about installation methods mentioned in this chapter, see [Chapter 3, Installing CodeReady Workspaces](#).

CHAPTER 5. UPGRADING CODEREADY WORKSPACES

This chapter describes how to upgrade a CodeReady Workspaces instance from version 2.7 to CodeReady Workspaces 2.8.

The method used to install the CodeReady Workspaces instance determines the method to proceed with for the upgrade:

- [Section 5.1, “Upgrading CodeReady Workspaces using OperatorHub”](#)
- [Section 5.2, “Upgrading CodeReady Workspaces using the CLI management tool”](#)
- [Section 5.3, “Upgrading CodeReady Workspaces using the CLI management tool in restricted environment”](#)

5.1. UPGRADING CODEREADY WORKSPACES USING OPERATORHUB

This section describes how to upgrade from an earlier minor version using the Operator from OperatorHub in the OpenShift web console.

OperatorHub supports **Automatic** and **Manual** upgrade strategies: **Automatic**:: The upgrade process starts when a new version of the Operator is published. **Manual**:: The update must be manually approved every time the new version of the Operator is published.

5.1.1. Specifying the approval strategy of CodeReady Workspaces in OperatorHub

Prerequisites

- An administrator account on an OpenShift instance.
- An instance of an earlier minor version of CodeReady Workspaces, installed using the Operator from OperatorHub on the same instance of OpenShift.

Procedure

1. Open the OpenShift web console.
2. Navigate to the **Operators** → **Installed Operators** section.
3. Click **Red Hat CodeReady Workspaces** in the list of the installed Operators.
4. Navigate to the **Subscription** tab and specify the approval strategy:
 - **Approval: Automatic**
or
Approval: Manual

Change Update Approval Strategy

What strategy is used for approving updates?

Automatic (default)

New updates will be installed as soon as they become available.

Manual

New updates need to be manually approved before installation begins.

Cancel

Save

5.1.2. Manually upgrading CodeReady Workspaces in OperatorHub

Prerequisites

- An administrator account on an OpenShift instance.
- An instance of an earlier minor version of CodeReady Workspaces, installed using the Operator from OperatorHub on the same instance of OpenShift.
- The approval strategy in the subscription is set to **Manual**.

Procedure

1. Open the OpenShift web console.
2. Navigate to the **Operators → Installed Operators** section.
3. Click **Red Hat CodeReady Workspaces** in the list of the installed Operators.
4. Navigate to the **Subscription** tab. Upgrades requiring approval are displayed next to **Upgrade Status**, for example **1 requires approval**.
5. Click **1 requires approval**, then click **Preview Install Plan**.
6. Review the resources that are listed as available for upgrade and click **Approve**.

Verification steps

1. Navigate to the **Operators → Installed Operators** page to monitor the progress of the upgrade. When complete, the status changes to **Succeeded** and **Up to date**.
2. The 2.8 version number is visible at the bottom of the page.

Additional resources

- [Upgrading installed Operators](#) section in the OpenShift documentation.

5.2. UPGRADING CODEREADY WORKSPACES USING THE CLI MANAGEMENT TOOL

This section describes how to upgrade from previous minor version using the CLI management tool.

Prerequisites

- An administrative account on an OpenShift instance.
- A running instance of a previous minor version of Red Hat CodeReady Workspaces, installed using the CLI management tool on the same instance of OpenShift, in the **<openshift-workspaces>** project.
- An installation of the **crwctl** 2.8 version management tool. See [Section 3.3.1, “Installing the crwctl CLI management tool”](#).

Procedure

1. In all running workspaces in the CodeReady Workspaces 2.7 instance, save and push changes back to the Git repositories.
2. Shut down all workspaces in the CodeReady Workspaces 2.7 instance.
3. Run the following command:

```
$ crwctl server:update -n <openshift-workspaces>
```



NOTE

For slow systems or internet connections, add the **--k8spodwaittimeout=1800000** flag option to the **crwctl server:update** command to extend the Pod timeout period to 1800000 ms or longer.

Verification steps

1. Navigate to the CodeReady Workspaces instance.
2. The 2.8 version number is visible at the bottom of the page.

5.3. UPGRADING CODEREADY WORKSPACES USING THE CLI MANAGEMENT TOOL IN RESTRICTED ENVIRONMENT

This section describes how to upgrade Red Hat CodeReady Workspaces using the CLI management tool in restricted environment. The upgrade path supports minor version update, from CodeReady Workspaces version 2.7 to version 2.8.

Prerequisites

- An administrative account on an instance of OpenShift.
- A running instance version 2.7 of Red Hat CodeReady Workspaces, installed using the CLI

management tool on the same instance of OpenShift, with the `crwctl --installer operator` method, in the `<openshift-workspaces>` project. See [Section 3.4, “Installing CodeReady Workspaces in a restricted environment”](#).

- The `crwctl` 2.8 management tool is available. See [Section 3.3.1, “Installing the crwctl CLI management tool”](#).

5.3.1. Understanding network connectivity in restricted environments

CodeReady Workspaces requires that each OpenShift Route created for CodeReady Workspaces is accessible from inside the OpenShift cluster. These CodeReady Workspaces components have a OpenShift Route: **codeready-workspaces-server**, **keycloak**, **devfile-registry**, **plugin-registry**.

Consider the network topology of the environment to determine how best to accomplish this.

Example 5.1. Network owned by a company or an organization, disconnected from the public Internet

The network administrators must ensure that it is possible to route traffic bound from the cluster to OpenShift Route host names.

Example 5.2. Private subnetwork in a cloud provider

Create a proxy configuration allowing the traffic to leave the node to reach an external-facing Load Balancer.

5.3.2. Building offline registry images

5.3.2.1. Building an offline devfile registry image

This section describes how to build an offline devfile registry image. Starting workspaces without relying on resources from the outside Internet requires building this image. The image contains all sample projects referenced in devfiles as **zip** files.

Prerequisites:

- A running installation of [podman](#) or [docker](#).

Procedure

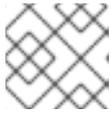
1. Clone the devfile registry repository and check out the version to deploy:

```
$ git clone git@github.com:redhat-developer/codeready-workspaces.git
$ cd codeready-workspaces
$ git checkout crw-2.8-rhel-8
```

2. Build an offline devfile registry image:

```
$ cd dependencies/che-devfile-registry
$ ./build.sh --organization <my-org> \
  --registry <my-registry> \
```

```
--tag <my-tag> \  
--offline
```

**NOTE**

To display full options for the **build.sh** script, use the **--help** parameter.

Additional resources

- [Customizing the registries.](#)

5.3.2.2. Building an offline plug-in registry image

This section describes how to build an offline plug-in registry image. Starting workspaces without relying on resources from the outside Internet requires building this image. The image contains plug-in metadata and all plug-in or extension artifacts.

Prerequisites

- NodeJS 12.x
- A running version of yarn. See [Installing Yarn](#).
- **./node_modules/.bin** is in the **PATH** environment variable.
- A running installation of [podman](#) or [docker](#).

Procedure

1. Clone the plug-in registry repository and check out the version to deploy:

```
$ git clone git@github.com:redhat-developer/codeready-workspaces.git  
$ cd codeready-workspaces  
$ git checkout crw-2.8-rhel-8
```

2. Build offline plug-in registry image:

```
$ cd dependencies/che-plugin-registry  
$ ./build.sh --organization <my-org> \  
  --registry <my-registry> \  
  --tag <my-tag> \  
  --offline
```

**NOTE**

To display full options for the **build.sh** script, use the **--help** parameter.

Additional resources

- [Customizing the registries.](#)

5.3.3. Preparing an private registry

Prerequisites

- The **oc** tool is available.
- The **skopeo** tool, version 0.1.40 or later, is available.
- The **podman** tool is available.
- An image registry accessible from the OpenShift cluster and supporting the format of the V2 image manifest, schema version 2. Ensure you can push to it from a location having, at least temporarily, access to the internet.

Table 5.1. Placeholders used in examples

<source-image>	Full coordinates of the source image, including registry, organization, and digest.
<target-registry>	Host name and port of the target container-image registry.
<target-organization>	Organization in the target container-image registry
<target-image>	Image name and digest in the target container-image registry.
<target-user>	User name in the target container-image registry.
<target-password>	User password in the target container-image registry.

Procedure

1. Log into the internal image registry:

```
$ podman login --username <user> --password <password> <target-registry>
```



NOTE

If you encounter an error, like **x509: certificate signed by unknown authority**, when attempting to push to the internal registry, try one of these workarounds:

- add the OpenShift cluster's certificate to **/etc/containers/certs.d/<target-registry>**
- add the registry as an insecure registry by adding the following lines to the Podman configuration file located at **/etc/containers/registries.conf**:

```
[registries.insecure]
registries = ['<target-registry>']
```

2. Copy images without changing their digest. Repeat this step for every image in the following table:

```
$ skopeo copy --all docker://<source-image> docker://<target-registry>/<target-organization>/<target-image>
```



NOTE

Table 5.2. Understanding the usage of the container-images from the prefix or keyword they include in their name

Usage	Prefix or keyword
Essential	not stacks- , plugin- , or -openj9-
Workspaces	stacks- , plugin-
IBM Z and IBM Power Systems	-openj9-

Table 5.3. Images to copy in the private registry

<source-image>	<target-image>
registry.redhat.io/codeready-workspaces/configbump-rhel8@sha256:db34b20374d99c2055612663a669a06f6dd0fc1fc19603761e993fd0870eddfc	configbump-rhel8@sha256:db34b20374d99c2055612663a669a06f6dd0fc1fc19603761e993fd0870eddfc
registry.redhat.io/codeready-workspaces/crw-2-rhel8-operator@sha256:a24dc83d8cdd8af715f0c4f235dcba0736bf395b7029ceaed0b8a683da5f74e0	crw-2-rhel8-operator@sha256:a24dc83d8cdd8af715f0c4f235dcba0736bf395b7029ceaed0b8a683da5f74e0
registry.redhat.io/codeready-workspaces/crw-2-rhel8-operator@sha256:a24dc83d8cdd8af715f0c4f235dcba0736bf395b7029ceaed0b8a683da5f74e0	crw-2-rhel8-operator@sha256:a24dc83d8cdd8af715f0c4f235dcba0736bf395b7029ceaed0b8a683da5f74e0
registry.redhat.io/codeready-workspaces/devfileregistry-rhel8@sha256:e3c360c031d8e68b62d1a28a4d736f41c5bfbfc17c23999b9e1f1e5820858bf1d	devfileregistry-rhel8@sha256:e3c360c031d8e68b62d1a28a4d736f41c5bfbfc17c23999b9e1f1e5820858bf1d
registry.redhat.io/codeready-workspaces/jwtproxy-rhel8@sha256:3f40bb8a2022545ac06a0b41cdb0239fdacfc34b37faffb21348a2041e96d0f2	jwtproxy-rhel8@sha256:3f40bb8a2022545ac06a0b41cdb0239fdacfc34b37faffb21348a2041e96d0f2

<source-image>	<target-image>
<p>registry.redhat.io/codeready-workspaces/machineexec-rhel8@sha256:19a8daf7f9adde981dcd588b0526fa7682111097849f60a9b0e81137bdd e8f6c</p>	<p>machineexec-rhel8@sha256:19a8daf7f9adde981dcd588b0526fa7682111097849f60a9b0e81137bdd e8f6c</p>
<p>registry.redhat.io/codeready-workspaces/plugin-java11-openj9-rhel8@sha256:ee7c41053b4c8615886745566fc306dbf5bd1b1d367e525266477ae17a26673e</p>	<p>plugin-java11-openj9-rhel8@sha256:ee7c41053b4c8615886745566fc306dbf5bd1b1d367e525266477ae17a26673e</p>
<p>registry.redhat.io/codeready-workspaces/plugin-java11-openj9-rhel8@sha256:ee7c41053b4c8615886745566fc306dbf5bd1b1d367e525266477ae17a26673e</p>	<p>plugin-java11-openj9-rhel8@sha256:ee7c41053b4c8615886745566fc306dbf5bd1b1d367e525266477ae17a26673e</p>
<p>registry.redhat.io/codeready-workspaces/plugin-java11-openj9-rhel8@sha256:ee7c41053b4c8615886745566fc306dbf5bd1b1d367e525266477ae17a26673e</p>	<p>plugin-java11-openj9-rhel8@sha256:ee7c41053b4c8615886745566fc306dbf5bd1b1d367e525266477ae17a26673e</p>
<p>registry.redhat.io/codeready-workspaces/plugin-java11-rhel8@sha256:d93195134cef6351b1f9e3165fecc09f464dc99ab33d11b68fadd613d04d1636</p>	<p>plugin-java11-rhel8@sha256:d93195134cef6351b1f9e3165fecc09f464dc99ab33d11b68fadd613d04d1636</p>
<p>registry.redhat.io/codeready-workspaces/plugin-java8-openj9-rhel8@sha256:8d8948134405e45bdd895932afa85b6cf0fbfe4e9bb58ae9753d233ddf74672b</p>	<p>plugin-java8-openj9-rhel8@sha256:8d8948134405e45bdd895932afa85b6cf0fbfe4e9bb58ae9753d233ddf74672b</p>
<p>registry.redhat.io/codeready-workspaces/plugin-java8-openj9-rhel8@sha256:8d8948134405e45bdd895932afa85b6cf0fbfe4e9bb58ae9753d233ddf74672b</p>	<p>plugin-java8-openj9-rhel8@sha256:8d8948134405e45bdd895932afa85b6cf0fbfe4e9bb58ae9753d233ddf74672b</p>
<p>registry.redhat.io/codeready-workspaces/plugin-java8-openj9-rhel8@sha256:8d8948134405e45bdd895932afa85b6cf0fbfe4e9bb58ae9753d233ddf74672b</p>	<p>plugin-java8-openj9-rhel8@sha256:8d8948134405e45bdd895932afa85b6cf0fbfe4e9bb58ae9753d233ddf74672b</p>

<source-image>	<target-image>
<p>registry.redhat.io/codeready-workspaces/plugin-java8-rhel8@sha256:ecaa9ddef5ca8db9552f1b5e66f7aacb19d72e488d718d8135b1e1d9f66a1a7a</p>	<p>plugin-java8-rhel8@sha256:ecaa9ddef5ca8db9552f1b5e66f7aacb19d72e488d718d8135b1e1d9f66a1a7a</p>
<p>registry.redhat.io/codeready-workspaces/plugin-kubernetes-rhel8@sha256:cf1d0e24f8bae0f87cae0b1577dfd25e124437d78031d7076fabebb2dcf48d7f</p>	<p>plugin-kubernetes-rhel8@sha256:cf1d0e24f8bae0f87cae0b1577dfd25e124437d78031d7076fabebb2dcf48d7f</p>
<p>registry.redhat.io/codeready-workspaces/plugin-openshift-rhel8@sha256:13ce6d8fdeeea0cc5a220eb8abd2811c31bb2a424736759be9a6df15c8f77fd</p>	<p>plugin-openshift-rhel8@sha256:13ce6d8fdeeea0cc5a220eb8abd2811c31bb2a424736759be9a6df15c8f77fd</p>
<p>registry.redhat.io/codeready-workspaces/pluginbroker-artifacts-rhel8@sha256:cda306cb7e5c42faa6ab43218d39984d4955134b3ca9654968c28b05e0796c3a</p>	<p>pluginbroker-artifacts-rhel8@sha256:cda306cb7e5c42faa6ab43218d39984d4955134b3ca9654968c28b05e0796c3a</p>
<p>registry.redhat.io/codeready-workspaces/pluginbroker-metadata-rhel8@sha256:0143a80b869620af08a0d60165dc9d13357a79e7243502832326cf053c17ee38</p>	<p>pluginbroker-metadata-rhel8@sha256:0143a80b869620af08a0d60165dc9d13357a79e7243502832326cf053c17ee38</p>
<p>registry.redhat.io/codeready-workspaces/pluginregistry-rhel8@sha256:3f5163a2303de7f538eca2cc560403f38b920af1169821dfa06dbef695fb10c6</p>	<p>pluginregistry-rhel8@sha256:3f5163a2303de7f538eca2cc560403f38b920af1169821dfa06dbef695fb10c6</p>
<p>registry.redhat.io/codeready-workspaces/server-rhel8@sha256:6635e8c160c8c73c00c9b05eccab08a4ff23d344f102ef0097a3798bf108217a</p>	<p>server-rhel8@sha256:6635e8c160c8c73c00c9b05eccab08a4ff23d344f102ef0097a3798bf108217a</p>
<p>registry.redhat.io/codeready-workspaces/stacks-cpp-rhel8@sha256:06cd3600c3b6c3dca0451b10b46961fd0db4140c7dddc4f9637984022f5cfc09</p>	<p>stacks-cpp-rhel8@sha256:06cd3600c3b6c3dca0451b10b46961fd0db4140c7dddc4f9637984022f5cfc09</p>

<source-image>	<target-image>
registry.redhat.io/codeready-workspaces/stacks-dotnet-rhel8@sha256:ea77974b206c7d7abcd5cd32149f6bb669d3cf867135553af4d7dddd24ba9cf	stacks-dotnet-rhel8@sha256:ea77974b206c7d7abcd5cd32149f6bb669d3cf867135553af4d7dddd24ba9cf
registry.redhat.io/codeready-workspaces/stacks-golang-rhel8@sha256:e01d32e58a55a552f0d35b9a6210b7a2cc8ed444f8ae54a24113dcc85f4d80db	stacks-golang-rhel8@sha256:e01d32e58a55a552f0d35b9a6210b7a2cc8ed444f8ae54a24113dcc85f4d80db
registry.redhat.io/codeready-workspaces/stacks-php-rhel8@sha256:95c324ed660924bf76e10b461d75aa5be2a323f26e5033239f7cbfe1ec10b26e	stacks-php-rhel8@sha256:95c324ed660924bf76e10b461d75aa5be2a323f26e5033239f7cbfe1ec10b26e
registry.redhat.io/codeready-workspaces/theia-endpoint-rhel8@sha256:60c84fca55a997a6aab4ca07b8ff7d859948c1f525adeba2ae624c84fe059a56	theia-endpoint-rhel8@sha256:60c84fca55a997a6aab4ca07b8ff7d859948c1f525adeba2ae624c84fe059a56
registry.redhat.io/codeready-workspaces/theia-rhel8@sha256:de36fdf140ba6367e6edf577d6dbaffa270e5e5ecf0890e498f5907f8287858f	theia-rhel8@sha256:de36fdf140ba6367e6edf577d6dbaffa270e5e5ecf0890e498f5907f8287858f
registry.redhat.io/codeready-workspaces/traefik-rhel8@sha256:0698a776c6ae2f08238cf011d69ac2c67f934b1e25ec38701a9e360430fd10f7	traefik-rhel8@sha256:0698a776c6ae2f08238cf011d69ac2c67f934b1e25ec38701a9e360430fd10f7
registry.redhat.io/jboss-eap-7/eap-xp2-openj9-11-openshift-rhel8@sha256:95d2ce73a0759de5befdbec115514a555752e2f20070fbfe356801da6d0a2bd6	eap-xp2-openj9-11-openshift-rhel8@sha256:95d2ce73a0759de5befdbec115514a555752e2f20070fbfe356801da6d0a2bd6
registry.redhat.io/jboss-eap-7/eap-xp2-openj9-11-openshift-rhel8@sha256:95d2ce73a0759de5befdbec115514a555752e2f20070fbfe356801da6d0a2bd6	eap-xp2-openj9-11-openshift-rhel8@sha256:95d2ce73a0759de5befdbec115514a555752e2f20070fbfe356801da6d0a2bd6

<source-image>	<target-image>
<p>registry.redhat.io/jboss-eap-7/eap-xp2-openj9-11-openshift-rhel8@sha256:95d2ce73a0759de5befdbec115514a555752e2f20070fbfe356801da6d0a2bd6</p>	<p>eap-xp2-openj9-11-openshift-rhel8@sha256:95d2ce73a0759de5befdbec115514a555752e2f20070fbfe356801da6d0a2bd6</p>
<p>registry.redhat.io/jboss-eap-7/eap-xp2-openjdk11-openshift-rhel8@sha256:647d092383a760edc083eafb2d7bc3208d6409097281bedbd5eaccde360e7e39</p>	<p>eap-xp2-openjdk11-openshift-rhel8@sha256:647d092383a760edc083eafb2d7bc3208d6409097281bedbd5eaccde360e7e39</p>
<p>registry.redhat.io/jboss-eap-7/eap73-openjdk8-openshift-rhel7@sha256:d16cfe30eaf20a157cd5d5980a6c34f3fcbcf2fd225e670a0138d81007dd919</p>	<p>eap73-openjdk8-openshift-rhel7@sha256:d16cfe30eaf20a157cd5d5980a6c34f3fcbcf2fd225e670a0138d81007dd919</p>
<p>registry.redhat.io/rh-sso-7/sso74-openj9-openshift-rhel8@sha256:ed11770a85ca95fc9cbb2cade539a67ff0e127cff73a89a017415800e032bd5b</p>	<p>sso74-openj9-openshift-rhel8@sha256:ed11770a85ca95fc9cbb2cade539a67ff0e127cff73a89a017415800e032bd5b</p>
<p>registry.redhat.io/rh-sso-7/sso74-openj9-openshift-rhel8@sha256:ed11770a85ca95fc9cbb2cade539a67ff0e127cff73a89a017415800e032bd5b</p>	<p>sso74-openj9-openshift-rhel8@sha256:ed11770a85ca95fc9cbb2cade539a67ff0e127cff73a89a017415800e032bd5b</p>
<p>registry.redhat.io/rh-sso-7/sso74-openshift-rhel8@sha256:3154fd4f6ce080260de9d2b4c02930b67b57f1181f4e660f5ddfc9f6050420b1</p>	<p>sso74-openshift-rhel8@sha256:3154fd4f6ce080260de9d2b4c02930b67b57f1181f4e660f5ddfc9f6050420b1</p>
<p>registry.redhat.io/rhel8/postgresql-96@sha256:32d73d737acec3daabc3f5c8236588454c8f57f7a2656ac7a50cf3a04f520b9b</p>	<p>postgresql-96@sha256:32d73d737acec3daabc3f5c8236588454c8f57f7a2656ac7a50cf3a04f520b9b</p>
<p>registry.redhat.io/rhsc1/mongodb-36-rhel7@sha256:9f799d356d7d2e442bde9d401b720600fd9059a3d8eefea6f3b2ffa721c0dc73</p>	<p>mongodb-36-rhel7@sha256:9f799d356d7d2e442bde9d401b720600fd9059a3d8eefea6f3b2ffa721c0dc73</p>

<source-image>	<target-image>
registry.redhat.io/ubi8/ubi-minimal@sha256:2f6b88c037c0503da7704bccd3fc73cb76324101af39ad28f16460e7bce98324	ubi8ubi-minimal@sha256:2f6b88c037c0503da7704bccd3fc73cb76324101af39ad28f16460e7bce98324

Verification steps

- Verify the images have the same digests:

```
$ skopeo inspect docker://<source-image>
$ skopeo inspect docker://<target-registry>/<target-organization>/<target-image>
```

Additional resources

- To find the sources of the images list, see the values of the **relatedImages** attribute in the [CodeReady Workspaces Operator ClusterServiceVersion sources](#).

5.3.4. Upgrading CodeReady Workspaces using the CLI management tool in restricted environment

This section describes how to upgrade Red Hat CodeReady Workspaces using the CLI management tool in restricted environment.

Prerequisites

- An administrative account on an OpenShift instance.
- A running instance version 2.7 of Red Hat CodeReady Workspaces, installed using the CLI management tool on the same instance of OpenShift, with the `crwctl --installer operator` method, in the **<openshift-workspaces>** project. See [Section 3.4, "Installing CodeReady Workspaces in a restricted environment"](#).
- Essential container images are available to the CodeReady Workspaces server running in the cluster. See [Section 5.3.3, "Preparing an private registry"](#).
- The **crwctl** 2.8 management tool is available. See [Section 3.3.1, "Installing the crwctl CLI management tool"](#).

Procedure

1. In all running workspaces in the CodeReady Workspaces 2.7 instance, save and push changes back to the Git repositories.
2. Stop all workspaces in the CodeReady Workspaces 2.7 instance.
3. Run the following command:

```
$ crwctl server:update --che-operator-image=<image-registry>/<organization>/crw-2-rhel8-operator:2.8 -n openshift-workspaces
```

- *<image-registry>*: A host name and a port of the container-image registry accessible in the restricted environment.
- *<organization>*: An organization of the container-image registry. See: [Section 5.3.3, "Preparing a private registry"](#).

Verification steps

1. Navigate to the CodeReady Workspaces instance.
2. The 2.8 version number is visible at the bottom of the page.



NOTE

For slow systems or internet connections, add the **--k8spodwaittimeout=1800000** flag option to the **crwctl server:update** command to extend the Pod timeout period to 1800000 ms or longer.

CHAPTER 6. UNINSTALLING CODEREADY WORKSPACES

This section describes uninstallation procedures for Red Hat CodeReady Workspaces. The uninstallation process leads to a complete removal of CodeReady Workspaces–related user data. The method previously used to install the CodeReady Workspaces instance determines the uninstallation method.

- For CodeReady Workspaces installed using OperatorHub, for the OpenShift Web Console method see [Section 6.1, “Uninstalling CodeReady Workspaces after OperatorHub installation using the OpenShift web console”](#).
- For CodeReady Workspaces installed using OperatorHub, for the CLI method see [Section 6.2, “Uninstalling CodeReady Workspaces after OperatorHub installation using OpenShift CLI”](#).
- For CodeReady Workspaces installed using `crwctl`, see [Section 6.3, “Uninstalling CodeReady Workspaces after `crwctl` installation”](#)

6.1. UNINSTALLING CODEREADY WORKSPACES AFTER OPERATORHUB INSTALLATION USING THE OPENSIFT WEB CONSOLE

This section describes how to uninstall CodeReady Workspaces from a cluster using the OpenShift Administrator Perspective main menu.

Prerequisites

- CodeReady Workspaces was installed on an OpenShift cluster using OperatorHub.

Procedure

1. Navigate to the OpenShift web console and select the Administrator Perspective.
2. In the **Home** > **Projects** section, navigate to the project containing the CodeReady Workspaces instance.



NOTE

The default project name is `<openshift-workspaces>`.

3. In the **Operators** > **Installed Operators** section, click **Red Hat CodeReady Workspaces** in the list of installed operators.
4. In the **Red Hat CodeReady Workspaces Cluster** tab, click the displayed Red Hat CodeReady Workspaces Cluster, and select the **Delete cluster** option in the **Actions** drop-down menu on the top right.



NOTE

The default Red Hat CodeReady Workspaces Cluster name is `<red-hat-codeready-workspaces>`.

5. In the **Operators** > **Installed Operators** section, click **Red Hat CodeReady Workspaces** in the list of installed operators and select the **Uninstall Operator** option in the **Actions** drop-down menu on the top right.

- In the **Home > Projects** section, navigate to the project containing the CodeReady Workspaces instance, and select the **Delete Project** option in the **Actions** drop-down menu on the top right.

6.2. UNINSTALLING CODEREADY WORKSPACES AFTER OPERATORHUB INSTALLATION USING OPENSIFT CLI

This section provides instructions on how to uninstall a CodeReady Workspaces instance using **oc** commands.

Prerequisites

- CodeReady Workspaces was installed on an OpenShift cluster using OperatorHub.
- The **oc** tool is available.

Procedure

The following procedure provides command-line outputs as examples. Note that output in the user terminal may differ.

To uninstall a CodeReady Workspaces instance from a cluster:

- Sign in to the cluster:

```
$ oc login -u <username> -p <password> <cluster_URL>
```

- Switch to the project where the CodeReady Workspaces instance is deployed:

```
$ oc project <codeready-workspaces_project>
```

- Obtain the CodeReady Workspaces cluster name. The following shows a cluster named **red-hat-codeready-workspaces**:

```
$ oc get checluster
NAME          AGE
red-hat-codeready-workspaces 27m
```

- Delete the CodeReady Workspaces cluster:

```
$ oc delete checluster red-hat-codeready-workspaces
checluster.org.eclipse.che "red-hat-codeready-workspaces" deleted
```

- Obtain the name of the CodeReady Workspaces cluster service version (CSV) module. The following detects a CSV module named **red-hat-codeready-workspaces.v2.8**:

```
$ oc get csv
NAME                                DISPLAY          VERSION  REPLACES          PHASE
red-hat-codeready-workspaces.v2.8  Red Hat CodeReady Workspaces 2.8      red-hat-codeready-workspaces.v2.7 Succeeded
```

- Delete the CodeReady Workspaces CSV:

```
$ oc delete csv red-hat-codeready-workspaces.v2.8
clusterserviceversion.operators.coreos.com "red-hat-codeready-workspaces.v2.8" deleted
```

6.3. UNINSTALLING CODEREADY WORKSPACES AFTER CRWCTL INSTALLATION

This section describes how to uninstall an instance of Red Hat CodeReady Workspaces that was installed using the **crwctl** tool.

Prerequisites

- The **crwctl** tool is available.
- The **oc** tool is available.
- The **crwctl** tool installed the CodeReady Workspaces instance on OpenShift.

Procedure

1. Sign in to the OpenShift cluster:

```
$ oc login -u <username> -p <password> <cluster_URL>
```

2. Export the name of the CodeReady Workspaces namespace you want to remove:

```
$ export codereadyNamespace=<codeready-namespace-to-remove>
```

3. Export your user access token and Keycloak URLs:

```
$ export KEYCLOAK_BASE_URL="http://${KEYCLOAK_URL}/auth"
```

```
$ export USER_ACCESS_TOKEN=$(curl -X POST
${KEYCLOAK_BASE_URL}/realms/codeready/protocol/openid-connect/token \
-H "Content-Type: application/x-www-form-urlencoded" \
-d "username=admin" \
-d "password=admin" \
-d "grant_type=password" \
-d "client_id=codeready-public" | jq -r .access_token)
```

4. Stop the server using the UAT:

```
$ crwctl/bin/crwctl server:stop -n ${codereadyNamespace} --access-
token=${USER_ACCESS_TOKEN}
```

5. Delete your project and your CodeReady Workspaces deployment:

```
$ oc project ${codereadyNamespace}
```

```
$ oc delete deployment codeready-operator
```

```
$ oc delete checluster codeready-workspaces
```

```
❯ $ oc delete project ${codereadyNamespace}
```

6. Verify that the removal was successful by listing the information about the project:

```
❯ $ oc describe project ${codereadyNamespace}
```

7. Remove a specified **ClusterRoleBinding**:

```
❯ $ oc delete clusterrolebinding codeready-operator
```